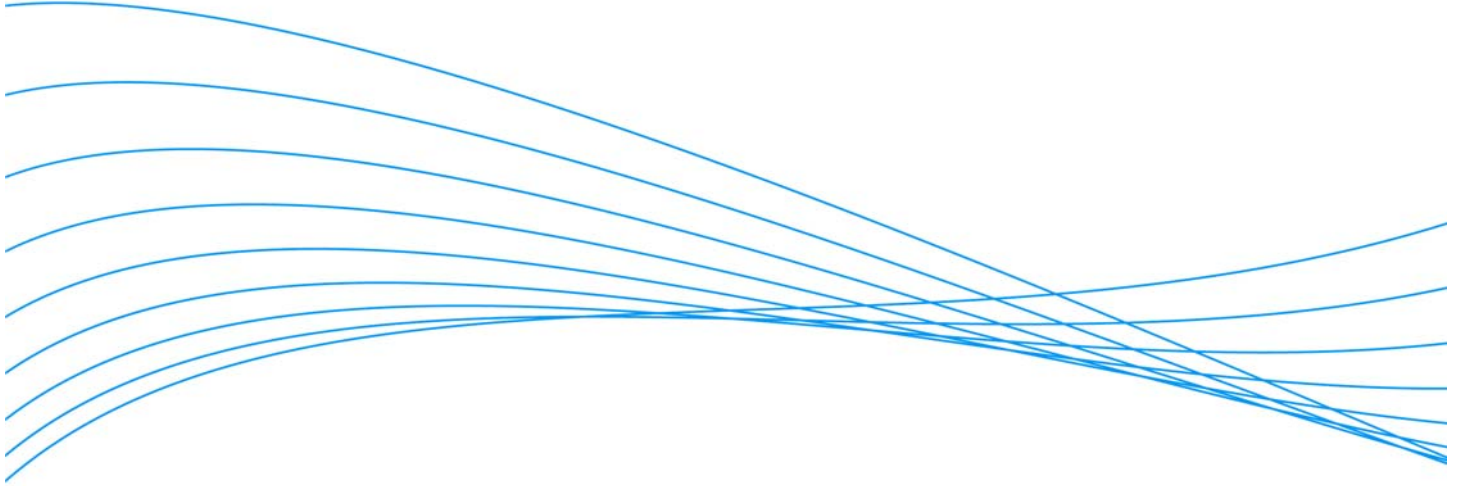


ProCurve Networking Delivers Protocol VLANs



Introduction	2
What are Protocol VLANs?	2
Simplified Deployment	4
Application of PVLANS	5
Configuring Protocol VLANs.....	6
Summary.....	6

Introduction

VLANs are a powerful tool in the network administrator's tool box as they are used to contain groups of nodes for privacy and performance reasons. Combined with an IP routing switch, VLANs provide a high degree of flexibility in administratively controlling the distribution of the services, management of performance and enhancing the security of business critical applications and services. This combination of VLANs and IP routing has proven so powerful that it's become a very common model for network deployment - a powerful solution, but not perfect.

Problems can arise when business critical services reside on systems that do not support IP. What happens when some users requiring access to these services are not connected to the VLAN where the service resides? Perhaps they are located on another floor or in another building? Extending VLANs is frequently not an option as this would violate the administrative boundaries of the VLAN creating a network that is much more difficult to manage.

Where an extension of the VLAN is possible, it may be the simplest, easiest solution to implement. Performance or security needs may necessitate keeping this application specific protocol traffic separate from the rest of the network data.

Consider a business critical application that resides on a Novel server running IPX. If users in different VLANs require access, how will that access be provided without significantly disrupting the existing VLAN/IP subnet configuration? Considering that users of this service could be on different floors or in different buildings it may not be possible.

Another possibility might be that of a service that resides in an existing AppleTalk network. If the network is built on legacy hardware those devices may not be able to keep up with the wire-speed capabilities of today's devices. That is, by placing them directly in an existing VLAN they be become overwhelmed by the normal levels of broadcast and multicast traffic. Isolating these devices will substantially improve their performance and may postpone or eliminate the need to upgrade to more current hardware. It has the added benefit of containing the AppleTalk broadcast packets to the set of devices that need them.

What are Protocol VLANs?

Briefly described, Protocol VLANs (PVLANS) allow untagged packets to be mapped to a VLAN based on the packet protocol type. When a protocol VLAN is configured, packets received on member ports will be examined by the switch and will be assigned VLAN membership based on the packet protocol type and the packet encapsulation.

ProCurve switches use the same eight protocol classifications for Protocol VLANs as can be configured for port filters. They are: IPv4, ARP, IPv6, IPX, AppleTalk, DECNet, NetBEUI, and SNA. As Table 1 shows, each filter is composed of multiple components – usually frame type and frame encapsulation. When an IPX protocol VLAN is configured, any untagged packet matching the encapsulation and frame types defined in this table will be classified as a member of the IPX protocol VLAN when received on a port which is a member of that protocol VLAN.

Table 1- Protocol VLAN Filters

Protocol VLAN Type	Frame Type	Eth Type / LSAP
IPv4	EtherII	0x0800
	SNAP	0x0800
	SAP	0x5E5E
	SAP	0x0606
ARP	EtherII	0x0806
	SNAP	0x0806
	SAP	0x0806
IPv6	EtherII	0x0800
	EtherII	0x86DD
	SNAP	0x0800
	SNAP	0x08DD
	SAP	0x5E5E
	SAP	0x0606
IPX	Raw	Any
	EtherII	0x8137
	EtherII	0x8138
	SNAP	0x8137
	SNAP	0x8138
	SAP	0xE0E0
AppleTalk	EtherII	0x809B
	SNAP	0x809B
DECLAT	EtherII	0x6004
	SNAP	0x6004
NetBEUI	SAP	0xF0F0
SNA	EtherII	0x80D5
	SNAP	0x80D5

Protocol VLANs can be applied any way on any port – with two restrictions. First, there can be only three protocol types applied to each port. It doesn't matter whether they are in a single VLAN or shared among two or three. The switch will return an error message when the sum exceeds three for any port.

The other restriction is that a protocol VLAN type can only be applied once to a port. If the user attempts to make a port a member of two protocol VLANs that each have the same Protocol VLAN type, the switch will return an error message when the second is applied.

Finally, though it is not required, every IPv4 protocol VLAN should also contain the ARP protocol type. Failure to include the ARP type will likely cause ARP to fail.

Simplified Deployment

ProCurve has simplified configuration of Protocol VLANs by eliminating the need for the network administrator to know frame types and encapsulations. Rather, the classification can be selected by their common, user-friendly names (i.e. IPX, or AppleTalk).

Protocol VLAN filters are applied only on received packets that are untagged. Tagged packets received on that same port are not subject to the Protocol VLAN filters.

Once packets are placed in these VLANs they are switched and routed according to the same rules as port-based VLANs.

Protocol VLANs simplify end-node configuration in cases where the end-node will use multiple protocols. Without PVLANS, administrators desiring to have protocols running on different VLANs would be forced to configure at least one tagged VLAN interface on the end node. Where this is not possible, the administrator may have to resort to multiple interfaces. With the introduction of Protocol VLANs, the untagged interface is simply connected to the ProCurve switch and the switch assigns incoming packets to a VLAN based on the protocol type.

It is important to note that ports can be members of multiple protocol VLANs so long as the protocols configured in those VLANs are not duplicated and the combined total of protocols specified does not exceed three. For example, given protocol VLANs as defined in Table 2, Table 3 shows examples of valid and invalid assignments.

Table 2- Protocol VLAN Filters

Protocol VLAN #	Protocols Configured		
VID100	IPX		
VID200	AppleTalk		
VID300	IPv6		
VID400	NetBEUI		
VID500	ARP	IPv4	
VID600	ARP	IPv4	AppleTalk
VID700	NetBEUI	IPv6	
VID800	NetBEUI	AppleTalk	IPX

Table 3- Protocol VLAN port configuration

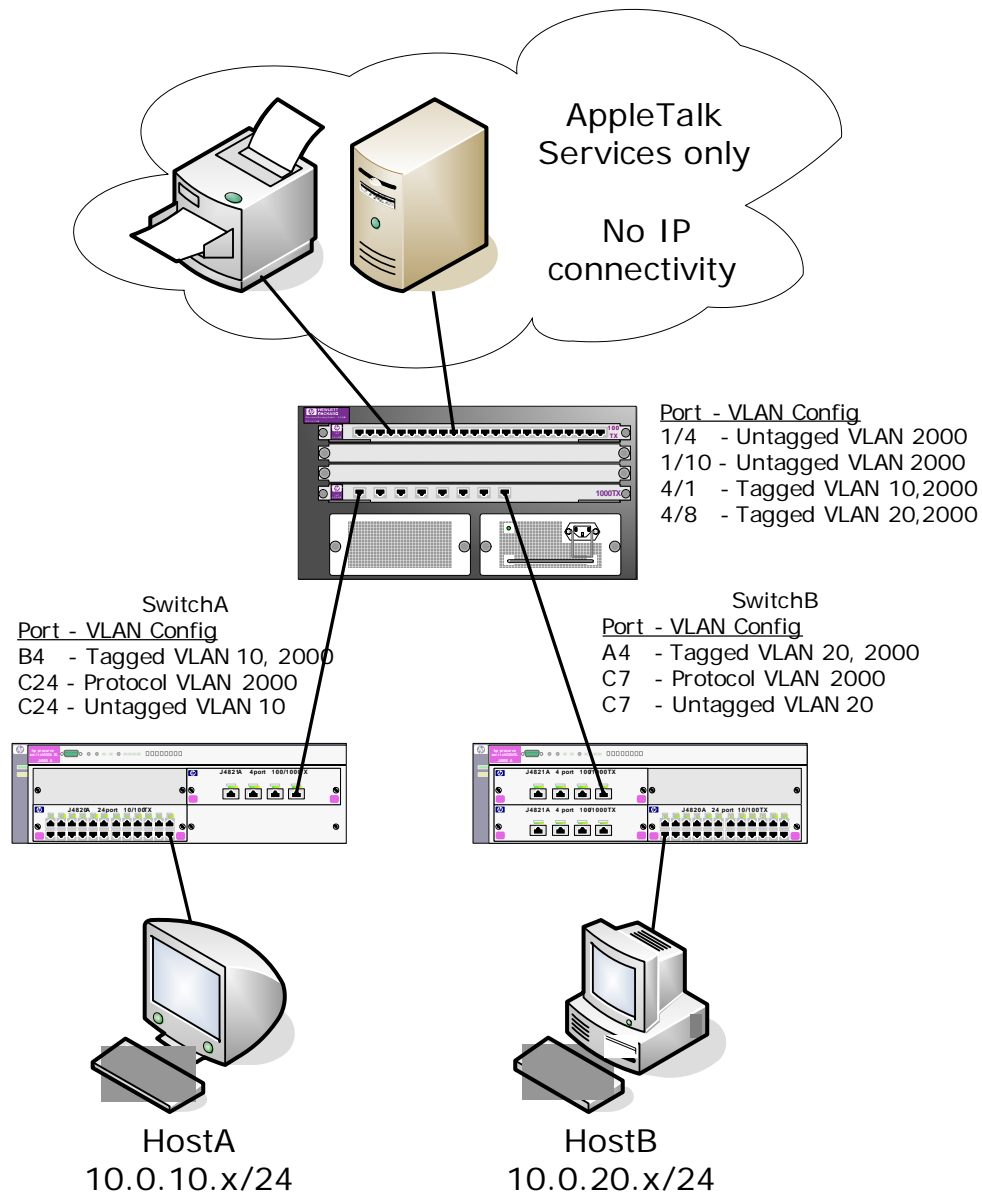
	Per port Protocol VLAN memberships (VID)			Reason
Permitted	100	200	300	
Permitted	200	500		
Not Permitted	100	200	500	Too many Protocol filters
Not Permitted	400	700		NetBEUI configured in both Protocol VLANs
Not Permitted	100	600		Too many Protocol filters

As with port-based VLANs and tagged VLANs, Protocol VLANs can be named to ease management recognition.

Application of PVLANS

One application of Protocol VLANs allows for network resources to be isolated on their own VLAN. Recall the legacy AppleTalk network described earlier. Devices designed and built for networks of 5-10 years ago may not be able to keep up with data rates in today's networks. Moderate traffic levels by today's standards could overwhelm older AppleTalk devices. Protocol VLANs provide a way to limit the packets the devices see to only AppleTalk packets. Security concerns might also warrant strict isolation of those resources. By removing those devices from the general network they become invisible to most would-be intruders.

Figure 1



As Figure 1 shows, HostA and HostB are currently on different VLANs and different IP subnets. By configuring Protocol VLAN 2000 we have provided access to the AppleTalk service from anywhere. Even though HostA and HostB may be on different floors or different buildings, a private AppleTalk network can be created so long as 802.1Q tagging is supported on all switches and routers.

Configuring Protocol VLANs

Configuring the protocol VLAN to isolate AppleTalk packets on the network shown in Figure 1 is fairly quick. In this case, the only devices that need to have a protocol VLANs configured are the 5304xl. The following commands will create a Protocol VLAN for AppleTalk packets, make each of the connected clients' untagged members of the protocol VLAN and the uplink to the 9304 a tagged member. Note: these steps assume HostA and HostB already have IP connectivity. It is perfectly acceptable for C24 on SwitchA and D7 on SwitchB to be untagged members of a port-based VLAN and also be members of a Protocol VLAN.

```
SwitchA(config) # vlan 2000 protocol appletalk
SwitchA(vlan-2000 proto) # untagged c24
SwitchA(vlan-2000 proto) # tagged b4
```

On SwitchB, the instructions are similar:

```
SwitchB(config) # vlan 2000 protocol appletalk
SwitchB(vlan-2000 proto) # untagged d7
SwitchB(vlan-2000 proto) # tagged a4
```

And finally, on the 9300:

```
ProCurve9304(config) # vlan 2000
ProCurve9304(vlan-2000) # untagged 1/4, 1/10
ProCurve9304(vlan-2000) # tagged 4/1, 4/8
```

A second VLAN, this one port-based, is assumed to already exist and will carry all non-AppleTalk packets. Each of the clients connected to the 5300xl will then be untagged members of both the port-based VLAN and a protocol VLAN. The uplinks to the 9300 is a tagged member of VLAN 2000.

The legacy AppleTalk network is connected to the ProCurve 9402 as an untagged member of VLAN 2000. The link between SwitchA and the 9304 is a tagged member of VLANs 10 and 2000 while the link between SwitchB and the 9304 is a tagged member of VLANs 20 and 2000.

Following these commands, the clients are members of both a port-based VLAN and protocol VLAN 2000. A packet received by the 5304xl from one of these clients will be classified as a member of VLAN 2000 only if it is an AppleTalk packet as defined in Table 1.

A network analyzer attached to the link between the switches would show all AppleTalk packets received from the HostA and HostB are tagged members of VLAN 2000 while all other packets are tagged members of either VLAN 10 or VLAN 20.

Note that some clients may require a port-based VLAN be available to support complementary protocols. For instance, a Microsoft Windows node running a NetBEUI client cannot function if connected to a port that is configured only for a NetBEUI protocol VLAN. There is an associated discovery mechanism that uses a protocol type that does not fit the NetBEUI classification type but is required for NetBEUI to function.

Summary

The task of integrating legacy protocols and network devices becomes increasingly challenging as network capacity and demands for network security grow. Protocol VLANs offer the network administrator one more tool for providing services to the user community while maximizing protection of those resources. They offer the opportunity to extend the benefits of VLAN protection to devices that do not support 802.1Q tagging.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-0658ENW, 5/2005