VLAN Introduction and Phone Configuration

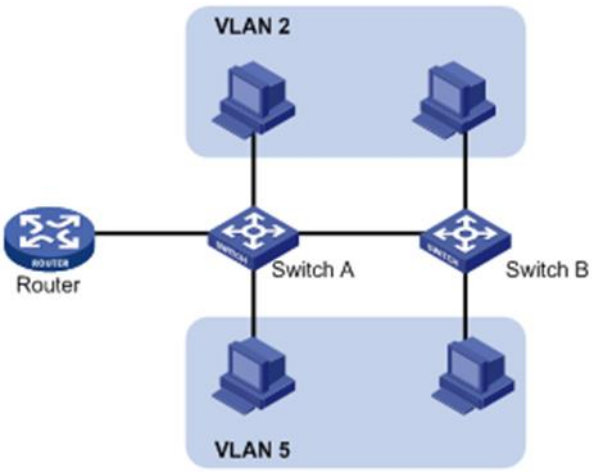
Version: <1.1>
Release date: <2018-5-13>

Contents

1 VLAN

1.1 VLAN Introduction

Although connecting LANs through switches can fix the collision problem, the broadcast packets cannot be isolated. Virtual Local Area Network (VLAN) is introduced to solve this problem. VLAN technology can divide a LAN into multiple logical LANs, which are VLANs. Each VLAN is a broadcast domain. The hosts within a VLAN can communicate with each other like in a LAN; however, the hosts of different VLANs cannot communicate directly. Therefore, broadcast packets are restricted within a VLAN, as shown in Figure 1-1.



VLAN assignment is not limited by physical locations. That is, the hosts at different physical locations can be added to the same VLAN. The hosts in a VLAN can be connected to the same switch or different switches, or even the switches under different routers.

VLAN technology has the following advantages:

1. Restricting broadcast domains: A broadcast domain is restricted within a VLAN. When the volume of routed traffic is reduced, the delay generated by routers is also shortened. This saves bandwidth and improves network processing capability.

2. Enhancing the security of LAN: The layer 2 packets of each VLAN are isolated from those of other VLANs. That is, the hosts in a VLAN cannot directly communicate with the hosts in other VLANs. To implement the communication between VLANs, a router, layer 3 switch or another layer 3 device is required.

3. Building virtual workgroups flexibly: VLAN technology can assign hosts to different workgroups. The hosts at different physical locations can be added to the same workgroup, without the need of installing new network cables or reconfiguring the hub or router, implementing flexible network building and maintenance.

1.2 VLAN Working Mechanism

To enable network devices to distinguish packets of different VLANs, the packets must carry the specific tags that identify the VLANs. Traditional switches work at the data link layer of the OSI model, so they can identify only the data link layer encapsulation on packets. Therefore, the VLAN tags also need to be added to the data link layer.

As a VLAN standard on the Ethernet, IEEE 802.1Q tags the Ethernet data frames carrying VLAN member information. The VLAN-awareness devices can identify the VLAN member information and VLAN formats. When a data frame from a phone enters the VLAN-awareness stage, a tag is added to the frame to indicate that this phone is a VLAN member. Each packet must be unique in a VLAN. On a network without VLAN configured, in the VLAN-awareness stage, a packet is considered to be transmitted over the local host (or default) VLAN.

802.1Q inserts a 4-byte tag between the source MAC address and Ethernet type fields, two of which indicate the Tag Protocol Identifier (TPID) and the other two indicate the Tag Control Information (TCI). The TCI field includes Priority Code Point (PCP), Canonical Format Indicator (CFI), and VLAN ID (VID).

In a traditional Ethernet data frame, the upper-layer protocol type field is encapsulated behind the destination and source MAC addresses, as shown in Figure 1-2.

Figure 1-2 Traditional Ethernet frame encapsulation format

DA indicates the destination MAC address, SA indicates the source MAC address, and Type indicates the protocol type of the frame.

According to IEEE 802.1Q, a 4-byte VLAN tag is inserted behind the destination and source MAC addresses to identify the VLAN information.

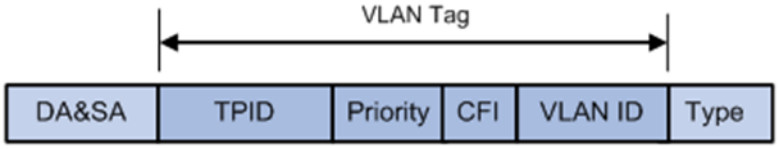


Figure 1-3 Fields in a VLAN tag

As shown in Figure 1-3, a VLAN tag includes four fields: TPID, Priority, CFI, and VLAN ID.

1. The 16-bit TPID field indicates whether the data frame carries a VLAN tag, and has a default value of 0x8100.

2. The 3-bit Priority field indicates the 802.1p priority.

3. The 1-bit CFI field indicates whether the MAC address is encapsulated in the standard format in different media. The value 0 indicates that the MAC address is encapsulated in standard format, and the value 1 indicates that the MAC address is not in standard format. The default value is 0.

4. The 12-bit VLAN ID field indicates the ID of the VLAN to which the packet belongs. The

value ranges from 0 to 4095. The values 0 and 4095 are reserved, so the VLAN ID ranges from 1 to 4094.

Network devices identify the VLANs to which packets belong according to the VLAN IDs, and process the packets depending on whether VLAN tags are carried and the values of VLAN tags.

1.3 VLAN Application

1.3.1 LLDP

Link Layer Discovery Protocol (LLDP) enables a phone to receive or send the device-related information from or to a directly connected device.

LLDP organizes the local information, such as management address, device capabilities, device identifiers, and interface identifiers, into different Type/Length/Value (TLVs). Each type of information forms a TLV, and multiple TLVs form a Link Layer Discovery Protocol Data Unit (LLDPDU). The information transmitted by LLDP is called LLDPDUs. An LLDPDU consists of a group of TLVs, and each TLV contains the specified type of transport information related to the device or interface.

The format of each TLV is as follows:

Type	Length	Value
7 bits	9 bits	0-511 bytes

Figure 1-4 TLV format

LLDP-MED was published by TIA. It is an extension of LLDP running between the endpoint devices and network devices. If voice devices are deployed on an Ethernet, the related TLVs need to be configured to obtain information about the voice devices. LLDP-MED provides dedicated support for VoIP applications and provides the following functions:

1) Performance discovery: Use LLDP-MED to determine the functions enabled and disabled on the connected device. It can identify the type of connected device, for example, phone, switch, or relay.
2) Voice VLAN configuration: Provide a mechanism to notify a VLAN-enabled device of the switch information. This device supports the plug-and-play network.

1. LLDP functions on phones

When the application type is voice, the phone decides whether to update the VLAN configuration according to the LLDPDU. If the version of VLAN configured on the phone differs from the VLAN version sent by the switch, the phone updates the VLAN configuration and restarts. In this way, the phone can learn the switch's VLAN ID, and communicate with the switch in this VLAN.

2. LLDP configuration

An X6 series phone is used as an example. The following is the LLDP configuration interface.

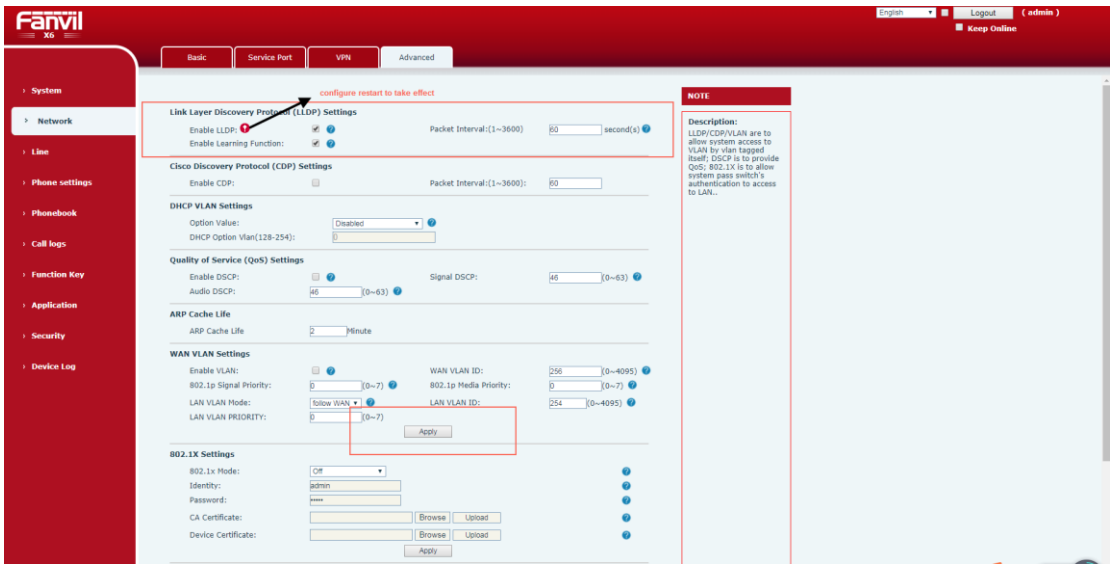


Figure 1-5 LLDP configuration

Configure LLDP on webpage:

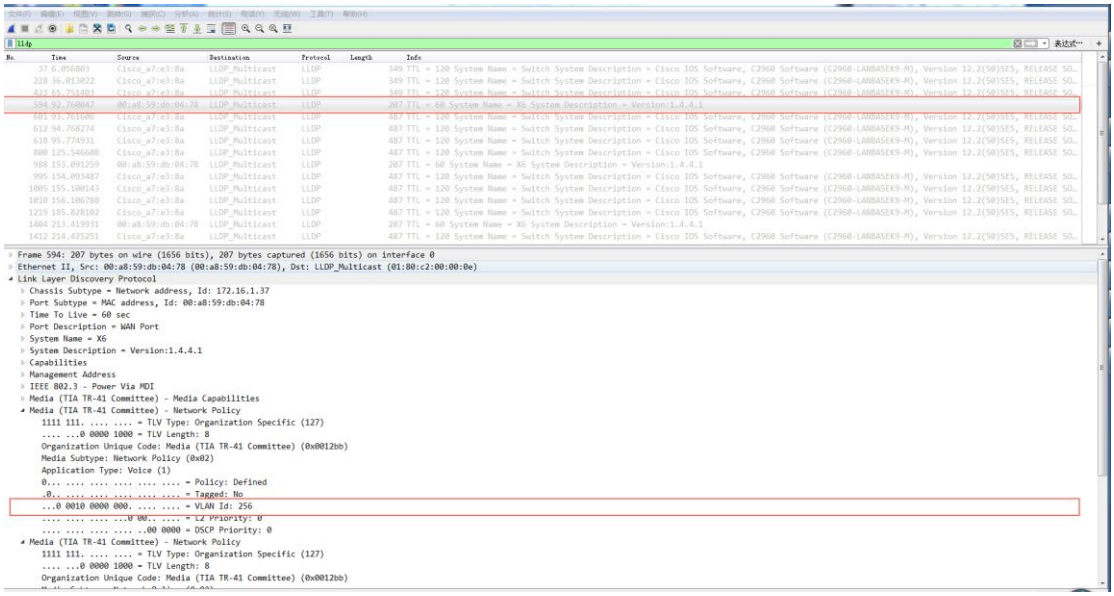
1) Log in to the webpage as an administrator. The default user name and password are admin.
2) Choose **Network** > **Advanced**.
3) In the Lin**k Layer Discovery Protocol (LLDP) Settings** area, choose whether to enable LLDP by clicking the options.
4) Enter the expected time value in **Packet Interval**. The value ranges from 1 to 3600, in seconds.
5) Click **Apply** to confirm the settings.
6) The configuration takes effect after the phone restarts.

1. Configuration verification

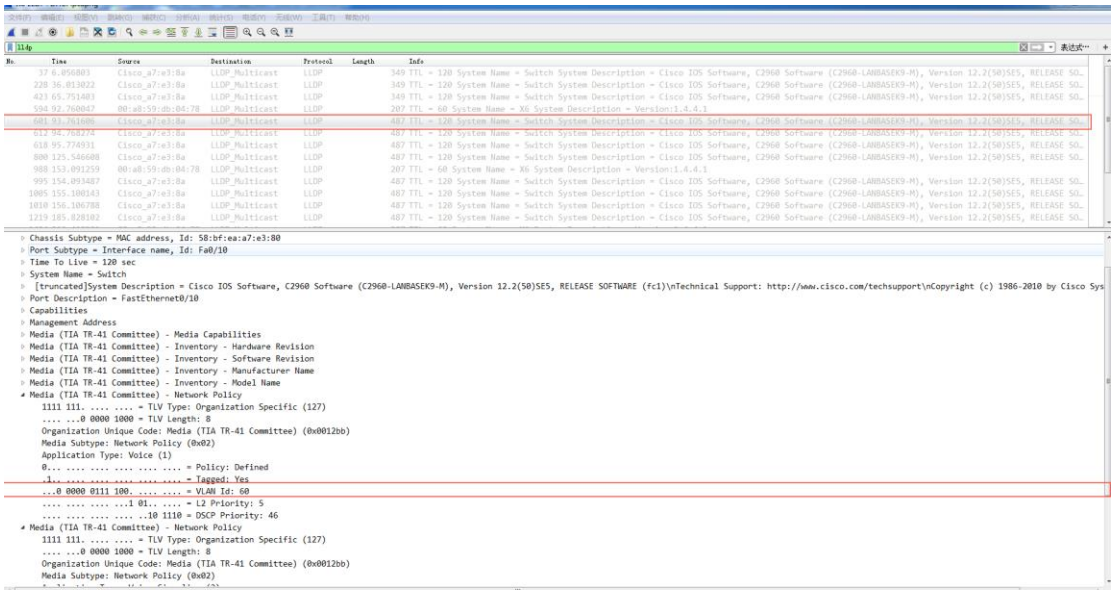
After LLDP is enabled, the phone will:

1) Send its own information (for example, hardware modification, firmware revision, and SN) to the multicast addresses on the network periodically.
2) Receive LLDPDUs through the network (WAN) or WLAN interfaces.
3) Support MAC/PHY configurations, for example, rate and duplex mode.
4) Take precedence of the VLAN information obtained from network policy over the manual configuration.

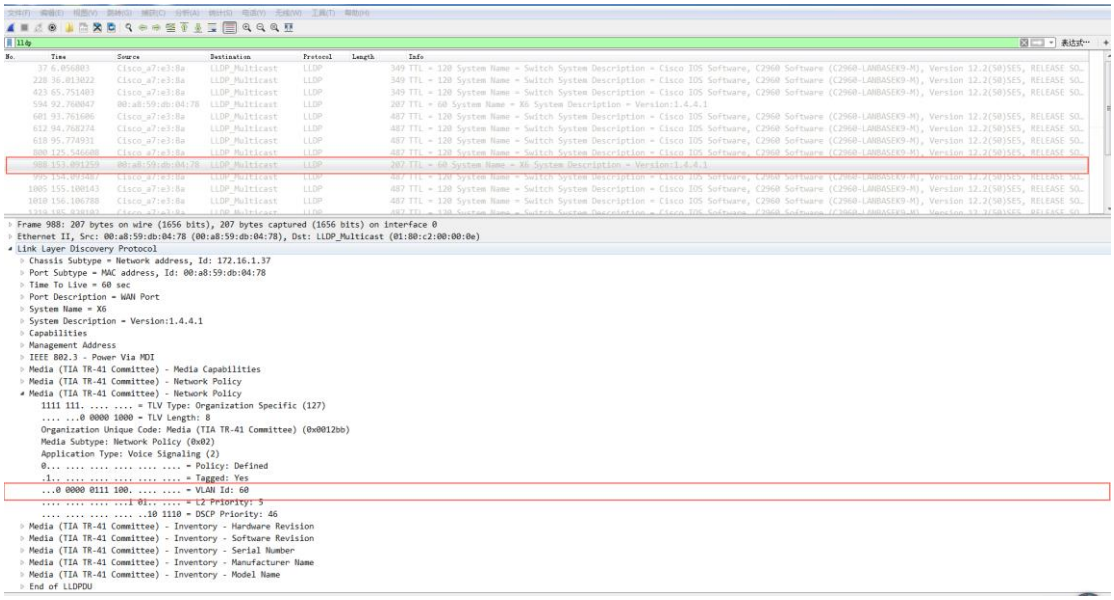
The following figure shows the LLDPDU sent by a phone. An LLDPDU includes multiple TLVs (before VLAN ID is obtained):



The following figure shows the LLDPDU received by a phone. An LLDPDU includes multiple TLVs (sent by switch):



The following figure shows the LLDPDU sent by a phone. An LLDPDU includes multiple TLVs (after VLAN ID is obtained):



1.3.2 CDP

Cisco Discovery Protocol (CDP) enables a phone to receive or send the device-related information from or to a directly connected device, and store other devices' information.

1. CDP application on phones

After CDP is enabled on a phone, the phone periodically sends its own information to the directly connected CDP-enabled switch. The phone can also receive CDP packets from the directly connected switch. If the version of VLAN configured on the phone differs from the VLAN version sent by the switch, the phone updates the VLAN configuration and restarts. In this way, the phone can learn the switch's VLAN ID, and communicate with the switch in this VLAN.

2. CDP configuration

An X6 series phone is used as an example. The following is the CDP configuration interface.

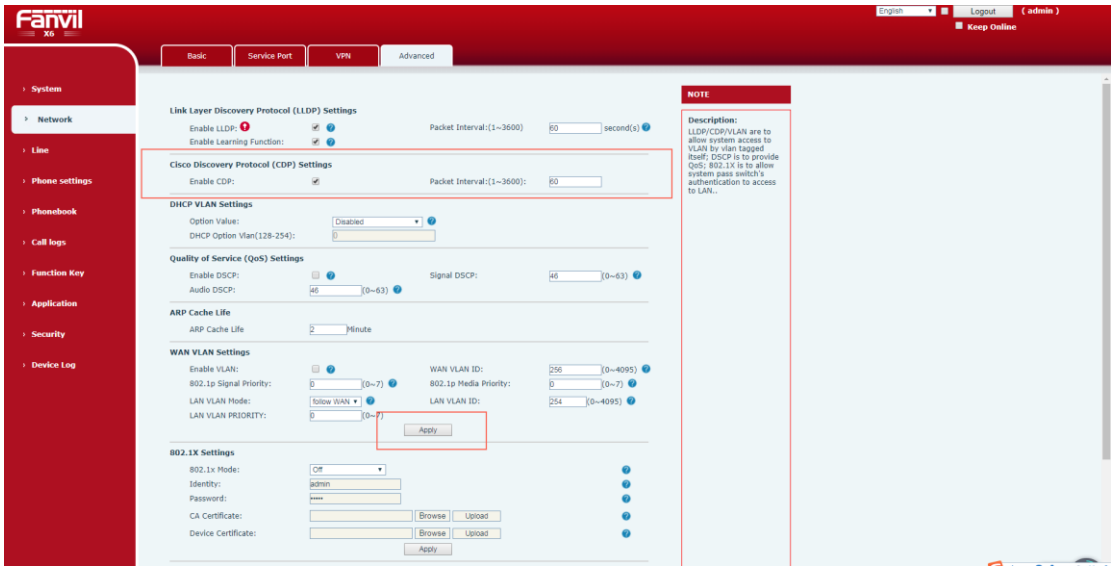


Figure 1-6 CDP configuration

1) Log in to the webpage as an administrator. The default user name and password are admin.

2) Choose **Network** > **Advanced**.

3) In the **Cisco Discovery Protocol (CDP) Settings** area, choose whether to enable CDP by clicking the options.

4) Enter the expected time value in **Packet Interval**. The value ranges from 1 to 3600, in seconds.

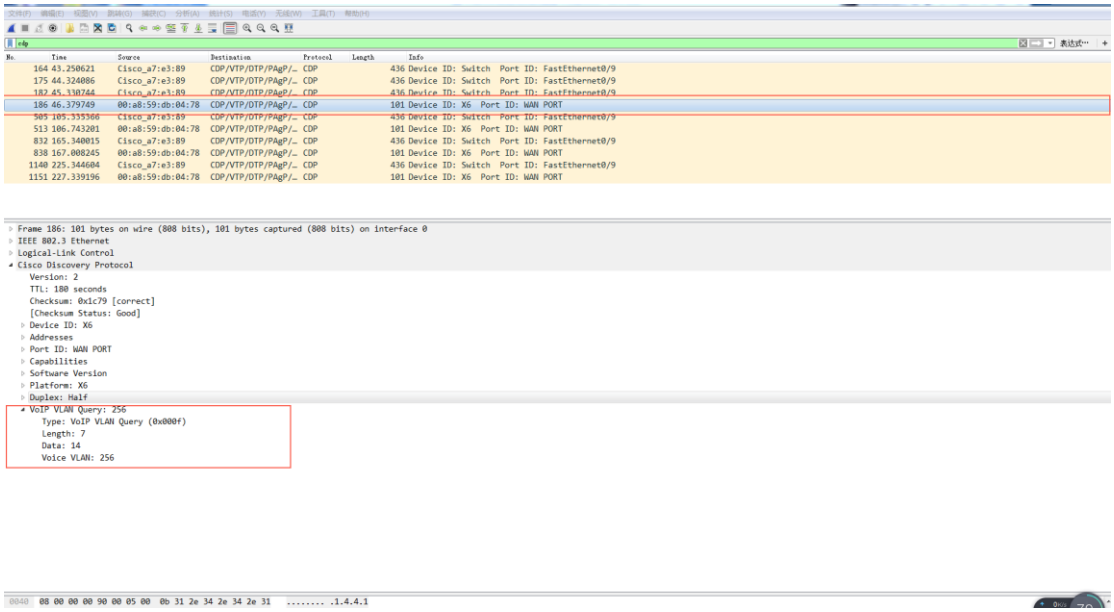
5) Click **Apply** to confirm the settings.

3. Configuration verification

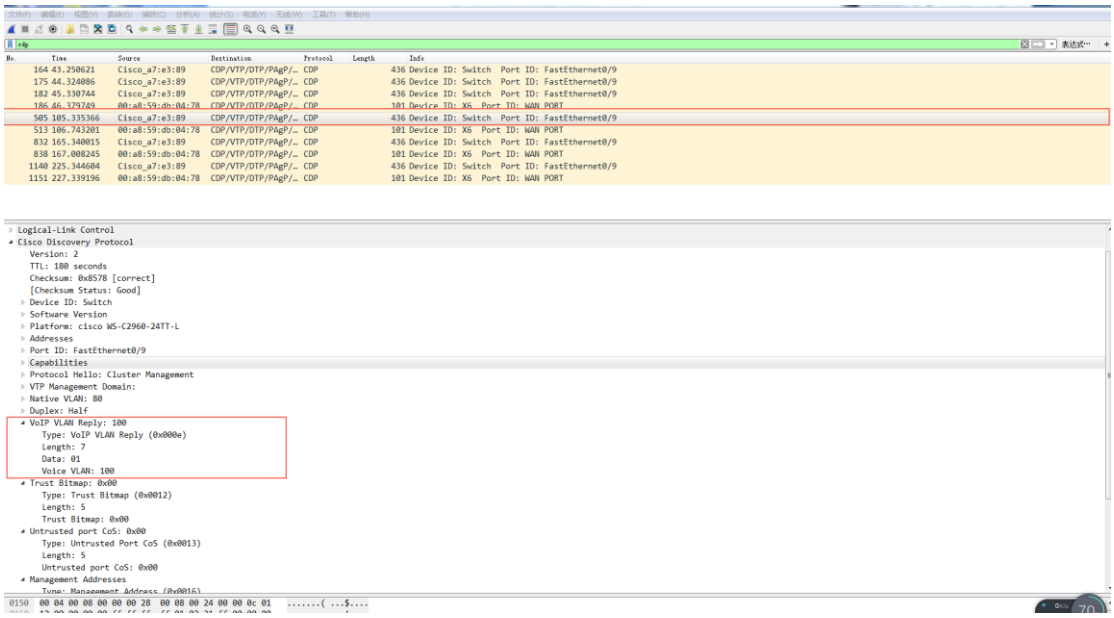
After CDP is enabled, the phone will:

1) Send its own information (for example, software modification, device ID, and power consumption) to the multicast addresses on the network periodically.
2) Receive CDP packets through the network (WAN) or WLAN interfaces.
3) Obtain the VLAN ID of the connected interface.

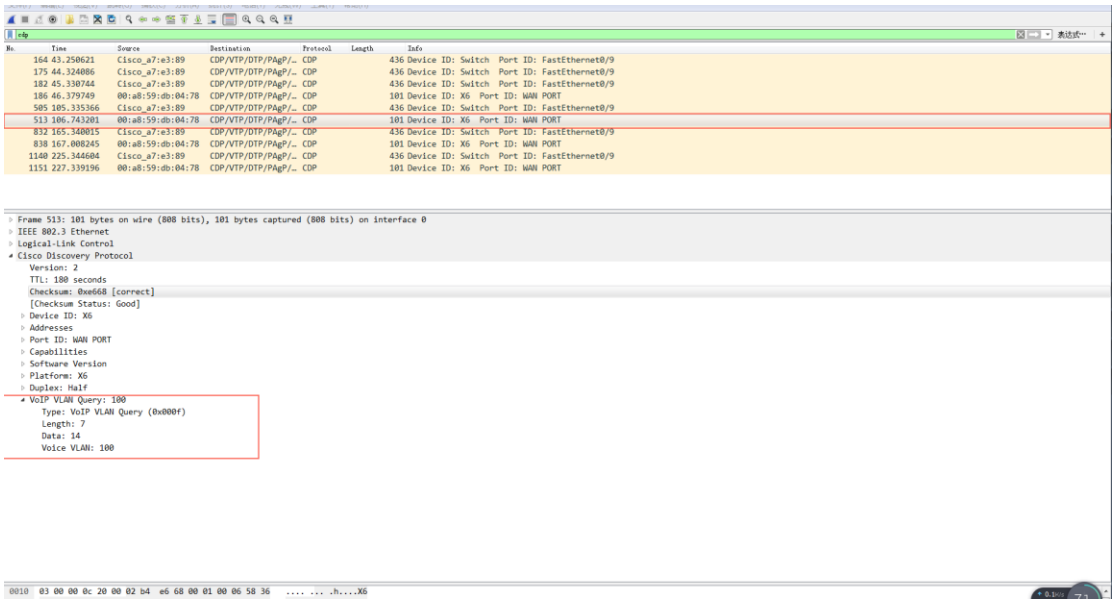
The following figure shows the CDP packet sent by a phone (before the switch VLAN ID and VLAN Query are learned):



The following figure shows the CDP packet received by a phone from a switch (VLAN Reply is used):



The following figure shows the CDP packet sent by a phone (VLAN Query is displayed after the switch VLAN ID is learned):



1.3.3 DHCP VLAN

1. DHCP VLAN Introduction

The phones can discover VLANs by using DHCP. When the VLAN discovery mode is set to DHCP, the phone will detect a DHCP option of a valid VLAN ID. By default, the pre-defined option 132 is used to carry the VLAN ID. You can also define the DHCP option used to carry VLAN ID.

2. DHCP VLAN configuration

An X6 series phone is used as an example. The following is the DHCP VLAN configuration interface.

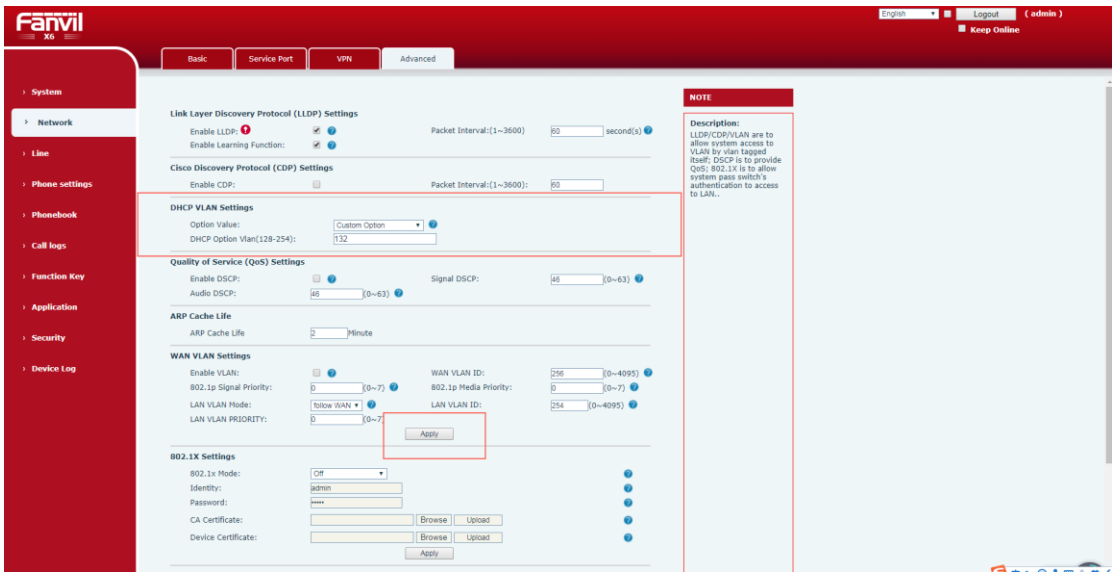


Figure 1-7 DHCP VLAN configuration

1) Log in to the webpage as an administrator. The default user name and password are admin.

2) Choose **Network > Advanced**.

3) In the **DHCP VLAN** area, select a desired value from the **Option Value** drop-down list.

4) Enter a value in the **DHCP Option Vlan** box. You can enter a maximum of 5 values and separate them with commas.

5) Click **Apply** to confirm the settings.

3. Configuration verification

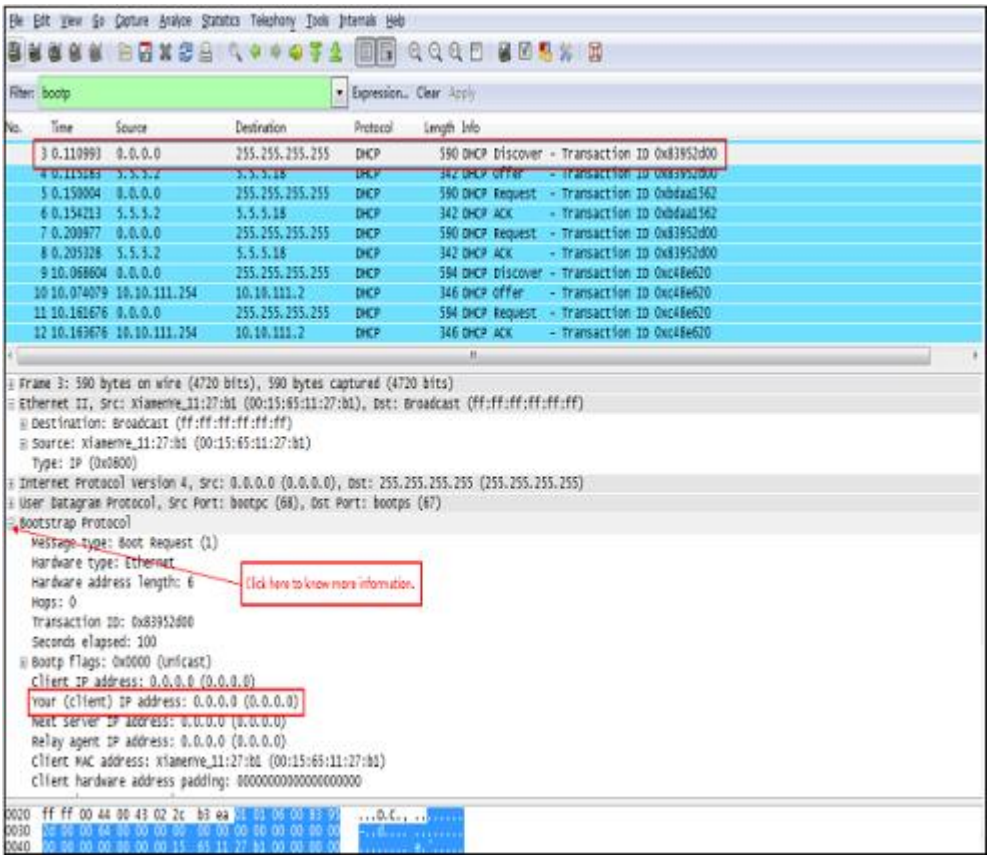
When a phone is configured to use DHCP to discover VLAN and the DHCP option is set to 132, the phone will:

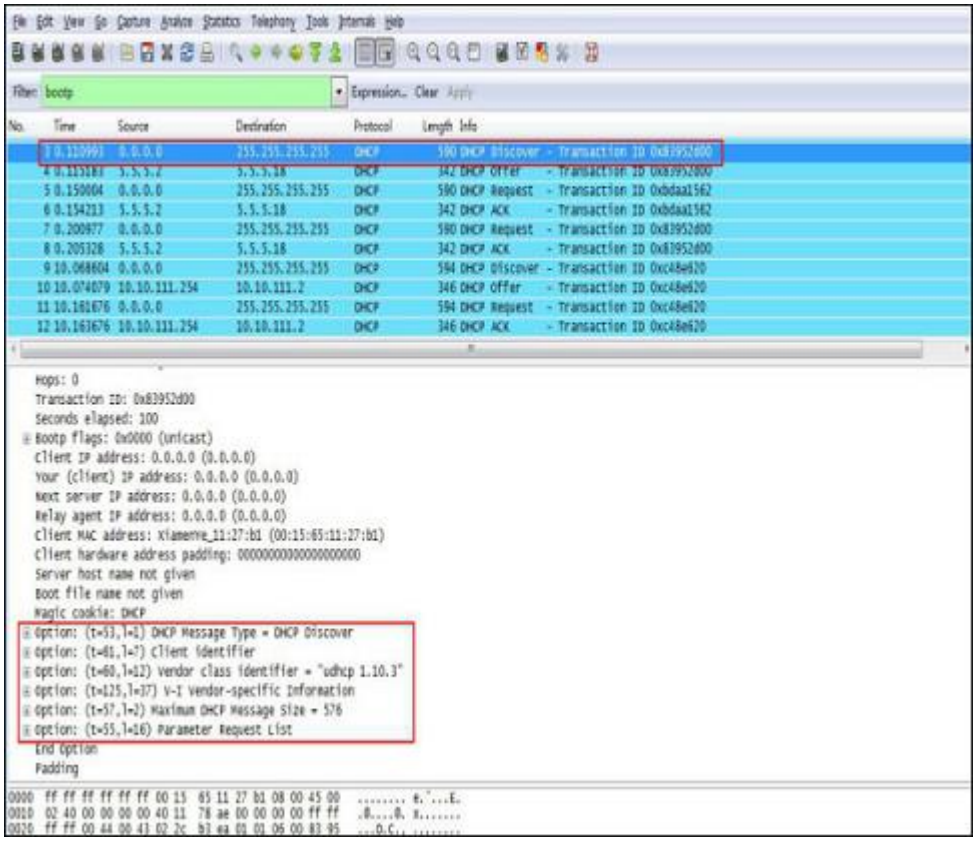
1) Broadcast a DHCP discover message to check whether there is an available DHCP server.

2) If the DHCP server sends a DHCP message carrying option 132, the phone will receive the message, send a DHCP request, and save the VLAN ID carried in DHCP option 132 sent by the DHCP server.

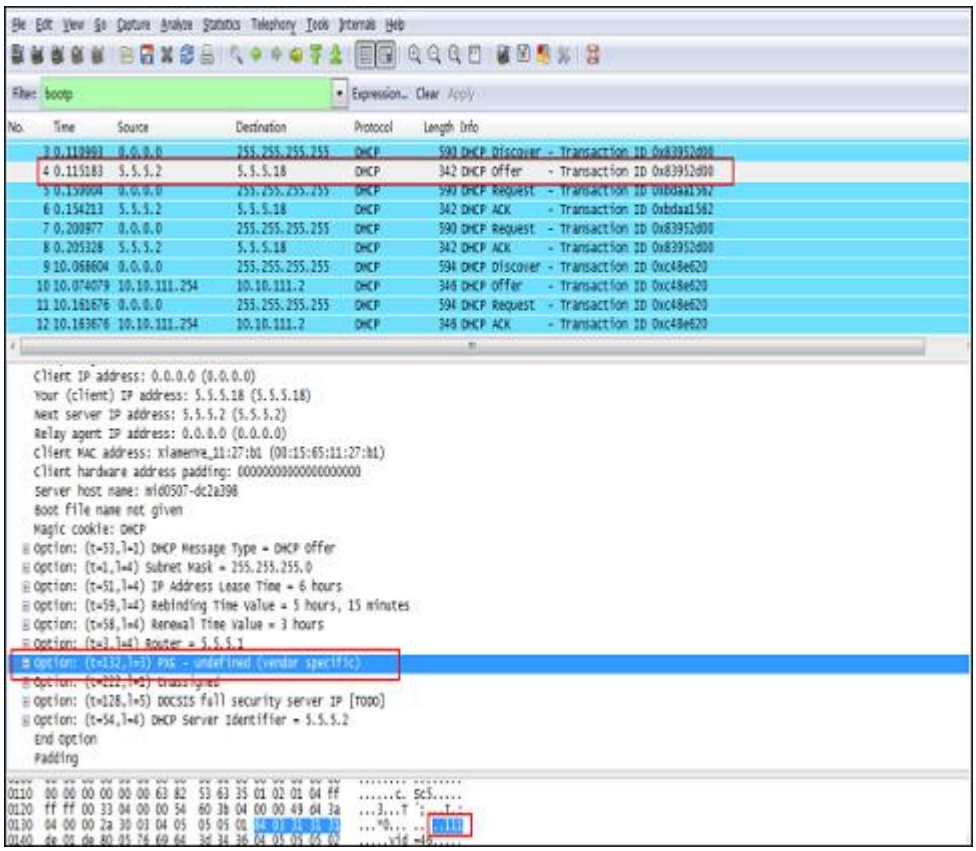
3) After obtaining the VLAN ID from the DHCP server, the phone releases the borrowed IP address, starts a new DHCP discovery period, and uses the known voice VLAN ID. Then the phone uses the VLAN ID carried in DHCP option 132 to send all packets.

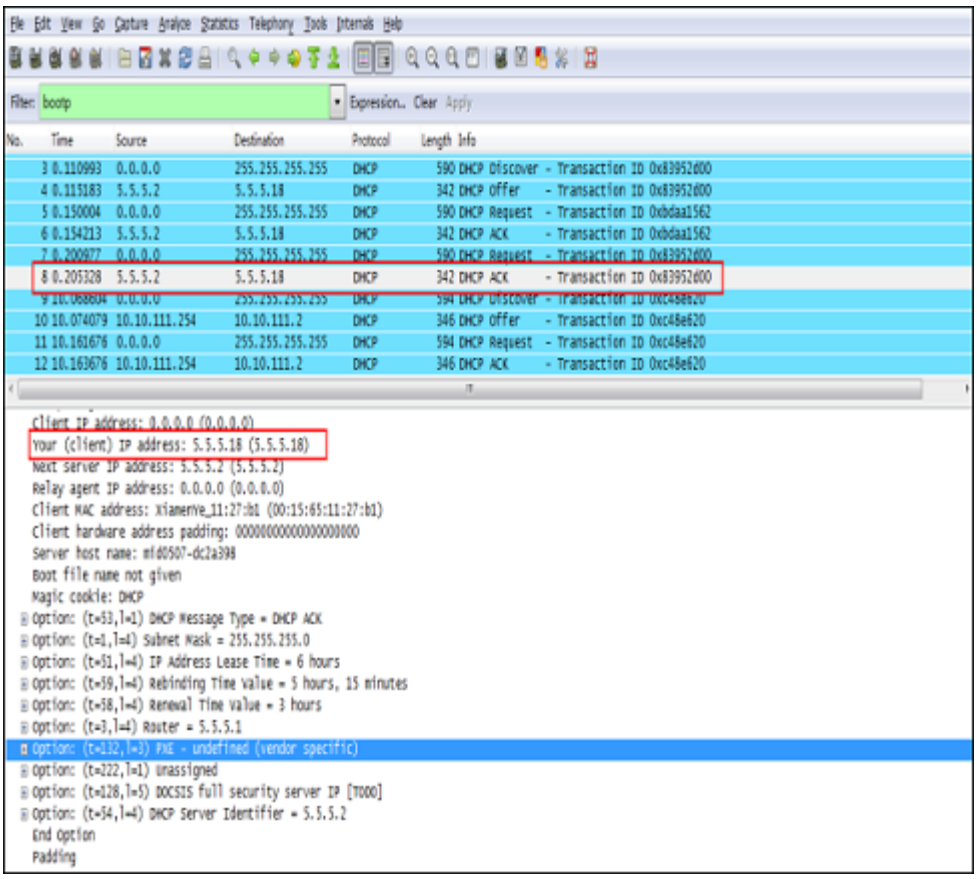
The following figure shows the DHCP discover message sent by a phone (before VLAN ID is obtained):





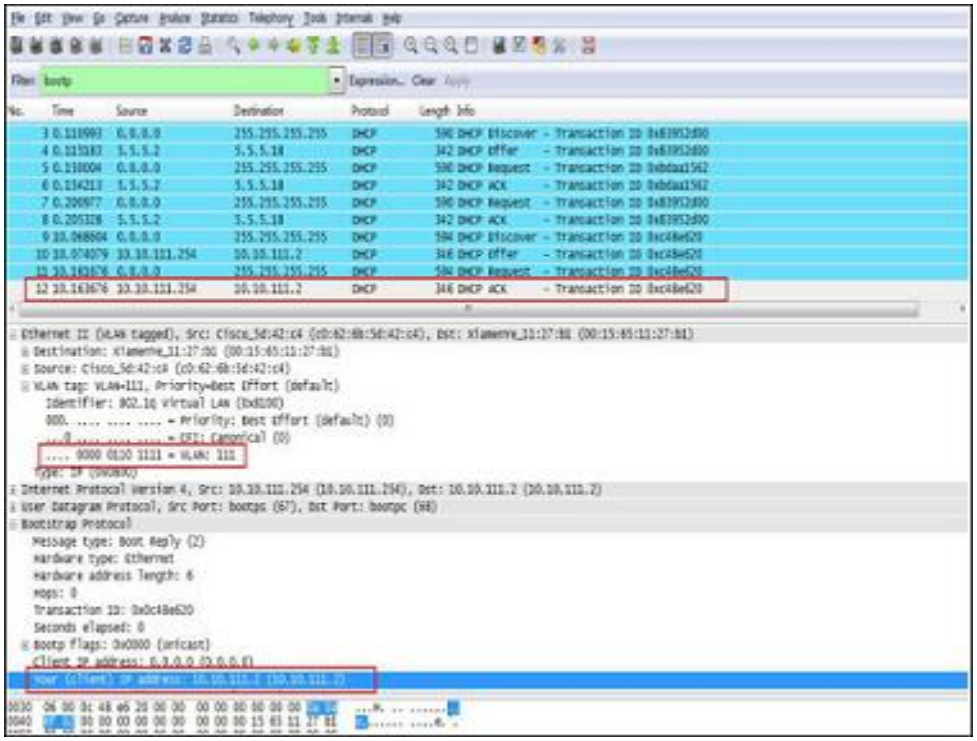
The following figure shows the DHCP offer message received by a phone (DHCP server sends a DHCP offer message carrying option 132):





The following figure shows the DHCP message received by a phone (DHCP server sends ACK message to the phone):

After obtaining the VLAN ID from the DHCP server, the phone releases the borrowed IP address (5.5.5.18), and initiates a new DHCP discover message using VLAN tag 111. The following figure shows the DHCP message received by a phone:



Then, the phone obtains an IP address (10.10.111.2) from a DHCP server in VLAN 111.

1.3.4 VLAN Manual Configuration

1. VLAN Introduction

By default, VLAN is disabled on phones. You can configure VLAN by using web user interface, phone user interface, or configuration file. Before configuring VLAN through the phone, you need to obtain the VLAN ID from the network administrator. The prerequisite of configuring VLAN feature is to confirm the type of connected interface (access, trunk, or hybrid interface). This ensures that tagged and untagged packets can be transmitted through the phone. The VLAN feature may affect the network functions of the phone. Before the configuration, contact the administrator to obtain more information.

2. VLAN configuration

You can enable or disable VLAN, and assign VLAN Ids and priorities to the Internet (WAN) and PC (LAN) ports.

Configure VLAN for the Internet (WAN) port on the web user interface:

An X6 series phone is used as an example. The following is the VLAN configuration interface.

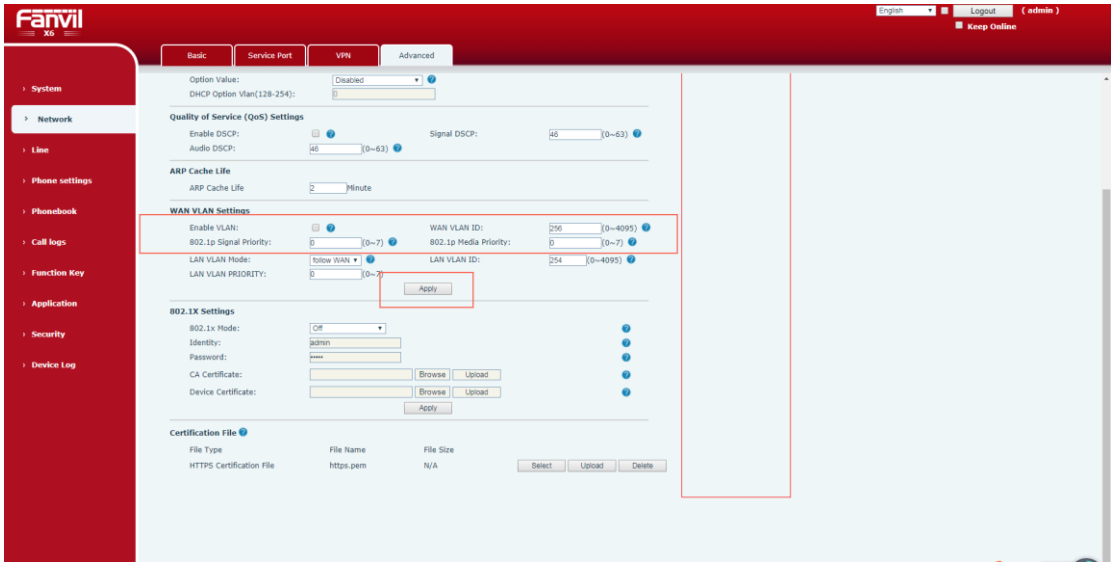


Figure 1-8 VLAN configuration

1) Log in to the webpage as an administrator. The default user name and password are admin.

2) Choose **Network** > **Advanced**.

3) In the **WAN VLAN Settings** area, choose whether to enable VLAN.

4) Enter a WAN VLAN ID, ranging from 1 to 4094.

5) Enter the priority value, ranging from 0 to 7. The highest priority is 7.

6) Click **Apply** to confirm the settings.

Configure VLAN for the PC port on the web user interface:

An X6 series phone is used as an example. The following is the VLAN configuration interface.

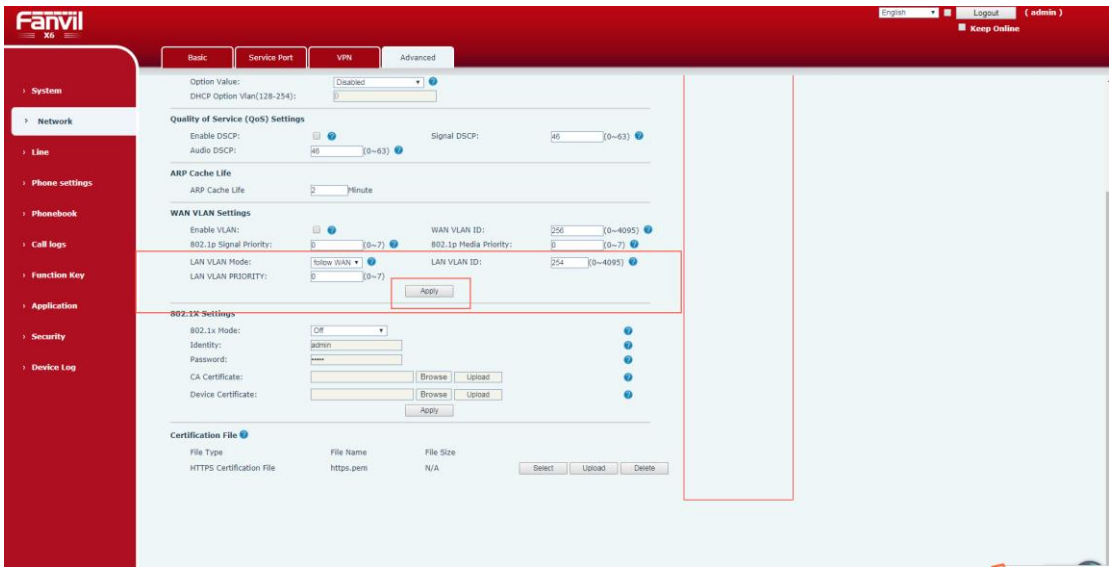


Figure 1-9 LAN VLAN configuration

1) Log in to the webpage as an administrator. The default user name and password are admin.

2) Choose **Network** > **Advanced**.

3) Select a value from the **LAN VLAN Mode** drop-down list.

4) Enter a LAN VLAN ID, ranging from 1 to 4094.

5) Enter the priority value, ranging from 0 to 7. The highest priority is 7.

Configure the VLAN (WAN) port on the phone user interface:

An X6 series phone is used as an example. The following is the VLAN configuration interface.

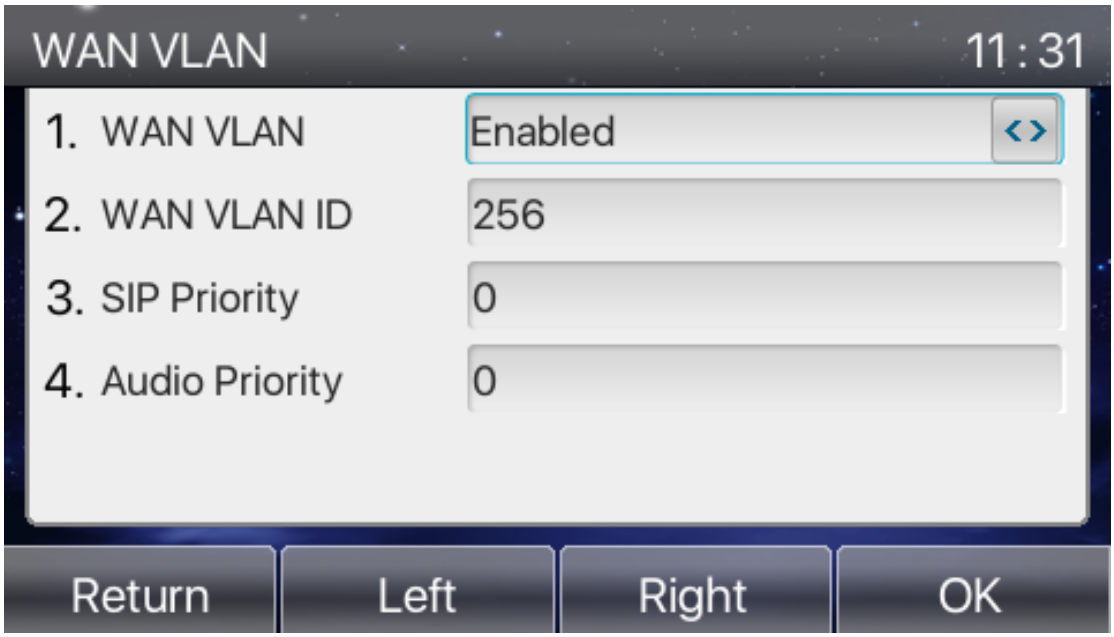


Figure 2-1 WAN VLAN configuration

1) Choose **Menu** > **Advanced**. Enter the password **123**. Choose **Network** > **QoS&Vlan** > **WAN VLAN**.

2) Press Left/Right on the phone or Left/Right softkey to choose whether to enable WAN WLAN.

3) Enter a WAN VLAN ID, ranging from 1 to 4094.

4) Enter the priority value, ranging from 0 to 7. The highest priority is 7.

5) Press **OK** to save the configuration.

Configure the VLAN (WAN) port on the phone user interface:

An x6 series phone is used as an example. The following is the VLAN configuration interface.

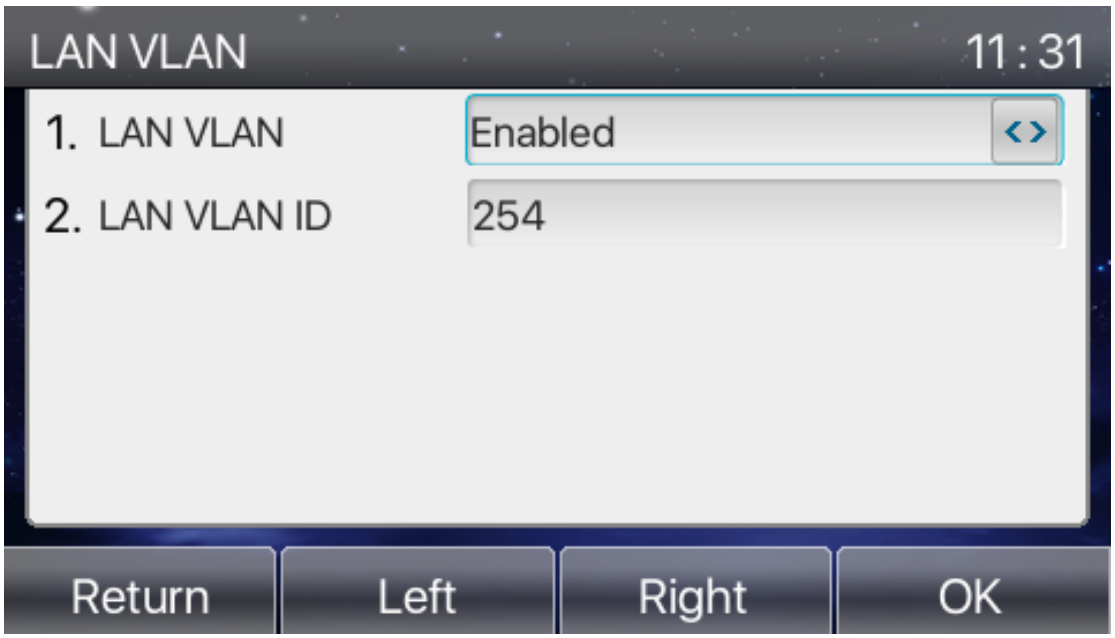


Figure 2-2 LAN VLAN configuration

1) Choose **Menu** > **Advanced**. Enter the password **123**. Choose **Network** > **QoS&Vlan** > **LAN VLAN**.

2) Press Left/Right on the phone or Left/Right softkey to set the LAN WLAN value.

3) Enter a LAN VLAN ID, ranging from 1 to 4094.

4) Enter the priority value, ranging from 0 to 7. The highest priority is 7.

5) Press **OK** to save the configuration.

3. Configuration verification

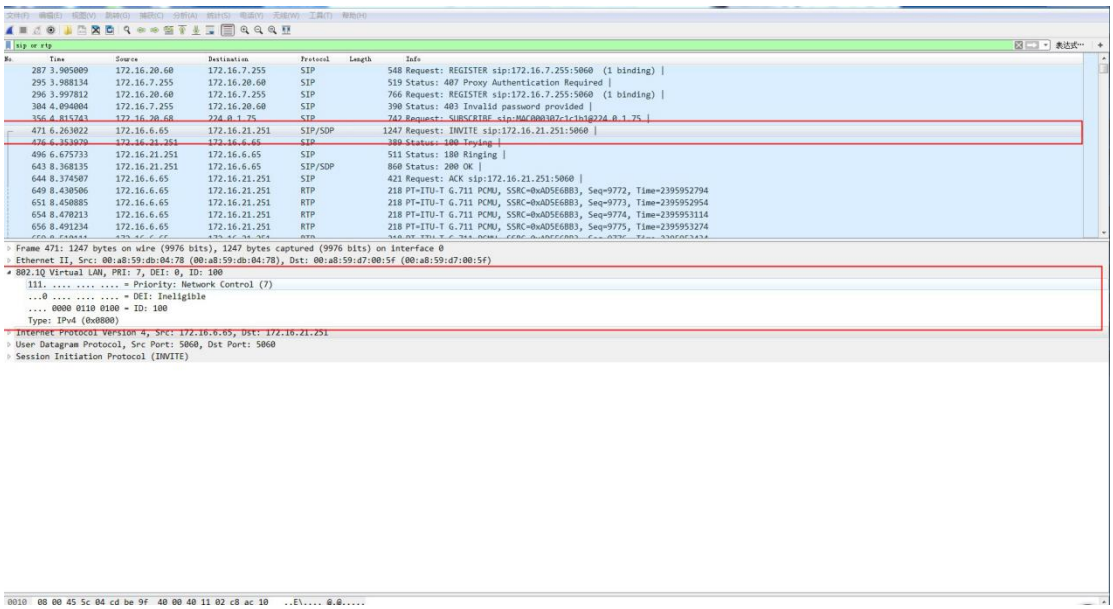
Check whether the audio and signal settings of 802.1p are correct. Perform the following operations on the phone:

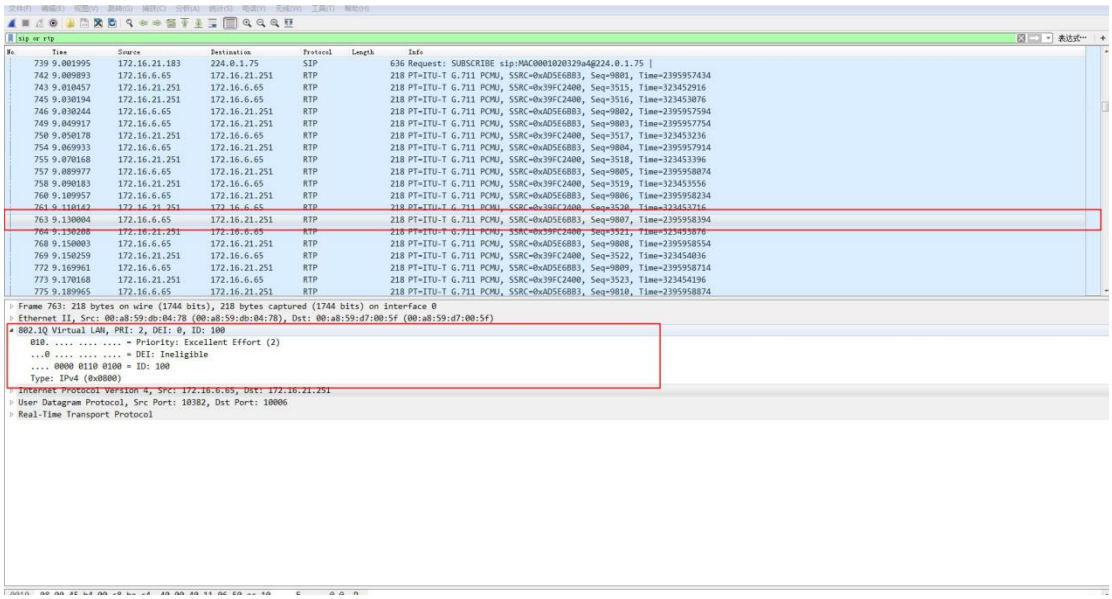
1) Test the static IP address set on the phone. Enable VLAN on the webpage or phone. Set the VLAN ID to 100, enable DSCP, and set the audio DSCP and signal DSCP to different values.

2) The value of 802.1p signal priority ranges from 0 to 7, for example, 7. The value of 802.1p media priority ranges from 0 to 7, for example, 2.

3) Capture the SIP or RTP packets by calling another phone with the test phone's IP address. In the data link layer of SIP (SIP/SDP) packets, you can find the VLAN tag, which includes the VLAN ID. In addition, the value of **Priority** is the value of 802.1p signal priority, and the value of signal DSCP is the value set on the test phone. In the data link layer of RTP packets, you can find the VLAN tag, which includes the test phone's VLAN ID. In addition, the value of **Priority** is the value of 802.1p media priority, and the value of audio DSCP is the value set on the test phone.

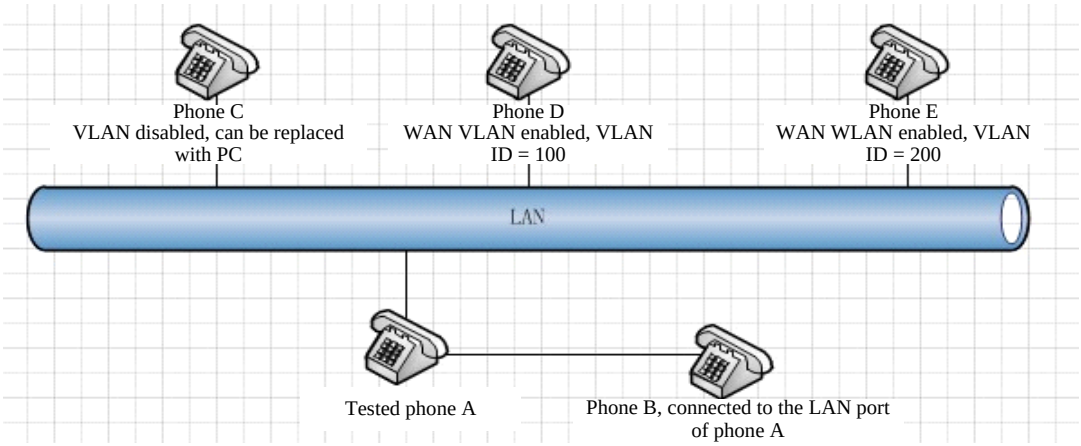
The following figures show the captured packets:





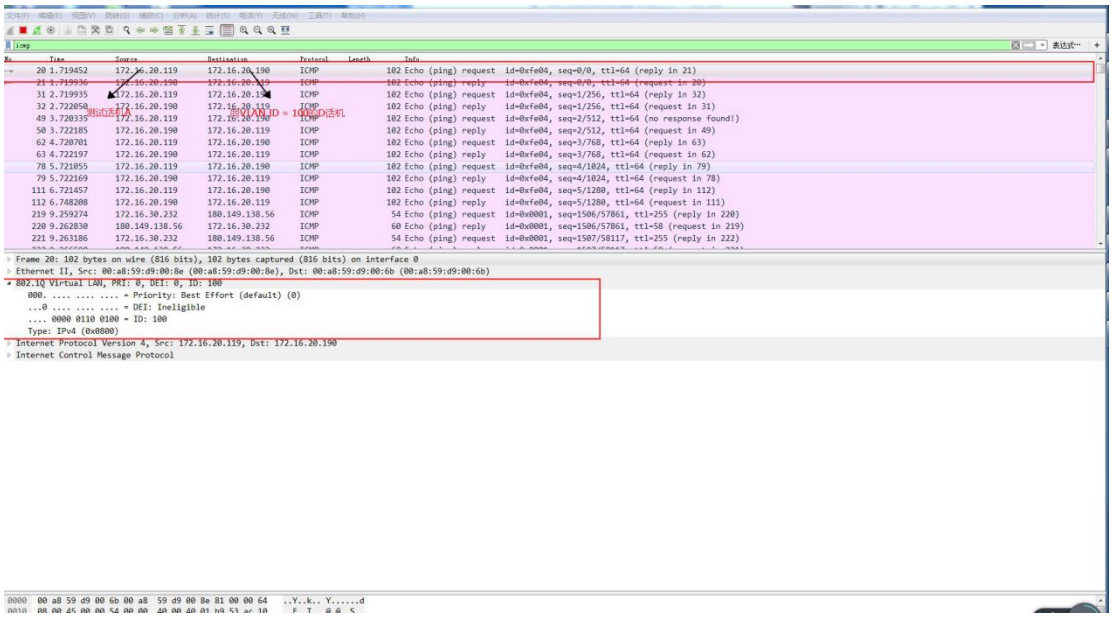
Enable WAN VLAN. The phones with the same VLAN tag configured can communicate with each other. Perform the following operations on the phone:

Test environment: Test phone A and auxiliary test phones C, D, and E are connected to the same hub or switch. Phone B is connected to the LAN port of phone A, as shown below:

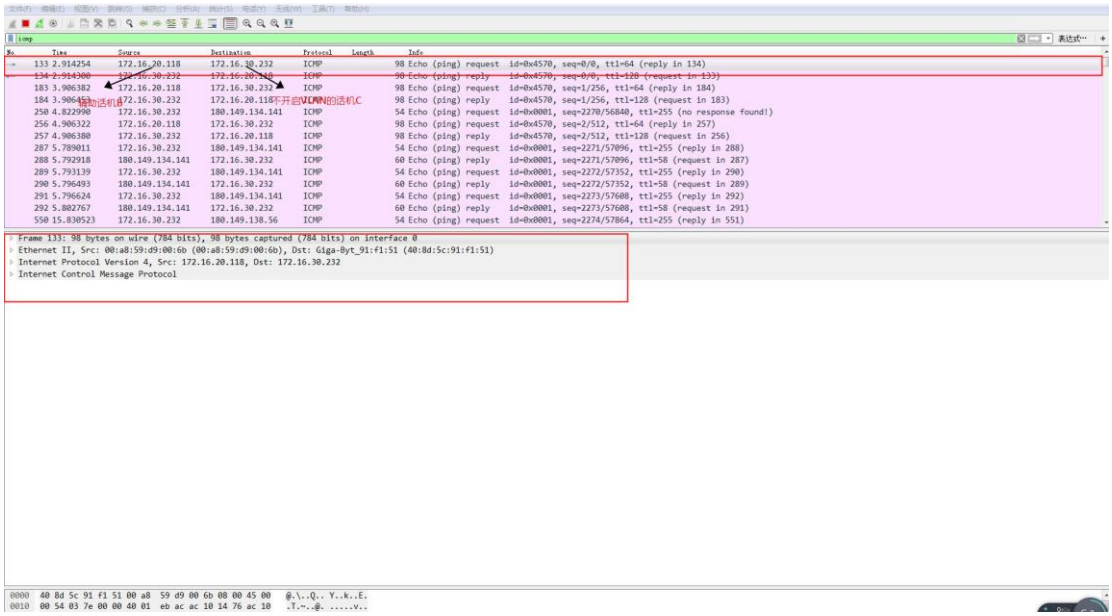


1) Log in to the webpage, set the WLAN ID to 100, disable LAN VLAN, and save the configuration (if VLAN has been enabled and the PC cannot visit the webpage, disable VLAN on the LCD first).

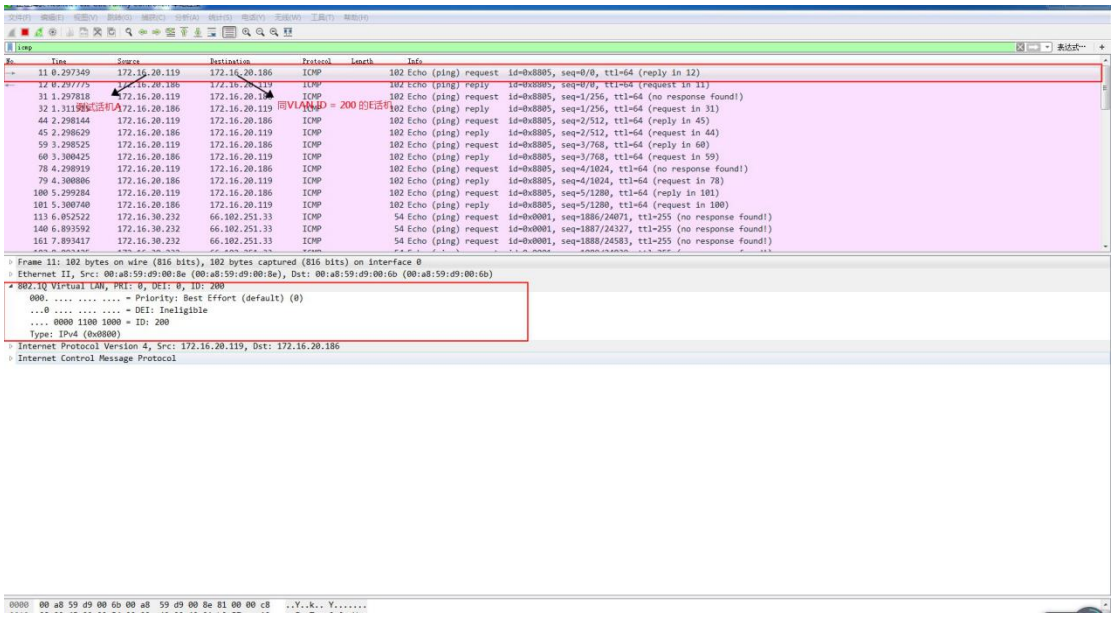
2) Ping phones B, C, D, and E from phone A. You can see that phone A can ping phone D successfully, but cannot ping phones B, C, and E. By capturing packets, you will find that the packets sent by phone A carry tag 100. The captured packets are as follows:



3) Ping phones A, C, D, and E from phone B. You can see that phone B can ping phone C successfully, but cannot ping phones A, D, and E. By capturing packets, you will find that the packets sent by phone B do not carry tag 100. The captured packets are as follows:



4) Change the VLAN ID of the WAN port to 200 and repeat steps 2 and 3. You can find that phone A can ping phone E successfully, but cannot ping phones B, C, and D. By capturing packets, you will find that the packets sent by phone A carry tag 200. Phone B can ping phone C successfully, but cannot ping phones A, D, and E. By capturing packets, you will find that the packets sent by phone B do not carry a VLAN tag.



2 VLAN Configuration on Cisco Catalyst 2960 Switch

2.1 Default Values of Ethernet VLAN

Default values and value ranges of Ethernet VLAN

Parameter	Default Value	Range
VLAN ID	1	1 to 4094. **Note** : Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	VLANxxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number.	No range
IEEE 802.10 SAID	100001 (100000 plus the VLAN ID)	1 to 4294967294
MTU size	1500	1500 to 18190
Translational bridge1	0	0 to 1005
Translational bridge2	0	0 to 1005
VLAN state	Active	Active, suspend

2.2 Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID. Enter a new VLAN ID to create

	Command	Purpose
		a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** : The available VLAN ID range for this command is 1 to 4094.
Step 3	**name** *vlan-name*	(Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the vlan-id with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size (or other VLAN characteristic).
Step 5	**remote-span**	(Optional) Configure the VLAN as the RSPAN VLAN for a remote SPAN session. **Note**: The switch must be running the LAN Base image to use RSPAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show vlan**{**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 8	**copy running-config startup config**	(Optional) Save the switch configuration.

2.3 Deleting a VLAN

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Note: When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no vlan** *vlan-id*	Remove the VLAN by entering the VLAN ID.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan brief**	Verify the VLAN removal.

Step 5	**copy running-config startup config**	(Optional) Save the switch configuration.

2.4 Assigning Static-Access Ports to a VLAN

Note: If you assign an interface to a VLAN that does not exist, a new VLAN is created.

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN:

	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config interface***interface-id*	Verify the VLAN membership mode of the interface.
Step 7	**copy running-config startup-config**	(Optional) Save the switch configuration.

2.5 Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as a trunk port:

	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured for trunking, and enter interface configuration mode.
Step 3	**switchport mode trunk**	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode).
Step 4	**switchport access vlan***vlan-id*	(Optional) Specify the default

	Command	Purpose
		VLAN, which is used if the interface stops trunking.
Step 5	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN for IEEE 802.1Q trunks.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces***interface-id* **switchport**	Display the switch port configuration.
Step 8	**show interfaces***interface-id* **trunk**	Display the trunk configuration of the interface.
Step 9	**copy running-config startup-config**	(Optional) Save the switch configuration.

To return an interface to its default configuration, use the **default interface** *interface-id* command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** command.

Configured allowed VLANs on the trunk port:

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 4	**switchport trunk allowed vlan** {**add** |**all**	**except** |**remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. The *vlan-list* parameter is either a single VLAN number or a range of VLANs described by two VLAN numbers

	Command	Purpose
		separated by a hyphen. The VLAN numbers range from 1 to 4096. All VLANs are allowed by default.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces***interface-id***switchport**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save the switch configuration.

2.6 Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define the interface that is configured as the IEEE 802.1Q trunk, and enter interface configuration mode.
Step 3	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save the switch configuration.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.