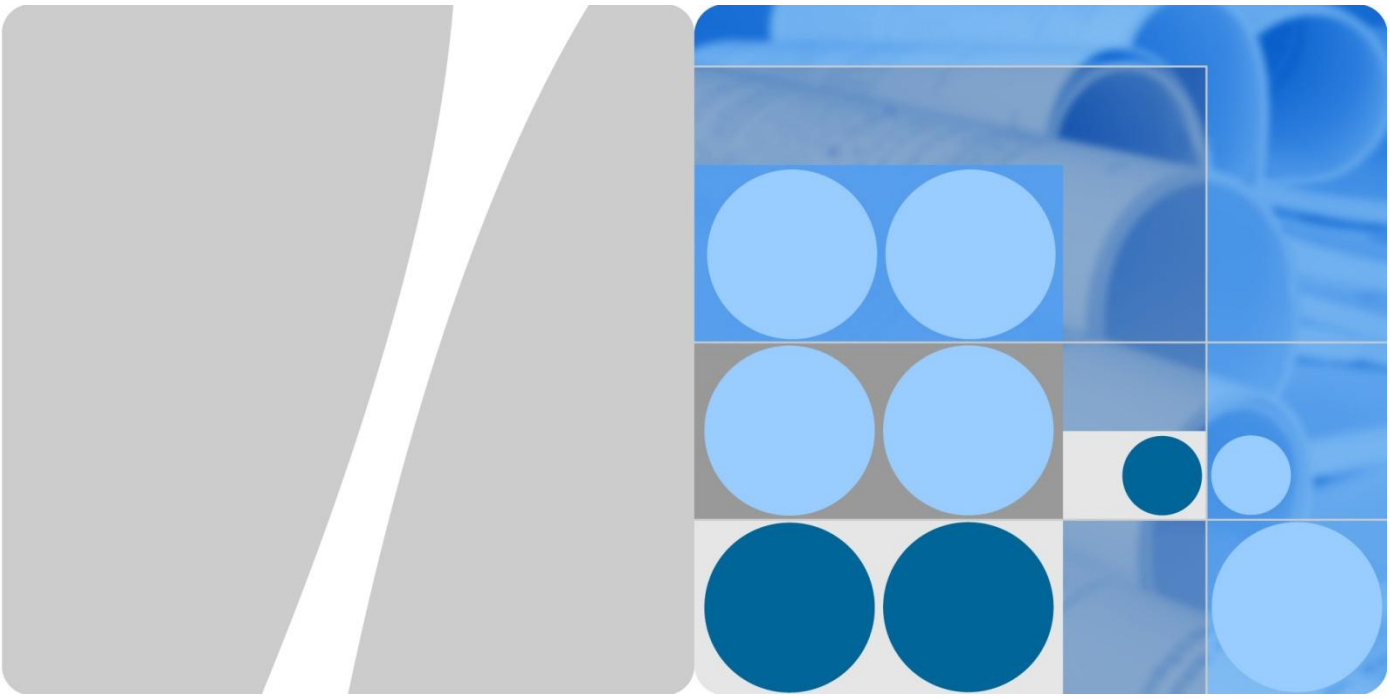


VLAN and QinQ Technology White Paper

Issue 1.01

Date 2012-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Abstract

Virtual Local Area Networks (VLANs) logically divide devices in a LAN into different network segments to implement virtual work groups. As defined by the IEEE 802.1Q VLAN standard drafted in 1999, QinQ expands the VLAN space by adding an 802.1Q VLAN tag to an 802.1Q-tagged packet. As Ethernet networks develop, more QinQ encapsulation and termination modes are used for fine-grained service management. The white paper explains the QinQ technology.

Keywords

VLAN, QinQ, selective QinQ, VLAN mapping, voice VLAN, super VLAN, MUX VLAN, guest VLAN

Abbreviation List

Abbreviation	Full Name
VLAN	Virtual Local Area Network
QinQ	802.1Q in 802.1Q
TPID	Tag Protocol Identifier
ACL	Access Control List
VPN	Virtual Private Network
QoS	Quality of Service
CSMA/CD	Carrier Sense Multiple Access/Collision Detect

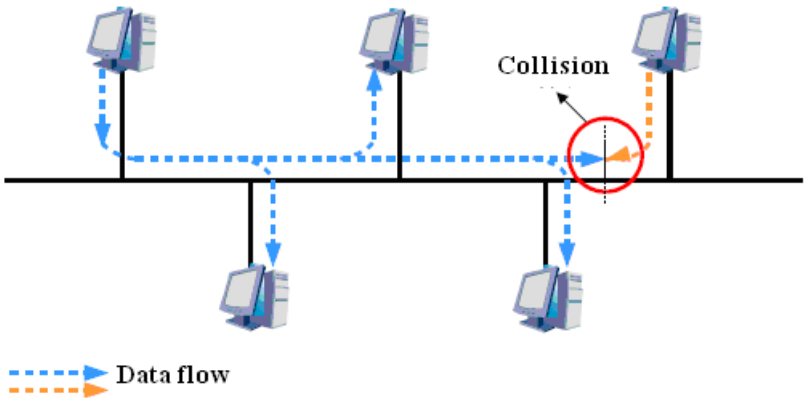
Contents

1 VLAN Technology

1.1 Background

In the traditional Ethernet networking, multiple hosts are connected through a coaxial cable as shown in Figure 1-1.

Figure 1-1 Networking of the traditional LAN



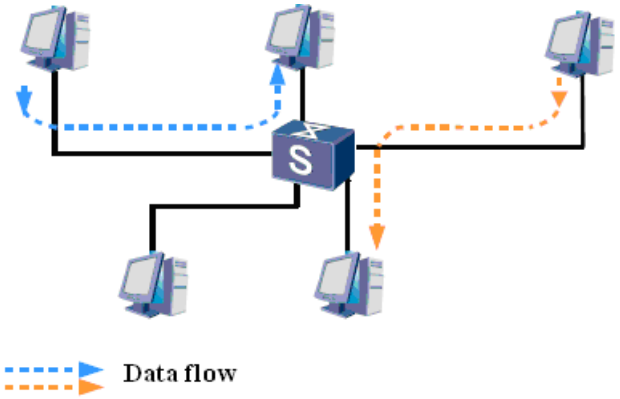
This networking mode has the following disadvantages:

- Only one host is allowed to send packets at a time. If two or more hosts send packets simultaneously, the packets collide.
- Packets from a host are broadcast over the network, and all the other hosts can receive packets from this host. In this manner, the network forms a broadcast domain. As the number of hosts increases, their broadcasts consume a large amount of bandwidth.
- All hosts share a transmission channel, which cannot ensure security of the transmitted data.

  Ethernet uses Carrier Sense Multiple Access/Collision Detect (CSMA/CD) technology to ensure that information is transmitted in the collision domain without interference. However, when many hosts are on the network, problems arise, such as severe collisions and excess broadcast packets. These problems impair performance and lead to network unavailability.

To enable LANs to accommodate more hosts and prevent collisions, bridges are introduced to connect two collision domains. A bridge is evolved to Layer 2 switches. See Figure 1-2.

Figure 1-2 L2 switch networking



Bridges and Layer 2 switches forward data from inbound interfaces to outbound interfaces. By separating the network segments attached to these interfaces, Layer 2 switches solve the problem of excessive collisions on the shared media and limit the collisions to interfaces. Compared to bridges, switches can separate multiple collision domains.

Layer 2 switches receive all data frames on the network, learn source MAC addresses of frames, and create a MAC address table to record the mapping between MAC addresses and interfaces. The switches can then perform Layer 2 forwarding based on their destination MAC addresses. If the destination MAC address of a frame is not in the MAC address table, Layer 2 switches broadcast the frame to all interfaces except the inbound interface of the frame. For this reason, broadcast storms can still occur on the network.

The VLAN technology solves this problem by dividing a LAN into multiple logical VLANs. Hosts in a VLAN communicate as on a LAN. In addition, VLANs cannot communicate with each. Therefore, broadcast frames are restricted in a VLAN.

The division of a VLAN is not restricted by its physical location. Hosts in different physical locations can belong to the same VLAN. Users of a VLAN can connect to the same switch or multiple switches, or even to multiple routers.

1.2 VLAN Functions

Functions of the VLAN are as follows:

- Restrict broadcast domains. Restricting a broadcast domain in a VLAN saves bandwidth and increases the network processing capability.
- Enhance LAN security. Layer 2 frames between VLANs are isolated. That is, users of a VLAN cannot communicate with users of a different VLAN. If users of different VLANs need to communicate with each other, Layer 3 devices, such as routers or Layer 3 switches, are required.

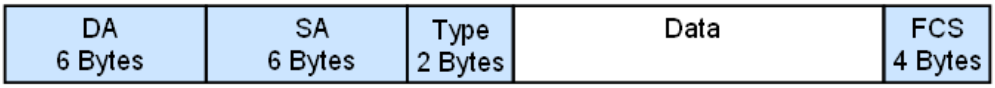
- Construct virtual work groups flexibly. VLANs can be used to divide users into different work groups. Users of a work group are not limited by their physical locations. Network establishment and maintenance are convenient and flexible.

1.3 VLAN Principle

To enable network devices to identify frames of different VLANs, frames must have data fields that identify the VLANs. Common switches work at the data link layer of the OSI model and identify frames of the data link layer. Therefore, the VLAN identification fields are added to the data link layer header.

Traditional Ethernet frames encapsulate upper level protocols after the destination MAC address and the source MAC address. See Figure 1-3.

Figure 1-3 Encapsulation format of traditional Ethernet frames



In Figure 1-3, DA indicates the destination MAC address. SA indicates the source MAC address. Type indicates the protocol type of the frame.

IEEE 802.1Q stipulates that a VLAN tag of four bytes should be encapsulated after the destination MAC address and the source MAC address.

Figure 1-4 Fields of a VLAN tag

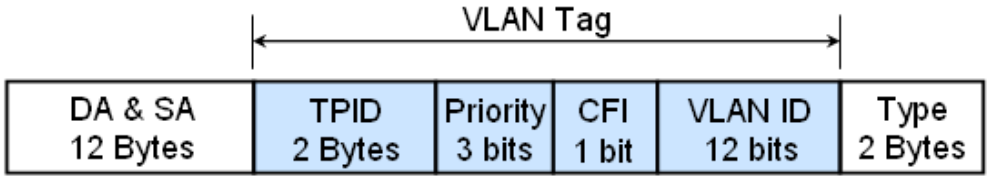


Figure 1-4 shows that a VLAN tag consists of four fields:

- Tag Protocol Identifier (TPID): determines whether a data frame contains a VLAN tag. The length of the TPID is 16 bits. The default value is 0x8100.
- Priority: represents the 802.1P priority of a frame. The length of the Priority is 3 bits.
- Canonical Format Indicator (CFI): identifies whether the MAC address is encapsulated in the standard format in different transmission mediums. The length of the CFI is 1 bit. The value 0 indicates the MAC address is encapsulated in the standard format. The value 1 indicates that the MAC address is not encapsulated in the standard format. The default value is 0.
- VLAN ID: identifies the number of the VLAN to which a frame belongs. The length of the VLAN ID is 12 bits. The value ranges from 0 to 4095. Because 0 and 4095 are reserved values of the protocol, the VLAN ID ranges from 1 to 4094.

  Network devices use VLAN IDs to identify the VLAN to which a frame belongs and process the frame depending on whether the frame carries a VLAN tag and the value of the carried VLAN tag.

2 VLAN Mapping

VLAN mapping can be used to modify VLAN tags carried in the following modes:

- Single-tagged 1:1 VLAN mapping: The outer VLAN ID of a frame is mapped to a new VLAN ID. Each VLAN ID is mapped to a different VLAN ID.
- Single-tagged N:1 VLAN mapping: The outer VLAN ID of a frame is mapped to a new VLAN ID. Multiple VLAN IDs are mapped to the same VLAN ID.
- Double-tagged 2:2 VLAN mapping: The outer and inner VLAN IDs of a frame are mapped to new outer and inner VLAN IDs.
- Double-tagged 1:1 VLAN mapping: The outer VLAN ID of a frame is mapped to a new outer VLAN ID. The inner VLAN ID remains unchanged.
- Double-tagged N:1 VLAN mapping: The outer VLAN ID of a frame is mapped to a new outer VLAN ID. The inner VLAN ID remains unchanged. An outer VLAN ID or a segment of VLAN ID of a frame can be mapped to a new outer VLAN ID. The inner VLAN ID remains unchanged.

3 Super-VLAN

3.1 Concept

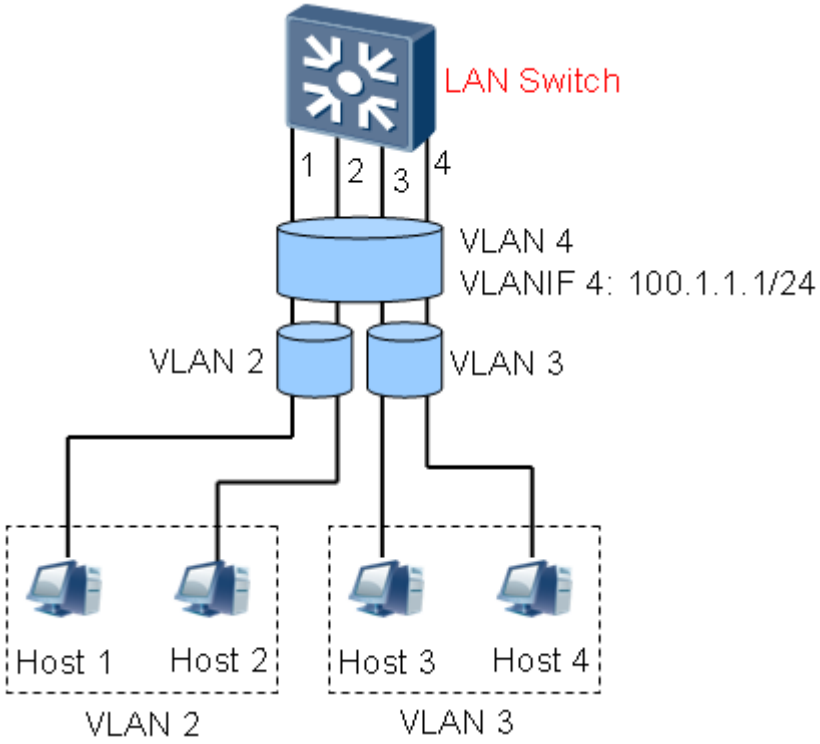
To implement inter-VLAN communication on switches, you need to configure IP addresses for the VLANIF interfaces. If the network has a large number of VLANs, they require a large number of IP addresses. VLAN aggregation can eliminate the need to use an excessive number of IP addresses for VLANs.

VLAN aggregation is also known as super-VLAN. A super-VLAN contains multiple sub-VLANs. Each sub-VLAN is a broadcast domain. Sub-VLANs are separated in Layer 2. Layer 3 interfaces can be configured in a-super VLAN, but cannot be configured in a sub-VLAN. When a user in a sub-VLAN needs to communicate at Layer 3, the IP address of a Layer 3 interface in the super-VLAN is used as the gateway IP address. Multiple sub-VLANs share one IP network segment, saving IP addresses.

In addition, to implement Layer 3 interworking between different sub-VLANs and interworking of sub-VLANs with other networks, the proxy ARP function is used. proxy ARP forwards and processes ARP request and reply packets to implement Layer 3 interworking between Layer 2 isolated ports.

3.2 Super-VLAN Networking

Figure 3-1 Super-VLAN networking



Interface 1 of the switch connects to Host1, Interface 2 to Host2, Interface 3 to Host3, and Interface 4 to Host4. Host1 and Host2 belong to sub-VLAN 2. Host3 and Host4 belong to sub-VLAN 3. Sub-VLAN 2 and sub-VLAN 3 belong to super-VLAN 4. The default gateway IP address of Host1 to Host4 is 100.1.1.1. Proxy ARP enables VLAN 2 to communicate with VLAN 3 through Layer 3.

3.3 Characteristics of Super-VLANs

A super-VLAN has the following characteristics:

- All broadcast packets and unknown traffic are transmitted in sub-VLANs. All traffic in a sub-VLAN is exchanged only in the sub-VLAN, isolating traffic between sub-VLANs.
- Hosts are deployed in sub-VLANs. You can configure an IP address for each host on the same network segment as the VLANIF interface IP address. The subnet mask of each host in a sub-VLAN is the same as the subnet mask defined by the super-VLAN. In addition, the gateway IP address is the IP address of the VLANIF interface in the super-VLAN.
- All traffic among sub-VLANs is transmitted by the VLANIF interface in the super-VLAN. For example, ICMP messages are not redirected between sub-VLANs. This is because sub-VLANs of a super-VLAN share the same network segment. When a sub-VLAN is added to a super-VLAN, the system adds an ARP entry to the IP ARP table. IP unicast packets can therefore transverse sub-VLANs. To ensure security, this function can be disabled.

- When the multicast routing protocol is enabled for a super-VLAN, IP multicast traffic among sub-VLANs is transmitted by the VLANIF interface in the super-VLAN.

The super-VLAN has the following limitations:

- A VLANIF interface cannot be configured in a super-VLAN.
- A sub-VLAN cannot be used as the super-VLAN.
- Usually, a super-VLAN does not have member ports.
- If a client moves from a sub-VLAN to another sub-VLAN, you must clear IP ARP caches on the client and the switch.

4 Voice VLANs

4.1 Concept

Multiple traffic types, such as voice and data, may coexist on broadband networks. Voice traffic requires non-delay and expedited forwarding and security.

The traditional method of increasing the transmission priority of voice traffic is to use ACLs to classify traffic and quality of service (QoS) to ensure the transmission quality. Voice VLANs help simplify these user configurations and facilitate management of transmission policies.

A voice VLAN is configured for voice traffic. By adding the ports that connect to voice devices to a voice VLAN, you can configure QoS attributes for the voice traffic, improving transmission priority and ensuring voice quality.

4.2 Implementation of Voice VLANs

A switch supporting voice VLANs identifies whether a data stream is a voice data stream based on the source MAC address in the received data frame. If the source MAC address of the frame matches the Organizationally Unique Identifier (OUI), the frame is sent in a voice VLAN. An OUI is the first 24 bits of a MAC address and is allocated to a device vendor by the IEEE.

4.3 Working Modes of Voice VLANs

A voice VLAN works in two modes:

Auto mode (dynamic)

A switch identifies voice data according to the source MAC address of a frame. When detecting voice traffic that passes through a receive port, the switch adds the port to the voice VLAN and maintains ports in the voice VLAN through the aging mechanism. During the aging period, if the port does not receive data from the source MAC address, the system deletes the port from the voice VLAN.

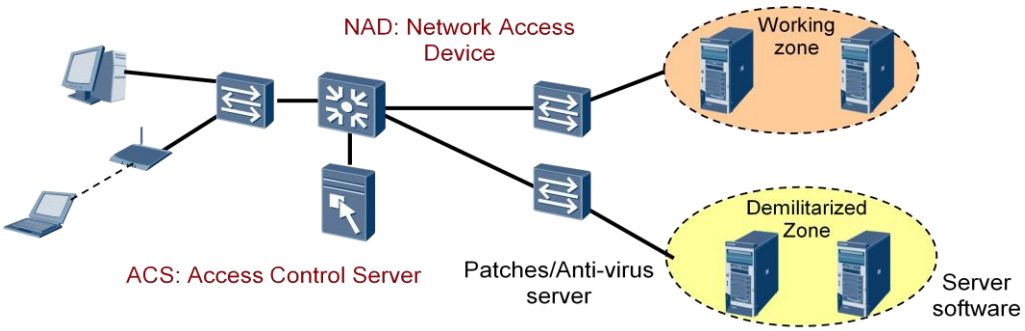
Manual mode (static)

A port is manually designated as a member port of a voice VLAN.

5 Guest VLANs

Before passing 802.1X authentication, a user authentication interface belongs to the default VLAN (guest VLAN). When users access resources in the guest VLAN, no authentication is required, whereas users cannot access other network resources. Clients that do not pass authentication belong to the guest VLAN and can access resources only in the guest VLAN server. Users can obtain 802.1x client software to upgrade clients or other application programs, such as antivirus software and operating system (OS) patches, from the guest VLAN. If no client passes authentication on a port for a period of time due to absence of the authentication client or client software with earlier version, the access device will add the port to a guest VLAN. When a client is authenticated successfully, the port is deleted from the guest VLAN and the user can access special network resources through the port.

Figure 5-1 Guest VLAN networking



- When the network access device (NAD) detects that a client has no client software installed, the NAD sets the VLAN of the port as a guest VLAN. The client can access only the demilitarized zone. The NAD can force the user to download the client software from the software server through the URL of the authentication page.
- The NAD detects the client again after a configurable period of time. If the client software is installed, the NAD performs 802.1x authentication for the client. After the client passes authentication, the port is added to the default VLAN and the client can access default resources through the VLAN.
- Clients obtain IP addresses through the Dynamic Host Configuration Protocol (DHCP) and set up connections with the ACS for security check. After the clients pass the security check, the ACS assigns a new VLAN through the CoA interface. Users in this VLAN can access the working zone.

- When detecting that a client is attacked by viruses, the ACS sets the VLAN to a guest VLAN and requests the user to update the antivirus signature database or install patches through URL redirection.
- After the user updates the antivirus signature database and the ACS detects that the client is safe, the VLAN is updated through the RADIUS COA interface.

6 MUX VLAN

6.1 Concept

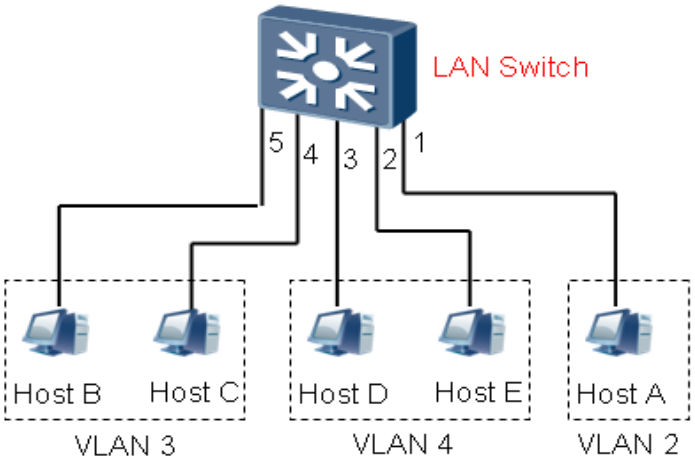
Similar to a Cisco Private VLAN, a MUX VLAN provides a Layer 2 traffic isolation mechanism between VLAN ports.

MUX VLANs include three types of ports:

- Subordinate separate port (isolated port): Separate ports belong to a separate VLAN and can communicate with MUX VLAN ports only. Traffic from a separate port can be forwarded to the related MUX VLAN port only. Except the traffic from MUX VLAN ports, the MUX VLAN discards all traffic destined for separate ports.
- Subordinate group port (community port): Group ports belong to the group VLAN and can communicate with each other and with relevant MUX VLAN ports. Group ports and separate ports are isolated in Layer 2.
- MUX VLAN port (promiscuous port): A MUX VLAN is the master VLAN. A MUX VLAN port can communicate with all ports, including separate ports and group ports. VLANs that correspond to separate ports and group ports need to be bound to the MUX VLAN.

6.2 MUX VLAN Networking

Figure 6-1 MUX VLAN networking



In Figure 6-1, VLAN 2 is the MUX VLAN and connects to port 1 of the switch. VLAN 3 is a group VLAN and connects to ports 4 and 5. VLAN 4 is a separate VLAN and connects to ports 2 and 3. The MUX VLAN technology implements the following functions:

- Host A can ping Host B and Host C; Host B and Host C can also ping Host A.
- Host A can ping Host D and Host E; Host D and Host E can also ping Host A.
- Host B and Host C can ping each other.
- Host D and Host E cannot ping each other.
- Host B and Host C are isolated from Host D and Host E, that is, they cannot ping each other.

The use of the MUX VLAN ensures security of data communication on the network. Users only need to connect to the default gateway. A MUX VLAN ensures security of Layer 2 data communication without multiple VLANs and IP subnets. All users connect to the MUX VLAN, so all users can connect to the default gateway and do not communicate with other users in the MUX VLAN. The MUX VLAN isolate all ports in a VLAN. Users in the same VLAN are not affected.

7 QinQ

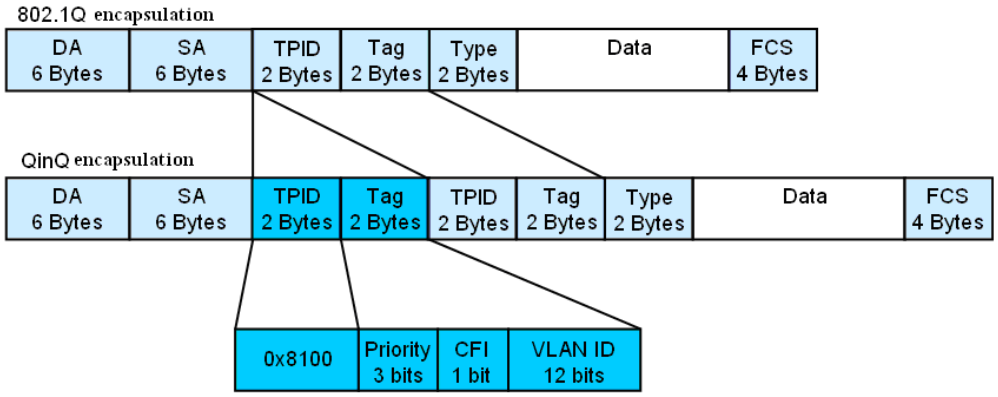
7.1 Background

The 12-bit VLAN tag field specified in IEEE 802.1Q cannot completely identify and isolate a large number of users on expanding metro Ethernet networks, as this field can only identify a maximum of 4096 VLANs. QinQ is used to solve the problem.

7.2 Principle and Application

QinQ, also known as stacking VLAN, is standardized by IEEE 802.1ad. QinQ encapsulates the VLAN tag of a private network in the VLAN tag of the public network. Therefore, the frame travels across the backbone network (public network) of a carrier with double VLAN tags. Packets are forwarded based on their outer VLAN tags on the public network. Inner VLAN tags of packets are transmitted as data on the public network. The QinQ is a flexible and easy-to-implement Layer 2 VPN technique, which is an extension to Multi-Protocol Label Switching (MPLS) VPN on the core network. QinQ can be used with MPLS VPN to form an end-to-end VPN solution.

Figure 7-1 Format of QinQ packets



QinQ packets have a fixed format. An 802.1Q-tagged packet is encapsulated in another 802.1Q tag. QinQ packets have four more bytes than common 802.1Q-tagged packets.

With great extensibility, the QinQ technology supports stacking, which is only limited by the Ethernet frame length.

In the industry, QinQ is also called Tag in Tag, VLAN VPN, stacking VLAN, and SVLAN.

Adding a VLAN tag increases 4096 VLANs. A double-tagged Ethernet frame can support 4096 × 4096 VLANs.

QinQ has the following advantages:

- Saves public VLAN IDs.
- Allows users to plan their own private VLAN IDs so that the private VLAN IDs do not conflict with the public VLAN ID.
- Provides a simple Layer 2 VPN solution for small-scale MANs or enterprise networks.

Compared to an MPLS-based Layer 2 VPN, QinQ has the following features:

- Provides a simpler Layer 2 VPN tunnel.
- Be implemented through static configuration, without a signaling protocol.

Different vendors use different TPIDs of QinQ packets. Huawei uses the default value 0x8100, while some vendors use 0X9100. To implement interworking, Huawei supports the QinQ protocol type setting on interfaces. That is, users can set the TPID to 0x9100 on a Huawei device interface (the value can be specified by the users randomly). The interface replaces the TPID value in the outer tag of the packet with 0x9100 and then transmits the packet, so QinQ packets sent to other ports can be identified by non-Huawei devices.

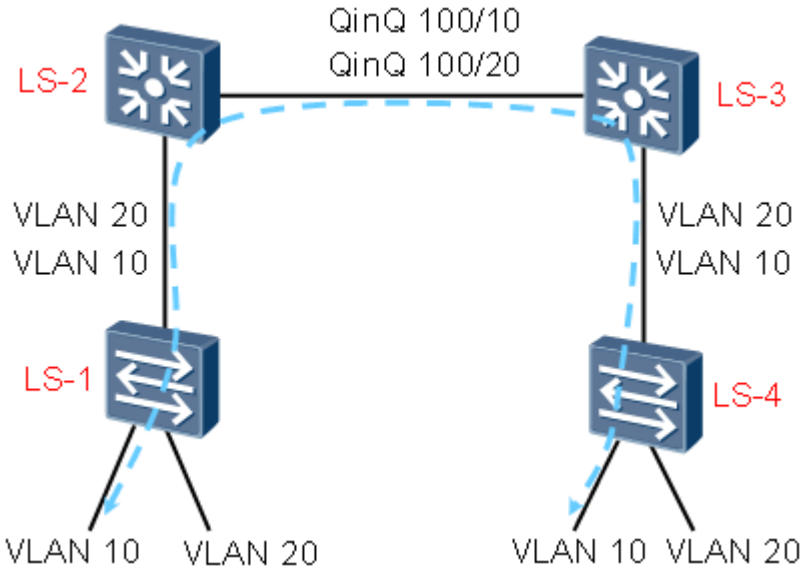
7.3 Implementation of QinQ

There are two types of QinQ implementations: basic QinQ and selective QinQ.

Basic QinQ

Basic QinQ is a port-based feature implemented through VLAN VPN. When a frame arrives at an interface that has VLAN VPN enabled, the switch will tag it with the interface's default VLAN tag, regardless of whether the frame is tagged or untagged. If the packet received is tagged, it has double VLAN tags after encapsulation. If the packet received is untagged, it has the default VLAN tag of the interface after encapsulation.

Figure 7-2 Implementation of basic QinQ



Basic QinQ frame processing works as follows (Figure 7-2):

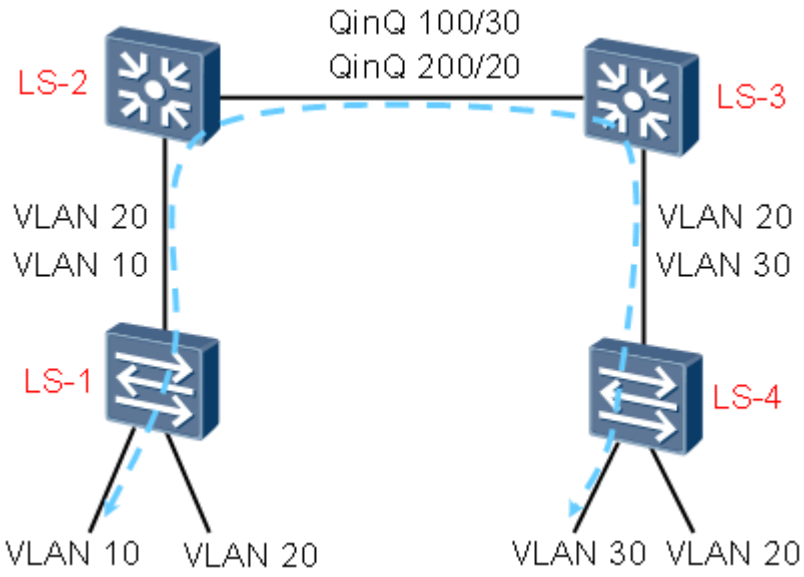
1. Switch LS-1 receives a frame with VLAN IDs of 10 and 20 and sends the frame to switch LS-2.
2. After receiving the frame, LS-2 adds an outer tag with VLAN 100.
3. The frame carrying double tags is forwarded on the network based on the Layer 2 forwarding process.
4. After receiving the frame from VLAN 100, switch LS-3 strips off the outer VLAN tag with VLAN 100. LS-3 sends the frame to switch LS-4. The frame has only one tag with VLAN 10 or 20.
5. After receiving the frame, LS-4 forwards the frame based on the VLAN ID and destination MAC address.

Interface-based QinQ has inflexible encapsulation of the outer VLAN tag. Switches have interface-based QinQ enabled cannot choose encapsulation methods for the outer VLAN tag based on service types.

Selective QinQ

Selective QinQ can choose whether to tag frames or determine the type of outer VLAN tags to be encapsulated based on the traffic classification result. Selective QinQ can classify traffic based on the VLAN tag, priority, MAC address, IP protocol, source IP address, destination IP address, or port number of an application program.

Figure 7-3 Implementation of selective QinQ



Selective QinQ frame processing works as follows (Figure 7-3):

1. Switch LS-1 receives a frame with VLAN IDs of 10 and 20 and sends the frame to switch LS-2.
2. After receiving the frame with VLAN 10, LS-2 substitutes the existing tag with 30 and adds an outer VLAN tag with VLAN 100. After receiving the frame with VLAN 20, LS-2 keeps the existing tag and adds an outer VLAN tag with VLAN 200.
3. The frame with double tags is forwarded based on the Layer 2 forwarding process.
4. After receiving the frame, switch LS-3 strips off the outer VLAN tag with VLAN 100 or 200. LS-3 sends the frame to switch LS-4. The frame has only one tag with VLAN30 or 20.
5. After receiving the frame, LS-4 forwards the frame based on the VLAN ID and destination MAC address.

8 Application of VLAN Mapping and Selective QinQ

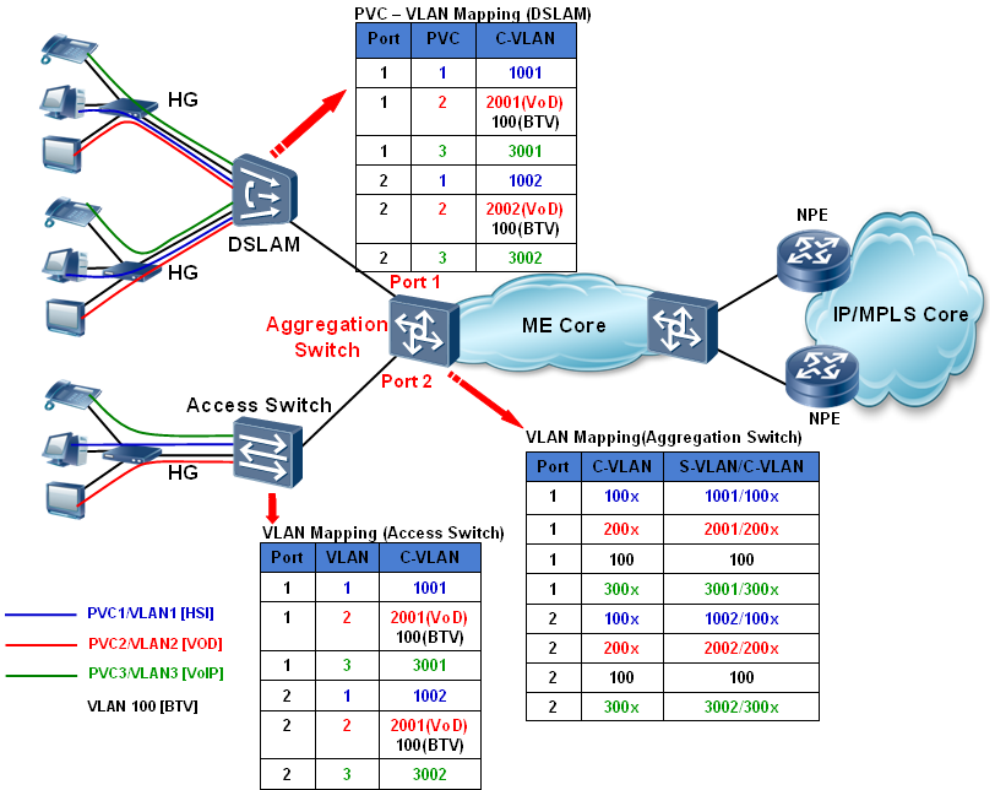
8.1 Individual User Access to the MAN

VLAN mapping and the selective QinQ can easily encapsulate the outer VLAN tag of a frame based on different users, services, and priorities, and implement different solutions for different services.

VLAN mapping and selective QinQ technologies are widely used on MANs.

8.1.1 Application of 1:1 VLAN Mapping and Selective QinQ

Figure 8-1 Application of VLAN Mapping and Selective QinQ in MANs



As shown in Figure 8-1, MANs use the QinQ technology. There are two access modes for broadband users: ADSL and LAN access. A user uses multiple services, such as HSI, VoIP, and IPTV.

In ADSL access, the digital subscriber line access multiplexer (DSLAM) supports multiple permanent virtual connections (PVCs) and uses different PVCs to carry different services. For example, PVC 1 is used to carry HSI service, PVC 2 carries IPTV service, and PVC 3 carries VoIP service. All home gateways (HGs) use the same configuration. The DSLAM maps the PVC to a VLAN according to the port number and PVC. Figure 8-1 shows the mapping relationship. For example, The VLAN IDs for Internet access of PCs range from 1001 to 2000. The VLAN IDs for the VoD service range from 2001 to 3000. The VLAN IDs of the VoIP service range from 3001 to 4000. For the BTV service, multicast VLAN 100 is used.

In LAN access, HGs use different VLANs for different services. For example, VLAN 1 carries the HSI service, VLAN 2 carries the IPTV service, and VLAN 3 carries the VoIP service. All HGs use the same configuration. The access switch maps VLANs as shown in Figure 8-1. Multicast VLAN 100 is also used for the BTV service.

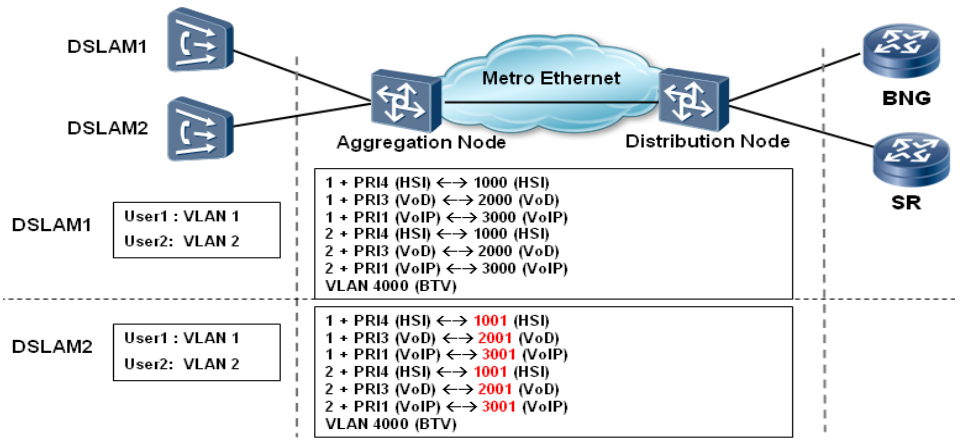
The aggregation switch tags services with different outer VLAN tags based on VLAN IDs. For example, on port 1, the aggregation switch tags the Internet access service with the outer VLAN tag of VLAN 1001, the VoD service with the outer VLAN tag of VLAN 2001, and the VoIP service with the outer VLAN tag of VLAN 3001. The inner VLAN tags represent user information. The outer VLAN tags represent service information, and also location information of DSLAMs or access switches. Different DSLAMs or access switches are tagged with different outer VLAN tags. User data is forwarded to the NPE according to the outer VLAN tags and MAC addresses. The NPE performs QinQ termination and enters the IP forwarding procedure or relevant VPN.

The NPE can perform HQoS scheduling based on the double tags and create a DHCP binding table to prevent network attacks. The NPE can also implement DHCP+ authentication based on the double tags. You can also enable QinQ VRRP on the NPE to ensure reliable access.

8.1.2 Application of VLAN Mapping Based on 802.1p Priority-Based Traffic Distribution

Different networks use different access modes, and have different traffic distribution methods. When multiple services of a user use the same VLAN ID, different services have different 802.1p priorities, and are distinguished and mapped to stack VLANs.

Figure 8-2 VLAN mapping based on VLAN IDs and priorities

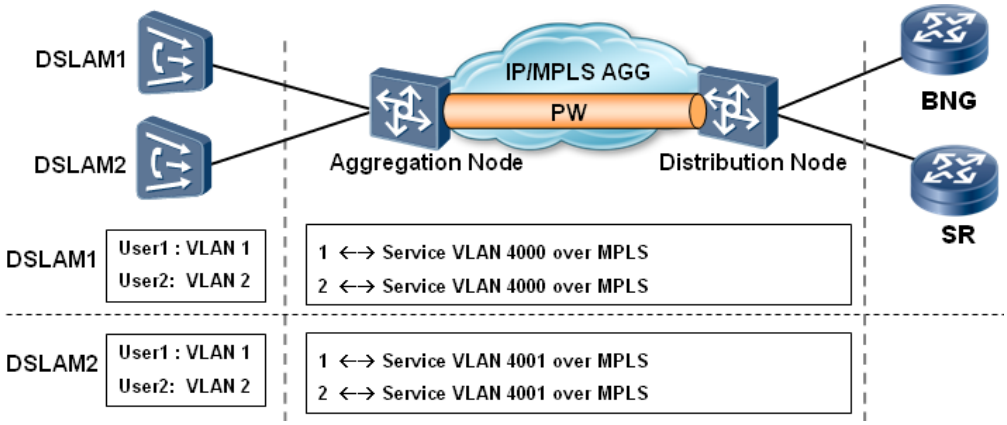


- The aggregation node (AGG) isolates service traffic from user's interfaces to correct stack VLANs. That is, the DSLAM tags customer VLAN tags and identifies services with 802.1p priorities. The AGG converts a customer VLAN tag into a stack VLAN tag based on the 802.1p priority. In addition, different users use the same stack VLAN, reducing workload of the SR and BNG that terminate double-tagged frames.
- To distinguish DSLAMs, the AGG uses different VLANs for frames from different DSLAMs after conversion.
- The AGG must forward outgoing traffic from each stack VLAN to correct user interfaces based on users' IP addresses in the downlink direction.
- The multicast service uses the MVLAN on the entire network. The AGG identifies the IGMP control frame and puts the frame into the multicast VLAN in the uplink direction.

8.1.3 Application of VLL/VPLS after VLAN Mapping

In addition to VLAN or QinQ, EoMPLS can be used to carry services through MPLS tunnels.

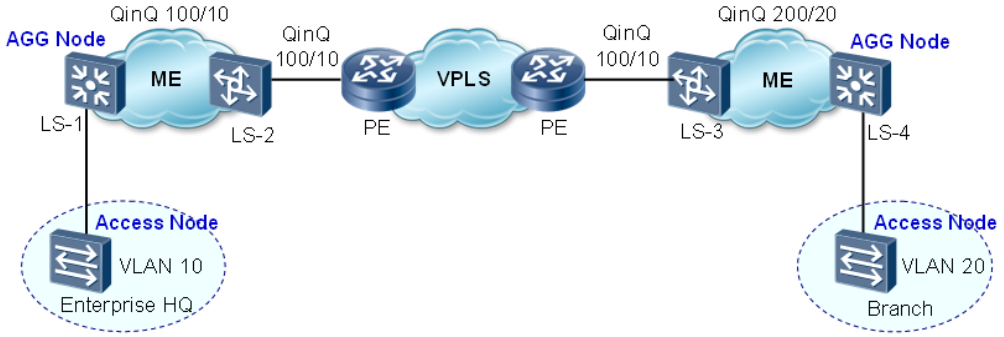
Figure 8-3 Application of VLL/VPLS after VLAN mapping



- The AGG maps user traffic to the unified stack VLAN from the customer VLAN in the uplink direction. Then user traffic passes the virtual leased line (VLL) tunnel. That is, the DSLAM adds the customer VLAN tag to packets. In addition, different users use the same stack VLAN ID, reducing workload of the SR and BNG that terminate frames carrying VLAN tags.
- To distinguish DSLAMs, the AGG uses different VLANs for frames from different DSLAMs after conversion.
- The AGG must forward traffic from each stack VLAN to correct user interfaces based on users' IP address in the downlink direction.

8.2 Enterprise Users' Access through Leased Lines

Figure 8-4 Application of VLAN mapping and selective QinQ in enterprise leased lines



An enterprise deploys two sites in the headquarters and a branch. The two sites can access each other.

The VPLS technology is applied to the backbone network and the QinQ technology is applied to the ME network. As shown in Figure 8-4, the headquarters is in VLAN 10. When user data passes the MAN, LS-1 tags the data with outer VLAN 100 that is assigned by the MAN of the headquarters. Data is transmitted with double tags on the MAN.

The user data travels across the backbone network through VPLS to the MAN of the branch. Because two MANs belong to different VLANs, LS-2 uses 2:2 VLAN mapping to change the two tags, mapping outer VLAN 100 to VLAN 200 and VLAN 10 to VLAN 20. The user data is transmitted on the MAN, carrying Tags 200 and 20. LS-4 strips off the outer tag and forwards the user data to the network of the branch.