Tech Guide

Implementing VLANs in a SkyPilot Network

January 15, 2007

Table of Contents

Purpose

There a number of advantages to implementing VLANs in a Skypilot network. VLANs can create "virtual" broadcast domains, which are used to separate network traffic. This document describes how VLANs work, and explains how to configure them on Skypilot devices. There are both benefits and limitations to implementing VLANs in a network.

Benefits

1 ***Security:*** VLANs have the ability to provide additional security not available in a shared media network environment. By nature, a switched network delivers frames only to the intended recipients, and broadcast frames only to other members of the same broadcast domain. VLANs allow the network administrator to segment users requiring access to sensitive information into separate broadcast domains, regardless of physical location.

2 ***Network Segmenting:*** VLANs will allow LAN administrators to logically group users. IP addresses, subnet masks, and local network protocols will be more consistent across the entire VLAN.

3 ***Physical Topology Independence:*** VLANs provide independence from the physical topology of the network by allowing physically diverse workgroups to be logically connected within a single broadcast domain.

Limitations

1. ***Equipment:*** VLANs require an 802.1q configurable Ethernet switch to properly segment nodes on a network. These switches tend to be more expensive than generic Ethernet hubs.
2. ***Operational Complexity:*** Because of the operational complexity involved in deployment, a system administrator who is cognizant of configuration requirements is required.

VLAN Communications

An Ethernet switch acts as an intelligent traffic forwarder. Frames are sent only to the ports where the destination device is attached. Broadcast and multicast frames are limited by VLAN boundaries, so only stations whose ports are members of the same VLAN as the source device see these frames. As a result, bandwidth is optimized and network security is enhanced.

Most VLAN switches come out-of-the-box with a single VLAN enabled on all switch ports. This is often referred to as the “default” or “native” VLAN and in many cases is VLAN ID 1. Via configuration, multiple VLANs can be enabled on a single switch and ports can be assigned to specific VLANs. A single VLAN can also span multiple switches by configuring uplink/downlink ports as “trunk ports”. 802.1Q is a common, vendor independent trunking protocol. To share VLANs between switches a tag with a VLAN identifier (VID) is inserted into each frame; a VID must be assigned to each VLAN. Ports on a VLAN switch follow Filtering Database rules, which enable each port to accept frames that are tagged, untagged, or both. By assigning the same VID to VLANs on multiple switches, one or more VLANs (broadcast domain) can be extended across a large network.

Note: Network administrators must ensure ports on non-802.1Q-compliant devices attached to the network are configured to transmit untagged frames. Many network interface cards for PCs and printers are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame.

VLAN Concepts and Definitions

The OSI seven layer model is a useful device for describing key concepts about VLAN. For this discussion only the lower three layers of the OSI model are helpful to describe key concepts, and this document will center on layers 2 and 3:

Layer	Name	Address Type	Function
3	Network	IP	IP routing between hosts(devices)
2	Data Link	MAC	VLAN, ARP, Ethernet switching, access to physical medium
1	Physical	Non Applicable	Modulation rate, Frequency, Output Power,

			Connector type.

A generic 24 port Ethernet switch illustrates how traffic flows between two connected servers, as shown in Figure 1.

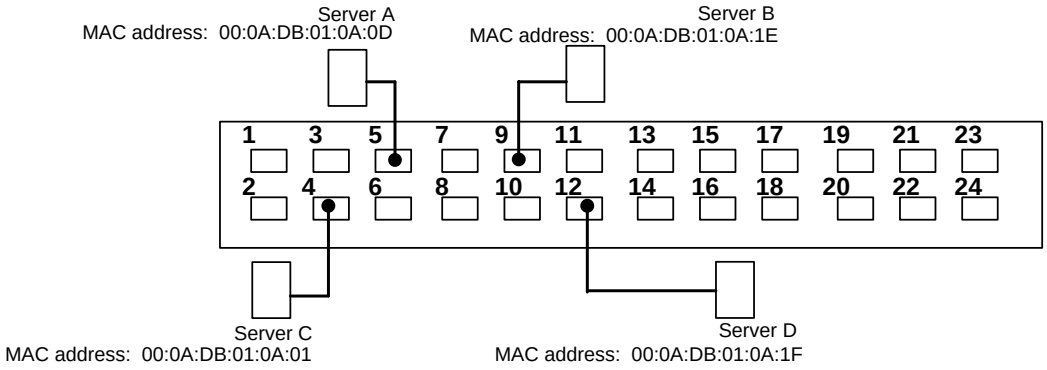

Figure 1: Generic Ethernet Switch

Consider an example where Server A is going to send traffic to Server C. Server A consults its ARP[1] cache for the IP address of Server C. If Server C's IP address is not found in its ARP cache, Server A sends out an ARP request asking all stations in its broadcast domain. A broadcast is one source sending to all destinations in its domain. The Ethernet switch shown above is a single broadcast domain. So the ARP request from Server A will be sent out on ports 4, 9, and 12. Server C would answer the ARP request. Server A would then add an entry in its ARP cache listing Server C's IP address followed by Server C's MAC address.

The next time A needs to send traffic to C it has C's MAC address in its ARP cache. Thus, A forms frames destined for C with C's MAC address as the destination MAC address. The switch maintains a MAC address table of address(es) that are connected through each of its ports. For traffic leaving Server A headed to Server C, the Ethernet frames enter the switch on port 5. The switch looks up the MAC address for Server C and finds it assigned to port 4. These frames are not seen on any other ports.

Taking this concept a step further; a VLAN, virtual LAN, is a method to run separate broadcast domains (at the Data Link Layer or Layer 2 of the OSI model) on one physical Ethernet switch. They are often used to separate traffic based on function or to isolate one group of user's (or customer's) traffic from one another. A common practice in telecom and service provider networks is to separate customer and traffic management.

[1] ARP, Address Resolution Protocol, builds a table relating IP to MAC addresses.

Another way to think of VLAN is it provides the ability to make one physical Ethernet switch act as if it were multiple switches. Figure 2 below is a generic 24-port Ethernet configured with two VLANs.

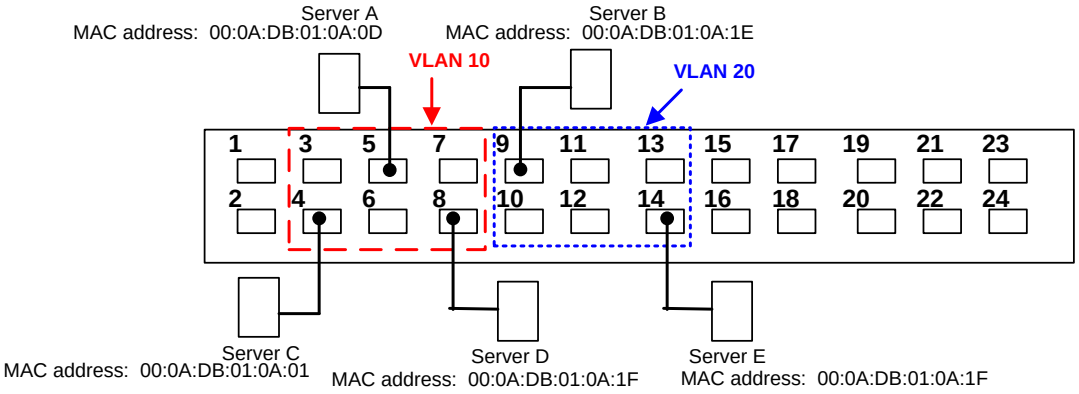

Figure 2: Ethernet Switch with 2 VLANs Enabled

Using our previous example of A sending traffic to C, and assuming A lacks an ARP cache entry for C, A's ARP request would now only be broadcast to ports 4 and 8 on this VLAN switch configuration. As before, C would respond to the ARP request and A's ARP table would be populated with C's MAC address thereby allowing communication between the two hosts at layer 2. The same principle applies for communications between A and D, as well as C and D. However, Server B and Server E would have no way to communicate at layer 2 with Servers A, C or D since they are not members of the same VLAN. Traffic between VLAN 10 and VLAN 20 would require layer 3 functionality as found in an IP router.

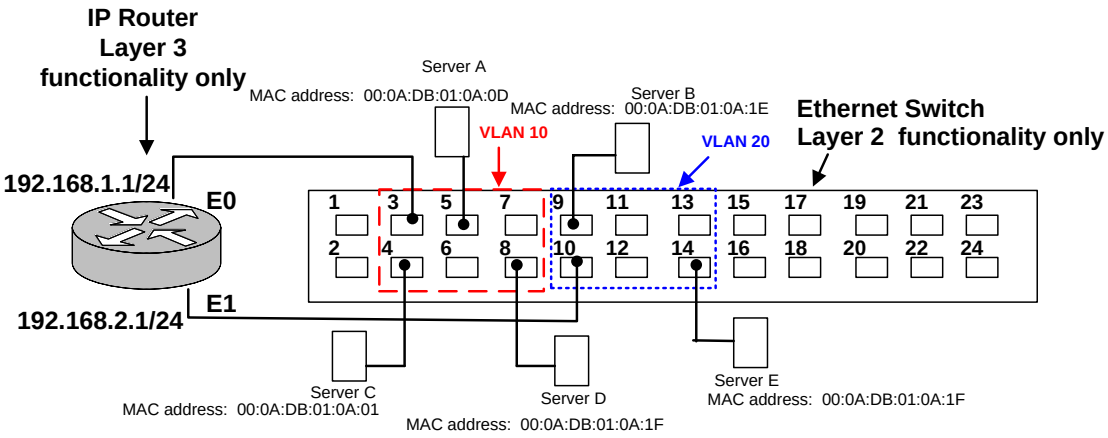

Figure 3: Communicating Between VLANs

For traffic to flow between Server's B and D, as shown in Figure 3, the IP router would have to determine a path between the servers based on IP address. By definition, B and D would have to be on different IP subnets. Packets originating at B headed for D will be processed

by the IP router (after the router performes similar ARP functions to obtain the respective MAC addresses). The router will check its routing table to see if it has a port that will direct the packet to D. For this discussion, the layer 2 and 3 functions are performed in different physical devices. It should be noted that there are VLAN switches on the market that perform both layer 2 and 3 functions.

It is possible to run the same VLAN over multiple physical Ethernet switches as in Figure 4.

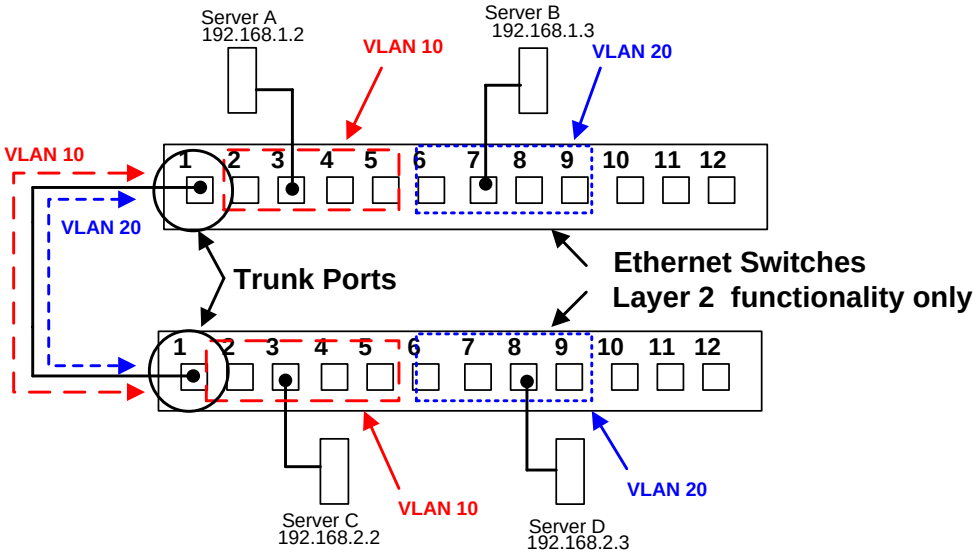

Figure 4: Shared VLAN Shared by Two Switches

In the above example, VLAN 10 is configured on both switches for Ports 2 through 5. These Ports are configured as access ports. Ethernet frames leaving and entering access ports are not altered or tagged with a VLAN ID. Ports 6 through 9 on both switches are configured to share VLAN 20. To achieve this, each switch is configured with a trunk port that allows both VLANs 10 and 20 to pass between the switches. Ethernet frames leaving a trunk port have been altered by the addition of a VLAN ID tag. This allows a VLAN to be shared by both physical switches.

As an example, Server A is sending traffic to Server C. The Ethernet frames leaving port 1 on the top switch have a tag added to them, which identifies the frames as being part of VLAN 10. When this frame arrives at port 1 on the bottom switch, the bottom switch will look in its MAC address table for the MAC address of C, and after removing the VLAN tag, sends the frame out on port 3 for Server C.

SkyPilot and VLANs

SkyPilot uses VLANs to separate the two different types of traffic which may flow to or through a SkyPilot node. The two different types of traffic are management and data. Any traffic directed towards the IP address of a SkyPilot device is considered ***management*** traffic. Examples of management traffic include telnet connectivity to the device, SNMP polling of the device, DHCP transaction by the device, and configuration and software downloads by the device. Traffic directed toward an end-user, and thereby passing through the SkyPilot device, such as a PC connected to the Ethernet port of a SkyConnector, is **data** traffic.

The SkyPilot system allows for one management VLAN, and up to 4059 data VLANs. The use of VLAN 1 as the management VLAN is not recommended as most Cisco switches define VLAN 1 as a native VLAN. The Ethernet port of the SkyGateway acts as an 802.1q trunk port for both management and data VLANs.

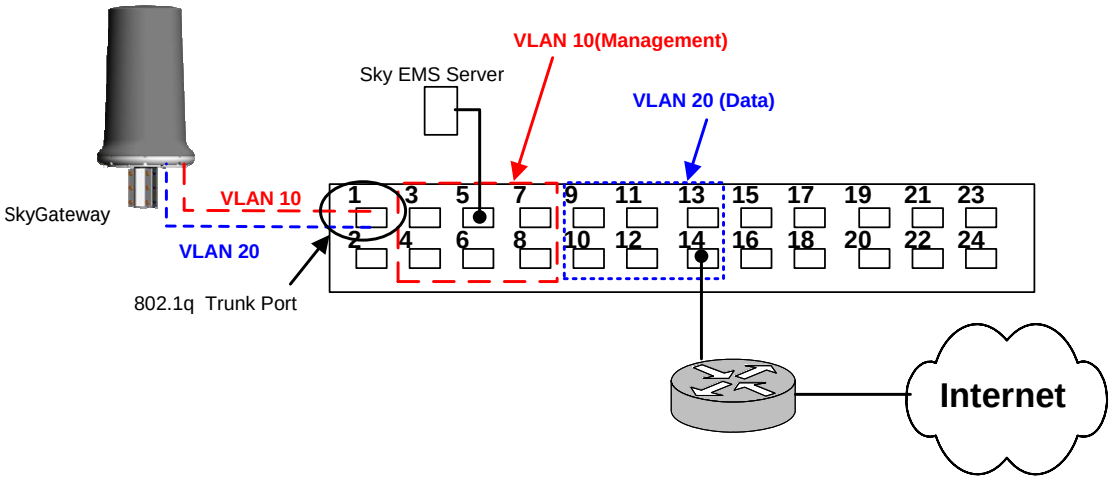

Figure 5: VLAN Support of SkyGateway Ethernet Port

SkyPilot VLAN Configuration

Management VLAN

A Skypilot network can have only one management VLAN. This VLAN is **only** configured on the SkyGateway and can only be configured via the CLI. The management VLAN ID is propagated to all associated SkyPilot devices in that domain through the HELLO protocol messages, which are internal to the SkyPilot system. The following is an example of how to configure the management VLAN on a SkyGateway:

```
> set  vlan
Select a VLAN action:  quit, enable, disable, modify, p2p <q| e | d | m | p>: m
Enter management VLAN ID (0-4096) [0] :  10
VLAN ID changed: 10
Select a VLAN action:  quit, enable, disable, modify, p2p < q | e | d | m | p>: e
VLAN setting changed:  enable
Select a VLAN action:  quit, enable, disable, modify, p2p < q | e | d | m | p>: q
```

To verify this setting:

```
> show vlan
Management :   10
Data            :   Not set

VLAN ID P2P  Enabled
 ----------------------------
```

Data VLAN

The steps involved to configure data VLANs depend upon which provisioning method is defined on the device. For auto provisioning, there are two steps:

1. Define the VLAN in SkyProvision.

    a. Select VLAN from the SkyProvision menu.
    b. Push the Add button.
    c. Enter the VLAN name and Tag and then press OK. The tag is equivalent to VLAN id.
    d. The comment is optional and can be used to note site specific information about this VLAN.

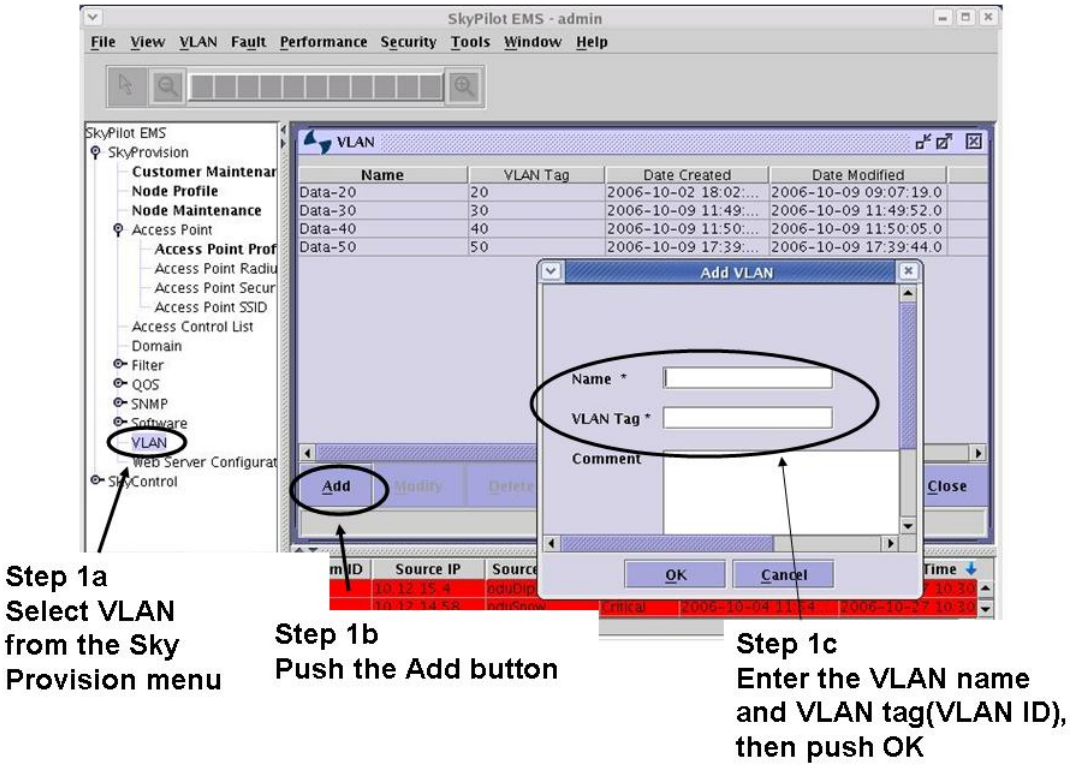

Figure 6: Defining VLAN in SkyProvision

.

2. Add the VLAN to the Node Profile of a SkyPilot device. Data VLANs are only enabled on SkyExtenders, SkyExtender DualBands, SkyExtender TriBands, and SkyConnectors, and not enabled on SkyGateways.

a. Select Node Profile from SkyProvision menu
b. Select a Connector node profile
c. Push the Attributes button
d. Select the VLAN tab
e. Select the Data tab, then the VLAN to be assigned , then push Apply

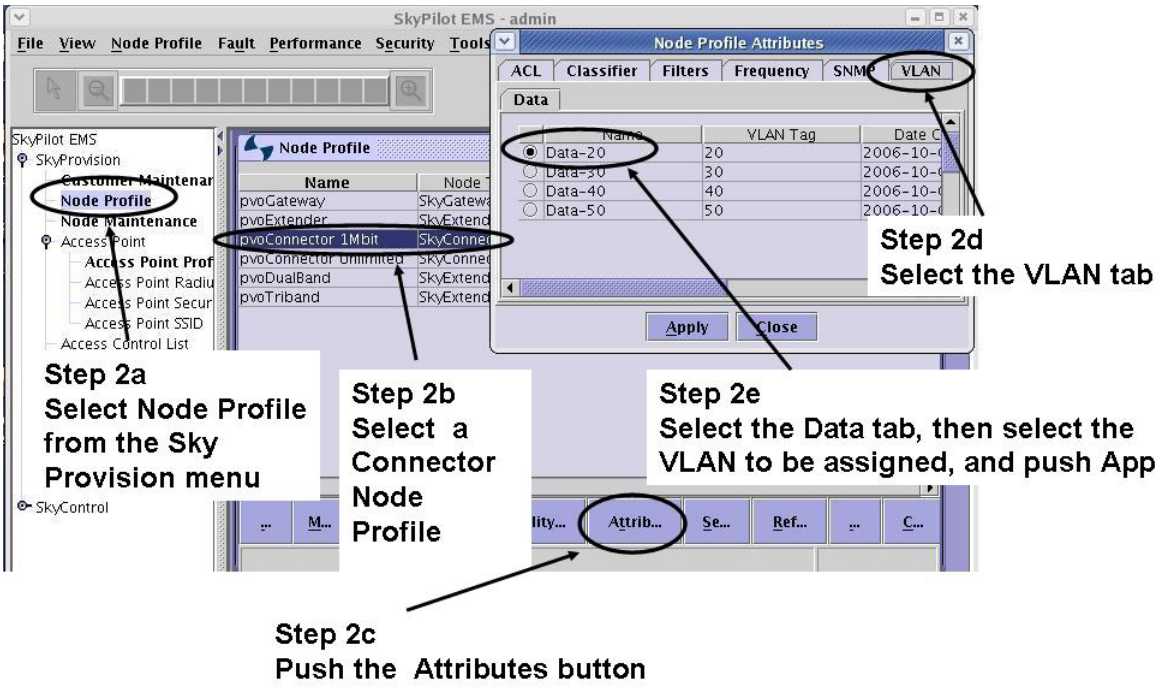

Figure 7: Adding VLAN to Node Profile

For devices that are set to manual provisioning, the data VLANs are configured in the CLI of the device:

> set prov vlan

-> Select a VLAN action: quit, enable, disable, modify <q|e|d|m>: e
VLAN setting changed: enable

-> Select a VLAN action: quit, enable, disable, modify <q|e|d|m>: m

-> Enter data VLAN ID (1-4096) [0]: 20
VLAN ID changed: 20

-> Select a VLAN action: quit, enable, disable, modify <q|e|d|m>: q

To verify this setting run the following:

> show vlan
Management : 10
Data : **20** (P2P Disabled)

***Important**:* When a node is provisioned with a Data VLAN, the Ethernet port now has the Data VLAN ID. Connection to the management side of the unit through the Ethernet port is no longer available since it is now reserved for the Data VLAN and will only pass Data VLAN traffic. Any attempts to ping or telnet directly to the management side of the device from the Ethernet side will fail. Manual management configuration should instead be handled through the radio or the serial port, when available.

Peer-to-Peer

By default, regardless of destination, all traffic from end-users will be sent to the SkyGateway and then forwarded from the Ethernet port of the SkyGateway. This behavior ensures that the network operator can control traffic between subscribers by sending it through an external device (e.g. router, SMS, etc). SkyPilot defines traffic between end-users as “Peer-to-Peer” (or P2P). Since there are legitimate purposes for enabling end-users to exchange traffic (e.g. a single customer has 2 or more business locations and they want to allow traffic to pass between them), SkyPilot has added a feature that allows P2P traffic to be routed within the SkyPilot network. This feature uses a VLAN ID to identify specific traffic for which P2P communications is enabled.

Peer-to-Peer only needs to be configured on the SkyGateway. In Figure 8, VLAN 30 was added to the previous figure to illustrate the use of P2P. The following shows how to configure it on the Gateway with SkyProvision:

1. Select Node Profile from the SkyProvision menu
2. Select a Gateway Node Profile
3. Push the Attributes button
4. Select the VLAN tab
5. Select the Peer-to-Peer tab, then select the VLAN to be made Peer-to-Peer and push Apply

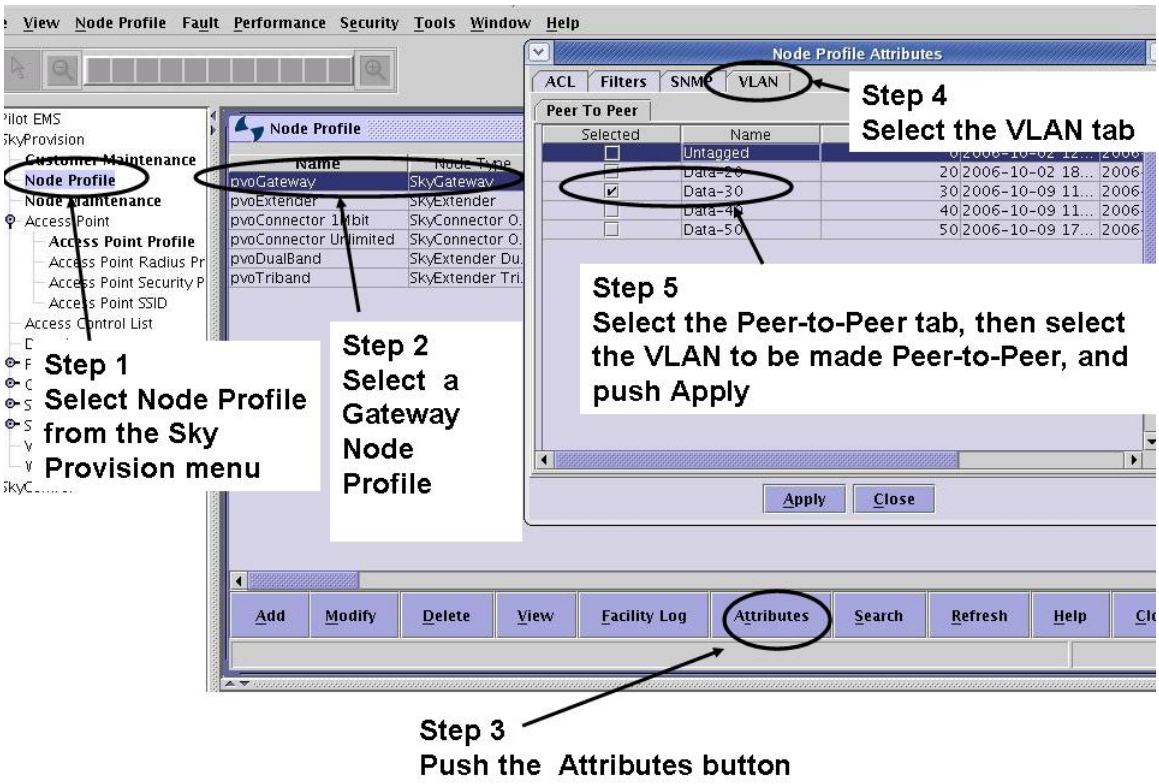

Figure 8: Configuring P2P in Node Profile

VLANS on SkyExtender DualBand and TriBand Access Points

The benefits of VLANs can be extended to SkyExtender DualBand and TriBand access points. Data VLANS are assigned on a per-SSID basis, each SSID can be assigned a different VLAN or the same VLAN. The following steps in Figure 9 both creates a new SSID and assigns a VLAN to it:

1. Select Access Point SSID from the SkyProvision menu
2. Push Add
3. Enter both new SSID and a previously defined VLAN
4. Enter the remaining SSID parameters and push OK

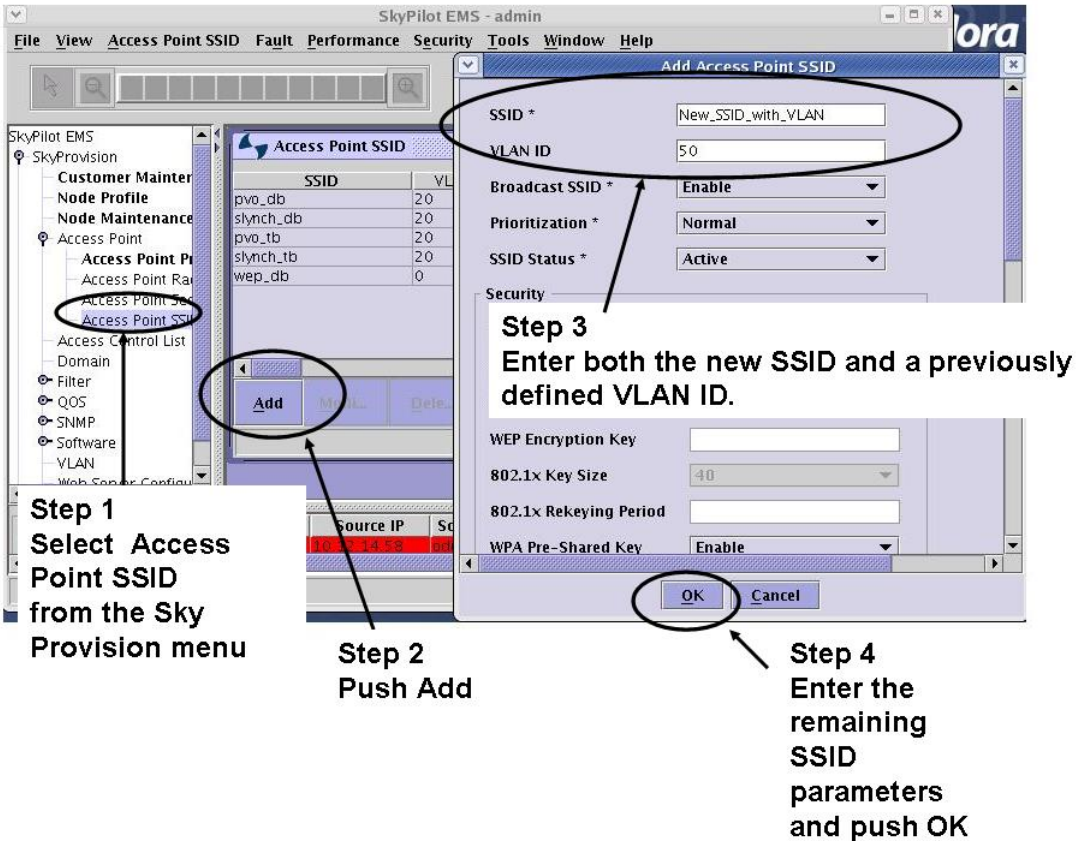

Figure 9: Configuring SSID and VLAN Parameters

Appendix

Example switch configuration #1

Demonstrates multiple ports set to different VLANS with two ports configured as Trunk ports.

```
Switch>en
Password:
Switch#
Switch#
Switch#show run
Building configuration...

Current configuration : 1732 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$TY9M$1ZJSYFyfZgrTiyovsjE1m1
enable password password
!
ip subnet-zero
!
cluster enable aaa 0
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 1000
!
interface FastEthernet0/4
 switchport access vlan 1001
!
interface FastEthernet0/5
!
```

```
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
 switchport access vlan 1000
!
interface FastEthernet0/10
 switchport access vlan 1000
!
interface FastEthernet0/11
 switchport access vlan 1000
!
interface FastEthernet0/12
 switchport access vlan 1000
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
 switchport mode trunk
!
interface FastEthernet0/18
 switchport access vlan 300
!
interface FastEthernet0/19
 switchport access vlan 300
!
interface FastEthernet0/20
 switchport access vlan 300
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport access vlan 300
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
```

```
ip default-gateway 10.4.78.128
ip http server
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password 123password456
 login
line vty 5 15
 password 123password456
 login
!
monitor session 1 source interface Fa0/2
monitor session 1 destination interface Fa0/16
end

Switch#
```

****

Example switch configuration #2

```
Current configuration : 1753 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CNS_Blue
!
boot-start-marker
boot-end-marker
!
logging buffered 128000 debugging
enable secret 5 $1$GkeL$wboVEk54IqZhIPw1BkV24/
enable password sensis2
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!
ip multicast-routing
!
define interface-range switch FastEthernet0/3/0 - 8
```

```
!
interface FastEthernet0/0
 ip address 10.20.0.1 255.255.0.0
 loopback
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description ip int addy = 172.20.3.126
 mac-address 0013.461e.6f51
 ip address dhcp
 duplex full
 speed auto
!
interface FastEthernet0/3/0
!
interface FastEthernet0/3/1
 switchport mode trunk
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface FastEthernet0/3/4
!
interface FastEthernet0/3/5
 switchport access vlan 7
!
interface FastEthernet0/3/6
 switchport access vlan 7
!
interface FastEthernet0/3/7
switchport trunk native vlan 7
 switchport mode trunk
!
interface FastEthernet0/3/8
 switchport trunk native vlan 7
 switchport mode trunk
!
interface Vlan1
 no ip address
!
interface Vlan7
 ip address 192.168.10.1 255.255.0.0
 ip pim sparse-dense-mode
!
ip default-gateway 172.20.0.1
ip classless
ip route 192.168.56.4 255.255.255.255 172.20.0.1
!
ip http server
no ip http secure-server
```

```
!
logging trap debugging
snmp-server community Barbados RO
!
control-plane
!
banner motd ^CINE Welcome to the Blue Network
Welcome to the Blue Network fellow Patricians:
^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 password sensis3
 login
!
scheduler allocate 20000 1000
ntp clock-period 17179966
ntp update-calendar
ntp server 172.20.102.10
```

Citations

Homan, Clare (1998). VLAN Information. Retrieved October, 2006 from http://net21.ucdavis.edu/newvlan.htm

ZyXEL Communications (2003). IEEE 802.1Q Tag-based VLAN. Retrieved October, 2006, from http://global.zyxel.com/support/supportnote/ies1000/app/8021q.htm

Sheldon, Tom (2001). VLAN (Virtual LAN). Retrieved October, 2006, from http://www.linktionary.com/v/vlan.html

Cisco Systems Inc. (1997). Cisco Documentation. *Overview of Routing between Virtual LANs.* Retrieved October, 2006, from http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm#34976

© 2007 SkyPilot Networks, Inc. All rights reserved. SkyGateway, SkyExtender, SkyConnector, SkyControl, SkyPilot, SkyPilot Networks, SkyProvision, the SkyPilot logo, and other designated trademarks, trade names, logos, and brands are the property of SkyPilot Networks, Inc. or their respective owners. Product specifications are subject to change without notice. This material is provided for informational purposes only; SkyPilot assumes no liability related to its use and expressly disclaims any implied warranties of merchantability or fitness for any particular purpose.

Leading the Mesh Revolution

2055 Island Drive
Redwood City , CA 94065
408.764.8000
US Toll Free 866 SKYPILOT
sales@skypilot.com