Using VLANs with Cisco Aironet Wireless Equipment

Document ID: 46141

In order to get Cisco Aironet drivers, firmware and utility software, use this link to the Cisco Wireless Downloads.

Introduction

This document provides a sample configuration to use virtual LANs (VLANs) with Cisco Aironet wireless equipment.

Prerequisites

Requirements

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

- Familiarity with Cisco Aironet wireless equipment
- Familiarity with LAN switching concepts of VLANs and VLAN trunking

Components Used

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

- Cisco Aironet Access Points and Wireless Bridges
- Cisco Catalyst Switches

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.

Related Products

You can use the switch side of this configuration with any of these hardware or software:

- Catalyst 6x00/5x00/4x00 that runs CatOS or IOS
- Catalyst 35x0/37x0/29xx that runs IOS
- Catalyst 2900XL/3500XL that runs IOS

Conventions

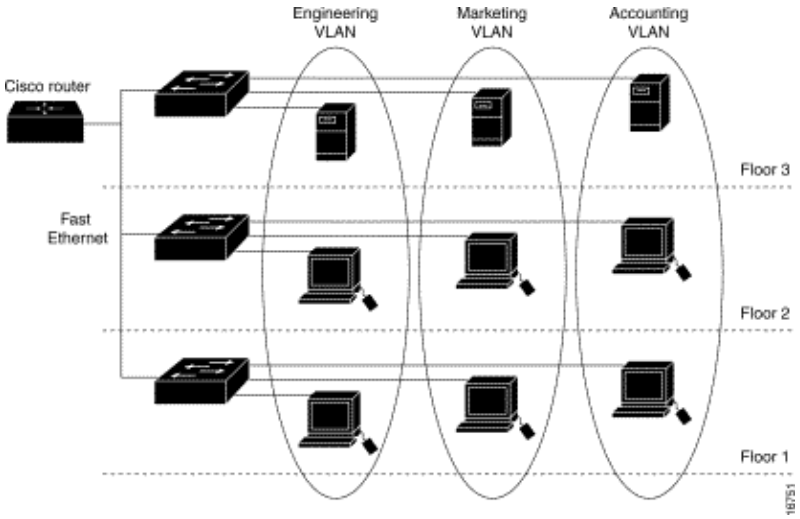
Refer to Cisco Technical Tips Conventions for more information on document conventions.

VLANs

A VLAN is a switched network that is logically segmented by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they can be intermingled with other teams. Use VLANs to reconfigure the network through software rather than physically unplug or move the devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment, such as LAN switches, that operate bridging protocols between them with a separate group for each VLAN.

When you connect a device to a Cisco Catalyst switch, the port where the device is connected is a member of VLAN 1. The MAC address of that device is a part of VLAN 1. You can define multiple VLANs on a single switch, and you can configure a switch port on most Catalyst models as a member of multiple VLANs.



When the number of ports in a network exceeds the port capacity of the switch, you must cross−connect multiple switch chassis, which defines a trunk. The trunk is not a member of any VLAN, but a conduit over which traffic passes for one or more VLANs.

In fundamental terms, the key in the configuration of an access point to connect to a specific VLAN is to configure its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID or name, it follows that, if the SSID on an access point is configured to recognize a specific VLAN ID or name, a connection to the VLAN is established. When this connection is made, associated wireless client devices that have the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point, so you can support up to 16 VLANs. You can assign only one SSID to a VLAN.

You extend VLANs into a wireless LAN when you add IEEE 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets that come from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

For example, employees and guests can access the wireless network of a company at the same time and be administratively separate. A VLAN maps to an SSID, and the wireless client attaches to the appropriate SSID. In networks with wireless bridges, you can pass multiple VLANs across the wireless link in order to provide connectivity to a VLAN from separate locations.

If 802.1q is configured on the FastEthernet interface of an access point, the access point always sends keepalives on VLAN1 even if VLAN 1 is not defined on the access point. As a result, the Ethernet switch connects to the access point and generates a warning message. There is no loss of function on either the access point or the switch, but the switch log contains meaningless messages that can cause more important messages to be wrapped and not seen.

This behavior creates a problem when all SSIDs on an access point are associated to mobility networks. If all SSIDs are associated to mobility networks, the Ethernet switch port to which the access point is connected can be configured as an access port. The access port is normally assigned to the native VLAN of the access point, which is not necessarily VLAN1. This causes the Ethernet switch to generate warning messages noting that traffic with an 802.1q tag is sent from the access point.

You can eliminate the excessive messages on the switch if you disable the keepalive function.

If you ignore minor points in these concepts when you deploy VLANs with Cisco Aironet wireless equipment, you can experience unexpected performance, for example:

- The failure to limit allowed VLANs on the trunk to those defined on the wireless device

  If VLANs 1, 10, 20, 30 and 40 are defined on the switch, but only VLANs 1, 10 and 30 are defined on the wireless equipment, you must remove the others from the trunk switchport.
- Misuse of the designation of infrastructure SSID

  When you install access points, only assign the infrastructure SSID when you use an SSID on:

  - ♦ workgroup bridge devices
  - ♦ repeater access points
  - ♦ non−root bridges

  It is a misconfiguration to designate the infrastructure SSID for an SSID with only wireless laptop computers for clients, and causes unpredictable results.

  In bridge installations, you can only have one infrastructure SSID. The infrastructure SSID must be the SSID that correlates to the Native VLAN.
- Misuse or incorrect design of guest mode SSID designation

  When you define multiple SSIDs/VLANs on Cisco Aironet wireless equipment, one (1) SSID can be assigned as guest mode SSID with the SSID broadcast in 802.11 radio beacons. The other SSIDs are not broadcast. The client devices must indicate which SSID to connect.
- Failure to recognize that multiple VLANs and SSIDs indicate multiple OSI Model Layer 3 subnets

  Deprecated versions of Cisco Aironet software permit binding multiple SSIDs to one VLAN. Current versions do not.
- OSI Model Layer 3 routing failures or incorrect designs

  Each SSID and its linked VLAN must have a routing device and some source to address clients, for example a DHCP server or the scope on a DHCP server.
- Misunderstand or incorrectly configure Native VLAN

  The routers and switches that make up the physical infrastructure of a network are managed in a different method than the client PCs that attach to that physical infrastructure. The VLAN these router and switch interfaces are members of is called the Native VLAN (by default, VLAN 1). Client PCs are members of a different VLAN, just as IP telephones are members of yet another VLAN. The administrative interface of the access point or bridge (interface BVI1) are considered and numbered a part of the Native VLAN regardless of what VLANs or SSIDs pass through that wireless device.

Significance of Native VLAN

When you use an IEEE 802.1Q trunk port, all frames are tagged except those on the VLAN configured as the "native VLAN" for the port. Frames on the native VLAN are always transmitted untagged and are normally received untagged. Therefore, when an AP is connected to the switchport, the native VLAN configured on the AP must match the native VLAN configured on the switchport.

Note: If there is a mismatch in the native VLANs, the frames are dropped.

This scenario is better explained with an example. If the native VLAN on the switchport is configured as VLAN 12 and on the AP, the native VLAN is configured as VLAN 1, then when the AP sends a frame on its native VLAN to the switch, the switch considers the frame as belonging to VLAN 12 since the frames from the native VLAN of the AP are untagged. This causes confusion in the network and results in connectivity problems. The same happens when the switchport forwards a frame from its native VLAN to the AP.

The configuration of native VLAN becomes even more important when you have a Repeater AP setup in your wireless network. You cannot configure multiple VLANs on the Repeater APs. Repeater APs support only the native VLAN. Therefore, the native VLAN configuration on the root AP, the switch port to which the AP is connected, and the Repeater AP, must be the same. Otherwise traffic through the switch does not pass to and from the Repeater AP.

An example for the scenario where the mismatch in the Repeater AP's native VLAN configuration can create problems is when there is a DHCP server behind the switch to which the root AP is connected. In this case the clients associated with the Repeater AP do not receive an IP address from the DHCP server because the frames (DHCP requests in our case) from the Repeater AP's native VLAN (which is not the same as root AP and the switch) are dropped.

Also, when you configure the switch port, *ensure that all the VLANs that are configured on the APs are allowed on the switchport.* For example, if VLANs 6, 7, and 8 exist on the AP (Wireless Network) the VLANs have to be allowed on the switchport. This can be done using this command in the switch:

```
switchport trunk allowed vlan add 6,7,8
```

By default, a switchport configured as a trunk allows all VLANs to pass through the trunk port. Refer to Interaction with Related Switches for more information on how to configure the switchport.

Note: Allowing all VLANs on the AP can also become a problem in some cases, specifically if it is a large network. This can result in high CPU utilization on the APs. Prune the VLANs at the switch so that only the VLAN traffic that the AP is interested in passes through the AP to avoid high CPU.

VLANs on Access Points

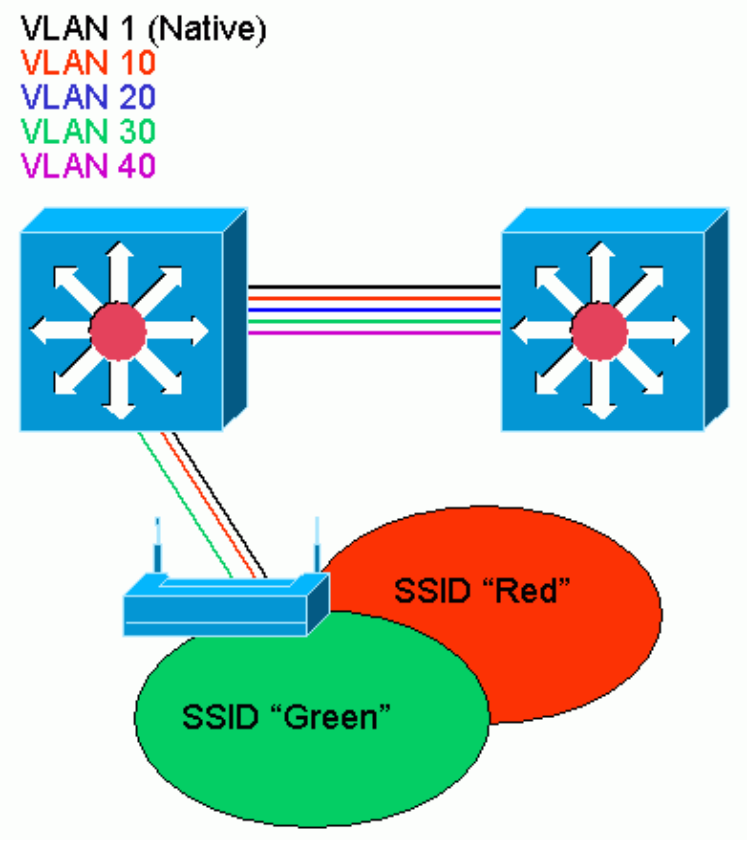
In this section, you are presented with the information to configure the features described in this document.

Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Concepts with Access Points

This section discusses concepts about how to deploy VLANs on access points and refers to this network diagram.

In this sample network, VLAN 1 is the Native VLAN, and VLANs 10, 20, 30 and 40 exist, and are trunked to another switch chassis. Only VLANs 10 and 30 are extended into the wireless domain. The Native VLAN is required to provide management capability and client authentications.

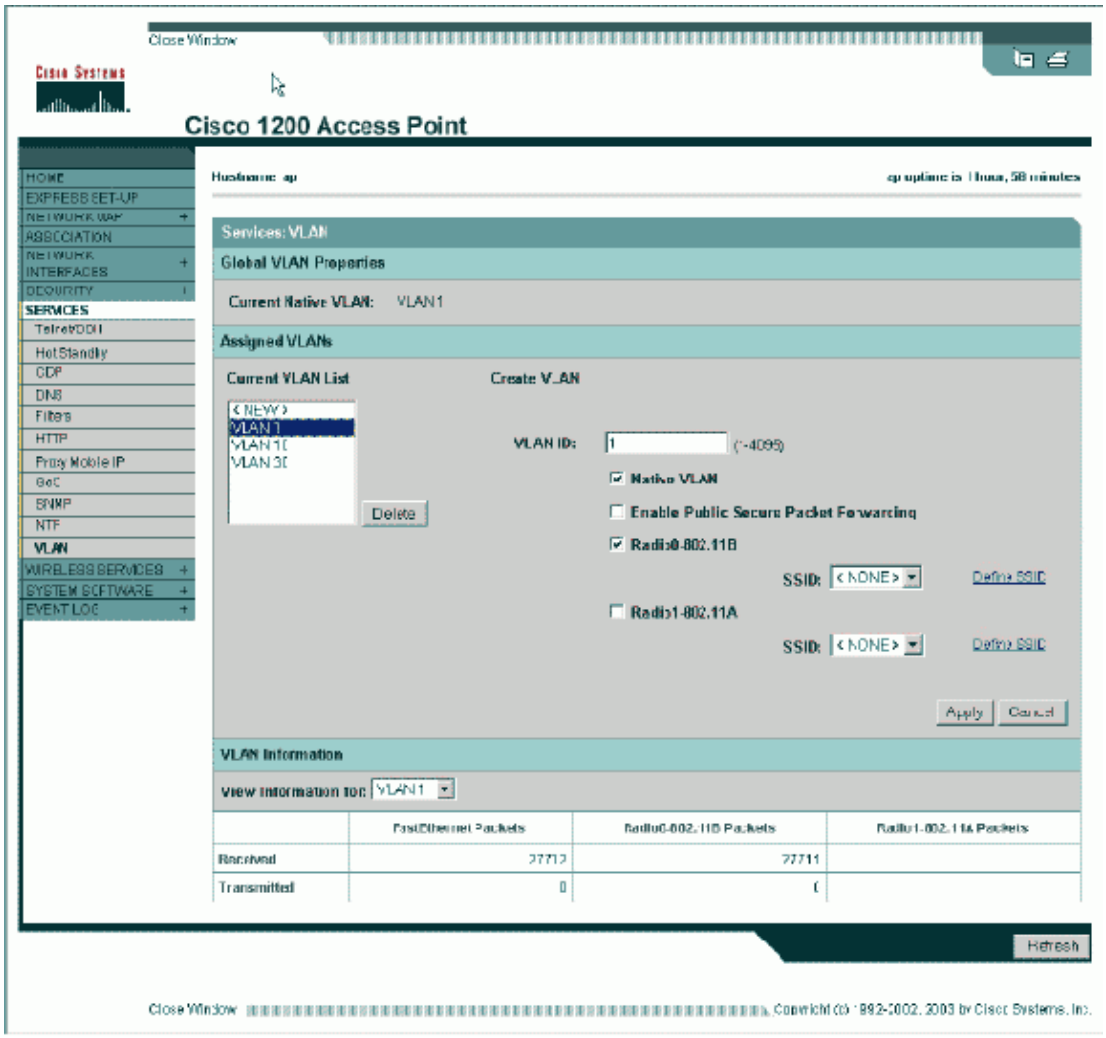


Access Point Configuration

In order to configure the access point for VLANs, complete these steps:

1. From the AP GUI, click Services > VLAN to navigate to the **Services: VLAN** page .

    a. The first step is to configure the native VLAN. From the Current VLAN List, select **New**.
    b. Enter the VLAN number of the Native VLAN in the VLAN ID box. The VLAN number must match the Native VLAN configured on the switch.
    c. Because interface BVI 1 is associated to the subinterface of the Native VLAN, the IP address assigned to interface BVI 1 must be in the **same IP subnet** as other infrastructure devices on the network (that is, the interface SC0 on a Catalyst switch that runs CatOS.)
    d. Select the checkbox for the Native VLAN.
    e. Select check boxes for the radio interface or interfaces where this VLAN applies.
    f. Click **Apply**.

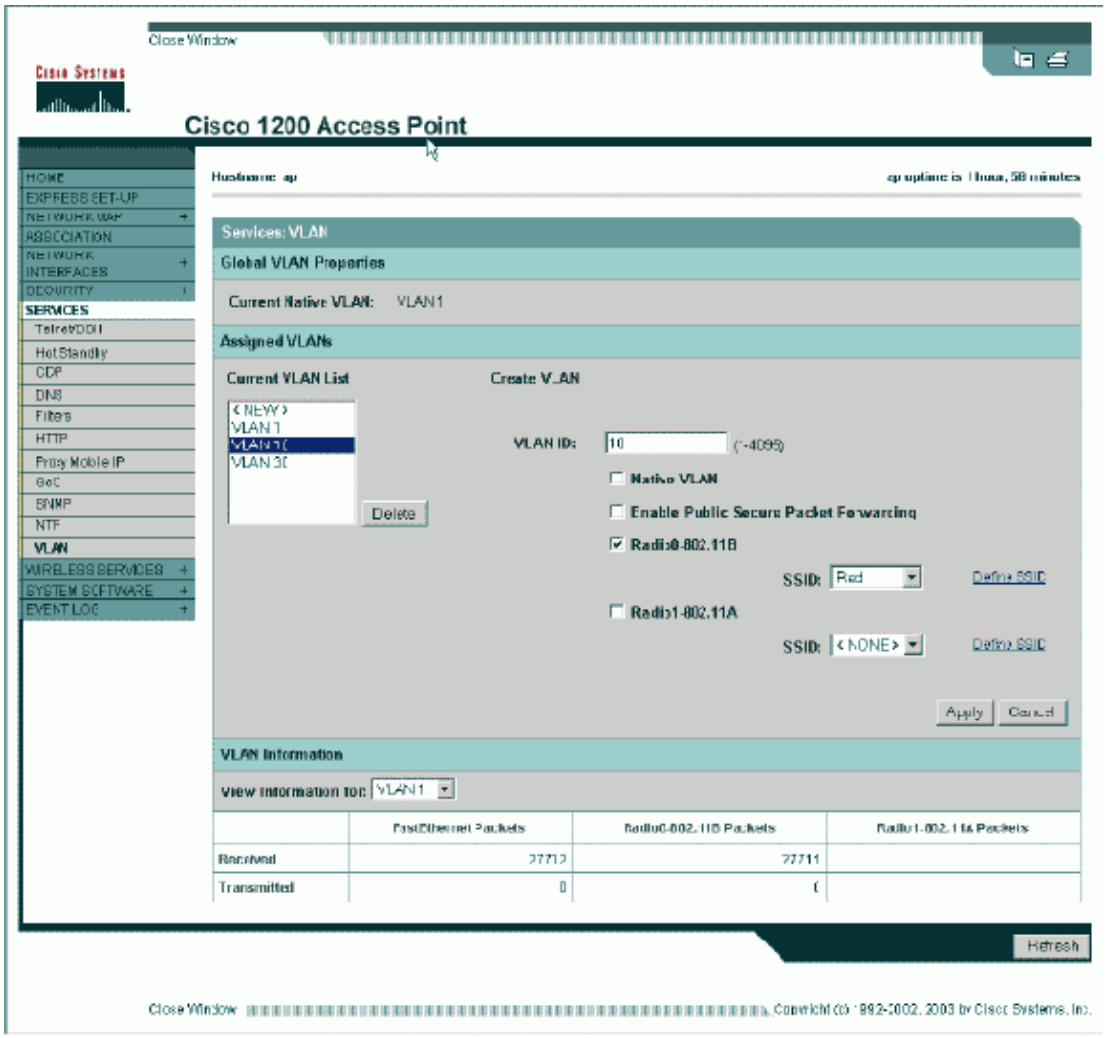


Or, from the CLI, issue these commands:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# interface FastEthernet0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# end
AP# write memory
```

2. In order to configure other VLANs, follow these steps:

   a. From the Current VLAN List, select **New**.
   b. Enter the VLAN number of the desired VLAN in the VLAN ID box. The VLAN number must match a VLAN configured on the switch.
   c. Select check boxes for the radio interface or interfaces where this VLAN applies.
   d. Click **Apply**.



Or, from the CLI, issue these commands:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# interface FastEthernet0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# end
AP# write memory
```

e. Repeat steps 2a through 2d for each VLAN desired or enter these commands from the CLI with appropriate changes to the subinterface and VLAN numbers:

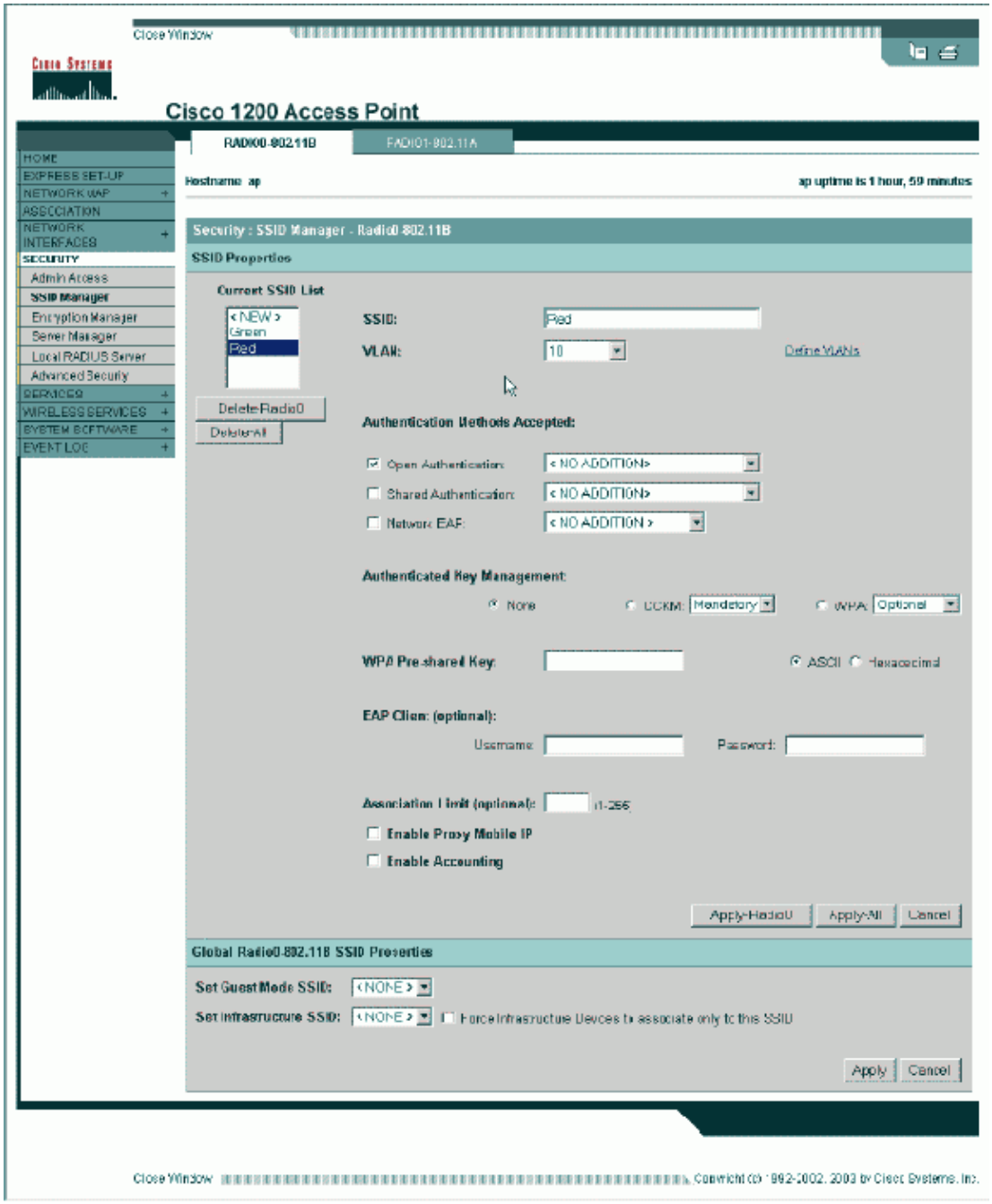
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.30

AP(config-subif)# encapsulation dot1Q 30

AP(config-subif)# interface FastEthernet0.30

AP(config-subif)# encapsulation dot1Q 30

AP(config-subif)# end
AP# write memory
```

3. The next step is to associate the configured VLANs to the SSIDs. In order to do this, click **Security** > **SSID Manager**.

Note: You do not need to associate every VLAN defined on the access point with an SSID. For example, for security reasons, most access point installations do not associate an SSID with the Native VLAN.

a. In order to create a new SSID, choose **New**.
b. Enter the desired SSID (case−sensitive) in the SSID box.
c. Select the desired VLAN number to associate this SSID with from the dropdown list.

   Note: In order to keep this document within its intended scope, security for an SSID is not addressed.
d. Click **Apply−RadioX** to create the SSID on the selected radio, or **Apply−all** to create it on all radios.



Or from the CLI, issue these commands:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Red
AP(config-if-ssid)# vlan 10
AP(config-if-ssid)# end
AP# write memory
```

4. Repeat steps 3a through 3d for each SSID desired or enter these commands from the CLI with appropriate changes to the SSID.

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Green
AP(config-if-ssid)# vlan 30
AP(config-if-ssid)# end
AP# write memory
```

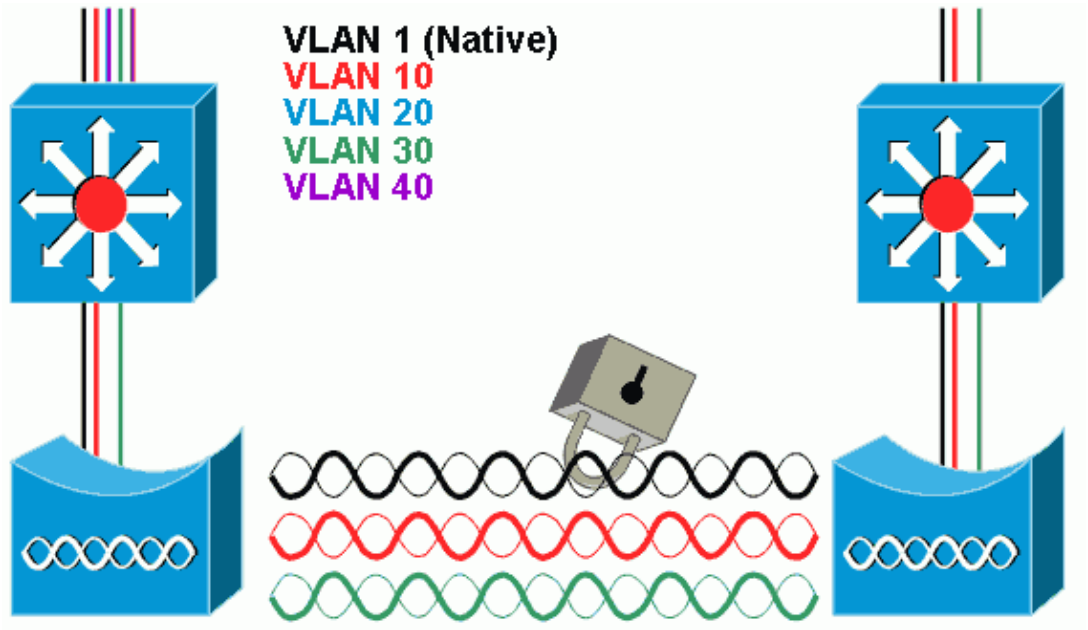
Note: These examples do not include authentication. Some form of authentication (Open, Network−EAP) is required for clients to associate.

VLANs on Bridges

Concepts on Bridges

This section discusses concepts related to how to deploy VLANs on bridges and refers to this network diagram.

In this sample network, VLAN 1 is the Native VLAN, and VLANs 10, 20, 30 and 40 exist. Only VLANs 10 and 30 are extended to the other side of the link. The wireless link is encrypted.



In order to encrypt data that passes over the radio link, apply encryption to only the SSID of the Native VLAN. That encryption applies to all other VLANs. When you bridge, there is no need to associate a separate SSID with each VLAN. VLAN configurations is the same on both the root and non−root bridges.

Bridge Configuration

In order to configure the bridge for VLANs, like the sample network diagram, complete these steps:

1. From the AP GUI, click **Services > VLAN** to navigate to the **Services: VLAN** page.

    a. The first step is to configure the Native VLAN. In order to do this, choose <**New**> from the Current VLAN List.
    b. Enter the VLAN number of the Native VLAN in the VLAN ID box. This must match the Native VLAN configured on the switch.
    c. Because interface BVI 1 is associated to the subinterface of the Native VLAN, the IP address assigned to interface BVI 1 must be in the **same IP subnet** as other infrastructure devices on the network (i.e. interface SC0 on a Catalyst switch that runs CatOS.)
    d. Select the checkbox for the Native VLAN.
    e. Click **Apply**.

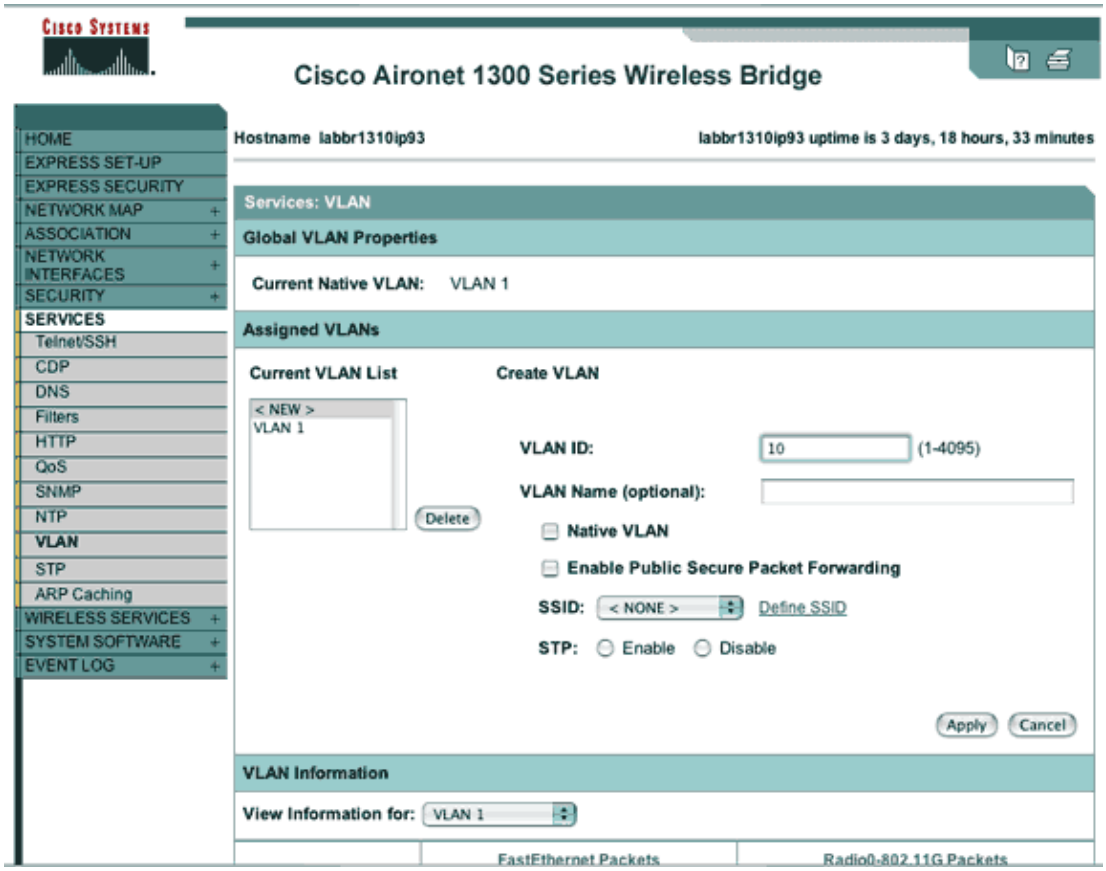
    Or, from the CLI, issue these commands:

```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# interface FastEthernet0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# end
bridge# write memory
```

2. In order to configure other VLANs, follow these steps:

    a. From the Current VLAN List, select **New**.

b. Enter the VLAN number of the desired VLAN in the VLAN ID box. The VLAN number must match a VLAN configured on the switch.
c. Click **Apply**.



Or, from the CLI, issue these commands:

```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# interface FastEthernet0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# end
bridge# write memory
```

d. Repeat steps 2a through 2c for each VLAN desired or enter the commands from the CLI with appropriate changes to the subinterface and VLAN numbers.

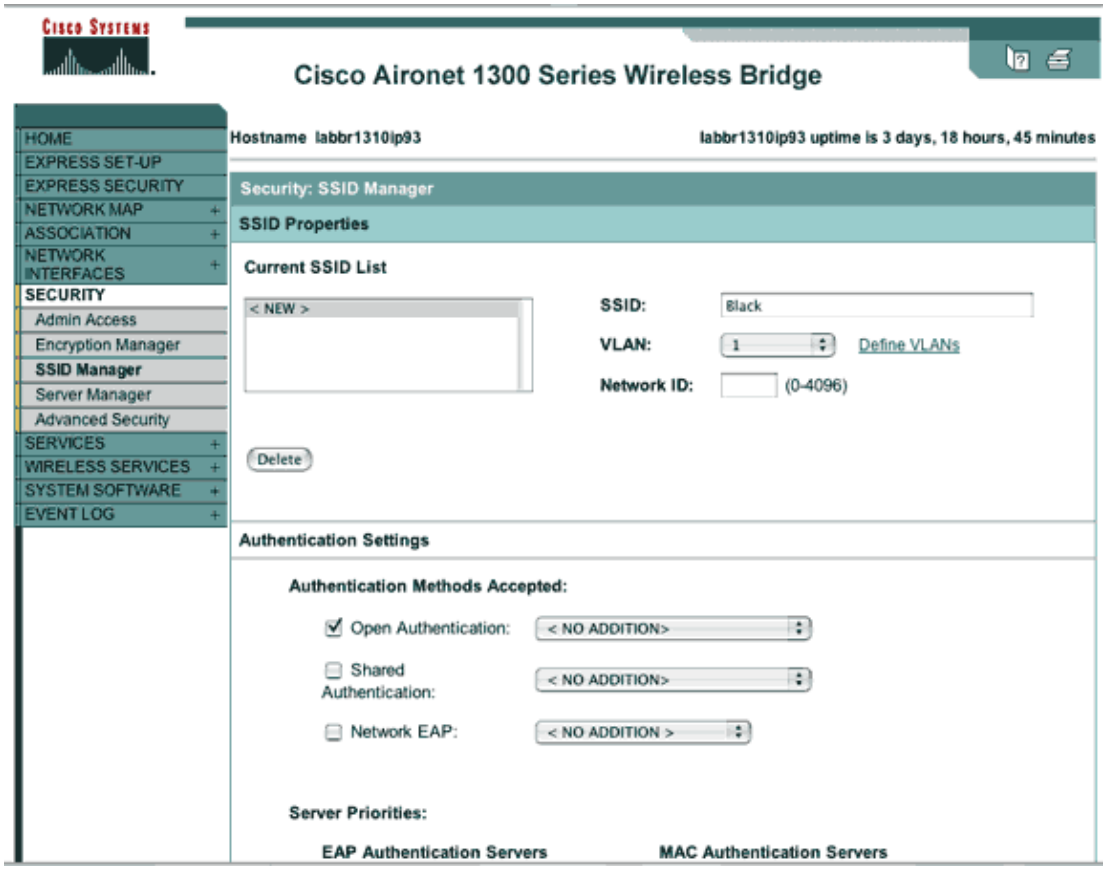
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30

bridge(config-subif)# encapsulation dot1Q 30

bridge(config-subif)# interface FastEthernet0.30

bridge(config-subif)# encapsulation dot1Q 30

bridge(config-subif)# end
bridge# write memory
```

3. From the SSID Manager (under the **Security > SSID Manager** menu item,) associate the Native VLAN with an SSID.

Note: When you bridge, the only SSID that you must associate with a VLAN is the one that correlates to the Native VLAN. You must designate this SSID as the Infrastructure SSID.

a. From the Current SSID List, select **New**.
b. Enter the desired SSID (case−sensitive) in the SSID box.
c. Select the VLAN number that correlates to the Native VLAN from the dropdown list.

   Note: In order to keep this document within its intended scope, security for an SSID is not addressed.
d. Click **Apply** to create the SSID on the radio and associate it to the Native VLAN.



e. Scroll back down to the bottom of the page, and under **Global Radio0−802.11G SSID Properties** select the **SSID** from the **Set Infrastructure SSID** dropdown list. Click **Apply**.

Or from the CLI, issue these commands:

```
AP# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Black
AP(config-if-ssid)# vlan 1
AP(config-if-ssid)# infrastructure-ssid
AP(config-if-ssid)# end
AP# write memory
```

Note: When VLANs are in use, SSIDs are configured under the physical Dot11Radio interface, not under any logical subinterface.

Note: This example does not include authentication. The root and non−root bridges require some form of authentication (Open, Network−EAP, etc.) in order to associate.

Use a RADIUS Server to Assign Users to VLANs

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network. For information on this feature, refer to the section Using a RADIUS Server to Assign Users to VLANs of the document *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB.*

Use a RADIUS Server for Dynamic Mobility Group Assignment

You can also configure a RADIUS server to dynamically assign mobility groups to users or user groups. This eliminates the need to configure multiple SSIDs on the access point. Instead, you need to configure only one SSID per access point. For information on this feature, refer to the section Using a RADIUS Server for Dynamic Mobility Group Assignment of the document *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB.*

Bridge Group Configuration on Access Points and Bridges

In general, bridge groups create segmented switching domains. Traffic is confined to hosts within each bridge group, but not between the bridge groups. The switch forwards traffic only among the hosts that make up the bridge group, which restricts broadcast and multicast traffic (flooding) to only those hosts. Bridge groups relieve network congestion and provide additional network security when they segment traffic to certain areas of the network.

Refer to Bridging Overview for detailed information.

In a wireless network, bridge groups are configured on the wireless access points and bridges in order for the data traffic of a VLAN to be transmitted from wireless media to the wired side and vice versa.

Perform this step from the AP CLI in order to enable bridge groups globally on the access point/bridge.

This example uses the bridge−group number 1.

Ap(configure)#**bridge** *1*

Note: You can number your bridge groups from 1 to 255.

Configure the radio interface and the Fast Ethernet interface of the wireless device to be in the same bridge group. This creates a path between these two different interfaces, and they are in the same VLAN for tagging purposes. As a result, the data transmitted from the wireless side through the radio interface is transmitted to the Ethernet interface to which the wired network is connected and vice versa. In other words, radio and

Ethernet interfaces that belong to the same bridge group actually bridge the data between them.

In an access point/bridge, you need to have one bridge group per VLAN so that traffic can pass from the wire to the wireless and vice versa. The more VLAN you have that need to pass traffic across the wireless, the more bridge groups that are needed.

For example, if you have only one VLAN to pass traffic across the wireless to wired side of your network, configure only one bridge group from the CLI of the AP/bridge. If you have multiple VLANs to pass traffic from the wireless to wired side and vice versa, configure bridge groups for each VLAN at the radio sub−interface, as well as the Fast Ethernet sub−interface.

1. Configure the bridge group in the wireless interface with the **bridge group** dot11radio interface command.

   This is an example.

   ```
   AP# configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   AP(config)# interface Dot11Radio0.1
   Ap(config−subif)# encapsulation dot1q 1 native
   Ap(config−subif)# bridge group 1

   !−−− Here "1" represents the bridge group number.


   ap(config−subif)# exit
   ```
2. Configure the bridge group with the same bridge group number ("1" in this example) in the Fast Ethernet interface so that VLAN 1 traffic is passed across the wireless interface to this wired side and vice versa.

   ```
   Ap(config)# interface fastEthernet0.1
   Ap(config−subif)# encapsulation dot1q 1 native
   Ap(config−subif)# bridge group 1

   !−−− Here "1" represents the bridge group number.


   Ap(config−subif)# exit
   ```

   Note: When you configure a bridge group on the radio interface, these commands are set automatically.

   - **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**

   Note: When you configure a bridge group on the Fast Ethernet interface, these commands are set automatically.

   - **no bridge−group** *1* **source−learning**
   - **bridge−group** *1* **spanning−disabled**

Integrated Routing and Bridging (IRB)

Integrated routing and bridging makes it possible to route a specific protocol between routed interfaces and bridge groups, or route a specific protocol between bridge groups. Local or unroutable traffic can be bridged

among the bridged interfaces in the same bridge group, while routable traffic can be routed to other routed interfaces or bridge groups

With integrated routing and bridging, you can do this:

- Switch packets from a bridged interface to a routed interface
- Switch packets from a routed interface to a bridged interface
- Switch packets within the same bridge group

Enable IRB on the wireless access points and bridges in order to route your traffic between bridge groups or between routed interfaces and bridge groups. You need an external router or a Layer 3 switch in order to route between bridge groups or between bridge groups and routed interfaces.

Issue this command in order to enable IRB in the AP/bridge.

AP**(configure)#bridge irb**

Integrated routing and bridging uses the concept of a Bridge−Group Virtual Interface (BVI) in order to route traffic between routed interfaces and bridge groups or between bridge groups.

A BVI is a virtual interface within the Layer 3 switch router that acts like a normal routed interface. A BVI does not support bridging but actually represents the correspondent bridge group to routed interfaces within the Layer 3 switch router. It has all the network layer attributes (such as a network layer address and filters) that apply to the correspondent bridge group. The interface number assigned to this virtual interface corresponds to the bridge group that this virtual interface represents. This number is the link between the virtual interface and the bridge group.

Perform these steps in order to configure the BVI on access points and bridges.

1. Configure the BVI and assign the correspondent number of the bridge group to the BVI. This example assigns bridge group number 1 to the BVI.

```
Ap(configure)#interface BVI 1
AP(config−if)#ip address 10.1.1.1 255.255.0.0

!−−− Assign an IP address to the BVI.


Ap(config−if)#no shut
```

2. Enable a BVI to accept and route routable packets received from its correspondent bridge group.

```
Ap(config)# bridge 1 route ip!−−−

!−−−

This example enables the BVI to accept and route the IP packet.
```

   It is important to understand that you only need a BVI for the management/native VLAN in which the AP is located (in this example, VLAN 1). You do not need a BVI for any other subinterface, irrespective of how many VLANs and bridge groups you configure on your AP/bridge. This is because you tag the traffic in all other VLANs (except the native VLAN) and send it out to the switch though a dot1q trunked interface onto the wired side. For example, if you have 2 VLANs on your network, you need two bridge groups, but only one BVI correspondent to the management VLAN is sufficient in your wireless network.

When you enable routing for a given protocol on the bridge group virtual interface, packets that come from a routed interface, but are destined for a host in a bridged domain, are routed to the bridge group virtual interface and are forwarded to the correspondent bridged interface.

All traffic that is routed to the bridge group virtual interface is forwarded to the correspondent bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it comes directly from the bridge group virtual interface.

Refer to Configure Bridging for more detailed information on bridging and IRB.

Interaction with Related Switches

In this section, you are presented with the information to configure, or verify the configuration of the Cisco switches that connect to Cisco Aironet wireless equipment.

Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Switch Configuration Catalyst OS

In order to configure a switch that runs Catalyst OS to trunk VLANs to an access point, the command syntax is **set trunk** <*module #/port #*> **on dot1q** and **set trunk** <*module #/port #*> <*vlan list*>.

An example from to the sample network diagram, is:

```
set trunk 2/1 on dot1q
set trunk 2/1 1,10,30
```

Switch Configuration IOS Based Catalyst Switches

From interface configuration mode, enter these commands, if you want to:

- Configure the switchport to trunk VLANs to an access point
- On a Catalyst switch that runs IOS
- The CatIOS includes but is not limited to:
    - 6x00
    - 4x00
    - 35x0
    - 295x

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan add 1,10,30
```

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

Switch Configuration Catalyst 2900XL/3500XL

From interface configuration mode, enter these commands, if you want to configure the switchport to trunk VLANs to an access point on a Catalyst 2900XL or 3500XL switch that runs IOS:

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,10,30
```

Verify

Use this section to confirm that your configuration works properly.

Verify the Wireless Equipment

- **show vlan** displays all VLANs currently configured on the access point, and their status

```
ap#show vlan

Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.1
Dot11Radio0.1
Virtual-Dot11Radio0.1

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

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 1          36954                  0
        Bridging        Bridge Group 1          36954                  0

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.10
Dot11Radio0.10
Virtual-Dot11Radio0.10

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.30
Dot11Radio0.30
Virtual-Dot11Radio0.30

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0

ap#
```

- **show dot11 associations** displays information about associated clients, per SSID/VLAN

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :
```

```
Others:  (not related to any ssid)

ap#
```

Verify the Switch

- On a Catalyst OS based switch, **show trunk** <*module #/port #*> displays the status of a trunk on a given port

```
Console> (enable) show trunk 2/1
* – indicates vtp domain mismatch
Port      Mode         Encapsulation  Status        Native vlan
––––––––  ––––––––––   –––––––––––––  ––––––––––––  ––––––––––
 2/1      on           dot1q          trunking      1

Port      Vlans allowed on trunk
––––––––  ––––––––––––––––––––––––––––––––––––––––––––––––––––––––
 2/1      1,10,30

Port      Vlans allowed and active in management domain
––––––––  ––––––––––––––––––––––––––––––––––––––––––––––––––––––––
 2/1      1,10,30

Port      Vlans in spanning tree forwarding state and not pruned
––––––––  ––––––––––––––––––––––––––––––––––––––––––––––––––––––––
 2/1      1,10,30
Console> (enable)
```

- On a IOS based switch, **show interface fastethernet** <*module #/port #*> **trunk** displays the status of a trunk on a given interface

```
2950g#show interface fastEthernet 0/22 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/22      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/22      1,10,30

Port        Vlans allowed and active in management domain
Fa0/22      1,10,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/22      1,10,30
2950gA#
```

- On a Catalyst 2900XL/3500XL switch, **show interface fastethernet** <*module #/port #*> **switchport** displays the status of a trunk on a given interface

```
cat3524xl#show interface fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1,10,30,1002–1005
Trunking VLANs Active: 1,10,30
Pruning VLANs Enabled: 2–1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
```

```
Voice VLAN: none
Appliance trust: none
Self Loopback: No
wlan-cat3524xl-a#
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Configuring VLANs (Access Point Configuration Guide)**
- **Configuring VLANs (Bridge Configuration Guide)**
- **Trunking Technical Support**
- **Interaction with Related Switches**
- **System Requirements to Implement Trunking**
- **Overview of Bridging**
- **Wireless Authentication Types on a Fixed ISR Configuration Example**
- **Wireless Authentication Types on Fixed ISR Through SDM Configuration Example**
- **Wireless LAN Connectivity Using an ISR with WEP Encryption and LEAP Authentication Configuration Example**
- **Basic Wireless LAN Connection Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 15, 2009 Document ID: 46141