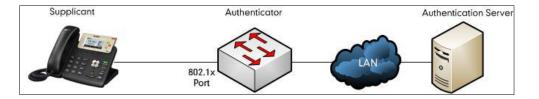
About 802.1X

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.

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

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

Authentication Protocol	IP Phone Models	Firmware Version
	T58A T49G, T40P, T29G, 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
	T58A T49G, T40P, T29G, 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, W60P and CP920	Firmware version 81 or later
	W53P and CP930W-Base	Firmware version 83 or later
	T46G, T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
EAP-TTLS/EAP-MSCHAPv2	T58A T49G, T40P, T29G, 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, W60P and CP920	Firmware version 81 or later
	W53P and CP930W-Base	Firmware version 83 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-PEAP/GTC	T58A T49G, T40P, T29G, 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, W60P and CP920	Firmware version 81 or later

Authentication Protocol	IP Phone Models	Firmware Version
	W53P and CP930W-Base	Firmware version 83 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-TTLS/EAP-GTC	T58A T49G, T40P, T29G, 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, W60P and CP920	Firmware version 81 or later
	W53P and CP930W-Base	Firmware version 83 or later
EAP-FAST	T58A T29G, 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, W60P and CP920	Firmware version 81 or later
	W53P and CP930W-Base	Firmware version 83 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.

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. 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-T58A/CP960 IP phones running firmware version 80 or later
- SIP-T54S/T52S/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T2 3P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later
- W53P and CP930W-Base IP phones running firmware version 83 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.		
0-Disabled		
1-EAP-MD5		
2-EAP-TLS		
3-EAP-PEAP/MSCHAPv2		
4 -EAP-TTLS/EAP-MSCHAPv2		
5-EAP-PEAP/GTC		
6-EAP-TTLS/EAP-GTC		
7 -EAP-FAST		
Note: 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	٦.	
Note : It works only if the value of the parameter "r	network.802 1x.mode" is set t	to 1, 2, 3, 4,
5, 6 or 7. If you change this parameter, the IP phon 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	Blank
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	will reboot to make the chan	ge take
effect.		
Web User Interface:		
Network->Advanced->802.1x->MD5 Password		
Phone User Interface:		
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x
Settings->MD5 Password		
	URL within 511	Blank
network.802_1x.root_cert_url	characters	ыапк
Description:		
Configures the access URL of the CA certificate.		
Note: It works only if the value of the parameter "r	network.802_1x.mode" is set t	to 2, 3, 4, 5,
	*.crt, *.cer or *.der.	
6 or 7. The format of the certificate must be *.pem,		
6 or 7. The format of the certificate must be *.pem, Web 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		
Note : 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.		
0 -EAP-None		
1 -EAP-MD5		
2 -EAP-TLS		
3 -EAP-PEAP/MSCHAPv2		
4-EAP-TTLS/EAP-MSCHAPv2		
5-EAP-PEAP/GTC		
6-EAP-TTLS/EAP-GTC		
7 -EAP-FAST		
If it is set to 0 (EAP-None), 802.1x authentication is no	t required.	
Note: If you change this parameter, the IP phone will effect.	reboot to make the chang	e take
Web User Interface:		
Network->Advanced->802.1x->802.1x Mode		
Phone User Interface:		
Menu->Settings->Advanced Settings (default passwo ->Network->802.1x->802.1x Mode	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	EAP-FAST.	
0-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-Ba authenticated PAC provisioning using certificate based		by serve
Note: It works only if the value of the parameter "stat (EAP-FAST). If you change this parameter, the IP phon take effect.		
Web User Interface:		
Notwork > Advanced > 802.1x > Provisioning Mode		

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.	
Note: 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.		
Note : 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.		
Note : It works only if the value of the parameter "stati 3, 4, 5, 6 or 7. If you change this parameter, the IP photake effect.		
Web User Interface:		

Parameters	Permitted Values	Default
Network->Advanced->802.1x->MD5 Password		
Phone User Interface:		
Menu->Settings->Advanced Settings (default passwo ->Network->802.1x->MD5 Password	rd: admin)	
static.network.802_1x.root_cert_url	URL within 511 characters	Blank
Description:		
Configures the access URL of the CA certificate.		
Note : It works only if the value of the parameter "stati 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	T, you also need to set th on_mode" to 1 (Authentic	e value of
Web User Interface:		
Network->Advanced->802.1x->CA Certificates		
Phone User Interface:		
None		
static.network.802_1x.client_cert_url	URL within 511 characters	Blank
Description:		
Configures the access URL of the device certificate.		
Note: It works only if the value of the parameter "stati	c.network.802_1x.mode" i	
		is set to 2
(EAP-TLS). The format of the certificate must be *.pem		is set to 2
(EAP-TLS). The format of the certificate must be *.pem Web User Interface:		is set to 2
		is set to 2
Web User Interface:		s set to 2
Web User Interface: Network->Advanced->802.1x->Device Certificates		is set to 2
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface:	0 or 1	is set to 2
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None		
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None static.network.802_1x.proxy_eap_logoff.enable	0 or 1	
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None static.network.802_1x.proxy_eap_logoff.enable Description:	0 or 1	
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None static.network.802_1x.proxy_eap_logoff.enable Description: Enables or disables the 802.1x-logoff feature for the Personal Person	0 or 1	
Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None static.network.802_1x.proxy_eap_logoff.enable Description: Enables or disables the 802.1x-logoff feature for the P 0-Disabled	0 or 1 C port.	0

Parameters	Permitted Values	Default
None		
Phone User Interface:		
None		

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
static.network.802_1x.proxy_eap_logoff.enable = 1

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., y00000000000.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 the latest Auto Provisioning Guide for your phone on Yealink Technical Support.
- 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.
- 2) Enter the password for authentication in the **MD5 Password** field.

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

- 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.
 - 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 DSSKey Features Settings Directory Network Security LLDP NOTE Basic Active Enabled PC Port VLAN It is used to logically divide a Packet Interval (1~3600s) 60 It 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. NAT CDP Active Disabled Advanced -Packet Interval (1~3600s) 60 The priority of VLAN assignment method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN 802.1x NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STUN is one of the NAT traversal techniques. 802.1x Mode EAP-TLS • Provisioning Mode Unauthenticated Provisic -Anonymous Identity Anonymous Identity yealink You can configure NAT traversal for the IP phone. MD5 Password Browse... Quality of Service (QoS) It is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements. CA Certificates Upload Browse... Device Certificates Upload Confirm Cance
- 5) In the **Device Certificates** field, click **Browse** to select the desired client (*.pem or *.cer) certificate from your local system.

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

ealink 1236	Status Aco	ount Network DS	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
nuvunccu		Packet Interval (1~3600s)	60		through software instead of physically relocating devices or
		r adicerintervar (1 30003)	00		connections.
		:			The priority of VLAN assignment method (from highest to lowest) :LLDP/CDP->manual
		÷			method (from highest to
	802.1x	÷			method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal
	802.1x	802.1x Mode	EAP-PEAP/MSCHAPv2	-	method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN
	802.1x	802.1x Mode Provisioning Mode	EAP-PEAP/MSCHAPv2 Unauthenticated Provisic		method (from highest to lowest):LLDP/CDP>manual configuration>DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections
	802.1x		Unauthenticated Provisic		method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STU is one of the NAT traversal
	802.1x	Provisioning Mode Anonymous Identity	Unauthenticated Provisic		method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STU
	802.1x	Provisioning Mode Anonymous Identity Identity	Unauthenticated Provisic Anonymous yealink		method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintan IP connections traversing NAT gateways. STU is one of the NAT traversal techniques. You can configure NAT travers
	802.1x	Provisioning Mode Anonymous Identity	Unauthenticated Provisic	-	method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STU is one of the NAT traversal techniques. You can configure NAT travers for the IP phone.
	802.1x	Provisioning Mode Anonymous Identity Identity	Unauthenticated Provisic Anonymous yealink		lowest): LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STU is one of the NAT traversal techniques. You can configure NAT travers for the IP phone. Quality of Service (QoS)
	802.1x	Provisioning Mode Anonymous Identity Identity MDS Password	Unauthenticated Provisic Anonymous yealink	-	method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways. STU is one of the NAT traversal techniques. You can configure NAT travers for the IP phone.

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

Yealink 1236	Status	nt Network DS	SKey Features Setting	Log Out English(English) - S Directory Security
Basic PC Port NAT Advanced	LTDb CDb	Active Packet Interval (1~3600s) Active Packet Interval (1~3600s)	Enabled • 60 Disabled • 60	NOTE VLAN It 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. The priority of VLAN assignment method (from highest to lowest) iLDP/CDP-manual
	802.1x	802.1x Mode Provisioning Mode Anonymous Identity Identity MD5 Password CA Certificates Device Certificates Confirm	EAP-TTLS/EAP-MSCHAP Unauthenticated Provisic Anonymous yealink upload Browse Upload Cancel	configuration->DHCP VLAN NAT Traversal It is a general term for techniques that establish and maintain IP connections traversing NAT gateways, STUN is one of the NAT traversal techniques. You can configure NAT traversal for the IP phone. Quality of Service (QoS) It is the ability to provide different priorities for different packets in the network, allowing the transport of traffic with special requirements.

- 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.

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

Network DSS Active Packet Interval (1~3600s) Active Packet Interval (1~3600s)	SKey Features Enabled 60 Disabled 60	Settings	Directory Security NOTE VLAN It is used to logically divide a physical network into severa broadcast domains. VLAN membership can be configur through software instead of
Packet Interval (1~3600s) Active	60 Disabled	•	VLAN It is used to logically divide a physical network into severa broadcast domains. VLAN membership can be configur
Packet Interval (1~3600s) Active	60 Disabled	•	It is used to logically divide a physical network into severa broadcast domains. VLAN membership can be configur
Active	Disabled	•	It is used to logically divide a physical network into severa broadcast domains. VLAN membership can be configur
		•	broadcast domains. VLAN membership can be configur
		-	
Packet Interval (1~3600s)	60		
			physically relocating devices connections.
			The priority of VLAN assignmethod (from highest to
:			lowest) :LLDP/CDP->manual configuration->DHCP_VLAN
			NAT Traversal
802.1x Mode	EAP-PEAP/GTC	•	It is a general term for
Provisioning Mode	Unauthenticated Provisic	-	techniques that establish an maintain IP connections
			traversing NAT gateways. S [*] is one of the NAT traversal
		-	techniques.
			You can configure NAT trave for the IP phone.
MDD Passworu		[Pressure]	
CA Certificates	Upload	browse	Quality of Service (QoS) It is the ability to provide
		Browse	different priorities for different packets in the network, allowing the transport of trai
	Provisioning Mode Anonymous Identity Identity MD5 Password CA Certificates Device Certificates	Anonymous Identity Anonymous Identity yealink MD5 Password CA Certificates Upload	Anonymous Identity Anonymous Identity yealink MD5 Password CA Certificates Upload Browse Upload Browse

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.

				<u></u>				
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basic	LLDF	,					NOTE	
PC Port			Active	Ena	pled	•	VLAN	
POPUL			Packet Interval (1~36	i00s) 60			It is used to lo	
NAT	CDP						physical netwo broadcast dom	ains. VLAN
Advanced			Active	Disa	bled	-	membership ca through softwa	in be configured are instead of
			Packet Interval (1~36	i00s) 60			physically relocations.	ating devices or
							N	
							method (from	
			:				lowest) :LLDP/ configuration->	
	802	.1x					NAT Traversal	
			802.1x Mode	EAF	-TTLS/EAP-GTC	-	It is a general t techniques that	term for
					and all the second second second			
			Provisioning Mode	110	uthenticated Provisi	- - - -	maintain IP cor	
			Provisioning Mode		uthenticated Provisi	*	traversing NAT is one of the N	gateways. STU
			Anonymous Identity	And	nymous	*	traversing NAT	gateways. STU
			Anonymous Identity Identity	And yea	nymous ink		traversing NAT is one of the N techniques. You can config	gateways. STU IAT traversal Jure NAT travers
			Anonymous Identity	And yea	nymous		traversing NAT is one of the N techniques. You can config for the IP phor	gateways. STU IAT traversal Jure NAT travers ne.
			Anonymous Identity Identity	Anc yea	nymous ink	Browse	traversing NAT is one of the N techniques. You can config for the IP phor Quality of Ser It is the ability	gateways. STU IAT traversal nure NAT travers ne. rvice (QoS) to provide
			Anonymous Identity Identity MD5 Password	Anc yea	nymous ink		traversing NAT is one of the N techniques. You can config for the IP phor Quality of Ser It is the ability	gateways. STU IAT traversal Iure NAT travers ne. rvice (QoS) to provide ties for different

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

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

Manthala			_	_	Log Out English(English) -
Yealink 1236	Status	Network DSS	Key Features	Settings	Directory Security
Basic	LLDP				NOTE
PC Port		Active Packet Interval (1~3600s)	Enabled 60	-	VLAN
NAT	CDP	Tackerinkeivar(1 36003)	00		It is used to logically divide a 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
	802.1x				configuration->DHCP VLAN
		802.1x Mode	EAP-FAST	•	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 MD5 Password	yealink		You can configure NAT traversal for the IP phone.
		CA Certificates	Upload	Browse	Quality of Service (QoS) It is the ability to provide
		Device Certificates	Upload	Browse	different priorities for different packets in the network, allowing the transport of traffic with special requirements.
	C	Confirm	Cancel		Wah Saniar Tuna

- 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.

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.

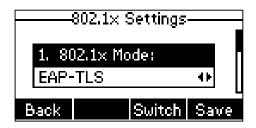
The following takes a SIP-T23G IP phone running firmware version 81 as an example.

To configure 802.1x via phone user interface:

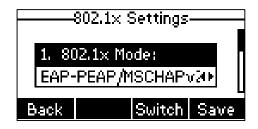
- Press Menu->Settings->Advanced Settings (default password: admin)
 ->Network->802.1x.
- Press (•) or (•), or the Switch soft key to select the desired value from the 802.1x
 Mode field.
 - a) If you select EAP-MD5:

	802.1× Settings	;
1. 80)2.1× Mode:	
EAP-	MD5	41
Back	Switch	Save

- 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:

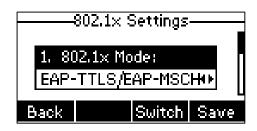


- 1) Enter the user name for authentication in the Identity field.
- 2) Leave the MD5 Password field blank.
- c) If you select EAP-PEAP/MSCHAPv2:

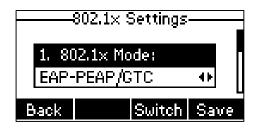


- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.

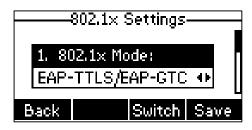
d) If you select EAP-TTLS/EAP-MSCHAPv2:



- 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:

	802.1× Setting)S
1. 80)2.1x Mode:	
EAP	FAST	41
Back	Swite	h Save

- 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

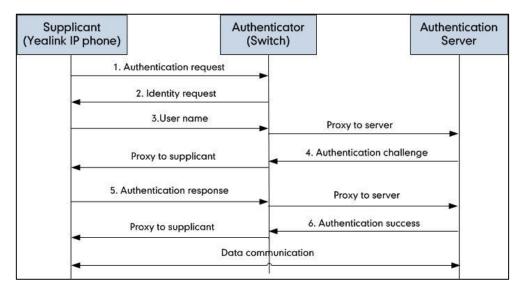
Reboot the phone to activate the 802.1X authentication on the phone. The 802.1X authentication process is divided into two basic stages:

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 a RADIUS server as the authentication server:



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.

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:

Eile Edit View Go	shark 1.10.5 (SVN Rev 5426) Capture Analyze Statistics	Telephony	ools Inter		
•• ▲ ■ ፈ	🕒 🗎 🗶 🔁 🔍 🍝	🌼 🤪 茶		∃ 0, 0, 0, 17 ¥ M 🥵 % 13	
Filter: eap eapol			▼ Đ	xpression 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	
<[m	
				(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 fr	om /trunk-1.10)]	
File Edit View Go Capture Analyze Statistics	Telephony <u>T</u> ools <u>I</u> ntern	als <u>H</u> elp
● ● 💉 🔳 🔬 🖻 🛅 🗙 😂 🔍 🔶	* 4) 7 🕹 🗐	∃ 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		1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Dor
123 17.858234000 xiamenYe_73:4c:f1	Nearest EAP	60 Response, TLS EAP (EAP-TLS)
124 17.867698000 Cisco_5d:42:94		1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Dor
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 Dor
130 18.447360000 XiamenYe_73:4c:f1		1366 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted H
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 H
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. F
<pre> # Frame 118: 60 bytes on wire (480 bits # Ethernet II, Src: XiamenYe_73:4c:f1 (# 802.1X Authentication</pre>		
Version: 802.1X-2001 (1)		
Type: EAP Packet (0)		
Length: 12		
Extensible Authentication Protocol		
Code: Response (2)		
Id: 1		
Length: 12		
Type: Identity (1)		
Identity: yealink		

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 /trun	k-1.10)]	- • •
ile <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Intern	ials <u>H</u> elp	
D 🖲 🔏 📕 🔏	🕒 🗎 🗶 🔁 🔍 🔶	🏟 🥥 👬	1	E) C. C. Q. 🗹 📓 🖉 🅵 % 🔀	
ilter: eap eapol			▼ Exp	pression Clear Apply Save Filter	
o. Time	Source	Destination	Protocol L		
	cisco_5d:42:94	Nearest	EAPOL	60 Start	
10 3.928791000		Nearest	EAP	60 Request, Identity	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
12 3.991711000		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
14 4.004604000		Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	XiamenYe_73:4c:f1	Nearest	TLSV1	116 Client Hello	
17 4.128973000		Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
19 4.138955000		Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
21 4.148933000		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		Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
33 4.797998000		Nearest	TLSV1	61 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
35 4.808518000		Nearest	TLSV1	77 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSV1	162 Application Data, Application Data	
37 4.825426000		Nearest	TLSV1	109 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
39 4.840065000		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	
				III.	
Ethernet II, Sr 802.1X Authenti Version: 802. Type: EAP Pac Length: 12	<pre>c: X1amenYe_73:4c:f1 cation IX-2001 (1) ket (0) thentication Protocol nse (2) ity (1)</pre>			(480 bits) on interface 0 .Dst: Nearest (01:80:c2:00:00:03)	

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	APv2.pcapng [Wireshark 1.1	0.5 (SVN Rev	54262 from ,	/trunk-1.10)]	- • •
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Interna	als Help	
0 (• 🖌 🔳 🔬	🖹 🗂 🗙 🔍 🔶	👳 🥥 🐺	2 🗏 🗄] 0, 0, 0, 11 # M 🥦 % 11	
Filter	: eap eapol			💌 Exp	ression Clear Apply Save Filter	
No.	Time	Source	Destination	Protocol Le	ength Info	
		<pre>xiamenYe_73:4c:f1</pre>	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)	
		<pre>xiamenYe_73:4c:f1</pre>	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	
		<pre>xiamenYe_73:4c:f1</pre>	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	
		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		60 Response, Tunneled TLS EAP (EAP-TTLS)	
40	5.260661000	C15C0_50:42:94	Nearest	EAP	60 Success	
۰					m	+
⊕ Et ⊡ 80	hernet II, Sr 2.1X Authenti Version: 802. Type: EAP Pac Length: 12	c: XiamenYe_73:4c:f1 cation 1X-2001 (1) ket (0)			(480 bits) on interface 0 Dst: Nearest (01:80:c2:00:00:03)	
		thentication Protocol				
	Code: Respo	nse (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-PEAP/GTC protocol:

📕 EA	P-PEAP GTC.pcapn	g [Wireshark 1.10.5 (SVN R	Rev 54262 from	m /trunk-1.10)]	
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Interr	nals Help	
0		🖹 🗎 🗶 🔁 🔍 🔶	* * 7			
	• 🛲 🛲 🙉		** ** '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 xiamenye 73:4c:f1	Nearest	TLSV1 EAP	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 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	FAP	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	
70	13,161368000	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	
110	14.220732000	cisco_5d:42:94	Nearest	EAP	60 Success	
(m	÷
					d (480 bits) on interface O	
	hernet II, Sro 2.1X Authentio		(00:15:65:	73:4c:f1)	, Dst: Nearest (01:80:c2:00:00:03)	
	Version: 802.1					
	Type: EAP Pack					
	Length: 12					
		thentication Protocol				
	Code: Respor					
	Id: 1					
	Length: 12					
	Type: Identi	ity (1)				
- F	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	<u>Capture</u> Analyze Statistics	Telephony	<u>T</u> ools <u>I</u> nter	mals <u>H</u> elp	
D 🛈 🔏 🔳 🖽	🖻 🖺 🗶 🔁 🔍 🗢	👒 🤪 Ŧ	2 🗐	🗐 Q, Q, Q, 🖻 🖉 🕺 🧏 🕱	
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	Nearest	EAP	60 Request, Tunneled TLS EAP (EAP-TTLS)	
	xiamenYe_73:4c:f1	Nearest	TLSV1	112 Client Hello	
	cisco_5d:42:94 XiamenYe_73:4c:f1	Nearest	TLSV1	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	EAP TLSV1	526 Server Hello. Certificate. Server Kev 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	
	xiamenye 73:4c:f1		TLSV1	130 Application Data. Application Data	
	cisco_5d:42:94	Nearest	EAP	60 Success	
				m	
				i (480 bits) on interface 0	
		(00:15:65:	73:4c:f1)	, Dst: Nearest (01:80:c2:00:00:03)	
802.1X Authent					
	2.1x-2001 (1)				
Type: EAP Pa	acket (0)				
Length: 12	Authentication Protocol				
Code: Resp Td: 1	Jonse (2)				
Id: 1 Length: 12					
Type: Ider					

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

eap-fast.pcapng [Wir	reshark 1.10.5 (SVN Rev 54	262 from /trun	k-1.10)]		
le <u>E</u> dit <u>V</u> iew <u>G</u> o <u>(</u>	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp	
0 0 🗸 🗰 🖉	🖹 🖀 🗙 🛃 🔍 🔶	🔹 🥥 🐺	4 🗐	🗐 Q Q Q 🔟 📓 🗹 🍕 💥 🗒	
ilter: eap eapol			- E	xpression Clear Apply Save Filter	
o. Time	Source	Destination	Protocol	Length Info	
	xiamenye_45:6f:bb	Nearest	EAPOL	60 Start	
257 20.039456000		Nearest	EAP	60 Request, Identity	
	XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity	
259 20.057032000		Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
261 20.065574000		Nearest	TLSV1	60 Ignored Unknown Record	
	XiamenYe_45:6f:bb	Nearest	TLSV1	80 Client Hello	
264 20.150405000		Nearest	TLSV1	1030 Server Hello, Certificate, Certificate Request, Server Hello Done	
	XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)	
266 20.162252000		Nearest	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	
270 20.305528000		Nearest	TLSV1	109 Change Cipher Spec, Encrypted Handshake Message, Application Data	
	XiamenYe_45:6f:bb	Nearest	TLSV1	63 Application Data	
72 20.348633000		Nearest	TLSV1	87 Application Data	
	XiamenYe_45:6f:bb	Nearest	TLSV1	83 Application Data	
274 20.359229000		Nearest	TLSV1	115 Application Data	
	XiamenYe_45:6f:bb	Nearest	TLSV1	131 Application Data	
276 20.372628000		Nearest	TLSV1	279 Application Data	
77 20.382206000	XiamenYe_45:6f:bb	Nearest	TLSV1	65 Application Data	
				m	,
				ed (480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
	learest (01:80:c2:00:		+3.01.00)	, DSL. Near ESE (01.00.12.00.00.05)	
	Ye_45:6f:bb (00:15:6)		
	uthentication (0x888				
	000000000000000000000000000000000000000		000000000000000000000000000000000000000	19999	
802.1X Authentic	ation				
version: 802.1	X-2001 (1)				
Type: EAP Pack	et (0)				
Length: 10					
Extensible Aut	hentication Protocol				
Code: Respon	ise (2)				
Id: 1					
Length: 10					
Type: Identi					
Identity: ye	alink				

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:

	Vireshark 1.10.5 (SVN Rev 54262		
<u>File Edit V</u> iew	Go Capture Analyze Statistics	Telephony	Tools Internals Help
0 0 🖌 📕	🧟 🖹 🖹 🗶 🔍 🗢	🔹 🥥 👬	사 🗐 🕞 🔍 이 이 🔄 🐺 🖾 🍕 💥 💢
Filter: eap eap	bl		Expression Clear Apply Save Filter
No. Time	Source	Destination	
	3000 Cisco_5d:42:94	Nearest	EAPOL 60 Start
	5000 Cisco_5d:42:94	Nearest	EAP 60 Request, Identity
	0000 XiamenYe_73:4c:f1	Nearest	EAP 60 Response, Identity
	0000 C1sco_5d:42:94	Nearest	EAP 60 Request, TLS EAP (EAP-TLS) TLSV1 112 Client Hello
	LOOO XiamenYe_73:4c:f1 DOOO Cisco 5d:42:94	Nearest	
	1000 Cisco_5d:42:94	Nearest Nearest	TLSv1 1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hel
	3000 cisco_5d:42:94	Nearest	EAP 60 Response, TLS EAP (EAP-TLS) TLSV1 1042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hel
	3000 Cisco_30:42:94 3000 XiamenYe_73:4c:f1	Nearest	EAP 60 Response. TLS EAP (EAP-TLS)
	3000 Cisco_5d:42:94	Nearest	
	000 XiamenYe_73:4c:f1	Nearest	TLSVI 1366 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encry
	1000 Cisco_5d:42:94	Nearest	EAP 60 Request. TLS EAP (EAP-TLS)
	3000 XiamenYe 73:4c:f1	Nearest	TLSV1 827 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encry
	L000 Cisco 5d:42:94	Nearest	TLSV1 87 Change Cipher Spec, Encrypted Handshake Message
134 18.487070	0000 xiamenYe_73:4c:f1	Nearest	EAP 60 Response, TLS EAP (EAP-TLS)
146 19.51681	5000 cisco_5d:42:94	Nearest	EAP 60 Success
4			II
× L			
			es captured (480 bits) on interface 0
Ethernet II 802.1X Auth		(00:15:65:	73:4c:f1), Dst: Nearest (01:80:c2:00:00:03)
	entication 802.1X-2001 (1)		
	Packet (0)		
Length: 1			
	2 e Authentication Protoco		
	esponse (2)		
Id: 1	eshouse (e)		
Length:	12		
	dentity (1)		
	y: Anonymous		

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

🗲 EAP-PEAP MSCHPv2.pcapng [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]							
<u>File E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	<u>T</u> ools <u>I</u> nterr	nals <u>H</u> elp			
0 🖲 🛋 🗮 🔬	🖻 🖺 🗶 😂 I 🔍 🔶	🔶 🥥 🖗	2 🗉	∃ Q, Q, Q, 17 ¥ ⊠ 18 % \$			
Filter: eap eapol			▼ Ex	pression Clear Apply Save Filter			
lo. Time	Source	Destination		ength Info			
	cisco_5d:42:94	Nearest	EAPOL	60 Start			
10 3.928791000		Nearest	EAP	60 Request, Identity			
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity			
12 3.991711000		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)			
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Legacy Nak (Response Only)			
14 4.004604000		Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)			
	XiamenYe_73:4c:f1	Nearest	TLSV1	116 Client Hello			
17 4.128973000		Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)			
19 4.138955000		Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)			
21 4.148933000		Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message			
31 4.779122000		Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message			
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)			
33 4.797998000		Nearest	TLSV1	61 Application Data			
34 4.800342000 35 4.808518000	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data			
		Nearest	TLSV1	77 Application Data			
36 4.81803/000 37 4.825426000	xiamenYe_73:4c:f1	Nearest	TLSV1 TLSV1	162 Application Data, Application Data 109 Application Data			
		Nearest					
39 4.840065000	xiamenYe_73:4c:f1	Nearest	TLSV1 TLSV1	98 Application Data, Application Data 61 Application Data			
	xiamenye 73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data			
56 5.877757000		Nearest	EAP	60 Success			
30 3.8///3/000	C15C0_30:42:94	Nearest	EAP				
				II			
<pre>Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet II, src: Xiamerwe_73:4c:f1 (00:15:65:73:4c:f1), Dst: Nearest (01:80:c2:00:00:03) 802.1X Authentication Version: 802.1X-2001 (1) Type: LAP Packet (0) Length: 12 Extende 10 Authentication Protocol Odd: 1 Length: 12 Type: L4P Line 12 Type: L4P Line 14 Type: L4</pre>							

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

EAP-TTLS EAP-MSCHAPv2.pcapng (Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10))								
		Capture Analyze Statistics						
0 () 🧸 🔳 🙇	🕒 🗎 🗶 🤁 🛛 🔍 🔶	🌳 🏟 ዥ	2	∃ 0, 0, 0, 11 ₩ M 🥵 % 💢			
Filter: eap eapol								
No.		Source	Destination	Protocol	Length 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			
		C1SC0_5d:42:94	Nearest	EAP	60 REQUEST, ILS 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				
		cisco_5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
		xiamenYe_73:4c:f1 Cisco 5d:42:94	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS)			
			Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
		XiamenYe_73:4c:f1 Cisco_5d:42:94	Nearest	EAP	60 Response, Tunneled TLS EAP (EAP-TTLS) 526 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
		Cisco_5d:42:94 XiamenYe_73:4c:f1	Nearest	TLSV1 TLSV1				
		cisco_5d:42:94	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 87 Change Cipher Spec, Encrypted Handshake Message			
		XiamenYe 73:4c:f1	Nearest	TLSV1	210 Application Data, Application Data			
		Cisco 5d:42:94	Nearest	TLSV1	113 Application Data			
		XiamenYe 73:4c:f1	Nearest	FAP	60 Response, Tunneled TLS EAP (EAP-TTLS)			
		cisco 5d:42:94	Nearest	EAP	60 Success			
40	5.200001000	01300_30.42.34	Near esc	EAP	00 Success			
<						,		
Eti 802	hernet II, Sr 2.1X Authenti	c: XiamenYe_73:4c:f1 cation			(480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)			
	version: 802.							
	Type: EAP Pac	ket (0)						
	Length: 12							
		thentication Protocol						
	Code: Respo	nse (2)						
	Id: 1							
	Length: 12	in. (1)						
	Type: Ident							
	Identity: A	nonyillous						

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 F	Rev 54262 fro	m /trunk-1.10)]	- • •
<u>Eile</u>	<u>Edit V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Interr	nals <u>H</u> elp	
0.6		🖹 🗎 🗶 🔁 🛛 🔍 🔶	* * *	2	s) d d @ 🖸 📓 🛛 🍓 💥 🛛	
00	•		·· ·• U			
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 xiamenye 73:4c:f1	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 60 Response, Protected EAP (EAP-PEAP)	
			Nearest	EAP	50 Response, Protected EAP (EAP-PEAP) 522 Server Hello. Certificate. Server Key Exchange. Server Hello Done	
		Cisco_5d:42:94	Nearest	TLSV1	222 Server Hello, Certificate, Server Key Exchange, Server Hello Done 226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		XiamenYe_73:4c:f1 Cisco_5d:42:94	Nearest	TLSV1 TLSV1		
		XiamenYe 73:4c:f1	Nearest	FAP	83 Change Cipher Spec, Encrypted Handshake Message	
		cisco 5d:42:94			60 Response, Protected EAP (EAP-PEAP)	
		XiamenYe 73:4c:f1	Nearest Nearest	TLSV1 TLSV1	61 Application Data 98 Application Data, Application Data	
		cisco_5d:42:94	Nearest	TLSV1 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	
		XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		Cisco_5d:42:94	Nearest	FAP	60 Success	
	14.2207 52000	01300_30.42.34	Near ese	EAF		
۰					m	+
					d (480 bits) on interface 0	
	nernet II, Sro 2.1X Authentio		(00:15:65:	73:4c:f1)	, Dst: Nearest (01:80:c2:00:00:03)	
	/ersion: 802.1					
	Type: EAP Pack					
	enoth: 12	ket (0)				
		thentication Protocol				
	Code: Respor					
	Id: 1					
	Length: 12					
	Type: Ident:	ity (1)				
	Identity: A					
	zachercy: A					

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

E E	AP-TTLS EAP-GTC .	pcapng [Wireshark 1.10.5 (S	VN Rev 54262	2 from /trun	k-1.10)			
_		Capture Analyze Statistics						
-								
θ	• 🛋 💻 🔬	🖻 🖩 🕷 😂 I 🔍 🔶	** એ 🚯		∃ 0, 0, 0, 11 ¥ M ⁶ , % X			
Filte	r: eap eapol			▼ Ex	pression 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 XiamenYe 73:4c:f1	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)			
		Cisco 5d:42:94	Nearest Nearest	EAP	60 Response, Legacy Nak (Response Only) 60 Request, Tunneled TLS EAP (EAP-TTLS)			
		Cisco_50:42:94 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	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			
34	4 3,957962000	cisco 5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message			
3	5 3.966814000	XiamenYe_73:4c:f1	Nearest	TLSV1	114 Application Data, Application Data			
3	5 3.976751000	cisco_5d:42:94	Nearest	TLSV1	97 Application Data			
		xiamenYe_73:4c:f1	Nearest	TLSV1	130 Application Data, Application Data			
4	8 5.011940000	cisco_5d:42:94	Nearest	EAP	60 Success			
					m			
E E		c: xiamenye_73:4c:f1 cation 1x-2001 (1)			(480 bits) on interface 0 , DSt: Nearest (01:80:c2:00:00:03)			
		thentication Protocol						
	Code: Respo							
	Td: 1	136 (2)						
	Length: 12							
		ity (1)						
	Type: Identity (1) Identity: Anonyous							
	identity. Anonymous							

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

🗲 ea	p-fast.pcapng [W	/ireshark 1.10.5 (SVN Rev 54	1262 from /trur	nk-1.10)]	
Eile	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp
0	• 🛋 🔳 🔬	🖻 🖺 🗶 🍠 🔍 🔶	🌸 🥥 😚	2	B) Q, Q, Q, 17 👹 18 🥵 % 💢
Filter	eap eapol			▼ Đ	xpression Clear Apply Save Filter
	Time	Source	Destination	Protocol	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	Nearest	TLSV1	80 Client Hello
		cisco_5d:42:94	Nearest	TLSV1	1030 Server Hello, Certificate, Certificate Request, Server Hello Done
		xiamenYe_45:6f:bb	Nearest	EAP	60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
		Cisco_5d:42:94	Nearest	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
316	27.641334000	XiamenYe_45:6f:bb	Nearest	TLSV1	65 Application Data
					III .
Fr	ame 299: 60 by	ytes on wire (480 bit	s), 60 byte	es captur	ed (480 bits) on interface 0
			(00:15:65:4	15:6f:bb)	, Dst: Nearest (01:80:c2:00:00:03)
	2.1X Authentic				
	version: 802.1	1x-2001 (1)			
	Type: EAP Pack	ket (0)			
	Length: 19				
-		thentication Protocol			
	Code: Respor	nse (2)			
	Id: 1				
	Length: 19				
	Type: Ident				
	Identity: A	nonymous			

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.

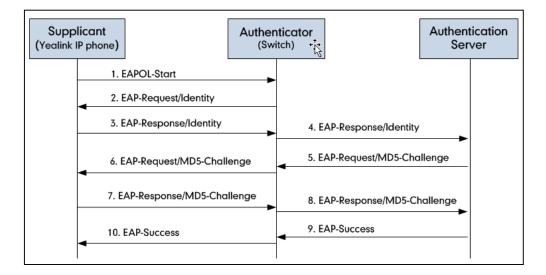
TTLS (Tunneled Transport Layer Security) -Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

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.

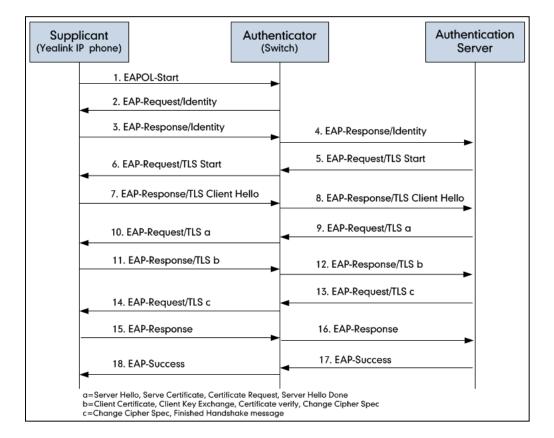


- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header 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.

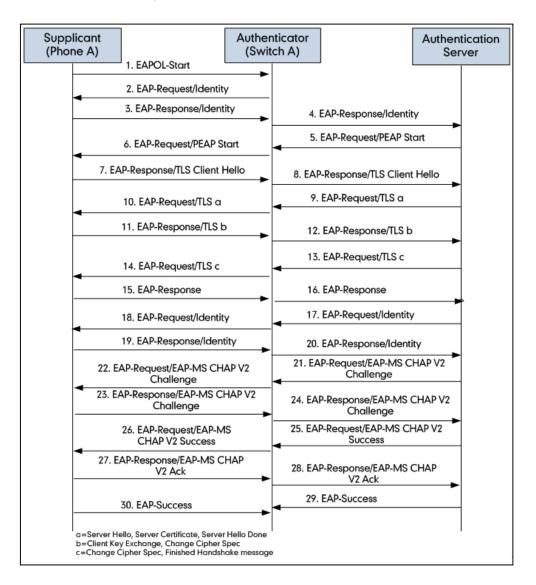
After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to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