VLANs on Aironet Access Points Configuration Example

Document ID: 69773

Contents

Introduction

This document provides a configuration example that shows how to configure VLANs on Cisco Aironet Access Points (APs) with use of the command−line interface (CLI).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of the basic configuration of Aironet APs
- Knowledge of the configuration of the Aironet 802.11a/b/g Client Adapter with the Aironet Desktop Utility
- Basic knowledge of the configuration of Cisco Catalyst switches and Cisco routers

Components Used

The information in this document is based on these software and hardware versions:

- Aironet 1240AG Series AP that runs Cisco IOS® Software Release 12.4(3g)JA1
- Aironet 802.11a/b/g Client Adapter
- Aironet Desktop Utility that runs firmware version 2.5
- Catalyst 2950 switch that runs Cisco IOS Software Release 12.1(19)EA1
- 2800 ISR Router that runs Cisco IOS Software Release 12.4(11)T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

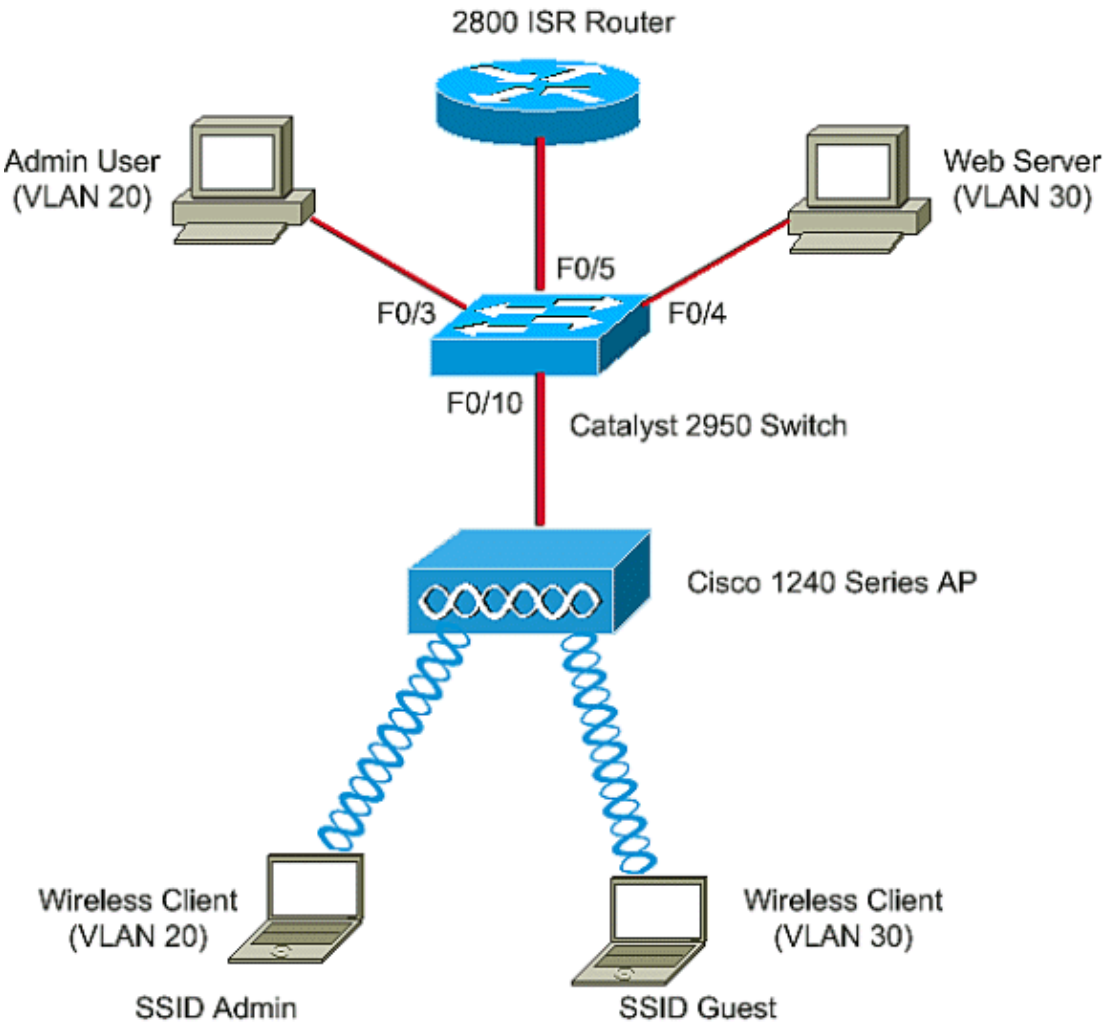
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Network Diagram

This document uses this network setup.

An Aironet 1200 Series AP has three VLANs VLAN 2, VLAN 20, and VLAN 30. The setup in this document uses VLAN 2 as the native VLAN, VLAN 20 for the administrative (admin) department, and VLAN 30 for guest users. Wireless users who belong to the admin department must connect to the AP and should be able to connect to the admin department users on the wired network (on VLAN 20). The wireless guest users must be able to connect to a web server that is on the wired segment on VLAN 30. A Catalyst 2950 switch connects the AP to the wired network. A 2800 ISR router connects to the same switch and acts as a DHCP server for wireless clients that belong to VLAN 20 and VLAN 30. The router needs to assign IP addresses to clients from their respective subnet. You must configure the AP, Catalyst switch, and the router for an implementation of this setup.



Below is the list of IP addresses used for the devices in the document. All the IP addresses use /24 subnet

mask

- AP Bridge−Group Virtual Interface (BVI) IP address (VLAN 2)¡72.16.1.20
- Wireless client (SSID Admin) that connects to VLAN 20 gets an IP address from the DHCP server of the router from the subnet 172.16.2.0
- Wireless client (SSID Guest) that connects to VLAN 30 gets an IP address from the DHCP server of the router from the subnet 172.16.3.0
- Admin user on the wired network on VLAN 20¡72.16.2.60 (Static IP)
- Web server on VLAN 30¡72.16.3.60 (Static IP)
- Sub−interface of the router in VLAN 2¡72.16.1.1
- Sub−interface of the router in VLAN 20¡72.16.2.1
- Sub−interface of the router in VLAN 30¡72.16.3.1

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

In order to configure the AP to connect to a specific VLAN, you must configure the service set identifier (SSID) to recognize the VLAN. Either a VLAN ID or a name identifies a VLAN. Therefore, if you configure the SSID on an AP to recognize a specific VLAN ID or name, you can establish a connection to the VLAN. After establishment of the connection, the wireless clients that connect to the AP with use of the specific SSID are assigned to that VLAN. Because you can configure up to 16 SSIDs on an AP, you can create 16 VLANs on an AP. In order to configure VLANs on APs and establish connectivity, you must complete these steps:

1. Configure the native VLAN on the AP.
2. Configure VLANs for the guest users and the admin users on the AP.
3. Configure the Catalyst switch.
4. Configure the router

Configure the Native VLAN on the AP

The VLAN, to which the Access Point itself and other infrastructure devices such as the switch, to which the access point connects, is called native VLAN. Native VLAN of the Access Point is usually different from other VLANs configured on the Access Point. It is **BVI interface**, which is used for the management of the Access Point that is assigned an IP address in the native VLAN subnet. The traffic, for example, management traffic, sent to and by the Access Point itself assumes the native VLAN, and it is untagged. All untagged traffic that is received on an IEEE 802.1Q (dot1q) trunk port is forwarded with the native VLAN that is configured for the port. If a packet has a VLAN ID that is the same as the native VLAN ID of the sending port, the switch sends the packet without a tag. Otherwise, the switch sends the packet with a tag.

In order to configure a native VLAN on an AP, issue these commands in global configuration mode on the AP:

```
AccessPoint<config>#interface fastethernet 0.2
AccessPoint<config−subif>#encapsulation dot1q 2 native

!−−− Configure the encapsulation as dot1q and assign VLAN 2 as the native VLAN
!−−− on the Fast Ethernet interface.

AccessPoint<config−subif>#exit
AccessPoint<config>#interface dot11radio 0.2
AccessPoint<config−subif>#encapsulation dot1q 2 native
```

```
!--- Configure the encapsulation as dot1q and assign VLAN 2 as the native VLAN
!--- on the radio interface.

AccessPoint<config-subif>#end
```

Configure VLANs for Guest Users and Admin Users on the AP

Here, you need to configure two VLANs, one for the guest users and the other for the admin department users. You also need to associate the SSID to the specific VLANs. This example configures:

- VLAN 20 for the admin department and uses the SSID **Admin**
- VLAN 30 for guest users and uses the SSID **Guest**

In order to configure these VLANs, enter these commands in global configuration mode:

```
AccessPoint#configure terminal

!--- Enter global configuration mode.

AccessPoint(config)#interface dot11radio 0

!--- Enter radio interface configuration mode.

AccessPoint(config-if)#ssid Admin

!--- Configure the SSID "Admin".

AccessPoint(config-if-ssid)#vlan 20

!--- Assign VLAN 20 to the SSID.

AccessPoint(config-if-ssid)#authentication open

!--- Configure open authentication for the SSID.

AccessPoint(config-if-ssid)#end

AccessPoint(config) interface fastethernet 0.20

!--- Enter subinterface mode on the Fast Ethernet interface.

AccessPoint(config-subif) encapsulation dot1Q 20

!--- Set the encapsulation as dot1q for VLAN 20.

AccessPoint(config-subif) bridge-group 20

!--- Assign the subinterface to bridge group 20.

AccessPoint(config-subif) exit

AccessPoint(config) interface dot11radio 0.20

!--- Enter subinterface mode on the radio interface.

AccessPoint(config-subif) encapsulation dot1Q 20

!--- Set the encapsulation as dot1q for VLAN 20.

AccessPoint(config-subif) bridge-group 20

!--- Assign the subinterface to bridge group 20.
```

```
AccessPoint(config-subif) exit
```

Repeat the same procedure in order to configure VLAN 30 for the admin users:

```
AccessPoint#configure terminal
AccessPoint(config)#interface dot11radio 0
AccessPoint(config-if)#ssid Guest
AccessPoint(config-if-ssid)#vlan 30
AccessPoint(config-if-ssid)#authentication open
AccessPoint(config-if-ssid)#end

AccessPoint(config) interface fastethernet 0.30
AccessPoint(config-subif) encapsulation dot1Q 30
AccessPoint(config-subif) bridge-group 30
AccessPoint(config-subif) exit

AccessPoint(config) interface dot11radio 0.30
AccessPoint(config-subif) encapsulation dot1Q 30
AccessPoint(config-subif) bridge-group 30
AccessPoint(config-subif) exit
```

Note: This document uses open authentication for both SSIDs Admin and Guest. The authentication types are tied to the SSIDs that you configure for the AP. For information on how to configure different authentication types on the AP, refer to Configuring Authentication Types.

Configure the Catalyst Switch

The next step is to configure the switch ports which will connect the APs and the router to the wired network. You should configure the switch port which connects to the AP and the router as a trunk port because this port carries traffic from all VLANs on the wireless network. In this example, the VLANs are VLAN 20, VLAN 30, and the native VLAN 2. When you configure the switch port, which connects to the AP and the router, ensure that the native VLANs that you configure match the native VLAN on the AP and the router. Otherwise, frames are dropped. In order to configure the trunk port on the switch, issue these commands from the CLI on the switch:

Note: This document uses the Catalyst 2950 switch. The configurations on the switch port can vary, which depends on the switch model that you use. As shown in the diagram, interface fastethernet **0/5** connects to the **Router**, and interface fastethernet **0/10** connects to the **Access Point**.

```
Switch#configure terminal
Switch<config>#interface fastethernet 0/5

!--- Enter the interface mode for Fast Ethernet 0/5.

Switch<config-if>#switchport mode trunk

!--- Configure the switch port mode to trunk mode.

Switch<config-if>#switchport trunk encapsulation dot1q

!--- Configure the encapsulation on the switch port to dot1q.

Switch<config-if>#switchport trunk native vlan 2

!--- Configure the native VLAN as VLAN 2.

Switch<config-if>#switchport trunk allowed vlan add 2,20,30

!--- Configure the list of VLANs that are allowed on the trunk port.
```

```
Switch<config-if>#switchport nonegotiate


Switch#configure terminal
Switch<config>#interface fastethernet 0/10

!--- Enter the interface mode for Fast Ethernet 0/10

Switch<config-if>#switchport mode trunk

!--- Configure the switch port mode to trunk mode.

Switch<config-if>#switchport trunk encapsulation dot1q

!--- Configure the encapsulation on the switch port to dot1q.

Switch<config-if>#switchport trunk native vlan 2

!--- Configure the native VLAN as VLAN 2.

Switch<config-if>#switchport trunk allowed vlan add 2,20,30

!--- Configure the list of VLANs that are allowed on the trunk port.

Switch<config-if>#switchport nonegotiate
```

Note: Cisco IOS Software−based Aironet wireless equipment does not support Dynamic Trunking Protocol (DTP). Therefore, the switch must not try to negotiate DTP.

Configure the Router

The router is configured as the DHCP server for the wireless clients in VLAN 20 and VLAN 30. The router has three sub−interfaces, one for each VLAN 2, 20, and 30 so that it can assign IP addresses to clients in the subnet of their respective VLAN and perform inter−VLAN routing.

```
Router#configure terminal
Router<config>#interface fastethernet 0/0.2

!--- Configures a Sub-interface .2 on fastethernet 0/0

Router<config-subif>#encapsulation dot1q 2 native

!--- configures the encapsulation as dot1q and assigns VLAN 2 to the sub-interface
This command also makes VLAN 2 as the Native VLAN. Here number 2 is the VLAN-id.

Router<config-subif>#ip address 172.16.1.1 255.255.255.0

!--- Assign ip address from Native VLAN 2 subnet - 172.16.1.0 /24 to the sub-interface

Router<config-subif>#exit
Router<config>#interface fastethernet 0/0.20

!--- Configures a Sub-interface .20 on fastethernet 0/0

Router<config-subif>#encapsulation dot1q 20

!--- configures the encapsulation as dot1q and assigns VLAN 20 to the sub-interface
Here number 20 is the VLAN-id.

Router<config-subif>#ip address 172.16.2.1 255.255.255.0

!--- Assign ip address from  VLAN 20 subnet - 172.16.2.0 /24 to the sub-interface

Router<config-subif>#exit
```

```
Router<config>#interface fastethernet 0/0.30

!--- Configures a Sub-interface .30 on fastethernet 0/0

Router<config-subif>#encapsulation dot1q 30

!--- configures the encapsulation as dot1q and assigns VLAN 30 to the sub-interface
Here number 30 is the VLAN-id.

Router<config-subif>#ip address 172.16.3.1 255.255.255.0

!--- Assign ip address from  VLAN 30 subnet - 172.16.3.0 /24

Router<config-subif>#exit


DHCP Configuration starts here

Router<config>#ip dhcp excluded-address 172.16.2.1
Router<config>#ip dhcp excluded-address 172.16.3.1

!--- excluded-address command is used to exclude the specified ip addresses
from the DHCP pool. In this case router's  sub-interface addresses are excluded.

Router<config>#ip dhcp pool pool1

!--- Creates a DHCP pool with a name pool1 and enters the DHCP config mode

router<dhcp-config>#network 172.16.2.0 /24

!--- From this pool Clients are assigned ip addresses from  172.16.2.0 /24 Subnet i.e. fro

router<dhcp-config>#default-router 172.16.2.1

!--- Default-gateway assigned to the client from this pool is 172.16.2.1 . Default-router

Router<config>#ip dhcp pool pool2

!--- Creates a DHCP pool with a name pool2 and enters the DHCP config mode

router<dhcp-config>#network 172.16.3.0 /24

!--- From this pool Clients are assigned ip addresses from  172.16.3.0 /24 Subnet i.e. fro

router<dhcp-config>#default-router 172.16.3.1

!--- Default-gateway assigned to the client from this pool is 172.16.3.1 .
```

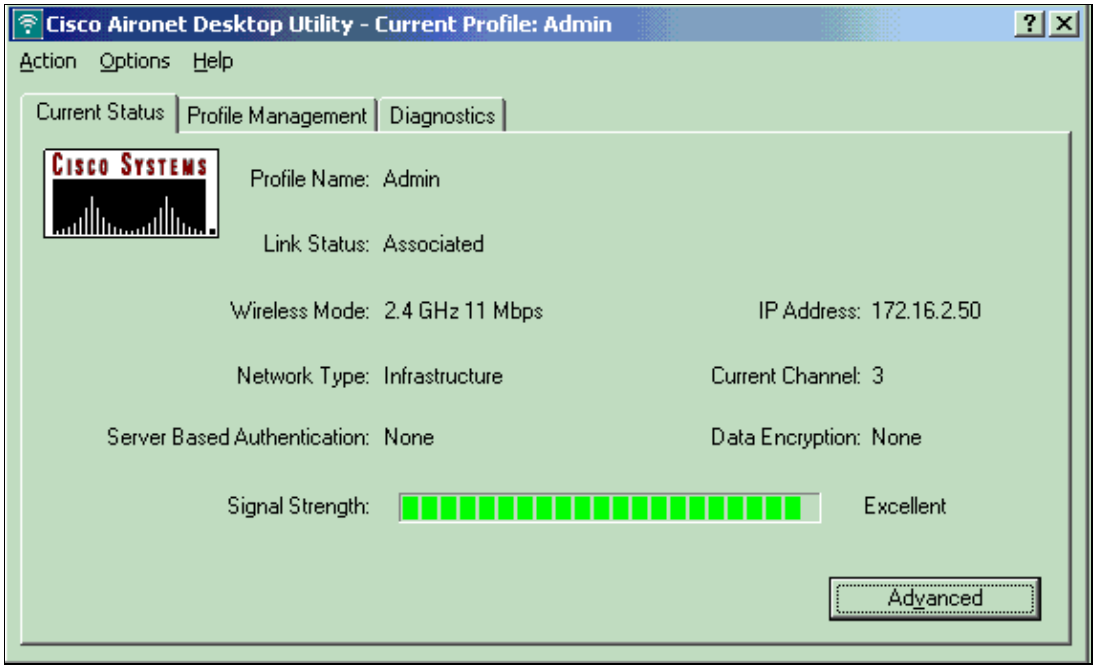
Verify

Use this section to confirm that your configuration works properly.

You can check if the configuration works as expected. The wireless client (admin user) who is configured with SSID **Admin** must get connected to VLAN 20. The same user should be able to connect to the admin user on the wired network, which is also on the same VLAN. In order to verify, activate the wireless client profile for the Admin user.

Note: This document does not explain how to configure the wireless client in order to set up profiles. For information on how to configure the wireless client adapter, refer to Configuring the Client Adapter.

This example window shows that the wireless client is associated to the AP:



The **show dot11 associations** command on the AP also verifies that the client gets connected to VLAN 10:

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

```
AccessPoint#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Admin] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 172.16.2.50     CB21AG/PI21AG Admin User      self           Assoc
```

You can issue the **show vlans** command on the AP in order to display the VLANs that are configured on the AP. Here is an example:

```
AccessPoint#show vlans

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.2
FastEthernet0.2

This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1              1380                712
        Other                                         0                 63

   0 packets, 0 bytes input
   733 packets, 50641 bytes output
```

```
        Bridging        Bridge Group 1               1380                 712
        Other                                          0                  63

   1381 packets, 98016 bytes input
   42 packets, 12517 bytes output

Virtual LAN ID:  20 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.20
FastEthernet0.20

   Protocols Configured:   Address:             Received:        Transmitted:
        Bridging        Bridge Group 20              798                 622
        Other                                          0                  19

   247 packets, 25608 bytes input
   495 packets, 43585 bytes output
        Bridging        Bridge Group 20              798                 622
        Other                                          0                  19

   552 packets, 37536 bytes input
   148 packets, 21660 bytes output

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.30
FastEthernet0.30

   Protocols Configured:   Address:             Received:        Transmitted:
        Bridging        Bridge Group 30              693                 609
        Other                                          0                  19

   106 packets, 13373 bytes input
   517 packets, 48029 bytes output
        Bridging        Bridge Group 30              693                 609
        Other                                          0                  19

   605 packets, 47531 bytes input
   112 packets, 15749 bytes output
```

You can now check if the wireless admin user is able to connect to the admin user on the wired side, which is configured for the same VLAN. Issue the **ping** command on the wireless client. Here is an example:

```
D:\>ping 172.16.2.60

Pinging 172.16.2.60 with 32 bytes of data:

Reply from 172.16.2.60: bytes=32 time<10ms TTL=255
Reply from 172.16.2.60: bytes=32 time<10ms TTL=255
Reply from 172.16.2.60: bytes=32 time<10ms TTL=255
Reply from 172.16.2.60: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.2.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Similarly, you can check if the guest users get connected to VLAN 30. You can issue the **ping** command on the guest wireless client in order to test the connectivity to the web server on the wired side. Here is an example:

```
D:\>ping 172.16.3.60

Pinging 172.16.3.60 with 32 bytes of data:
```

```
Reply from 172.16.3.60: bytes=32 time<10ms TTL=255
Reply from 172.16.3.60: bytes=32 time<10ms TTL=255
Reply from 172.16.3.60: bytes=32 time<10ms TTL=255
Reply from 172.16.3.60: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.3.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Troubleshoot

Use this section to troubleshoot your configuration.

Troubleshooting Procedure

Follow these instructions in order to troubleshoot your configuration:

1. Check if the native VLAN that is configured on the switch port and connected to the AP matches the native VLAN of the AP.

   If there is a mismatch in the native VLAN, connectivity through the switch does not happen.
2. Ensure that all the VLANs that are configured on the wireless side are allowed on the switch port that is configured as the trunk.

   By default, all VLANs are allowed through the trunk port.
3. Check if the **bridge−group** command is configured on all the VLANs except the native VLAN.

   You do not need to configure a bridge group on the subinterface that you set up as the native VLAN. This bridge group is automatically moved to the native subinterface in order to maintain the link to BVI 1, which represents both the radio and Ethernet interfaces.

   Caution: When you configure the **bridge−group** command, these commands automatically get enabled:

   ```
   bridge-group 10 subscriber-loop-control
   bridge-group 10 block-unknown-source
   no bridge-group 10 source-learning
   no bridge-group 10 unicast-flooding
   bridge-group 10 spanning-disabled
   ```

   These are standard default settings, and you should not change them unless you are directed. If you remove these commands, the WLAN can fail to function as expected.

Troubleshooting Commands

You can also use these commands in order to troubleshoot your configuration on the AP:

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show vlans**
- **show vlans dot1q**
- **show dot11 associations**

On the Catalyst 2950 switch, you can use these commands in order to troubleshoot the configuration:

- **show vlans**
- **show interface fastethernet** *x*/*x* **switchport**
- **show interface fastethernet** *x*/*x* **trunk**

On the router, issue these commands in order to troubleshoot the configuration.

- **debug ip dhcp server packet**
- **show ip interface brief**

Here is an output of successful IP−address assignment to the client in SSID **Admin**.

```
Router#debug ip dhcp server packet
*Nov 23 18:02:06.637: DHCPD: DHCPREQUEST received from client 0040.96ac.e657.

!−−− Router receives the DHCP Request from the client

*Nov 23 18:02:06.637: DHCPD: No default domain to append − abort update
*Nov 23 18:02:06.637: DHCPD: Sending DHCPACK to client 0040.96ac.e657 (172.16.2.50).

!−−− Router acknowledges the client's request

*Nov 23 18:02:06.637: DHCPD: creating ARP entry (172.16.2.2, 0040.96ac.e657).
*Nov 23 18:02:06.637: DHCPD: unicasting BOOTREPLY to client 0040.96ac.e657 (172.16.2.50).

!−−− Router assigns ip address to the client from the VLAN 10 subnet
```

Related Information

- **Using VLANs with Cisco Aironet Wireless Equipment**
- **EAP Authentication with RADIUS Server**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 21, 2008 Document ID: 69773