



# Yealink Technical White Paper Virtual Local Area Network (VLAN)

Version 9.42 Apr.2018

## About VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

## **IEEE 802.1Q**

IEEE 802.1Q is the networking standard that supports VLANs on an Ethernet network. The specification defines a standard method for tagging Ethernet packets with VLAN membership information. A VLAN-aware device is the one which understands VLAN memberships and VLAN formats. When a packet from the phone enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the phone. Each packet must be distinguishable as being within exactly one VLAN. A packet in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

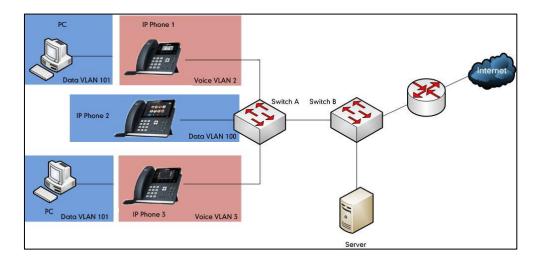
802.1Q adds a 4-byte tag between the source MAC address and the Ethernet type fields of the Ethernet frame. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP (Priority Code Point), CFI (Canonical Format Indicator), and VID (VLAN ID).

## Voice VLAN

As voice traffic is delay and jitter sensitive for the phone, it requires higher priority over data traffic to reduce delay and packet loss during transmission. To simplify configuration procedures and better manage voice transmission policies, the connected switch can be configured to provide voice VLAN function and transmit the voice traffic of the phone in a dedicated VLAN, called voice VLAN.

Voice VLAN is a special access port feature of the switch which allows phones to be automatically configured and easily associated with a logically separate VLAN. This feature provides various benefits, but one particular benefit is that when voice VLAN is enabled on a switch port, this port is also enabled to allow simultaneous access for a PC. This feature allows a PC to be daisy chained to a phone and the connection for both PC and phone to be trunked through the same physical Ethernet cable.

The purpose of VLAN configurations on the phone is to insert tag with VLAN information to the packets generated by the phone. When VLAN is properly configured for the ports (Internet port and PC port) on the phone, the phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tags described in IEEE Std 802.3.



## **Major Benefits of Using VLANs**

VLANs offer many benefits that are not found in typical LANs. Major benefits of segregating phones into VLAN(s) are listed as below:

- **Performance Enhancements:** VLAN is used to minimize the broadcast domain. Creating smaller domain for phone can reduce overhead and limit resource utilization. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.
- **Ease of Administration:** Much of the cost associated with network additions and relocations can be saved through the use of VLANs. phone can be shifted from one workgroup or department to another without installing new network cabling and reconfiguring hubs or routers.
- Security: VLANs can be used to create secure user groups and prevent others outside of the broadcast domain from receiving sensitive data of the phone. They can also be used to enhance firewall functions and restrict network access for one or more users. By segregating phones into VLANs, security filters can be implemented in the network to prevent the phones from receiving unnecessary traffic from other devices. This helps prevent disruption due to DoS attacks or attempts to compromise the devices. It also allows locking down access to configuration and signaling servers to only allow access from the phones.

## **Yealink Phones Compatible with VLAN Method**

There are four ways to get VLAN ID for Internet (WAN) port, but the VLAN used is chosen by the priority of each method (from highest to lowest): LLDP/CDP>Manual>DHCP VLAN. There is only one way to get VLAN ID for PC port: Manual.

**Note** LLDP and CDP methods have the same priority to get VLAN ID. Normally, the VLAN ID get for the phone by LLDP and CDP methods will be the same.

## **VLAN Discovery Method on Yealink Phones**

## **Automatic Discovery Method for VLAN**

## **LLDP**

## Introduction

LLDP (Link Layer Discovery Protocol) allows phones to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocol, and store the information that is learned about other devices. Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

Each of the TLV components has the following basic structure:

Туре	Length	Value
7 bits	9 bits	0-511 octets

#### LLDP supports advertising the following TLVs:

- Mandatory LLDP TLVs: Chassis ID, Port ID, and Time to Live (TTL) are included in an LLDPDU by default.
- **Optional LLDP TLVs**: System Name, System Description and so on, the phone sends the optional TLVs along with the mandatory TLVs in an LLDPDU.
- Organizationally Specific TLVs: MAC/PHY Configuration/Status and Port VLAN ID, which are defined in IEEE Standard 802.3 and 802.1 respectively.

The LLDP frame ends with a special TLV, named end of LLDPDU in which both the type and

length fields are 0.

## **LLDP-MED**

LLDP-MED (Media Endpoint Discovery) is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED specifically provides support for voice over IP (VoIP) applications and provides the following capabilities:

- Capabilities Discovery–allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled. It can be used to indicate whether the connected device is a phone, a switch, a repeater, etc.
- Voice VLAN Configuration-provides a mechanism for a switch to notify a device which VLAN to use, which enables "plug and play" networking.
- Power Management-provides information related to how the device is powered, power priority, and how much power the device needs.
- Inventory Management-provides a means to manage device and the attributes of the device such as model number, serial number, software revision, etc.
- Location Identification Discovery–provides location information from the switch to the device when placing an emergency call.

## In addition to the TLVs advertised by LLDP, LLDP-MED also supports advertising the following TLVs:

- LLDP-MED capabilities TLV
- Network policy TLV
- Power management TLV
- Inventory management TLV
- Location identification TLV (not supported by phones)

It should be noted that either LLDP or LLDP-MED-but not both-can be used at any given time on an interface between two devices.

#### **LLDP Feature on Yealink Phones**

LLDP provides exceptional interoperability benefits, IP telephony troubleshooting, automatic deployment of policies and advanced PoE (Power over Ethernet). When LLDP feature is enabled on phones, the phones periodically advertise their own information to the directly connected LLDP-enabled switch. The phones can also receive LLDP packets from the connected switch. When the application type is "voice", phones decide whether to update the VLAN configurations obtained from the LLDP packets. When the VLAN configurations on the phones are different from the ones sent by the switch, the phones perform an update and reboot. This allows the phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

## **Supported TLVs of Phones**

TLVs supported by phones are summarized in the following table:

TLV Type	TLV Name	Description							
	Chassis ID	Specifies the IP address of the phone.							
	Port ID	Specifies the MAC address of the phone.							
Mandatory TLVs	Time to Live	Specifies the lifetime of the transmitted information on the phone. The default value is 180s.							
	End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU. No further processing of TLVs after this is necessary. This is a mandatory TLV and therefore must be present at the end of the data stream.							
	System Name	Specifies the administratively-assigned name for the phone (per RFC3418). For more information, refer to Appendix B: System Names on page 25.							
Optional	System Description	Specifies the description of the phone.							
TLVs	System Capabilities	Specifies the supported and enabled capabilities of the phone. The Telephone capability is supported and enabled by default.							
	Port Description	Specifies the description of the sending port. The default value is "WAN PORT".							
IEEE Std 802.3 Organization ally Specific TLV	MAC/PHY Configuration/St atus	<ul> <li>Specifies duplex and bit rate settings of the phone.</li> <li>The Auto-Negotiation is supported and enabled by default.</li> <li>The advertised capabilities of PMD Auto-Negotiation are: <ul> <li>10BASE-T (half duplex mode)</li> <li>10BASE-T (full duplex mode)</li> <li>100BASE-TX (half duplex mode)</li> <li>100BASE-TX (full duplex mode)</li> <li>100BASE-TX (full duplex mode)</li> <li>100BASE-T (full duplex mode)</li> </ul> </li> <li>100BASE-T (full duplex mode)</li> <li>100BASE-TX (full duplex mode)</li> <li>100BASE-TX (full duplex mode)</li> <li>100BASE-T (full duplex mode).</li> </ul>							

TLV Type	TLV Name	Description						
		Yealink T48S/T46S/T42S Skype for Business phones that have Gigabit Ethernet support 1000BASE-T.						
	Media Capabilities	<ul> <li>Specifies the MED device type of the phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU.</li> <li>The supported LLDP-MED TLV types are: <ul> <li>LLDP-MED Capabilities</li> <li>Network Policy</li> <li>Extended Power via MDI-PD</li> <li>Inventory</li> </ul> </li> </ul>						
	Network Policy	Specifies the port VLAN ID, application type, L2 priority and DSCP value.						
	Extended Power-via-MDI	Specifies power type, source, priority and value. For more information on power value, refer to Appendix D: Power Values on page 26.						
LLDP-MED TLVs	Inventory - Hardware Revision	Specifies the hardware revision of phone.						
	Inventory - Firmware Revision	Specifies the firmware revision of phone.						
	Inventory - Software Revision	Specifies the software revision of phone.						
	Inventory - Serial Number	Specifies the serial number of phone.						
	Inventory - Manufacturer Name	Manufacturer name of phone. The default value is "Yealink".						
	Inventory - Model Name	Specifies the model name of phone. For more information, refer to Appendix C: Model Names on page 25.						
	Asset ID	Specifies the asset identifier of phone.						

## **Configuring LLDP Feature**

LLDP is enabled on phones by default. You can configure LLDP via web user interface or using

configuration files. You can also configure the sending frequency of LLDP packet. The default sending frequency is 60s. The followings take configurations of a T46S Skype for Business phone running firmware version 8 as examples.

#### To configure LLDP feature via web user interface:

**1.** Log into the web user interface with the administrator credential.

The default administrator user name and password are both "admin".

- 2. Click on Network->Advanced.
- 3. In the LLDP block, select the desired value from the pull-down list of Active.
- 4. Enter the desired time (in seconds) in the Packet Interval (1~3600s) field.

Yealink	_	_		_	_		Log Out
ICCAINT 1465	Status	Account	Network F	eatures	Settings	Directory	Security
Basic	LLD	P 🕜					NOTE
PC Port			Active Packet Interval (1~3600s)	Enabled 60		-	VLAN A VLAN is a logical local area
Advanced	CDP	0					network (or LAN) that extends beyond a single traditional LAN
			Active	Enabled		•	to a group of LAN segments, given specific configurations.
			Packet Interval (1~3600s)	60			0.05

5. Click **Confirm** to accept the change.

The web user interface prompts the warning "Some settings you changed take effect when you restart your machine! Do you want to reboot now?".

**6.** Click **OK** to reboot the phone.

#### To configure LLDP feature using configuration files:

1. Add/Edit LLDP parameters in configuration files.

The following table shows the information of parameters:

Parameters	Permitted Values	Default									
static.network.lldp.enable	0 or 1	1									
Description:											
Enables or disables LLDP on the phone.											
<b>0</b> -Disabled											
1-Enabled											
static.network.lldp.packet_interval	Integer from 1 to 3600	60									
Description:	Description:										
Configures the interval (in seconds) for the phon	e to send the LLDP request										

The following shows an example of LLDP configuration in configuration files:

static.network.lldp.enable = 1

static.network.lldp.packet\_interval = 60

**2.** Upload configuration files to the root directory of the provisioning server and trigger phones to perform an auto provisioning for configuration update.

For more information on auto provisioning, refer to

Yealink\_Skype\_for\_Business\_HD\_IP\_Phones\_Auto\_Provisioning\_Guide.

## **Verifying the Configuration**

After LLDP feature is enabled, the phone performs the following:

- Periodically advertises information (e.g., hardware revision, firmware revision, serial number) of the phone to a multicast address on the network.
- Allows LLDP packets to be received from the Internet (WAN) port or WLAN port.
- Supports the MAC/PHY configuration (e.g., speed rate, duplex mode).
- Obtains VLAN info from the network policy, which takes precedence over manual settings.

The following figure shows the LLDP packet sent by the phone, the packet contains multiple TLVs (before obtaining VLAN ID).

<u>File Edit View Go Capture Analyze St</u>	atistics Telephony Tools I	internals Help			
				¥ 🗹 🍕 %   💢	
Filter: Ildp	<b></b>	Expression Clea	Apply		
Time Source 305 36.0984580 X1 amenYe_41:46:dd		rotocol Length		4 = 0.0.0.0 Port Id = 00:15:65:41:46:00 TTL -	0
305 36.0984580 XTamenye_41:46:dd 314 37.0954890 Xiamenye 41:46:dd				I = 0.0.0.0 Port Id = 00:15:65:41:46:dd TTL =	
328 37.6762480 XiamenYe_41:46:dd				<pre>i = 0.0.0.0 Port Id = 00:15:65:41:46:dd TTL =</pre>	
336 38,1003050 C15C0 5d:42:98				1 = c0:62:60:5d:42:80 Port Id = Fa1/0/22 TTL	
359 39.1069640 cisco_5d:42:98	LLDP_Multicast L			= c0:62:6b:5d:42:80 Port Id = Fa1/0/22 TTL	
372 40.1137510 cisco_5d:42:98	LLDP_Multicast L	LDP 545	chassis	= c0:62:6b:5d:42:80 Port Id = Fa1/0/22 TTL	= 120 System Name = yealink-cisco
568 63.4176990 cisco_5d:42:98	LLDP_Multicast L			<pre>= c0:62:6b:5d:42:80 Port Id = Fa1/0/22 TTL</pre>	
798 93 4243020 cisco 5d-42-98	IIDP Multicast I	I DP 545		I = c0:62:6b:5d:42:80 Port Td = Fa1/0/22 TTL	= 120 System Name = vealink-cisco
*			1		,
Frame 328: 221 bytes on wire (1					
🗄 Ethernet II, Src: XiamenYe_41:4	6:dd (00:15:65:41:46:	dd), Dst: LLDP_	Multicast	01:80:c2:00:00:0e)	
Link Layer Discovery Protocol					
E Chassis Subtype = Network add	ress				
Port Subtype = MAC address Time To Live = 180 sec					
Inme To Live = 180 sec System Name = SIP-T465					
System Description = 66,9,254	124				
Capabilities	. 124				
Port Description = WAN PORT					
IEEE 802.3 - MAC/PHY Configur	ation/Status				
	action, beacas				
TIA - Network Policy					
1111 111 = TLV T	vpe: Organization Spe	cific (127)			
0 0000 1000 - TLV L					
Organization Unique Code: T	IA (0x0012bb)				
Media Subtype: Network Poli					
Application Type: Voice (1)					
1 = Polic					
.0 = Tagge	d: NO				
0 0000 0000 000. = VLAN					
= L2 Pr	lority: 0				
00 0000 = DSCP value: 0					

The following figure shows the LLDP packet received by the phone, the packet contains multiple TLVs (sent by the switch).

<u>File Edit View Go Capture An</u> a	lyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools	Internals <u>H</u> elp							
24 em em em em i i i i i i i i i i i i i i	😂 🖴 I 🔍 🗢 🏟 🧛 🕇 🛓		. 0. 🗹   🌌	🖻 🅵 🐝  🖼					
Filter: Ildp		<ul> <li>Expression Clear</li> </ul>	Apply						
Time Source	Destination	Protocol Length	Info						
568 63.4176990 cisco_5d:42:	98 LLDP_Multicast	LLDP 545	Chassis Id	<pre>= c0:62:6b:5d:42:</pre>	80 Port Id	= Fa1/0/22 TT	L = 120 Sy	stem Name = )	, vealink-cisco
798 93.4243020 Cisco_5d:42:				= c0:62:6b:5d:42:					
845 97.4168990 X1amenYe_41:				= 10.10.222.19 Po					
125 123.380655 cisco_5d:42:	98 LLDP_Multicast	LLDP 545		= c0:62:6b:5d:42:	80 Port Id	= Fa1/0/22 TT	L = 120 Sy	stem Name = )	yealink-cisco
Link Layer Discovery Prot			m						•
Port Description = Fast     Capabilities     Management Address     Management Address     TIA - Media capabilitie     TIA - Inventory - Hardw     TIA - Inventory - Softw     TIA - Inventory - Manuf     TIA - Network Policy	isco3750.yealink.com ription = Cisco IOS Softwa thernet/0/22 s are Revision are Revision are Revision acturer Name Name TLV Type: organization Sp TLV Length: 8 dod: TLA (Dx0012bb) Policy (Dx02) Policy (Dx02) Policy (Dx02) Policy (Dx02) VLAN IGI 222 La Priority: 5		-е (С3750-IР	SERVICESK9-M), Ve	rsion 12.24	(55)SE6, RELEA	SE SOFTWAR	E (fc1)\nTech	nnical Suppor

The following figure shows the LLDP packet sent by the phone, the packet contains multiple TLVs (after obtaining VLAN ID).

File	Edit View G	o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatist	ics Telephony Tools I	nternals Hein	ein
	Lan Tour of				
			~ • • • • u 🛎		
Filter	: Ildp			Expression	on Clear Apply
No.	Time	Source	Destination	Protocol	Length Info
	228 37.6762 236 38.1003 236 38.1003 237 9.1069 259 9.1067 259 9.3 4243 259 9.3 4	80 x1 mm rv_11.46:dd 50 c1 soc. 561.42:98 50 x1 amerive_41:46:dd 1 bytes on wire (1766 5 soc. x1 amerive_41:46:dd 1 bytes on wire (1766 5 soc. x1 amerive_41:46:cd 2 soc. 2 soc. 5	LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast LLDP_MUIT(cast Cost), 221 byte: d (00:15:65:41:46: S 4 on/Status : Organization Spe th: S (0x002)bb Deffined Yes 2222	LLDP LLDP LLDP LLDP LLDP LLDP LLDP LLDP	221 chasis 1d = 0.0.0.0 port 1d = 00:15:65:41:46:dd TTL = 180 System Name = 177-465 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = Fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:80 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:60 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:60 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:60 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:60 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = c0:62:6b:51:42:60 Port 1d = fal/0/22 TTL = 120 System Name = yealink-ci 545 chassis 1d = fal/0/22 TTL = fal/0/22

## CDP

#### Introduction

CDP (Cisco Discovery Protocol) allows phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

#### **CDP Feature on Yealink Phones**

When CDP feature is enabled on phones, the phones periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive CDP packets from the connected switch. When the VLAN configurations on the phones are different from the ones sent by the switch, the phones perform an update and reboot. This allows the

phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

## **Configuring CDP Feature**

CDP is disabled on phones by default. You can configure CDP via web user interface or using configuration files. You can also configure the sending frequency of CDP packet. The default sending frequency is 60s.

## **Configuring CDP via Web User Interface**

The followings take configurations of a T46S Skype for Business phone running firmware version 9 as examples.

#### To configure CDP feature via web user interface:

**1.** Log into the web user interface with the administrator credential.

The default administrator user name and password are both "admin".

- 2. Click on Network->Advanced.
- 3. In the CDP block, select the desired value from the pull-down list of Active.
- 4. Enter the desired time (in seconds) in the Packet Interval (1~3600s) field.

ealink   1465	Status	Account	Network Fea	atures Settings	Directory	Security				
Basic	LLDP	0				NOTE				
C Bort			Active	Enabled						
PC Port			Packet Interval (1~3600s)	60		VLAN A VLAN is a logical local area				
Advanced	CDP	0				network (or LAN) that extend beyond a single traditional LAN				
			Active	Enabled	•	to a group of LAN segments, given specific configurations.				
			Packet Interval (1~3600s)	60		QoS				
	VLAN	0				When the network capacity is insufficient, QoS could provide				
	WAN	Port	Active	Disabled	-	priority to users by setting the				
			VID (1-4094)	1		value.				
			Priority	0		Local RTP Port Define the port for voice				

5. Click Confirm to accept the change.

The web user interface prompts the warning "Some settings you changed take effect when you restart your machine! Do you want to reboot now?".

6. Click **OK** to reboot the phone.

#### To configure CDP feature using configuration files:

1. Add/Edit CDP parameters in configuration files.

The following table shows the information of parameters:

Parameters	Permitted Values	Default
static.network.cdp.enable	0 or 1	0

Parameters	Permitted Values	Default								
Description:										
Enables or disables CDP on the phone.										
0-Disabled										
1-Enabled										
static.network.cdp.packet_interval	Integer from 1 to 3600	60								
Description:										
Configures the interval (in seconds) for the phone to send the CDP request.										

The following shows an example of CDP configuration in configuration files:

static.network.cdp.enable = 1

static.network.cdp.packet\_interval = 60

**2.** Upload configuration files to the root directory of the provisioning server and trigger phones to perform an auto provisioning for configuration update.

For more information on auto provisioning, refer to

Yealink\_Skype\_for\_Business\_HD\_IP\_Phones\_Auto\_Provisioning\_Guide.

## **Verifying the Configuration**

After CDP feature is enabled, the phone performs the following:

- Periodically advertises information (e.g., software revision, device ID, power consumption) of the phone to a multicast address on the network.
- Allows CDP packets to be received from the Internet (WAN) port or WLAN port.
- Obtains VLAN ID of connecting ports.

The following figure shows the CDP packet sent by the phone (before obtaining VLAN ID-with VLAN Query field).

Eile	<u>E</u> di	t <u>V</u> iew <u>G</u> o	<u>Capture</u>	<u>A</u> nalyze <u>S</u> tatis	stics Te	elephony	Tools	Internals <u>H</u> el	p												
	8	94 94 94	1 🖻 🖪	<b>X 2</b> 8	୍	• 🔶 🌍	<b>₹</b> 2		⊕ (	ર્ષ	21	¥ 🗹	<b>16</b> %	Ħ							
Filt	er: c	dp						Expression	Cle	ar App	oly										
No.		Time	Source		Desti	ination		Protocol	Le	ngth In	nfo										
				e_41:46:dd											Port ID:						
			14 cisco_5			/VTP/DTP,									50.yealink.			FastEth	ernet1/	0/22	
				e_41:46:dd											Port ID:						
				e_41:46:dd											Port ID: 1						
			62 Cisco_5			/VTP/DTP,									50.yealink.			FastEth	ernet1/	0/22	
				e_41:46:dd											Port ID: 1						
			32 Cisco_5			/VTP/DTP									50.yealink.			FastEth	ernet1/	0/22	
			00 xiameny 48 cisco 5	e_41:46:dd		VTP/DTP,									Port ID: 1 50.yealink.					(0. (0.0	
	1/10	181.4192	48 C15C0_5	0:42:98	CDP/	/VIP/DIP,	/PAGP/	UDCDP		517 D		10: 3	/ealink-c	15C03/	50. yearink.	com Po	rt 10:	Fasteth	ernet1/	0/22	
< []	_									-	m	_									•
				on wire (99	2 bits	s), 124	bytes	captured	(992 l	oits)											
		802.3 Et																			
		cal-Link (																			
Ξ 🤇			ry Protoco	51																	
		rsion: 2																			
		L: 180 se																			
			xc241 [cor																		
			T460015654	146DD																	
		dresses nt ID: WA	DODT																		
		oabilitie																			
		ftware Ve																			
		atform: T																			
		plex: Hal																			
			mption: 80	000 mW																	
			uery: 512																		
ľ				ery (0x000f	5																
		ength: 8			·																
		Data																			
		voice VLA	N: 512																		

The following figure shows the CDP packet received by the phone (with VLAN Reply field).

<u>File Edit View Go Cap</u>	ture <u>A</u> nalyze <u>S</u> tatist	ics Telephony <u>T</u> ools	Internals Help							
<b>.</b>	🖥 💥 😂 占 🛛	् 🗢 🔿 🐴 🖥		ର୍ ପ୍ 🖭	🧸 🗹 👧	<b>%</b>   😫				
Filter: cdp			Expression Cle	ear Apply						
No. Time Sou	rce	Destination	Protocol L	ength Info						
1052 102.491507 xia	amenYe_41:46:dd	CDP/VTP/DTP/PAGE	/UD CDP	116 Device	ID: T4600	15654146DD	Port ID: WAN	PORT		
1059 103. 395614 cis	sco_5d:42:98	CDP/VTP/DTP/PAGE	/UD CDP	517 Device	ID: yeali	nk-cisco375	0.yealink.com	Port ID:	FastEthernet1/0/22	
1185 118.399333 xia							Port ID: WAN			
1198 119. 396632 xia							Port ID: WAN			
1199 119.409462 cis		CDP/VTP/DTP/PAgP							: FastEthernet1/0/22	
1210 120.40/969 X1	amenye_41:46:dd	CDP/VTP/DTP/PAGE	/UDCDP		ID: 14600	15654146DD	PORT ID: WAN	PORT		_
•				m						•
🗷 Logical-Link Contr										
Cisco Discovery Pr	otocol									
Version: 2										
TTL: 180 seconds										
Device ID: yeali Software Version		Innk.com								
Platform: cisco										
Addresses	w5-C5/30v2-2415									
Port ID: FastEth	ernet1/0/22									
	criticity of th									
Protocol Hello:	Cluster Manageme	nt								
VTP Management D										
Mative VLAN: 5										
Duplex: Half										
VOIP VLAN Reply:										
	N Reply (0x000e)									
Length: 7										
Data	-									
Voice VLAN: 22										
Trust Bitmap: 0x										
<ul> <li>Untrusted port C</li> <li>Management Addre</li> </ul>										
Location: \003\0										
Elecation: (003(0		S miel								

The following figure shows the CDP packet sent by the phone (after obtaining VLAN ID-without VLAN Query field).

Ele Edit View Go Capture Analyze Statist	tics Telephony <u>T</u> ools Internals <u>H</u> elp	
Bi Bi Bi Bi Bi Di Bi	्, ⇔ ⇔ ୠ क़ ऺ॒   ॎॖॾॎ । Q, Q, Q, 17   ₩ ⊠ 5, %   ₩	
Filter: cdp	Expression Clear Apply	
No. Time Source	Destination Protocol Length Info	
1059 103.395614 cisco_5d:42:98	CDP/VTP/DTP/PAgP/UDCDP 517 Device ID: yealink-cisco3750.yealink.com Port ID: FastEthernet1/0/22	
1185 118.399333 xiamenye_41:46:dd		
1198 119. 396632 xiamenYe_41:46:dd		
1199 119.409462 cisco_5d:42:98 1210 120.407969 xiamenYe_41:46:dd	CDP/VTP/DTP/PAgP/UDCDP 517 Device ID: yealink-cisco3750.yealink.com Port ID: FastEthernet1/0/22 CDP/VTP/DTP/PAgP/UDCDP 124 Device ID: T460015654146DD Port ID: WAN PORT	
1225 121.414332 cisco 5d:42:98	CDP/VTP/DTP/PAGP/UDCDP 517 Device 1D: vedifik-cisco3750.yealink.com Port ID: FastEthernet1/0/22	
1706 181.067700 xiamenYe_41:46:dd		
-	m	F.
B IEEE 802.3 Ethernet Logical-Link Control Clogical-Link Control Clogical-Link Control Clogical-Link Control The Clogical Correct] B Device ID: T4600156514600 Addresses Type: Addresses (0x0002) Length: 17 Number of addresses: 1 B P 2004 Control Clogical Clogical Clogical Clogical B Clogical Clogical Clogical Clogical Clogical Clogical B Clogical Clogical Clogical B Clogical Clogical Clogical B Clogical Clogical Clogical Clogical B Clogical Clogical Clogical Clogical B Clogical Clogical Clogical Clogical Clogical B Clogical Clogical Clogical Clogical Clogical Clogical Clogical B Clogical	8 bits), 116 bytes captured (028 bits)	

## **DHCP VLAN**

Phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the phone will detect DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to detect the VLAN ID.

## **Configuring DHCP Option on a DHCP Server**

Before using DHCP VLAN feature on phones, you must make sure that the DHCP option on the DHCP server is configured properly. This section provides instructions on how to configure a DHCP option for windows using DHCP Turbo.

## To configure DHCP option on a DHCP server:

- **1.** Start the DHCP Turbo application.
- 2. Right click **Option Types**, and then select **New Option Type**.

🍇 DHCP Turbo on loca	lhost (	modified)	)					-		_			X
<u>File Edit View Bindings</u>	s <u>T</u> ools	<u>H</u> elp											
			*	9	<b>C</b>	<u>s</u>	<b>h</b> ?						
Servers / Ė- Ilocalhost		Filter	Standar	d Option	ns			•	·				
🗄 避 Scopes		Tag			Option								<b></b>
			pe Ctrl Ctrl		SMTP ser POP3 ser NNTP ser	vers							
	■ <u>R</u> edo		Ctrl	+Y	WWW serv								
1			Ctrl	+X	Finger s IRC serv		s						
	 		Ctrl	+c	Streetta		rvers						
0	Paste		Ctrl	+V	Streetta User cla		servers						
	Delet	e	Del		User cla Device F								
	Selec	t All	Ctrl	+A			nformation						
Q	🤹 <u>F</u> ind		Ctrl	+F	Subnet S SIP Serv		ion						
	Prope		Ctrl		Cablelab	s Cli	ent Configuration						
Create a new option type		Descrip			Yealink :	Phone	Test VLAN ID						 •

3. Enter the desired option in the Tag field.

The custom options range from 128 to 254.

- 4. Enter the desired name in the Name field.
- 5. Select string from the pull-down list of Type.

/ Opt	tion Properties	X
Tag	132	
Name	Yealink Phone Test VLAN ID	
Туре	string 💌	
🔲 Si	gned 🗌 Arrayed	
Descri	ption	
	<u>O</u> K <u>C</u> ancel	

- 6. Click **OK** to finish setting the option properties.
- 7. Click 🔄 to accept the change.
- 8. Double click Named Policies.

9. Right click Global, and then select New Option.

le <u>E</u> dit <u>V</u> iew <u>B</u> indings <u>T</u> ools	-	[	[ ] ]		
🖪 💐 将 🐚 I	🖿 🔀 🦻	8 9 9	Sr <b>k</b> ?		
rvers 🛆	Tag 🗸	Name		Value	
localhost					
E-BScopes					
- Doption Types - Named Policies					
Glabal					
- 🧭 🕅 Ex 🖅 New Option	. Ctrl+V				
🤐 🎯 Datat 🔊 Undo	Ctrl+Z				
C Redo	Ctrl+Y				
Å Cu <u>t</u>	Ctrl+X				
🕒 Сору	Ctrl+C				
Paste	Ctrl+V				
Delete	Del				
Select <u>A</u> II	Ctrl+A				
🔍 <u>F</u> ind	Ctrl+F				
🛠 Properties	Ctrl+P				

The Option Selector screen displays as below:

	lector		
llter	Standard Options	•	
Tag $ abla$	Name		<b>^</b>
/ 🖅 – 6	Magic cookie		
/ 🖅 – 5	Home directory		
🚛 – 1	Boot file		
🚛 1	Subnet mask		
/ 🖅 2	Time offset		
/ 🖅 🖅	Gateways		
/ 🖅 4	Time servers		
/ 🔄 5	IEN116 name servers		
/ 🔁 6	Domain name servers		
/ 🔁 7	Log servers		
/ 🖅 8	Cookie/Quote servers		
···· ⁄ 🛃 9	LPR servers		
/ 🖅 10	Impress servers		
/ 🖅 🖅	RLP servers		
/ 🖅 12	Hostname		
/ 🖅 13	Boot file size		
/ 🖅 🖉	Merit dump file		
/ 🖅 🖅	Domain name		
/ 🖅 16	Swap servers		
/ 🖅 🖅	Root path		
/ 🖅 18	Extensions path		
/ 🔁 19	IP forwarding		-
escription			5
Jescription			3
		QK	Cancel

- **10.** Scroll down and double click the option created above.
- 11. Fill the VLAN ID to be assigned in the input field.

Three formats of valid values: VLAN-A=*VLANID*, *VLANID* and VID=*VLANID*. VLAN ID ranges from 1 to 4094.

🖅 Yea	alink Phon	e Test VLAN ID	×
11	1		
	Expressio	on	Build
	<u>o</u> k	Cancel	$\underline{A}$ dvanced >>

- **12.** Click **OK** to finish setting a custom option.
- **13.** Click **accept** the change.

Then you can find the configured option under **Global** option.

🍇 DHCP Turbo on localhost				
<u>File Edit View Bindings T</u> ools	<u>H</u> elp			
🛛 🖪 🛛 🕷 👔	🛋 🔀 🛠	r> ? (%   №?		
Servers /	Tag $\nabla$	Name		Value
Docalhost	<i>d</i> <b>2</b>  132	Yealink Fhone Test V	lan ID	111
Download complete	J			

## **Configuring DHCP Option on Yealink Phones**

DHCP VLAN is enabled on phones by default. You can configure DHCP VLAN via web user interface or using configuration files. You can also configure the DHCP option. The default DHCP option is 132. The followings take configurations of a T46S Skype for Business phone running firmware version 8 as examples.

#### To configure DHCP VLAN feature via web user interface:

**1.** Log into the web user interface with the administrator credential.

The default administrator user name and password are both "admin".

- 2. Click on Network->Advanced.
- 3. In the VLAN block, select the desired value from the pull-down list of DHCP VLAN Active.
- 4. Enter the desired value in the **Option** field.

You can specify 5 options at most and separate options by commas. The default value is 132.

			_	_	Log Out
Yealink 1465	Status Accoun	t Network Fea	tures Settings	Directory	Security
Deale	LLDP 🕜				NOTE
Basic		Active	Disabled	*	VLAN
PC Port		Packet Interval (1~3600s)	60		A VLAN is a logical local area network (or LAN) that extends
Advanced	CDP 🕜				beyond a single traditional LAN to a group of LAN segments,
		Active	Enabled	•	given specific configurations.
		Packet Interval (1~3600s)	60		QoS When the network capacity is
	VLAN 🕜				insufficient, QoS could provide priority to users by setting the
	WAN Port	Active	Disabled	•	value.
		VID (1-4094)	1		Local RTP Port Define the port for voice transmission.
		Priority	0	*	You can click here to get
	PC Port	Active	Disabled	•	more guides.
		VID (1-4094)	1		
	19245	Priority	0	+	
	DHCP VLAN	Active	Enabled	-	
		Option (1-255)	132		

#### 5. Click **Confirm** to accept the change.

The web user interface prompts the warning "Some settings you changed take effect when you restart your machine! Do you want to reboot now?".

6. Click **OK** to reboot the phone.

#### To configure DHCP VLAN feature using configuration files:

1. Add/Edit DHCP VLAN parameters in configuration files.

The following table shows the information of parameters:

Parameters	Permitted Values	Default						
static.network.vlan.dhcp_enable	0 or 1	1						
Description:								
Enables or disables DHCP VLAN discovery feature on the phone.								
<b>0</b> -Disabled								
1-Enabled								
static.network.vlan.dhcp_option	Integer from 128 to 254	132						
Description:								
Specifies the DHCP option used to detect the VL	AN ID.							
You can specify 5 options at most and separate of	options by commas.							

The following shows an example of DHCP VLAN configuration in configuration files:

static.network.vlan.dhcp\_enable = 1

static.network.vlan.dhcp\_option = 132

**2.** Upload configuration files to the root directory of the provisioning server and trigger phones to perform an auto provisioning for configuration update.

For more information on auto provisioning, refer to

*Yealink\_Skype\_for\_Business\_HD\_IP\_Phones\_Auto\_Provisioning\_Guide.* 

#### **Verifying the Configuration**

When the phone is configured to use DHCP for VLAN discovery, and the DHCP option is set to 132, the following processes occur:

- **1.** The phone broadcasts a DHCP Discover message to find out if there is a DHCP server available.
- 2. If the DHCP server sends a DHCP Offer message with the Option 132, the phone will accept the Offer, send a DHCP Request, and save the VLAN ID provided by the DHCP server in the DHCP option 132.
- **3.** After obtaining the VLAN ID from DHCP server, the phone will release the leased IP address and start a new DHCP Discover cycle with the now known Voice VLAN ID tag.

After this process, the phone will send all packets with the VLAN ID obtained from the DHCP server in the DHCP option 132.

The following figure shows the DHCP Discover message sent by the phone (before obtaining VLAN ID):

<u>Ele</u>		Capture Analyze Sta	tistics Telephony <u>T</u> ools In	ternals <u>H</u> elp								
<b>e</b> (		⊨ 🐻 🗶 😂 占	🔍 🗢 🔿 🐺 👱		ପ୍ପ୍ଷ୍ 🖭	🛛 🗹 月	8 % I 😫					
Filter:	bootp		•	Expression	Clear Apply							
lo.	Time	Source	Destination	Protocol	Length Info							
- r	3 0.110993	0.0.0.0	255.255.255.255	DHCP	590 DHCP	Discover	- Transact	tion ID	0x83952d00	1		
	4 0.115183		5.5.5.18	DHCP	342 DHCP				0X83952d00	-		
	5 0.150004		255.255.255.255	DHCP			- Transact					
	6 0.154213		5.5.5.18	DHCP	342 DHCP				0xbdaa1562			
	7 0.200977		255.255.255.255	DHCP			- Transact					
	8 0.205328		5.5.5.18	DHCP	342 DHCP				0x83952d00			
	9 10.068604	10.10.111.254	255.255.255.255	DHCP	346 DHCP		- Transact					
	11 10.161676		255, 255, 255, 255	DHCP			- Transact					
		10.10.111.254	10.10.111.2	DHCP	346 DHCP		- Transact					
	12 10.1050/0	10.10.111.234	10.10.111.2	UNCE	540 DHCP .	ACK.	- II alisaci		0XC48E020			
Use B00 H H H T S B C Y	er Datagram P Dtstrap Proto lessage type: dardware type ardware addr dops: 0 fransaction I seconds elaps sootp flags: lient IP add rour (client)	rotocol, Src Port col Boot Request (1) : Ethernet ess length: 6 D: 0x83952d00	Click here to know mo	rt: bootps	; (67)	15.255.2	55.255)					
c	lient MAC ad	re address paddir	1:27:b1 (00:15:65:11: g: 0000000000000000000000	00								
1020 1030 1040	2d 00 00 64	00 00 00 00 00	ea 01 01 06 00 83 95 00 00 00 00 00 00 00 00 11 27 b1 00 00 00 00 00	D.C., d								

Image         Image <th< th=""><th></th><th>lit <u>V</u>iew <u>G</u>o</th><th></th><th>atistics Telephony <u>T</u>ools Ir</th><th></th><th></th><th></th><th></th><th></th><th></th></th<>		lit <u>V</u> iew <u>G</u> o		atistics Telephony <u>T</u> ools Ir						
Internation         Protocol         Length         Info           30.110983         0:0:0:0:0         255.255.255.255         DEEP         190 DEEP DISCOVER         Transaction 10 0x83952000           40.113183         3:5:5:2         5:5:18         DEEP DISCOVER         Transaction 10 0x83952000           50.150004         0:0:0.0         255.255.255.255         DEEP DISCOVER         Transaction 10 0x83952000           50.150004         0:0:0.0         255.255.255.255         DEEP DISCOVER         Transaction 10 0x83952000           60.156228         5:5:5:2         5:5:18         DEEP DISCOVER         Transaction 10 0x83952000           80.20028         5:5:5:2         5:5:5:25:5:5:5:5:5:5:5:5:5:5:5:5:5:5:5:				) 이 수 🌣 🌍 👍 🛂		ର୍ପ୍ 🖸 🔛 👹 🖾 🖡	8 % I 🖬			
1010003         0.0.00         155/15/25/01/55         0xc/         500 (scher)         00120000           4.0.11593         0.0.00         255/25/255/255         0KP         500 0KPD BicScher         1 restanction 10 0x33922000           5.0.150004         0.0.0.0         255/255/255         DKP         590 0KPD Request         1 restanction 10 0x33922000           6.0.154213         5.55.2         5.5.18         DKPP         590 0KPD Request         1 restanction 10 0x33922000           8.0.20328         5.5.5.2         5.5.5.18         DKPP         590 0KPC Request         1 restanction 10 0x3392200           9.0.068604         0.0.0.0         255/255/255         DKP         590 0KPC Request         1 restanction 10 0x3392200           9.10.068604         0.0.0.0         255/255/255         DKP         590 0KPC Request         1 restanction 10 0x486620           11.10.16167         0.0.0.0         255/255/255         DKP         594 0KPC Request         1 restanction 10 0x486620           12.10.163676         10.10.111/24         10.10.111/2         UKP         346 0KPC Request         1 restanction 10 0x486620           12.10.163676         10.0.0.0         0.0.0.0         0.0.0         0.0.0         0.0.0           0.00000000000000000000000000000000000	Filter:	bootp		-	Expression	Clear Apply				
4 0.110183       5.5.5.2       5.5.5.18       DHEP       42 DHEP OFFE       - Transaction 10 0x83932000         5 0.50004       0.0.0.0       255.255.255.25       DHEP       90 DHEP Request - Transaction 10 0xbdaal562         6 0.154213       5.5.5.2       5.5.5.5       DHEP       342 DHEP ACK       - Transaction 10 0xbdaal562         7 0.20097       0.0.0.0       255.255.255.25       DHEP ACK       - Transaction 10 0x83932000         9 10.068604       0.0.0.0       255.255.255.25       DHEP ACK       - Transaction 10 0x63952000         9 10.068604       0.0.0.0       255.255.255.25       DHEP ACK       - Transaction 10 0xc486620         10 10.074079       10.0.111.254       10.10.111.2       DHEP AGK       - Transaction 10 0xc486620         12 10.168676       10.0.0.0       255.255.255.25       DHEP AGK       - Transaction 10 0xc486620         12 10.168676       10.0.10.11.24       10.10.111.2       DHEP AGK       - Transaction 10 0xc486620         12 10.168676       10.0.0.0       0.0.0.0       0.0.0.0       DHEP AGK       - Transaction 10 0xc486620         12 10.168676       10.0.0.0       0.0.0.0.0       0.0.0.0       DHEP AGK       - Transaction 10 0xc486620         12 10.161875       10.0.0.0       0.0.0.0       DHEP AGK       - Transa	lo.	Time	Source	Destination	Protocol	Length Info				
5 0.150004       0.0.0.0       255.255.255       DHCP       990 DHCP Request - Transaction ID 0xbdal562         7 0.200977       0.0.0       255.255.255       DHCP       142 DHCP ACK       - Transaction ID 0xbdal562         9 0.066604       0.0.0       255.255.255       DHCP Fequest - Transaction ID 0xbdal562         9 0.066604       0.0.0       255.255.255       DHCP Fequest - Transaction ID 0xbdal562         9 0.066604       0.0.0       255.255.255       DHCP Fequest - Transaction ID 0xc48e620         10 10.07097       0.0.0.0       255.255.255       DHCP Fequest - Transaction ID 0xc48e620         11 10.161676       0.0.0.0       255.255.255       DHCP Fequest - Transaction ID 0xc48e620         12 10.163676       10.10.111.2       DHCP Fequest - Transaction ID 0xc48e620         12 10.163676       10.10.111.2       DHCP Fequest - Transaction ID 0xc48e620         12 10.163676       10.0.0.111.2       DHCP Fequest - Transaction ID 0xc48e620         12 10.163676       10.0.0.0.0       DHCP Fequest - Transaction ID 0xc48e620         12 10.163676       10.0.0.0.0.0.0.0.0       DHCP Fequest - Transaction ID 0xc48e620         13 Bootpf Flags: 0x0000       0.0.0.0.0.0.0.0       DHCP Fequest - Transaction ID 0xc48e620         10 Bootpf Flags: 0x00000       0.0.0.0.0.0.0.0       DHCP FeqUEst - TransactiD ID 0xc48e620										
6 0.154213 5.5.2 5.5.2 5.5.5.8 DHCP 342 DHCP ACK - Transaction ID 0xbdaal562 7 0.20097 0.0.0.0 255.255,255.25 DHCP 390 DHCP Request - Transaction ID 0x8395200 8 0.205328 5.5.5.2 5.5.18 DHCP 342 DHCP ACK - Transaction ID 0x8395200 9 10.08606 0.0.0.0 255.255,255.25 DHCP 340 DHCP Discover - Transaction ID 0xc486620 10 10.074079 10.0.111.254 10.10.111.2 DHCP 346 DHCP Offer - Transaction ID 0xc486620 12 10.163676 10.0.0 255.255,255.25 DHCP 594 DHCP Discover - Transaction ID 0xc486620 12 10.163676 10.0.0 125.255,255.25 DHCP 594 DHCP Discover - Transaction ID 0xc486620 12 10.163676 10.0.0.0 (0.0.0.0) Transaction ID: 0x63952000 Seconds elapsed: 100 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 (0.0.0.0) Next server IP address: 0.0.0.0 (0.0.0.0) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client Mack addressi x Namerve_11:27:b1 (00:115:65:11:27:b1) Client Mack addressi x Namerve_11:27:b1 (00:15:65:11:27:b1) Client IP addressi x 10.0.0 (Discover Bootf Flags addring: 000000000000000000000000000000000000									•	
7 0.200977       0.0.0.0       255.255.255       DHCP       590 DHCP Request - Transaction ID 0x33952d00         9 10.068604       0.0.0.0       255.255.255       DHCP       594 DHCP Discover - Transaction ID 0x43952d00         9 10.068604       0.0.0.0       255.255.255       DHCP       594 DHCP Discover - Transaction ID 0x438620         11 10.161676       0.0.0.0       255.255.255       DHCP       594 DHCP Discover - Transaction ID 0xc48e620         11 10.161676       0.0.0.0       255.255.255       DHCP       594 DHCP Request - Transaction ID 0xc48e620         12 10.163676       10.10.111.2       DHCP       346 DHCP ACK - Transaction ID 0xc48e620         """"""""""""""""""""""""""""""""""										
8 0.20328       5.5.5.2       5.5.5.18       DHCP ACK       - Transaction ID 0x83952d00         9 10.06860       0.0.0.0       255.255.255.25       DHCP Discover - Transaction ID 0xc486620         11 10.161676       0.0.0.0       255.255.255.55       DHCP Discover - Transaction ID 0xc486620         12 10.163676       10.0.0.11.254       10.10.111.2       DHCP Discover - Transaction ID 0xc486620         12 10.163676       10.0.10.11.12       DHCP Discover - Transaction ID 0xc486620         12 10.163676       10.0.11.12       DHCP Discover - Transaction ID 0xc486620         """"""""""""""""""""""""""""""""""										
9 10.068604         0.0.0         255.255.255         DHCP         954 DHCP Discover         Transaction ID 0xc48e620           11 10.161676         0.0.0         255.255.255         DHCP         954 DHCP PGRequest         Transaction ID 0xc48e620           11 10.161676         0.0.0         255.255.255         DHCP         954 DHCP PGRequest         Transaction ID 0xc48e620           12 10.163676         10.10.111.2         DHCP         346 DHCP PGRequest         Transaction ID 0xc48e620           """"""""""""""""""""""""""""""""""										
1010.074079 10.10.111.254 10.10.111.2 DKCP 340 DKCP Offer - Transaction ID 0xc48e620 1110.1618676 10.0.0 255.255.255.25 DKCP 340 DKCP Ack - Transaction ID 0xc48e620 1210.163876 10.10.111.254 10.10.111.2 DKCP 346 DKCP ACK - Transaction ID 0xc48e620 mr anastion ID: 0x5395200 seconds elapsed: 100 Bootp flags: 0x0000 (unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (Client) IP address: 0.0.0.0 (0.0.0.0) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: xiamerve_11:27:b1 (00:15:65:11:27:b1) Client Macra address: xiamerve_11:27:b1 (00:15:65:11:27:b1) Client mane not given Magi Ccookie: DKCP DKCP Message Type = DKCP Discover Bootp flags in differ i field identifier Bootp flags inter i dentifier = "udhcp 1.0.3" Bootp flags inter i dentifier = "udhcp 1.0.5" Bootp flags inter i dentifier = "u										
1110.161076 0.0.0.00       255.255.255.255       DHCP       344 DHCP Request - Transaction ID 0xc48e620         1210.163676 10.10.111.254       10.10.111.2       DHCP       346 DHCP Acquest - Transaction ID 0xc48e620         Hops: 0       Transaction ID 0xc48e620       ID 0xc48e620         Boopf Flags: 0x0000 (unicast)       ID 0xc48e620         Client IP address: 0.0.0.0 (0.0.0.0)       Vour (client) IP address: 0.0.0.0 (0.0.0.0)         Nets server IP address: 0.0.0.0 (0.0.0.0)       Nets server IP address: 0.0.0.0 (0.0.0.0)         Client Machaera addxix server_11271bl (0.0013:165:11:27:bl)       Client Machaera addxix server_127:address in 0.0000000000000000000000000000000000										
12 20.163676 10.10.111.254 10.0.111.2       OKCP       346 DKCP ACK       - Transaction ID 0xc486620         """"""""""""""""""""""""""""""""""										
massation ID: 0x83952d00         seconds elapsed: 100         Bootp flags: 0x0000 (unicast)         Client IP address: 0.0.0.0 (0.0.0.0)         Your (Client) IP address: 0.0.0.0 (0.0.0.0)         Nets server IP address: 0.0.0.0 (0.0.0.0)         Nets yearus IP address: 0.0.0.0 (0.0.0.0)         Sector flags         Sector flags         Client MA camero sci Xismenve_ILI27.bl (0001515511127:bl)         Client MA camero sci Xismenve flags         Boott flags										
Hops: 0 Transaction ID: 0x83952000 Seconds elapsed: 100 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0		10.1050/0	10.10.111.234	10.10.111.2	DIREF		- mansaccion a	0 070406020		
Padding	C1 YC Ne C1 C1 Se BC Ma BC Ma B OP B OP B OP B OP B OP B OP B OP B OP	ient IP add uur (client) stt server I ient Mac add ient hardwa rver host n oot file nam ugic cookie: ttion: (t=53 ttion: (t=12 ttion: (t=57 ution: (t=57 ution: (t=57 ution: (t=57)	ress: 0.0.00 (C IP address: 0.0 P address: 0.0 C P address: 0.0 dress: xiamenye re address paddi ame not given e not given DHCP J=1) DHCP Messa ,1=7) Client idd ,1=12) Vendor Cl 5,1=37) V-I Vendor J=2) Maximum DH	0.0.0) 0.0 (0.0.0.0) 0.0 (0.0.0.0) 0.0 (0.0.0.0) 11:27:bl (00:15:65:11: ng: 0000000000000000000 the type - DHCP Discove mtifier ass identifier = "udht for-specific Informatic CP Message Size = 576	00 r p 1.10.3					

The following figure shows the DHCP Offer message received by the phone (DHCP server sends a DHCP Offer message with the Option 132):

<u>File</u>	Ele Edit View Go Capture Analyze Statistics Telephony Tools Internals Help									
		⊨ 🛃 🗶 🛃 🗎	् 🗢 🛸 😜 春 👱		ପ୍ର୍ଷ୍ 🖭	🏽 🗹 🐔	3 🖗 🛙 🛱 👘			
Filter:	bootp		-	Expression.	. Clear Apply					
No.	Time	Source	Destination	Protocol	Length Info					
	3 0.110993	0.0.0.0	255, 255, 255, 255	DHCP	590 DHCP (	Discover	- Transaction	ID 0x83952d00		
	4 0.115183	5.5.5.2	5.5.5.18	DHCP	342 DHCP (		- Transaction			
	5 0.150004	0.0.0.0	255.255.255.255	DHCP	590 DHCP 1	Request	- Transaction	ID Oxbdaa1562		
	6 0.154213	5.5.5.2	5.5.5.18	DHCP	342 DHCP /	ACK	- Transaction	ID 0xbdaa1562		
	7 0.200977	0.0.0.0	255.255.255.255	DHCP	590 DHCP	Request	- Transaction	ID 0x83952d00		
	8 0.205328	5.5.5.2	5.5.5.18	DHCP	342 DHCP /	ACK	- Transaction	ID 0x83952d00		
	9 10.068604		255.255.255.255	DHCP			- Transaction			
		10.10.111.254	10.10.111.2	DHCP	346 DHCP (		- Transaction			
	11 10.161676		255.255.255.255	DHCP			- Transaction			
1	12 10.163676	10.10.111.254	10.10.111.2	DHCP	346 DHCP /	ACK	- Transaction	ID 0xc48e620		
<										
	Relay agent IP address: 0.0.0.0 (0.0.0.0) Client Mardware address: 2016 (001565111:27:b1) Client hardware address padding: 0000000000000000 Server host name: mid0057-dC23398 Boot file name not given Magic cookie: DKCP © option: (L=3, 1=4) DKLPt Message Type = DKCP Offer © option: (L=3, 1=4) DKLPt Message Type = DKCP Offer © option: (L=3, 1=4) DKLPt Message Type = DKCP offer © option: (L=3, 1=4) DKLPt Message Type = DKCP offer © option: (L=3, 1=4) DKLPt Message Type = DKCP offer © option: (L=3, 1=4) Relinding Time value = 5 hours, 15 minutes © option: (L=3, 1=4) Relinding Time value = 3 hours © option: (L=3, 1=4) Relinding time (vector specific)									
ter Option: (t=222,1=1) Unassigned © Option: (t=242,1=5) DecSIS full security server IP [TODO] ⊚ Option: (t=54,1=4) DHCP Server Identifier = 5.5.5.2 End Option Padding										
0120										

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

Ele Edit Wew Go Capture Analyze Statistics Telephony Iools Internals Help									
	볼 볼 볼 볼 🖮 🗁 🖂 2 🐇 😂 占 🔍 🔶 🗢 🌫 🖉 🔄 🔍 오. 이, 한 1 😹 10 🔨 11 🗍								
Filter: bootp	<ul> <li>Expression</li> </ul>	on Clear Apply							
No. Time Source	Destination Protocol	l Length Info							
3 0.110993 0.0.0.0	255.255.255.255 DHCP	590 DHCP Discover - Transaction ID 0x83952d00							
4 0.115183 5.5.5.2	5.5.5.18 DHCP	342 DHCP offer - Transaction ID 0x83952d00							
5 0.150004 0.0.0.0	255.255.255.255 DHCP	590 DHCP Request - Transaction ID 0xbdaa1562							
6 0.154213 5.5.5.2	5.5.5.18 DHCP	342 DHCP ACK - Transaction ID 0xbdaa1562							
7 0.200977 0.0.0.0	255.255.255.255 DHCP	590 DHCP Request - Transaction ID 0x83952d00							
8 0.205328 5.5.5.2	5.5.5.18 DHCP	342 DHCP ACK - Transaction ID 0x83952d00							
9 10.068604 0.0.0.0		594 DHCP Discover - Transaction ID 0XC486620							
10 10.074079 10.10.11		346 DHCP Offer - Transaction ID 0xc48e620							
11 10.161676 0.0.0.0	255.255.255.255 DHCP	594 DHCP Request - Transaction ID 0xc48e620							
12 10.163676 10.10.11	1.254 10.10.111.2 DHCP	346 DHCP ACK - Transaction ID 0xc48e620							
*		m b							
<pre>client IF address: 0.0.0.0 (0.0.0.0) Vour (client) IF address: 5.5.5.18 (5.5.5.18) Next server IP address: 5.5.5.18 (5.5.5.2) Relay agent IP address: 5.0.0.0 (0.0.0.0.0) Client MAC address: xiamerve_ll:27.bl (00:15:65:11:27:bl) Client hardware address paddrig: 00000000000000000 Server host name: mid0507-dc2a398 Boot file name not given Magic cookte: DKP @ option: (c+3, 1-4) DKP Message Type = DKCP ACK @ option: (c+3, 1-4) DKP Message Type = DKCP ACK @ option: (c+3, 1-4) DKP Message Time = 6 hours @ option: (c+3, 1-4) DKP Message Time = 6 hours @ option: (c+3, 1-4) DKP Message Time = 6 hours @ option: (c+3, 1-4) Rebinding Time Value = 3 hours, 15 minutes @ option: (c+3, 1-4) Rebinding Time Value = 3 hours @ option: (c+3, 1-4) Rebind</pre>									

After obtaining the VLAN ID from DHCP server, phone will release the leased IP address (5.5.5.18) and start a new DHCP Discover message with the VLAN-tag 111.

The following figure shows the DHCP messages received by the phone:

File Edit Vie	v Go Canture Analyze Sta	tistics Telephony <u>T</u> ools Internals	Help					
		Q, ⇔ ⇒ ⊕ 7 ½   🗐			8.0 I <b>6</b> 7			
			≝ <b>¤ ~ ~ ~</b> ~ ~		210 I 856			
Filter: bootp		<ul> <li>Expres</li> </ul>	sion Clear Apply					
No. Time	Source	Destination Proto	ol Length Info					
3 0.11		255.255.255.255 DHCP			Transaction			
	5183 5.5.5.2	5.5.5.18 DHCP	342 DHCP		Transaction			
	0004 0.0.0.0	255.255.255.255 DHCP			Transaction			
	4213 5.5.5.2	5.5.5.18 DHCP	342 DHCP		Transaction			
	0977 0.0.0.0	255.255.255.255 DHCP			Transaction			
	5328 5.5.5.2	5.5.5.18 DHCP	342 DHCP		Transaction			
	68604 0.0.0.0	255.255.255.255 DHCP			Transaction			
	74079 10.10.111.254	10.10.111.2 DHCP	346 DHCP		Transaction			
	61676 0.0.0.0	255.255.255.255 DHCP			Transaction		-	
12 10.1	63676 10.10.111.254	10.10.111.2 DHCP	346 DHCP	ACK -	Transaction	ID 0xc48e620		
٠			m					,
Ethernet II (VLAN tagged), Src: cisco_5d:42:c4 (c0:62:60:5d:42:c4), Dst: xiamenve_11:27:b1 (00:15:65:11:27:b1) © Destination: xiamerve_11:27:b1 (00:15:65:11:27:b1) © ULAN tag: VLAN-111, Proifvy-Gest Effort (default) Identifier: 80:1Q virtual LAW (0x8100) 000 0000 01:0 111 = VLAN: 111 Type: TP (UXUS0U) Titernet Protocol version 4, src: 10.10.111.254 (10.10.111.254), Dst: 10.10.111.2 (10.10.111.2) Uset atagram Protocol, src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (58) Mediane Type: Thermet Protocol, Src Port: bootps (67), Dst Port: bootpc (58) Mediane Type: Stort Regione Stort St								
client	IP address: 0.0.0.0 (0. lient) IP address: 10.1							
0030 06 00 0040 <mark>61 02</mark>								

After this process, the phone has obtained an IP address (10.10.111.2) from the DHCP server in the VLAN 111.

## **Manual Configuration for VLAN**

VLAN is disabled on phones by default. You can configure VLAN via web user interface or phone user interface or using configuration files. Before configuring VLAN on the phone, you need to obtain the VLAN ID from your network administrator. When you configure VLAN feature, the most important issue is to confirm the type of the connected port (access, trunk, and hybrid) on the switch. This ensures that the traffics (tagged/untagged) from the phones can be transmitted properly. VLAN feature could affect the ability of the phones to function in the network. Contact your network administrator for more information before configuration.

## **Configuring VLAN Feature**

You can enable or disable VLAN, and set specific VLAN IDs and priorities for the Internet (WAN) port and PC port respectively. The followings take configurations of a T46S Skype for Business phone running firmware version 8 as examples.

#### **Configuring VLAN Feature via Web User Interface**

To configure VLAN for Internet port via web user interface:

- 1. Click on Network->Advanced.
- In the WAN Port block, select the desired value from the pull-down list of WAN Port Active.
- 3. Enter the VLAN ID in the VID (1-4094) field.

4. Select the desired value (0-7) from the pull-down list of **Priority**.

Yealink 1465				_	Log Out
	Status Account	Network Fea	tures Settings	Directory	Security
Basic	LLDP 🕜				NOTE
PC Port		Active	Enabled	•	VLAN
		Packet Interval (1~3600s)	60		A VLAN is a logical local area network (or LAN) that extends
Advanced	CDP 🕜				beyond a single traditional LAN to a group of LAN segments,
		Active	Enabled	•	given specific configurations.
		Packet Interval (1~3600s)	60		QoS
	VLAN 🕜				When the network capacity is insufficient, QoS could provide
	WAN Port	Active	Enabled	•	priority to users by setting the value.
		VID (1-4094)	1		Local RTP Port
		Priority	0		Define the port for voice transmission.
	PC Port	Active	Disabled	•	You can click here to get
		VID (1-4094)	1		more guides.
		Priority	0	•	
	DHCP VLAN	Active	Enabled	-	
		Option (1-255)	132		
	Port Link 🕜				
		WAN Port Link	Auto Negotiate	•	
		PC Port Link	Auto Negotiate	•	
	Voice QoS		Tomes		
		Voice QoS (0~63)	46		
		SIP Qos (0~63)	26		

5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that the settings will take effect after a reboot.

6. Click **OK** to reboot the phone.

To configure VLAN for PC port via web user interface:

- 1. Click on Network->Advanced.
- 2. In the PC Port block, select the desired value from the pull-down list of Active.
- 3. Enter the VLAN ID in the VID (1-4094) field.

4. Select the desired value (0-7) from the pull-down list of Priority.

ealink   1465	Status	Account	Network	Features	Settings	Directory	Security	
Basic	LLDP (	0					NOTE	
PC Port			Active	E	nabled	•	VIAN	
PCPOIL			Packet Interval (1~36	600s) 60	)		A VLAN is a logical local area	
Advanced	CDP 🕜	)					network (or LAN) that extends beyond a single traditional LAN	
			Active	E	nabled	•	to a group of LAN segments, given specific configurations.	
			Packet Interval (1~3600s)		)		005	
	VLAN	0					When the network capacity is insufficient, QoS could provide	
	WAN Po	ort	Active	D	sabled	*	priority to users by setting the	
			VID (1-4094)				value.	
			Priority	0		•	Local RTP Port Define the port for voice	
	PC Port	k.	Active VID (1-4094)		abled		transmission.	
							You can click here to get more guides.	
			Priority	0		·	more guides.	
	DHCP V	VLAN	Active	E	nabled	-		
			Option (1-255)	13	32			
	Port Lin	ink 🕜						
			WAN Port Link	A	uto Negotiate	÷		
			PC Port Link	A	uto Negotiate	•		
	Voice Qo	os 🕜						
			Voice QoS (0~63)	40	5			
			SIP Qos (0~63)	26	5			

#### 5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that the settings will take effect after a reboot.

6. Click **OK** to reboot the phone.

#### To configure VLAN for Internet port (or PC port) via phone user interface:

- Press Menu->Setting->Advanced (default password: admin)
   ->Network->VLAN->WAN Port (or PC Port).
- Press (•) or (•), or the Switch soft key to select the desired value from the VLAN Status field.
- 3. Enter the VLAN ID (1-4094) in the VID Number field.
- **4.** Enter the priority value (0-7) in the **Priority** field.
- 5. Press the Save soft key to accept the change.

A dialog box pops up to prompt that the settings will take effect after a reboot.

6. Press **OK** to reboot the phone.

#### **Configuring VLAN Feature Using Configuration Files**

#### To configure VLAN for Internet (WAN) port and PC port using configuration file:

1. Add/Edit VLAN for Internet (WAN) port and PC port parameters in configuration files.

The following table shows the information of parameters:

Parameters	Permitted Values	Default						
static.network.vlan.internet_port_enable	0 or 1	0						
Description:								
Enables or disables the phone to tag VLAN ID in port.	packets sent from the Inter	net (WAN)						
0-Disabled								
<b>1</b> -Enabled								
static.network.vlan.internet_port_vid Integer from 1 to 4094 1								
Description:								
Configures the VLAN ID that associates with the	particular VLAN.							
static.network.vlan.internet_port_priority	Integer from 0 to 7	0						
Description:								
Specifies the priority used for transmitting VLAN packets.								
static.network.vlan.pc_port_enable	0 or 1	0						
Description:								
Enables or disables the phone to tag VLAN ID in	packets sent from the PC p	ort.						
<b>0</b> -Disabled								
1-Enabled								
static.network.vlan.pc_port_vid	Integer from 1 to 4094	1						
Description:								
Configures the VLAN ID that associates with the particular VLAN.								
static.network.vlan.pc_port_priority	Integer from 0 to 7	0						
Description:								
Specifies the priority used for transmitting VLAN	packets.							

The following shows an example of VLAN configuration in configuration files:

static.network.vlan.internet\_port\_enable = 1

static.network.vlan.internet\_port\_vid = 77

static.network.vlan.internet\_port\_priority = 5
static.network.vlan.pc\_port\_enable = 1
static.network.vlan.pc\_port\_vid = 76
static.network.vlan.pc\_port\_priority = 3

 Upload configuration files to the root directory of the provisioning server and trigger phones to perform an auto provisioning for configuration update.
 For more information on auto provisioning, refer to
 Yealink\_Skype\_for\_Business\_HD\_IP\_Phones\_Auto\_Provisioning\_Guide.

## Verifying the Configuration

The phone reboots after VLAN feature has been enabled. After starting up, the phone will be assigned with a subnet address defined for VLAN 77.

The following figure shows the VLAN ID sent and received by the phone:

Eile	Edi	: ⊻ie	v <u>G</u>	o <u>⊂</u> aptu	re <u>A</u> naly	ze	Statistics	Telephony	Tools	Help	
		04		💓   E		×	28	0,4	•		77 월   🗐 🗐   Q, Q, Q, 177   ₩ 121 158 3%   123
Filter	: sip	)									▼ Expression Clear Apply
No.	Tin	ne		Source			Destinatio	on	Proto	col	Info
1	12.	4493	22	10.2	.11.21	6	10.2.1	L.199	SIP	/SDF	Request: INVITE sip:201@10.2.1.199, with session description
		4511			.1.199			L1.216	SIP		Status: 100 Trying
		4528			.1.199		10.2.8				Request: INVITE sip:201010.2.8.216:5062, with session description
		4893			.8.216		10.2.1		SIP		Status: 100 Trying
		6490		10.2			10.2.1				Status: 180 Ringing
		6518			.1.199		10.2.1		SIP		Status: 180 Ringing
		4119			.8.216		10.2.1				Status: 200 OK, with session description
				10.2				L1.216			Status: 200 OK, with session description
		4963			.11.21		10.2.8		SIP		Request: ACK s1p:201010.2.8.216:5062
2	34.	4967	'49	10.2	.11.21	6	10.2.8	3.216	SIP		Request: ACK sip:201010.2.8.216:5062
4											
											captured (7264 bits)
										.2:23	<u>2:f9)</u> , Dst: Cisco_40:da:55 (6c:50:4d:40:da:55)
- 8								, ID: 7			
	011 = Priority: Excellent Effort (3)										
	0 = CFI: Canonical (0)										
				0100 1		ID:	77				
				0×0800							
											Dst: 10.2.1.199 (10.2.1.199)
							Port:	na-loca	Inse i	506	2), Dst Port: sip (5060)
+ S	Session Initiation Protocol										

## **Appendix**

## **Appendix A: Glossary**

**IEEE** (Institute of Electrical and Electronics Engineers) –a professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

**TIA** (Telecommunications Industry Association) –accredited by the American National Standards Institute (ANSI) to develop voluntary, consensus-based industry standards for a wide variety of ICT products.

**IEEE 802.3** –a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet.

**Port-based VLAN** –a port-based VLAN is a group of ports on a Gigabit Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

**Port and Protocol-based VLAN** –initially defined in IEEE 802.1v (currently amended as part of 802.1Q-2003) enables data frame classification and assignment to unique VLANs based on the received data frame type and the protocol information in its payload.

**TPID** (tag protocol identifier) –a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. It is used to distinguish the frame from untagged frames.

**PCP** (Priority Code Point) –a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority.

**CFI** (Canonical Format Indicator) –used for compatibility reason between Ethernet type network and Token Ring type network. It is always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.

## **Appendix B: System Names**

Model	System Name
SIP-T48S	SIP-T48S
SIP-T46S	SIP-T46S
SIP-T42S	SIP-T42S
SIP-T41S	SIP-T41S

The following table outlines the Yealink phone models and their system names:

## **Appendix C: Model Names**

The following table outlines the Yealink phone models and their model names:

Model	Model Name
SIP-T48S	T48S
SIP-T46S	T46S
SIP-T42S	T42S
SIP-T41S	T41S

## **Appendix D: Power Values**

Model	Power Value
SIP-T48S	10800mW
SIP-T46S	7600mW
SIP-T42S	6800mW
SIP-T41S	12500mW

The following table outlines the power value sent in LLDP-MED:

## **Appendix E: Normative References**

LLDP and LLDP-MED: http://en.wikipedia.org/wiki/Link\_Layer\_Discovery\_Protocol

CDP: http://en.wikipedia.org/wiki/Cisco\_Discovery\_Protocol

IEEE 802.3: http://www.ieee802.org/3/

VLAN: http://en.wikipedia.org/wiki/Virtual\_LAN

IEEE 802.1q: http://en.wikipedia.org/wiki/802.1Q

LLDP on Cisco Switch:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2\_55\_se/configuration/guide/swlldp.html

CDP on Cisco Switch:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2\_55\_se/ configuration/guide/scg3750/swcdp.html

## **Customer Feedback**

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.