

VLAN Feature on Yealink IP Phones



Version 15.42 | May. 2020

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.

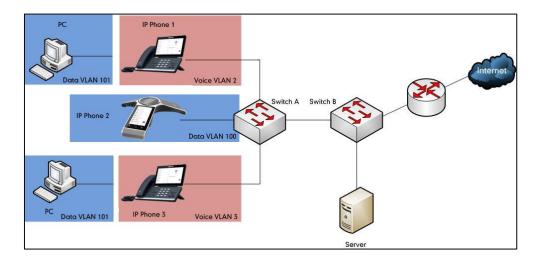
802.1Q adds a 4-byte tag between the source MAC address and the Ethernet type fields of the Ethernet frame. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP (Priority Code Point), CFI (Canonical 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. The Manual method for PC port is not available on

CP960 Teams IP Phones.

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 1.	
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 MAC/PHY Organizatio Configuration/St		Specifies duplex and bit rate settings of the phone. The Auto-Negotiation is supported and enabled by default. The advertised capabilities of PMD Auto-Negotiation are: • 10BASE-T (half duplex mode)	
nally Specific TLV	atus	 TOBASE-T (half duplex mode) 10BASE-T (full duplex mode) 100BASE-TX (half duplex mode) 100BASE-TX (full duplex mode) 1000BASE-T (full duplex mode). 	

TLV Type	TLV Name	Description
		Note : By default, all phones have the PMD Advertised Capability set for 10BASE-T and 100BASE-TX.
		Yealink MP56/T58A/T56A/T55A/VP59 Teams phones that have Gigabit Ethernet support 1000BASE-T.
		Specifies the MED device type of the phone and the supported LLDP-MED TLV type can be encapsulated in LLDPDU.
	Media	The supported LLDP-MED TLV types are:
	Capabilities	LLDP-MED Capabilities
		Network Policy
		Extended Power via MDI-PD
		Inventory
	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 2.
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 2.
	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 T58A Teams IP phone 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, turn on the LLDP feature.
- 4. Enter the desired time (in seconds) in the Packet Interval (1~3600s) field.

Yealink T58			
Status	LLDP		
🚱 Network 🔷 🗠	Active		0
	Packet Interval (1-3600s)	60	Ø
PC Pat	CDP 🔞		
🙂 Features 🗸 🗸	Active		0
Settings ~	Packet Interval (1~3600s)	60	Ø
🥥 Security 🗸 🗸	WAN Port		
	Active	000	0
	VID (1-4294)		0
	Priority		• 0

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.						
0-Disabled						
1-Enabled						
static.network.lldp.packet_interval	Integer from 1 to 3600	60				

Parameters	Permitted Values	Default			
Description:					
Configures the interval (in seconds) for the phone	e to send the LLDP reques	t.			

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_Teams_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).

Efe Edit View Go Capture Analyze Statistics Telephony Iools Internals Help							
2 z z z z z z z z z z z z z z z z z z z							
Filter: Ildp	▼ Expressi	ion Clear Appiy					
Time Source 3/D 360.0984/580 X1amerYee_41146:dd 328 37.6762480 X1amerYee_41146:dd 328 37.6762480 X1amerYee_41146:dd 328 37.6762480 X1amerYe_41146:dd 329 39.1069640 C1sco_5d:42:98 359 39.1069640 C1sco_5d:42:98 329 39.1069640 C1sco_5d:42:98 568 63.4176990 C1sco_5d:42:98 368 4176990 C1sco_5d:42:98 568 63.4176990 C1sco_5d:42:98 378 41 24300 C1sco_5d:42:98 578 43.4176990 C1sco_5d:42:98 378 41 24300 C1sco_5d:42:98 578 43.4176990 C1sco_5d:42:98 378 41 24300 C1sco_5d:42:98 578 43.4176990 C1sco_5d:42:98 38 51 251 bytes on wirre (17 578 53.211 bytes on wirre (17	Destination Protocol LLOP_MUIT(ast LLOP LLOP_MUIT(ast LLOP LLOP	Length Info 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 <th1< th=""> 1 <th1< th=""> 1 <th1< th=""> <th1< <="" th=""></th1<></th1<></th1<></th1<>					

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

File	Edit View	<u>Go Capture Analyze Sta</u>	atistics Telephony Tool	ls Internals Help						
EX #			Q, 🗢 💩 🐺			1 🖬 🗹 🍕 🔆 🙀				
-			1 ~ ~ ~ ~ T							
Filter:	lldp			 Expression 	Clear Apply					
	Time	Source	Destination	Protocol Le	ngth Info					
568	63.4176990	cisco_5d:42:98	LLDP_Multicast	LLDP	545 chass	is Id = c0:62:6b:5d:42:80				
		Cisco_5d:42:98	LLDP_Multicast	LLDP		is Id = c0:62:6b:5d:42:80 Port Id = Fa1/0/22 TTL = 120 System Name = yealink-cisco				
			LLDP_Multicast	LLDP		is Id = 10.10.222.19 Port Id = 00:15:65:41:46:dd TTL = 180 System Name = SIP-T465				
1125	123.380655	cisco_5d:42:98	LLDP_Multicast	LLDP	545 Chass	is Id = c0:62:6b:5d:42:80 Port Id = Fa1/0/22 TTL = 120 System Name = yealink-cisco				
۹						т — — — — — — — — — — — — — — — — — — —				
🗄 Li	nk Layer D	iscovery Protocol								
		btype = MAC address		42:80						
		pe = Interface name	, Id: Fa1/0/22							
		ve = 120 sec								
		e = yealink-cisco37								
				ware, C3750 Sof	tware (C3	750-IPSERVICESK9-M), Version 12.2(55)SE6, RELEASE SOFTWARE (fc1)\nTechnical Suppor				
	Capabiliti	iption = FastEthern	et1/0/22							
	Management									
	Management									
		a Capabilities								
		ntory - Hardware Re	vision							
		ntory - Software Re								
		ntory - Manufacture								
	TIA - Inve	ntory - Model Name								
	TIA - NEtwork Policy									
	1111 111 = TLV Type: organization specific (127)									
	00000 1000 = TLV Length: 8									
	organization Unique Code: TIA (0x0012bb)									
I	Media Subtype: Network Policy (0x02)									
1		ion Type: voice (1)								
1		= Polic								
1		1 1011 110 - VI AN								
			0 0001 1011 110. = VLAN IG: 222 1 01 = L2 Priority: 5							
			iority: 5							

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

File	Ele Edit View Go Capture Analyze Statistics Telephony Iools Internais Help							
			3 🗛 Q, 🗢 🔿 🙀					
Filte	r: Ildp			Expression	on Clear Apply			
No.	Time	Source	Destination	Protocol	Length Info			
	336 38.1 359 39.1 372 40.1 568 63.2 798 93.4 845 97.2 ame 845 chernet ink Laye Chassis Port Su Time TS System Capabil Port De IEEE 80 TIA - N TIA - N 1111 Orgam Media Appli 0 	II, Src: XiamenYe er Discovery Proto S Subtype = Networ ubtype = MAC addre O tive = 180 sec Name = SP-TS8 Description = S8.1 lities escription = WAN F 02.3 - MAC/PHY Cor wedia capability uttor capability 111	2:98 LLDP_Multi 2:98 LLDP_Multi 2:98 LLDP_Multi 2:98 LLDP_Multi 2:98 LLDP_Multi 2:98 LLDP_Multi 4:46:dd (DO:15:65 col k address 50 50 00RT figuration/Status TLV Type: organizat TLV Type: organizat	Cast LLDP Cast LLDP Cast LLDP Cast LLDP Cast LLDP Cast LLDP bytes captured :41:46:dd), Dst:	: LLDP_Multicast (01:80:c2:00:00:0e)			

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 T58A Teams phone 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, turn on the CDP feature.
- 4. Enter the desired time (in seconds) in the Packet Interval (1~3600s) field.

Yealink	T58			
Status	~	LLDP		
Network	^	Active		0
		Packet Interval (1~3600s)	60	0
PC Port		CDP 🔞		
Advanced		Active		0
Features	Ÿ	Packet Interval (1-3600s)	60	0
Settings	~	VLAN 🔞		
🥑 Security	Ť	WAN Port		
		Active	OFF	0
		VID (1-4094)		0
		Priority	0	- 0

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:

Permitted Values	Default
0 or 1	0

Parameters	Permitted Values	Default				
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_Teams_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).

Image: Second	
Filter: Cdp Expression. Clear Apply No. Time Source Destination Protocol Length Info 1052 102.431507 xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 116 Device ID: 74600156541460D Port ID: FastEthernet1/0/22 1105 103.39513 xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 74600156541460D Port ID: FastEthernet1/0/22 1105 113.39333 xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 74600156541460D Port ID: FastEthernet1/0/22 1105 113.39642 Xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 74600156541460D Port ID: WAN PORT 1109 113.306462 Xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 74600156541460D Port ID: WAN PORT 1210 102.007400 Xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 7460135641460D Port ID: WAN PORT 1210 102.00740 Xitamerve_412.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 7460135641460D Port ID: WAN PORT 1210 1212.0174.01769 Xitamerve_411.461d CCP/VTP/07P/PAgP/U0CCP 124 Device ID: 7460135641460D Port ID: WAN PORT 1210 121.40700 Xitamerve_411.461d CCP/VTP/07P/PAgP/U0CCP	
No. Time Source Destination Protocol Length Info 1052 102.41507 Xiamertve_41:46:40 CDP//TP/D7P/PAgP/UDCOP 116 Device 1D: 74600156541460D Port ID: WAN PORT 1059 103.39514 (sics_o.514:298 CDP//TP/D7P/PAgP/UDCOP 120 Device 1D: 74600156541460D Port ID: FastEthernet1/0/22 1189 119.39623 Xiamerve_41:46:40 CDP//TP/D7P/PAgP/UDCOP 124 Device 1D: 74600156541460D Port ID: WAN PORT 1199 119.39632 Xiamerve_41:46:40 CDP//TP/D7P/PAgP/UDCOP 124 Device 1D: 74600156541460D Port ID: FastEthernet1/0/22 1210 120.407696 Xiamerve_41:46:40 CDP//TP/D7PP/PAgP/UDCOP 124 Device 1D: 74601165541460D Port ID: FastEthernet1/0/22 1210 120.407696 Xiamerve_41:46:40 CDP//TP/D7PP/PAgP/UDCOP 110 Device 1D: 7460115541460D Port ID: FastEthernet1/0/22 1210 120.407696 Xiamerve_41:46:40 CDP//TP/D7PP/PAgP/UDCOP 120 Device 1D: 746011554160D Port ID: FastEthernet1/0/22 1210 121.60700 Xiamerve_41:46:40 CDP//TP/D7PP/PAgP/UDCOP 110 Device 1D: 74601155416D Port ID: FastEthernet1/0/22 1216 124.0248 Cisco_5dif2:38 CDP//TP/D7PP/PAgP/UDCOP	
1052 102,401507 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 116 Device ID: Y4601055414600 Port ID: WAN PORT 1059 103,39514 (Sico_S14:298 CDP/VTP/DTP/PAgP/UDCOP 137 Device ID: Y480116 Com Port ID: FastEthernet1/0/22 1185 118,39333 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1198 119,30663 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1199 119,306462 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1199 119,306462 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: FastEthernet1/0/22 1201 120,407696 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1210 121,007696 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1201 120,007696 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1210 120,007500 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1216 121,007500 Xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 124 Device ID: Y480155414600 Port ID: WAN PORT 1216 121,414:18 L914454 on wire (992 bit5), 124 by	
105103.3956142(5sco_5d:42:98 CDP/VTP/DTP/PAgP/UCCDP 517 Device 1D: yealink-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1185118.39563243tamerve_41:46:dd CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye400155511460D Port ID: WAN PORT 1198119.396632(sico_3d:42:98 CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye400155511460D Port ID: WAN PORT 1298119.396632(sico_3d:42:98 CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye400155511460D Port ID: WAN PORT 120120.4074695xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye4011Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1210120.4074695xiamerve_41:46:dd CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye4011Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1225121.41342(sisco_cdk-42:98 CDP/VTP/DTP/PAgP/UCCDP 124 Device 1D: Ye401Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1718181.419248(sisco_sdk-42:98 CDP/VTP/DTP/PAgP/UCCDP 116 Device 1D: Ye401Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1718181.419248(sisco_sdk-42:98 CDP/VTP/DTP/PAgP/UCCDP 116 Device 1D: Ye401Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1718181.419248(sisco_sdk-42:98 CDP/VTP/DTP/PAgP/UCCDP 116 Device 1D: Ye401Kk-cisco3750.yealink.com Port ID: FastEthernet1/0/22 1718181.419248(sisco_sdk-41:4:98 CDP/VTP/DTP/PAgP/UCCDP 116 Device 1D: Ye401Kk-cisco3750.yealink.com 1718181.4192	
1185 1185 <th< td=""><td></td></th<>	
1198 110.396632 xitamerve_41:46:dd CDP/VTP/07P/PAgP/UBCDP 124 Device 1D: YeaDING-55414600 Port ID: WAN PORT 1201 120.407495 xitamerve_41:46:dd CDP/VTP/07P/PAgP/UBCDP 127 Device 1D: YeaDING-553030_VERITK_com Port ID: FastEthernet1/0/22 1212 121.41323 cisco_5414600 Port ID: WAN PORT 124 Device 1D: YeaDING-553030_VERITK_com Port ID: FastEthernet1/0/22 1221 121.41323 cisco_5414238 CDP/VTP/07P/PAgP/UBCDP 124 Device 1D: YeaDINK-cisco3730_VERITK_com Port ID: FastEthernet1/0/22 1716 181.41324 cisco_5614460 CDP/VTP/07P/PAgP/UBCDP 116 Device 1D: YeaDINK-cisco3730_VERITK_com Port ID: FastEthernet1/0/22 r r r m m r r r r m 124 Device 1D: YeaDINK-cisco3730_VERITK_com Port ID: FastEthernet1/0/22 m m r r r m m r r r r r r r r r m r r r r r r r r r r r r r	
1199 113.409482 c15co_35142198 CDP/VTP/DTP/PAgP/U0COP 517 Device 1D: yeal1nk.ccfsco3750.yeal1nk.com Port 1D: sastethernet1/0/22 1210 120.007096 xiamerw_e1.416.61d COP/VTP/DTP/PAgP/U0COP 124 Device 1D: yeal00565146000 port 1D: waw PORT 1201 121.00700 xiamerw_e1.416.61d COP/VTP/DTP/PAgP/U0COP 517 Device 1D: yeal1nk.ccfsco3750.yeal1nk.com Port 1D: fastEthernet1/0/22 1706 181.067700 xiamerw_e1.416.61d COP/VTP/DTP/PAgP/U0COP 517 Device 1D: yeal1nk.c1sco3750.yeal1nk.com Port 1D: fastEthernet1/0/22 1716 181.64.19248 c1sco_5d:42:98 COP/VTP/DTP/PAgP/U0COP 517 Device 1D: yeal1nk.c1sco3750.yeal1nk.com Port 1D: FastEthernet1/0/22 171 Faste 1198: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) 126 Device 1D: yeal1nk.c1sco3750.yeal1nk.com Port 1D: FastEthernet1/0/22 18 Legical-Link COP/VTP/DTP/PAgP/U0COP 517 Device 1D: yeal1nk.c1sco3750.yeal1nk.com Port 1D: FastEthernet1/0/22 19 Faske 1198: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) 110 Device 1D: yeal1nk.c1sco3750.yeal1nk.com Port 1D: FastEthernet1/0/22 10 Ecse 0nds 2 Logical-Link Ecse 0nds 110 Port 1D: FastEthernet1/0/22 11 Ecse 0nds 2 Logical-Link 120 bytes 0nds 1100 bytes 0nds 110 bytes 0nds	
1210 120.407695 xitamerve_41:46:dd CDP/VTP/07P/Aps/U0CDP 124 Device ID: 1460015551460D Port ID: WAN PORT 1225 121:4132:c15c0_514:42:98 CDP/VTP/07P/Aps/U0CDP 517 Device ID: yealink-c155730.yealink.com Port ID: FastEthernet1/0/22 1706 181.067700 xitamerve_41:46:dd CDP/VTP/07P/Aps/U0CDP 517 Device ID: yealink-c155730.yealink.com Port ID: FastEthernet1/0/22 1716 181.419248 c1sco_5d:42:98 CDP/VTP/07P/Aps/U0CDP 517 Device ID: yealink-c15co3750.yealink.com Port ID: FastEthernet1/0/22 17 IS181.419248 c1sco_5d:42:98 CDP/VTP/07P/Aps/U0CDP 517 Device ID: yealink-c1sco3750.yealink.com Port ID: FastEthernet1/0/22 17 IS181.419248 c1sco_5d:42:98 CDP/VTP/07P/Aps/U0CDP 517 Device ID: yealink-c1sco3750.yealink.com Port ID: FastEthernet1/0/22 18 Logical-Link control IE III IIII IIII IIIIIIIIIIIIIIIIIIIIIIIIIII	
1225 121.41432c fisco_3di:42:98 CDP/VTP/DTP/PAgP/UDCOP 517 Device 1D: yealink.cdm Port 1D: FastEthernet1/0/22 1706 181.067700 xiamew_e.1146:dc (CDP/VTP/DTP/PAgP/UDCOP 517 Device 1D: yealink.cdm Port 1D: FastEthernet1/0/22 1716 1581.419248 Cisco_3di:42:98 CDP/VTP/DTP/PAgP/UDCOP 517 Device 1D: yealink.cdm Port 1D: FastEthernet1/0/22 10 Frame 1108: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) 125 Device 1D: yealink.cdm Port 1D: FastEthernet1/0/22 11 Frame 1108: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) 10 2 Cisco Discovery Protocol version: 2 TT: 130 seconds 10 ID Device 1D: 14600155414600 10	
1706 181.067700 x1mmemve_41:46:dd CDP/VTP/DTP/PAgP/UDCOP 116 Device ID: 14600156541460D Port ID: WAN PORT 1716 181.419248 C1sco_5d:42:98 CDP/VTP/DTP/PAgP/UDCOP 517 Device ID: yealink-c1sco3750.yealink.com Port ID: FastEthernet1/0/22 0 Frame 1108: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) 18 IEEE 802.3 Ethernet 10 Gisco Discovery Protocol Version: 2 TT: 130 seconds 10 Device ID: yealink.com Port ID: FastEthernet1/0/22 116 Device ID: yealink.com Port ID: FastEthernet1/0/22 117 L: 180 seconds 118 Device ID: yealink.com Port ID: FastEthernet1/0/22 119 Device ID: yealink.com Port ID: FastEthernet1/0/22 110 Device ID: yealink.com Port ID: FastEthernet1/0/22 111 Device ID: yealink.com Port ID: FastEthernet1/0/22 112 Device ID: yealink.com Port ID: FastEthernet1/0/22 113 Device ID: yealink.com Port ID: FastEthernet1/0/22 114 Device ID: yealink.com Port ID: FastEthernet1/0/22 115 Device ID: yealink.com Port ID: FastEthernet1/0/22 115 Device ID: yealink.com Port ID: FastEthernet1/0/22 116 Device ID: yealink.com Port ID: FastEthernet1/0/22 117 Device ID: yealink.com Port ID: FastEthernet1/0/22 118 Device ID: yealink.com Port ID: FastEthernet1/0/22 119 Device	
1716 181.419248 c1sco_5d:42:98 CDP/VTP/DTP/PAGP/UDCOP 517 Device ID: yealink-c1sco3730.yealink.com Port ID: FastEthernet1/0/22 (
p reams 11082 124 bytes on wire (992 bits), 124 bytes captured (992 bits) = IEEE 0023 pitch-tink thermet = clisco biscowery protocol version: 2 TTL: 180 seconds = Checksum: 0xc241 [correct] = Device D: r4600156514600	
IEEE 802.3 Ethernet IEEE 802.3 Ethernet Iogical-ink Control Iogical-ink Control Control Control Version: 2 Tri.: 180 seconds E checksum: 0xc241 [correct] Bevice I: 746001565414600	•
IEEE 802.3 Ethernet IeEE 802.3 Ethernet Iogical-ink Control Contro Control Control Control Control Control C	_
Cisco Discovery Protocol Version: 2 TTL: 180 seconds Encksum: 0xc241 [correct] Device ID: 746001555414600	
Version: 2 TTL: 180 seconds @ Checksum: 0xc241 [correct] D bevice [0: T460015554146DD	
TTL: 180 seconds □ checksum: 0xc41 [correct] □ bevice 10: 746001565414600	
⊞ Checksum: 0xc241 [correct] B Device ID: T4600156541460D	
B Device ID: T460015654146DD	
T Addresses	
B PORT ID: WAN PORT	
⊞ Capabilities	
🗄 Software Version	
H Platform: T46	
⊞ Duplex: Half ■ Power Consumption: 8000 mW	
W VOIP VLAN QUERY 512	
Type: VIP VLAN Query (0x000f)	
Length: 8	
Data	
Voice VLAN: 512	

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

File Edit View Go Capture Analyze Statistics Telephony Tools Interr	nals Help
■ ■ ■ ● ● ● 7 ±	
Filter: cdp 💌 Ex	pression Clear Apply
No. Time Source Destination Pr	rotocol Length Info
1052 102.491507 xiamenYe_41:46:dd CDP/VTP/DTP/PAqP/UDC	DP 116 Device ID: T460015654146DD Port ID: WAN PORT
1059 103.395614 Cisco_5d:42:98 CDP/VTP/DTP/PAgP/UDC	
1185 118.399333 xiamenye_41:46:dd CDP/VTP/DTP/PAgP/UDC	
1198 119. 396632 xiamenYe_41:46:dd CDP/VTP/DTP/PAgP/UDC	
1199 119.409462 Cisco_5d:42:98 CDP/VTP/DTP/PAgP/UDC	
1210 120.407969 x1amenye_41:46:dd CDP/VIP/DIP/PAQP/UDC	
	m
Cisco Discovery Protocol	
version: 2	
TTL: 180 seconds	
E Checksum: 0x3706 [correct]	
Device ID: yealink-cisco3750.yealink.com	
Software Version Platform: cisco WS-C3750V2-24TS	
Addresses	
Port ID: FastEthernet1/0/22	
Capabilities	
Protocol Hello: Cluster Management	
VTP Management Domain: vealink	
R Native VLAN: 5	
Duplex: Half	
□ VOIP VLAN Reply: 222	
Type: VoIP VLAN Reply (0x000e)	
Length: 7	
Data	
Voice VLAN: 222	
Trust Bitmap: 0x00	
Untrusted port CoS: 0x00	
Management Addresses	
■ Location: \003\002	
Dowor Available: 0 mW 4204067205 mW	

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

Eile Edit View Go Capture Analyze Stati	stics Telephony Iools Internals Help	
	़ ♦ ♦ 🕹 🖗 🕹 । 🗐 🕞 । Ө. ९. ९. 🕾 । 😹 🗵 🥵 % । 🐹	
Filter: cdp	Expression Clear Apply	
No. Time Source	Destination Protocol Length Info	
1052 102.491507 XTamenye_41:40:00 1059 103.395614 Cisco_5d:42:98	CDP/VTP/DTP/PAGP/DUCDP IIO DEVICE ID: 1400013034140DD POTL ID: WAN PORT 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	CDP/YTP/DTP/PAQP/UDCDP 517 Device ID: yealink-cisco3750.yealink.com Port ID: FastEthernet1/0/22	
1210 120.407969 xiamenYe_41:46:dd		
1225 121.414332 cisco_5d:42:98	CDP/VTP/DTP/PAgP/UDCDP 517 Device ID: yealink-cisco3750.yealink.com Port ID: FastEthernet1/0/22	
1706 181.067700 xiamenYe_41:46:dd	CDP/VTP/DTP/PAgP/UDCDP 116 Device ID: T460015654146DD Port ID: WAN PORT	
<	m	E F
Ename 1706: 116 bytes on wire (92	28 bits), 116 bytes captured (928 bits)	
IEEE 802.3 Ethernet		
E Logical-Link Control		
Cisco Discovery Protocol		
Version: 2		
TTL: 180 seconds		
Gecksum: 0xfa3d [correct]		
Device ID: T460015654146DD		
Addresses		
Type: Addresses (0x0002)		
Length: 17 Number of addresses: 1		
IP address: 10.10.222.19		
# Port TD: WAN PORT		
Capabilities		
Software version		
Platform: T46		
⊞ Duplex: Half		
Power Consumption: 8000 mW		

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 localhos	t (modified)			_		X
<u>File Edit View Bindings To</u>	ols <u>H</u> elp					
🛛 🖪 🛛 🖌 🐚		*	୦ 🖉	∖ ?		
Servers /	Filter	Standard Opt	ions		_	
🗄 🛃 Scopes	Tag ∇		Option			
≝Option Types Æ Ne ⊕-∭Named Polici 		e Ctrl+V Ctrl+Z	SMTP serves POP3 serves NNTP serves	s		
🕘 Database 🔿 Re		Ctrl+Y	WWW server			
🧚 Cu	t	Ctrl+X	- Finger ser IRC server			
🕨 <u>C</u> o	ру	Ctrl+C	Streettalk			
💼 <u>P</u> a	ste	Ctrl+V	Streettalk User class	DA servers	s	
De	elete	Del	Device FQD	r		
Se	lect <u>A</u> ll	Ctrl+A	Relay Agen		i on	
🥂 <u>F</u> in	nd	Ctrl+F	Subnet Sel SIP Server	ction		
	operties	Ctrl+P	Cablelabs			-
Create a new option type	Descript	ion	Yealink Ph	ne lest vi	AN 10	 -

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.

Option Properties	X
Tag 132 🚖	
Name Yealink Phone Test VLAN ID	
Type string 💌	
🗌 Signed 🔲 Arrayed	
Description	
<u>OK</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.

🖪 🔰 🕺	•		1 🛠	0	0	<u></u>	k ?	
					-	3		
rvers /		Tag 🗸			Name		Value	
· 💷 localhost ⊨- 🛃 Scopes								
- Docopes Option Typ	45							
E. Named Poli								
Glabal								
	New Option	Ctrl+\	/					
👘 🍎 Datat 🖍 📋	<u>J</u> ndo	Ctrl+2						
CH 🛛	Redo	Ctrl+	()					
1 0	Cut	Ctrl+)	c					
	Сору	Ctrl+(:					
aller -	Paste	Ctrl+\	/					
	_ elete	Del						
	- Select <u>A</u> ll	Ctrl+/						
	Eind	Ctrl+F	:					
	 Properties	Ctrl+F	,					

The Option Selector screen displays as below:

🖅 Option Sele	ctor		×
Filter	Standard Options	T	
Tag ∇	Name		_
	Magic cookie		
	Home directory		
	Boot file		
	Subnet mask		
	Time offset		
	Gateways		
⁄ 🖅 4	Time servers		
	IEN116 name servers		
	Domain name servers		
🖅 7	Log servers		
	Cookie/Quote servers		
	LPR servers		
/ 🖅 10	Impress servers		
🖅 11	RLP servers		
🖅 12	Hostname		
/ 🖅 13	Boot file size		
/ 🖅 14	Merit dump file		
/ 🖅 15	Domain name		
/ 🖅 16	Swap servers		
/ 🖅 17	Root path		
🖅 18	Extensions path		
/ 🖅 19	IP forwarding		•
Description.			
Description			<u> I</u>
1			
		<u> </u>	Cancel
		<u></u>	241111

- **10.** Scroll down and double click the option created above.
- $\label{eq:linear} \textbf{11.} \ \textbf{Fill the VLAN ID to be assigned in the input field.}$

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

/ Yealink P	hone Test VLAN II	D <u>×</u>
111		
☐ Expre	ssion	Build
<u>0</u> K	Cancel	\underline{A} dvanced $>>$

- 12. Click OK to finish setting a custom option.
- **13.** Click *a* to 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		
🛛 🖪 🛛 🗮 🏷 🐚	🛋 🔀 🛠	♥ ♥ §	
Servers 🛆	Tag ∇	Name	Value
Docalhost	₽	Yealink Phone Test VLAN ID	111
Download complete	-		

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 T58A Teams phone 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, turn on the DHCP VLAN feature.
- 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.

Yealink 158						Ab	Put
		n	60	0			
Network ·		IAN Port					
		Active	OFF	0			
PC Port		VID (1-4094)		0			
Advanced Features		Priority	0 -	0			
	P	C Port					
		Active	1941	0			
	<i>.</i>	VID (1-4094)		0			
		Priority	0 *	0			
	C	HCP VLAN					
		Active		0			
		Option (1-255)	132	0			

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:

Permitted Values	Default							
0 or 1	1							
Description:								
Enables or disables DHCP VLAN discovery feature on the phone.								
0-Disabled								
Integer from 128 to 254	132							
Description:								
AN ID.								
options by commas.								
	0 or 1 ure on the phone. Integer from 128 to 254 AN ID.							

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_Teams_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):

File I	Edit View Go	Capture Analyze St	itistics Telephony <u>T</u> ools Int	ernals Help							
			Q, 🗢 🚸 💫 🐺 👱		0 1	a 🕅 🖪					
					•••=		9 9 W 1 828				
Filter:	bootp		-	Expression Clear	Apply						
No.	Time	Source	Destination	Protocol Len	gth Info						
	3 0.110993		255.255.255.255				- Transacti				
	4 0.115183		5.5.5.18		342 DHCP C		- Transacti				
	5 0.150004 6 0.154213		255.255.255.255		342 DHCP R 342 DHCP A		- Transacti				
	7 0.200977		255, 255, 255, 255				- Transactio				
	8 0.205328		5.5.5.18		342 DHCP A		- Transacti				
	9 10.068604		255, 255, 255, 255				- Transacti				
	10 10.074079	10.10.111.254	10.10.111.2	DHCP	346 DHCP C	offer	- Transacti	on ID 0xc	18e620		
	11 10.161676		255.255.255.255	DHCP	594 DHCP P	Request	- Transacti	on ID Oxc	18e620		
	12 10.163676	10.10.111.254	10.10.111.2	DHCP	346 DHCP A	ACK	- Transacti	on ID 0xc	18e620		
<											
Int Use	Type: IP (0x0 ternet Protoc	col Version 4, Sr Protocol, Src Por	:15:65:11:27:b1) c: 0.0.0.0 (0.0.0.0), c t: bootpc (68), Dst Por			5.255.25	5.255)				
N H H S	Message type: Hardware type Hardware addr Hops: 0 Transaction 1 Seconds elaps	: Boot Request (1 e: Ethernet ress length: 6 ID: 0x83952d00 sed: 100	Click here to know mon	e information.							
	<u>Client IP add</u> Your (client) Next server I Relay agent I Client MAC ad		.0.0 (0.0.0.0)								
0020 0030 0040	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., de.'							

	©4 @4 @4		atistics Telephony <u>T</u> ools J 🔍 🗢 🐟 🥸 🚰 👱		, •	1 8 % 🛱			
Filter:	pootp		-	Expression.	Clear Apply				
No.	Time	Source	Destination	Protocol	Length Info				
	0.115183		5.5.5.18	DHCP		- Transaction 1			
		0.0.0.0	255.255.255.255	DHCP		- Transaction 1			
	0.154213		5.5.5.18	DHCP	342 DHCP ACK	- Transaction I			
	0.200977		255.255.255.255	DHCP	342 DHCP Request	- Transaction 1 - Transaction 1			
	10.068604		5.5.5.18 255.255.255	DHCP		 Transaction 1 r - Transaction 1 			
		10.10.111.254	10.10.111.2	DHCP	346 DHCP Offer	 Transaction 1 Transaction 1 			
	10.161676		255, 255, 255, 255	DHCP		- Transaction 1			
		10.10.111.254	10.10.111.2	DHCP	346 DHCP ACK	- Transaction I			
Hops: 0 Transaction ID: 0x83952d00 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) Next server IP address: 0.0.0.0 (0.0.0.0) Client MAC address: xiamenve_11:27:b1 (00:15:65:11:27:b1) Client MAC address: xiamenve_10000000000000000 Server host name not given Boot file name not given Boot fi									
	Padding Padding 00 ff ff ff ff ff f0 0 15 65 11 27 b1 08 00 45 00e.'E.								

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

<u>F</u> ile <u>E</u>	<u>Edit V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statis</u>	tics Telephon <u>y T</u> ools <u>I</u> nt	ternals <u>H</u> elp						
		⊨ 🛃 🗶 😂 🔺	् 🗢 🛸 🤪 春 👱		ପ୍ର୍ଷ୍ 🗹	🏼 🖉 🖁	§ % 😫			
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	Request	- Transaction	ID 0xbdaa1562		
	6 0.154213		5.5.5.18	DHCP	342 DHCP		- Transaction			
	7 0.200977		255.255.255.255	DHCP			- Transaction			
	8 0.205328		5.5.5.18	DHCP	342 DHCP		- Transaction			
	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		
۰					m					
	Next server IP address: 5.5.12 (5.5.2) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: xiamenve_li27:bl (00:15:65:11:27:bl) Client hardware address: padding: 00000000000000000 Server host name: mid0507-dc23398 Boot file name not given MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP MagTic cookie: DHCP <									
		2,1=1) Unassigned	ined (vendor specifi	0						
. € C	© Option: (t=125,1=5) DOCSIS full security server IP [TODD] © Option: (t=54,1=4) DHCP Server Identifier = 5.5.5.2 End Option Padding									
0120 0130	ff ff 00 33 04 00 00 2a	00 00 63 82 53 6 04 00 00 54 60 3 30 03 04 05 05 0	3 35 01 02 01 04 ff 0 04 00 00 49 d4 3a 5 01 84 03 31 31 31 4 36 04 05 05 05 02		Şc5					

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

<u>File Edit V</u> iew <u>G</u> o	Capture Analyze Statis	tics Telephon <u>y T</u> ools <u>I</u>	nternals <u>H</u> elp						
	🕒 🖬 🗶 🈂 🔒	् 🗢 🔿 🐼 🕹		QQ 🕅	🏼 🗹 🍕	» 🖗 🛛 🔀			
Filter: bootp		-	Expression	Clear Apply					
No. Time	Source	Destination	Protocol	Length Info					_
	0.0.0.0	255, 255, 255, 255	DHCP		Discover	- Transaction	TD 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		255.255.255.255	DHCP				ID 0x83952d00		
8 0.205328		5.5.5.18	DHCP	342 DHCP			ID 0x83952d00		
9 10.068604		255.255.255.255	DHCP				1D 0XC48e620		
	10.10.111.254	10.10.111.2	DHCP	346 DHCP			ID 0xc48e620		
11 10.161676		255.255.255.255	DHCP	346 DHCP			ID 0xc48e620		
12 10.1636/6	10.10.111.254	10.10.111.2	DHCP		ACK	- Transaction	1D 0XC48e620		
<				III					,
Client IP address: 0.0.0.0 (0.0.0.) Your (Client) IP address: 5.5.5.18 (5.5.5.18) Next Server IP address: 5.5.5.2 (5.5.2) Relay agent IP address: 5.5.5.2 (5.5.2) Client Mardware Address: Yallo (00:15:65:11:27:b1) Client hardware address: padding: 000000000000000000000000000000000000									

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	View Go	Capture Analyze Statist	ics Telenhony Tools In	ternals Help						
	<u></u>		_				1 42 1 19			
			~~~ <u>~</u> ~~~			<b>W</b> 🗆 0	9 70   28			
Filter: bo	ootp		-	Expression Cle	ear Apply					
No. 1	Time	Source	Destination	Protocol L	ength Info					
	0.110993		255.255.255.255	DHCP				on ID 0x83952d0		
	0.115183		5.5.5.18	DHCP	342 DHCP			on ID 0x83952d0		
	0.150004		255.255.255.255	DHCP				on ID Oxbdaa156		
	0.154213		5.5.5.18	DHCP	342 DHCP			on ID Oxbdaa156		
	0.200977		255.255.255.255	DHCP	342 DHCP			on ID 0x83952d0 on ID 0x83952d0		
	10.068604		255, 255, 255, 255	DHCP				on ID 0x8395200 on ID 0xc48e620		
		10.10.111.254	10.10.111.2	DHCP	346 DHCP			on ID 0xc48e620		
	10.161676		255.255.255.255	DHCP				on ID 0xc48e620		
		10.10.111.254	10.10.111.2	DHCP	346 DHCP			on ID 0xc48e620		
4										
o selecco		AN tagged), Src: Ci		. church an an	Date: vide		27.bt (00.45			
ULAN IC OC Type Interr	<pre>© Destination: XiamenYe_11:27:b1 (00:15:65:11:27:b1) © Source: (5:co_5:d4:2:c4 (co:62:65:65:d4:2:c4) U KAN tag: VLAN-11, Priority-Best Effort (default) Identifier: 802.10 vitrual LAN (00:80:00) 000 Priority: Best Effort (default) (0) 000 effic canonical (0) 0000 0110 1111 = VLAN: 111 Type: IP (UXUSOU) Thremet Protocol Version 4, Src: 10.10.111.254 (10.10.111.254), DSt: 10.10.111.2 (10.10.111.2)</pre>									
<pre>iliser batagram Protocol, src Port: bootps (67), Dst Port: bootpc (68) Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x0c45e620 seconds elapsed: 0 Bootp flags: 0x0000 (unicast) Client 1P address: 10.10.111.2 (10.10.111.2)</pre>										
0030 06	5 00 0c 48	e6 20 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 0a 0a 00 15 65 11 27 b1							

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. PC port is not applicable on CP960 Teams IP phones. The followings take configurations of a T58A Teams IP phone as examples.

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

#### To configure VLAN for Internet port via web user interface:

- 1. Click on Network->Advanced.
- 2. In the VLAN block, turn on WAN Port feature.
- 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   158					About
Status ~	LLDP				NOTE
work ^	Active		0		Network advance
	Packet Interval (1-3600s)	60	0		O Click here to get more product doe
ort	CDP 🕜				
iced	Active		0		
tures 🗸	Packet Interval (1-3600s)	60	0		
gs ~	VLAN 🕜				
anty ∼	WAN Port				
	Active		0		
	V1D (1-4294)	1	0		
	Priority	0	· 0		

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.

Yealink   T58					Abou	t Language <del>v</del>	
Status ×	LLDP						
Network ^	Active		0		NOTE Network advance		
Basic	Packet Interval (1-3600s)	60	0		<ul> <li>Click here to get more product of</li> </ul>	locuments.	
PC Port	CDP 🔞	00	•				
Advanced	Active		0				
🙂 Features 🛛 🗸	Packet Interval (1~3600s)	60	0				
Settings ~	VLAN	00	•				
🥏 Security 🗸 🗸	WAN Port						
	Active		0				
	VID (1-4294)	1	0				
	Priority						
	PC Port						
	Active		0				
	VID (1-4094)	1	0				
	Priority	· 0 *					
	e invity.	• •	•				

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:

- Tap ->Settings->Device Settings->Network(default password: admin)->VLAN->WAN Port (or PC Port).
- 2. Turn on WAN Port (or PC Port).

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

3. Tap CANCEL.

- 4. Enter the VLAN ID (1-4094) in the VID field.
- 5. Enter the priority value (0-7) in the **Priority** field.
- **6.** Tap  $\checkmark$  to accept the change.

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

7. Tap **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	packets sent from the Inte	rnet						
(WAN) port.								
0-Disabled								
1-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	port.						
Note: It is not applicable on CP960 Teams IP ph	ones.							
0-Disabled								
1-Enabled								
static.network.vlan.pc_port_vid	Integer from 1 to 4094	1						

Parameters	Permitted Values	Default					
Description:							
Configures the VLAN ID that associates with the particular VLAN.							
Note: It is not applicable on CP960 Teams IP phones.							
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

**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_Teams_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	Edit y	jew <u>G</u> o	o <u>⊂</u> apture <u>A</u> nalyze	Statistics Telephony	Tools Help	lp
	<b>u</b> 0	1	🕷   🗁 🗔 🎗	। 🔁 占   🔍 🐳	🧼 🍛	) 🛜 👱   🗐 🗐   Q. Q. Q. 🔟   👪 🗹 畅 %   💢
Filter	sip					▼ Expression Clear Apply
No.	Time		Source	Destination	Protocol	
	2.44		10.2.11.216	10.2.1.199		DPRequest: INVITE sip:201@10.2.1.199, with session description
	2.45		10.2.1.199	10.2.11.216	SIP	Status: 100 Trying
	2.45		10.2.1.199	10.2.8.216		DPRequest: INVITE sip:201@10.2.8.216:5062, with session description
	2.48		10.2.8.216	10.2.1.199	SIP	Status: 100 Trying
	3.64		10.2.8.216	10.2.1.199		Status: 180 Ringing
	3.65		10.2.1.199	10.2.11.216	SIP	Status: 180 Ringing
	04.41		10.2.8.216	10.2.1.199		DP Status: 200 OK, with session description
	4.41		10.2.1.199	10.2.11.216		DPStatus: 200 OK, with session description
	4.49		10.2.11.216	10.2.8.216	SIP	Request: ACK sip:201010.2.8.216:5062
2:	4.49	6749	10.2.11.216	10.2.8.216	SIP	Request: ACK sip:201@10.2.8.216:5062
4						
						es captured (7264 bits)
						22:f9), Dst: Cisco_40:da:55 (6c:50:4d:40:da:55)
E 80				3, CFI: 0, ID: 77		
				iority: Excellen		t (3)
				I: Canonical (0)		
			$0100 \ 1101 = II$	D: 77		
			0×0800)		aa	
						, Dst: 10.2.1.199 (10.2.1.199)
			m Protocol, Sr iation Protoco		ise (sue	062), Dst Port: sip (5060)
1± 26	:55100	i init	Taction Protoct	1		

# 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**

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

Model	System Name
SIP-T58A	SIP-T58
SIP-T56A	SIP-T56A
SIP-T55A	SIP-T55A

Model	System Name
SIP-CP960	SIP-CP960
VP59	VP59
MP56	MP56

# **Appendix C: Model Names**

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

Model	Model Name
SIP-T58A	SIP-T58
SIP-T56A	SIP-T56A
SIP-T55A	SIP-T55A
SIP-CP960	SIP-CP960
VP59	VP59
MP56	Teams_MP56

# **Appendix D: Power Values**

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

Model	Power Value
SIP-T58A	11400mW
SIP-T56A	8800mW
SIP-T55A	7000mW
SIP-CP960	12000mW
VP59	12900mW
MP56	8100mW

# **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.