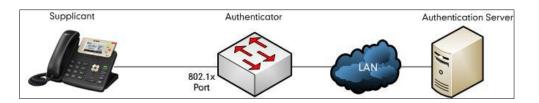
About 802.1X

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

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

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



Yealink IP Phones Compatible with 802.1X

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

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

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

Authentication Protocol	IP Phone Models	Firmware Version
	T58A T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960, and W56P	Firmware version 80 or later
	T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 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
EAP-TTLS/EAP-MSCHAPv2	T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 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

Authentication Protocol	IP Phone Models	Firmware Version
	T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
	T58A T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later
EAP-TTLS/EAP-GTC	T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 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
	T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	Firmware version 81 or later
	VP59, W53P, and CP930W-Base	Firmware version 83 or later

Authentication Protocol	IP Phone Models	Firmware Version
	T57W, T54W, T53W, T53, T48U, T46U, T43U and T42U	Firmware version 84 or later
	T33P, T33G, T31P, T31G, T31, T30P and T30	Firmware version 85 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 the 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 the 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-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23
 G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later

- SIP-T57W/T54W/T53W/T53/T48U/T46U/T43U/T42U IP phones running firmware version 84 or later
- SIP-T33P/T33G/T31P/T31G/T31/T30P/T30 IP phones running firmware version 85 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	Parameters Permitted Values Def			
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	6-EAP-TTLS/EAP-GTC			
7-EAP-FAST				
Note: If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Advanced->802.1x->802.1x Mode				
Phone User Interface:				
Menu->Settings->Advanced Settings (default pass	Menu->Settings->Advanced Settings (default password: admin) ->Network->802.1x			
Settings->802.1x Mode				
network.802_1x.identity	String within 32 characters	Blank		

Parameters	Permitted Values	Default		
Description:				
Configures the user name for 802.1x authentication.				
Note: It works only if the value of the parameter "no	etwork.802_1x.mode" is set t	o 1, 2, 3, 4,		
5, 6 or 7. If you change this parameter, the IP phor	ne 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 Settings->Identity	word: admin) ->Network->80	2.1x		
	String within 32	Diank		
network.802_1x.md5_password	characters	Blank		
Description:				
Configures the password for 802.1x authentication				
Note : It works only if the value of the parameter "no 6 or 7. If you change this parameter, the IP phone effect.				
6 or 7. If you change this parameter, the IP phone				
6 or 7. If you change this parameter, the IP phone effect.				
6 or 7. If you change this parameter, the IP phone effect. Web User Interface:				
6 or 7. If you change this parameter, the IP phone effect. Web User Interface: Network->Advanced->802.1x->MD5 Password	will reboot to make the chan	ge take		
6 or 7. If you change this parameter, the IP phone effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass	will reboot to make the chan	ge take		
6 or 7. If you change this parameter, the IP phone effect. Web User Interface: Network->Advanced->802.1x->MD5 Password Phone User Interface: Menu->Settings->Advanced Settings (default pass Settings->MD5 Password	will reboot to make the chang word: admin) ->Network->80 URL within 511	ge take 2.1x		
6 or 7. If you change this parameter, the IP phone 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	will reboot to make the chang word: admin) ->Network->80 URL within 511	ge take 2.1x		
6 or 7. If you change this parameter, the IP phone 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:	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters	ge take 2.1x Blank		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate.	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters	ge take 2.1x Blank		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate. Note: It works only if the value of the parameter "network.	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters	ge take 2.1x Blank		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate. Note: It works only if the value of the parameter "monos of the certificate must be *.pem,	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters	ge take 2.1x Blank		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate. Note: It works only if the value of the parameter "mone 6 or 7. The format of the certificate must be *.pem, Web User Interface:	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters	ge take 2.1x Blank		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate. Note: It works only if the value of the parameter "no 6 or 7. The format of the certificate must be *.pem, Web User Interface: Network->Advanced->802.1x->CA Certificates	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters etwork.802_1x.mode" is set t *.crt, *.cer or *.der. URL within 511	ge take 2.1x Blank o 2, 3, 4, 5,		
6 or 7. If you change this parameter, the IP phone 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: Configures the access URL of the CA certificate. Note: It works only if the value of the parameter "no 6 or 7. The format of the certificate must be *.pem, Web User Interface: Network->Advanced->802.1x->CA Certificates network.802_1x.client_cert_url	will reboot to make the chang word: admin) ->Network->80 URL within 511 characters etwork.802_1x.mode" is set t *.crt, *.cer or *.der. URL within 511 characters	ge take 2.1x Blank o 2, 3, 4, 5,		

Parameters Permitted Values		Default
(EAP-TLS). The format of the certificate must be *.pem.		
Web User Interface:		
Network->Advanced->802.1x->Device Certificates		

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

 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., y000000000xx.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.
- 2. 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	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		

Parameters	Permitted Values	Default		
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	ot required.			
Note: If you change this parameter, the IP phone will r effect.	eboot to make the change	e take		
Web User Interface:				
Network->Advanced->802.1x->802.1x Mode				
Phone User Interface:				
Menu->Settings->Advanced Settings (default passwor ->Network->802.1x->802.1x Mode	d: admin)			
static.network.802_1x.eap_fast_provision_mode	0 or 1	0		
Description:				
Configures the EAP In-Band provisioning method for E	EAP-FAST.			
0-Unauthenticated Provisioning				
1-Authenticated Provisioning				
If it is set to 0 (Unauthenticated Provisioning), EAP In- server unauthenticated PAC (Protected Access Crede Diffie-Hellman key exchange.		-		
If it is set to 1 (Authenticated Provisioning), EAP In-Ba authenticated PAC provisioning using certificate-based		l by server		
Note: It works only if the value of the parameter "static.network.802_1x.mode" is set to 7 (EAP-FAST). If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Advanced->802.1x->Provisioning Mode				
static.network.802_1x.anonymous_identity Characters Blan				
Description:				
Configures the anonymous identity (user name) for 80	2.1X authentication.			
It is used for constructing a secure tunnel for 802.1X authentication.				
Note: It works only if the value of the parameter "static.network.802_1x.mode" is set to 2,				
3, 4, 5, 6 or 7. If you change this parameter, the IP pho	one will reboot to make the	e change		

Parameters	Permitted Values	Default			
take effect.					
Web User Interface:					
Network->Advanced->802.1x->Anonymous Identity					
static.network.802_1x.identity	dentity String within 32 characters Blank				
Description:					
Configures the user name for 802.1x authentication.					
Note : It works only if the value of the parameter "static 2, 3, 4, 5, 6 or 7. If you change this parameter, the IP p take effect.					
Web User Interface:					
Network->Advanced->802.1x->Identity					
Phone User Interface:					
Menu->Settings->Advanced Settings (default passwor ->Network->802.1x->Identity	d: 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 "static 3, 4, 5, 6 or 7. If you change this parameter, the IP photake effect.					
Web User Interface:					
Network->Advanced->802.1x->MD5 Password					
Phone User Interface:					
Menu->Settings->Advanced Settings (default passwor Password	d: admin) ->Network->80	2.1x->MD			
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 "static 3, 4, 5, 6 or 7. If the authentication method is EAP-FAS the parameter "static.network.802_1x.eap_fast_provis Provisioning). The format of the certificate must be *.p	ST, you also need to set t ion_mode" to 1 (Authentic	he value o			

Parameters	Permitted Values	Default		
Web User Interface:				
Network->Advanced->802.1x->CA Certificates				
static.network.802_1x.client_cert_url URL within 511 characters Bla				
Description:				
Configures the access URL of the device certificate.				
Note : It works only if the value of the parameter "static.network.802_1x.mode" is set to 2 (EAP-TLS). The format of the certificate must be *.pem.				
Web User Interface:				
Network->Advanced->802.1x->Device Certificates				
static.network.802_1x.proxy_eap_logoff.enable	0 or 1	0		
Description:				
Enables or disables the 802.1x-logoff feature for the PC port.				
	•			
0-Disabled				
0-Disabled	sent to the authenticator	when the		

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
```

Reference the configuration file in the boot file (e.g., y000000000000.boot).
 Example:

include:config "http://10.2.1.158/static.cfg"

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

Applying the Configuration Files to Your Phone

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

- 1. Connect your phone to a network that is not 802.1X-enabled.
- Perform the auto provisioning process to apply the configuration files to the phone. Then the IP phone will reboot to make the settings effective.
 For more information on auto provisioning, refer to the latest Auto Provisioning Guide 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
Yealink 1236					English(English) 👻
	Status Accour	Network DS	SKey Features	Settings	Directory Security
Basic	LLDP				NOTE
		Active	Enabled	-	VLAN
PC Port		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
	802.1x	•			configuration->DHCP VLAN
	002.11	802.1x Mode	EAP-MD5		NAT Traversal It is a general term for
		Provisioning Mode	Unauthenticated Provisic -	7	techniques that establish and maintain IP connections
		Anonymous Identity			traversing NAT gateways. STUN is one of the NAT traversal
		Identity	vealink		techniques.
		MD5 Password	•••••	-	You can configure NAT traversal for the IP phone.
		CA Certificates		Browse	Quality of Service (QoS)
		CA Certificates	Upload		It is the ability to provide different priorities for different
		Device Certificates	Upload	Browse	packets in the network, allowing the transport of traffic
			opioad		with special requirements.
		Confirm	Cancel		Web Server 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.
 - 4) In the CA Certificates field, click Browse to select the desired CA certificate

(*.pem, *.crt, *.cer or *.der) from your local system.

5) In the **Device Certificates** field, click **Browse** to select the desired client (*.pem or *.cer) certificate from your local system.

Yealink 1236					Log Out English(English) 🗸
	Status Accoun	t Network DSS	6Key Features	Settings	Directory Security
Basic	LLDP				NOTE
PC Port		Active	Enabled	•	VLAN
NAT		Packet Interval (1~3600s)	60		It is used to logically divide a physical network into several
Advanced	CDP	Active	Disabled	•	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 assignment
		:			method (from highest to lowest) :LLDP/CDP->manual
	802.1x	•			configuration->DHCP VLAN
		802.1x Mode	EAP-TLS	•	NAT Traversal It is a general term for
		Provisioning Mode	Unauthenticated Provision	-	techniques that establish and 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	•••••	Browse	for the IP phone.
		CA Certificates	Upload		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.
		Confirm	Cancel		Web Server Type

- 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.

	Status Acc	count Network D	SSKey Features	Settings	Directory Security
Basic	LLDP				NOTE
DC Deat		Active	Enabled	•	M AN
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				
		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 is one of the NAT traversal
		Anonymous Identity	Anonymous		techniques.
			vealink		
		Identity	ycomit		You can configure NAT travers
		Identity MD5 Password	•••••	_	for the IP phone.
			•••••	Browse	for the IP phone. Quality of Service (QoS)
		MD5 Password		Browse	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.

ealink 1236				Log Ou English(English)
	Status	ount Network DS	SKey Features Settin	gs Directory Security
Basic	LLDP			NOTE
PC Port		Active	Enabled -	VLAN
NAT		Packet Interval (1~3600s)	60	It is used to logically divide a physical network into several
	CDP			broadcast domains. VLAN membership can be configured
Advanced		Active Packet Interval (1~3600s)	Disabled -	through software instead of physically relocating devices or
		Facket Interval (1~50005)	80	connections.
		•		The priority of VLAN assignmen method (from highest to
				lowest) :LLDP/CDP->manual configuration->DHCP_VLAN
	802.1x			NAT Traversal
		802.1x Mode	EAP-TTLS/EAP-MSCHAP	It is a general term for techniques that establish and
		Provisioning Mode	Unauthenticated Provisic 👻	maintain IP connections traversing NAT gateways. STU
		Anonymous Identity	Anonymous	is one of the NAT traversal techniques.
		Identity	yealink	You can configure NAT traversa
		MD5 Password	Browse	for the IP phone.
		CA Certificates	Upload Browse	It is the ability to provide
	2	Device Certificates	Browse	packets in the network,
			Upload	allowing the transport of traffic with special requirements.
		Confirm	Cancel	Web Comon Tune

- 5) Click **Upload** to upload the certificate.
- e) If you select EAP-PEAP/GTC:

- (Optional.) Enter the anonymous user name for authentication in the Anonymous Identity field.
- 2) Enter the user name for authentication in the Identity field.
- 3) Enter the password for authentication in the MD5 Password field.
- In the CA Certificates field, click Browse to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.

Basic LLDP Active Enabled PC Port Packet Interval (1-3600s) 60 NAT CDP Active Disabled Advanced Active Disabled membership can be through software in provise hy relocating connections. Box2.1x	Yealink 1236	Status	Network DSS	Key Features	Settings	Log Out English(English) • Directory Security
Basic Adive Enabled VLN PC Port Packet Interval (1~3600s) 60 The sued to logically physical network into braadcast domains. Network interestond into headcast doman			netholk Dos	Rey Features	Settings	
PC Port Packet Interval (1-3600s) 60 It is used to logically physical network into braadcast domains. Not compression and through software in a membership can be through software in a membership can be through software in a membership can be through software in a physical retrokent in the priority of VLAN method (from high software in a physical retrokent) Advanced Adve Disabled It is used to logically physical retrokent in the priority of VLAN method (from high software in a physical) retrokent in the priority of VLAN method (from high software in a physical) retrokent in the priority of VLAN method (from high software in a physical) retrokent in the priority of VLAN method (from high software in a physical) retrokent in the physical retrokent in the physical retrokent in the physical retrokent is a general term if techniques that estar markare in Provisioning Mode It is a general term if techniques. It is a off the NAT traversal 802.1x 802.1x Mode EAP-PEAP/GTC It is a general term if techniques. It is the advector of the NAT traversal is one of the NAT traversal is one of the NAT traversal NAT gate is one of the NAT traversal NAT gate is one of the NAT traversal NAT gate is one of the NAT traversal (AC certificates Upload It is the ability to priorites for the advector priorites for the advector priorites for the physical retrokent is one of the NAT traversal is one of the NAT t	Basic		Active	Enabled	-	NOTE
NAT CDP Advanced Active Disabled Advanced Active Disabled Packet Interval (1-3600s) 60 Connections. The priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of VLAM method (from high to be expected by the priority of the priority	PC Port					
Advanced Active Disabled membership can be through software in by proceeding software in by proceeding software in through software in the provide in the p	NAT	CDP				physical network into several
Packet Interval (1~3600s) 60 physically relocating of connections. Physically relocating of connections. The provide VLAN method (from higher lowest) ±LDP/CDP-3 configuration-3OHC) 802.1x 802.1x Mode EAP-PEAP/GTC 802.1x 802.1x Mode Unauthenticated Provisic + Provisioning Mode Unauthenticated Provisic + Ta connigment N Identity Yealink You can configure N MD5 Password Forwise. Guilty of Service in the ability to provide of the APT provise. CA Certificates Upload If service. It is the ability to provide.	Advanced		Active	Disabled	•	membership can be configured
802.1x Box 1 A Traversal Box 1 Mode Box 2.1x Mode CA Certificates Box 2.1x Mode Box 2.1x Mox 2.1x Mode Box 2.1x			Packet Interval (1~3600s)	60		physically relocating devices or
802.1x						
B02.1x B0			-			method (from highest to
802.1x Mode EAP-PEAP/GTC Its a general term if techniques that ests Provisioning Mode Unauthenticated Provisit ~ Its a general term if techniques that ests Anonymous Identify Anonymous Its a general term if techniques that ests Identity Yealnk You can configure N MD5 Password Forwsen Forwsen CA Certificates Upload Browsen Quality of Service			. •			configuration->DHCP VLAN
SU2_1X Mode EAP-PEAP/GTC techniques that ests Provisioning Mode Unauthenticated Provisic ~ maintain IP connecti Anonymous Identity Anonymous traversing NAT gate Identity yealink You can configure N MD5 Password for the IP phone. Guilty of Service CA Certificates Upload If service		802.1x				
Provisioning Mode Unauthenticated Provisic + traversing NAT gate Anonymous Identity Anonymous is one of the NAT traversing NAT gate Identity yealnk You can configure N MD5 Password •••••••• For the IP phone. CA Certificates Upload Upload			802.1x Mode	EAP-PEAP/GTC	-	techniques that establish and
Anonymous identity Anonymous techniques. Identity yeaink You can configure N MD5 Password For the IP phone. CA Certificates Browse Upload It is the ability to provide solution of freem provides of the freem provides of the provides			Provisioning Mode	Unauthenticated Provisic	-	traversing NAT gateways. STUN
MD5 Password ••••••• You can configure N for the IP phone. CA Certificates Upload Browse Quality of Service It is the ability to pr different priorities fo			Anonymous Identity	Anonymous		is one of the NAT traversal techniques.
CA Certificates Upload Browse Quality of Service It is the ability to produce of the ability to produce of the ability to produce of the ability of the a			Identity	yealink		You can configure NAT traversal
CA Certificates Upload It is the ability to pr different priorities fo			MD5 Password	•••••		for the IP phone.
different priorities fo			CA Certificates	beolau	Browse	Quality of Service (QoS) It is the ability to provide
Device Certificates Upload allowing the transpo		L	Device Certificates		Browse	different priorities for different packets in the network, allowing the transport of traffic with special requirements.

- 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.

ealink 1236					Log O English(English)	
	Status Accou	Int 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	12.			NAT Traversal	
		802.1x Mode	EAP-TTLS/EAP-GTC	•	It is a general term for techniques that establish and	
		Provisioning Mode	Unauthenticated Provisi	*	maintain IP connections traversing NAT gateways. STU	
		Anonymous Identity	Anonymous		is one of the NAT traversal	
		Identity	vealink		techniques.	
			-		You can configure NAT travers for the IP phone.	
		MD5 Password	•••••	-		
		CA Certificates	Upload	Browse	Quality of Service (QoS) It is the ability to provide	
			Ohnan	Browse	different priorities for different packets in the network,	
		Device Certificates	Upload	0.04/36	allowing the transport of traffic	
		Confirm			with special requirements.	

- 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.
 - (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.

ealink T23G	Status	Account	Network	DSSK	ey Featu	ires	Settings	Directory
	LLC							
Basic		PP						NOTE
PC Port			Active		Enabled	•		VLAN
			Packet Interval (1~3	600s)	60			It is used to logically divide a physical network into several
NAT	CDI	þ						broadcast domains. VLAN
Advanced	-		Active		Disabled	•		membership can be configured through software instead of
			Packet Interval (1~3	600s)	60			physically relocating devices or connections.
								The priority of VLAN assignmen method (from highest to
								lowest) :LLDP/CDP->manual configuration->DHCP VLAN
	802							
	802	.1x					1	NAT Traversal It is a general term for
			802.1x Mode		EAP-FAST	•		techniques that establish and maintain IP connections
			Provisioning Mode		Unauthenticated	Provisic 🔻		traversing NAT gateways. STU
			Anonymous Identity		Anonymous			is one of the NAT traversal techniques.
			Identity		yealink			
			MD5 Password					You can configure NAT travers for the IP phone.
						(Browse	Quality of Service (QoS)
			CA Certificates		Upload			It is the ability to provide different priorities for different
							Browse	packets in the network,
			Device Certificates		1			allowing the transport of traffic

- 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,

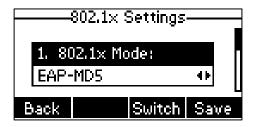
EAP-TTLS/EAP-GTC or EAP-FAST mode, you should upload CA certificate in advance using configuration files or via the web user interface. For SIP IP phones running firmware version 81 or later, the CA certificate needs to be uploaded only when **Authenticated Provisioning** mode is selected from the **Provisioning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

If you select EAP-TLS mode, you should upload the CA certificate and device certificate in advance using configuration files or via the 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:

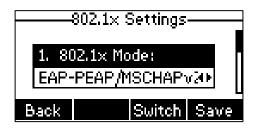
- 1. Press Menu->Settings->Advanced Settings (default password: admin) ->Network->802.1x.
- Press (•) or (•) , or the Switch soft key to select the desired value from the 802.1x
 Mode field.
 - a) If you select EAP-MD5:



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

	802.1× \$	Settings						
1. 80	1. 802.1× Mode:							
EAP-	TLS		41					
Back		Switch	Save					

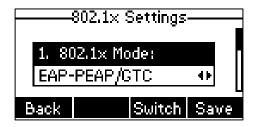
- 1) Enter the user name for authentication in the Identity field.
- 2) Leave the MD5 Password field blank.
- c) If you select EAP-PEAP/MSCHAPv2:



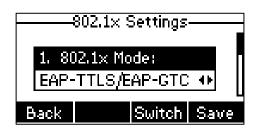
- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.
- d) If you select EAP-TTLS/EAP-MSCHAPv2:

802.	1× Settings						
1. 802.1:	« Mode:						
EAP-TTLS/EAP-MSCH+							
Back	Switch Save						

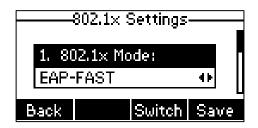
- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.
- e) If you select EAP-PEAP/GTC:



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



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



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

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

802.1X Authentication Process

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

Pre-authentication

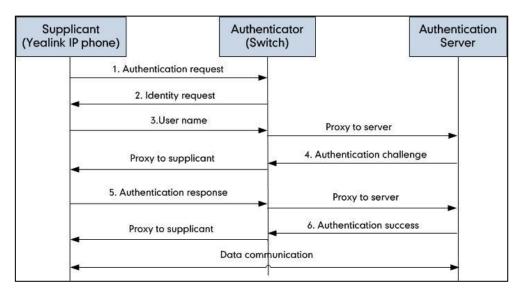
The 802.1X pre-authentication process begins with the IP phone that contains a supplicant service used for negotiation and authentication. When the IP phone connects to an unauthorized port, the authenticator blocks the IP phone from connecting to the network. Using one of the authentication protocols,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

for the authenticator, and then the authenticator forwards the information to the authentication server.

Authentication

After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator grants the IP phone access to the protected network on an authorized port. The following figure summarizes the 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 fi	rom /trunk-1.10)]		
File Edit View Go Capture Analyze Statistics	Telephony Tools Int	ernals <u>H</u> elp	
● ● 💉 🔳 🔬 🖻 🖄 🗶 😂 🔍 🗢	🔹 🤹 🐺 生 🔳) 🗐 I Q Q Q 🔟 I 📓 🕅 🥵 💥 I 💢	
Filter: eap eapol	-	Expression Clear Apply Save Filter	
No. Time Source	Destination Protoco	I Length 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 TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Certifica	ate 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	Nearest TLSV1		ate 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, Certifica	
130 18.447360000 XiamenYe_73:4c:f1	Nearest TLSv1		ange 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, Cha	ange 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	
٠		m	4
<pre> B Frame 118: 60 bytes on wire (480 bits B Ethernet II, Src: XiamenYe_73:4c:f1 B 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	i2 from /tru	ak-1.10)]	
ile <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inte	nals <u>H</u> elp	
	🕒 🗎 🗶 🔁 🔍 🔶	a a 🛪 🛣	1	🗐 🗨 Q. Q. 💟 📓 🖉 🅵 % 🗮	
		~ ~ u			
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)	
14 4.004604000		Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
	XiamenYe_73:4c:f1	Nearest	TLSV1	116 Client Hello	
	Cisco_5d:42:94	Nearest	TLSV1	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	Cisco_5d:42:94	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
	XiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
	cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
	cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
	xiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
	cisco_5d:42:94	Nearest	TLSV1	77 Application Data	
	xiamenYe_73:4c:f1	Nearest	TLSV1	162 Application Data, Application Data	
	cisco_5d:42:94	Nearest	TLSV1	109 Application Data	
	<pre>XiamenYe_73:4c:f1</pre>	Nearest	TLSV1	98 Application Data, Application Data	
	Cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
	XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
56 5.877757000	Cisco_5d:42:94	Nearest	EAP	60 Success	
				m	
Ethernet II, Sr 802.1X Authenti Version: 802. Type: EAP Pac Length: 12	c: XiamenYe_73:4c:f1 cation 1X-2001 (1)	(00:15:65:		d (480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
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-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 F	Rev 54262 from	m /trunk-1.10)]		
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Internal	s Help	
0		🖹 🗎 🗶 🛃 🔍 🔶	a a 🛪	1] (, , , , , , , , , , , , ,	
•	e 🛲 🛲 344		~ • U			
Filter:	eap eapol			▼ Expr	ession Clear Apply Save Filter	
No.		Source	Destination			
		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		L042 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		LO38 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)	
		Cisco_5d:42:94 XiamenYe_73:4c:f1	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		cisco_5d:42:94	Nearest	TLSV1 TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		XiamenYe 73:4c:f1	Nearest	EAP	83 Change Cipher Spec, Encrypted Handshake Message 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	
	2112207 52000	01000_00142104	near coe	674	m	
•						•
					(480 bits) on interface 0	
			(00:15:65:	73:4c:f1),	Dst: Nearest (01:80:c2:00:03)	
	2.1X Authentic					
	Version: 802.1					
	Type: EAP Pack	(U)				
	Length: 12	thentication Protocol				
	Code: Respor					
	Id: 1	ise (2)				
	Length: 12					
	Type: Ident:	ity (1)				
	Identity: y					
	zuenercy. y					

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

EAP-TTLS E	AP-GTC .p	capng [Wireshark 1.10.5 (9	WN Rev 54262	from /trunk	-1.10)]	
<u>E</u> lle <u>E</u> dit <u>V</u> ie	w <u>G</u> o	Capture Analyze Statistics	Telephony	<u>r</u> ools <u>I</u> ntern	als <u>H</u> elp	
0 🖲 🔏		🖻 🖹 🗶 🔁 🛛 🔍 🔶	🔿 🥥 🐺	2 6	∃ (Q, Q, Q, III) 👪 🗹 🍕 ※) 🙀	
Filter: eap e	eapol			- Exp	pression Clear Apply Save Filter	
lo. Time		Source	Destination	Protocol L	enath Info	
6 3.1281	12000	cisco_5d:42:94	Nearest	EAPOL	60 Start	
7 3.1313	27000	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	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	
		<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	114 Application Data, Application Data	
		cisco_5d:42:94	Nearest	TLSV1	97 Application Data	
		xiamenYe_73:4c:f1	Nearest	TLSV1	130 Application Data, Application Data	
48 5.0119	40000	Cisco_5d:42:94	Nearest	EAP	60 Success	
					III.	
					(480 bits) on interface 0	
			(00:15:65:7	'3:4c:f1),	Dst: Nearest (01:80:c2:00:00:03)	
802.1X A						
		LX-2001 (1)				
Туре: Б		(et (U)				
Length						
		thentication Protocol				
	Respor	ise (2)				
Id: 1	:h: 12					
	:n: 12 : Identi	(m) (1)				
Idem	tity: ye	earmik				

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

		ireshark 1.10.5 (SVN Rev 54				•
le	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	<u>T</u> ools <u>I</u> nter	mals <u>H</u> elp	
) 🔬 📕 🔬 🖲	🖻 🖀 🗶 🍠 🔍 🔶	👒 🤹 🖗	2 🗐	🗐 Q, Q, Q, 🔟 👹 🔟 畅 % 💢	
ilter	: eap eapol			▼ E	xpression Clear Apply Save Filter	
	Time	Source	Destination		Length Info	
		XiamenYe_45:6f:bb	Nearest	EAPOL	60 Start	
		cisco_5d:42:94	Nearest	EAP	60 Request, Identity	
		XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity	
		Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)	
		XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)	
		cisco_5d:42:94	Nearest	TLSV1	60 Ignored Unknown Record	
		XiamenYe_45:6f:bb Cisco_5d:42:94	Nearest	TLSV1	80 Client Hello	
		Cisco_50:42:94 XiamenYe 45:6f:bb	Nearest	TLSV1 EAP	1030 Server Hello, Certificate, Certificate Request, Server Hello Done 60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)	
		cisco_5d:42:94	Nearest	EAP TLSV1	483 Server Hello, Certificate, Certificate Request, Server Hello Done	
		XiamenYe 45:6f:bb	Nearest	TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
		Cisco_5d:42:94	Nearest	TLSV1	109 Change Cipher Spec. Encrypted Handshake Message. Application Data	
		XiamenYe 45:6f:bb	Nearest	TLSV1	63 Application Data	
		Cisco 5d:42:94	Nearest	TLSV1	87 Application Data	
		XiamenYe_45:6f:bb	Nearest	TLSV1	83 Application Data	
		Cisco 5d:42:94	Nearest	TLSV1	115 Application Data	
		XiamenYe_45:6f:bb	Nearest	TLSV1	131 Application Data	
		cisco_5d:42:94	Nearest	TLSV1	279 Application Data	
		XiamenYe 45:6f:bb	Nearest	TLSV1	65 Application Data	
	20.302200000	X1000000	Near ese	TESV4	m m	
-						
					ed (480 bits) on interface 0	
				45:6f:bb)), Dst: Nearest (01:80:c2:00:00:03)	
		Nearest (01:80:c2:00:				
		nYe_45:6f:bb (00:15:6)		
		Authentication (0x888				
	2.1X Authenti	000000000000000000000000000000000000000	000000000000000000000000000000000000000	0000000000	00000	
	Version: 802.					
	Type: EAP Pac					
	Length: 10	Kec (0)				
		thentication Protocol				
	Code: Respo					
	Id: 1	inse (e)				
	Length: 10					
	Type: Ident	ity (1)				

Sample Screenshots - Anonymous Identity

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

4 TLC			01	
	ark 1.10.5 (SVN Rev 54262 fr	-		
<u>File Edit View Go</u>	Capture Analyze Statistics	Telephony	<u>r</u> ools <u>I</u> nternals	Heb
0 0 🖌 📕 🔬	🖹 🗋 🗶 🎜 🔍 🔶	🏟 🥥 👬	1 🗐 🖬	IQQQ 🔄 📓 📓 % 🙀
Filter: eap eapol			 Expre 	ssion Clear Apply Save Filter
	Source	Destination		
116 17.805503000		Nearest	EAPOL	60 Start
117 17.808685000		Nearest	EAP	60 Request, Identity
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Identity
119 17.819739000		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)
	XiamenYe_73:4c:f1	Nearest		12 Client Hello
122 17.857040000		Nearest		042 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
	xiamenYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
124 17.867698000		Nearest		M42 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
	<pre>xiamenYe_73:4c:f1</pre>	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
126 17.882798000		Nearest		44 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
	XiamenYe_73:4c:f1	Nearest		166 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
131 18.457674000		Nearest	EAP	60 Request, TLS EAP (EAP-TLS)
	XiamenYe_73:4c:f1	Nearest		327 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
133 18.478941000		Nearest	TLSV1	87 Change Cipher Spec, Encrypted Handshake Message
	XiamenYe_73:4c:f1	Nearest	EAP	60 Response, TLS EAP (EAP-TLS)
146 19.516815000	C1SC0_5d:42:94	Nearest	EAP	60 Success
<				III
 Ethernet II, Sro 802.1X Authentic Version: 802.1 Type: EAP Pack Length: 12 	:: xiamenye_73:4c:f1 (:ation xx-2001 (1) :et (0) :hentication Protocol ise (2)			(480 bits) on interface 0 st: Nearest (01:80:c2:00:00:03)

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

EAP-	PEAP MSCHPv2.	pcapng [Wireshark 1.10.5	(SVN Rev 5426	i2 from /trun	k-1.10)]	
e <u>E</u> c	dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp	
		🕒 🗎 🗶 🔁 🔍 🔶	💩 📣 🛣	1 E	E C C Q 🗹 📓 🛛 🍕 💥	
	/		~ ~ T			
ter:	eap eapol			▼ Ex	pression Clear Apply Save Filter	
. Ti		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	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		Cisco_5d:42:94	Nearest	TLSV1	1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		XiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
		cisco_5d:42:94	Nearest	TLSV1	522 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
		xiamenYe_73:4c:f1	Nearest	TLSV1	226 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
31 4	.779122000	cisco_5d:42:94	Nearest	TLSV1	83 Change Cipher Spec, Encrypted Handshake Message	
		xiamenYe_73:4c:f1	Nearest	EAP	60 Response, Protected EAP (EAP-PEAP)	
334	.797998000	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	
364	.818037000	xiamenYe_73:4c:f1	Nearest	TLSV1	162 Application Data, Application Data	
		Cisco_5d:42:94	Nearest	TLSV1	109 Application Data	
		<pre>xiamenYe_73:4c:f1</pre>	Nearest	TLSV1	98 Application Data, Application Data	
394	.840065000	Cisco_5d:42:94	Nearest	TLSV1	61 Application Data	
		XiamenYe_73:4c:f1	Nearest	TLSV1	98 Application Data, Application Data	
56 5	5.877757000	Cisco_5d:42:94	Nearest	EAP	60 Success	
					m	
					d (480 bits) on interface 0	
			(00:15:65:	73:4c:f1)	, Dst: Nearest (01:80:c2:00:00:03)	
	.1X Authenti ersion: 802.					
	pe: EAP Pac					
	ength: 12	Ket (0)				
		thentication Protocol				
	Code: Respo					
	Id: 1	lise (2)				
	Length: 12					
	cengun, 12					
	Type: Ident	ity (1)				

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

📕 EA	EAP-TTLS EAP-MSCHAPv2.pcapng [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]							
Ele	Edit View Go	Capture Analyze Statistics	Telephony	Tools Intern	nals <u>H</u> elp			
0 (• 🖌 🔳 🔬	🖻 🛍 🗶 🔁 🔍 🔶	🕸 🥥 😽	4 8	🗐 Q, Q, Q, 🔟 🎬 🕅 🥵 % 💢			
Filter	: eap eapol			▼ Exp	pression 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			
		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	112 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, Tunneled TLS EAP (EAP-TTLS)			
		cisco 5d:42:94	Nearest					
		Cisco_5d:42:94 XiamenYe_73:4c:f1	Nearest	TLSV1 EAP	1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 60 Response, Tunneled TLS EAP (EAP-TTLS)			
		Cisco 5d:42:94	Nearest	EAP TLSV1	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	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			
× [
•								
					(480 bits) on interface 0			
			(00:15:65:)	73:4c:f1),	, Dst: Nearest (01:80:c2:00:00:03)			
	2.1X Authenti							
	version: 802.							
	Type: EAP Pac Length: 12	Ket (U)						
		thentication Protocol						
	Code: Respo							
	Id: 1	13e (2)						
	Length: 12							
	Type: Ident	ity (1)						
	Identity: A							
	Lucificity, A	nony mores						

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

<pre> for type go Capture Analyze Statistics Telephony Tools Internals Heb</pre>	×
Item Source Destination Protocol Length Info 30 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Report, I.dentity 31 12, 30085000 Sisco_5d:42:94 Nearest EAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest EAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest TAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest TAP 60 Report, I.Porteted EAP (EAP-PEAP) 41 12, 54485000 Sisco_5d:42:94 Nearest TAP 60 Report, Porteted EAP (EAP-PEAP) 41 12, 54485000 Sisco_5d:42:94 Nearest TAS 116 Cirint Hello 61 2, 52568000 Sisco_5d:42:94 Nearest TAS 120 Startes, Server Key Exchange, Server Hello Done 61 2, 52568000 Sisco_5d:42:94 Nearest TISV1 252 Server Hello, Certifficat, Server Key Exchange, Server Hello Done	
Item Source Destination Protocol Length Info 30 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Start 31 12, 303852000 Cisco_5d:42:94 Nearest EAPOL 60 Report, I.dentity 31 12, 30085000 Sisco_5d:42:94 Nearest EAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest EAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest TAP 60 Report, I.S EAP (EAP-PEAP) 31 12, 30085000 Sisco_5d:42:94 Nearest TAP 60 Report, I.Porteted EAP (EAP-PEAP) 41 12, 54485000 Sisco_5d:42:94 Nearest TAP 60 Report, Porteted EAP (EAP-PEAP) 41 12, 54485000 Sisco_5d:42:94 Nearest TAS 116 Cirint Hello 61 2, 52568000 Sisco_5d:42:94 Nearest TAS 120 Startes, Server Key Exchange, Server Hello Done 61 2, 52568000 Sisco_5d:42:94 Nearest TISV1 252 Server Hello, Certifficat, Server Key Exchange, Server Hello Done	
Time Source Destination Protocol length Info 30 12.303852000 Cisco_Sd:42:94 Nearest EAPOL 60 Start 31 12.303742000 Cisco_Sd:42:94 Nearest EAPOL 60 Start 31 12.303742000 Cisco_Sd:42:94 Nearest EAP 60 Response, Identity 32 12.303852000 Cisco_Sd:42:94 Nearest EAP 60 Response, Identity 32 12.30285000 Cisco_Sd:42:94 Nearest EAP 60 Response, Identity 34 12.30285000 Cisco_Sd:42:94 Nearest EAP 60 Response, Identity 41 12.5 JA888000 Sianomic Zisco_Sd:42:94 Nearest TLSVI 116 Ciston Hello 41 12.5 JA888000 Sianomic Zisco_Sd:42:94 Nearest TLSVI 116 Ciston Hello 51 12.5 S240000 Sianomic Zisco_Sd:42:94 Nearest TLSVI 116 Ciston Hello 51 12.5 S240000 Sianomic Zisco_Sd:42:94 Nearest TLSVI 128 Cistonge Sizcon Sianomic Sizco_Sd:42:94 51 12.5 S240000 Xianomic Xian	
30 12.303852000 citsco_36142:94 Nearest EAPOL 60 Start 312.30744000 citsco_36142:94 Nearest EAP 60 Request, Identity 32 12.30184000 xismenve_73:4c:f1 Nearest EAP 60 Request, Identity 32 12.30184000 citsco_3614:94 Nearest EAP 60 Request, ISER (EAP-TLS) 31 12.370267000 citsco_3614:94 Nearest TLSVI 116 Citent Hello 41 12.5138000 citsco_3614:94 Nearest TLSVI 116 Citent Hello 41 12.5138000 citsco_3614:94 Nearest TLSVI 11042 Server Hello, certificate, Server Key Exchange, Server Hello Done 43 12.525808000 citsco_3614:94 Nearest TLSVI 1042 Server Hello, certificate, Server Key Exchange, Server Hello Done 50 12.525808000 citsco_3614:94 Nearest TLSVI 1028 Server Hello, certificate, Server Key Exchange, Server Hello Done 51 12.53448000 citsco_3614:94 Nearest TLSVI 228 citent Key Exchange (FAP-FEAP) 51 12.53448000 cites_0414:94 Nearest TLSVI 226 Citent Key Exchange (FAP-FEAP) 51 12.53448000 cites_0414:94 Nearest TLSVI 226 Citent Key Exchange (FAP-FEAP) 51 13.1000 cites_0414:94 Nearest TLSVI 226 Citent Key Exchange (FAP-FEAP) 51 13.1000 cites_0414:94 Nearest TLSVI 226 Citent Key Exchange (FAP-FEAP) 51 13.1000 cites_0414:94 Nearest TLSVI 206 Offent Spec, Encrypted Handshake Message 61 13.132850000 cites_0414:94 Nearest TLSVI 30 Application Data 61 13.1000000 cites_0414:94 Nearest TLSVI 30 Application Data 61 13.100000000 cites_0414:94 Nearest TLSVI 30 Application Data 61 13.161360000 cites_0414:94 Nearest TLSVI 30 Application Data 61 13.161360000 cites_0414:94 Nearest TLSVI 30 Application Data 61 13.150770000 cites_0414:94 Nearest TLSVI 30 Application Data 71 13.106350000 cites_0414:94 Nearest TLSVI 30 Application Data 71 13.10635000 cites_0414:94 Nearest TLSVI 30 Application Data 71 13.106350000 cites_0414:94 Nearest TLSV	
31 12. 307446000 cisco_3d:42:94 Nearest EAP 60 Request, Identity 32 12. 301846000 Xiasor_2J:42:14 Nearest EAP 60 Request, Identity 31 12. 370207000 Cisco_3d:42:94 Nearest EAP 60 Request, TLS EAP (EAP-FLS) 31 12. 370807000 Xiasor_2J:42:94 Nearest EAP 60 Request, Protected EAP (EAP-FLS) 31 12. 370807000 Xiasor_2J:42:94 Nearest EAP 60 Request, Protected EAP (EAP-FLAP) 41 12. 514898000 Xiasor_2J:42:94 Nearest TLSV1 116 Citent Hello 41 12. 514898000 Xiasor_2J:42:94 Nearest TLSV1 110 Citent Hello 51 12. 524553000 Xiasor_2J:42:94 Nearest TLSV1 102 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12. 524553000 Xiasor_2J:42:94 Nearest TLSV1 125 Seponse, Protected EAP (EAP-FEAP) 51 12. 524553000 Xiasor_2J:42:94 Nearest TLSV1 125 Seponse, Protected EAP (EAP-FEAP) 51 12. 524563000 Xiasor_2J:42:94 Nearest TLSV1 225 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12. 51 534418000 Xiasor_2J:42:94 Nearest	
32 12.361184000 Ximmerve_73:4c:f1 Nearest EAP 60 Response, Identity 31 12.370207000 Cisco_342:394 Nearest EAP 60 Response, Legacy Nak (Response only) 33 12.370207000 Cisco_342:394 Nearest EAP 60 Response, Legacy Nak (Response only) 33 12.370287000 Cisco_342:394 Nearest EAP 60 Response, Legacy Nak (Response only) 33 12.370287000 Cisco_342:394 Nearest TLSVI 116 Client Hello 41 12.51381000 Cisco_342:394 Nearest TLSVI 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 43 12.52808000 Cisco_342:394 Nearest TLSVI 1032 Server Hello, Certificate, Server Key Exchange, Server Hello Done 50 12.53448000 Cisco_342:394 Nearest TLSVI 125 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12.53448000 Cisco_342:394 Nearest TLSVI 226 Client Key Exchange (Far-PEAP) 51 12.53448000 Cisco_342:394 Nearest TLSVI 226 Client Key Exchange (Far-PEAP) 51 12.53448000 Cisco_342:394 Nearest TLSVI 226 Client Key Exchange (Far-PEAP) 51 13.5577000 Ci	
33 12.370207000 cisco_5d:42:94 Nearest EAP 60 Request, TLS EAP (EAP-TLS) 34 12.370207000 xiacore_73:4c:f1 Nearest EAP 60 Request, TLS EAP (EAP-TLS) 35 12.328255000 xiacore_73:4c:f1 Nearest EAP 60 Request, Protected EAP (EAP-FEAP) 35 12.328255000 xiacore_73:4c:f1 Nearest EAP 60 Request, Protected EAP (EAP-FEAP) 47 12.513891000 xiacore_73:4c:f1 Nearest TLSV1 116 Citent Hello 47 12.513891000 xiacore_73:4c:f1 Nearest TLSV1 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 47 12.513891000 xiacore_73:4c:f1 Nearest TLSV1 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12.52526000 xiacore_73:4c:f1 Nearest TLSV1 225 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 13.15431000 xiacore_34:2:94 Nearest TLSV1 225 Server Hello, Certificate, Server Key Exchange, Server Hello Done 61 13.111673000 xiacore_34:2:94 Nearest TLSV1 225 Server Hello, Certificate, Server Key Exchange, Server Hello Done 61 13.111673000 xiacore_34:42:94 Nearest TLSV1 225 Serve	
34 12, 370987000 Ximmerve_77:4:cf1 Nearest EAP 60 Response, Legacy Nak (Response only) 35 12, 32825000 Cisco_44:2:94 Nearest TEV 60 Response, Legacy Nak (Response only) 45 12, 32825000 Cisco_44:2:94 Nearest TEV 116 Client Hello 47 12, 5138000 Cisco_44:2:94 Nearest TEV 104 Server Hello, certificate, server Key Exchange, server Hello Done 47 12, 5138000 Cisco_44:2:94 Nearest TEV 104 Server Hello, certificate, server Key Exchange, server Hello Done 50 12, 52480800 Cisco_44:2:94 Nearest TEV 103 Server Hello, certificate, server Key Exchange, server Hello Done 50 12, 53448000 Cisco_44:2:94 Nearest TEV 522 Server Hello, Certificate, server Key Exchange, server Hello Done 51 12, 53448000 Cisco_44:2:94 Nearest TEV 522 Server Hello, Certificate, server Key Exchange, choryted Handshake Message 61 13, 12623000 Cisco_44:2:94 Nearest TEV 522 Server Hello, Certificate, server Key Exchange, choryted Handshake Message 61 13, 12623000 Cisco_44:2:94 Nearest TEV 52 Server Hello, Cisco_44:2:4:94 Nearest 61 13, 12623000 Cisco_44:2:94 N	
3312.38285000 cisco_3d-42:94 Nearest EAP 60 Request, profected EAP (EAP-PEAP) 4512.47780200 Xianery 2:3:4:f1 Nearest TLSVI 116 (fint Hello 4712.513891000 cisco_3d:42:94 Nearest TLSVI 116 (fint Hello 4712.513891000 cisco_3d:42:94 Nearest TLSVI 116 (fint Hello 4712.513891000 cisco_3d:42:94 Nearest FLSVI 1002 Server Hello, certificate, server Key Exchange, Server Hello Done 4912.514898000 xiacovsci Nearest FLSVI 1038 Server Hello, certificate, server Key Exchange, Server Hello Done 5112.52580000 xiacovsci Nearest TLSVI 1208 Server Hello, certificate, server Key Exchange, Server Hello Done 5112.52580000 xiacovsci Nearest TLSVI 120 Server Hello, Certificate, Server Key Exchange, Server Hello Done 6113.11027000 xiacovsci Nearest TLSVI 120 Server Hello, Certificate, Server Key Exchange, Server Hello Done 613.11123227000 cisco_5d:42:94 Nearest TLSVI 130 Alphoneox Kangere, Server Hello Done 613.13063000 xiacovsci Nearest TLSVI 140 Application Data 613.14020000	
46 12.477092000 Ximmerve_73:4c:f1 Nearest TLSV1 116 C1ent Hello 47 12.5138000 Cisco_342:94 Nearest TLSV1 1042 Server Hello EAP 48 12.5138000 Simenve_73:4c:f1 Nearest TLSV1 1042 Server Hello EAP 912.52453000 Cisco_342:94 Nearest EAP EO Response, Protected EAP E	
47 12, 51383000 cisco_5d:42:94 Nearest TLSVI 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 47 12, 51383000 xiascore, 5d:42:94 Nearest TLSVI 1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done 49 12, 524553000 xiascore, 5d:42:94 Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12, 5254000 xiascore, 5d:42:94 Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 51 12, 5254000 xiascore, 5d:42:94 Nearest TLSVI 225 Cerver Hello, Certificate, Server Key Exchange, Server Hello Done 61 31,1026000 xiascore, 73:4c:f1 Nearest TLSVI 225 Cerver Hello, Certificate, Server Key Exchange, Server Hello Done 61 31,1026000 xiascore, 73:4c:f1 Nearest TLSVI 225 Cerver Hello, Certificate, Server Hello, Data 61 31,10360000 xiascore, 73:4c:f1 Nearest TLSVI 280 Application Data 61 31,10450000 xiascore, 73:4c:f1 Nearest TLSVI 98 Application Data 61 31,10450000 xiascore, 73:4c:f1 Nearest TLSVI 98 Application Data 61 31,151350000 xiascore, 73:4c:f1 <	
48.12, 514888000 ximmerve_73:4c:f1 Nearest EAP EAP esponse, Protected EAP (EAP-FEAP) 49.12, 5245808000 citamenve_73:4c:f1 Nearest EAP EAP esponse, Protected EAP (EAP-FEAP) 50.12, 524808000 citamenve_73:4c:f1 Nearest EAP EAP esponse, Protected EAP (EAP-FEAP) 50.12, 524808000 citamenve_73:4c:f1 Nearest EAP EAP esponse, Protected EAP (EAP-FEAP) 51.13, 50000 citamenve_73:4c:f1 Nearest TLSV 522 Server Hello, Certificate, Server Key Exchange, Server Hello Done 63.13, 120000 citamenve_73:4c:f1 Nearest TLSV 522 Server Hello, Pape, Encrypted Handshake Message 63.13, 13088000 citamenve_73:4c:f1 Nearest TLSV 83 Achange Cipher Spec, Encrypted Handshake Message 63.13, 13088000 citamenve_73:4c:f1 Nearest TLSVI 83 Application Data 65.13, 130643000 citamenve_73:4c:f1 Nearest TLSVI 98 Application Data 65.13, 150577000 ximenve_73:4c:f1 Nearest TLSVI 98 Application Data 65.13, 15057000 ximenve_73:4c:f1 Nearest TLSVI 98 Application Data 71.13, 16955000 citamenve_73:4c:f1<	
4912.524553000 cisco_3di42:94 Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 5012.52580000 xiamero, Zist.cfi Nearest TLSVI 1038 Server Hello, Certificate, Server Key Exchange, Server Hello Done 5012.52580000 xiamero, Zist.cfi Nearest TLSVI 222 Server Hello, Certificate, Server Key Exchange, Server Hello Done 5012.52580000 xiamero, Zist.cfi Nearest TLSVI 222 Server Hello, Certificate, Server Key Exchange, Server Hello Done 6013.1000000 xiamero, Zist.cfi Nearest TLSVI 226 Cilent Key Exchange, Change Cilent Key Exchange, Change Cilent Key Exchange, Change Cilent Key Exchange, Server Hello Done 6013.10000000 xiamere, Zist.cfi Nearest TLSVI 83 Change Cilent Key Exchange, Change Cilent Key Exchange, Server Hello Done 6013.10000000 xiamere, Zist.cfi Nearest TLSVI 83 Change Cilent Key Exchange, Server Hello Data 613.10000000 xiamere, Zist.cfi Nearest TLSVI 83 Change Cilent Key Exchange, Server Hello Nearest 613.100000000 xiamere, Zist.cfi Nearest TLSVI 83 Application Data Nearest 613.15050000 xiamere, Zist.cfi Nearest TLSVI 83 Applic	
50 12. 525808000 xismerve_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-FEAP) 51 12. 53448000 cisco_5424:944 Nearest TLS 5044800 cisco_5424:945 Nearest TLS 5044800 cisco_5424:945 62 13. 11673000 xismerve_73:4c:f1 Nearest TLS 5044800 cisco_5424:945 Nearest TLS 5044800 cisco_5424:945 63 13. 12327000 cisco_5424:945 Nearest TLS 5044800 cisco_5424:945 Nearest TLS 5044800 cisco_5424:945 63 13. 130886000 xismerve_73:4c:f1 Nearest TLS 14 60 Response, Protected EAP (EAP-FEAP) 66 13. 130886000 xismerve_73:4c:f1 Nearest TLS 14 61 Response, Protected EAP (EAP-FEAP) 66 13. 130886000 xismerve_73:4c:f1 Nearest TLS 14 61 Response, Protected EAP (EAP-FEAP) 66 13. 130886000 xismerve_73:4c:f1 Nearest TLS 14 98 Application Data, Application Data 67 13. 14824900 cisco_542:944 Nearest TLS 14 98 Application Data, Application Data 71 13. 16958000 cisco_542:944 Nearest TLS 14 98 Application Data, Application Data 71 13. 16958000 cisco_542:944 Nearest TLS 14 98 Application Data, Application Data 71 13. 16958000 cisco_542:944 Nearest TLS 14 98 Application Data	
51 12.534448000 cisco_5d:42:94 Nearest TLSVI 522 Server Hello, certificate, server Key Exchange, server Hello Done 61 13.1105000 xiamero, zisco:fi Nearest TLSVI 522 Server Hello, certificate, server Key Exchange, server Hello Done 61 13.1123227000 cisco_5d:42:94 Nearest TLSVI 226 Cilont Key Exchange, change, change, change, change, server Hello Done 61 13.1038000 xiamero, zisco:fi Nearest TLSVI 236 Cilont Key Exchange, change, ch	
62:13.111673000 ximmerve_73:4c:11 Nearest TLSV1 226 Client Key Exchange (thers pec, Encryptel Handshake Message 63:13.12232000 cisc_342:494 Nearest TLSV1 226 Client Key Exchange (thers pec, Encryptel Handshake Message 63:13.12328000 cisc_342:494 Nearest TLSV1 83 change (ther Spec, Encryptel Handshake Message 63:13.13268000 cisc_342:494 Nearest TLSV1 83 change (ther Spec, Encryptel Handshake Message 65:13.13676000 cisc_342:494 Nearest TLSV1 61 Application Data 66:13.13000 cisc_342:494 Nearest TLSV1 98 Application Data 69:13.13567000 ximenve_73:4c:11 Nearest TLSV1 98 Application Data 69:13.1586000 cisc_342:494 Nearest TLSV1 98 Application Data 70:13.16836000 cisc_342:494 Nearest TLSV1 98 Application Data 71:13.16955000 cisc_342:494 Nearest TLSV1 98 Application Data 71:13.16955000 cisc_35d:42:94 Nearest TLSV1 98 Application Data 71:13.16955000 cisc_35d:42:94 Nearest TLSV1 98 Application Data	
63 13.123827000 cisco_3di42:94 Nearest TLSVI 83 change cipher spec_incrypted Handshake Message 64 13.13086000 xiamerve_7:3:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP) 65 13.137643000 cisco_3di42:94 Nearest TLSVI 98 Application Data 66 13.14080000 xiamerve_7:3:4c:f1 Nearest TLSVI 98 Application Data 68 13.15077000 xiamerve_7:3:4c:f1 Nearest TLSVI 77 Application Data 69 13.15087000 cisco_3d:42:94 Nearest TLSVI 77 Application Data 69 13.15087000 cisco_3d:42:94 Nearest TLSVI 77 Application Data 69 13.15087000 cisco_3d:42:94 Nearest TLSVI 98 Application Data 71 13.16955000 cisco_3d:42:94 Nearest TLSVI 98 Application Data 71 13.16955000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 13.171939000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 13.10955000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 13.2000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 73 2000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 73 2000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 74 74 74 74 74 74 74 74 74 74 74 74 74 7	
64 13.130886000 xianenve_73:4c:f1 Nearest EAP 60 Response, Protected EAP (EAP-PEAP) 65 13.1376405000 citsc_0542:94 Nearest TLSVI 61 Application Data 66 13.140060000 xianenve_73:4c:f1 Nearest TLSVI 98 Application Data 67 13.14824000 citsc_0542:94 Nearest TLSVI 98 Application Data 68 13.150577000 xianenve_73:4c:f1 Nearest TLSVI 98 Application Data 69 13.15882000 citsc_0542:94 Nearest TLSVI 98 Application Data 70 13.161368000 xianenve_73:4c:f1 Nearest TLSVI 98 Application Data 70 13.161368000 citsc_0542:94 Nearest TLSVI 98 Application Data 71 31.1695000 citsc_0542:94 Nearest TLSVI 98 Application Data 72 13.171930000 citsc_0542:94 Nearest TLSVI 98 Application Data 72 13.17193000 citsc_0542:94 Nearest TLSVI 98 Application Data Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Former 32: 60 bytes on wire (480 bits).	
6513.137643000 cisco_3di42:94 Nearest TLSVI 61 Application Data 6513.14060000 xiasmery_73:4c:f1 Nearest TLSVI 98 Application Data 6613.14060000 xiasmery_73:4c:f1 Nearest TLSVI 98 Application Data 6613.14060000 xiasmery_73:4c:f1 Nearest TLSVI 96 Application Data 6813.1408000 cisco_5di42:94 Nearest TLSVI 61 Application Data 7013.1613680000 cisco_5di42:94 Nearest TLSVI 61 Application Data 7113.169554000 cisco_5di42:94 Nearest TLSVI 61 Application Data 713.169554000 cisco_5di42:94 Nearest TLSVI 61 Application Data 713.169554000 cisco_5di42:94 Nearest TLSVI 61 Application Data 713.16954000 cisco_5di42:94 Nearest TLSVI 98 Application Data 713.16954000 cisco_5di42:94 Nearest TLSVI 98 Application Data 1014.2007320000 cisco_5di42:94 Nearest TLSVI 98 Application Data Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits); on interface 0 themerett I, sor: Ni	
66 13.140060000 xianenve_73:4c:f1 Nearest TLSV1 98 Application Data, Application Data 67 13.14824000 cisco_3d:42:94 Nearest TLSV1 77 Application Data 68 13.150577000 xianenve_73:4c:f1 Nearest TLSV1 98 Application Data 691.3.15826000 cisco_3d:42:94 Nearest TLSV1 98 Application Data 713.14836000 cisco_3d:42:94 Nearest TLSV1 98 Application Data 713.16306000 cisco_3d:42:94 Nearest TLSV1 98 Application Data 713.16306000 cisco_3d:42:94 Nearest TLSV1 98 Application Data 713.16306000 cisco_3d:42:94 Nearest TLSV1 98 Application Data, Application Data 7213.171939000 cisco_3d:42:94 Nearest TLSV1 98 Application Data, Application Data 1014.2207320000 cisco_5d:42:94 Nearest TLSV1 98 Application Data, Application Data Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Termerst Termerst Clo1:80:c2:00:00:03)	
67 13.148243000 cisco_sdi42:94 Nearest TLSVI 77 Application Data 69 13.1557000 Xiamerve_73:4c:fl Nearest TLSVI 98 Application Data 69 13.158889000 Cisco_5d:42:94 Nearest TLSVI 98 Application Data 70 13.16388000 Xiamerve_73:4c:fl Nearest TLSVI 98 Application Data 71 13.169354000 Cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 13.171939000 Xiamerve_73:4c:fl Nearest TLSVI 98 Application Data 10 14.220732000 Cisco_5d:42:94 Nearest TLSVI 98 Application Data 72 13.171939000 Xiamerve_73:4c:fl Nearest TLSVI 98 Application Data 10 14.220732000 Cisco_5d:42:94 Nearest TLSVI 98 Application Data 7 Mearest TLSVI 98 Noticition Data Noticition Data 10 14.2207320000 Cisco_5d:42:94 Nearest TLSVI 98 Noticition Data 7 Frame 32: 60 bytes captured (480	
66 13. JS8977000 xismenve_73:4c:f1 Nearest TLSVI 98 Application Data, Application Data 67 13. JS889000 cisco_5d:42:94 Nearest TLSVI 61 Application Data 70 13. J61368000 xismenve_73:4c:f1 Nearest TLSVI 61 Application Data 71 13. J6955000 cisco_5d:42:94 Nearest TLSVI 61 Application Data 72 13. J1939000 xismenve_73:4c:f1 Nearest TLSVI 61 Application Data 72 13. J1939000 cisco_5d:42:94 Nearest TLSVI 61 Application Data 10 14. 220732000 cisco_5d:42:94 Nearest TLSVI 60 Success m m m m Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Eaverst (01:80:c2:00:00:03)	
6913.158889000 cisco_5d:42:94 Nearest TLSVI 61 Application Data 7013.161868000 xiamerve_73:4c:f1 Nearest TLSVI 98 Application Data 713.16186954000 xiamerve_73:4c:f1 Nearest TLSVI 98 Application Data 7213.1618600 xiamerve_73:4c:f1 Nearest TLSVI 98 Application Data 1014.220732000 xiamerve_73:4c:f1 Nearest TLSVI 98 Application Data 114.220732000 cisco_5d:42:94 Nearest TLSVI 98 Application Data 1014.220732000 cisco_5d:42:94 Nearest Coccess ""	
70 13.161368000 xiamenve_73:4c:f1 Nearest TLSvI 98 Application Data, Application Data 71 13.16958000 cisco_5d:42:94 Nearest TLSvI 61 Application Data 72 13.171939000 xiamenve_73:4c:f1 Nearest TLSvI 98 Application Data, Application Data 10 14.220732000 cisco_5d:42:94 Nearest EAP 60 Succes Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethermet II, Src: Xiamenve_73:4c:f1, Dot:Nearest (D1:80:c2:00:00:03)	
7.113.169554000 cisco_sdi42:94 Nearest TLSV1 61 Application Data 7.213.171939000 XiamenYe_73:4c:f1 Nearest TLSV1 98 Application Data, Application Data 10.14.220732000 Cisco_sdi42:94 Nearest EAP 60 Success "" "" Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet 11, Src: Xiamen'e_73:4c:f1, 00:15:65:73:4c:f1), DSt: Nearest (01:80:c2:00:00:03)	
72 13.171939000 xiamenve_73:4c:f1 Nearest TLSv1 98 Application Data, Application Data 10 14.220732000 Cisco_5d:42:94 Nearest EAP 60 Succes Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet II, Src: Xiamenve_73:4c:f1, Jost: Nearest (01:80:c2:00:00:03)	
اللہ اللہ اللہ اللہ اللہ اللہ اللہ اللہ	
Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 Ethernet II, Src: XiamenYe_73:4c:f1 (00:15:65:73:4c:f1), DSt: Nearest (01:80:c2:00:00:03)	
Ethernet II, Src: XiamenYe_73:4c:f1 (00:15:65:73:4c:f1), Dst: Nearest (01:80:c2:00:00:03)	
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: Anonymous	

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 EAP-GTC .p	capng [Wireshark 1.10.5 (S	VN Rev 54262	from /trun	k-1.10)]	
le	Edit View Go	Capture Analyze Statistics	Telephony	Tools Inter	nals Help	
_		🖹 🕅 🗙 🔁 🔍 🔶				
•			~~ ~~ ~~			
Filte	r: eap eapol			▼ Ex	pression Clear Apply Save Filter	
		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)	
		<pre>x1amenYe_/3:4c:T1 cisco 5d:42:94</pre>	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	FAP	60 Response. Tunneled TLS EAP (EAP-TTLS)	
		Cisco 5d:42:94	Nearest	TLSV1	526 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
3	3 3,938665000	XiamenYe 73:4c:f1	Nearest	TLSV1	222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
3	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	
		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	
					III	
E 8	thernet II, Sro 02.1X Authentic Version: 802.3 Type: EAP Pack Length: 12	c: Xiamenye_73:4c:fi cation IX-2001 (1) ket (0) thentication Protocol nse (2)			(480 bits) on interface 0 , Dst: Nearest (01:80:c2:00:00:03)	
	Identity: A					

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

🚺 eap	o-fast.pcapng [W	Vireshark 1.10.5 (SVN Rev 54	262 from /trur	nk-1.10)]	
<u>File</u>	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Telephony	Tools Inter	nals <u>H</u> elp
0 (🖻 🗎 🗶 🎜 🔍 🔶	\Rightarrow 😜 😚	2 🗐	B) Q, Q, Q, 17 👹 12 🥵 % 🕱
Filter:	eap eapol			▼ Đ	xpression Clear Apply Save Filter
lo.		Source	Destination		Length Info
		XiamenYe_45:6f:bb	Nearest	EAPOL	60 Start
		cisco_5d:42:94	Nearest	EAP	60 Request, Identity
		XiamenYe_45:6f:bb	Nearest	EAP	60 Response, Identity
		Cisco_5d:42:94	Nearest	EAP	60 Request, Protected EAP (EAP-PEAP)
		xiamenYe_45:6f:bb	Nearest	EAP	60 Response, Legacy Nak (Response Only)
		cisco_5d:42:94	Nearest	TLSV1	60 Ignored Unknown Record
		xiamenYe_45:6f:bb Cisco 5d:42:94	Nearest	TLSV1	80 Client Hello
		Cisco_5d:42:94 XiamenYe_45:6f:bb	Nearest	TLSV1	1030 Server Hello, Certificate, Certificate Request, Server Hello Done 60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
			Nearest	EAP	
		Cisco_5d:42:94 XiamenYe 45:6f:bb	Nearest	TLSV1	483 Server Hello, Certificate, Certificate Request, Server Hello Done
		cisco 5d:42:94	Nearest	TLSV1 TLSV1	222 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 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 Nearest	TLSV1 TLSV1	87 Application Data
		cisco 5d:42:94	Nearest	TLSV1	115 Application Data
		xiamenYe_45:6f:bb	Nearest	TLSV1	131 Application Data
		Cisco_5d:42:94			279 Application Data
		XiamenYe_45:6f:bb	Nearest	TLSV1 TLSV1	65 Application Data
\$16	27.641334000	X1amenye_45:6T:DD	Nearest	TLSVI	
_					m
					ed (480 bits) on interface 0
			(00:15:65:4	15:6f:bb)	, Dst: Nearest (01:80:c2:00:00:03)
	2.1X Authenti				
	/ersion: 802.				
	Type: EAP Pac	ket (0)			
	ength: 19.				
-		thentication Protocol			
	Code: Respo	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 are 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.
 - 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.

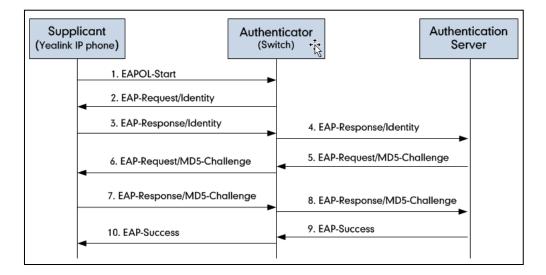
TTLS (Tunneled Transport Layer Security) –Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

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.

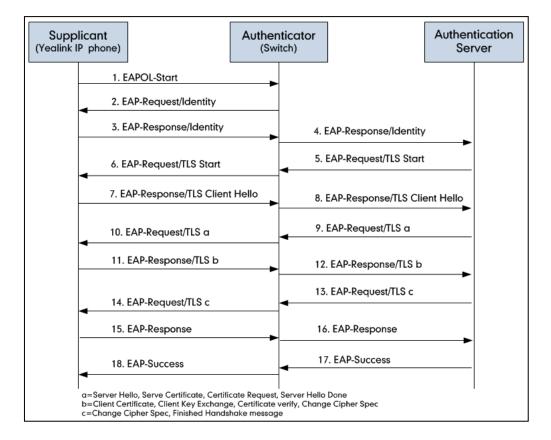


- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.
- 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.
- 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.

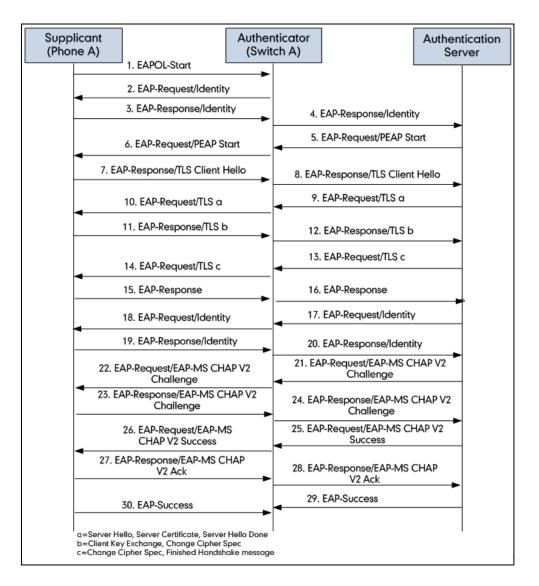
After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to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

- 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 response to the authentication server.
- 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.
- 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 response 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.