Service Set Identifiers

In the role of an access point, a wireless device can support up to 16 service set identifiers (SSIDs). In the role of a wireless bridge, the wireless device is typically configured with one SSID. In the following sections, this module describes how to configure and manage SSIDs on the wireless device:

Understanding SSIDs

The SSID is a unique token that identifies an 802.11 wireless network. It is used by wireless devices to identify a network and to establish and maintain wireless connectivity. An SSID must be configured and assigned to a wireless client device interface before the device can associate with an access point.

Multiple SSIDs on Wireless Devices in the Access Point Role

You can configure up to 16 SSIDs on a wireless device in the role of an access point and configure a unique set of parameters for each SSID. For example, you might use one SSID to allow guests to have limited access to the network and another SSID to allow authorized users to have access to secure data.

All SSIDs are active at the same time. Client devices can associate to the access point if the wireless client device SSID matches one of the access point SSIDs configured. If the client device meets the other security requirements configured on the access point for that SSID, the client device is allowed to join a network.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2009 Cisco Systems, Inc. All rights reserved.

SSIDs on Wireless Devices in Other Roles

In the role of a wireless bridge, typically the bridges are configured with one SSID because a bridge does not associate wirelessly with clients. (A wireless device in the role of a workgroup bridge can associate with wireless clients and might be configured with multiple SSIDs. For a complete description of wireless device roles, see the “Roles and the Associations of Wireless Devices” module.)

Configuring SSIDs

SSIDs are created globally and then assigned to an interface. The SSID is inactive until you use the **ssid** configuration command in interface mode to assign the SSID to a specific radio interface.

In Cisco IOS Release 12.3(4)JA and later, you can configure SSIDs globally or on a specific radio interface. When you create an SSID using the **ssid** interface command, the access point stores the SSID in global configuration mode.

SSID Parameters

These are the parameters you can configure for each SSID:

- Guest mode
- VLAN
- Client authentication method

Note For detailed information on supported client authentication types, see the software configuration guide for your wireless device.

- Maximum number of client associations
- RADIUS accounting for traffic using the SSID
- Redirection of packets received from client devices

If your network uses VLANs, you can assign one SSID to a VLAN. Client devices that use the SSID are grouped in that VLAN.

Using Spaces in SSIDs

In Cisco IOS Release 12.4 and later, you can include spaces in an SSID. Trailing spaces (spaces at the end of an SSID) are invalid. However, earlier versions of Cisco IOS did allow SSIDs to include trailing spaces. Trailing spaces made it appear that you had identical SSIDs configured on the access point; however, the trailing spaces made each SSID unique.

For example, in the following sample output from a **show configuration** command in privileged EXEC mode, there are no spaces shown in the SSIDs:

```
ssid buffalo
    vlan 77
    authentication open
```

```
ssid buffalo
    vlan 17
    authentication open

ssid buffalo
    vlan 7
    authentication open
```

The SSIDs appear to be identical, but in fact they are unique as a result of trailing spaces. Spaces are shown in the SSIDs in the following sample output from a **show dot11 associations** command in privileged EXEC mode:

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

Note The **show dot11 associations** command shows only the first 15 characters of the SSID. Use the **show dot11 associations client** command to see SSIDs that have more than 15 characters.

Creating a Global SSID

To create an SSID, use the **dot11 ssid** command in global configuration mode. Then you can assign the SSID to a specific interface by using the **ssid** configuration command in interface mode.

After an SSID is created in global configuration mode, you use the **ssid** configuration command to attach the SSID to an interface without entering SSID configuration mode. If you create an SSID on the interface (in interface mode) rather than in global configuration mode, the **ssid** command puts you into SSID configuration mode for the new SSID.

Note SSIDs created in Cisco IOS Releases 12.4 or later become invalid if you downgrade the Cisco IOS software to an earlier release.

To create a global SSID, follow these steps, beginning in privileged EXEC mode. After you create an SSID, you can assign it to specific radio interfaces.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Creates a global SSID and enters SSID configuration mode for this SSID. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. The first character cannot be the !, #, or ; character. The +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.
Step 3	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface to which you want to assign the SSID.

Step 4	**ssid** *ssid-string*	Assigns the global SSID that you created in Step 2 to the radio interface. Use the **no** form of the command to disable the SSID.
Step 5	**end**	Returns to privileged EXEC mode.

SSID Configuration Example

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 Global SSIDs

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

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

Guest Mode SSID

The guest mode SSID is included in beacon frames, in responses to probe requests without an SSID that matches the other access point SSIDs, and in responses to probe requests with a wildcard SSID. Enabling guest mode for an SSID helps clients that passively scan (do not transmit probe requests) to associate with the access point. The access point can have one guest mode SSID or none at all. (See the "Multiple Basic SSIDs" section on page 8 to see how to include multiple SSIDs in a beacon.)

If no guest mode SSID exists, the access point beacon contains no SSID, and probe requests with a wildcard SSID are ignored. Disabling the guest mode makes networks slightly more secure.

To enable a guest mode SSID, create the SSID and use the **guest-mode** command. For example:

```
AP(config-if-ssid)# guest-mode
```

To disable a guest mode SSID, use the **no guest-mode** command.

Note When you enable guest mode SSID for the 802.11g radio, you will enable guest mode for the 802.11b radio as well, because they both operate in the same 2.4-Ghz band.

Guest Mode SSID Configuration Example

This example shows how to:

- Name an SSID
- Configure the SSID for guest mode
- Assign the SSID to a radio interface

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# guest-mode
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

Including an SSID in an SSIDL IE

The access point beacon can advertise only one SSID. However, you can use a service set identification list (SSIDL), information element (IE) 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 that are required to associate using that SSID.

Note When multiple basic service set identifiers (BSSIDs) are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities. (See the "Multiple Basic SSIDs" section on page 8 to see how to include multiple SSIDs in a beacon.)

To include an SSID in an SSIDL IE, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enters configuration mode for a specific SSID.
Step 4	**information-element ssidl** [**advertisement**] [**wps**]	Includes 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 **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 **information-element ssidl** command to disable SSIDL IEs.

Assigning IP Redirection for an SSID

IP redirection for an SSID on an access point redirects all packets sent from client devices associated to that SSID to a specific IP address.

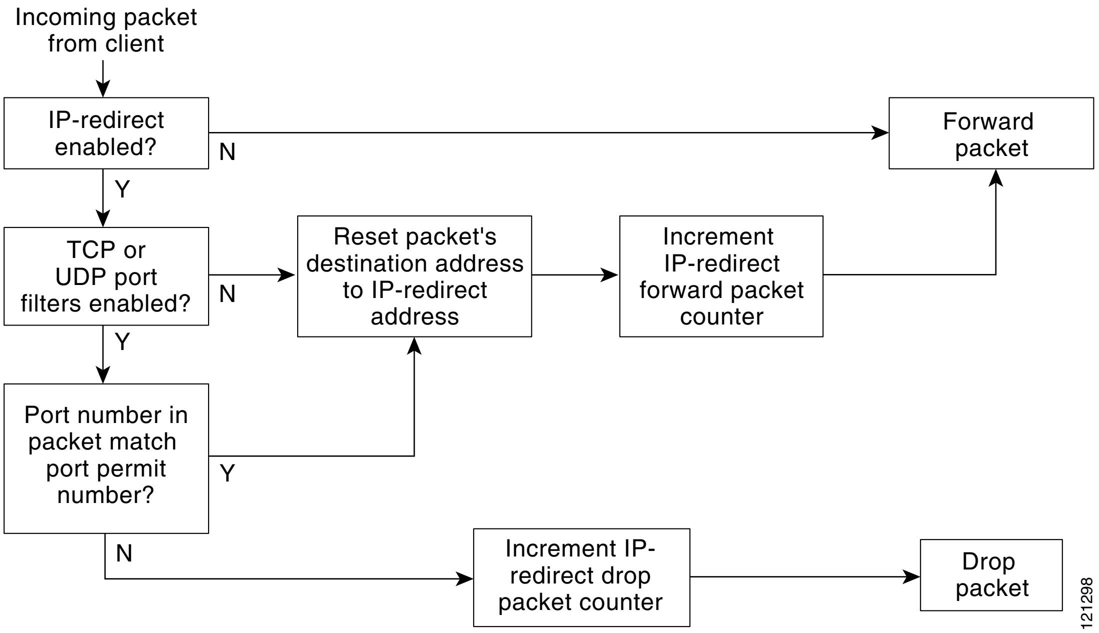
You can redirect all packets from client devices that are associated using an SSID, or you can redirect only packets that are directed to specific TCP or User Datagram Protocol (UDP) ports. When you configure the access point to redirect only the packets that are addressed to specific ports, the access point redirects those packets from clients using the SSID and drops all other packets from clients.

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.

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

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

Figure 1 Processing Flow for IP Redirection


Incoming packet from client
IP-redirect enabled?
N
Forward packet
Y
TCP or UDP port filters enabled?
N
Reset packet's destination address to IP-redirect address
Increment IP-redirect forward packet counter
Y
Port number in packet match port permit number?
Y
N
Increment IP-redirect drop packet counter
Drop packet
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 from client devices.
- Access control list parameters take precedence over IP redirection.

Configuring IP Redirection

To configure IP redirection for an SSID, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enters configuration mode for a specific SSID.
Step 4	**ip redirection host** *ip-address*	Enters IP-redirect configuration mode for the IP address. 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	**ip redirection host** *ip-address* **access-group** *acl* **in**	(Optional) Specifies 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 parameters defined in the ACL. The **in** parameter specifies that the ACL is applied to the incoming interface of 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 bridge group virtual interface (BVI) as long as a separate ACL is used for the BVI.

The following 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* to the IP address:

```
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
```

The following example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL applied to the BVI1 interface. When the access point receives packets from client devices associated by using the SSID *robin*, it redirects packets sent to the specified ports to the IP address and discards all other packets:

```
AP# configure terminal
AP(config)# interface bvi1
AP(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
AP(config-if-ssid)# end
```

Multiple Basic SSIDs

Standard beacons or responses to probe responses to probe requests with no SSID or a wildcard SSID contain only one SSID—the guest-mode SSID if a guest-mode SSID is configured. When multiple basic SSIDs (MBSSIDs) are enabled, all the SSIDs are included in the beacon. Cisco 802.11a, 802.11b/g, and 802.11n radios support up to 8 BSSIDs.

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, hot standby units, or workgroup bridges) might lose their association when you add or delete an MBSSID. When you add or delete an MBSSID, 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.

Configuring Multiple Basic SSIDs

This section describes how to enable MBSSIDs on an access point radio interface.

Requirements for Configuring Multiple BSSIDs

To configure MBSSIDs, your access points must meet these minimum requirements:

- VLANs must be configured.
- Access points must run Cisco IOS Release 12.4 or later.
- Wireless devices must contain a radio that supports MBSSIDs. To determine whether a radio supports MBSSIDs, enter the **show controllers** *radio_interface* command. The radio supports MBSSIDs 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 MBSSIDs:

- RADIUS-assigned VLANs are not supported when you enable MBSSIDs.
- 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 MBSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

- The guest-mode SSID and delivery traffic indicator message (DTIM) period configured in this command are applied only when MBSSIDs are enabled on the radio interface.

  When client devices receive a beacon that contains a DTIM, they “wake up” to check for pending packets. Longer intervals between DTIMs let battery-powered 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.
- 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.
- If you configure a DTIM period for a BSSID and you also use the **beacon** command to configure a DTIM period for the radio interface, the BSSID DTIM period takes precedence.
- Any Wi-Fi-certified client device can associate to an access point by using MBSSIDs.
- You can enable MBSSIDs on access points that participate in wireless domain services (WDS).

Steps for Configuring MBSSIDs on an Interface

To configure MBSSIDs on an interface, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *radio-interface*	Enters interface configuration mode for the radio interface to which you want to assign the SSID.
Step 3	**mbssid**	Enables MBSSIDs on the interface. You can also use the **dot11 mbssid** global configuration command to simultaneously enable MBSSIDs on all radio interfaces that support MBSSIDs.
Step 4	**exit**	Exits interface configuration mode.
Step 5	**dot11 ssid** *ssid-string*	Creates a global SSID and enter SSID configuration mode for this SSID. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. The first character cannot be the !, #, or ; character. The +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.
Step 6	**mbssid [guest-mode] [dtim-period** *period***]**	Enters the **mbssid** command in interface configuration mode to include the SSID name in the beacon and broadcast probe response and to configure the DTIM period for the SSID. The default DTIM period is 2, which means that every other beacon contains a DTIM. Include the **guest-mode** parameter to include the SSID in the beacon. Guest mode is disabled by default.
Step 7	**exit**	Exits interface configuration mode.
Step 8	**interface** *radio-interface*	Enters interface configuration mode for the radio interface to which you want to assign the SSID.

	Command	Purpose
Step 9	**ssid** *ssid-string*	Assigns the SSID to the radio interface. Use the **no** form of the command to disable the SSID on this interface.
Step 10	**exit**	Exits interface configuration mode.

The following example shows how 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
- Assign the SSID *visitor* to the radio interface

```
ap# configure terminal
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
```

Displaying Configured BSSIDs

To display the relationship between SSIDs and BSSIDs or MAC addresses, use the **show dot11 bssid** command in privileged EXEC mode . The following is sample output for the command:

```
AP1230# show dot11 bssid
Interface     BSSID           Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

Using a RADIUS Server for SSID Authorization

To prevent unauthorized client devices from associating to the access point, you can create a list of authorized SSIDs on your RADIUS authentication server.

The RADIUS SSID authorization process consists of these steps:

1. A client device associates to the access point using any SSID that is 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 any other 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 list of SSIDs from the RADIUS server are in the form of Cisco vendor-specific attributes (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). 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 vendor-ID for Cisco 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 “RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values” chapter of the Cisco IOS Security Configuration Guide at the following URL:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vsa_rad_discnct_ps6350_TSD_Products_Configuration_Guide_Chapter.html

To create a global SSID with RADIUS accounting, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Creates a global SSID and enter SSID configuration mode for this SSID. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. The first character cannot be the !, #, or ; character. The +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.

Step 3	**accounting** *list-name*	Enables 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 4	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface to which you want to assign the SSID.
Step 5	**ssid** *ssid-string*	Assigns the global SSID that you created in Step 2 to the radio interface. Use the **no** form of the command to disable the SSID.
Step 6	**end**	Returns to privileged EXEC mode.

Network Admission Control 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 are needed to help ensure that all wired and wireless devices that attempt to access a network meet corporate security policies. Infected or vulnerable endpoints must be automatically detected, isolated, and cleaned.

Network Admission Control (NAC) ensures that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) that access network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices that access 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.

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 noncompliant WLAN clients and provide remediation services to help ensure compliance.

Based on its health (software version, virus version, and so on) a client is placed on a separate VLAN that downloads the software required for upgrading the client to the software versions required for accessing the network. Four VLANs are specified for NAC support, one of which is the normal VLAN in which clients with 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 three 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 to 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 three 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 two different SSIDs per interface.

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

Dot11 subinterfaces are generated and configured automatically along with the dot1q encapsulation VLAN (equal to the number of configured VLANs). The subinterfaces on the wired side are also configured automatically, along with the bridge-group configurations under the FE0 subinterface.

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's SSID. If the VLAN is not one of the configured backup VLANs, the client is disassociated.

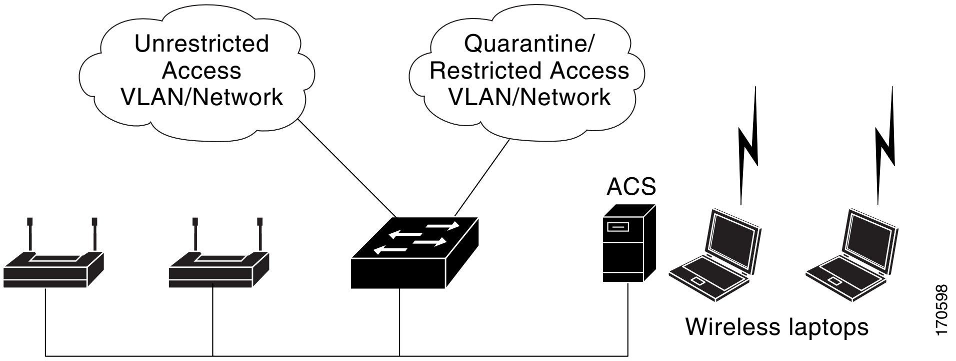
Data corresponding to the all the backup VLANs are sent and received using the BSSID that is assigned to the SSID. Therefore, all clients (healthy and unhealthy) listening to the BSSID corresponding with the SSID "wake up." If the multicast key being used corresponds to the VLAN (healthy or unhealthy),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

Configuring NAC

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 2 shows a typical network setup.

Figure 2 Typical NAC Network Setup


Unrestricted Access VLAN/Network
Quarantine/ Restricted Access VLAN/Network
ACS
Wireless laptops
170598

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

http://cisco.com/en/US/netsol/ns617/networking_solutions_sub_solution_home.html

To configure NAC for MBSSIDs on your access point, follow these steps:

Step 1 Configure your network as shown in Figure 2.

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
```