

Using 802.1x feature on Yealink T3XG Phones

Summary:

802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails.

For example , the employees set "802.1x Mode" to be "EAP-MD5 " , fill the correct username and password , then submit revised and restart, the devices can obtain the IP address ,and access the related resources ;Otherwise , the devices can't attach to a LAN.

The MD5 is Message-Digest Algorithm 5 .

Settings:

1.Web Interface:

1)Open the phone's web page ;

2)The client-side configuration via web management "Network -> Advanced", like below:

The screenshot displays the Yealink web management interface. The top navigation bar includes 'Status', 'Account', 'Network' (highlighted), 'DSS Key', 'Phone', 'Contacts', and 'Security'. The 'Network' section is expanded, showing 'Basic' and 'Advanced' sub-sections, with 'Advanced' selected. The '802.1x' configuration section is highlighted, showing the following settings:

- 802.1x Mode:** EAP-MD5 (selected)
- Identity:** aaa
- MDS Password:** ***

Other visible sections include:

- LLDP:** Active (Disabled), Packet Interval (120)
- VLAN:** Internet Port (Active, Disabled), VID (0), Priority (0); PC Port (Active, Disabled), VID (0), Priority (0)
- VPN:** Active (Disabled), Upload VPN Config (Browse...), Import
- Voice QoS:** Voice QoS (40), SIP QoS (40)
- Local RTP Port:** Maximum RTP Port (11800), Minimum RTP Port (11780)
- Web Server:** HTTP Port (80), HTTPS Port (443), Type (HTTP&HTTPS)
- Registration Random:** Registration Random (0)
- Use Static DNS:** Use Static DNS (Disabled)

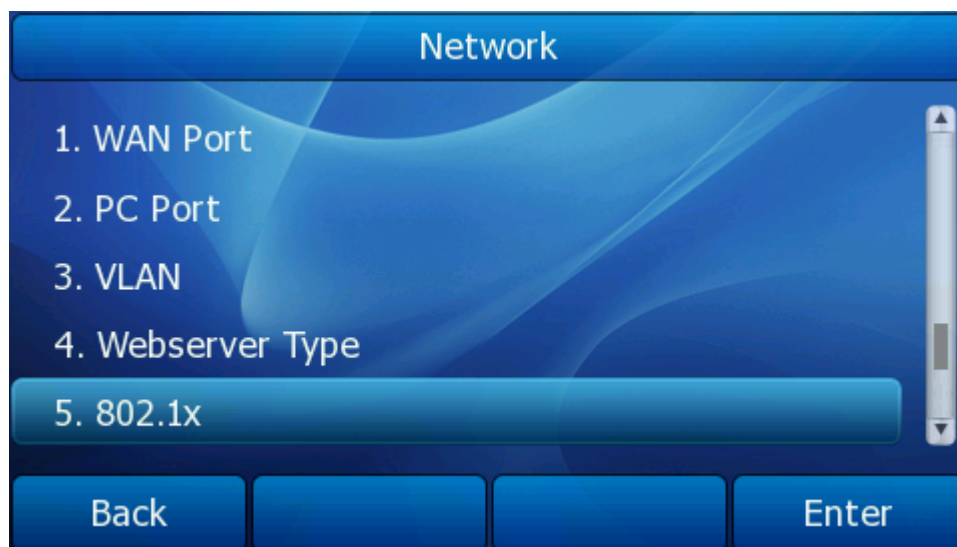
Buttons at the bottom include 'Confirm' and 'Cancel'. A 'NOTE' section on the right provides information about VLAN, QoS, and Local RTP Port.

3) Set "802.1x Mode" to be "EAP-MD5", fill in the correct Identity and MD5 password, click Confirm button ;

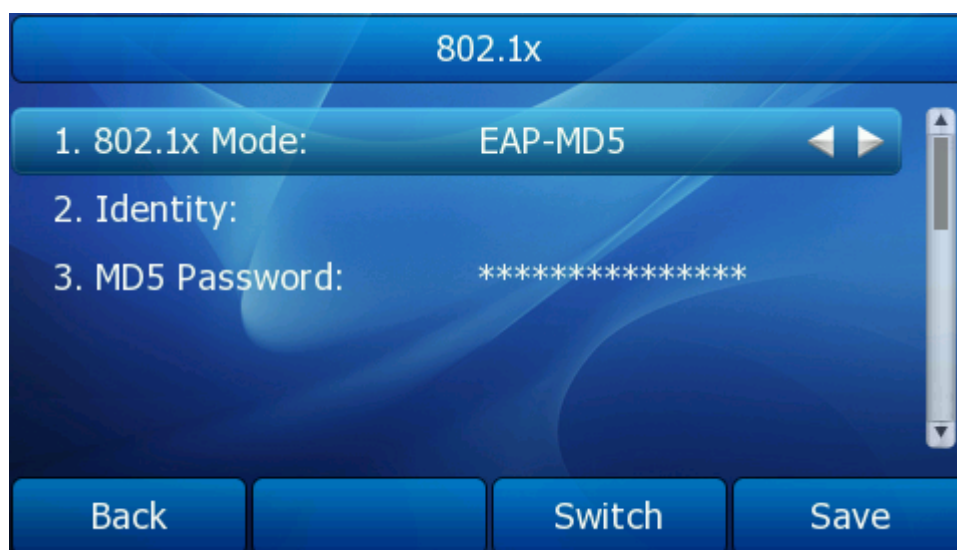
4) The phone's configuration go into effect and restart .

2. On GUI:

1) Go to the menu : Menu-> Setting->Advanced Settings->Network->802.1x Settings



2) Set "802.1x Mode" to be "EAP-MD5", fill in the correct Identity and MD5 password, press the "save" button ;



3) The phone's configuration go into effect and restart .

Basic use :

The yealink phones through the port authentication , phones can access the IP address and registered accounts, make calls .

Phones use the same operation as usual . Port configuration please consult the server vendors .

In the certification process ,we can use the "Wireshark" to get the trace .(Please filter : eap | | eapol)

1) Use common server .If the phone has been opened 802.1X mode , the phone will send the "Start " message to the server when the phone restart . The phone sends the message every three seconds, and sends for three times in all .You can refer the screenshot as below :

Filter: ▼ Expression... Clear Apply

No. ↓	Time	Source	Destination	Protocol	Info
364	50.432231	XiamenYe_12:08:ab	Nearest	EAPOL	Start
386	53.431800	XiamenYe_12:08:ab	Nearest	EAPOL	Start
435	56.431559	XiamenYe_12:08:ab	Nearest	EAPOL	Start

2) Used the server requires authentication . You can refer the screenshot as below :

No. ↓	Time	Source	Destination	Protocol	Info
95	12.335966	Vmware_41:5e:e0	Nearest	EAPOL	Logoff
96	12.337358	Vmware_41:5e:e0	Nearest	EAPOL	Logoff
97	12.338598	Vmware_41:5e:e0	Nearest	EAPOL	Logoff
98	12.374629	Cisco_1b:6b:8e	Nearest	EAP	Request, Identity [RFC3748]
100	12.383215	Cisco_1b:6b:8e	Nearest	EAP	Request, Identity [RFC3748]
101	12.397368	Cisco_1b:6b:8e	Nearest	EAP	Request, Identity [RFC3748]
103	14.346688	Vmware_41:5e:e0	Nearest	EAPOL	Logoff
104	14.365871	Cisco_1b:6b:8e	Nearest	EAP	Request, Identity [RFC3748]
105	14.369638	Vmware_41:5e:e0	Nearest	EAP	Response, Identity [RFC3748]
106	14.391183	Cisco_1b:6b:8e	Nearest	EAP	Request, MD5-Challenge [RFC3748]
107	14.392239	Vmware_41:5e:e0	Nearest	EAP	Response, MD5-Challenge [RFC3748]
122	15.449117	Cisco_1b:6b:8e	Nearest	EAP	Success

Frame 107 (64 bytes on wire, 64 bytes captured)

Ethernet II, Src: Vmware_41:5e:e0 (00:0c:29:41:5e:e0), Dst: Nearest (01:80:c2:00:00:03)

802.1X Authentication

Version: 2
 Type: EAP Packet (0)
 Length: 25
 Extensible Authentication Protocol

Code: Response (2)
 Id: 2
 Length: 25
 Type: MD5-Challenge [RFC3748] (4)
 Value-size: 16
 Value: E5A07EE0A1B46709B7056A698363194B
 Extra data (3 bytes): 616161

0000	01 80 c2 00 00 03 00 0c	29 41 5e e0 88 8e 02 00)A^.....
0010	00 19 02 02 00 19 04 10	e5 a0 7e e0 a1 b4 67 09 ~...g.
0020	b7 05 6a 69 83 63 19 4b	61 61 61 00 00 00 00 00	..j!.c.k aaa.....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Authentication successfully ,you can see the "Success" message on the " Wireshark " ; If username or password fill in error , you can see the "Failure" message on the " Wireshark " .