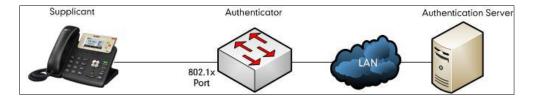
About 802.1X

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
	T58V/A, T56A, 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
	T58V/A, T56A, 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	Firmware version 83 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, 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	Firmware version 83 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-PEAP/GTC	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later

Authentication Protocol	IP Phone Models	Firmware Version
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	Firmware version 81 or later
	W53P	Firmware version 83 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-TTLS/EAP-GTC	T58V/A, T56A, 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	Firmware version 83 or later
EAP-FAST	T58V/A, T56A, 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	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-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/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 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 we ffect.	vill reboot to make the chang	ge take

Parameters	Permitted Values	Default		
Web User Interface:				
Network->Advanced->802.1x->802.1x Mode				
Phone User Interface:				
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x		
Settings->802.1x Mode				
twork.802_1x.identity String within 32 characters				
Description:				
Configures the user name for 802.1x authentication	۱.			
Note: It works only if the value of the parameter "n	network.802_1x.mode" is set t	to 1, 2, 3, 4,		
5, 6 or 7. If you change this parameter, the IP phon	e will reboot to make the cha	ange take		
effect.				
Web User Interface:				
Network->Advanced->802.1x->Identity				
Phone User Interface:				
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x		
Settings->Identity				
network.802_1x.md5_password String within 32 characters Blank				
network.802_1x.md5_password	-	Blank		
network.802_1x.md5_password Description:	-	Blank		
	characters	Blank		
Description:	characters			
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone v	characters	to 1, 3, 4, 5,		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone w effect.	characters	to 1, 3, 4, 5,		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone v effect. Web User Interface:	characters	to 1, 3, 4, 5,		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone v effect. Web User Interface: Network->Advanced->802.1x->MD5 Password	characters	to 1, 3, 4, 5,		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone v effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface:	characters	to 1, 3, 4, 5, ge take		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone v effect. Web User Interface: Network->Advanced->802.1x->MD5 Password	characters	to 1, 3, 4, 5, ge take		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone we effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass	characters	to 1, 3, 4, 5, ge take		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone we effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass Settings->MD5 Password	characters network.802_1x.mode" is set to will reboot to make the change word: admin) ->Network->8 URL within 511	to 1, 3, 4, 5, ge take 02.1x		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone we effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass Settings->MD5 Password network.802_1x.root_cert_url	characters network.802_1x.mode" is set to will reboot to make the change word: admin) ->Network->8 URL within 511	to 1, 3, 4, 5, ge take 02.1x		
Description: Configures the password for 802.1x authentication. Note: It works only if the value of the parameter "n 6 or 7. If you change this parameter, the IP phone we effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass Settings->MD5 Password network.802_1x.root_cert_url Description:	characters network.802_1x.mode" is set to will reboot to make the change word: admin) ->Network->8 URL within 511 characters	to 1, 3, 4, 5, ge take 02.1x Blank		

Parameters Permitted Values Defau				
Web User Interface:				
Network->Advanced->802.1x->CA Certificates				
Phone User Interface:				
None				
	URL within 511			
network.802_1x.client_cert_url	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

1. 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	Defaul
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	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.	
0 -Unauthenticated Provisioning		
1-Authenticated Provisioning		
If it is set to 0 (Unauthenticated Provisioning), EAP In-	Band provisioning is enabl	ed by
server unauthenticated PAC (Protected Access Creden	tial) provisioning using an	onymou
Diffie-Hellman key exchange.		
	nd provisioning is enabled	by serve
-		
authenticated PAC provisioning using certificate based		
If it is set to 1 (Authenticated Provisioning), EAP In-Bar authenticated PAC provisioning using certificate based Note: It works only if the value of the parameter "stat	ic.network.802_1x.mode" is	
authenticated PAC provisioning using certificate based	ic.network.802_1x.mode" is	

Parameters	Permitted Values	Default		
Network->Advanced->802.1x->Provisioning Mode				
Phone User Interface:				
None				
tatic.network.802_1x.anonymous_identity Characters				
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				
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 pho take effect.				

Parameters	Permitted Values	Default				
Web User Interface:	L					
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	tatic.network.802_1x.root_cert_url Characters Blan					
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_provision 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				
Note : It works only if the value of the parameter "static (EAP-TLS). The format of the certificate must be *.pem	_	is set to 2				
<i>,</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				
(EAP-TLS). The format of the certificate must be *.pem Web User Interface: Network->Advanced->802.1x->Device Certificates	_	is set to 2				
(EAP-TLS). The format of the certificate must be *.pem Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface:	_	is set to 2 0				
(EAP-TLS). The format of the certificate must be *.pem Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None						
(EAP-TLS). The format of the certificate must be *.pem Web User Interface: Network->Advanced->802.1x->Device Certificates Phone User Interface: None static.network.802_1x.proxy_eap_logoff.enable	0 or 1					
(EAP-TLS). The format of the certificate must be *.pem 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					
(EAP-TLS). The format of the certificate must be *.pem 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 Press	0 or 1					
(EAP-TLS). The format of the certificate must be *.pem 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 Pro- 0-Disabled	0 or 1 C port.	0				

Parameters	Permitted Values	Default
Web User Interface:		
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., y0000000000000.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 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.

Yealink 1236					Log Out English(English) -
	Status Account	Network DSS	Key Features	Settings	Directory Security
Basic PC Port NAT Advanced	LLDP CDP	Active Packet Interval (1~3600s) Active Packet Interval (1~3600s)	Enabled - 60 Disabled - 60		NOTE VLAI It is used to logically divide a physical network into several broadcast domans. VLAN membership can be configured through software instead of physically relocating devices or connections.
	802.1x	÷			The priority of VLAN assignment method (from highest to lowest) :LLDP/CDP->manual configuration->DHCP VLAN
		802.1x Mode	EAP-MD5	1	NAT Traversal It is a general term for
		Provisioning Mode Anonymous Identity	Unauthenticated Provisic *	-	techniques that establish and maintain IP connections traversing NAT gateways. STUN is one of the NAT traversal
		Identity	yealink	1	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 with special requirements.
	C	Confirm	Cancel		Wah Sarrier Type

- 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 Cancel Confirm
- 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					Log O English(English)
	Status Acco	ount Network DS	SKey Features	Settings	Directory Security
Basic	LLDP				NOTE
PC Port		Active	Enabled	•	VLAN
PC POIL		Packet Interval (1~3600s)	60		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				
		802.1x Mode	EAP-PEAP/MSCHAPv2	_	NAT Traversal It is a general term for
		Provisioning Mode	Unauthenticated Provisic		techniques that establish and maintain IP connections
		-		*	traversing NAT gateways. STU
		Anonymous Identity	Anonymous		techniques.
		Identity	yealink		You can configure NAT travers
		MD5 Password	•••••		for the IP phone.
		CA Certificates		Browse	Quality of Service (QoS)
			Upload	Deriver	It is the ability to provide different priorities for different
		Device Certificates	Upload	Browse	packets in the network, allowing the transport of traffic
					with special requirements.
		Confirm	Cancel		Web Server Type

- 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.

ealink 1236					Log Ot English(English)
Centrix (1256	Status	ount Network DS	SKey Features	Settings	Directory Security
Basic	LLDP				NOTE
PC Port		Active Packet Interval (1~3600s)	Enabled •		VLAN It is used to logically divide a
NAT	CDP	Active	Disabled 👻		physical network into several broadcast domains. VLAN membership can be configured
Advanced		Packet Interval (1~3600s)	60		through software instead of physically relocating devices or connections.
		•			The priority of VLAN assignmer method (from highest to lowest) :LLDP/CDP->manual
	802.1x				configuration->DHCP VLAN
		802.1x Mode	EAP-TTLS/EAP-MSCHAP		It is a general term for techniques that establish and
		Provisioning Mode Anonymous Identity	Unauthenticated Provisic * Anonymous		maintain IP connections traversing NAT gateways. STU is one of the NAT traversal
		Identity	yealink		techniques. You can configure NAT travers
		MD5 Password	•••••		for the IP phone.
		CA Certificates	Upload	rowse	Quality of Service (QoS) It is the ability to provide different priorities for different
		Device Certificates	Upload	rowse	packets in the network, allowing the transport of traffic with special requirements.
		Confirm	Cancel		Web Coming Tupo

- 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.

					Log Out
Yealink 1236					English(English) 🔫
	Status Acc	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 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-PEAP/GTC		It is a general term for techniques that establish and
		Provisioning Mode	Unauthenticated Provisi	c -	maintain IP connections
		Anonymous Identity	Anonymous		traversing NAT gateways. STUN is one of the NAT traversal
		Identity	yealink		techniques.
		MD5 Password			You can configure NAT traversal for the IP phone.
		land the second		Browse	Quality of Service (QoS)
		CA Certificates	Upload		It is the ability to provide different priorities for different
		Device Certificates		Browse	packets in the network,
			Upload		allowing the transport of traffic with special requirements.
		Confirm	Cancel		

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.

						\square		
	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basic	LLDP						NOTE	1
PC Port			Active	Enab	led	-	VLAN	
POPOIL			Packet Interval (1~360	00s) 60			It is used to lo	
NAT	CDP						physical netwo broadcast dom	ains. VLAN
Advanced			Active	Disat	iled	-	membership ca through softwa	n be configured are instead of
			Packet Interval (1~360	00s) 60			physically relocations.	ating devices or
							0.000	
							method (from	
			:				lowest) :LLDP/ configuration->	
	802.1	Lx					NAT Traversal	
			802.1x Mode	FAP	TTLS/EAP-GTC	•	It is a general t techniques that	term for
			Provisioning Mode		uthenticated Provisi		maintain IP cor	nections
					intendeaced Provisi		traversing NAT	gateways. STU
							is one of the N	AT traversal
			Anonymous Identity		nymous		is one of the N techniques.	AT traversal
			Anonymous Identity Identity	yeali	nk		techniques. You can config	ure NAT travers
			Anonymous Identity	yeali			techniques. You can config for the IP phor	ure NAT travers ie.
			Anonymous Identity Identity	yeal	nk	Browse	techniques. You can config	ure NAT travers ie. r vice (QoS)
			Anonymous Identity Identity MD5 Password	yeal	nk	Browse	techniques. You can config for the IP phor Quality of Sen It is the ability	ure NAT travers re. rvice (QoS) to provide ies 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 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-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	yealink		You can configure NAT traversal
		MD5 Password	•••••		for the IP phone.
		CA Certificates	Upload	Browse	Quality of Service (QoS) It is the ability to provide different priorities for different
		Device Certificates	Upload	Browse	packets in the network, allowing the transport of traffic with special requirements.
	C	Confirm	Cancel		Wah Sarvar 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.

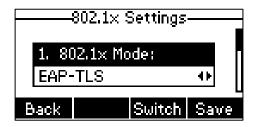
The following takes a SIP-T23G IP phone running firmware version 81 as an example.

To configure 802.1x via phone user interface:

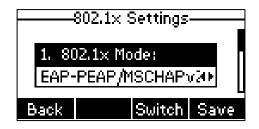
- Press Menu->Settings->Advanced Settings (default password: admin)
 ->Network->802.1x.
- Press (•) or (•), or the Switch soft key to select the desired value from the 802.1x
 Mode field.
 - a) If you select EAP-MD5:

	802.1× Setting]s						
1. 802.1× Mode:								
EAP-MD5 🔸								
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.
- b) If you select EAP-TLS:

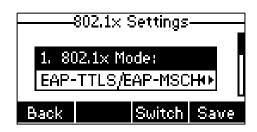


- 1) Enter the user name for authentication in the Identity field.
- 2) Leave the MD5 Password field blank.
- c) If you select EAP-PEAP/MSCHAPv2:

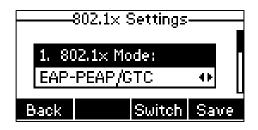


- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.

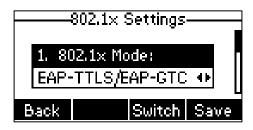
d) If you select EAP-TTLS/EAP-MSCHAPv2:



- 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× Settir	ngs					
1. 8	02.1x Mode:						
EAP	EAP-FAST						
Back	Swit	ch 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

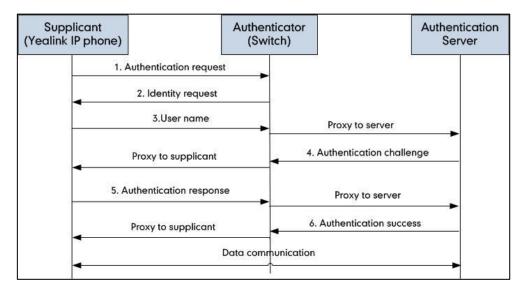
Reboot the phone to activate the 802.1X authentication on the phone. The 802.1X authentication process is divided into two basic stages:

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:

0 0 1 1 1	Capture Analyze Statistics		2] • • • • • • • • ■] • • • • • • • • • •	
Filter: eap eapol	Source	Destination		pression Clear Apply Save Filter	
	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	FAP	60 Request, TLS EAP (EAP-TLS)	
8 2.277015000		Nearest	FAP	60 Response, Legacy Nak (Response Only)	
10 2.284961000		Nearest	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)	
	xiamenYe 73:4c:f1		EAP	60 Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)	
	cisco_5d:42:94	Nearest	EAP	60 Success	
				m	
				(480 bits) on interface 0	
Ethernet II, S 802.1X Authent		0:62:6b:5d:4	12:94), D	st: Nearest (01:80:c2:00:00:03)	
Version: 802					
Type: Start					

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:

le Edt ykw go Capture Analyze Statistics Telephony Iook Internals Heb	
senil eapol Expression Clear Apply Save Filter 1 Destination Protocol Length Info 9:3-93231000 Cfsco_5dr42:94 Near est EAPOL 60 Start 13:3-93211000 Cfsco_5dr42:94 Near est EAPOL 60 Start 13:3-93211000 Cfsco_5dr42:94 Near est EAPOL 60 Start 13:3-93211000 Cfsco_5dr42:94 Near est EAPOL 60 Request, Identity 13:3-93211000 Cfsco_5dr42:94 Near est EAP 60 Request, Identity 13:3-99211000 Cfsco_5dr42:94 Near est EAP 60 Request, Protected EAP (EAP-FEAP) 14:004604000 Cfsco_5dr42:94 Near est TAPOL 60 Request, Protected EAP (EAP-FEAP) 14:0124000 Cfsco_5dr42:94 Near est TAPOL 60 Request, Protected EAP (EAP-FEAP) 14:130143000 Cfsco_5dr42:94 Near est TAPOL 60 Request, Protected EAP (EAP-FEAP) 14:130143000 Cfsco_5dr42:94 Near est TAPOL 60 Request, Protected EAP (EAP-FEAP) 14:130143000 Cfsco_5dr42:94 Near est TAPOL 60 Request, Protected EAP (EAP-FEAP) 14:130143000 Cfsco_5dr42:94 Near est TAPOL 6	
Source Destination Protocol Lengh Info 9 3.932731000 C15co_35142194 Near est EAPPL 60 Start 13.986270000 C15co_35142194 Near est EAPPL 60 Request, Identity 13.986270000 C15co_35142194 Near est EAP 60 Request, Identity 13.980270000 C15co_35142194 Near est EAP 60 Request, Protected EAP (EAP-FLS) 13.9902714000 C15co_35142194 Near est EAP 60 Request, Protected EAP (EAP-FEAP) 14.00140000 C15co_35142194 Near est EAP 60 Request, Protected EAP (EAP-FEAP) 14.103140000 C15co_35142194 Near est TLSV1 116 C11ernt Hello 12.4.1389750000 C15co_35142194 Near est TLSV1 116 C11ernt Hello 14.1301400000 Xiamery-Z14ctfl Near est	
Time Source Destination Protocol length Info 9 3.925112000 Cisco_5d:42:94 Nearest EAPOL 60 Start 10 3.92679000 Cisco_5d:42:94 Nearest EAPOL 60 Start 13 3.98510000 Cisco_5d:42:94 Nearest EAPOL 60 Response, Identity 13 3.98100000 Cisco_5d:42:94 Nearest EAP 60 Response, Identity 13 3.9811000 Cisco_5d:42:94 Nearest EAP 60 Response, Identity 13 3.9811000 Cisco_5d:42:94 Nearest EAP 60 Request, I's EAP No 14 4.004604000 Cisco_5d:42:94 Nearest EAP 60 Request, Protect AP (EAP-PEAP) 14 4.004604000 Cisco_5d:42:94 Nearest EAP 60 Request, Protect AP (EAP-PEAP) 14 4.130140000 Cisco_5d:42:94 Nearest TLSV1 116 Client Hello 14 4.130140000 Cisco_5d:42:94 Nearest TLSV1 104 Client Hello 14 4.130140000 Cisco_5d:42:94 Nearest TLSV1 104 Client Hello 14 4.130140000 Cisco_	
0 3.925112000 cisco_5d:42:94 Nearest EAPOL 60 Start 13.925112000 cisco_5d:42:94 Nearest EAP 60 Request, Identity 13.9851660000 Ximmerve_73:4c:f1 Nearest EAP 60 Request, Identity 13.992110000 cisco_5d:42:94 Nearest EAP 60 Request, TLS EAP (EAP-TLS) 13.992110000 cisco_5d:42:94 Nearest EAP 60 Request, TLS EAP (EAP-TLS) 13.992110000 cisco_5d:42:94 Nearest EAP 60 Request, Protected EAP (EAP-FLS) 14.004604000 cisco_5d:42:94 Nearest TLSV1 116Cient Hello 14.1034000 cisco_5d:42:94 Nearest TLSV1 116Cient Hello 14.13049000 cisco_5d:42:94 Nearest TLSV1 116Cient Hello 14.13049000 cisco_5d:42:94 Nearest TLSV1 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 19.4.13305000 cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 19.4.130450000 cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 19.4.130355000 cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 20.4.100224000 ximmerve_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
10.3:282791000 cisco_5d:42:94 Nearest EAP 60 Request, Identity 13:396530000 Xianew-Zistcff1 Nearest EAP 60 Request, Identity 13:396230000 Xianew-Zistcf1 Nearest EAP 60 Request, ILS EAP (EAP-TLS) 13:396231000 Xianew-Zistcf1 Nearest EAP 60 Request, ILS EAP (EAP-TLS) 13:396231000 Xianew-Zistcf1 Nearest EAP 60 Request, Protected EAP (EAP-TLS) 14:4.004604000 Xianew-Zistcf1 Nearest EAP 60 Request, Protected EAP (EAP-TLS) 14:0124000 Xianew-Zistcf1 Nearest EAP 60 Request, Protected EAP (EAP-FEAP) 15:4.091224000 Xianew-Zistcf1 Nearest EAP 60 Request, Protected EAP (EAP-FEAP) 14:4.01245073000 Xianew-Zistcf1 Nearest TLSV1 116 (Filent Hello 14:4.138453000 Xianew-Zistcf1 Nearest TLSV1 104 Seryonse, Protected EAP (EAP-FEAP) 19:4.138455000 Xianew-Zistcf1 Nearest TLSV1 103 Server Hello, Certificat, Server Key Exchange, Server Hello Done 20:4.10020000 Xianew-Zistcf1<	
13.981630000 xiamerve_73:4c:f1 Nearest EAP 60 Response, Identify 13.991711000 cisc_3d:42:94 Nearest EAP 60 Request, TLS EAP (EAP-FLS) 13.4.002604000 xiamerve_73:4c:f1 Nearest EAP 60 Request, TLS EAP (EAP-FLS) 14.004604000 cisc_3d:42:94 Nearest EAP 60 Request, Protected EAP (EAP-FLAS) 14.00124000 xiamerve_73:4c:f1 Nearest EAP 60 Request, Protected EAP (EAP-FLAS) 14.00124000 xiamerve_73:4c:f1 Nearest TLSV1 1166 client Hello 14.10140000 xiamerve_73:4c:f1 Nearest TLSV1 1162 Server Hello, Certificate, Server Key Exchange, Server Hello Done 14.130140000 xiamerve_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 19.4.130355000 cisc_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 20.4.100200000 xiamerve_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
12 3:99:711000 cisco_sd:42:94 Nearest EAP 60 Request, TLS EAP (EAP-TLS) 13:39:23:1000 xiamev xiamev 60 Request, TLS EAP (EAP-TLS) 13:39:23:1000 xiamev xiamev 60 Request, Protected EAP (EAP-PEAP) 14:0.04604000 xiamev xiamev EAP 60 Request, Protected EAP (EAP-PEAP) 15:0.01224000 xiamev xiamev xiamev xiamev 15:0.01224000 xiamev xiamev xiamev xiamev 14:0.12424000 xiamev xiamev xiamev xiamev 14:0.12424000 xiamev xiamev xiamev xiamev 15:0.01224000 xiamev xiamev xiamev xiamev 14:1.01420000 xiamev xiamev xiamev xiamev 14:1.130420000 xiamev xiamev xiamev xiamev 19:1.138955000 xiamev xiamev xiamev xiamev xiamev 19:1.138955000 xiamev xiamev xiamev xiamev xiamev	
13.3.992514000 xiamerve_73:4c:f1 Nearest EAP 60 Response, Legacy Nak (Response only) 14.4.004604000 Cisco_5d:42:94 Nearest EAP 60 Request, Protected EAP (EAP-PEAP) 15.4.091224000 xiamerve_73:4c:f1 Nearest TLSV1 116 Client Hello 17.4.128973000 Cisco_5d:42:94 Nearest TLSV1 116 Client Hello 18.4.130149000 Xiamerve_73:4c:f1 Nearest TLSV1 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 18.4.130149000 Xiamerve_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 19.4.138955000 Cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 20.4.100204000 Xiamerve_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
14 4.004604000 Cisco_Sd:42:94 Nearest EAP 60 Request, protected EAP (EAP-PEAP) 15 4.001224000 Xiamerve_Zistc:f1 Nearest T.SU 116 (Tient Hello 15 4.001224000 Xiamerve_Zistc:f1 Nearest T.SU 116 (Tient Hello 15 4.101240000 Xiamerve_Zistc:f1 Nearest T.SU 116 (Tient Hello 16 4.10140000 Xiamerve_Zistc:f1 Nearest T.SU 116 (Tient Hello 18 4.130140000 Xiamerve_Zistc:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP) 19 4.138955000 Cisco_Sd:42:94 Nearest T.SU 103 Server Hello, Certificat, Server Key Exchange, Server Hello Done 20 4.140024000 Xiamerve_Zistc:f1 Nearest T.SU 103 Server Hello, Certificat, Server Key Exchange, Server Hello Done	
154.091224000 Xiamerve_73:4c:f1 Nearest TLSV1 116 Client.Hello 174.128973000 Cisco_5d:42:94 Nearest TLSV1 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 184.130149000 Xiamerve_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP) 194.138955000 Cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 204.140024000 Xiamerve_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP)	
12 4.128973000 cisco_5d:42:94 Nearest TLSVI 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 18 4.130149000 Xiamery Carbony Xiamery Carbony Xiamery Carbony Xiamery Carbony 19 4.138955000 Sico_5d:42:94 Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 20 4.140024000 Xiamery Carbony Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
18 4.130149000 XiamerVe_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP) 19 4.138955000 Cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 20 4.140024000 XiamerVe_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP)	
194.138955000 Cisco_5d:42:94 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 204.140024000 xiamenYe_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP)	
20 4.140024000 Xiamenye_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP)	
21 4.148933000 Cisco_5d:42:94 Nearest TLSv1 522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
30 4.764896000 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 TLSVI 61 Application Data	
404.843186000 xiamenve_73i4c:f1 Nearest TLSVI 98.Application Data, Application Data 565.877757000 cisco_5d:42:94 Nearest EAP 60 Success ∢ @ Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 @ thermer 11. src: xiamenve_73:4c:f1 (00:15:667:73:4c:f1). 0st: 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	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:

📕 EA	P-PEAP GTC.pcapn	g [Wireshark 1.10.5 (SVN R	Rev 54262 fro	m /trunk-1.10	0]	
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Interr	nals Help	
0		🖹 🗎 🗶 🔁 🔍 🔶				
	y 🧥 🗯 🔬					
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	
		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 Authentic		(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)				
- C	Identity: ye					

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

EAP-TTLS EAP-GT	C.pcapng [Wireshark 1.10.5	(SVN Rev 5426	2 from /trur	nk-1.10)]	
ie <u>E</u> dit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics	Telephony	<u>T</u> ools <u>I</u> nte	mals <u>H</u> elp	
) 🖲 🔏 🔳 🖉	i 🖻 🖺 🗙 🔁 i 🔍 🗧	🗆 🏟 🤹 🖗	2 🗐	🗐 Q, Q, Q, 🔟 🖉 🕺 🦂 💥 🧱	
ilter: eap eapol			• E	xpression Clear Apply Save Filter	
o. Time	Source	Destination		Length Info	
6 3.12811200		Nearest	EAPOL	60 Start	
	O Cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
	0 XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity	
	0 Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)	
	0 xiamenYe_73:4c:f1 0 cisco 5d:42:94	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
	0 Cisco_5d:42:94 0 XiamenYe 73:4c:f1	Nearest	EAP	60 Request, Tunneled TLS EAP (EAP-TTLS) 112 Client Hello	
	0 Cisco_5d:42:94	Nearest	TLSV1 TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	0 XiamenYe_73:4c:f1	Nearest	EAP	60 Response. Tunneled TLS EAP (EAP-TTLS)	
	0 Cisco_5d:42:94	Nearest	EAP TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	0 XiamenYe_73:4c:f1	Nearest	EAP	60 Response. Tunneled TLS EAP (EAP-TTLS)	
	0 Cisco_5d:42:94	Nearest	TLSV1	526 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	0 XiamenYe 73:4c:f1	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	0 Cisco 5d:42:94	Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message	
	XiamenYe 73:4c:f1	Nearest	TLSV1	114 Application Data, Application Data	
36 3.97675100	0 cisco_5d:42:94	Nearest	TLSV1	97 Application Data	
37 3.98050400	0 xiamenYe_73:4c:f1	Nearest	TLSV1	130 Application Data, Application Data	
48 5.01194000	0 Cisco_5d:42:94	Nearest	EAP	60 Success	
				III.	
				d (480 bits) on interface O	
		(00:15:65:	73:4c:f1)), Dst: Nearest (01:80:c2:00:00:03)	
802.1X Authen					
	2.1x-2001 (1)				
Type: EAP P Length: 12	acket (0)				
	Authentication Protoco				
Code: Res					
Id: 1	polise (2)				
Length: 1	2				
Type: Ide					

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

	g [Wireshark 1.10.5 (SVN Rev 54				•
le <u>E</u> dit <u>V</u> iew	Go Capture Analyze Statistics	s Telephony	<u>T</u> ools Inte	mais Help	
) 🖲 🔏 🔳 .	🧉 🖻 🖀 🗶 😂 🔍 🤞	P 🌳 🚳 春	2 🗐	🗐 Q, Q, Q, 🔟 🖉 🕺 % 🕱	
lter: eap eapo	31		▼ E	xpression Clear Apply Save Filter	
. Time	Source	Destination		Length Info	
	2000 xiamenye_45:6f:bb	Nearest	EAPOL	60 Start	
	5000 cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
	0000 XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity	
	2000 Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	000 xiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
	1000 cisco_5d:42:94	Nearest	TLSV1	60 Ignored Unknown Record	
	0000 xiamenYe_45:6f:bb	Nearest	TLSV1	80 Client Hello	
	000 cisco_5d:42:94	Nearest	TLSV1	1030 Server Hello, Certificate, Certificate Request, Server Hello Done	
	0000 xiamenYe_45:6f:bb	Nearest	EAP	60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)	
	2000 cisco_5d:42:94	Nearest	TLSV1	483 Server Hello, Certificate, Certificate Request, Server Hello Done	
	'000 xiamenYe_45:6f:bb	Nearest	TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	3000 cisco_5d:42:94	Nearest	TLSV1	109 Change Cipher Spec, Encrypted Handshake Message, Application Data	
	000 XiamenYe_45:6f:bb	Nearest	TLSV1	63 Application Data	
	1000 cisco_5d:42:94	Nearest	TLSV1	87 Application Data	
	3000 XiamenYe_45:6f:bb	Nearest	TLSV1	83 Application Data	
	0000 cisco_5d:42:94	Nearest	TLSV1	115 Application Data	
	000 XiamenYe_45:6f:bb	Nearest	TLSV1	131 Application Data	
	8000 cisco_5d:42:94	Nearest	TLSV1	279 Application Data	
77 20.382206	5000 XiamenYe_45:6f:bb	Nearest	TLSV1	65 Application Data	
				ed (480 bits) on interface 0	
			45:6f:bb)	, Dst: Nearest (01:80:c2:00:00:03)	
	on: Nearest (01:80:c2:00				
	iamenYe_45:6f:bb (00:15:)		
	1x Authentication (0x88				
Padding: 0 802.1X Authe	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0000000000	0000	
	802.1X-2001 (1) Packet (0)				
Length: 10					
	e Authentication Protoco	1			
	esponse (2)				
Id: 1	isponse (2)				
Length:	10 dentitv (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:

	0.5 (SVN Rev 54262 from /trunk-1.	
<u>File Edit View Go Capture</u>	<u>Analyze</u> Statistics Telephony	Tools Internals Help
00412) 🗶 😂 🔍 🗢 🔶 🐺	F 👱 🗐 🖬 0, Q, Q, 🔟 🖉 🕺 🥵 💥 🗒
Filter: eap eapol		Expression Clear Apply Save Filter
No. Time Source		
116 17.805503000 Cisco		
117 17.808685000 Cisco		
118 17.809519000 Xiame		
119 17.819739000 Cisco		
120 17.823631000 xiame		
122 17.857040000 cisco 123 17.858234000 xiame		
123 17.858234000 X1ame 124 17.867698000 Cisco		
125 17.869098000 Cisco 125 17.869098000 Xiame		
126 17.882798000 Cisco		
130 18.447360000 Xiame		
131 18,457674000 Cisco		
132 18,459768000 Xiame		
133 18,478941000 cisco		
134 18.487070000 xiame	nYe_73:4c:f1 Nearest	
146 19.516815000 cisco	_5d:42:94 Nearest	EAP 60 Success
		m
* L		
		rtes captured (480 bits) on interface 0
		::73:4c:f1), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication		
Version: 802.1X-200		
Type: EAP Packet (0 Length: 12	9	
Extensible Authenti	cation Protocol	
Code: Response (2		
Id: 1	/	
Length: 12		
Type: Identity (1)	
Identity: Anonymo		
enterney r whorry me		

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

🗲 EAI	P-PEAP MSCHPv2,	pcapng [Wireshark 1.10.5 (SVN Rev 5426	2 from /trur	k-1.10)]	• ×		
Ele	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp			
0 (ا 🗴 🔳 🛕	🖹 ិ 🗶 🛃 🔍 🔶	🏟 🥥 7	1	🗐 Q, Q, Q, 🗹 👹 🗹 🥵 % 🚊			
Filter:	eap eapol			▼ E	pression Clear Apply Save Filter			
No.	Time	Source	Destination	Protocol	Length Info			
9	3.925112000	cisco_5d:42:94	Nearest	EAPOL	60 Start			
10	3.928791000	cisco_5d:42:94	Nearest	EAP	60 Request, Identity			
11	3.981630000	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity			
12	3.991711000	Cisco_5d:42:94	Nearest	EAP	60 Request, TLS EAP (EAP-TLS)			
13	3.992514000	<pre>xiamenYe_73:4c:f1</pre>	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)			
21	4.148933000	Cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done			
30	4.764896000	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			
٠ 📃					m	•		
					d (480 bits) on interface 0 . Dst: Nearest (01:80:c2:00:00:03)			
	2.1X Authenti		(00.13:03:)	(3.4CIL)	, DSC. NEW ESC (01.00.02.00.00.03)			
	version: 802.	1X-2001 (1)						
	Type: EAP Pac	ket (0)						
Length: 12								
	Extensible Au	thentication Protocol						
	Code: Respo	nse (2)						
	Id: 1							
Length: 12								
Type: Identity (1)								
	Identity: Anonymous							

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	P-PEAP GTC.pcapn	g [Wireshark 1.10.5 (SVN F	Rev 54262 fro	m /trunk-1.1	0)]	
Eie g	<u>Edit V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inten	nals <u>H</u> elp	
0.0		🖹 🗎 💥 🔁 🔍 🔶	💩 📣 🐺	1	∃ 0, 0, 0, 17 ¥ 12 56 % 12	
	e ann ann an 1					
Filter:	eap eapol			▼ Ex	rpression Clear Apply Save Filter	
No.		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)	
		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 cisco 5d:42:94	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP) 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		Cisco_50:42:94 XiamenYe 73:4c:f1	Nearest	TLSV1	60 Response. Protected EAP (EAP-PEAP)	
		Cisco_5d:42:94	Nearest	EAP TLSV1	60 Response, Protected EAP (EAP-PEAP) 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	EAP 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	
		XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
		Cisco_5d:42:94	Nearest	FAP	60 Success	
+						Þ
	ame 32: 60 bud	tes on wire (480 hits)) 60 hvrte	s canture	d (480 bits) on interface 0	,
					. Dst: Nearest (01:80:c2:00:00:03)	
802	2.1X Authentio	cation			, , ,	
×	version: 802.1	LX-2001 (1)				
1	Type: EAP Pack	ket (0)				
	Length: 12					
E	Extensible Aut	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:

E	AP-TTLS FAP-GTC .	pcapng [Wireshark 1.10.5 (S	VN Rev 5426	2 from /trun	k-1.10)]	
_		Capture Analyze Statistics				
-						
Θ	• 🔺 📕 🔬	🖻 🏼 🗶 😂 I 🔍 🗢	🥯 🤪 🕆		∃ 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_5d:42:94 XiamenYe 73:4c:f1	Nearest	EAP TLSV1	112 Client Hello	
		cisco 5d:42:94	Nearest	TLSV1 TLSV1	112 Client Hello 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	
		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	3 5.011940000	Cisco_5d:42:94	Nearest	EAP	60 Success	
					m	
E E	thernet II, Sr 02.1X Authenti Version: 802. Type: EAP Pac	c: XiamenYe_73:4c:f1 cation 1X-2001 (1)			(480 bits) on interface 0 , DSt: Nearest (01:80:c2:00:00:03)	
	Length: 12					
		thentication Protocol				
	Code: Respo	nse (2)				
	Id: 1					
	Length: 12 Type: Ident	1111 (1)				
_	Identity: A					
	ruentity: A	nonymous				

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	íreshark 1.10.5 (SVN Rev 54	262 from /trun	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 8	
Filter	eap eapol			▼ Ex	pression Clear Apply Save Filter
		Source	Destination	Protocol I	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 Cisco 5d:42:94	Nearest	TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
			Nearest	TLSV1	109 Change Cipher Spec, Encrypted Handshake Message, Application Data
		xiamenYe_45:6f:bb Cisco_5d:42:94	Nearest	TLSV1 TLSV1	63 Application Data 87 Application Data
		XiamenYe 45:6f:bb	Nearest	TLSV1	83 Application Data
		Cisco 5d:42:94	Nearest	TLSV1 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
510	27.041554000	xTalleITTE_45.01.00	Near esc	TLOVI	m Maria Ma
					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				
	Type: EAP Pack	(et (0)			
	Length: 19				
-		thentication Protocol			
	Code: Respor	15e (2)			
	Id: 1				
	Length: 19				
	Type: Identi				
	Identity: Ar	Tonymous			

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.

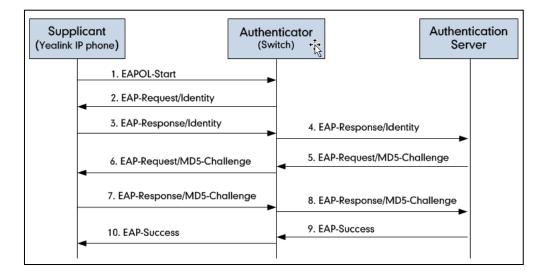
TTLS (Tunneled Transport Layer Security) -Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

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.

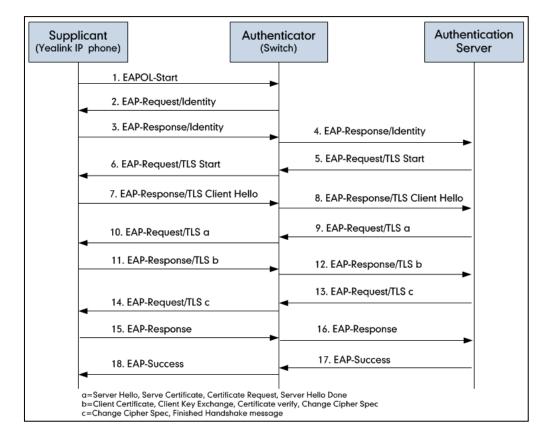


- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header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

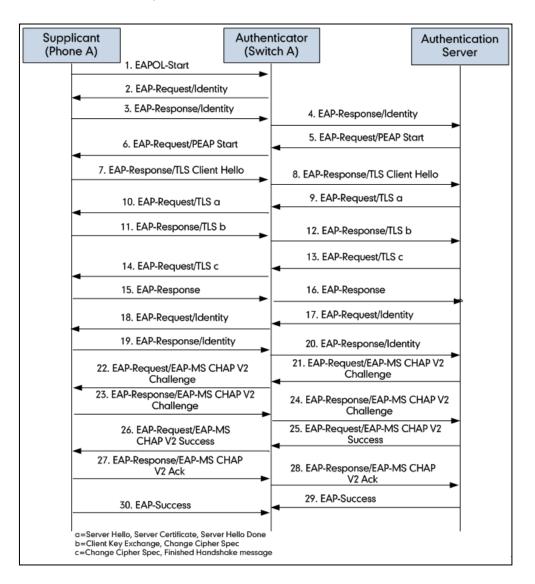
After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to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