Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1Q tags to be transported over ATM permanent virtual circuits (PVC) used in Asymmetric Digital Subscriber Line 2+ (ADSL2+) uplinks. Additionally, 802.1P marking is allowed and is based on 802.1Q tagging.

Note Although this document uses the generic term ADSL, this feature requires an ADSL2+ uplink.

Prerequisites for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

- You must have a basic understanding of ATM, bridging, DHCP, and VLANs before configuring this feature.

Restrictions for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

• Supports only one bridged 802.1Q VLAN.

• Can be configured only on a point-to-point ATM subinterface.

• Uses ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol (AAL5SNAP) encapsulation to enable the transport of an 802.1Q tag over an ATM PVC.

Information About Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Benefits of Preserve 802.1Q Tagging with 802.1P Marking

• CPE can carry traffic with 802.1P-marked provider-specific 802.1Q tags.

• Voice, video, and data services can be deployed at customer premises. This service combination offers a real-time channel dedicated to VoIP traffic and a second channel that delivers best-effort Internet service.

• All traffic is marked with an 802.1P marking which is implemented using VLAN-based service differentiation.

Note   Support for PVCs configured with Route-Bridge Encapsulation (RBE) was introduced with CSCtt22809.

VLAN-Based Service Differentiation over ADSL

VLAN-based service differentiation allows service providers to offer a range of broadband-enabled services and applications to end users. It supports IP connectivity applications that require real-time network performance and applications that use best-effort, or Internet-grade performance.

The original VLAN tag in an inbound packet is changed to the value configured by the **bridge-dot1q encap** command before the tag leaves the device. For example, if you enter the command **bridge-dot1q encap 10**, a VLAN tag of 70 in a packet inbound from the local network is changed to a value of 10 in the egress packet. Any 802.1P value is changed to 0, and frames without VLAN tags are sent out over ATM with an added VLAN header as shown in the figure in the "Transporting 802.1P Marked 802.1Q Tags" section.

From an Ethernet perspective, this service is carried over a dedicated VLAN from the hand-over point to the end-user premises. This VLAN-based service differentiation at the PVC level is shown in the figure below.

Figure 1: VLAN-Based Service Differentiation at PVC Level
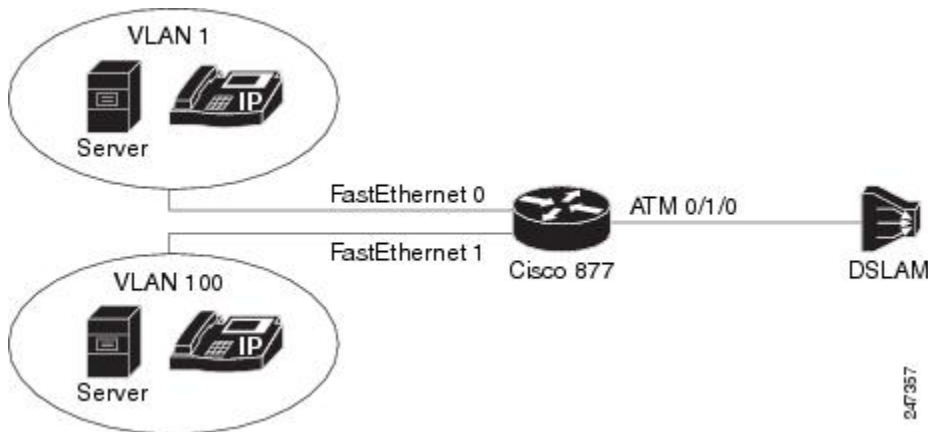
The Ethernet VLAN used by the voice, video, and data services must be identified at the customer premises by an 802.1Q VLAN ID configured using the **bridge-dot1q encap** command. The VLAN is identified at the service provider's end by a service-provider-assigned 802.1ad customer VLAN ID.

The **bridge-dot1q encap** command changes the local VLAN ID to the VLAN ID required by the service provider. The operation of this command is shown in the figure below.

Figure 2: Operation of the bridge-dot1q encap Command
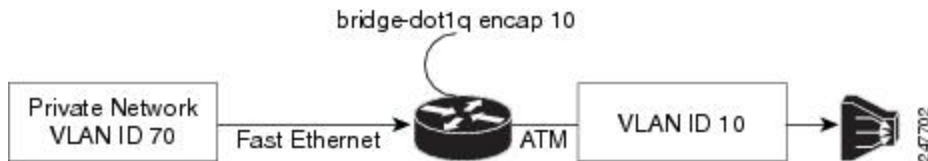
The figures in the "Transporting 802.1P Marked 802.1Q Tags" section show the PDU data structure in greater detail.

Transporting 802.1P Marked 802.1Q Tags

An 802.1Q VLAN tag is inserted into the MAC Protocol Data Unit (PDU), and this PDU is sent to the Digital Subscriber Line Access Multiplexer (DSLAM). Incoming and outgoing PDU structures are shown in the two figures below.

The figure below shows the packet structure when the incoming Ethernet frames do not have a VLAN header.

Figure 3: Incoming and Outgoing Packet Structures When No Incoming VLAN ID Is Present
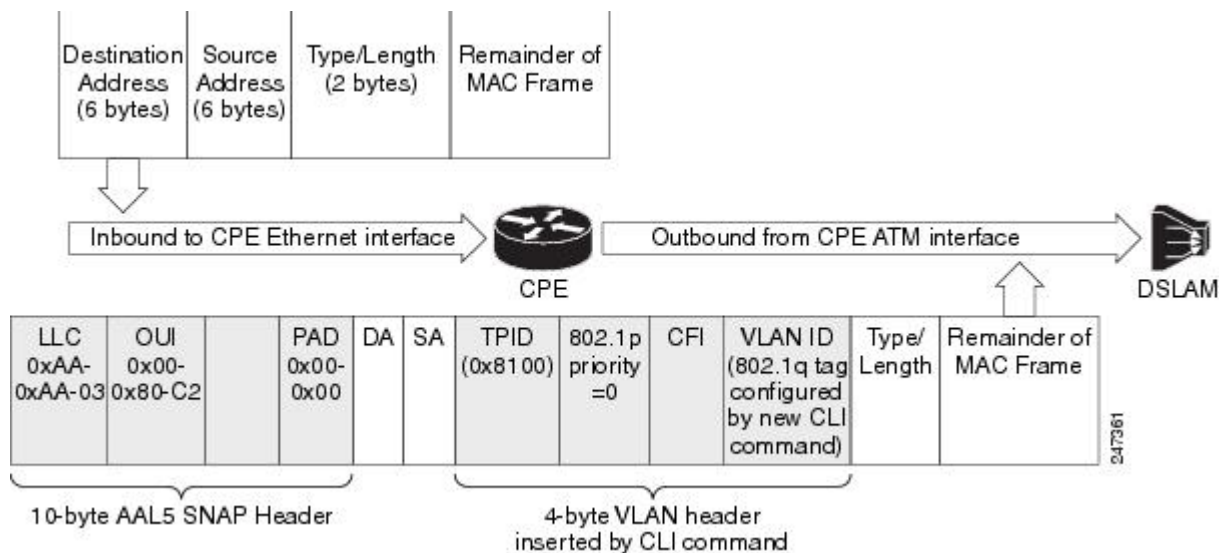
The figure below shows that a 4-byte VLAN header has been inserted in the outgoing packet, with an 802.1P value. The VLAN ID value is configured by the **bridge-dot1q encap** command.

The figure below shows the incoming packet structure when the incoming Ethernet packets contain a VLAN header.

Figure 4: Incoming and Outgoing Packet Structures When an Incoming VLAN ID Is Present
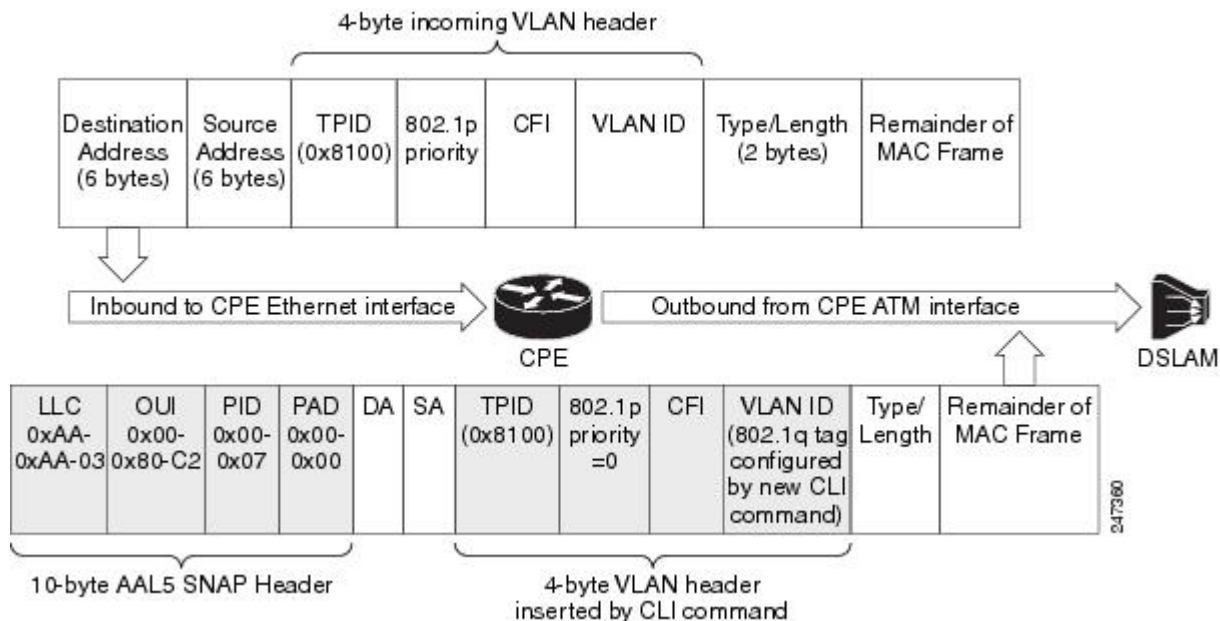
The outgoing packet structure is the same as in figure 1.

Note   The 802.1P priority that was configured earlier is changed to 0, and any VLAN ID that is configured is set to the ID configured by the **bridge-dot1q encap** command.

The CPE is connected to the DSLAM via an ATM interface that is configured as the bridging interface. The CPE establishes a PPP over Ethernet (PPPoE) session over the bridging ATM interface with the service provider. The VLAN and voice traffic enter customer devices via VLAN ports or a Switched Virtual Interface (SVI).

In the CPE, the packet is classified as data or voice traffic based on the VLAN ID, Differentiated Services Code Point (DSCP), protocol, source MAC address, or port. The packets are marked with the quality of service (QoS) group, and routed from VLAN via the Bridge Virtual Interface (BVI) to the ATM PVC bridging interface.

If the packet requires encapsulation, ATM provides the default VLAN ID. If there is a QoS service policy attached to the PVC, packets are classified against the QoS group. QoS marks the corresponding VLAN ID and 802.1P or class of service (CoS) value into the packet VLAN header. The QoS VLAN ID overwrites the default VLAN ID. If there is no service policy attached in PVC, the packets are sent out with the default VLAN ID and default CoS marking.

Packets returning from the service provider's network and destined to the customer's network carry VLAN tags. The ATM PVC interface removes the VLAN tag before passing it for further processing. These packets do not require classification or QoS marking.

Using PPPoE, the CPE device acts as a PPPoE Dialer client and gets the IP address dynamically from the service provider by using the Point-to-Point Protocol. The Dialer interface has to be configured and associated with the ATM PVC interface. The packets are sent out with the default VLAN ID as PPPoE supports only one VLAN ID per PVC. PPP control packets such as PPPoE Active Discovery Initiation (PADI), PPPoE Active Discovery Request (PADR), PPPoE Active Discovery Terminate (PADT) and keepalive packets are marked with higher priority CoS markings similar to the real-time traffic. The VLAN header has to be removed from the packet at the ingress interface (ATM PVC) when the packet returns.

How to Configure Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Configuring Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs

Perform this task to configure the Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature.

Note   Only one **bridge-dot1q encap** *vlan-id* command can be configured under a PVC. Only one VLAN ID is allowed per session using PPPoE. The PPPoE session can be disconnected if the configured VLAN ID (set using the **set vlan-inner** or **bridge-dot1q encap** *vlanid* command) differs from the default VLAN ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-all egress**
4. **match qos-group** *number*
5. **class-map match-all ingress**
6. **match input-interface** *name*
7. **policy-map egress-policy**
8. **class egress**
9. **set cos** *number*
10. **set vlan-inner** *number*
11. **exit**
12. **exit**
13. **policy-map ingress-policy**
14. **class ingress**
15. **set qos-group** *number*
16. **exit**
17. **exit**
18. Enter one of the following:

    • **interface atm** *interface-id* **point-to-point**
    • **interface atm** *slot* **/ 0 point-to-point**
    • **interface atm** *slot/ port-adaptor/***0 point-to-point**

19. **bridge-group** *group-number*
20. **pvc** *vpi/vci*
21. **bridge-dot1q encap** *provider-vlan-id*
22. **encapsulation aal5snap**
23. **service-policy out egress-policy**
24. **pppoe-client dial-pool-number** *number*
25. **pppoe-client control-packets vlan cos** *number*
26. **service-policy input ingress-policy**
27. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	**Purpose**
Step 3	**class-map match-all egress** **Example:** Device(config)# class-map match-all egress	Determines how packets are evaluated when multiple match criteria exist for the egress.
Step 4	**match qos-group** *number* **Example:** Device(config)# match qos-group 101	Identifies a specific quality of service (QoS) group value as a match criterion. The range is from 0 to 1023.
Step 5	**class-map match-all ingress** **Example:** Device(config)# class-map match-all ingress	Determines how packets are evaluated when multiple match criteria exist for the ingress.
Step 6	**match input-interface** *name* **Example:** Device(config)# match input-interface Vlan2	Configures a class map to use the specified input interface as a match criterion.
Step 7	**policy-map egress-policy** **Example:** Device(config)# policy-map egress-policy	Creates or modifies a policy map that can be attached to one or more interfaces to specify an egress service policy and enters policy-map configuration mode.
Step 8	**class egress** **Example:** Device(config-pmap)# class egress	Specifies the name of the egress class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode.
Step 9	**set cos** *number* **Example:** Device(config-pmap-c)# set cos 5	Sets the CoS value. The range is from 0 to 7. **Note** The "set cos <value>" command marks the DOT1Q packets sent through the ATM interface with a cos(bitp) value over ATM AAL header. To set the "set cos <value>" command in action, a policy needs to be installed on the interface using the command "service-policy out <policy-name>". Once the policy is enabled, the "set cos <value>" command attaches the specific cos value under the VLAN header. This feature is available from 17.7 release.
Step 10	**set vlan-inner** *number* **Example:** Device(config-pmap-c)# set vlan-inner 333	(For PPPoE) Sets the inner VLAN value. The range is from 1 to 4094.
Step 11	**exit** **Example:** Device(config-pmap-c)# exit	Exits policy-map class configuration mode and returns to policy-map configuration mode.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.
Step 13	**policy-map ingress-policy** **Example:** `Device(config)# policy-map ingress-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify an ingress service policy and enters policy-map configuration mode.
Step 14	**class ingress** **Example:** `Device(config-pmap)# class ingress`	Specifies the name of the ingress class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode
Step 15	**set qos-group** *number* **Example:** `Device(config-pmap-c)# set qos-group 101`	Sets the CoS value for a CoS group. The range is from 0 to 1023.
Step 16	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 17	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.

Step 18	Enter one of the following:
	
	    • **interface atm** *interface-id* **point-to-point**
	    • **interface atm** *slot* **/ 0 point-to-point**
	    • **interface atm** *slot*/ *port-adaptor*/**0 point-to-point**
	
	Example:
	`Device(config)# interface atm0 point-to-point`
	
	Example:
	`Device(config)# interface atm 0/0 point-to-point`
	
	Example:
	`Device(config)# interface atm 0/1/0.1 point-to-point`
		Specifies the ATM point-to-point interface using the appropriate format of the command and enters interface or subinterface configuration mode.

Step 19	**bridge-group** *group-number* **Example:** `Device(config-if)# bridge-group 1`	Assigns the interface or subinterface to a bridge group.
Step 20	**pvc** *vpi/vci* **Example:**	Creates a PVC of a specified virtual path identifier (VPI)/virtual circuit identifier (VCI) number and enters

	Command or Action	Purpose
	`Device(config-if)# pvc 9/117`	interface ATM VC configuration mode or subinterface ATM VC configuration mode.
Step 21	**bridge-dot1q encap** *provider-vlan-id* **Example:** `device(config-if-atm-vc)# bridge-dot1q encap`	Enables the router to include the 802.1Q VLAN ID in the MAC PDU. The service provider VLAN ID range is from 1 to 4094.
Step 22	**encapsulation aal5snap** **Example:** `Device(config-if-atm-vc)# encapsulation aal5snap`	Specifies the ATM Adaptation Layer 5 (AAL5) encapsulation type. AAL5SNAP is used so that two or more protocols can be multiplexed over the virtual circuit.
Step 23	**service-policy out egress-policy** **Example:** `Device(config-if-atm-vc)# service-policy out egress-policy`	Defines the service policy at the egress.
Step 24	**pppoe-client dial-pool-number** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures a PPP over Ethernet (PPPoE) client and specifies dial-on-demand routing (DDR) functionality.
Step 25	**pppoe-client control-packets vlan cos** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client control-packets vlan cos 6`	Enables CoS marking for PPPoE control packets on the PPPoE client.
Step 26	**service-policy input ingress-policy** **Example:** `Device(config-if-atm-vc)# service-policy input ingress-policy`	Defines the service policy at the ingress.
Step 27	**end** **Example:** `Device(config-if-atm-vc)# **end**`	Exits interface ATM VC configuration mode, or subinterface ATM VC configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp authentication**

- **debug ppp negotiation**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**

   • **debug aaa authorization**

> ⚠
>
> **Caution**   Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

Configuration Examples for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Example: Traffic from Multiple Incoming VLANs Bridged to a VLAN

The following example shows how the traffic from multiple incoming VLANs is bridged to a single outgoing VLAN. The traffic arrives on Layer 2 Fast Ethernet ports and a DHCP server assigns IP addresses on the private network. Network Address Translation (NAT) is enabled. A static IP address is used on the outgoing Bridge-Group Virtual Interface (BVI) interface.

This topology is shown in the figure below.

Figure 5: Topology: Traffic from Multiple Incoming VLANs Bridged to a Single Outgoing VLAN
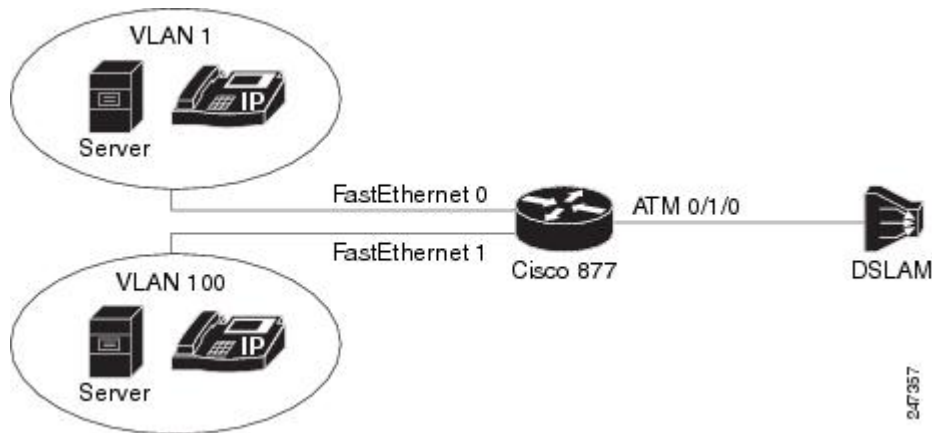
The following configuration is for the Cisco 877 router.

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
!
bridge irb
!
```

```
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 0/110
  bridge-dot1q encap 10
  encapsulation aal5snap
!
interface FastEthernet0
 switchport access vlan 1
!
interface FastEthernet1
 switchport access vlan 100
!
interface Vlan1
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan100
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI1
 ip address 10.0.0.0 255.0.0.0
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip nat pool test 10.0.0.0 10.0.0.0 netmask 255.0.0.0
ip nat inside source list 101 pool test overload
ip nat inside source list 102 pool test overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
!
```

Example: Traffic from Multiple VLANs Arrives at the Router over a Layer 3 Port

The following example shows how traffic from multiple VLANs arrives at the router over a Layer 3 port. All this traffic is bridged over a single ATM virtual circuit to the service provider's DSLAM and tagged with a single VLAN tag. Both WAN and LAN IP addresses are provided by DHCP servers.

This topology is shown in the figure below.

Figure 6: Topology: Traffic From Multiple VLANs Arrives at the Router over a Layer 3 Port
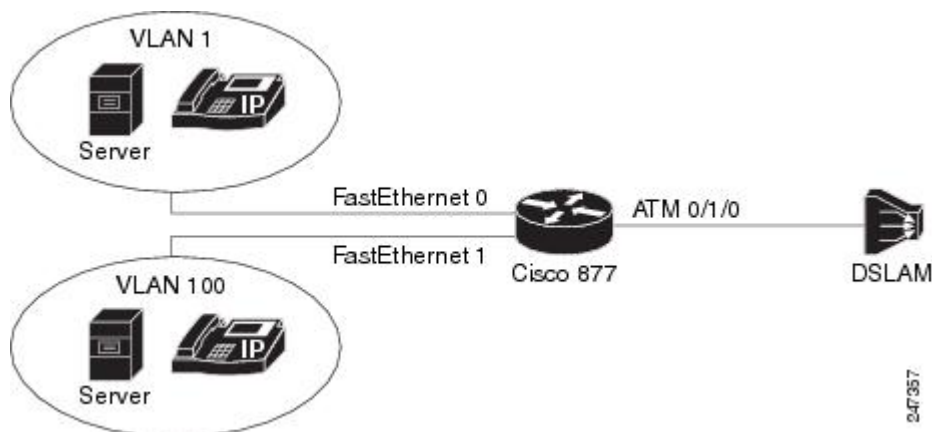
The following configuration is for the Cisco 877 router.

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
bridge irb
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
 interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/1.2
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface ATM0/1/0
 no ip address
 no atm ilmi-keepalive
!
!
interface ATM0/1/0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 9/117
  bridge-dot1q encap 10
  encapsulation aal5snap
```

```
!
!
interface BVI1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
!
ip nat inside source list 101 interface BVI1 overload
ip nat inside source list 102 interface BVI1 overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List , All Releases
ATM commands	Cisco IOS Asynchronous Transfer Mode Command Reference

Standards and RFCs

Standard/RFC	Title
IEEE 802.1P	*Traffic Class Expediting and Dynamic Multicast Filtering*
IEEE 802.1Q	*Virtual LANs*
IEEE 802.3	*LAN/MAN CSMA/CD (Ethernet) Access Method*
ITU-T G.992.1 (G.dmt)	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers*
ITU-T G.992.5	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers-Extended Bandwidth ADSL2 (ADSL2+)*
ITU-T I363.5	*B-ISDN ATM Adaptation Layer Specification: Type 5 AAL*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Feature Name	Releases	Feature Information
Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks	15.1(2)T	The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1P marking based on 802.1Q tags and transportation of these tags over ATM PVC used in ADSL2+ uplinks. The following commands were introducef: **pppoe-client control-packets vlan cos**, **set vlan-inner**.
Transporting VLAN Tags over DSL Links	15.0(1)XA	The Transporting VLAN Tags over DSL Links feature allows 802.1Q tags to be transported over ATM PVCs used in ADSL2+ uplinks. The following command was introducef: **bridge-dot1q encap**.

Glossary

802.1ad—An amendment to IEEE 802.1Q that enables a service provider to offer bridged VLANs over its network.

802.1P—A 3-bit field within an Ethernet frame header added when using IEEE 802.1Q on an IEEE 802.1D network. It specifies a priority value from 0 and 7 that can be used by quality of service (QoS) disciplines to differentiate traffic.

802.1Q—A networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks. 802.1Q is commonly referred to as VLAN tagging.

AAL5SNAP—ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol. A type of network encapsulation that supports multiplexing of two or more protocols over a virtual circuit.

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

BVI—Bridge Group Virtual Interface. A logical Layer 3-only interface associated with a bridge group when integrated bridging and routing (IRB) is configured.

CPE—Customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. This term can also refer to any telephone equipment residing on the customer site.

CVLAN—Customer Virtual Local Area Network.

DSL—Digital subscriber line. A public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL.

DSLAM—Digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

IRB—Integrated routing and bridging. Integrated Services Digital Network (ISDN) User Part. An upper-layer application supported by Signalling System 7 for connection setup and tear down.

NAT—Network Address Translation. A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

PVC—Permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, this is called a permanent virtual connection.

VoIP—Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with plain old telephone service (POTS) like functionality, reliability, and voice quality.