

# Yealink Technical White Paper

# **802.1X Authentification**

June. 2017

# **Table of Contents**

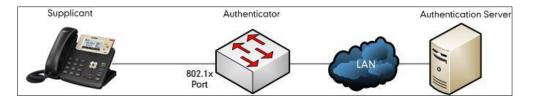
About 802.1X	3
Yealink IP Phones Compatible with 802.1X	3
Configuring 802.1X Settings	5
Configuring 802.1X Using Configuration Files	6
Configuring 802.1X via Web User Interface	12
Configuring 802.1X via Phone User Interface	17
802.1X Authentication Process	19
Sample Screenshots - Identity	21
Sample Screenshots - Anonymous Identity	
Troubleshooting	27
Why doesn't the IP phone pass 802.1X authentication?	27
Appendix A: Glossary	
Appendix B: 802.1X Authentication Process	
A Successful Authentication Using EAP-MD5 Protocol	
A Successful Authentication Using EAP-TLS Protocol	30
A Successful Authentication Using EAP-PEAP/MSCHAPv2 Protocol	
A Successful Authentication Using EAP-TTLS/EAP-MSCHAPv2 Protocol	
A Successful Authentication Using EAP-PEAP/GTC Protocol	34
A Successful Authentication Using EAP-TTLS/EAP-GTC Protocol	34
A Successful Authentication Using EAP-FAST Protocol	

# About 802.1X

The IEEE 802.1X standard defines a Port-based Network Access Control (PNAC) and authentication protocol that restricts unauthorized clients from connecting to a LAN. The IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) defined in RFC3748 which is known as "EAP over LAN" or EAPOL.

802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is a client device (such as an IP phone) that wishes to attach to the network. The authenticator is a network device, such as an Ethernet switch. And the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is like providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name, password or digital certificate for the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant is allowed to access resources located on the protected side of the network.



# Yealink IP Phones Compatible with 802.1X

802.1X is the most widely accepted form of port-based network access control in use and is available on Yealink IP phones. Yealink IP phones support 802.1X authentication based on EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST protocols.

Authentication Protocol	IP Phone Models	Firmware Version
EAP-MD5	All IP phones	All Versions
EAP-TLS	T46G, T42G, T41P, CP860	Firmware version 71 or later
EAP-ILS	T48G	Firmware version 72 or later

The table below lists the protocols supported by Yealink SIP IP phones with different versions.

Authentication Protocol	IP Phone Models	Firmware Version
	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	T46G,T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	T46G, T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
EAP-TTLS/EAP-MSCHAPv2	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-PEAP/GTC	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S,	Firmware version 81 or later

Authentication Protocol	entication Protocol IP Phone Models	
	T42S, T41S, T40G, T27G, W52P	
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-TTLS/EAP-GTC	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
EAP-FAST	T58V/A, T56A, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, T49G, T48G, T46G, T42G, T41P, T40P, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later

Yealink IP phones support 802.1X as a supplicant, both Pass-thru Mode and Pass-thru Mode with Proxy Logoff. When the device connected to the phone disconnects from the PC port, the Yealink IP phone can provide additional security by sending an EAPOL Logoff message to the Ethernet switch. This functionality, also known as proxy logoff, prevents another device from using the port without first authenticating via 802.1X. The Pass-thru Mode is available on Yealink IP phones running specified firmware version. You can ask your system administrator or contact Yealink Field Application Engineer (FAE) for more information.

# **Configuring 802.1X Settings**

The 802.1X authentication on Yealink IP phones is disabled by default. You can configure the 802.1X authentication in one of the following three ways:

- Configuring 802.1X Using Configuration Files
- Configuring 802.1X via Web User Interface
- Configuring 802.1X via Phone User Interface

For detailed descriptions of the authentication parameters in configuration files, you can refer to Configuring 802.1X Using Configuration Files on page 6. When setting up a large number of IP phones, Yealink recommends using the boot file (for new auto provisioning mechanism) and configuration files. If you are provisioning a few phones, you can use the web user interface or

phone user interface to configure 802.1X feature.

If the EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC or EAP-FAST protocol is preferred in your 802.1X environment, make sure that the firmware running on your new phone supports the protocol.

The followings provide system administrator with the procedures to successfully configure Yealink IP phones in a secure 802.1X environment.

## **Configuring 802.1X Using Configuration Files**

The following IP phones use the new auto provisioning mechanism:

- SIP-T58V/T58A/T56A/CP960 IP phones running firmware version 80 or later
- SIP-T54S/T52S/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27P/T2 7G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, W52P and W56P IP phones running firmware version 81 or later

Other IP phones or the IP phones listed above running old firmware version use the old auto provisioning mechanism.

#### For Old Auto Provisioning Mechanism

1. Add/Edit 802.1X authentication parameters in the configuration file.

The following table shows the information of parameters:

Parameters	Permitted Values	Default
network.802_1x.mode	0, 1, 2, 3, 4, 5, 6 or 7	0
Description:		
Configures the 802.1x authentication method.		
<b>0</b> -Disabled		
1-EAP-MD5		
2-EAP-TLS		
<b>3</b> -EAP-PEAP/MSCHAPv2		
4-EAP-TTLS/EAP-MSCHAPv2		
5-EAP-PEAP/GTC		
6-EAP-TTLS/EAP-GTC		
<b>7</b> -EAP-FAST		
<b>Note:</b> If you change this parameter, the IP phone v	vill reboot to make the chang	ge take
effect.		
Web User Interface:		
Network->Advanced->802.1x->802.1x Mode		
Phone User Interface:		

Parameters	Permitted Values	Default			
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x			
Settings->802.1x Mode					
network.802_1x.identity	String within 32 characters	Blank			
Description:					
Configures the user name for 802.1x authentication	۱.				
<b>Note</b> : It works only if the value of the parameter "r 5, 6 or 7. If you change this parameter, the IP phone effect.					
Web User Interface:					
Network->Advanced->802.1x->Identity					
Phone User Interface:					
Menu->Settings->Advanced Settings (default pass Settings->Identity	word: admin) ->Network->8	02.1x			
network.802_1x.md5_password String within 32 characters					
Description:					
Configures the password for 802.1x authentication					
Note: It works only if the value of the parameter "r	network.802_1x.mode" is set t	to 1, 3, 4, 5,			
6 or 7. If you change this parameter, the IP phone effect.	will reboot to make the chan	ge take			
Web User Interface:					
Network->Advanced->802.1x->MD5 Password					
Phone User Interface:					
Menu->Settings->Advanced Settings (default pass Settings->MD5 Password	word: admin) ->Network->8	02.1x			
network.802_1x.root_cert_url	URL within 511 characters	Blank			
Description:					
Configures the access URL of the CA certificate.					
<b>Note</b> : It works only if the value of the parameter "r		to 2, 3, 4, 5,			
6 or 7. The format of the certificate must be *.pem,	^.crt, *.cer or *.der.				
Web User Interface:					
Network->Advanced->802.1x->CA Certificates					
Phone User Interface:					

Parameters	Permitted Values	Default
None		
network.802_1x.client_cert_url	URL within 511 characters	Blank
Description:		
Configures the access URL of the device certificate		
<b>Note</b> : It works only if the value of the parameter "r (EAP-TLS). The format of the certificate must be *.p	—	to 2
Web User Interface:		
Network->Advanced->802.1x->Device Certificates		
Phone User Interface:		
None		

The following shows an example of the EAP-TLS protocol for 802.1X authentication in configuration files:

```
network.802_1x.mode = 2
network.802_1x.identity = yealink
network.802_1x.root_cert_url = http://192.168.1.8:8080/ca.crt
network.802_1x.client_cert_url = http://192.168.1.8:8080/client.pem
```

**2.** Upload the configuration files, CA certificate and client certificate to the root directory of the provisioning server.

#### **Applying the Configuration Files to Your Phone**

Once you have edited and configuration file (e.g., y0000000000xx.cfg) using the parameters introduced above, you need to do the following to apply the files to your phone:

- **1.** Connect your phone to a network that is not 802.1X-enabled.
- Perform the auto provisioning process to apply the configuration files to the phone. Then the IP phone will reboot to make the settings effective.
   For more information on auto provisioning, refer to *Yealink\_SIP-T2 Series\_T19(P) E2\_T4\_Series\_CP860\_W56P\_IP\_Phones\_Auto\_Provisioning\_Guide.*
- Connect the phone to the 802.1X-enabled network and reboot the phone.
   You can make a phone call to verify whether the phone is authenticated.

#### For New Auto Provisioning Mechanism

 Add/Edit 802.1X authentication parameters in the configuration file (e.g., static.cfg). The following table shows the information of parameters:

Parameters	Permitted Values	Default
static.network.802_1x.mode	0, 1, 2, 3, 4, 5, 6 or 7	0
Description:		
Configures the 802.1x authentication method.		
<b>0</b> -EAP-None		
<b>1</b> -EAP-MD5		
<b>2</b> -EAP-TLS		
<b>3</b> -EAP-PEAP/MSCHAPv2		
<b>4</b> -EAP-TTLS/EAP-MSCHAPv2		
5-EAP-PEAP/GTC		
<b>6</b> -EAP-TTLS/EAP-GTC		
<b>7</b> -EAP-FAST		
If it is set to 0 (EAP-None), 802.1x authentication is no	t required.	
<b>Note:</b> If you change this parameter, the IP phone will effect.	reboot to make the chang	je take
Web User Interface:		
Network->Advanced->802.1x->802.1x Mode		
Phone User Interface:		
Menu->Settings->Advanced Settings (default passwo	rd: admin)	
->Network->802.1x->802.1x Mode		
static.network.802_1x.eap_fast_provision_mode	0 or 1	0
Description:		
Configures the EAP In-Band provisioning method for I	EAP-FAST.	
<b>0</b> -Unauthenticated Provisioning		
1-Authenticated Provisioning		
If it is set to 0 (Unauthenticated Provisioning), EAP In- server unauthenticated PAC (Protected Access Creden Diffie-Hellman key exchange.		•
If it is set to 1 (Authenticated Provisioning), EAP In-Bar authenticated PAC provisioning using certificate based		l by server
<b>Note:</b> It works only if the value of the parameter "static (EAP-FAST). If you change this parameter, the IP phone take effect.		
Web User Interface:		

Network->Advanced->802.1x->Provisioning Mode

Parameters	Permitted Values	Default
Phone User Interface:		
None		
static.network.802_1x.anonymous_identity	String within 512 characters	Blank
Description:		
Configures the anonymous identity (user name) for 80	2.1X authentication.	
It is used for constructing a secure tunnel for 802.1X a	uthentication.	
<b>Note:</b> It works only if the value of the parameter "stati 3, 4, 5, 6 or 7. If you change this parameter, the IP pho take effect.		
Web User Interface:		
Network->Advanced->802.1x->Anonymous Identity		
Phone User Interface:		
None		
static.network.802_1x.identity	String within 32 characters	Blank
Description:		
Configures the user name for 802.1x authentication.		
<b>Note</b> : It works only if the value of the parameter "stati 2, 3, 4, 5, 6 or 7. If you change this parameter, the IP pl take effect.		
Web User Interface:		
Network->Advanced->802.1x->Identity		
Phone User Interface:		
Menu->Settings->Advanced Settings (default passwor ->Network->802.1x->Identity	rd: admin)	
static.network.802_1x.md5_password	String within 32 characters	Blank
Description:		
Configures the password for 802.1x authentication.		
Configures the password for 802.1x authentication. <b>Note</b> : It works only if the value of the parameter "stati 3, 4, 5, 6 or 7. If you change this parameter, the IP pho take effect.		

Parameters	Permitted Values	Default
Network->Advanced->802.1x->MD5 Password		
Phone User Interface:		
Menu->Settings->Advanced Settings (default passwo	rd: admin)	
->Network->802.1x->MD5 Password		
static.network.802_1x.root_cert_url	URL within 511 characters	Blank
Description:		
Configures the access URL of the CA certificate.		
3, 4, 5, 6 or 7. If the authentication method is EAP-FAS	•	
the parameter "static.network.802_1x.eap_fast_provisio Provisioning). The format of the certificate must be *.p		ated
		ated
Provisioning). The format of the certificate must be *.p		ated
Provisioning). The format of the certificate must be *.p Web User Interface:		ated
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates		ated
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface:		Blank
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None	em, *.crt, *.cer or *.der. URL within 511	
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url	em, *.crt, *.cer or *.der. URL within 511	
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url Description:	em, *.crt, *.cer or *.der. URL within 511 characters	Blank
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url Description: Configures the access URL of the device certificate.	em, *.crt, *.cer or *.der. URL within 511 characters c.network.802_1x.mode"	Blank
Provisioning). The format of the certificate must be *,p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url Description: Configures the access URL of the device certificate. Note: It works only if the value of the parameter "stati	em, *.crt, *.cer or *.der. URL within 511 characters c.network.802_1x.mode"	Blank
Provisioning). The format of the certificate must be *.p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url Description: Configures the access URL of the device certificate. Note: It works only if the value of the parameter "stati (EAP-TLS). The format of the certificate must be *.per	em, *.crt, *.cer or *.der. URL within 511 characters c.network.802_1x.mode"	Blank
Provisioning). The format of the certificate must be *,p Web User Interface: Network->Advanced->802.1x->CA Certificates Phone User Interface: None static.network.802_1x.client_cert_url Description: Configures the access URL of the device certificate. Note: It works only if the value of the parameter "stati (EAP-TLS). The format of the certificate must be *.perform Web User Interface:	em, *.crt, *.cer or *.der. URL within 511 characters c.network.802_1x.mode"	Blank

The following shows an example of the EAP-TLS protocol for 802.1X authentication in configuration files:

```
static.network.802_1x.mode = 2
static.network.802_1x.anonymous_identity = Anonymous
static.network.802_1x.identity = yealink
static.network.802_1x.root_cert_url = http://192.168.1.8:8080/ca.crt
static.network.802_1x.client_cert_url = http://192.168.1.8:8080/client.pem
```

**2.** Reference the configuration file in the boot file (e.g., y000000000000.boot). Example: include:config "http://10.2.1.158/static.cfg"

**3.** Upload the boot file, configuration file, CA certificate and client certificate to the root directory of the provisioning server.

#### **Applying the Configuration Files to Your Phone**

Once you have edited a boot file (e.g., y000000000000.boot) and configuration file (e.g., static.cfg) using the parameters introduced above, you need to do the following to apply the files to your phone:

- 1. Connect your phone to a network that is not 802.1X-enabled.
- Perform the auto provisioning process to apply the configuration files to the phone. Then the IP phone will reboot to make the settings effective. For more information on auto provisioning, refer to *Yealink\_SIP-T2\_Series\_T19(P)*

E2\_T4\_Series\_T5\_Series\_W5\_Series\_CP\_Serires\_IP\_Phones\_Auto\_Provisioning\_Guide\_V81.

Connect the phone to the 802.1X-enabled network and reboot the phone.
 You can make a phone call to verify whether the phone is authenticated.

#### **Configuring 802.1X via Web User Interface**

The following takes a SIP-T23G IP phone running firmware version 81 as an example.

- 1. Connect your phone to a network that is not 802.1X-enabled.
- 2. Login to the web user interface of the phone.
- 3. Click on Network->Advanced.
- 4. In the 802.1x block, select the desired protocol from the pull-down list of 802.1x Mode.
  - a) If you select EAP-MD5:
    - 1) Enter the user name for authentication in the **Identity** field.

Yealink 1236	_	_	_	_	_	_	En	Log Out glish(English) 🗸
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basic	ш	P					NOTE	
			Active	Ena	bled	-		
PC Port			Packet Interval (1~3	600s) 60			VLAN It is used to k	gically divide a
NAT	CD	p					physical netw broadcast dor	ork into several nains. VLAN
Advanced			Active	Disa	bled			an be configured are instead of
			Packet Interval (1~3	600s) 60			physically relo- connections.	cating devices or
							The priority o	VLAN assignment
			:				method (from lowest) :LLDP	highest to /CDP->manual
			•				configuration-	>DHCP VLAN
	802	.1x					NAT Traversa	
		L	802.1x Mode	EAP	MD5	-	It is a general	term for at establish and
			Provisioning Mode	Unau	uthenticated Provisi	c 🕶	maintain IP co	nnections
			Anonymous Identity				is one of the	T gateways. STUN NAT traversal
		1	Identity	yeali	nk		techniques.	
			MD5 Password		••••		You can confi for the IP pho	gure NAT traversal ine.
			CA Certificates	Upl	oad	Browse	Quality of Se It is the ability	
			Device Certificates	Upl	beo	Browse	different prior packets in the	ities for different
				Opi			with special re	
		C	onfirm		Cancel		Web Comor	lune.

2) Enter the password for authentication in the MD5 Password field.

- b) If you select EAP-TLS:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Leave the MD5 Password field blank.
  - **4)** In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.
  - 5) In the **Device Certificates** field, click **Browse** to select the desired client (\*.pem or \*.cer) certificate from your local system.

ealink 1236	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
	LLDI	,					NOTE	
Basic			Active	For	bled	-	NOTE	
PC Port					ibied	-	VLAN	
			Packet Interval (1~3	600s) 60			It is used to log physical networ	
NAT	CDP						broadcast doma	ains. VLAN
Advanced			Active	Dis	abled	•	membership car through softwa	
			Packet Interval (1~3	600s) 60			physically reloca	ting devices or
							connections.	
							The priority of M method (from h	
			•				lowest) :LLDP/0	CDP->manual
	802.		•				configuration->	DHCP VLAN
	002.						NAT Traversal	
			802.1x Mode	EAP	-TLS		It is a general to techniques that	
			Provisioning Mode	Una	uthenticated Provis	ic -	maintain IP con	nections
		1.1	Anonymous Identity	Ano	nymous		traversing NAT	
		1	dentity	veal	nk		techniques.	
							You can configu	ure NAT travers
			MD5 Password	•••	•••••	-	for the IP phon	e.
		6	CA Certificates			Browse	Quality of Ser	vice (QoS)
				Up	load	-	It is the ability t different prioriti	
		10	Device Certificates			Browse	packets in the r	

- 6) Click Upload to upload the certificates.
- c) If you select EAP-PEAP/MSCHAPv2:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Enter the password for authentication in the **MD5 Password** field.
  - In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

						Eng	Log Out lish(English) 👻
Yealink 1236			$\longrightarrow$				
	Status A	Account Network	DSSKey	Features	Settings	Directory	Security
Basic	LLDP					NOTE	<b>_</b>
		Active	Enable	d	•	1.00	
PC Port		Packet Interval (1~36	00s) 60			VLAN It is used to lo	gically divide a
NAT	CDP					physical netwo broadcast dom	ork into several
Advanced		Active	Disable	ed	•	membership control through software	an be configured are instead of
		Packet Interval (1~36	00s) 60			physically reloc connections.	ating devices or
		÷				The priority of method (from lowest) :LLDP, configuration-:	/CDP->manual
	802.1x					NAT Traversa	
		802.1x Mode	EAP-PE	AP/MSCHAPv2		It is a general techniques the	term for at establish and
		Provisioning Mode	Unauth	enticated Provisic ¬	-	maintain IP co traversing NAT	nnections gateways, STUN
		Anonymous Identity	Anonyn	nous	]	is one of the M techniques.	
		Identity	yealink				
		MD5 Password		••	7	for the IP pho	gure NAT traversal ne.
		CA Certificates	Upload		Browse	Quality of Se It is the ability	to provide
		Device Certificates	Uploa	i	Browse	packets in the	ansport of traffic
		Confirm		Cancel		Web Conver 1	

- 5) Click **Upload** to upload the certificate.
- d) If you select EAP-TTLS/EAP-MSCHAPv2:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Enter the password for authentication in the MD5 Password field.

**4)** In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

	_	_		_	_	_	_	Log Out
Yealink 1236							Eng	glish(English) 🚽
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basic	LLDI	þ					NOTE	
			Active	Ena	pled	•		
PC Port			Packet Interval (1~3	600s) 60				ogically divide a
NAT	CDP						physical netwo broadcast don	ork into several nains. VLAN
Advanced			Active	Disa	bled	•		an be configured vare instead of
			Packet Interval (1~3	600s) 60		_		cating devices or
			:				method (from	
							lowest) :LLDP configuration-	/CDP->manual >DHCP VLAN
	802.1	x					NAT Traversa	al
		1	802.1x Mode	EAP-	TTLS/EAP-MSCHAP	•	It is a general	term for at establish and
			Provisioning Mode	Unau	thenticated Provisic	<b>v</b>	maintain IP co	nnections
			Anonymous Identity	Anon	ymous		is one of the I	T gateways. STUN NAT traversal
			Identity	yealin	k		techniques.	
			MD5 Password				You can confi for the IP pho	gure NAT traversal
						Browse	Quality of Se	arvice (OoS)
			CA Certificates	Uplo	ad		It is the ability	
			Device Certificates		_	Browse	packets in the	e network,
				Uplo	ad		allowing the to with special re	ransport of traffic equirements.
		C	onfirm		Cancel		Web Comer	huno.

- 5) Click **Upload** to upload the certificate.
- e) If you select EAP-PEAP/GTC:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Enter the password for authentication in the MD5 Password field.
  - In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

	Status	Account	Network	DSSKey	Features	Settings	Directory Security		
Basic	LLDF	0					NOTE		
			Active	En	abled	-			
PC Port			Packet Interval (1~3	600s) 60	1		VLAN It is used to logically divide a		
NAT	CDP						physical network into several broadcast domains, VLAN		
Advanced			Active	Dis	abled	-	membership can be configured through software instead of		
Tigranda			Packet Interval (1~3	600s) 60		_	physically relocating devices or		
							connections.		
							The priority of VLAN assignme method (from highest to		
							lowest) :LLDP/CDP->manual		
			- <b>F</b>			configuration->DHCP VLAN			
	802.3						NAT Traversal It is a general term for		
			802.1x Mode	EA	P-PEAP/GTC	*	techniques that establish and		
			Provisioning Mode	Un	authenticated Provisi	ic 💌	maintain IP connections traversing NAT gateways. STU		
			Anonymous Identity	An	onymous		is one of the NAT traversal techniques.		
			Identity	yea	link				
			MD5 Password	•••		_	You can configure NAT travers for the IP phone.		
						Browse	Quality of Service (QoS)		
			CA Certificates	U	bool		It is the ability to provide		
						Browse	<ul> <li>different priorities for different</li> </ul>		

- 5) Click **Upload** to upload the certificate.
- f) If you select EAP-TTLS/EAP-GTC:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Enter the password for authentication in the **MD5 Password** field.
  - In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

					Log Out English(English)
Yealink 1236					
	Status Account	Network DSS	SKey Features	Settings	Directory Security
Basic	LLDP				NOTE
		Active	Enabled	•	
PC Port		Packet Interval (1~3600s)	60		VLAN It is used to logically divide a
NAT	CDP				physical network into several broadcast domains. VLAN
Advanced		Active	Disabled	•	membership can be configured through software instead of
		Packet Interval (1~3600s)	60		physically relocating devices or connections.
					The priority of VLAN assignment
		:			method (from highest to lowest) :LLDP/CDP->manual
					configuration->DHCP VLAN
	802.1x				NAT Traversal
		802.1x Mode	EAP-TTLS/EAP-GTC	•	It is a general term for techniques that establish and
		Provisioning Mode	Unauthenticated Provisic	¥.	maintain IP connections traversing NAT gateways. STUN
		Anonymous Identity	Anonymous		is one of the NAT traversal techniques.
		Identity	yealink		You can configure NAT traversal
		MD5 Password	•••••		for the IP phone.
		CA Certificates		Browse	Quality of Service (QoS) It is the ability to provide
			Upload	Browse	different priorities for different
		Device Certificates	Upload	browse	packets in the network, allowing the transport of traffic
		Confirm	Cancel		with special requirements.

- 5) Click **Upload** to upload the certificate.
- g) If you select EAP-FAST:
  - (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
  - 2) Enter the user name for authentication in the **Identity** field.
  - 3) Enter the password for authentication in the **MD5 Password** field.
  - 4) Select the desired value from the pull-down list of Provisioning Mode.
  - 5) In the **CA Certificates** field, click **Browse** to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

	Status	Account	Network	DSSKey	Features		Settings	Directory	Security
Basic	LLD	Ρ						NOTE	
PC Port			Active	Ena	abled	•		VLAN	
PC POIL			Packet Interval (1~360	00s) 60				It is used to lo	
NAT	CDP	,						physical netwo broadcast don	ork into several
Advanced			Active	Dis	abled	•			an be configured
in the second seco			Packet Interval (1~360	00s) 60				physically reloc	ating devices or
			i donor intervar (1. oor	00)				connections.	
									VLAN assignme
			•					method (from lowest) :LLDP,	CDP->manual
								configuration :	>DHCP VLAN
								comguración	
	802	.1x						NAT Traversa	4
	802	.1x	802.1x Mode	EAI	P-FAST	•		NAT Traversa It is a general	4
	802	.1x	802.1x Mode Provisioning Mode		P-FAST nuthenticated Provi	▼ isic ▼		NAT Traversa It is a general techniques the maintain IP co	l term for at establish and nnections
	802	.1x		Una				NAT Traversa It is a general techniques the maintain IP co traversing NAT is one of the N	I term for at establish and nnections r gateways. STL
	802	.1x	Provisioning Mode Anonymous Identity	Una	nuthenticated Provi	▼ isic ▼		NAT Traversa It is a general techniques the maintain IP co traversing NAT	I term for at establish and nnections r gateways. STL
	802	.1x	Provisioning Mode Anonymous Identity Identity	Una Ano yea	authenticated Prov onymous link			NAT Traversa It is a general techniques this maintain IP co traversing NAT is one of the M techniques. You can config	I term for at establish and nnections Gateways. STL IAT traversal gure NAT traver
	802	.1x	Provisioning Mode Anonymous Identity	Una Ano yea	nuthenticated Provi			NAT Traversa It is a general techniques the maintain IP co traversing NAT is one of the N techniques. You can confle for the IP pho	l term for at establish and nnections r gateways. STL IAT traversal gure NAT traver ne.
	802	.1x	Provisioning Mode Anonymous Identity Identity	Una And yea	inthenticated Provi inymous link		Browse	NAT Traversa It is a general techniques the maintain IP co traversing NAT is one of the I techniques. You can confle for the IP pho Quality of Se	I term for at establish and nnections r gateways. STL IAT traversal gure NAT traver ne. rvice (QoS)
	802	.1x	Provisioning Mode Anonymous Identity Identity MD5 Password	Una And yea	authenticated Prov onymous link		Browse	NAT Traversa It is a general techniques the maintain IP co traversing NAT is one of the IP techniques. You can config for the IP pho Quality of Se It is the ability	I term for at establish and nnections gateways. STI IAT traversal gure NAT traver ne. rvice (QoS) to provide tiss for different

The CA certificate needs to be uploaded only when **Authenticated Provisioning** mode is selected from the **Provisioning Mode** field.

- 6) Click **Upload** to upload the certificate.
- 5. Click **Confirm** to accept the change.

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

- 6. Click **OK** to reboot the phone.
- 7. Connect the phone to the 802.1X-enabled network after reboot.
- **Note** If the Pass-thru mode is available on your new phone, you can select the Pass-thru mode from the pull-down list of **DOT1XSTAT Options** via web user interface.

#### **Configuring 802.1X via Phone User Interface**

If you select EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC,

EAP-TTLS/EAP-GTC or EAP-FAST mode, you should upload CA certificate in advance using configuration files or via web user interface. For SIP IP phones running firmware version 81 or later, the CA certificate needs to be uploaded only when **Authenticated Provisioning** mode is selected from the **Provisioning Mode** field.

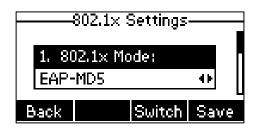
If you select EAP-TLS mode, you should upload CA certificate and device certificate in advance using configuration files or via web user interface.

The following takes a SIP-T23G IP phone running firmware version 81 as an example.

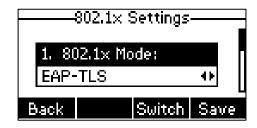
#### To configure 802.1x via phone user interface:

Press Menu->Settings->Advanced Settings (default password: admin)
 ->Network->802.1x.

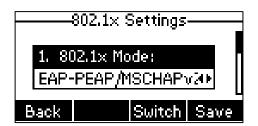
- Press (•) or (•), or the Switch soft key to select the desired value from the 802.1x
   Mode field.
  - a) If you select EAP-MD5:



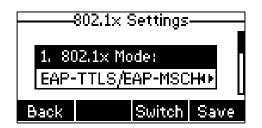
- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.
- **b)** If you select **EAP-TLS**:



- 1) Enter the user name for authentication in the **Identity** field.
- 2) Leave the MD5 Password field blank.
- c) If you select EAP-PEAP/MSCHAPv2:

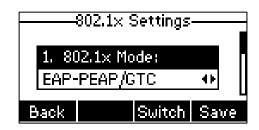


- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.
- d) If you select EAP-TTLS/EAP-MSCHAPv2:

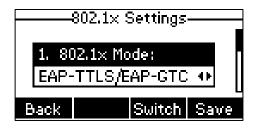


- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.

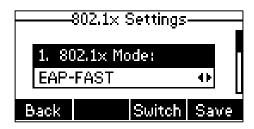
e) If you select EAP-PEAP/GTC:



- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.
- f) If you select EAP-TTLS/EAP-GTC:



- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.
- g) If you select EAP-FAST:



- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.
- 3. Press Save to accept the change.

The IP phone reboots automatically to make the settings effective after a period of time.

## 802.1X Authentication Process

Reboot the phone to activate the 802.1X authentication on the phone. The 802.1X authentication process is divided into two basic stages:

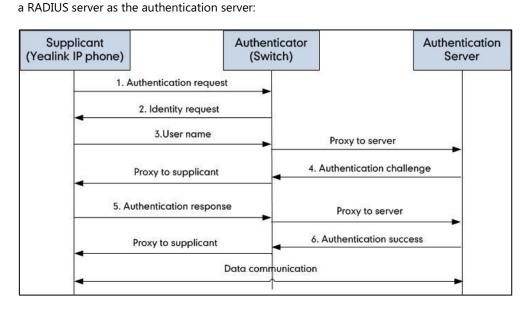
#### **Pre-authentication**

The 802.1X pre-authentication process begins with the IP phone that contains a supplicant service used for negotiation and authentication. When the IP phone connects to an unauthorized port, the authenticator blocks the IP phone from connecting to the network. Using one of the authentication protocols, the authenticator establishes a security negotiation with the

IP phone and creates an 802.1X session. The IP phone provides its authentication information for the authenticator, and then the authenticator forwards the information to the authentication server.

#### Authentication

After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator grants the IP phone access to the protected network on an authorized port. The following figure summarizes an implementation of the 802.1X authentication process using



For more details about the 802.1X authentication process using EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST protocols, refer to Appendix B: 802.1X Authentication Process on page 29.

If you are interested in the packets exchanged during the authentication process, we recommend you to use the Wireshark tool. Refer to http://wiki.wireshark.org for more information about the Wireshark tool.

## Sample Screenshots – Identity

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-MD5 protocol:

<u>Ele Edit View G</u> o	shark 1.10.5 (SVN Rev 5426) Capture Analyze Statistics	Telephony	ools Inter		
		🌳 🧼 🐴		∃) Q, Q, Q, [7]   ₩ M 🥵 %   13	
Filter: eap    eapol			▼ Ex	pression Clear Apply Save Filter	
No. Time	Source	Destination	Protocol	Length Info	
4 2.215736000	cisco_5d:42:94	Nearest	EAPOL	60 Start	
5 2.218751000	Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
6 2.266603000	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
7 2.276228000	cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
8 2.277015000	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
10 2.284961000	cisco_5d:42:94	Nearest	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)	
11 2.285802000	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)	
19 3.319329000	cisco_5d:42:94	Nearest	EAP	60 success	
<[				III	
				(480 bits) on interface 0	
		):62:6b:5d:4	12:94), D	st: Nearest (01:80:c2:00:00:03)	
802.1X Authenti					
version: 802.					
Type: Start (	1)				
Length: 0					

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-TLS protocol:

TLS.pcapng [Wireshark 1.10.5 (SVN Rev 54262 f	rom /trunk-1.:	L0)]	
File Edit View Go Capture Analyze Statistics	Telephony	Tools Intern	als <u>H</u> elp
● ● 🗶 🗮 🎢 🕒 🗎 🗙 ಿ 🔍 🗢	۰ 😜 🐐	<u>v</u>   EE	3] Q. Q. Q. [7]   😹 M 🖲 %   🐹
Filter: eap    eapol		▼ Exp	pression Clear Apply Save Filter
No. Time Source	Destination	Protocol L	ength Info
116 17.805503000 Cisco_5d:42:94	Nearest	EAPOL	60 Start
117 17.808685000 cisco_5d:42:94	Nearest	EAP	60 Request, Identity
118 17.809519000 XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity
119 17.819739000 Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)
120 17.823631000 xiamenYe_73:4c:f1	Nearest	TLSV1	112 Client Hello
122 17.857040000 cisco_5d:42:94	Nearest		1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello De
123 17.858234000 xiamenYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
124 17.867698000 cisco_5d:42:94	Nearest		1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello De
125 17.869098000 xiamenYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
126 17.882798000 cisco_5d:42:94	Nearest	TLSV1	644 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello D
130 18.447360000 XiamenYe_73:4c:f1	Nearest		1366 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
131 18.457674000 cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)
132 18.459768000 XiamenYe_73:4c:f1	Nearest	TLSV1	827 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
133 18.478941000 cisco_5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message
134 18.487070000 XiamenYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
146 19.516815000 cisco_5d:42:94	Nearest	EAP	60 Success
•			III
🗄 Frame 118: 60 bytes on wire (480 bit:			
Ethernet II, Src: XiamenYe_73:4c:f1	(00:15:65:	/3:4c:t1),	Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication			
version: 802.1X-2001 (1)			
Type: EAP Packet (0) Length: 12			
Extensible Authentication Protocol			
Extensible Authentication Protocol Code: Response (2)			
Id: 1			
Length: 12			
Type: Identity (1)			
Identity: yealink			
Idencity, yearink			

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-PEAP/MSCHAPv2 protocol:

EAP-PEAP MSCHPv2	pcapng [Wireshark 1.10.5 ]	(SVN Rev 5426	2 from /trunk-	1.10)]	
ile <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Internal	is <u>H</u> elp	
	🕒 🖺 💥 🔁 🔍 🔶	🔹 📣 🛣	1 EB	)  Q Q Q 🔟   👪 🗹 🅵 🔆   💢	
		~ ~ u			
ilter: eap    eapol			▼ Expr	ression Clear Apply Save Filter	
p. Time	Source	Destination	Protocol Le		
	cisco_5d:42:94	Nearest	EAPOL	60 Start	
	cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
	Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
	Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	XiamenYe_73:4c:f1	Nearest	TLSv1	116 Client Hello	
	Cisco_5d:42:94	Nearest		1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	cisco_5d:42:94	Nearest		1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	Cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	xiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
	cisco_5d:42:94	Nearest	TLSV1	77 Application Data	
	xiamenYe_73:4c:f1	Nearest	TLSV1	162 Application Data, Application Data	
	Cisco_5d:42:94	Nearest	TLSV1	109 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
	Cisco_5d:42:94	Nearest	TLSv1	61 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSv1	98 Application Data, Application Data	
56 5.877757000	Cisco_5d:42:94	Nearest	EAP	60 Success	
				m	
Frame 11: 60 by	tes on wire (480 bits/	), 60 bytes	s captured	(480 bits) on interface 0	
		(00:15:65:7	/3:4c:f1),	Dst: Nearest (01:80:c2:00:00:03)	
802.1X Authenti					
Version: 802.					
Type: EAP Pac	:ket (0)				
Length: 12					
	thentication Protocol				
Code: Respo	onse (2)				
Id: 1					
Length: 12					
Type: Ident					
Identity: y	/ealink				

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-TTLS/EAP-MSCHAPv2 protocol:

📕 EA	P-TTLS EAP-MSCH	IAPv2.pcapng [Wireshark 1.1	0.5 (SVN Rev	54262 from	/trunk-1.10)]	
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Intern	als Help	
0 (	• 🖌 🔳 🔬	🖻 🛍 🗶 🔁   🔍 🔶	🏟 🥥 🐺	2   🗏	]   Q, Q, Q, 177   II 188 189 🕺 💥   💢	
Filter	: eap    eapol			💌 Exp	oression Clear Apply Save Filter	
No.	Time	Source	Destination	Protocol L	ength Info	
		xiamenYe_73:4c:f1	Nearest	EAPOL	60 Start	
		Cisco_5d:42:94	Nearest	EAPOL	60 Start	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
		cisco_5d:42:94	Nearest	EAP	60 Request, Tunneled TLS EAP (EAP-TTLS)	
		XiamenYe_73:4c:f1	Nearest	TLSV1	112 Client Hello	
		cisco_5d:42:94	Nearest		1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		<pre>xiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
		Cisco_5d:42:94	Nearest		1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
		Cisco_5d:42:94	Nearest	TLSV1	526 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco_5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message	
		XiamenYe_73:4c:f1	Nearest	TLSV1	210 Application Data, Application Data	
		Cisco_5d:42:94 XiamenYe 73:4c:f1	Nearest	TLSV1 FAP	113 Application Data	
		cisco 5d:42:94	Nearest Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS) 60 Success	
40	5.260661000	C1SC0_50:42:94	Nearest	EAP		
۰					m	+
	hernet II, Sr 2.1X Authenti Version: 802. Type: EAP Pac Length: 12	c: XiamenYe_73:4c:f1 ( cation 1X-2001 (1)			(480 bits) on interface 0 Dst: Nearest (01:80:c2:00:00:03)	
	Code: Respo					
	Id: 1					
	Length: 12					
	Type: Ident	ity (1)				
	Identity: y					
	Tachercy, y	carring				

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-PEAP/GTC protocol:

📕 EAP	-PEAP GTC.pcapn	g [Wireshark 1.10.5 (SVN R	ev 54262 fror	m /trunk-1.10	))]	
Ele B	Edit <u>V</u> iew <u>Go</u>	Capture Analyze Statistics	Telephony	Tools Interr	ials Help	
0.6		🖹 🖹 🗙 🛃 🔍 🔶	a a T	4 IN	I) Q Q Q 🖸   🖬 🛛 🍕 %   🙀	
• •	e aa 🛲 aa i		~ <del>~</del> T			
Filter:	eap    eapol			▼ Ex	pression Clear Apply Save Filter	
No.		Source	Destination		ength Info	
		Cisco_5d:42:94	Nearest	EAPOL	60 Start	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
		xiamenYe_73:4c:f1	Nearest	TLSV1	116 Client Hello	
		cisco_5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		cisco_5d:42:94	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		Cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
		xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		cisco_5d:42:94	Nearest	TLSV1	77 Application Data	
		xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
		xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		Cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
		<pre>xiamenYe_73:4c:f1 Cisco_5d:42:94</pre>	Nearest	TLSv1	98 Application Data, Application Data 60 Success	
110	14.220/32000	C1SC0_50:42:94	Nearest	EAP		
<					m	•
e Eth		:: XiamenYe_73:4c:f1 (			d (480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
	/ersion: 802.1					
1	Type: EAP Pack	(0)				
	ength: 12					
- 6		hentication Protocol				
	Code: Respor	ise (2)				
	Id: 1					
	Length: 12					
_	Type: Identi	ity (1)				
	Identity: ye					

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-TTLS/EAP-GTC protocol:

	pcapng [Wireshark 1.10.5 (				
ile <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	<u>T</u> ools <u>I</u> nter	mals Help	
D 🖲 煮 📕 🦽	🕒 🛅 🗶 🔁 🔍 🔶	🏟 🤪 7	2 🗐		
ilter: eap    eapol			▼ E	xpression Clear Apply Save Filter	
o. Time	Source	Destination		Length Info	
	Cisco_5d:42:94	Nearest	EAPOL	60 Start	
	Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
	Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
	cisco_5d:42:94 xiamenye 73:4c:f1	Nearest	EAP	60 Request, Tunneled TLS EAP (EAP-TTLS) 112 Client Hello	
	cisco_5d:42:94	Nearest	TLSV1 TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	Cisco_5d:42:94 XiamenYe_73:4c:f1	Nearest	EAP	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 60 Response, Tunneled TLS EAP (EAP-TTLS)	
	Cisco_5d:42:94	Nearest	EAP TLSV1	1042 Server Hello. Certificate. Server Key Exchange. Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	FAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
	Cisco_5d:42:94	Nearest	TLSV1	526 Server Hello. Certificate. Server Key Exchange. Server Hello Done	
	XiamenYe 73:4c:f1	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	cisco 5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message	
	xiamenye 73:4c:f1	Nearest	TLSV1	114 Application Data, Application Data	
	cisco 5d:42:94	Nearest	TLSV1	97 Application Data	
37 3,980504000	xiamenye 73:4c:f1	Nearest	TLSV1	130 Application Data, Application Data	
48 5.011940000	Cisco_5d:42:94	Nearest	EAP	60 Success	
				III.	
				(480 bits) on interface 0	
		(00:15:65:	73:4c:f1)	, Dst: Nearest (01:80:c2:00:03)	
802.1X Authenti					
version: 802.					
Type: EAP Pac	:Ket (0)				
Length: 12	thentication Protocol				
Code: Respo					
td: 1	nise (2)				
Length: 12					
Leiguit, 12					
Type: Ident					

The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-FAST protocol:

		ireshark 1.10.5 (SVN Rev 54				•
le j	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	<u>T</u> ools <u>I</u> nter	mals Help	
	) 🔏 📕 🙇 🛛	🖻 🗟 🗶 🎜   🔍 🔶	👒 🤹 🖗	2 🗐	🗐   Q, Q, Q, 💟   👪 🗹 🥵 %   🔛	
ilter:	eap    eapol			▼ E	xpression Clear Apply Save Filter	
	Time	Source	Destination		Length Info	
		XiamenYe_45:6f:bb	Nearest	EAPOL	60 Start	
		cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
		XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
		cisco_5d:42:94	Nearest	TLSV1	60 Ignored Unknown Record	
		xiamenYe_45:6f:bb Cisco_5d:42:94	Nearest	TLSV1	80 Client Hello	
		Cisco_50:42:94 XiamenYe 45:6f:bb	Nearest	TLSV1 EAP	1030 Server Hello, Certificate, Certificate Request, Server Hello Done 60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)	
		cisco_5d:42:94	Nearest	EAP TLSV1	483 Server Hello, Certificate, Certificate Request, Server Hello Done	
		XiamenYe 45:6f:bb	Nearest	TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco_5d:42:94	Nearest	TLSV1	109 Change Cipher Spec. Encrypted Handshake Message. Application Data	
		XiamenYe 45:6f:bb	Nearest	TLSV1	63 Application Data	
		Cisco 5d:42:94	Nearest	TLSV1	87 Application Data	
		XiamenYe_45:6f:bb	Nearest	TLSV1	83 Application Data	
		Cisco 5d:42:94	Nearest	TLSV1	115 Application Data	
		XiamenYe_45:6f:bb	Nearest	TLSV1	131 Application Data	
		cisco_5d:42:94	Nearest	TLSV1	279 Application Data	
		XiamenYe 45:6f:bb	Nearest	TLSV1	65 Application Data	
	20. 302200000	Ardinerrie_45.01.00	Near ese	TESV4	iii	
-						
					ed (480 bits) on interface 0	
				45:6f:bb)	, Dst: Nearest (01:80:c2:00:00:03)	
		Nearest (01:80:c2:00:				
		nYe_45:6f:bb (00:15:6		)		
		Authentication (0x888 000000000000000000000000000000000			2000	
	2.1X Authenti		000000000000000000000000000000000000000	000000000		
	version: 802.					
	Type: EAP Pac					
	Length: 10	Ket (0)				
		thentication Protocol				
	Code: Respo					
	Id: 1					
	Length: 10					
	Type: Ident	ity (1)				

## Sample Screenshots - Anonymous Identity

The following screenshot of the Wireshark shows a sample of a successful authentication process with anonymous identity using EAP-TLS protocol:

TLS.pcapng (Wireshark 1	.10.5 (SVN Rev 54262 f	rom /trunk-1.1	0)]	
File Edit View Go Captu				
• • <b>/ / /</b> E	🎒 🗶 🎜   🔍 🔶	🏟 🤪 🐺	⊻   🗏 🛢	Q, Q, Q, 🖺   👹 🕅 🥦 %   🔛
Filter: eap    eapol			• Expre	ession Clear Apply Save Filter
No. Time Sour		Destination	Protocol Len	
116 17.805503000 cis		Nearest	EAPOL	60 Start
117 17.808685000 cis		Nearest	EAP	60 Request, Identity
118 17.809519000 xia		Nearest	EAP	60 Response, Identity
119 17.819739000 Cis		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)
120 17.823631000 xia		Nearest		112 Client Hello
122 17.857040000 cis 123 17.858234000 xia		Nearest		042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
123 17.858234000 X1a 124 17.867698000 cis		Nearest	EAP TLSV1 1	60 Response, TLS EAP (EAP-TLS) 042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
125 17.869098000 Xia		Nearest	EAP 1	60 Response. TLS EAP (EAP-TLS)
126 17.882798000 Cis		Nearest		644 Server Hello. Certificate. Server Kev Exchange. Certificate Request. Server Hello Do
130 18,447360000 Xia		Nearest		366 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
131 18.457674000 Cis		Nearest	FAP	60 Request. TLS EAP (EAP-TLS)
132 18,459768000 Xia		Nearest		827 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
133 18,478941000 cis		Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message
134 18.487070000 xia	menYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
146 19.516815000 cis	co_5d:42:94	Nearest	EAP	60 Success
٠				m
	iamenYe_73:4c:f1 on 001 (1) (0) tication Protocol (2) (1)			(480 bits) on interface 0 3st: Nearest (01:80:c2:00:00:03)

The following screenshot of the Wireshark shows a sample of a successful authentication process with anonymous identity using EAP-PEAP/MSCHAPv2 protocol:

🗲 EAF	P-PEAP MSCHPv2.	pcapng [Wireshark 1.10.5 (	SVN Rev 5426	i2 from /tru	nk-1.10)]	- • ×
Eile 🛛	<u>Edit V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp	
0 (		🕒 🖹 🗶 🛃 🔍 🔶	🏟 🥥 7	1 E	🗐 e o o 🕐 📓 🖉 🍢 🙀	
	eap    eapol				xpression Clear Apply Save Filter	
	Time	Source	Destination		Length Info	
		cisco_5d:42:94	Nearest	EAPOL	60 Start	
		cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
		<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	116 Client Hello	
		Cisco_5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		cisco_5d:42:94	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		<pre>XiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		Cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		XiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
31	4.779122000	cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
32	4.786949000	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
33	4.797998000	cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
34	4.800342000	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
35	4.808518000	cisco_5d:42:94	Nearest	TLSV1	77 Application Data	
36	4.818037000	xiamenYe_73:4c:f1	Nearest	TLSV1	162 Application Data, Application Data	
37	4.825426000	cisco_5d:42:94	Nearest	TLSV1	109 Application Data	
38	4.827896000	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
39	4.840065000	cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
40	4.843186000	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
56	5.877757000	Cisco_5d:42:94	Nearest	EAP	60 Success	
					m	
Et		c: xiamenYe_73:4c:f1			d (480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
	version: 802.					
-	Type: EAP Pac	ket (0)				
	ength: 12					
	Extensible Au	thentication Protocol				
	Code: Respo	nse (2)				
	Id: 1					
	Length: 12					
	Type: Ident	ity (1)				
	Identity: A					

The following screenshot of the Wireshark shows a sample of a successful authentication process with anonymous identity using EAP-TTLS/EAP-MSCHAPv2 protocol:

📕 EAP-1	TTLS EAP-MSCH	APv2.pcapng [Wireshark 1.1	0.5 (SVN Rev	54262 from	/trunk-1.10)]	
File Ed	lit View Go	Capture Analyze Statistics	Telephony	Tools Interr	nals Help	
0 0		🖹 🕅 💥 🔁 🔍 🔶				
••			🤎 💚 😗			
Filter:	eap    eapol			▼ Ex	pression Clear Apply Save Filter	
No. Ti		Source	Destination		ength Info	
		xiamenYe_73:4c:f1	Nearest	EAPOL	60 Start	
		Cisco_5d:42:94	Nearest	EAPOL	60 Start	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
		cisco_5d:42:94 XiamenYe 73:4c:f1	Nearest	EAP	60 Request, ILS EAP (EAP-TLS)	
		cisco 5d:42:94	Nearest Nearest	EAP	60 Response, Legacy Nak (Response Only) 60 Request, Tunneled TLS EAP (EAP-TTLS)	
		XiamenYe 73:4c:f1	Nearest	EAP TLSV1	112 Client Hello	
		cisco 5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
		cisco 5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response. Tunneled TLS EAP (EAP-TTLS)	
		Cisco_5d:42:94	Nearest	TLSV1	526 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco 5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message	
30 4	. 210832000	XiamenYe_73:4c:f1	Nearest	TLSV1	210 Application Data, Application Data	
31 4	.222184000	cisco_5d:42:94	Nearest	TLSV1	113 Application Data	
32 4	.224521000	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
46 5	.260661000	cisco_5d:42:94	Nearest	EAP	60 Success	
					m	
Ethe 802.		c: XiamenYe_73:4c:f1 ( cation			(480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
	pe: EAP Pac					
	ngth: 12					
		thentication Protocol				
	Code: Respon	nse (2)				
	Id: 1					
	Length: 12					
	Type: Identi					
	Identity: Ar	nonymous				

The following screenshot of the Wireshark shows a sample of a successful authentication process with anonymous identity using EAP-PEAP/GTC protocol:

EAP-	-PEAP GTC.pcapn	g [Wireshark 1.10.5 (SVN	Rev 54262 from	m /trunk-1.1	0)]	- • ×
ie E	dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp	
		🖹 🗎 🗙 🛃 🔍 🔶	🏟 🥥 📅	1	🗐 e. e. e. 🖭 📓 🕺 🛸 📓	
	eap    eapol				pression Clear Apply Save Filter	
		-			•	
o. T		Source	Destination		Length Info	
		cisco_5d:42:94 Cisco_5d:42:94	Nearest	EAPOL	60 Start 60 Request. Identity	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request. TLS EAP (EAP-TLS)	
		XiamenYe 73:4c:f1	Nearest	FAP	60 Response, Legacy Nak (Response Only)	
		Cisco 5d:42:94	Nearest	EAP	60 Request. Protected EAP (EAP-PEAP)	
		XiamenYe 73:4c:f1	Nearest	TI SV1	116 Client Hello	
		cisco 5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenye 73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		cisco 5d:42:94	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenye 73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		Cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
		xiamenye 73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
65 1	13.137643000	cisco 5d:42:94	Nearest	TLSV1	61 Application Data	
66 1	13.140060000	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		cisco 5d:42:94	Nearest	TLSV1	77 Application Data	
68 1	L3.150577000	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
69 1	L3.158889000	cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
70 1	L3.161368000	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
72 1	L3.171939000	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
110 1	L4.220732000	cisco_5d:42:94	Nearest	EAP	60 Success	
					m	
Fra	me 32: 60 byd	tes on wire (480 hits	) 60 hyte	s canture	d (480 bits) on interface 0	
Eth	ernet II, Sro	c: xiamenYe_73:4c:f1			, Dst: Nearest (01:80:c2:00:03)	
	.1X Authentio					
	ersion: 802.1					
	ype: EAP Pack	ket (0)				
	ength: 12					
E E:		thentication Protocol				
	Code: Respor	nse (2)				
	Id: 1					
	Length: 12					
	Type: Ident					
	Identity: An	nonymous				

The following screenshot of the Wireshark shows a sample of a successful authentication

process with anonymous identity using EAP-TTLS/EAP-GTC protocol:

EAP-TTLS EAP-GTC .p	capng [Wireshark 1.10.5 (	SVN Rev 5426	2 from /trun	k-1.10)]	
ile Edit View Go	Capture Analyze Statistics	Telephony	Tools Inten	nals Help	
	🖹 🕅 🗙 🔁 🔍 🔶	~ ~ ~			
		** <b>**</b> **			
ilter: eap    eapol			👻 Ex	pression Clear Apply Save Filter	
o. Time	Source	Destination		Length Info	
	Cisco_5d:42:94	Nearest	EAPOL	60 Start	
	Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
10 3.203136000		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
12 3.213804000		Nearest	EAP	60 Request, Tunneled TLS EAP (EAP-TTLS)	
	xiamenYe_73:4c:f1	Nearest	TLSV1	112 Client Hello	
15 3.344040000		Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
18 3.354466000		Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)	
20 3.366494000		Nearest	TLSV1	526 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
34 3.957962000		Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message	
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	114 Application Data, Application Data	
36 3.976751000		Nearest	TLSV1	97 Application Data	
	xiamenYe_73:4c:f1	Nearest	TLSV1	130 Application Data, Application Data	
48 5.011940000	Cisco_5d:42:94	Nearest	EAP	60 Success	
				m	
Ethernet II, Sr 802.1X Authenti Version: 802. Type: EAP Pac Length: 12	c: Xiamenye_73:4c:f1 cation Xx-2001 (1) ket (0) thentication Protocol nse (2)	(00:15:65:		(480 bits) on interface 0 , bst: Nearest (01:80:c2:00:00:03)	

The following screenshot of the Wireshark shows a sample of a successful authentication process with anonymous identity using EAP-FAST protocol:

eap-fast.pcapng [V	Vireshark 1.10.5 (SVN Rev 5	4262 from /trur	nk-1.10)]		
<u>File Edit View Go</u>	Capture Analyze Statistics	Telephony	Tools Internal	ls <u>H</u> elp	
0 🖲 🛋 🗮 🔬	🖻 🖀 🗶 🍠 I 🔍 🔶	• 🛸 💫 7	<u>2</u>   E   E	] 🔍 🔍 🔍 🔟   🕷 🖄   💢	
Filter: eap    eapol			• Expr	ression Clear Apply Save Filter	
o. Time	Source	Destination	Protocol Le		
	XiamenYe_45:6f:bb	Nearest	EAPOL	60 Start	
298 27.070149000		Nearest	EAP	60 Request, Identity	
	XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity	
300 27.110954000		Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
303 27.142441000		Nearest	TLSV1	60 Ignored Unknown Record	
304 27.192682000 305 27.206335000	xiamenYe_45:6f:bb	Nearest	TLSV1 TLSV1	80 Client Hello	
	Cisco_5d:42:94 XiamenYe_45:6f:bb	Nearest		1030 Server Hello, Certificate, Certificate Request, Server Hello Done 60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)	
		Nearest	EAP		
307 27.220253000	Cisco_5d:42:94 XiamenYe 45:6f:bb	Nearest	TLSV1	483 Server Hello, Certificate, Certificate Request, Server Hello Done	
308 27.441500000		Nearest	TLSV1 TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mossage, Application Data	Message
	xiamenYe_45:6f:bb	Nearest	TLSV1	63 Application Data	
311 27.548350000		Nearest	TLSV1	87 Application Data	
	XiamenYe 45:6f:bb	Nearest	TLSV1	83 Application Data	
313 27, 563043000		Nearest	TLSV1	115 Application Data	
	xiamenYe_45:6f:bb	Nearest		131 Application Data	
315 27.580263000		Nearest	TLSV1	279 Application Data	
	XiamenYe_45:6f:bb	Nearest	TLSV1	65 Application Data	
1	XTamerre_45.01.00	wear est		m	
Frame 299: 60 b			es captured	d (480 bits) on interface 0	
Ethernet II, Sr 802.1X Authenti		(00:15:65:4	15:6f:bb),	Dst: Nearest (01:80:c2:00:03)	
Version: 802.					
Type: EAP Pac Length: 19	ket (0)				
	thentication Protoco	1			
Code: Respo					
Id: 1	136 (2)				
Length: 19					
Type: Ident	ity (1)				
Identity: A					
Smallerey: A					

# Troubleshooting

#### Why doesn't the IP phone pass 802.1X authentication?

Do the following in sequence:

- Ensure that the 802.1X authentication environment is operational.
  - a) Connect another device (e.g., a computer) to the switch port.
  - b) Check if the device is authenticated successfully, and an IP address is assigned to it. If the device fails the authentication, check the configurations on the switch and authentication server.
- Ensure that the user name and password configured on the phone are correct. If EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST protocols are used, ensure that the certificate uploaded to the phone is valid.
  - a) Double click the certificate to check the validity time.
  - **b)** Check if the time and date on the phone is within the validity time of the uploaded certificate. If not, re-generate a certificate and upload it the phone.
- Ensure that the failure is not caused by network settings.
  - a) Disable LLDP feature and manually configure a VLAN ID for the Internet port of the phone to check if the authentication is successful. If the phone is authenticated successfully, contact your network administrator to troubleshoot the LLDP-related problem.
  - b) Disable VLAN feature on the phone to check if the authentication passes successfully.
     If the phone is authenticated successfully, capture the packet and feed back to your

network administrator.

- Contact Yealink FAE for support when the above steps cannot solve your problem.
  - **a)** Capture the packet and export configurations of the phone, switch and authentication server.
  - b) Provide the related information to Yealink FAE.

# **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.

**802.1X** – A port-based network access control, meaning it only provides an authentication mechanism for devices wishing to attach to a LAN.

**EAP** (Extensible Authentication Protocol) –An authentication framework which supports multiple authentication methods.

**TLS** (Transport Layer Security) –Provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

**MD5** (Message-Digest Algorithm) –Only provides authentication of the EAP peer for the EAP server but not mutual authentication.

**PEAP** (Protected Extensible Authentication Protocol) –A protocol that encapsulates the EAP within an encrypted and authenticated TLS tunnel.

**MSCHAPv2** (Microsoft Challenge Handshake Authentication Protocol version 2) –Provides for mutual authentication, but does not require a supplicant-side certificate.

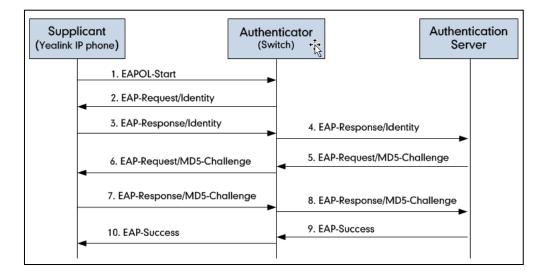
**TTLS** (Tunneled Transport Layer Security) -Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

**EAPOL** (Extensible Authentication Protocol over Local Area Network) –A delivery mechanism and doesn't provide the actual authentication mechanisms.

# **Appendix B: 802.1X Authentication Process**

## A Successful Authentication Using EAP-MD5 Protocol

The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-MD5 protocol.

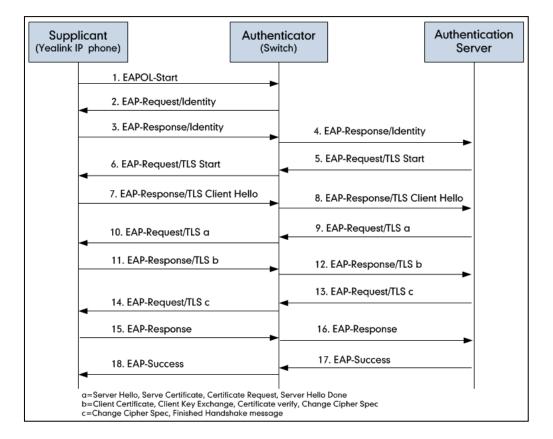


- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
- **5.** The authentication server recognizes the packet as an EAP-MD5 type and sends back a Challenge message to the authenticator.
- **6.** The authenticator strips the authentication server's frame header, encapsulates the remaining EAP frame into the EAPOL format, and sends it to the supplicant.
- 7. The supplicant responds to the Challenge message.
- 8. The authenticator passes the response to the authentication server.
- **9.** The authentication server validates the authentication information and sends an authentication success message.
- 10. The authenticator passes the successful message to the supplicant.

After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message onto the supplicant and blocks access to the LAN.

If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

## A Successful Authentication Using EAP-TLS Protocol



The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-TLS protocol.

- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
- **5.** The authentication server recognizes the packet as an EAP-TLS type and sends an "EAP-Request" packet with a TLS start message to the authenticator.
- **6.** The authenticator strips the authentication server's frame header, encapsulates the remaining EAP frame in the EAPOL format, and then sends it to the supplicant.
- 7. The supplicant responds with an "EAP-Response" packet containing a TLS client hello handshake message to the authenticator. The client hello message includes the TLS version supported by the supplicant, a session ID, a random number and a set of cipher suites.
- 8. The authenticator passes the response to the authentication server.
- **9.** The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes a TLS server hello handshake message, a server certificate message, a certificate request message and a server hello done message.
- **10.** The authenticator passes the request to the supplicant.

- **11.** The supplicant responds with an "EAP-Response" packet to the authenticator. The packet includes a TLS change cipher spec message, a client certificate message, a client key exchange message and a certificate verify message.
- **12.** The authenticator passes the response to the authentication server.
- **13.** The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes a TLS change cipher spec message and a finished handshake message. The change cipher spec message is sent to notify the authenticator that subsequent records will be protected under the newly negotiated cipher spec.
- 14. The authenticator passes the request to the supplicant.
- 15. The supplicant responds with an "EAP-Response" packet to the authenticator.
- **16.** The authenticator passes the response to the authentication server.
- **17.** The authentication server responds with a success message indicating the supplicant and the authentication server have successfully authenticated each other.
- 18. The authenticator passes the message to the supplicant.

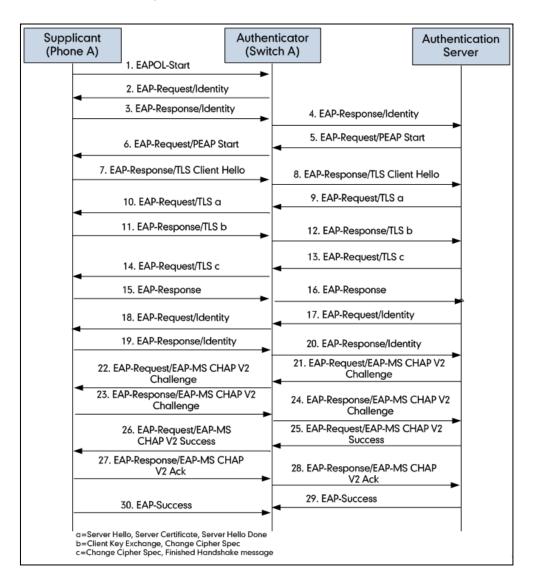
After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to the LAN.

If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

## A Successful Authentication Using EAP-PEAP/MSCHAPv2

#### Protocol

The following figure illustrates the scenario of a successful 802.1X authentication process using the EAP-PEAP/MSCHAPv2 protocol.



- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
- **5.** The authentication server recognizes the packet as a PEAP type and sends an "EAP-Request" packet with a PEAP start message to the authenticator.
- **6.** The authenticator strips the authentication server's frame header, encapsulates the remaining EAP frame in the EAPOL format, and then sends it to the supplicant.

- 7. The supplicant responds with an "EAP-Respond" packet containing a TLS client hello handshake message to the authenticator. The TLS client hello message includes TLS version supported by the supplicant, a session ID, a random number and a set of cipher suites.
- 8. The authenticator passes the respond to the authentication server.
- **9.** The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes a TLS server hello handshake message, a server certificate message and a server hello done message.
- 10. The authenticator passes the request to the supplicant.
- **11.** The supplicant responds with an "EAP-Response" packet to the authenticator. The packet includes a TLS change cipher spec message and a certificate verify message.
- 12. The authenticator passes the response to the authentication server.
- **13.** The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes a TLS change cipher spec message and a finished handshake message. The change cipher spec message is sent to notify the authenticator that subsequent records will be protected under the newly negotiated cipher spec.
- 14. The authenticator passes the request to the supplicant.
- 15. The supplicant responds with an "EAP-Response" packet to the authenticator.
- **16.** The authenticator passes the response to the authentication server. The TLS tunnel is established.
- 17. The authentication server sends an "EAP-Request/Identity" packet to the authenticator.
- 18. The authenticator passes the request to the supplicant.
- 19. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- 20. The authenticator passes the response to the authentication server.
- **21.** The authentication server sends an "EAP-Request" packet to the authenticator. The packet includes an MSCHAPv2 challenge message.
- 22. The authenticator passes the request to the supplicant.
- 23. The supplicant responds a challenge message to the authenticator.
- 24. The authenticator passes the message to the authentication server.
- **25.** The authentication server sends a success message indicating that the supplicant provides proper identity.
- 26. The authenticator passes the message to the supplicant.
- 27. The supplicant responds with an ACK message to the authenticator.
- 28. The authenticator passes the respond message to the authentication server.
- 29. The authentication server sends a successful message to the authenticator.
- 30. The authenticator passes the message to the supplicant.
  - After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to the LAN.

If the supplicant is disabled or reset after successful authentication, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

# A Successful Authentication Using EAP-TTLS/EAP-MSCHAPv2 Protocol

The 802.1X authentication process using the EAP-TTLS/EAP-MSCHAPv2 protocol is quite similar to that using the EAP-PEAP/MSCHAPv2 protocol. For more information, refer to the network resource.

## A Successful Authentication Using EAP-PEAP/GTC Protocol

The 802.1X authentication process using the EAP-PEAP/GTC protocol is quite similar to that using the EAP-PEAP/MSCHAPv2 protocol. For more information, refer to the network resource.

#### A Successful Authentication Using EAP-TTLS/EAP-GTC Protocol

The 802.1X authentication process using the EAP-TTLS/EAP-GTC protocol is quite similar to that using the EAP-PEAP/MSCHAPv2 protocol. For more information, refer to the network resource.

## A Successful Authentication Using EAP-FAST Protocol

The 802.1X authentication process using the EAP-FAST protocol is quite similar to that using the EAP-PEAP/MSCHAPv2 protocol. For more information, refer to the network resource.

# **Customer Feedback**

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