

Yealink Technical White Paper

802.1X Authentification

Sep. 2017

Table of Contents

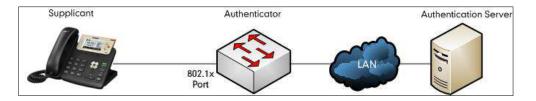
About 802.1X	3
Yealink IP Phones Compatible with 802.1X	3
Configuring 802.1X Settings	5
Configuring 802.1X Using Configuration Files	6
Configuring 802.1X via Web User Interface	12
Configuring 802.1X via Phone User Interface	17
802.1X Authentication Process	19
Sample Screenshots - Identity	21
Sample Screenshots - Anonymous Identity	
Troubleshooting	27
Why doesn't the IP phone pass 802.1X authentication?	27
Appendix A: Glossary	28
Appendix B: 802.1X Authentication Process	29
A Successful Authentication Using EAP-MD5 Protocol	29
A Successful Authentication Using EAP-TLS Protocol	
A Successful Authentication Using EAP-PEAP/MSCHAPv2 Protocol	32
A Successful Authentication Using EAP-TTLS/EAP-MSCHAPv2 Protocol	34
A Successful Authentication Using EAP-PEAP/GTC Protocol	34
A Successful Authentication Using EAP-TTLS/EAP-GTC Protocol	34
A Successful Authentication Using EAP-FAST Protocol	34

About 802.1X

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

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

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



Yealink IP Phones Compatible with 802.1X

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

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

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

Authentication Protocol	IP Phone Models	Firmware Version
	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	Firmware version 81 or later
	T46G,T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60B and CP920	Firmware version 81 or later
	T46G, T42G, T41P, CP860	Firmware version 71 or later
	T48G	Firmware version 72 or later
EAP-TTLS/EAP-MSCHAPv2	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60B and CP920	Firmware version 81 or later
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-PEAP/GTC	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S,	Firmware version 81 or later

Authentication Protocol	IP Phone Models	Firmware Version
	T42S, T41S, T40G, T27G, W52P, W60B and CP920	
	T48G, T46G, T42G, T41P	Firmware version 73 or later
EAP-TTLS/EAP-GTC	T58V/A, T56A, T49G, T40P, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60B and CP920	Firmware version 81 or later
EAP-FAST	T58V/A, T56A, T29G, T27P, T23P/G, T21(P) E2, T19(P) E2, T49G, T48G, T46G, T42G, T41P, T40P, CP860, CP960 and W56P	Firmware version 80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60B and CP920	Firmware version 81 or later

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

Configuring 802.1X Settings

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

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

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

phone user interface to configure 802.1X feature.

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

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

Configuring 802.1X Using Configuration Files

The following IP phones use the new auto provisioning mechanism:

- SIP-T58V/T58A/T56A/CP960 IP phones running firmware version 80 or later
- SIP-T54S/T52S/T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27P/T2 7G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60B, W52P and W56P IP phones running firmware version 81 or later

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

For Old Auto Provisioning Mechanism

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

The following table shows the information of parameters:

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

Parameters	Permitted Values	Default
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x
Settings->802.1x Mode		
network.802_1x.identity	String within 32 characters	Blank
Description:		
Configures the user name for 802.1x authenticatior	۱.	
Note : It works only if the value of the parameter "n	etwork.802 1x.mode" is set t	to 1, 2, 3, 4,
5, 6 or 7. If you change this parameter, the IP phon effect.		
Web User Interface:		
Network->Advanced->802.1x->Identity		
Phone User Interface:		
Menu->Settings->Advanced Settings (default pass Settings->Identity	word: admin) ->Network->8	02.1x
network.802_1x.md5_password	String within 32 characters	Blank
Description:		
Configures the password for 802.1x authentication.		
Note: It works only if the value of the parameter "n	etwork.802_1x.mode" is set t	to 1, 3, 4, 5,
6 or 7. If you change this parameter, the IP phone w	will reboot to make the chan	ge take
effect.		
Web User Interface:		
Network->Advanced->802.1x->MD5 Password		
Phone User Interface:		
Menu->Settings->Advanced Settings (default pass	word: admin) ->Network->8	02.1x
Settings->MD5 Password		
notwork 202 1s root cost un	URL within 511	Blank
network.802_1x.root_cert_url	characters	DIdIIK
Description:		
Configures the access URL of the CA certificate.		
Note: It works only if the value of the parameter "n	etwork.802_1x.mode" is set t	to 2, 3, 4, 5,
6 or 7. The format of the certificate must be *.pem,	*.crt, *.cer or *.der.	
Web User Interface:		
Network->Advanced->802.1x->CA Certificates		

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

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

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

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

Applying the Configuration Files to Your Phone

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

- **1.** Connect your phone to a network that is not 802.1X-enabled.
- Perform the auto provisioning process to apply the configuration files to the phone. Then the IP phone will reboot to make the settings effective.
 For more information on auto provisioning, refer to *Yealink_SIP-T2 Series_T19(P) E2_T4_Series_CP860_W56P_IP_Phones_Auto_Provisioning_Guide.*
- Connect the phone to the 802.1X-enabled network and reboot the phone.
 You can make a phone call to verify whether the phone is authenticated.

For New Auto Provisioning Mechanism

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

Parameters	Permitted Values	Default	
static.network.802_1x.mode	0, 1, 2, 3, 4, 5, 6 or 7	0	
Description:			
Configures the 802.1x authentication method.			
0 -EAP-None			
1 -EAP-MD5			
2 -EAP-TLS			
3 -EAP-PEAP/MSCHAPv2			
4 -EAP-TTLS/EAP-MSCHAPv2			
5-EAP-PEAP/GTC			
6-EAP-TTLS/EAP-GTC			
7 -EAP-FAST			
If it is set to 0 (EAP-None), 802.1x authentication is no	t required.		
Note: If you change this parameter, the IP phone will effect.	reboot to make the chang	e take	
Web User Interface:			
Network->Advanced->802.1x->802.1x Mode			
Phone User Interface:			
Menu->Settings->Advanced Settings (default passwo ->Network->802.1x->802.1x Mode	rd: admin)		
static.network.802_1x.eap_fast_provision_mode	0 or 1	0	
Description:			
Configures the EAP In-Band provisioning method for	EAP-FAST.		
0 -Unauthenticated Provisioning			
1-Authenticated Provisioning			
If it is set to 0 (Unauthenticated Provisioning), EAP In- server unauthenticated PAC (Protected Access Creden Diffie-Hellman key exchange.			
If it is set to 1 (Authenticated Provisioning), EAP In-Ba authenticated PAC provisioning using certificate based		l by server	
Note: It works only if the value of the parameter "stat	c.network.802_1x.mode" i	s set to 7	
(EAP-FAST). If you change this parameter, the IP phon take effect.	e will reboot to make the	change	
Web User Interface:			
Notwork > Advanced > 902.1x > Provisioning Mode			

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

Parameters	Permitted Values	Default			
Phone User Interface:					
None					
static.network.802_1x.anonymous_identity	String within 512 characters	Blank			
Description:					
Configures the anonymous identity (user name) for 80	02.1X authentication.				
It is used for constructing a secure tunnel for 802.1X a	uthentication.				
Note: It works only if the value of the parameter "state 3, 4, 5, 6 or 7. If you change this parameter, the IP phot take effect.					
Web User Interface:					
Network->Advanced->802.1x->Anonymous Identity					
Phone User Interface:					
None					
static.network.802_1x.identity	String within 32 characters	Blank			
Description:					
Configures the user name for 802.1x authentication.					
Note : It works only if the value of the parameter "stati 2, 3, 4, 5, 6 or 7. If you change this parameter, the IP p take effect.					
Web User Interface:					
Network->Advanced->802.1x->Identity					
Phone User Interface:					
Menu->Settings->Advanced Settings (default passwo ->Network->802.1x->Identity	rd: admin)				
static.network.802_1x.md5_password String within 32 characters					
		_			
Description:					
Description: Configures the password for 802.1x authentication.					
-					

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

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

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

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

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

Applying the Configuration Files to Your Phone

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

- 1. Connect your phone to a network that is not 802.1X-enabled.
- Perform the auto provisioning process to apply the configuration files to the phone. Then the IP phone will reboot to make the settings effective.
 For more information on auto provisioning, refer to *Yealink SIP IP Phones Auto Provisioning Guide_V81*.
- Connect the phone to the 802.1X-enabled network and reboot the phone.You can make a phone call to verify whether the phone is authenticated.

Configuring 802.1X via Web User Interface

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

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

Yealink 1234							6	(ing (Jehenpel
Comin K most	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basile	ш						NOTE	
PC Port			Active	Etab	led	•	VLAN	
			Packet Interval (1-3	600a) 60			R m used to b	ogically divide a ork into several
NAT	CD	P)					breadcast dor	
Advanced			Active	Daab	led .	•	through softw	are instead of ating devices a
			Packat Interval (1-3	600x) 60			connections.	using devices s
								f VLAH assignin
			•					CDP->manuai
	802	sta					configuration	
			802.1xMode	EAP-6	05		ILS a general	taim for
			Provisioning Mode	Singu	transcatarit Provinci	-	maintain IP co	
			Anonymous Identity				is one of the l	T gateways, 57 NAT traversal
		1	identity	yépán	6	1.1	techniques.	
			MD5 Pateword				You can confi for the IP pho	gure NAT trave
			CA Certificates			Browns	Quality of Se	
				10/0	10	Brown		tes for differen
			Device Certificates	1008	alt	Contraction of the	packets in the allowing the t	network, ransport of traff
		1.000		10			with special is	ouversents.
		9	unfirm		Cancel		Intelligible Measured	Depe

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

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

fealink 1726	Status	Account	Network	DSSKey	Featur	es)	Settings	Directory	Security
Basic	LLD							NOTE	
PCPort			Active	8	nabled			VLAR	
POPOR			Packet Interval (1-3	9006) 6	0			It is used to lo	
NAT	CDF	8						physical netwo broadcast, dom	WILL VLAN
Advanced			Active	0	eabled			through software	in be configured are instead of
-			Pachet interval (1-3	600s) e	0			physically reloc connections.	ating devices or
									VLAN assignmen
								method (from	highest to
								iowest) 1109/ configuration->	
	802	.1x						NAT Traversal	
			802.1xMede	6	P-TLS		2	It is a general t	term for at establish and
			Provisioning Mode	U	unithermicated P	minist -	3	maintain SP con	mettons
			Anonymous Identity	A	idhymicus			is one of the N	gateways. STU AT traversal
			tdently	38	alnk			techniques.	
			MDS Pasaword					You can config for the IP phot	pare NAT travers
			CA Certificates	E	2		Browskuu	Quality of Se	
			CITCHURALE	1.04	Ipland			It is the ability	to provide
			Device Certificates				BR0W58	different provid	tes for different

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

Yealink							1 an	Ling Out Anh/English)
TO CHITIK (12)5	Status	Account	Network	DSSKey	Features	Settings	Directory	Security
Basic		9P					NOTE	
PCPOT			Active	Enal	bied	(*)	VLAN	
PC PORT			Pactel Interval (1-38	93Dal 65			It is used to it	goly dvide a
RAT	CD						broadcast den	
Advanced			ACE/4	Dea	bled	•		an be configured - are instead of
The state of stores			Packel Interval (1-36	60 (KDR)			physically raise connections.	ating devices or
								VLAN assignment
			:				method (from	
							configuration-	
	802	18					BAT Travess	
			032.1x Mode	EAP-I	PEAP/MSOHAPV2	•		at establish and
			Provisioning Node	Onau	diarcocated Provac	-	maintain IP ca traversing NAT	mectors r gateways, STUN
			Anonymous identity	Anon	ителя		a one of the t techniques.	AT traversal
			Identity:	yealin	k			aure NAT traverial
			HDS Password				for the P abo	
			CA Certificates			Browse	Quality of Se	
			and a second state	Usk	bed			bes for different.
			Device Certificates	1104	640 T	L Bowen	packets in the allowing the ti	network, ransport of traffic
				0.004			with special re	
		6	min		Cancel		High Courses	Duna

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

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

itatus	Account	and the second se						plittinglisti
	Account	Network	DSSK	w F	catures	Settings	Directory	Security
LLD							NOTE	
		Active		Enabled		•	VIAN	
		Packet Interval (1-30	5006)	60			It is used to lo	opcally divide a
CDP							broadcast dan	TOPIS. VLAN
		Active		Deabled		•	through softw	are instead of
		Packet Interval (1-36	9004)	63			sumestans.	cating devices or
								VLAN assignme
		•					configuration	
802.1	*	1000 C 1000 C				-	NAT Traversa It is a general	
							techniques th	at establish and
					stad Proviec		traversing NA1	F gateways, STL
							Techniques.	ovi navelas
			1	realink;		6		page NAT baven
		MDS Password	12				for the IP pho	nł.
		CA Certificates		Miked		- Brancher	Quality of Se It is the ability	to provide
	_	Device Certificates		Ustad		Drome	packets in the allowing the to	network, reneport of treffi
		609 802.1x	Packet interval (1-3) COP Active Packet interval (1-3) Packet interval (1-3) 802.1x 802.1x 802.1x Made Provisioning Mode Anonymous identity Identity MIDS Pasawerd CX Certificates	Packet interval (1-3600s) CDP Active Packet interval (1-3600s) • • • • • • • • • • • • • • • • • • •	Packet interval (1-3690s) od CDP Active Disabled Packet interval (1-3690s) od Packet interval (1-3690s) od	Packet Interval (1-3600s) 64 CDP Active Deabled Packet Interval (1-3600s) 66 Packet Interval (1-3600s) 66 Packet Interval (1-3600s) 66 Provisioning Mode Provisioning Mode Recomment Identity yealsk M05 Password CA Certificates Uption Uption	Packet interval (1-5500s) 66 Active Daabled • Packet interval (1-5900s) 65 • • • • • • • • • • • • •	CDP Packet interval (1-3600s) G Active Active Deabled Active Deabled Active Packet interval (1-3600s) G Active Packet interval Composition Active Packet interval Active Packet Pa

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

	Status	Account	Network	DSSKey	Features	Setting	s Directory Security
Bank	LLD						NOTE
PCPut			Active	Drah	lied		VIAN
			Pactel Interval (1-260)	DH) 60			It is used to logically divide a physical metwork into several
NAT	CD#	S					broadcast domains, VLAN
Advancest			Active	Deab	ked		membership can be configured through software instead of
			Pastel merval (1-369)	Ds) 68			physically relocating denotes or connections.
							The prorty of VLAN assgrime
							method (from highest to lowest) 11LOP/COP -> manual
							configuration->644CP VLAN
	802.	tx _					HAT Traversal It is a general term for
			002.1x Mode	ENP-I	PEAP/GTC	(m)	techniques that establish and
			Provisioning Mode	Unio	therAsisteel Prove	61 ×	maintain IP connections traversing NAT gateways, STU
			Asonymous Mently	Anon	ymeus		is one of the NAT travenal factoriques.
			lawith	yeaks	6.		You can configure RAT travers
			HDS Password				for the IP phone.
			CA Certificates		-14	Browner	Quality of Service (QoS) It is the shifty to provide
		L.		Usk	ad l	Broves	different priorities for different
			Device Certificates	- Oak		- and an and	packets in the network, allowing the transport of traffic

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

ealink m					Log English(English)
	Status Accu	Network 05	SKey Features	Settings	Directory Security
Bask	LLDP				NOTE
PC Port		Activa	Enabled		VLAN
		Packel Interval (1-3600s)	60		It is used to logically divide a
NAT	COP				physical network and several broadcast domains. VLAN
Advanced		Adbre	Deabled	•	membership can be configure through software instead of
		Packet Interval (1-3600s)	60		physically relocating devices in connections.
					The prorty of VLAN assport
		:			method (from highest to lowest) 11.0P/COP->manual
		•			configuration->64CP VLAN
	902.1x				HAT Traversal
		802 Tx Mode	EAP-TTLS/EAP-GTC	•	It is a general term for techniques that establish and
		Provisioning Mode	Unauthenticated Preview	57 E	maintain IP connections travening NAT gateways, 51
		Anonymous identity	Anonymous		is one of the NAT travensi factoriques.
		sterf#y	yealink		You can configure NAT trave
		MDS Password			for the IP phone.
		CA Certificates	1	Browse_	Quality of Service (QoS)
			Ublead		It is the ability to provide different priorities for different
		Device Certificates	Opinad	Bolinia	packets in the network, allowing the transport of traf
		Confem	Cancel		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.
 - 5) (Optional.) In the CA Certificates field, click Browse to select the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.

Yealink					Log Ou English(English)
	Status Accou	Network DS	Skey Features	Settings	Directory Security
Turnit	LLDP				NOTE
PCPort		Active	Enabled		VLAN
		Packet Interval (1-36000)	60		It is used to logically divide a physical network into several
MAY	CDP				broadcast domains. VLAN membership can be configured
Advanced		Active	Deabled	•	through software instead of
		Packet Worvel (1×3600a)	68		physically relocating devices or connections.
					The priority of VLAN assignment
					method (from highest to lowest) sLOP/CDP->manual
	802.1x	1.57			configuration->OHCP VLAN
	002.18	802 fx Mode	EAP-FAST		HAT Transeal It is a general term for
		Provisioning Mode	Unauthenticated Provisio		techniques that establish and maintain IP connections
		Anothimous (dertil)	Approximities		traversing FAAT gateways. STU is one of the NAT traversal
		Identity	vealinik	-	bechriegues.
		MD5 Faseword			You can canfigure NAT traversa for the IP phone.
		CA Certificates	1	Brites-	Quality of Service (QoS)
		LA CELEBRA	Looat		It is the ability to provide different procibes for different.
		Device Certificates	Upload	Broass	packets in the network, allowing the transport of traffic
		Confirm	Cancel		with special requirements.
			10/1.0		Wals Samar Tona

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

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

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

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

Configuring 802.1X via Phone User Interface

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

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

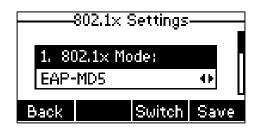
If you select EAP-TLS mode, you should upload CA certificate and device certificate in advance using configuration files or via web user interface.

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

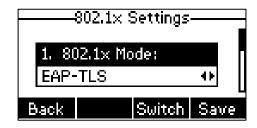
To configure 802.1x via phone user interface:

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

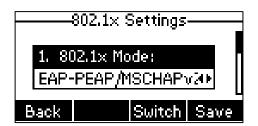
- Press (•) or (•), or the Switch soft key to select the desired value from the 802.1x
 Mode field.
 - a) If you select EAP-MD5:



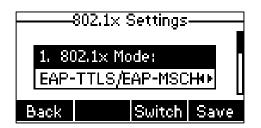
- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.
- **b)** If you select **EAP-TLS**:



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

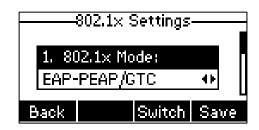


- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.
- d) If you select EAP-TTLS/EAP-MSCHAPv2:

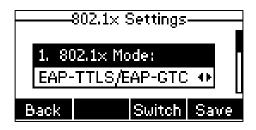


- 1) Enter the user name for authentication in the **Identity** field.
- 2) Enter the password for authentication in the MD5 Password field.

e) If you select EAP-PEAP/GTC:



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



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

	802.1× \$	Settings	
1. 80)2.1× Mo	de:	
EAP-	FAST		41
Back		Switch	Save

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

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

802.1X Authentication Process

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

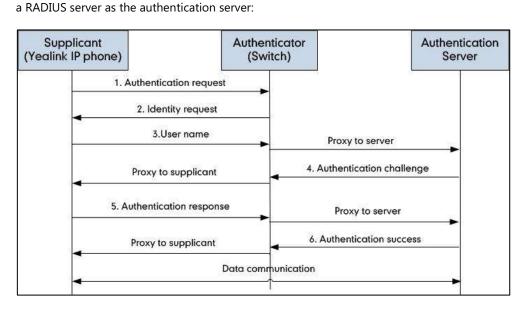
Pre-authentication

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

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

Authentication

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



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

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

Sample Screenshots – Identity

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

Filteri cop I capel			+ E4	pression Char South South Plan	
 Tree 4 2,215726000 5 2,11873600 6 2,266803000 7 2,274229000 8 3,877018000 8 3,77018000 8 3,785803000 1 2,265803000 1 2,265803000 1 4,518729000 	Source Efaces_3d:42:194 (1100_50142134 XFasser56_77746:171 (1100_50142134 (1100_50142134 HTasser56_71145:151 HTasser56_7144 HTasser56_7144 HTasser56_7144 HTasser56_7144	Cestination Near wat Near wat Near wat Near wat Near wat Near wat Near wat Near wat Near wat	Frended L EAPOL EAP EAP EAP EAP EAP EAP	<pre>rept be: 00 Start 00 Folgest, Identity 00 Folgest, IDentity 00 Folgest, This Tar (Car TLS) 00 Folgest, TLS Tar (Car TLS) 00 Folgest, PLS CTulleye Car (Car H0) 00 Folgest, MIS CTulleye Car (Car H0) (CHELINE) 00 Folgest, MIS CTULLEY 00 Folge</pre>	

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

TEEprineng Weinerbark 1.10.5 (Deht Rev 542	and the second sec			10.00
De Ditt yww Go Dottore Andre State		3.11 · · · ·		
O S A S I D D X D N	*****			
Filten exp () expol		+ Expression, Clear Arriv Save filter		
its. Time Source		tocal Length Info		
116 17. 895103000 class_\$5:42-98		HOL 60 Start		
117 17, 808689300 C1510, 58:42:04	NEAPAST EA			
118 17.809119000 htaserve_72:4c:f1				
113 11 813 19000 11050 738 41 m	MLACHER LA			
£30 17.833831000 x1,mmrvve_71(1):71		Lul LL2 Ellent cello	In the second se	54
122 17.857040000 (Vaco.56.42.84 123 17.858234000 stamerye_7314271	Mareit Ti Mareit Ed		e day Exchange, Certificate Research, Devo	m, 440110-04
324 17.807895000 21308078_72182.T1			r Any Cicharga, Certificate Assust, Servi	and had been seen
123 17.807098000 ctarb.50.42.04 123 17.808090000 stanerre_73.42.71		P. LOAD Server Wells, Cartificate, Deriv B Benzonna, TLE AAF (BDP-11.3)	a way exchange, curvincace audotec, nero	6. 04510 Oc
128 17.822798000 Cisto.32:43100			r say exchange, contribute Remonant, Berry	in the line of
130 18, 417360000 statemer 71/dc-f1			, servificate verify, thange digter upen,	
131 18.457674000 Ctorn.3d)42-04	Imarksz EA		d an entress the side strends a durate short	and the second
113 18, 454769300 xinnerve 7114c:P1			, certificate verify, shanie cluber liper.	starupt at
113 18,478941000 Ctsco.58:47.04		by) #7 Change Cipher Spec, Encrypted me		
1.14 14.4876/000H stanevye_7114s:P1				
144 19, 118832000 Chip, 36:47(94	Hearant: 44			
		· · · · · · · · · · · · · · · · · · ·		
<pre>strate 138: 00 bytes on wire (280 Ethernet 11, Src: Xiammire 72-14c) 902.33 Authorit(carion wersing: 002.34-2001 (1) Type: 02-24-2001 (1) Syste: 22 Extendible Authorit(carion Proto- Code: Seaponse (7) 134: 1 Length: 12 Type: Identity (1) Type: Identity (1) Type: Identity (1) Type: Identity (1)</pre>	1 (00:13:85:73:4	apured (480 bits) an interface 0 .:f1), Ont: Newrest (D1:80:c2:00:00:00)		

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

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

Be Edt Vow Do	Unit praying (Worskerk I. Determ (Volice: Statistics	Telephony 1	look jober	tak seb	
	日田 単語 16 - 16 - 1	* * *	祥 110月	9 444C # 8 9 # 8	
then eap eapd			(†) S.	presion. Clear http:// Save Flar	
K T. 1081203810 F 1, 10490300 F 1, 10490300 F 1, 10490300 F 1, 42890300 F 1, 42870300 F 1, 4417723000 T 1, 4417723000 T 1, 104114000 T 1, 104114000 F 1, 104413400 D 1, 408457300 D 4, 1148413400 D 4, 1148413400 T 4, 1148413400 T 4, 1148413400 T 4, 1148413400 T 4, 2221384390 T 4, 222138439 T 4, 22213843 T 4, 22213843 T 4, 2221384 T 4, 2241 T 4, 2241	Source (Frightmenne, 72) 147, (Tr. (Frightmenne, 72) 147, (Tr. Hammenne, 72) 147, (Tr. (Frightmenne, 72) 147, (Tr.), (Tr.	Creations and a second	Pootson 3 5.44901 5.44901 5.449 5.449 5.449 7.1341 6.449 71.34411 71.34411 71.34411 71.34411 71.34411 71.34411 71.34411 71.	<pre>ingl: bit 00 funct 00 funct 00 funct 00 funct 00 function 01 function 01 function 01 function 01 function 01 function 01 function 11 function 12 function 12</pre>	
-					
Ethernet II, Sr 802.1x sutherti Version: 802. Type: EAP Pac Length: 17	<pre>cl Xiammove_T3;4c;f1 cation Lx-300((3) ket (0) thestication regtocol res (2) ity (3)</pre>	600:13:63:7	3:41:51)	(460 bits) as interface 0 , Doi: Nearwest (01:00:02:00:00:01)	

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

No. Design () Design () Product Length () 10 12 2014/0000 Circle () 2014/0000 Circle () 2014/0000 11 12 2014/0000 Circle () Circle () <th>10 22, 39381,7000 11 17, 30744,6000 12 12, 361144006 14 12, 170387000 14 12, 170387000 15 12, 343410000 15 12, 343410000 47 12, 11 0851000</th> <th>clister, 30.42, 14 clister, 32.42, 44 Allessimer, 73.46;71 Allessi, 37.42, 14 Allessi, 37.42, 14 clister, 34.42, 14</th> <th>Anarest Anarest Anarest</th> <th>EADER EAP EAU</th> <th>40 TEarl 40 Request, identity</th> <th></th>	10 22, 39381,7000 11 17, 30744,6000 12 12, 361144006 14 12, 170387000 14 12, 170387000 15 12, 343410000 15 12, 343410000 47 12, 11 0851000	clister, 30.42, 14 clister, 32.42, 44 Allessimer, 73.46;71 Allessi, 37.42, 14 Allessi, 37.42, 14 clister, 34.42, 14	Anarest Anarest Anarest	EADER EAP EAU	40 TEarl 40 Request, identity	
L 12: 1071410000 Cites_15:10:10 12:12:201140000 Ximerry_33:40:11 12:12:20114000 Ximerry_33:40:11 12:12:20124000 Ximerry_33:40:11 12:12:20124000 Ximerry_33:40:11 12:12:20124000 Ximerry_33:40:11 12:12:20124000 Ximerry_33:40:11 12:12:20124000 Ximerry_33:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:20124000 Ximerry_13:40:11 14:12:12:2012400 Ximerry_13:40:11 14:12:12:2012400 Ximerry_13:40:11 14:12:12:2012400 Ximerry_13:40:11 14:12:12:2012400 Ximerry_13:40:11 14:12:12:2012400 Ximerry_13:40:11 15:12:2012400 Ximerry_13:40:11 15:12:	11 12.207446000 12 12.361184000 14 12.170987000 15 12.270987000 15 12.343430000 46 12.477092000 47 12.318891000	check_hd:a2:44 Nameme_/304c:f1 Ohen_hd:42:69 Stamme_/304c:F1 check_hd:42:64	APA*#51 Apa*#55 545/457	EAF	4D Request, identity	
12 12:201144000 41mmerrer, 73:40:11 wave voi 124 40 Accepted, Jewelly, 14 12:2000700 41000, 741000 41000, 74100 40000 4100 40000 4100 40000 4100 4000 4100 4000 4100	12 12, 161144006 14 12, 170797000 14 12, 1707947008 19 12, 14247000 10 12, 477092000 10 12, 477092000 10 12, 110890000	x1aneme_7314ct71 01000_3dt42100 30.ammins_7314tcYt c1000_3dt42100	56.67 657			
<pre>M1 12.1703H702H 33mmrym_17141-171 New rest LAP 00 forcemtes, sugary new (New rest) 151.3040000 c1cm_3/14.144 New rest LAP 00 reprot. Functional Lap 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c11em rest (c126.5/144.4/New rest) 471.3.4700000 c1 c125.3/141 New rest LLP 115 c126 c11em rest (c127.5/144.4/New rest) 471.3.41100000 c1 c125.3/141 New rest LLP 115 c126 c11em rest (c127.5/144.4/New rest) 471.3.41100000 c1 c125.3/141 New rest LLP 115 c126 c11em rest (c127.5/144.4/New rest) 471.3.41100000 c1 c125.3/141 New rest LLP 115 c126 c11em rest (c127.5/144.4/NeW rest) 471.3.41100000 c1 c125.3/141 New rest LLP 11 114 114 114 1141 New rest LLP 11 114 1141 New rest LLP 11 114 114 114 471.411000000 c126.3/141 New rest LLP 11 114 114 114 471.411000000 c126.3/141 New rest LLP 11 114 114 114 471.41100000 c126.3/141 New rest LLP 11 114 114 114 471.411000000 c126.3/141 New rest LLP 11 114 471.4110000000 c126.3/141 New rest LLP 11 471.411000000 c126.3/141 New rest LLP 11 471.4110</pre>	14 12.170947008 15 17.343436000 46 12.477092000 47 32.313893000	30ametris_731412YE c1sts_5d142196		E.A.F		
15 12.1.1.101 Support, Turning Tay (Late Tak) 16 12.1.101 11.1.101 11.1.101 17 12.1.101 Support, Turning Tay, Support 11.1.101 18 12.1.101 11.1.101 11.1.101 18 12.1.101 Support, Turning Late Tay, Support 11.1.101 18 12.1.111 Normation Late Tay, Support 11.1.101 11.1.101 11.1.101 Support, Turning Late Tay, Support 11.1.101 11.1.101 11.1.101 11.1.1.101 Normation Late Tay, Support 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.101 11.1.1.101 11.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.101 11.1.1.1.101 11.1.1.1.101 11.1.1.1.101 11.1.1.1.101 11.1.1.1.1.101 11.1.1.1.1.1.1.1.101 11	15 12.343430000 #e 13.477092000 47 32.313891000	c1103_34142(H)	hear ess.			
<pre>4# 11.4 (192000) class.32 4:04 A Workst TLDA LIS (first webs 4 51.1158/000 class.32 4:04 A Workst TLDA LIS (first webs 4 51.1158/000 class.32 4:04 A Workst TLDA LIS (first webs 4 51.1158/000 class.32 4:04 A Workst TLDA LIS (first webs 5 Separas, Printing LAP, CAP, CAP, CAP, CAP, CAP, CAP, CAP, C</pre>	#E 12,477092000 47 12,113891000			6.45	4D Response, Lagacy Hak (Response (H1y)	
42 13: 13:00100 (Cum.3d.2d.2d.) 4 workst T.C.M. (302) Server wells, certificat, server wells, terter, berrer server in terter bells use 42: 13: 40000 (Cum.3d.2d.2d.) 4 workst T.C.M. (302) Server wells, certificat, server ing Excluse, isorier wells use 42: 13: 54:000 (Cum.3d.2d.2d.) 4 workst T.C.M. (303) Server wells, certificat, server ing Excluse, isorier wells use 42: 13: 54:000 (Cum.3d.2d.2d.) 4 workst T.C.M. (303) Server wells, certificat, server ing Excluse, isorier wells use 42: 13: 54:000 (Cum.3d.2d.2d.) 4 workst T.C.M. (303) Server wells, certificat, server ing Excluse, isorier wells use 41: 13: 13: 1000 (Cum.3d.2d.2d.) 4 workst T.C.M. (302) Server wells, certificat, server ing Excluse, isorier wells use 41: 13: 13: 1000 (Cum.3d.2d.2d.) 4 workst T.C.M. (302) Server wells, certificat, server ing Excluse, isorier wells use 41: 13: 13: 1000 (Cum.3d.2d.2d.) 4 workst T.C.M. (302) Server wells, certificat, server ing Excluse, isorier wells, use 41: 13: 13: 1000 (Cum.3d.2d.2d.) 4 workst T.C.M. (400) (Cum.exp (Cum.ad.2d.) 400 (Cum.2d.2d.) 400 (Cum.2d.2d.) 400 (Cum.2d.2d.) 400 (Cum.2d.2d.) 400 (Cum.2d.2d.) 400 (Cum.2d.2d.2d.) 400 (Cum.2d.2d.4d.) 400 (Cum.2d.2d.2d.) 400 (Cum.2d.2d.	47 12.11 1891000		AM9/101	3.57		
<pre>4 32. 31488000 2) Alexamps.714.517 Were the Lew CD Sectors, Printing LAW (24.9-54.9) 4 32. 51488000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 55448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 514480000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 514480000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51448000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 514491000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51491000 21 Alexamps.714.517 Were the Line Control (24.9-54.9) 5 12. 51491000 21 Alexamps.714.517 Were the Line Control (24.9) 5 12. 51491000 21 Alexamps.714.517 Were the Line Control (24.9) 5 12. 51491000 21 Alexamps.714.517 Were the Line Control (24.9) 5 12. 51491000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21. 51491000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line Control (24.9) 5 21.512.511401000 21 Alexamps.714.517 Were the Line</pre>						
44 12. Statistic close, Statistic and Statis	the set of an annalysis.					
<pre>D112.503000000 Ximmerry_13.4:11 Norrest Law 00 Semperture (APU (First-SLAP)) D112.50300000 Ximmerry_13.4:11 Norrest LAW 00 Semperture (APU (First-SLAP)) D12.514575000 Ximmerry_13.4:11 Norrest LAW 00 Semperture (APU (First-SLAP)) D12.514575000 Ximmerry_13.4:11 Norrest LAW 00 Semperture (APU (First-SLAP)) D12.514750000 Ximmerry_13.4:11 Norrest LAW 00 Semperture (APU (First-SLAP)) D12.51475000 Ximmerry_13.4:11 Norrest LAW 00 Semperture (APU (First-SLAP)) D12.514750000 Ximmerry_13.4:11 Norrest TINI 00 Semperture (APU (First-SLAP)) D12.514750000 Ximmerry_13.4:11 Norrest Ximmerry (First-SLAP) D12.514750000 Ximmerry_13.4:11 Norrest Ximmerry (First-SLAP) D12.514750000 X</pre>						
11 12: JAMAIBOOD C (Cocc. 34 12) M Workst T. 1.541 32: Server wills, Certif(Cat., Server Mr, ToChenge, Driver wills Doro 511:11370700 C (Coc. 37.12) M Workst T. 1.541 32: Server wills, Certif(Cat., Server Mr, ToChenge, Driver Mr, Makage 511:11370700 C (Coc. 37.12) M Workst T. 1.541 32: Certif(Cat. 20, Cat., Server Mr, ToChenge, Driver Mr, Makage 511:11370700 C (Coc. 37.12) M Workst T. 1.541 32: Certif(Cat. 20, Cat., Server Mr, ToChenge, Driver Mr, Makage 511:11370700 C (Coc. 37.12) M Workst T. 1.541 32: Certif(Cat. 20, Cat., Server Mr, Makage 511:11070700 C (Coc. 37.12) M Workst T. 1.541 42: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 42: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst T. 1.541 43: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst 14: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst 14: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst 14: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Workst 14: 40 (Old The Data 511:11070700 C (Coc. 37.12) M Wo						
AL 11.1137/1000 Ximmerine, 71-4:11 wareners 11.501 276 Claret sey Cacharge Claret sey Claret sey Claret sey Cacharge Claret sey Cla						
He 11.1112/1700 C100.57.14; H Marver TLSAL BY Charge Cluber Spec. Everyted moveled Mediage 01.11108/000 C100.57.14; H Marver TLSAL BY CLARPTON FULL BY CLARPTO						
00 11.11000000 tisements_110:000 00 11.11000000 tisements_110:000 00 11.11000000 tisements_110:000 00 11.1000000 tisements_110:000 00 11.1000000 tisements_110:000 00 11.1000000 tisements_110:000 00 11.1000000 tisements_110:000 00 11.1000000 tisements_110:000 01 11.000000 tisements_110:000 01 11.000000 tisements_110:000 01 11.000000 tisements_110:000 01 11.000000 tisements_110:000 01 11.00000 tisements_110:000 01 11.000000 tisements_110:000 01 11.000000 01 11.000000000000000000000000000000000						
H 11.11174-1000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 400/101/94 D12 01.11.1000000 Yimeswar 7140.74 01.11.100000 Yimeswar 7140.74 01.11.100000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.1000000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.100000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.00000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.00000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.00000 C1002.51.42.94 Nov-ett 11.0-1 40 ett 11.0000 01.11.000000 01.11.000000 C10000000 01.11.0000000 01.11.0000000000						
00 11.10000000 viewows_714;1;1; www.set 1.641 46 epification beta, Application beta 01 11.1007/006 views.41 54 www.set 1.641 47 480/041/0 beta 01 11.1007/006 views.41 54 www.set 1.641 46 epification beta 01 01.000000000000000000000000000000000						
<pre>6* 11.1402/3000 C(sus.34) 41.54</pre>						
Milling States and Sta						
eg 13.116855000 C (sam_34/14) Warver TLSA1 & application bas 71.1161865000 C (sam_34/4/14) Warver TLSA1 & application bas 71.1161865000 C (sam_34/4/14) Warver TLSA1 & application bas 71.1161865000 C (sam_34/4/14) Warver TLSA1 & application bas 81.901101000 C (sam_34/4/14) Warver TLSA1 & application bas 80.50000 C (sam_34/14) Warver CLSA1 & application bas 80.500000000000000000000000000000000000						
TI III LELINE ALL ALL ALL ALL ALL ALL ALL ALL ALL AL						
11 13.10015000 C(sam.34.42.54 Worker T(54) & Angel(sam)(sam) but in but is application bu						
72 31.1/1/10/000 sissemme_72-4:ff wearest title! 46 epil/isitim bata, application bata D1 14.7/07/2000 fises Not 32:04 Nearest Law 80 Secrets Frame 32: 40 bytem on wire (ABD bits), 40 bytem taptured (ABD bits) on Interface 8 Ethermet II, Sci Xiemenna_T1-4:f1 (D013163:T144:f1), Doi: Nearest (D1:00:C100:00:00) D02:XX authentication Version 802:XX-2001 (1) Type: Law market (0) Langth: 12 extensible authentication wroncol						
rrame 32: 40 bytes in wire (400 bits), 40 bytes captured (50 bits) an interface 0 Ebbernet II, Sec. Ximmunk_73.46(F1 (50)33183)F1(46(F1), DBL) New 455 (51:85:62100:00103) Wershen: 807,1X-2001 (1) Type: Lew pracket (0) Langth: 12 market Nibe authentication econoci						
* rame 31: 40 bytes an wire (ABO bits), 40 bytes captured (ABO bits) an Interface 0 coherent II, Sec: Xiemerea_T3-4c:f1 (Doil3:05:T1(4c:f1), Dali mearest (D1:B0:c2:00:00:03) MO2.1X authentication Version: 802.3X-2001 (1) Type: Law market (0) Langth: L2 marketNibe authentication wronocol						
tobernet II, Set: Xiemenne_3:44:f1 (00:13:83:71:44:f1), Ost: Newerst (01:80:02:00:00:01) Ost: XA authentitation Version: 802.3X-2001 (1) Type: Law packet (0) Langth: L2 Extensible authentication pronocol						
tbernet II, Sri: Xiemenna_314c(fl (0013193)T14c(fl), Ost) mean est (01-80:c2:00:00:01) 02.18 Auchtenitication Version: 802.3X-2001 (1) Type: Law market (0) Lamgth: L7 Extensible auchtentication promocol	ram 37: 45 ho	ten ten och er földer halten	a cara ta a cara a		d (AEV bilst) on Interface 2	
NO.13 Authentitation Version: 807.1X-2001 (1) Type: Learnet action: (0) Learnet: 12 Extensible authentication econocol						
type: two Packet (0) Langth: 12 mattenille autheotication eronacol			11111111111111			
Langth: 12 Instensible wither fication econocol	Version: 802.7	1X-2001 (1)				
Extensible authentication ecotocol	Type: EAP Fac	ket (0)				
Ende: Response (2)						
101 3.						

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

the first year for	Denare Anivor Statatics Teleph	any Jose Inte	nak jian	
	日日本日 (1994)	(7 1 回)	🔟 Q Q Q 🖉 🗰 🖉 🙀 🐉	
Filter est (estal		(f) =	greator, Dee Appy Save Rhe	
[93.189776036 10 3.200110586 11 4.1106847059 12 1.1106847059 12 1.121394000 13 1.132173060 13 1.134404055 14 3.14404055 14 3.14404055 14 3.14404055 15 4.158846050 15 4.168846050 15 4.1688460000000000000000000000000000000000	stanerve_714ccf1 Hear Chen,Sci2:04 Namerve_754cf1 Hear Chen,Sci2:04 Hear Chen,Sci2:04 Hear Chen,Sci2:04 Hear Chen,Sci2:04 Hear Chen,Sci2:04 Hear	etcl A.PC 247 A.P 813 A.P 814 A.P 815 A.P 816 A.P 817 A.P 818 T.L.PA 818 T.L.PA 818 T.B.PA	<pre>Length twi 60 Years 60 Rears, 100mm(Hy, 60 Response, Tawn Thy 60 Response, Tawn Thy 60 Response, Town New Thi 60 Response, Townshell III Carl (2004 Thi 10 Response, Townshell III Carl (2004 Thi 10 Response, Tawnshell III The 10 Response, Tawnshell III Carl (2004 Thi 10 Response), Tawnshell III Carl (2004 Thi 10 Response), Tawnshell III Carl (2004 Thi 10 Response), Tawnshell (2004 Thi 10 Res</pre>	
EThernet 21, 3r 02.1s Authent3 version: 002. Typs: EAP Pac Congth: 12 Externible Au Code: Respo	c: slamerne_73i4c:f1 (0011 cattion 14-2001 (1) kat (0) shart(cation Protocol nose (2)		(440 htts) en interface 0 , mot) wearest (01:40/c2/00/00/07)	

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

THE PROPERTY AND	ireskaris 1.303. (SAW Res 14	Set area larte	e-CIDE		10.00
Ent then Dr.	Optime Broker Stateter	Telephony (and prov	wa tinta	
	10 D 12 20 10 4		▲ / 個別	14440 #K * s #	
attact to be a set of the	International Action	005.01	- Annotation		
ter: ner I mood			+ 10	pression. Over Arriv See New	
Tires	Sharey	Destination	Protocol -	length into	
	35aleevite_43107.00	New wet	AAPOL -	1.1. Web defeated, including the latency	
	11110.54:42104	SAME WIT:	3.1.P	#2 Heguppt, telectivy	
	#1am(srive_45107108	Nearest.	EMP.	R0 Response, Inercity	
	CTUDE, MC-42194	Vedranit.	EAP .	42 Hegenst, Protected Int (LAP -FLAP) 45 Hegentre, Legacy Mak (Response Unity)	
	winnia Labolation	NUMBER OF COLUMN	71.70/2	45 Yorur ed introdu enterd	
	whiterry_dbiefild	And of Addition	PL 543	as client with	
	CT110.0.00-07194	WHAT NOT	TERMIN	1050 Derver Holls, Centificate, Centificate Respect, Deven Holls form	
	winnership, d'5 (107 (108	NEAR STR.	EAP .	fil Benguman, Allesthis Authentization via Secura Turnaling DAP (EAP-CAUT)	
	Witness Satisfields	APACEST.	TINUE	483 Derver Hella, Certificate, Certificate mequest, perver Hella base	
	slassres at 10.07.00	ARM WITE	11.041	III CATTIFICADE, Climit May Exclusion, chamas clubber tiper, Decourted maniplake secur-	100
	CT10000.0010071002	TRAFFICT.	T1-24/3	IN these these see, second entitles welles, and that he had	
1 20.318254000	WINDOWSTYN, 45,107-34	Many work :	Thinks.	63 Astr21rutttur Sata	
	stano, 58143198	totar wort	11.502	87 Application suca	
	winnerrie_45107188	statest.	73.542	BT Application wata	
	070000.38142194	AND MUCH	75.542	111 martine for the second sec	
	Adapterra., 43:00:00	Fearman.	TEPT	112 AntiStrative Date	
	mines_bmi42164	NEAP NET.	71.55/2	379 Application mate	
77 30, 341306000	stammin_strate	ADAUT WILL	71,992	Wilderfication mata	
				and the second	
ethernet II, m Destination Sector: Alame Type: 602.1x Padding: 0000 802.1x Authenti Version BDL Type: 6AP Fac Length: 10	C: stammers_15:00:00 Nearest (01.80:02:00 Authentication (0x88) Goulepecondoscondosc Gation 1x-2001 (1) Net (0) Destilation Frotour	(001150651) 00103) 514310F186) 63 00000000000000	risteffickel) F	d (ABB bits) um interface 0 , nori mearwar (ULING:c2:00.00:00)	

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:

Filter aspill eacol		Expression, Char large Save filter
No. There Sectors (1997) 112 (199	Definition for a second	to increase, Joseff Up; to increase, Joseff Up; to increase Jo
ream 118. 60 bytes on whre (280 b) Schermet 11, Src: Xiammin, 75:46:10 892.1X withertication version: 502.1X-3001 (1) Type: 52.7 Factor (0) Length: 52 bitterstbic Authoritication Protoco Code: Supports (2) 30.1 Length: 52 Type: Sourting (2) Type: Sourting (2) Type: Sourting (2)	(00:13:85:73:4) J	ptored (480 bits) an interface 8 (f1), Ost: Newrest (01:80:c2:00:00:00)

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

Chem exp () + appl IS. Time Source ID. 10:11:2010 Cisco10:42 ID. 2.422/32:200 Cisco	194	60 Response, Identity	
6-1,82512900 C5500,30:42 10-1,42679000 C5500,30:42 11-1,981630000 x1amenve.73 11-1,981711000 x1amenve.73 11-1,99111000 x1amenve.71	194	nn 60 thart 50 Beguent, identity 6 60 Response, Identity	
14 -000239000 10 accm26 15 -20069000 10 accm2, doi:0 18 -100040000 10 accm2, doi:0 18 -100040000 11 accm2, doi:0 15 -20040000 11 accm2, doi:0 15 -20040000 11 accm2, doi:0 15 -704800000 11 accm2, doi:0 15 -70480000 11 accm2, doi:0 14 -90040000 11 accm2, doi:0 15 -70480000 11 accm2, doi:0 14 -90040000 11 accm2, doi:0 15 -90040000 11 accm2, doi:0 16 -90040000 11 accm2, doi:0 16 -90040000 11 accm2, doi:0 16 -90040000 11 accm2, doi:0 17 -900400000 11 accm2, doi:0 18 -900400000 11 accm2, doi:0 19 -900400000	184 Description Construction Construction 184 Head right Construction Construction <	 e0 Paipersin, segary said (sequence coly); e0 Paipersin, recarding (said-sequence); e15 Clear set10; e15	
in the second		Restaura and a second	

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

Fiber: exp expôt			100	greation Clear http:// Sales Plan	
6 1. 188203810 7 1. 1949.04000 8 21.428912500 9 21.4481275200 12 1.4481275200 12 1.4481275200 12 1.448121600 12 1.5454200 12 1.5454200 12 1.91454000 12 1.9045400 12 1.9045400 12 1.9045400 12 4.1845400 12 4.1845400 12 4.221284200 12 4.221284200	Source (7) Salacenee, 7/1145(17) (7) Salaceneee, 7/1145(17) (7) Salaceneee, 7/1145(17) (7) Salaceneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Construction Notations to Notation of the Notation of the	Protection SAPPOL SAPPOL SAPPOL SAP SAP SLOP SLOP SLOP SLOP SLOP SLOP SLOP SLO	 Lingth Tab. All Itals Al	
				The second se	
Stherman II, Sr 800,1x suthern1 Version: 802, Type: EAP Pac Length: 17	ci Xiamanya_73:4c:f1 cation 1x-300 (1) ket (0) themication restocol rss (2) ity (1)	(00:13:63:	73:41:F1)	(400 Stit) on interface 0 , Oni: Nearest (01:00:02:00:00:01)	

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

And the second second second	Centure gradient gradientes		**************************************	9 4 4 4 5 8 6 5 8 8	
Ren au Lespa			2.1	pretóżk, Oker Amily Save Filler	
10 12. TOP27000 10 12. TOP27000 10 12. TOP2700000 40 12. TOP30000 40 12. TOP30000 40 12. SC48000 40 12. SC48000 40 12. SC48000 40 12. SC48000 40 12. SC48000 40 12. SC48000 40 13. L1027000 40 13. L10270000 40 13. L102700000 40 13. L1027000000000000	Chico, 34: 42-44 Xianeritar , 35: 34: 44 O Bits, 34: 34: 44 O Bits, 34: 34: 44 Chico, 34: 44: 54 Chico, 34: 54: 54: 54: 54: 54: 54: 54: 54: 54: 5	Decision of the second	Protocol 5:400, 8:20 8:20 1:40	<pre>big the for the second starting for accurate starting for acquires, this saw (second starting (wild)) for acquires, this saw (second starting (wild)) for acquires, the saw (second starting (wild)) for acquires, the same starting (second starting (sec</pre>	
Stbernet II, Sri 802.1X authenti Version: 802.1 Type: 84P Fac Length: 12	C: Alementa_73:46:f1 cation IX-2001 (1) ker (0) thertication mrotocol ros (2)	(00)13:65:1	THACIF1)	d (A40 bis) an interface 0 , Dil Newest (DI-BD-L100-00.01)	

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

Fitter eap eapol			(+) H	greatory Dear Acces Save filter	
1 1.187740306 10 1.0014 11 1.10444 12 1.2014 12 1.32731040 12 1.32731040 13 1.16444 14 1.15444 14 1.15444 15 1.3244 16 1.4444 16 1.4544 16 1.4544 16 1.55474000 13 1.55474000 14 1.55474000 14 1.55474000 14 1.55474000 15 1.95474000 14 1.55474000 15 1.9644000 16 1.56774000 16 1.56774000 16 1.56774000 16 1.96742000 11 1.964414000 16 1.974740000 16 1.974740000 16 1.974740000	Secure Class, Sci2100 Krance, 27142 (271 Krance, 27142 (2714) Krance, 27142 (2714) Kr	Destination Environment Environment Environment Media dest Media dest	Portocell 8.1491 2.47 2.47 2.47 2.47 2.47 1.101 1.101 2.47 7.101 1.101 2.47 7.101 1.101 2.47 7.101 1.101	<pre>Leggt bit 60 Heart 60 Heart 60 Heart, 100 Heart 60 Heart 70 Heart</pre>	
				*	
Ethernet 11, 37 822.1x Authent Version: 832. Type: EAP Par Cength: 12	ci slamenve_73/4c/f1 Lation 13-2001 (1) kat (0) mhernication Protocol mod (2)	(00/15/65)		(480 htts) up interface 0 , not incurest (01:40:(2:09:00:00)	

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

tet: exp [expo		Party Party	miton, Dear Atom Save Mer
AN MARCHINE ST	and the second sec	- MM (200	
Time Source	All INT THE INSUMEST	Protocol Lan	ger ans 60 mart southers of
## 27.070149000 (inco Sc		ENP.	50 Reinwort, Interfity
19 27.071627000 xTanetree		EAF	The second se
0 J7.110834000 01000-54		LOP	do Repart, Provide Law (Law Haw)
IL 17.112012000 xlamerry	ALINFIN HANTALL	EAP	80 Galpertan, Legacy has (Response 00/15)
19 17.142441000 clock_H	162194 Hear-est	TUP-1.	VO. zgłócest Grácowi kitoriu
14 27.142682009 xiamiro's		0.545	80 Client sells
15 27-206335000 C1500.56			HIQ Server Hells, Cartificate, Tertificate Request, Server Hells Derw
36 37-259168050 stanenve		KAP	. 00 neiperas, Flexible Authentication via Accure Yoursling nat (East-Fair)
17 27.20033090 Cists,54			403 Server Helle, Certificate, Certificate Republi, Server Hello Done
6.17.az1500000 slapenre			222 cartificate, cfient say Exchange, change cluber spec, torrygrad washinke matta
0 27.400212000 Class,3s			139 Shanga Cipber Spec, Encrypted Haidchake Heccarg, Application Date
10-27.539445000 xlaekmii			HE 40071Cation para
11 17. SABITUGOO S'AND, As		TL 501	BT Application Data
12.27.333172000 Alamanya		TL051	BE Applisation dutta
13.37.543043000 clubb_30 04 27.587037000 xtammarra			115 applistation wata 133 Applitation Wata
13-27. MR283000 Clacp_34			279 And Fication data
E 27. 641234000 timerrie			65 AddTtration Jura
			(480 bits) on interface D DSt: Mearest (01:80:62:00:08:03)
10.1x authentication	serection the faultings	-3101-0031-1	ACT MEANEST (METROPOLITION)
version: 802.1x-2001 (1)		
Type: LAP Packet (0)	-,		
Lergth: 19			
Extensible Authenticat	ion Protocol		
code: #exponse (2)	2011 (N 200207) -		
10: 1			
cength: 19			
Type: Identity (1)			

Troubleshooting

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

Do the following in sequence:

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

network administrator.

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

Appendix A: Glossary

IEEE (Institute of Electrical and Electronics Engineers) –A professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

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

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

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

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

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

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

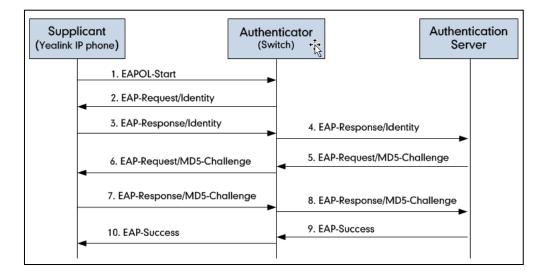
TTLS (Tunneled Transport Layer Security) -Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

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

Appendix B: 802.1X Authentication Process

A Successful Authentication Using EAP-MD5 Protocol

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

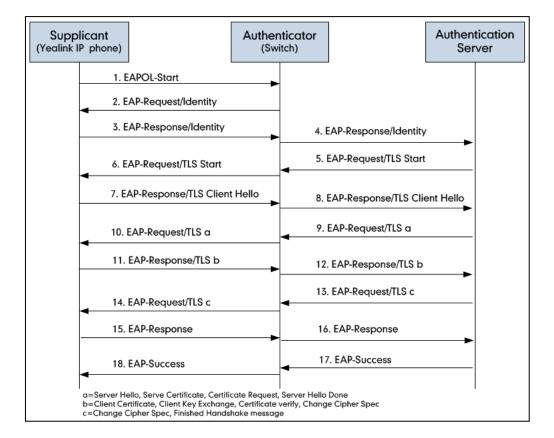


- 1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
- 2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
- 3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
- **4.** The authenticator strips the Ethernet header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

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

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

A Successful Authentication Using EAP-TLS Protocol



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

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

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

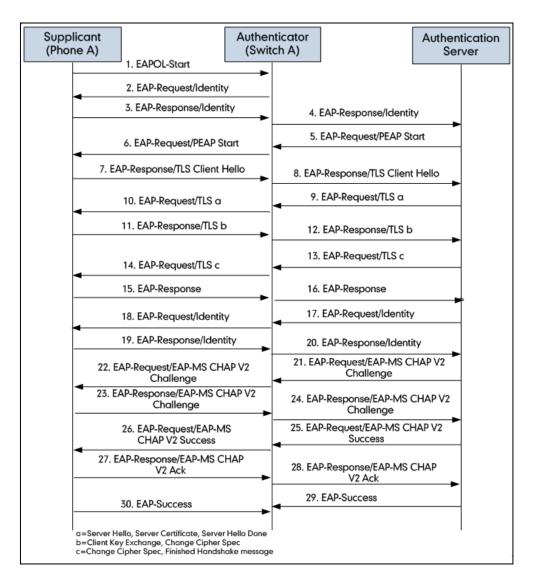
After the supplicant is authenticated successfully, the authenticator provides network access permissions. If the supplicant does not provide proper identification, the authentication server responds with a rejection message. The authenticator passes the message to the supplicant and blocks access to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

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

A Successful Authentication Using EAP-PEAP/MSCHAPv2

Protocol

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



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

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

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

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

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

A Successful Authentication Using EAP-PEAP/GTC Protocol

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

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

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

A Successful Authentication Using EAP-FAST Protocol

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

Customer Feedback

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