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

First Published: October 21, 2009
Last Updated: Sept 17, 2010

The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1Q tags to be transported over Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVC) used in Asymmetric Digital Subscriber Line 2+ (ADSL2+) uplinks. In addition, 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks" section on page 16.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

Configuration Skills

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

Routers Supported

You must configure this feature on a supported router. Table 1 lists the routers supported in this release.

Table 1 Routers Supported

ADSL Mode	ADSL Card Types	Supported Platforms
Fixed Configuration Routers/Platforms		
A Digital Subscriber Line (ADSL) over Plain Old Telephone Service (POTS) and ADSL over ISDN		Cisco 876, Cisco 877, Cisco 877M, Cisco 878, Cisco 1801, Cisco 1801M, Cisco 1802, Cisco 1803, Cisco 867, Cisco 886, Cisco 887, Cisco 888 (including Wireless, Integrated Access Devices (IAD), and Survivable Remote Site Telephony (SRST) variants)
Modular Configuration Routers/Platforms		
ADSL over POTS and ADSL over ISDN SHDSL HWICs	HWIC-1ADSL, HWIC-ADSL-B/ST, HWIC-1ADSLI, HWIC-ADSLI-B/ST, HWIC-1ADSL-M HWIC-2SHDSL, HWIC-4SHDSL	Cisco 1841, Cisco 2801, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845, Cisco 1921, Cisco 1941, Cisco 2901, Cisco 2911, Cisco 2921, Cisco 2951, Cisco 3925, and Cisco 3945. **Note** In addition to the above mentioned platforms, HWIC-1ADSL-M, HWIC-2SHDSL and HWIC-4SHDSL modules are supported on Cisco 3925e and Cisco 3945e.

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

The following restrictions apply to this release:

- Supports only one bridged 802.1Q VLAN.
- Configures only on a point-to-point ATM subinterface.
- Uses 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

This feature supports the deployment of voice, video, and data services on customer premises equipment (CPE) by enabling the router to transport 802.1Q tags over ATM PVCs. This feature requires an ADSL2+ data connection.

To configure the Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature, you should understand the following concepts:

- VLAN-Based Service Differentiation over ADSL, page 3
- Transporting 802.1P Marked 802.1Q Tags, page 4
- Benefits of Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks Feature, page 6

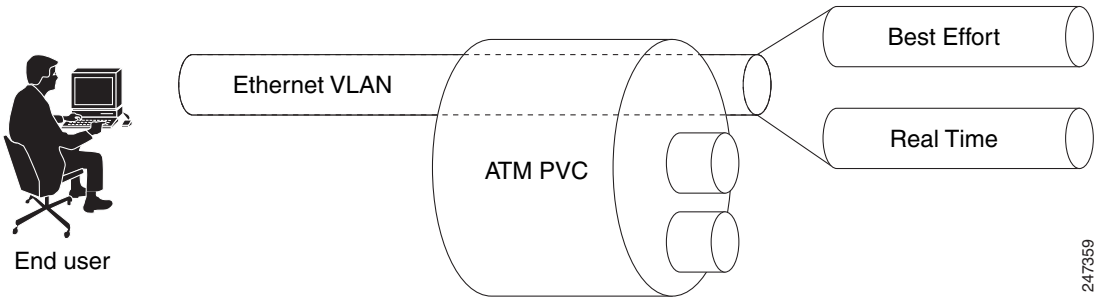
VLAN-Based Service Differentiation over ADSL

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 router. 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 Figure 3.

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 PVC level is shown in Figure 1.

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 Figure 2.

Figure 2 Operation of the bridge-dot1q encap Command

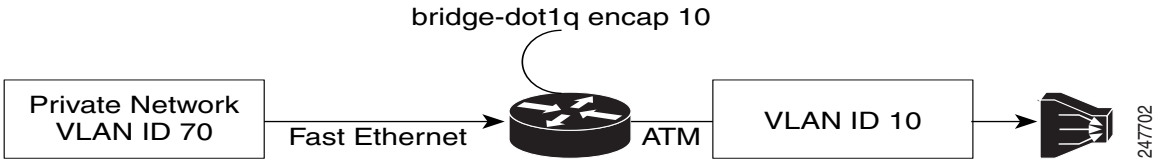


Figure 3 and Figure 4 show the PDU data structure in greater detail.

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 Figure 3 and in Figure 4.

Figure 3 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

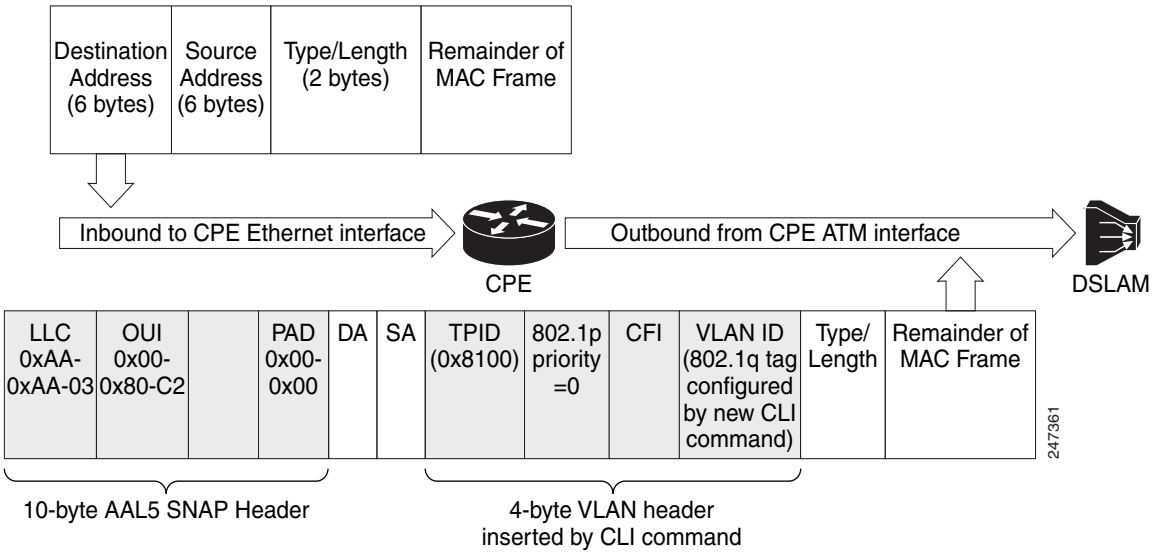
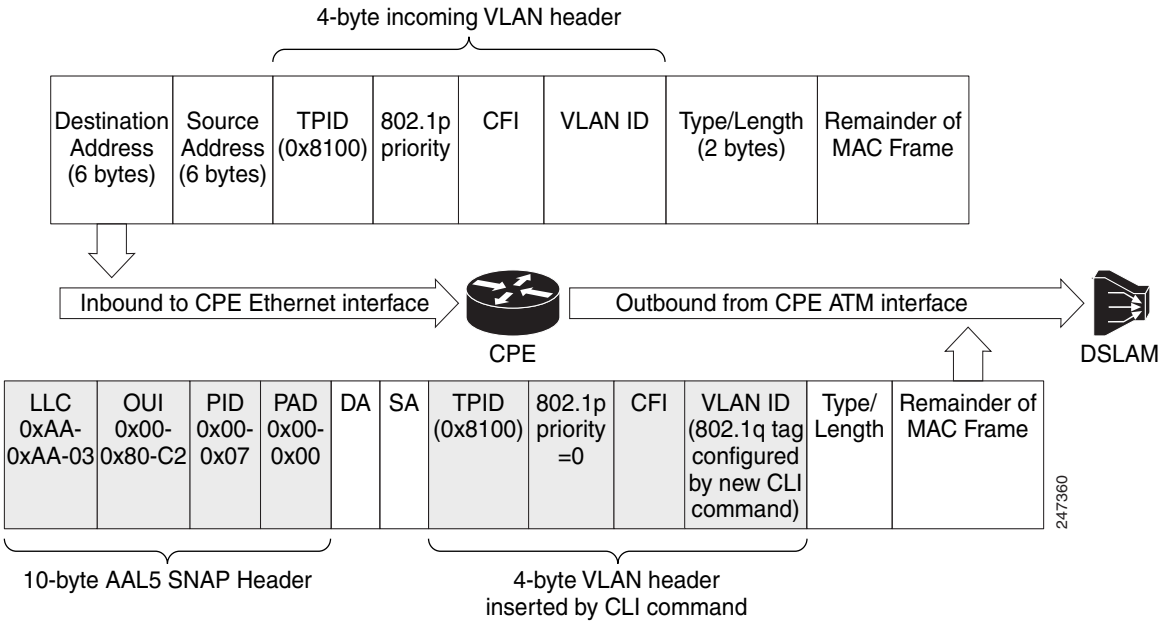


Figure 3 shows that a 4-byte VLAN header has been inserted in the outgoing packet, with an 802.1P value. The VLAN ID value is configured by the **bridge-dot1q encap** command.

Figure 4 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 3.

Note The 802.1P priority that was configured earlier is changed to 0, and any VLAN ID 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 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 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.

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

This feature offers the following benefits:

- Customer premise equipment (CPE) to carry traffic with 802.1P marked provider-specific 802.1Q tags.
- Deployment of voice, video, and data services at customer premises. This service combination offers a real-time channel dedicated to Voice over IP (VoIP) traffic, and a second channel that delivers best-effort Internet service.
- All traffic is marked with an 802.1P marking and implemented using VLAN-based service differentiation.

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

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

Restrictions

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-inner** *number*
10. **set vlan-inner** *number*
11. **policy-map ingress-policy**
12. **class ingress**
13. **set qos-group** *number*
14. **interface atm** *interface-id* **point-to-point**
15. **bridge-group** *group-number*
16. **pvc** *vpi/vci*
17. **encapsulation aal5snap**
18. **service-policy out egress-policy**
19. **bridge-dot1q encap** *provider-vlan-id*
20. **pppoe-client dial-pool-number** *number*
21. **pppoe-client control-packets vlan cos** *number*
22. **service-policy input ingress-policy**
23. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-all egress** **Example:** `Router(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:** `Router(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:** `Router(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:** `Router(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:** `Router(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.
Step 8	**class egress** **Example:** `Router(config-pmap)# class egress`	Specifies the name of the egress 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.
Step 9	**set cos-inner** *number* **Example:** `Router(config-pmap-c)# set cos-inner 5`	Sets the inner CoS value. The range is from 0 to 7.
Step 10	**set vlan-inner** *number* **Example:** `Router(config-pmap-c)# set vlan-inner 333`	(For PPPoE) Sets the inner VLAN value. The range is from 1 to 4094.

	Command or Action	Purpose
Step 11	**policy-map ingress-policy** **Example:** `Router(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.
Step 12	**class ingress** **Example:** `Router(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.
Step 13	**set qos-group** *number* **Example:** `Router(config-pmap-c)# set qos-group 101`	Sets the CoS value for a CoS group. The range is from 0 to 1023.

Step 14	**interface atm** *interface-id* **point-to-point**
	or
	interface atm *slot*/**0 point-to-point**
	or
	interface atm slot/*port-adaptor*/**0 point-to-point**
	
	Example:
	`Router(config)# interface atm0 point-to-point`
	or
	
	Example:
	`Router(config)# interface atm 0/0 point-to-point`
	or
	
	Example:
	`Router(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 15	**bridge-group** *group-number* **Example:** `Router(config-if)# bridge-group 1`	Assigns the interface or subinterface to a bridge group.
Step 16	**pvc** *vpi/vci* **Example:** `Router(config-if)# pvc 9/117`	Creates a PVC of a specified VPI/VCI number and enters interface ATM VC configuration mode or subinterface ATM VC configuration mode.
Step 17	**bridge-dot1q encap** *provider-vlan-id* **Example:** `Router(config-if-atm-vc)# bridge-dot1q encap 10`	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 18	**encapsulation aal5snap** **Example:** `Router(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.

	Command or Action	Purpose
Step 19	**service-policy out egress-policy** **Example:** `Router(config-if-atm-vc)# service-policy out egress-policy`	Defines the service policy at the egress.
Step 20	**pppoe-client dial-pool-number** *number* **Example:** `Router(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures a PPP over Ethernet (PPPoE) client and to specifies dial-on-demand routing (DDR) functionality.
Step 21	**pppoe-client control-packets vlan cos** *number* **Example:** `Router(config-if-atm-vc)# pppoe-client control-packets vlan cos 6`	Enables CoS marking for PPPoE control packets on the PPPoE client.
Step 22	**service-policy input ingress-policy** **Example:** `Router(config-if-atm-vc)# service-policy input ingress-policy`	Defines the service policy at the ingress.
Step 23	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits interface ATM VC configuration mode, or subinterface ATM VC configuration mode.

Troubleshooting Tips

You need to verify that the **bridge-dot1q encap** and **encapsulation aal5snap** commands are configured to carry the tagged VLAN traffic if the 802.1P marked 802.1Q tags are not transported in the MAC PDUs sent to the DSLAM.

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

This section provides the following configuration examples:

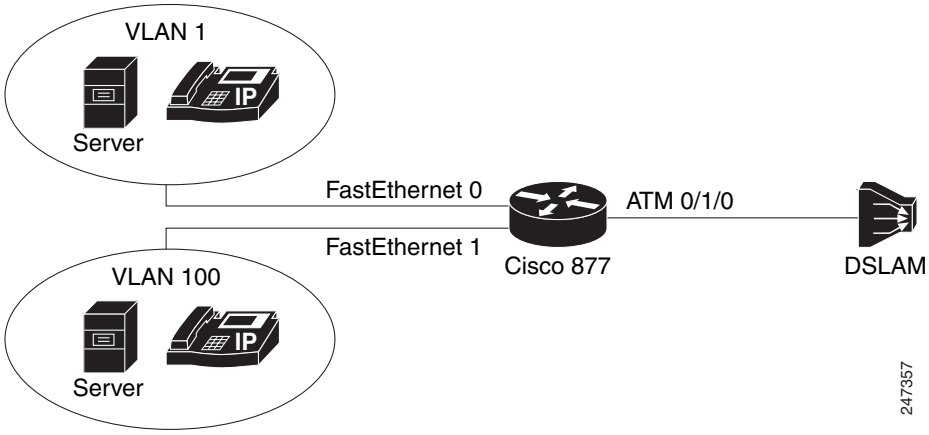
- Example: Traffic from Multiple Incoming VLANs Bridged to a Single Outgoing VLAN, page 11
- Example: Traffic from Multiple VLANs Arrive at Router over Layer-3 Port, page 12

Example: Traffic from Multiple Incoming VLANs Bridged to a Single Outgoing VLAN

This example shows how the traffic from multiple incoming VLANs is bridged to a single outgoing VLAN. The traffic is arriving 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 Figure 5.

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
!
```

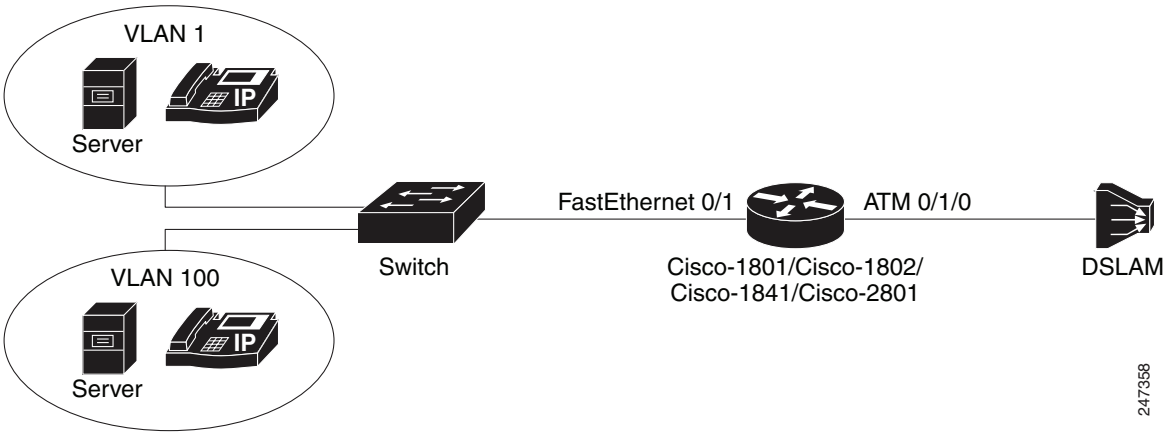
```
interface FastEthernet1
 switchport access vlan 100
!

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 12.0.0.1 255.0.0.0
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 12.0.0.2
ip nat pool test 12.0.0.1 12.0.0.1 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 Arrive at Router over Layer-3 Port

This example shows how traffic from multiple VLANs arrive 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 Figure 6.

Figure 6 Topology: Traffic From Multiple VLANs Arrive at Router over 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
ATM commands: complete command syntax, command mode, command history, usage guidelines, and examples.	*Cisco IOS Asynchronous Transfer Mode Command Reference*

Standards

Standard	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 I363.5	*B-ISDN ATM Adaptation Layer Specification: Type 5 AAL*
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+)*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2684	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support 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

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2 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.

Table 2 Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Feature Name	Releases	Feature Information
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 Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVC) used in ADSL2+ uplinks. The following command was introduced: **bridge-dot1q encap**.
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 transported over ATM PVC used in ADSL2+ uplinks. The following commands were introduced: **set vlan-inner**, **pppoe-client control-packets vlan cos**.

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 when using IEEE 802.1Q on an IEEE 802.1D network. It specifies a priority value of between 0 and 7 inclusive 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. Logical Layer 3-only interface associated with a bridge group when 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. 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 set up and tear down.

NAT—Network Address Translation. 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 POTS-like functionality, reliability, and voice quality.