Htek IP Phones 802.1x Guide

Version 2.0.4.4.24
Feb. 2018

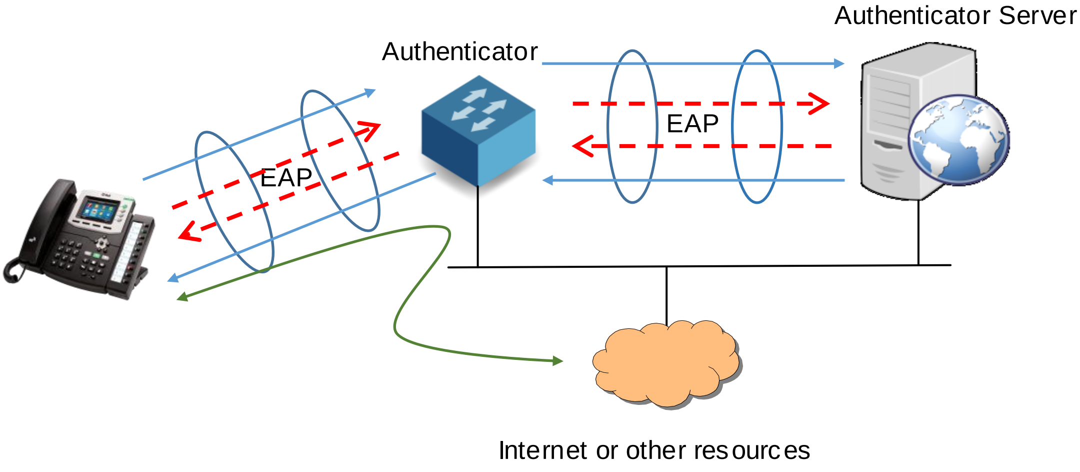
Table of Contents

About 802.1x

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802, which is known as "EAP over LAN" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004.

The 802.1x protocal protects the net be not accessed by the device which is not authorized. An analogy to this is 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, to 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 (client device) is allowed to access resources located on the protected side of the network.



Htek Phone compatible with 802.1x

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

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

Authentication Protocal	IP Phone Models	Firmware version
EAP-MD5	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.97 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.97 or later
EAP-PEAP/MSCHAPV2	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.98 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.98 or later
EAP-TTLS/EAP-MSCHAPv2	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.98 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.98 or later
EAP-PEAP/GTC	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.98 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.98 or later
EAP-TTLS/EAP-GTC	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.98 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.98 or later
EAP-FAST	UC802, UC802T, UC803, UC803T, UC804, UC804T, UC804G, UC806, UC806T, UC806G, UC840, UC842, UC860, UC862	Firmware version 1.0.3.98 or later
	UC902, UC903, UC912, UC912G, UC923, UC924, UC926, UC924E, UC926E	Firmware version 2.0.3.98 or later

Htek IP Phone UC802,UC803,UC804,UC804T,UC806,UC806T,UC840,UC860 support 802.1x as a supplicant, both Pass-thru Mode and Pass-thru Mode with Proxy Logoff. When the device is disconnected from the IP Phone PC port, the Htek IP Phone can provide additional security by sending an EAPOL Logoff message to the Ethernet switch. The proxy logoff will prevents another device from using the port without first authenticating via 802.1x.

802.1x Settings

The 802.1x authentication is disabled on Htek IP Phone by default, you need configure it by three ways:

Configuring 802.1x using configuration files.

Configuring 802.1x via web interface.

Configuring 802.1x via LCD interface.

The first way can be used to autoprovisioning. When you configure 802.1x on the LCD please make sure the phone has its own useful certificate in it. Otherwise you need upload the certificate via web interface.

Configuration files for 802.1x

1. The following table shows the parameters for 802.1x

Web Setting Path	Permitted Values	Descriptions	Parameter
Network→Advanced→802.1x Mode	Number: 0,1,2,3,4,5,6,7	802.1x Mode: 0 - Disable 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	P8626
Network→Advanced→Identity	String within 31 characters	The user name of 802.1x account	P8627
Network→Advanced→MD5 Password	String within 31 characters	The password for account when using MD5 mode.	P8628
Management→Autoprovision→802.1x CA cert URL	URL within 255 characters	The URL locate to your CA cert. The CA cert must be .crt or .pem format.	P20987
Management→Autoprovision→802.1x DEV cert URL	URL within 255 characters	The URL locate to your device cert. The device cert must be .pem format.	P20988

Configure your custom setting in your condfiguration file, for example:

<!--Network/Advance/802.1X-->

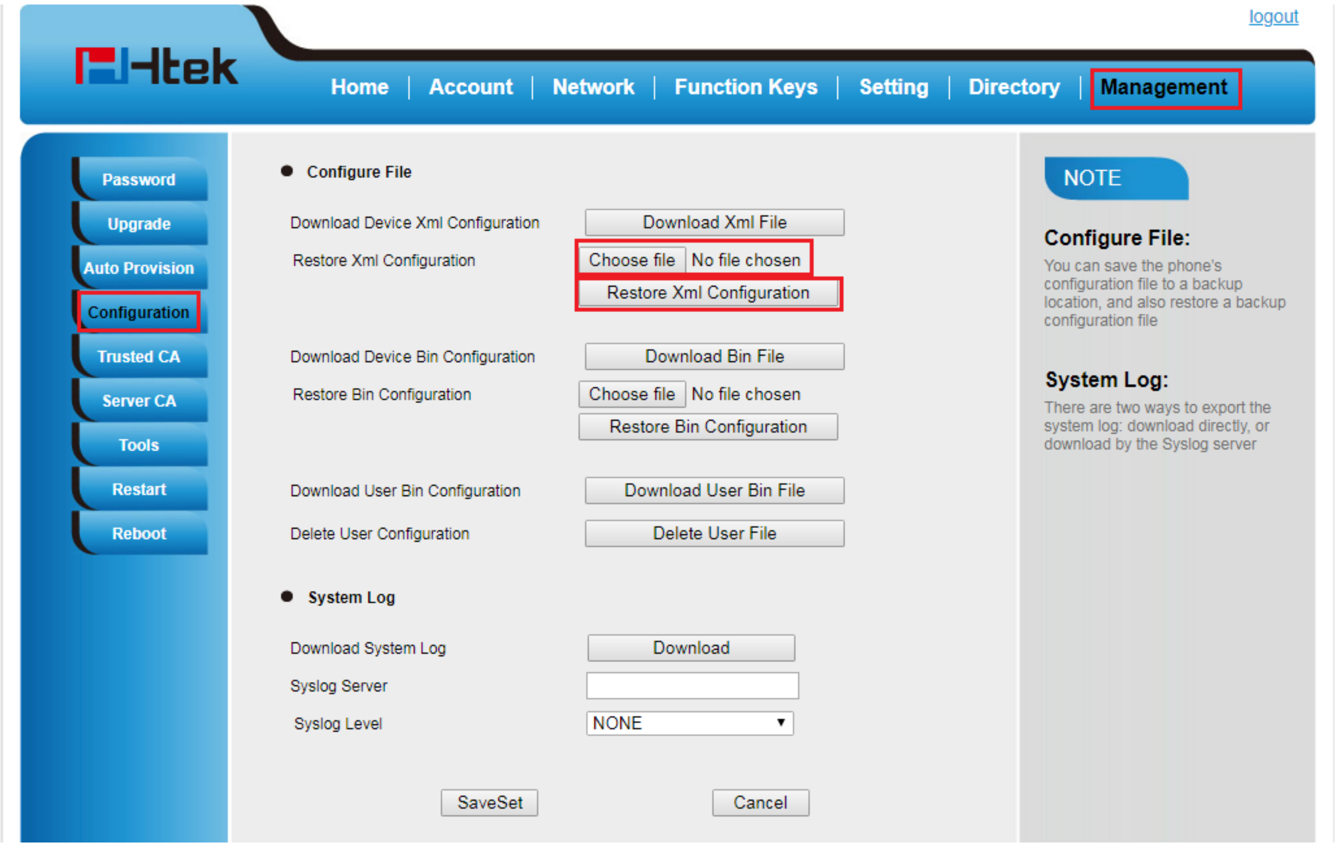
```
<P8626 para="802.1XMode">2</P8626>
<P8627 para="Identity">wirelessuser</P8627>
<P8628 para="MD5Password" />
……
<P20987 para="802.1x CA cert URL">http://192.168.0.54/ca.crt</P20987>
<P20988 para="802.1x DEV cert URL">http://192.168.0.54/device.pem</P20988>
```

When the phone loads the configuration file, it will try to get the cert from the server you have set. Ensure the cert files is stored on your server.

Applying the Configuration file to your phone

Once you have edited the configuration file (cfgmac.xml e.g. cfg001fc11a0001.xml) using the introduced parameters. You can do as follow to ensure the file is effective on your phone.

1. Connect your phone to a network without 802.1x.
2. Log on the phone web, upload your configuration file. Access Management→Configuration, choose your configuration file then upload.



Configure File:

You can save the phone's configuration file to a backup location, and also restore a backup configuration file

System Log:

There are two ways to export the system log: download directly, or download by the Syslog server

Or perform the auto provisioning. Then the phone will reboot to make the settings effective.

For more information about auto provisioning, please refer to

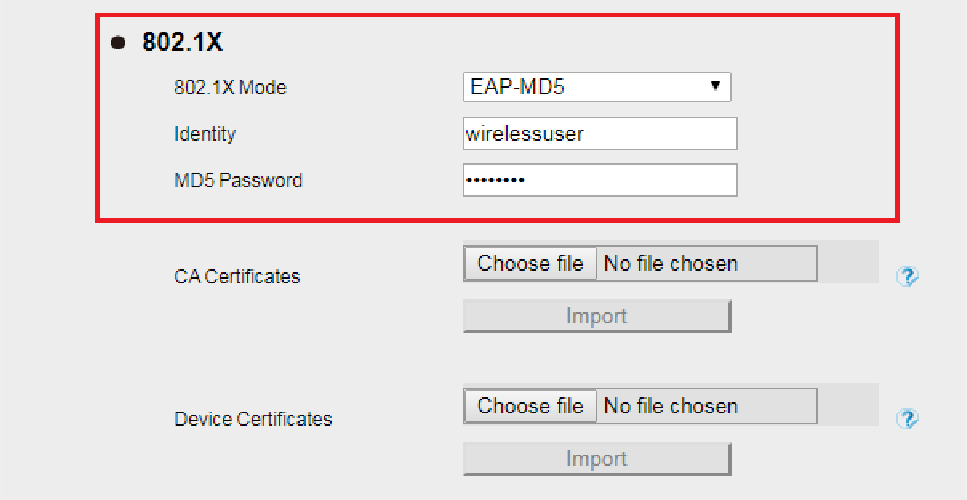
Htek_UC8xx_Series_IP_Phones_Auto_Provision_User_Guide_V4_4_24.doc and Htek_UC9xx_Series_IP_Phones_Auto_Provision_User_Guide_V4_4_24.doc

Configuring 802.1x via web interface

1. Connect your phone to a network without 802.1x.
2. Log on your phone web page.
3. Access Network→Advanced.
4. In the 802.1x block, select the desired protocol from the pull-down list of 802.1x Mode.

I. 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.



● 802.1X

802.1X Mode: EAP-MD5

Identity: wirelessuser

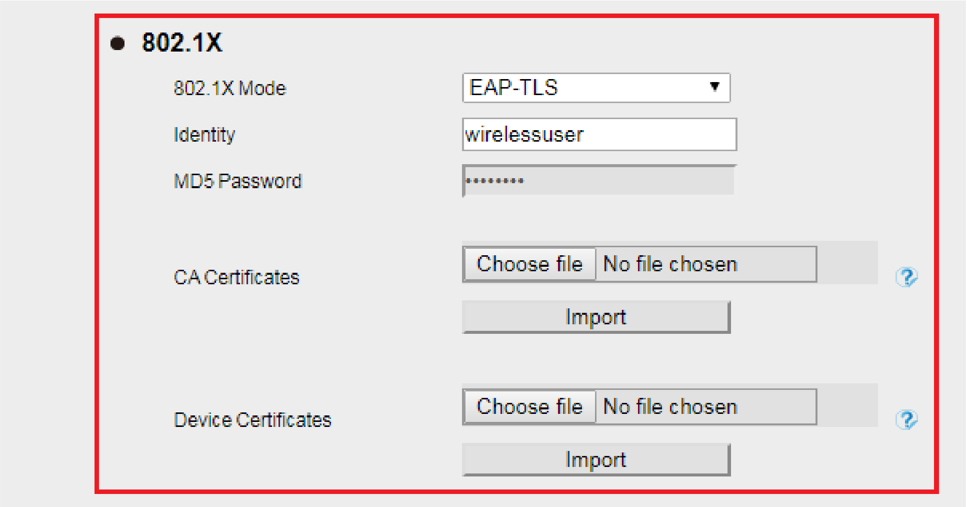
MD5 Password: ••••••••

CA Certificates: Choose file No file chosen

Device Certificates: Choose file No file chosen

II. If you select EAP-TLS:

1) Enter the user name for authentication in the Identity field.
2) Leave the MD5 Password field blank.
3) In the CA Certificates field, click Choose file to select the desired CA certificate.(*.crt, *.pem) from your local system. And upload the file.
4) In the Device Certificates field, click Choose file to select the desired client certificate(*.pem) from your local system(the *.pem file must contain the certificate and key file both in it). Click Import to upload the certificate.



● 802.1X

802.1X Mode: EAP-TLS

Identity: wirelessuser

MD5 Password: ••••••••

CA Certificates: Choose file No file chosen

Import

Device Certificates: Choose file No file chosen

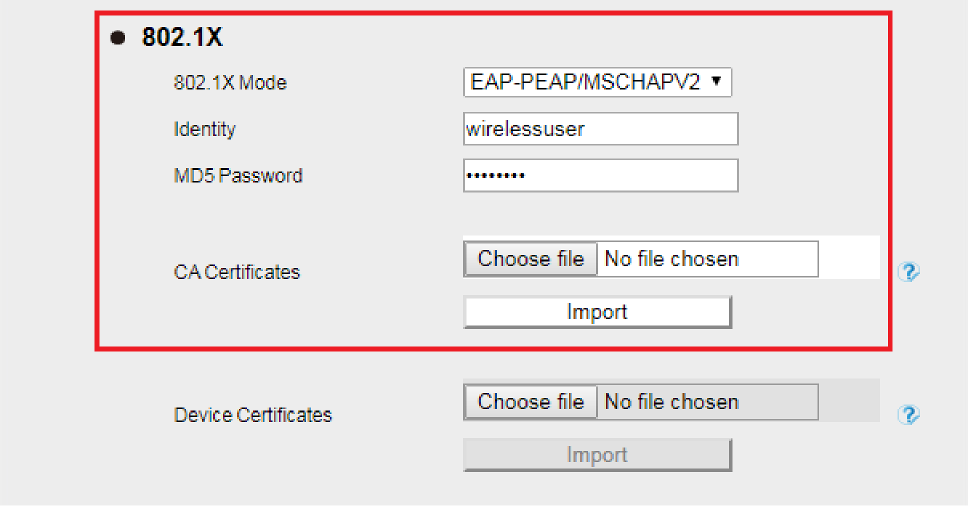
Import

III. 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.

3) In the CA Certificates field, click Choose file to select the desired CA certificate(*.crt, *.pem) in your system. Click Import to upload the certificate.



● 802.1X

802.1X Mode: EAP-PEAP/MSCHAPV2

Identity: wirelessuser

MD5 Password: ••••••••

CA Certificates: Choose file No file chosen

Import

Device Certificates: Choose file No file chosen

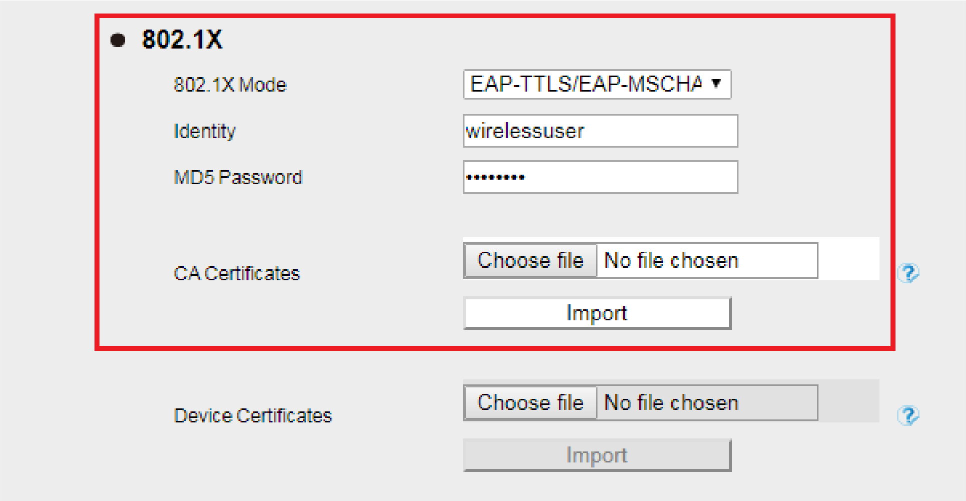
Import

IV. 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.

3) In the CA Certificates field, click Choose file to select the desired CA certificate(*.crt, *.pem) from your local system. Click Import to upload the certificate.

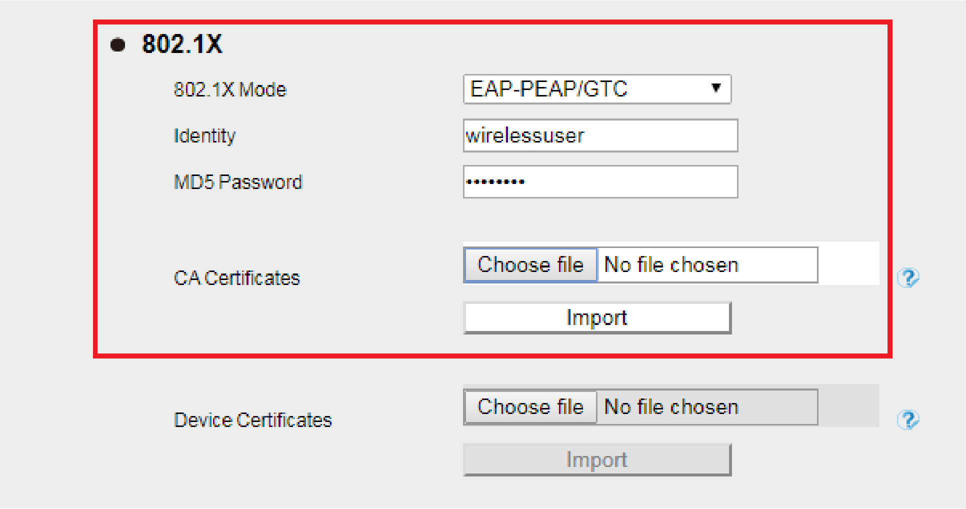


● 802.1X

802.1X Mode	EAP-TTLS/EAP-MSCHA ▾
Identity	wirelessuser
MD5 Password	••••••••
CA Certificates	Choose file No file chosen Import
Device Certificates	Choose file No file chosen Import

V. 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.
3) In the CA Certificates field, click Choose file to select the desired CA certificate(*.crt, *.pem) from your local system. Click Import to upload the certificate.

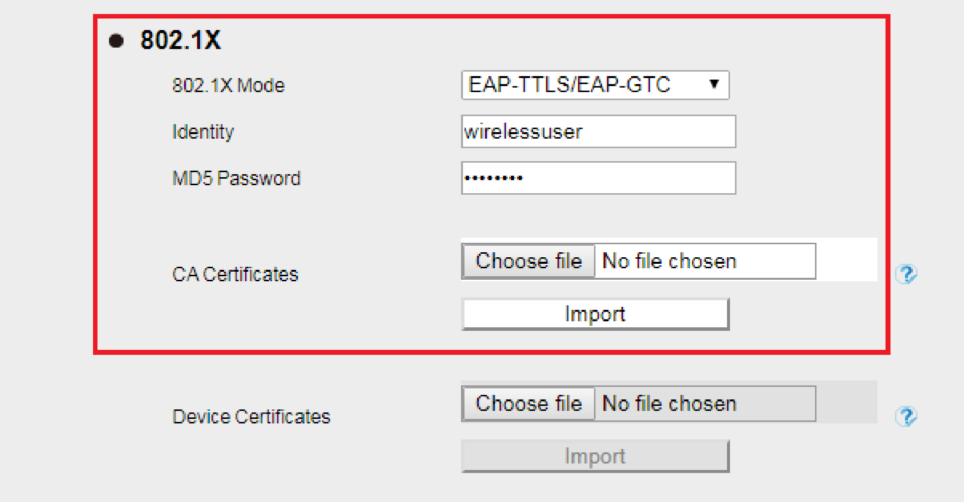


● 802.1X

802.1X Mode	EAP-PEAP/GTC ▾
Identity	wirelessuser
MD5 Password	••••••••
CA Certificates	Choose file No file chosen Import
Device Certificates	Choose file No file chosen Import

VI. 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.
3) In the CA Certificates field, click Choose file to select the desired CA certificate(*.crt, *.pem) from your local system. Click Import to upload the certificate.



● 802.1X

802.1X Mode: EAP-TTLS/EAP-GTC

Identity: wirelessuser

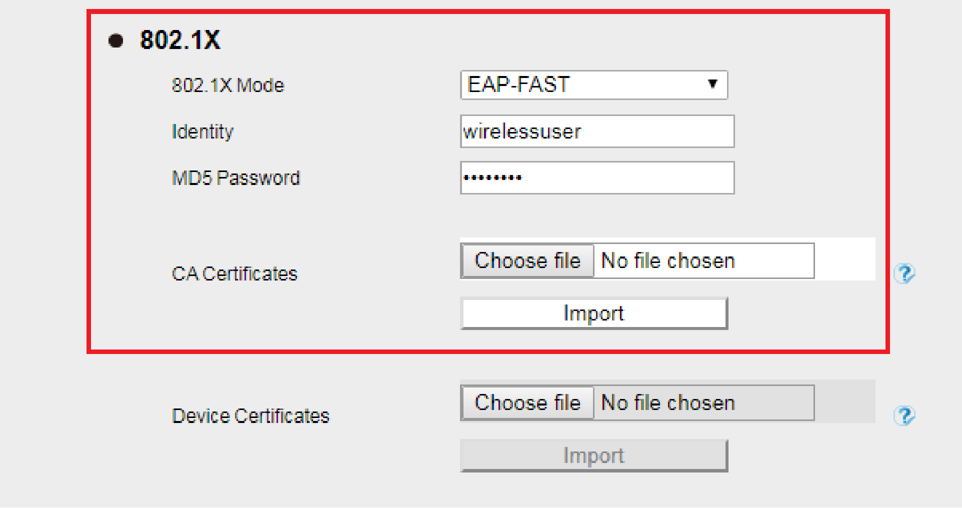
MD5 Password: ••••••••

CA Certificates: No file chosen

Device Certificates: No file chosen

VII. 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) In the CA Certificates field, click Choose file to select the desired CA certificate(*.crt, *.pem)from your local system. Click Import to upload the certificate.



● 802.1X

802.1X Mode: EAP-FAST

Identity: wirelessuser

MD5 Password: ••••••••

CA Certificates: No file chosen

Device Certificates: No file chosen

5. Click Saveset to accept the change.
6. A alert box will remind you the saving change will make the phone reboot.
7. Click OK to reboot the phone.
8. After phone reboot, connect the phone to the network with 802.1x-endabled.

Configuring 802.1x on LCD GUI

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 via loading the configuration files or via web user interface.

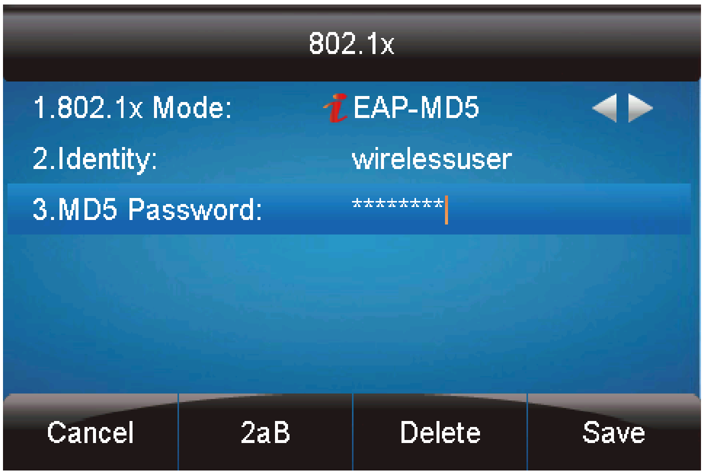
If you select EAP-TLS mode, you should upload CA certificate and device certificate via loading the configuration files or via web user interface.

To configure the 802.1x on the LCD GUI:

1. Press Menu→Settings→Advanced Setting(default password: admin)→ Network →802.1x

2. Press > or <, or the Switch soft key to select the desired value from the 802.1x Mode field.

I. If you select EAP-MD5:



802.1x

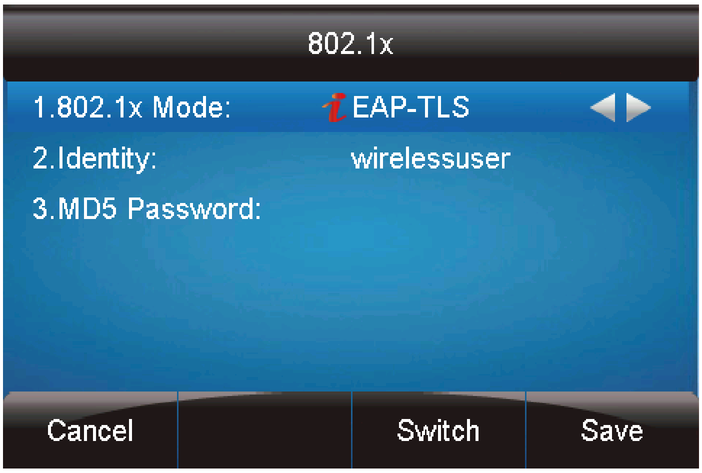
1.802.1x Mode: EAP-MD5

2.Identity: wirelessuser

3.MD5 Password: ********

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

II. If you select EAP-TlS:



802.1x

1.802.1x Mode: EAP-TLS

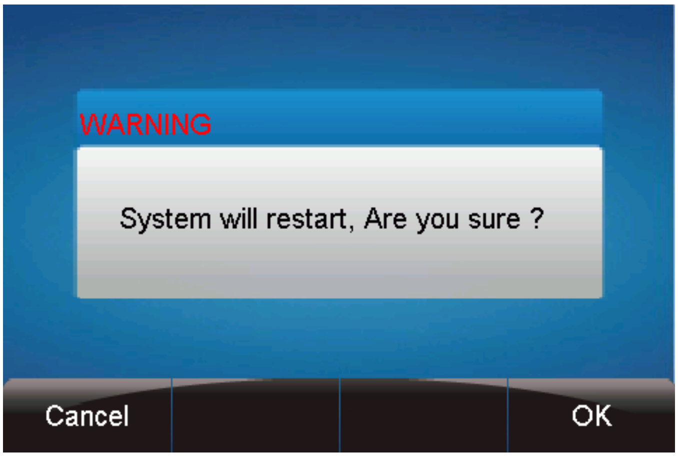
2.Identity: wirelessuser

3.MD5 Password:

1) Enter the user name for authentication in the Identity field.
2) Leave the MD5 Password field blank.

3. Press Save soft key or ✓ to save your change.

Once you save the change, the LCD will alert:


WARNING

System will restart, Are you sure ?

Press OK, or it will restart automatically after 5 seconds.

802.1x Authentication Process:

When the phone is 802.1x enabled and is connected into the network 802.1x enabled. The 802.1x authentication process is divided into two basic stages:

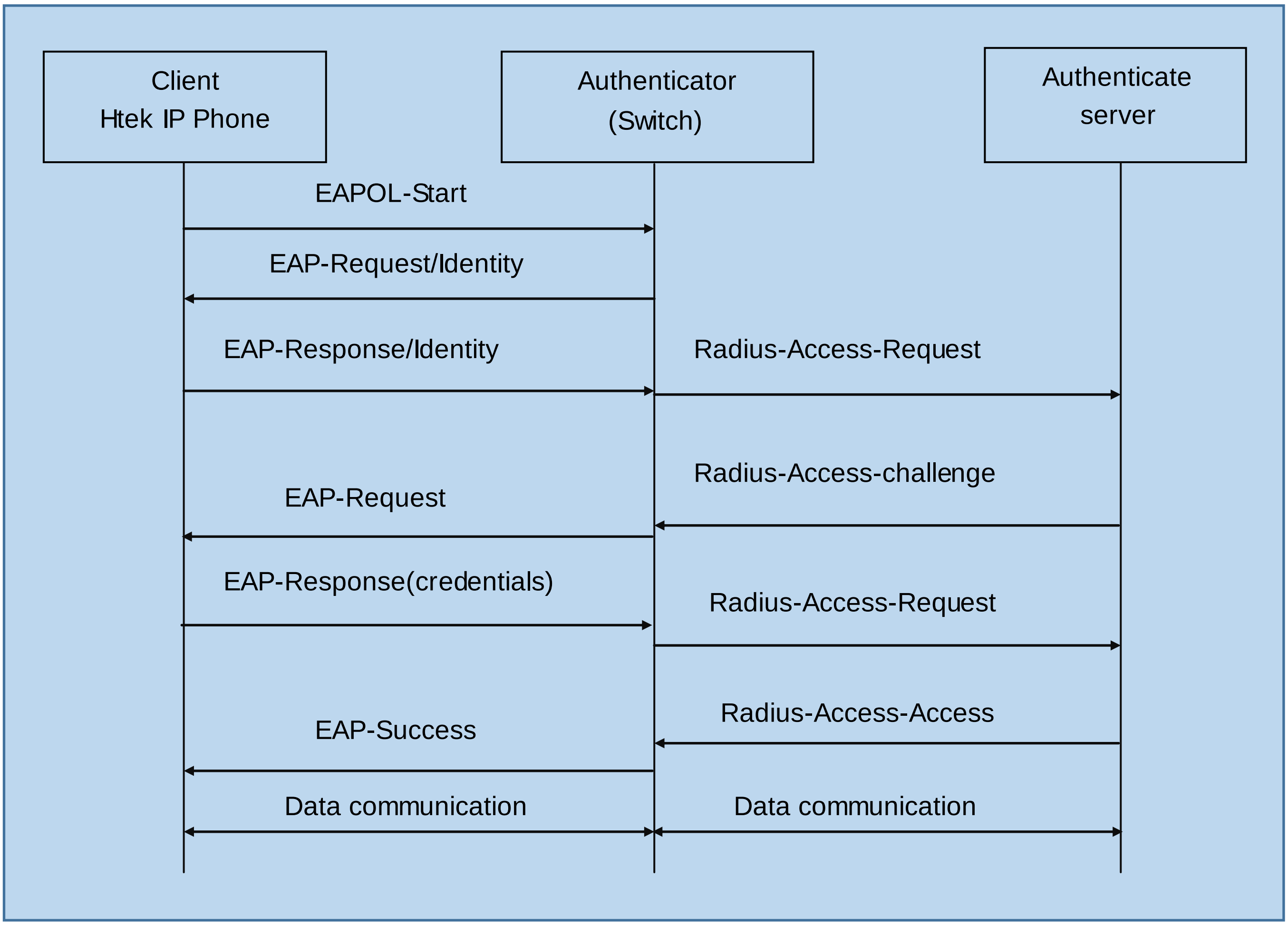
Pre-authentication

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

Authentication

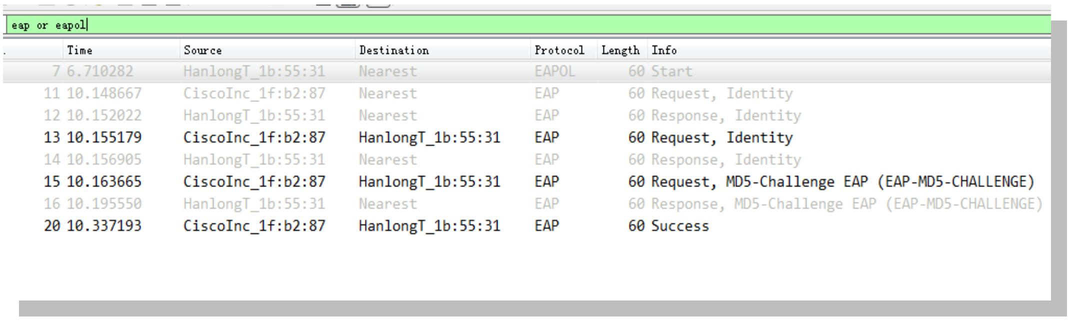
After the authentication server authenticates the IP phone, the authentication server initiates the authentication stage of the process. During this phase, the authenticator facilitates an exchange of keys between the IP phone and the authentication server. After these keys are established, the authenticator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

The following figure summarizes an implementation of the 802.1X authentication process using a **RADIUS** server as the authentication server:



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

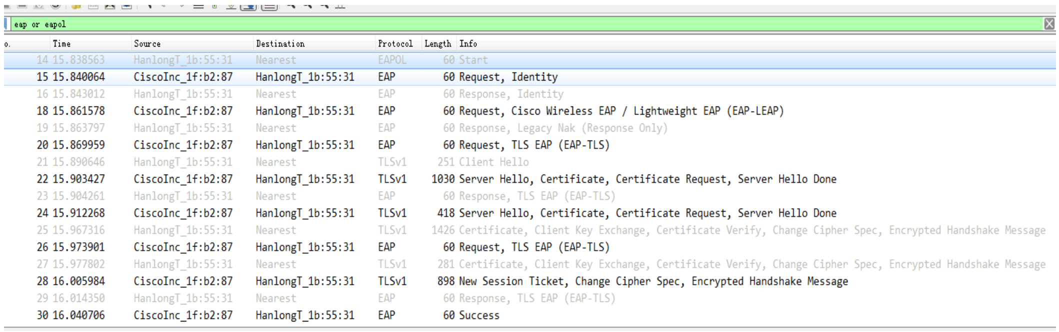
The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-MD5 protocol:



```
eap or eapol

     Time       Source             Destination        Protocol  Length  Info
   7 6.710282   HanlongT_1b:55:31  Nearest            EAPOL         60  Start
  11 10.148667  CiscoInc_1f:b2:87  Nearest            EAP           60  Request, Identity
  12 10.152022  HanlongT_1b:55:31  Nearest            EAP           60  Response, Identity
  13 10.155179  CiscoInc_1f:b2:87  HanlongT_1b:55:31  EAP           60  Request, Identity
  14 10.156905  HanlongT_1b:55:31  Nearest            EAP           60  Response, Identity
  15 10.163665  CiscoInc_1f:b2:87  HanlongT_1b:55:31  EAP           60  Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
  16 10.195550  HanlongT_1b:55:31  Nearest            EAP           60  Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
  20 10.337193  CiscoInc_1f:b2:87  HanlongT_1b:55:31  EAP           60  Success
```

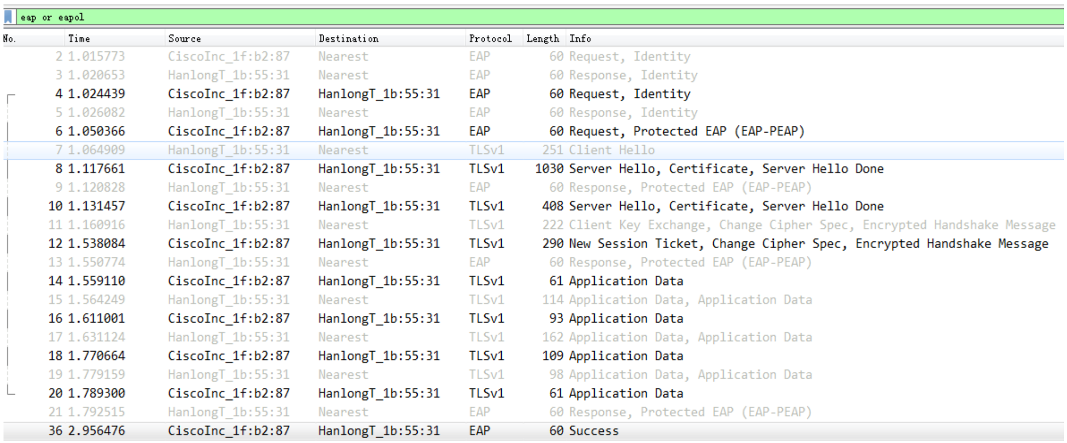
The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-TLS protocol:



eap or eapol

o.	Time	Source	Destination	Protocol	Length	Info
14	15.838563	HanlongT_1b:55:31	Nearest	EAPOL	60	Start
15	15.840064	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Identity
16	15.843012	HanlongT_1b:55:31	Nearest	EAP	60	Response, Identity
18	15.861578	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Cisco Wireless EAP / Lightweight EAP (EAP-LEAP)
19	15.863797	HanlongT_1b:55:31	Nearest	EAP	60	Response, Legacy Nak (Response Only)
20	15.869959	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, TLS EAP (EAP-TLS)
21	15.890646	HanlongT_1b:55:31	Nearest	TLSv1	251	Client Hello
22	15.903427	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	1030	Server Hello, Certificate, Certificate Request, Server Hello Done
23	15.904261	HanlongT_1b:55:31	Nearest	EAP	60	Response, TLS EAP (EAP-TLS)
24	15.912268	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	418	Server Hello, Certificate, Certificate Request, Server Hello Done
25	15.967316	HanlongT_1b:55:31	Nearest	TLSv1	1426	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
26	15.973901	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, TLS EAP (EAP-TLS)
27	15.977802	HanlongT_1b:55:31	Nearest	TLSv1	281	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
28	16.005984	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	898	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
29	16.014350	HanlongT_1b:55:31	Nearest	EAP	60	Response, TLS EAP (EAP-TLS)
30	16.040706	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Success

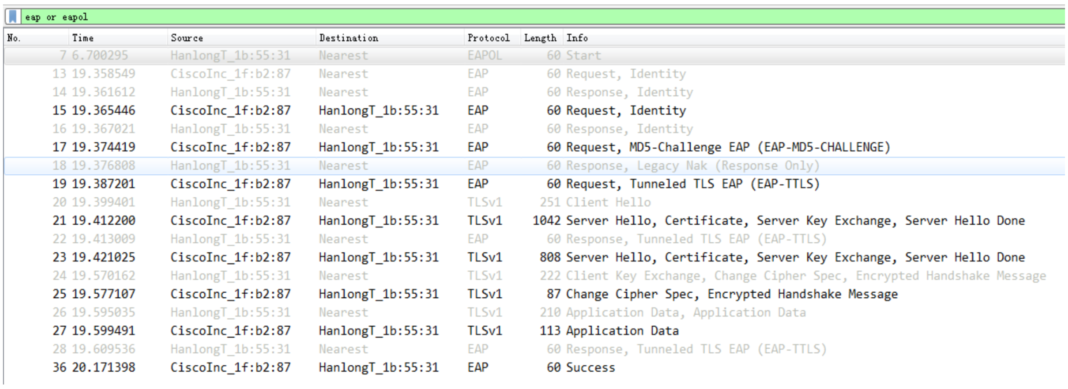
The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-PEAP/MSCHAPv2 protocol:



eap or eapol

No.	Time	Source	Destination	Protocol	Length	Info
2	1.015773	CiscoInc_1f:b2:87	Nearest	EAP	60	Request, Identity
3	1.020653	HanlongT_1b:55:31	Nearest	EAP	60	Response, Identity
4	1.024439	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Identity
5	1.026082	HanlongT_1b:55:31	Nearest	EAP	60	Response, Identity
6	1.050366	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Protected EAP (EAP-PEAP)
7	1.064909	HanlongT_1b:55:31	Nearest	TLSv1	251	Client Hello
8	1.117661	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	1030	Server Hello, Certificate, Server Hello Done
9	1.120828	HanlongT_1b:55:31	Nearest	EAP	60	Response, Protected EAP (EAP-PEAP)
10	1.131457	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	408	Server Hello, Certificate, Server Hello Done
11	1.160916	HanlongT_1b:55:31	Nearest	TLSv1	222	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
12	1.538084	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	290	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
13	1.550774	HanlongT_1b:55:31	Nearest	EAP	60	Response, Protected EAP (EAP-PEAP)
14	1.559110	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	61	Application Data
15	1.564249	HanlongT_1b:55:31	Nearest	TLSv1	114	Application Data, Application Data
16	1.611001	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	93	Application Data
17	1.631124	HanlongT_1b:55:31	Nearest	TLSv1	162	Application Data, Application Data
18	1.770664	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	109	Application Data
19	1.779159	HanlongT_1b:55:31	Nearest	TLSv1	98	Application Data, Application Data
20	1.789300	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	61	Application Data
21	1.792515	HanlongT_1b:55:31	Nearest	EAP	60	Response, Protected EAP (EAP-PEAP)
36	2.956476	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Success

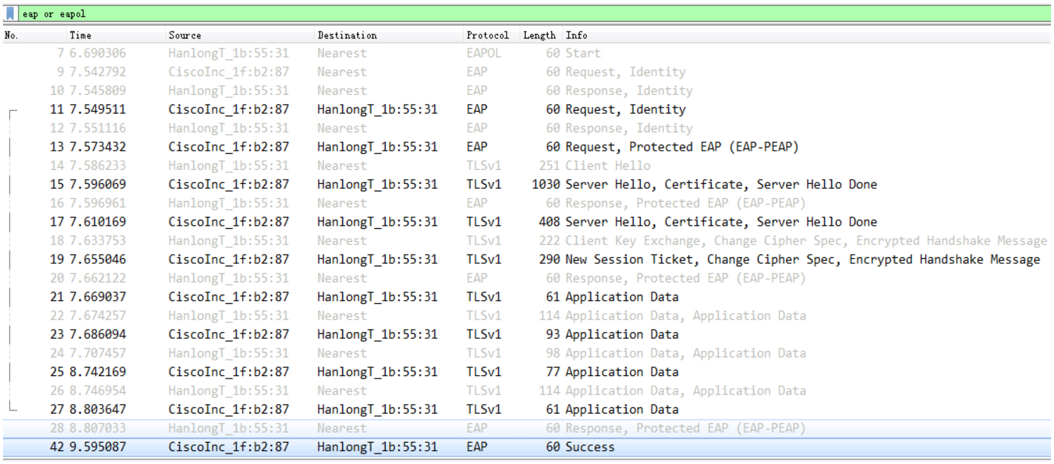
The following screenshot of the Wireshark shows a sample of a successful authentication process using the EAP-TTLS/EAP-MSCHAPv2 protocol:



eap or eapol

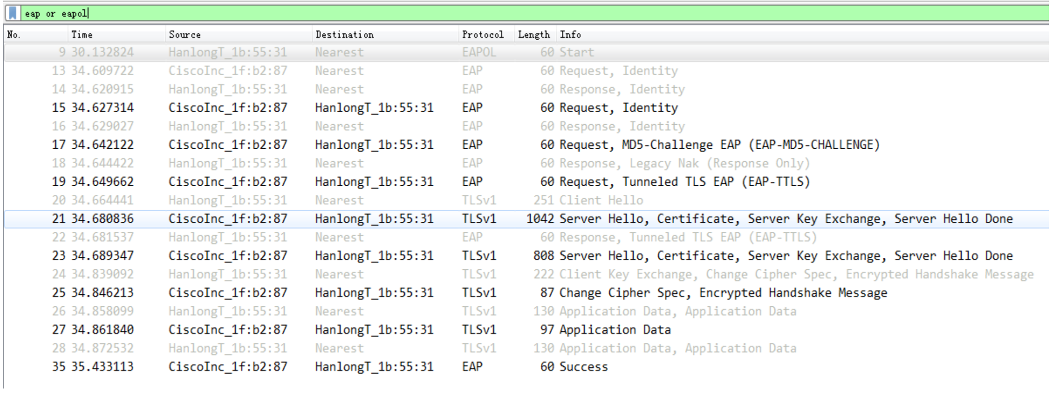
No.	Time	Source	Destination	Protocol	Length	Info
7	6.700295	HanlongT_1b:55:31	Nearest	EAPOL	60	Start
13	19.358549	CiscoInc_1f:b2:87	Nearest	EAP	60	Request, Identity
14	19.361612	HanlongT_1b:55:31	Nearest	EAP	60	Response, Identity
15	19.365446	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Identity
16	19.367021	HanlongT_1b:55:31	Nearest	EAP	60	Response, Identity
17	19.374419	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
18	19.376808	HanlongT_1b:55:31	Nearest	EAP	60	Response, Legacy Nak (Response Only)
19	19.387201	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Request, Tunneled TLS EAP (EAP-TTLS)
20	19.399401	HanlongT_1b:55:31	Nearest	TLSv1	251	Client Hello
21	19.412200	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	1042	Server Hello, Certificate, Server Key Exchange, Server Hello Done
22	19.413009	HanlongT_1b:55:31	Nearest	EAP	60	Response, Tunneled TLS EAP (EAP-TTLS)
23	19.421025	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	808	Server Hello, Certificate, Server Key Exchange, Server Hello Done
24	19.570162	HanlongT_1b:55:31	Nearest	TLSv1	222	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
25	19.577107	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	87	Change Cipher Spec, Encrypted Handshake Message
26	19.595035	HanlongT_1b:55:31	Nearest	TLSv1	210	Application Data, Application Data
27	19.599491	CiscoInc_1f:b2:87	HanlongT_1b:55:31	TLSv1	113	Application Data
28	19.609536	HanlongT_1b:55:31	Nearest	EAP	60	Response, Tunneled TLS EAP (EAP-TTLS)
36	20.171398	CiscoInc_1f:b2:87	HanlongT_1b:55:31	EAP	60	Success

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



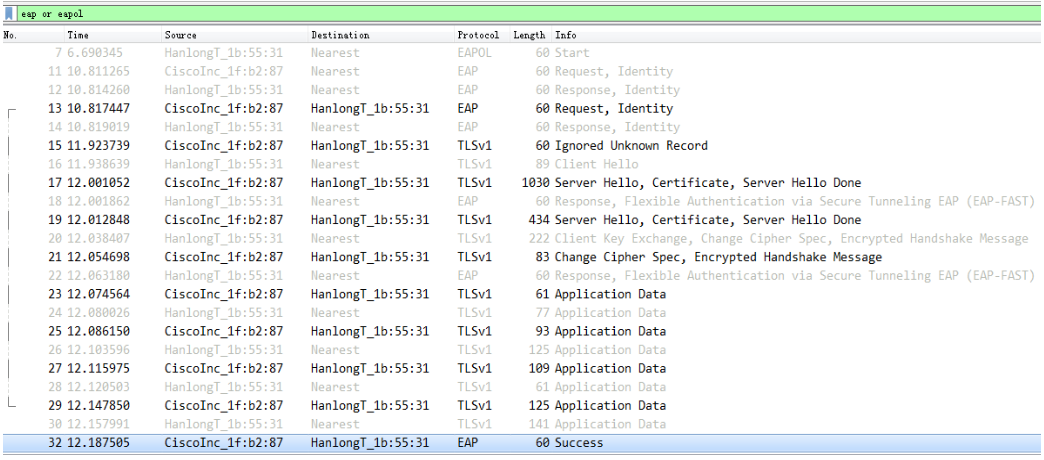
```
eap or eapol
No.    Time       Source              Destination         Protocol  Length  Info
     7 6.690306   HanlongT_1b:55:31   Nearest             EAPOL       60 Start
     9 7.542792   CiscoInc_1f:b2:87   Nearest             EAP         60 Request, Identity
    10 7.545809   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    11 7.549511   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, Identity
    12 7.551116   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    13 7.573432   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, Protected EAP (EAP-PEAP)
    14 7.586233   HanlongT_1b:55:31   Nearest             TLSv1      251 Client Hello
    15 7.596069   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1     1030 Server Hello, Certificate, Server Hello Done
    16 7.596961   HanlongT_1b:55:31   Nearest             EAP         60 Response, Protected EAP (EAP-PEAP)
    17 7.610169   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      408 Server Hello, Certificate, Server Hello Done
    18 7.633753   HanlongT_1b:55:31   Nearest             TLSv1      222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    19 7.655046   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      290 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
    20 7.662122   HanlongT_1b:55:31   Nearest             EAP         60 Response, Protected EAP (EAP-PEAP)
    21 7.669037   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       61 Application Data
    22 7.674257   HanlongT_1b:55:31   Nearest             TLSv1      114 Application Data, Application Data
    23 7.686094   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       93 Application Data
    24 7.707457   HanlongT_1b:55:31   Nearest             TLSv1       98 Application Data, Application Data
    25 8.742169   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       77 Application Data
    26 8.746954   HanlongT_1b:55:31   Nearest             TLSv1      114 Application Data, Application Data
    27 8.803647   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       61 Application Data
    28 8.807033   HanlongT_1b:55:31   Nearest             EAP         60 Response, Protected EAP (EAP-PEAP)
    42 9.595087   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Success
```

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



```
eap or eapol
No.    Time        Source              Destination         Protocol  Length  Info
     9 30.132824   HanlongT_1b:55:31   Nearest             EAPOL       60 Start
    13 34.609722   CiscoInc_1f:b2:87   Nearest             EAP         60 Request, Identity
    14 34.620915   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    15 34.627314   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, Identity
    16 34.629027   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    17 34.642122   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
    18 34.644422   HanlongT_1b:55:31   Nearest             EAP         60 Response, Legacy Nak (Response Only)
    19 34.649662   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, Tunneled TLS EAP (EAP-TTLS)
    20 34.664441   HanlongT_1b:55:31   Nearest             TLSv1      251 Client Hello
    21 34.680836   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1     1042 Server Hello, Certificate, Server Key Exchange, Server Hello Done
    22 34.681537   HanlongT_1b:55:31   Nearest             EAP         60 Response, Tunneled TLS EAP (EAP-TTLS)
    23 34.689347   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      808 Server Hello, Certificate, Server Key Exchange, Server Hello Done
    24 34.839092   HanlongT_1b:55:31   Nearest             TLSv1      222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    25 34.846213   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       87 Change Cipher Spec, Encrypted Handshake Message
    26 34.858099   HanlongT_1b:55:31   Nearest             TLSv1      130 Application Data, Application Data
    27 34.861840   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       97 Application Data
    28 34.872532   HanlongT_1b:55:31   Nearest             TLSv1      130 Application Data, Application Data
    35 35.433113   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Success
```

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



```
eap or eapol
No.    Time        Source              Destination         Protocol  Length  Info
     7 6.690345    HanlongT_1b:55:31   Nearest             EAPOL       60 Start
    11 10.811265   CiscoInc_1f:b2:87   Nearest             EAP         60 Request, Identity
    12 10.814260   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    13 10.817447   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Request, Identity
    14 10.819019   HanlongT_1b:55:31   Nearest             EAP         60 Response, Identity
    15 11.923739   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       60 Ignored Unknown Record
    16 11.938639   HanlongT_1b:55:31   Nearest             TLSv1       89 Client Hello
    17 12.001052   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1     1030 Server Hello, Certificate, Server Hello Done
    18 12.001862   HanlongT_1b:55:31   Nearest             EAP         60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
    19 12.012848   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      434 Server Hello, Certificate, Server Hello Done
    20 12.038407   HanlongT_1b:55:31   Nearest             TLSv1      222 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    21 12.054698   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       83 Change Cipher Spec, Encrypted Handshake Message
    22 12.063180   HanlongT_1b:55:31   Nearest             EAP         60 Response, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
    23 12.074564   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       61 Application Data
    24 12.080026   HanlongT_1b:55:31   Nearest             TLSv1       77 Application Data
    25 12.086150   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1       93 Application Data
    26 12.103596   HanlongT_1b:55:31   Nearest             TLSv1      125 Application Data
    27 12.115975   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      109 Application Data
    28 12.120503   HanlongT_1b:55:31   Nearest             TLSv1       61 Application Data
    29 12.147850   CiscoInc_1f:b2:87   HanlongT_1b:55:31   TLSv1      125 Application Data
    30 12.157991   HanlongT_1b:55:31   Nearest             TLSv1      141 Application Data
    32 12.187505   CiscoInc_1f:b2:87   HanlongT_1b:55:31   EAP         60 Success
```

Troubleshooting

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

Check the following several points 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 into 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 Htek 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 Htek FAE.

Appendix A: Glossary

IEEE (Institute of Electrical and Electronics Engineers) - A professional association with its corporate office in New York City and its operations center in Piscataway, New Jersey. IEEE was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers. And it is dedicated to advancing technological innovation and excellence.

802.1x - An access protocol and authentication based on Client/Server. It can restrict unauthorized users / devices to access the LAN / WLAN through an access port (access port). Only after authentication, normal data can be smoothly through the Ethernet port.

EAP – An authentication framework frequently used in wireless networks and point-to-point connections.

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

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.

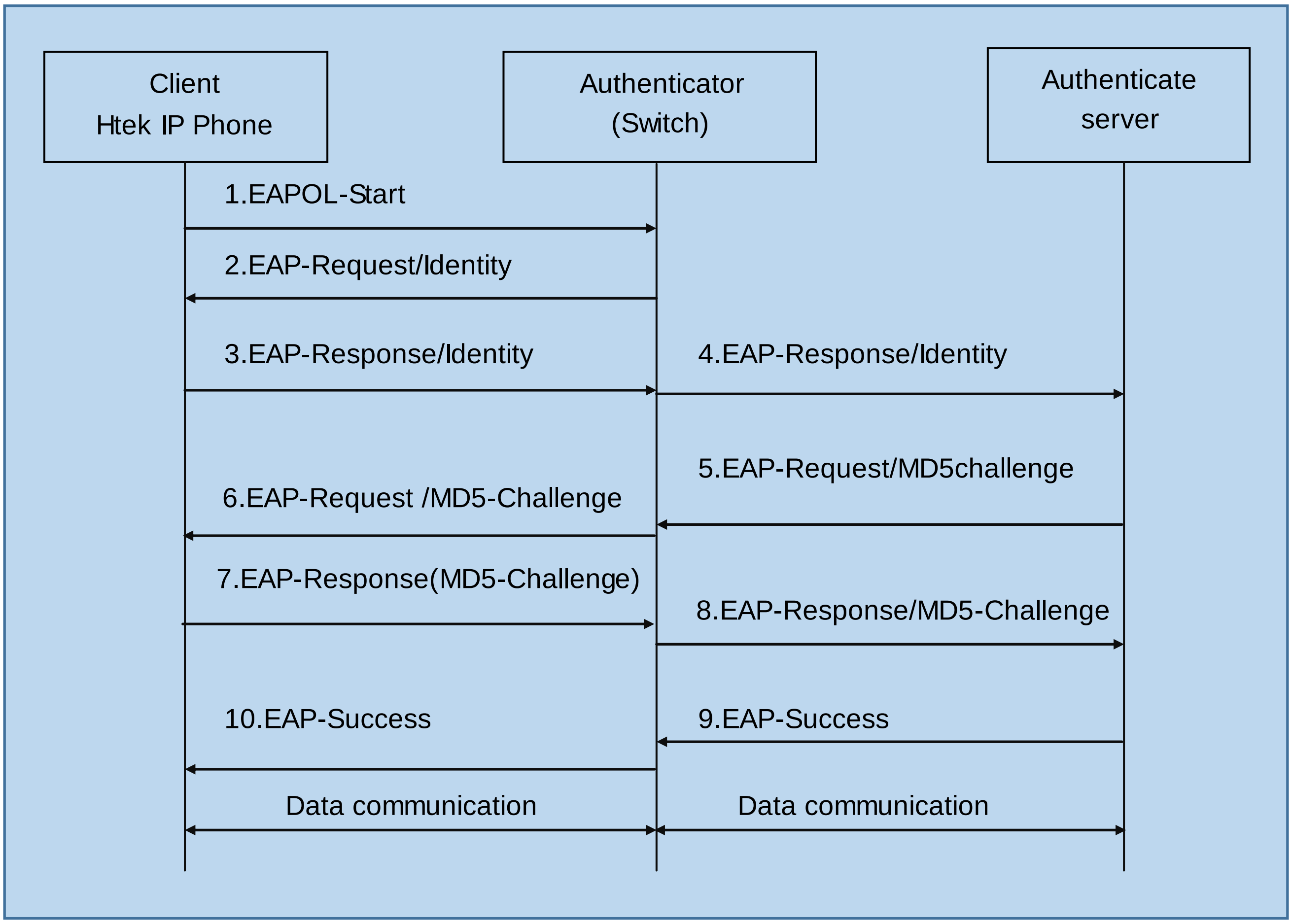
TTLS (Tunneled Transport Layer Security) – Extends TLS to improve some weak points, but it does not require a supplicant-side certificate.

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.

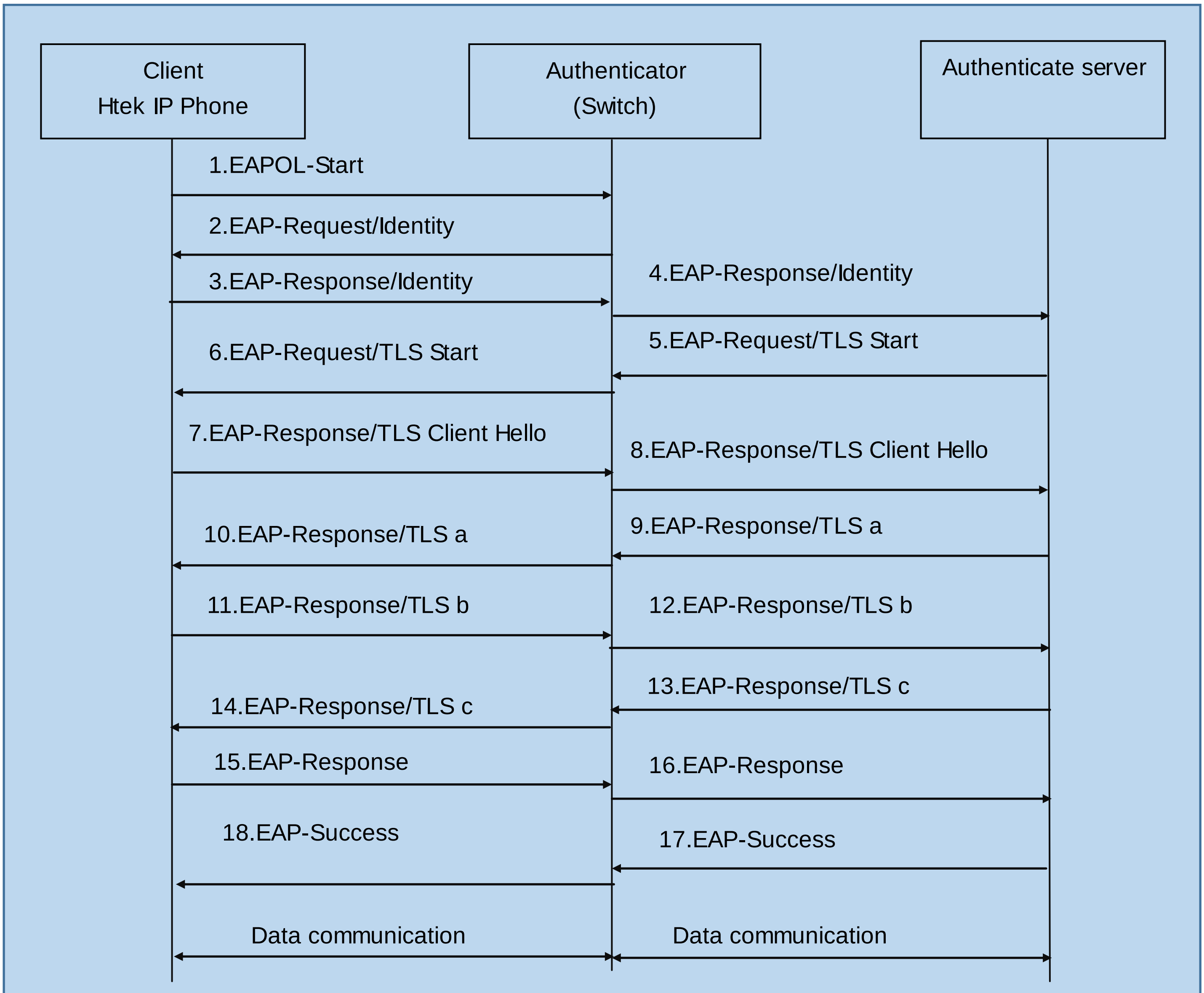


1. The supplicant sends an "EAPOL-Start" packet to the authenticator.
2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator.
4. The authenticator strips the Ethernet header and encapsulates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

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.



a: Server Hello, Serve Certificate, Certificate Request, Server Hello Done

b: Client Certificate, Client Key Exchange, Certificate verify, Change Cipher Spec

c: Change Cipher Spec, Finished Handshake message

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.

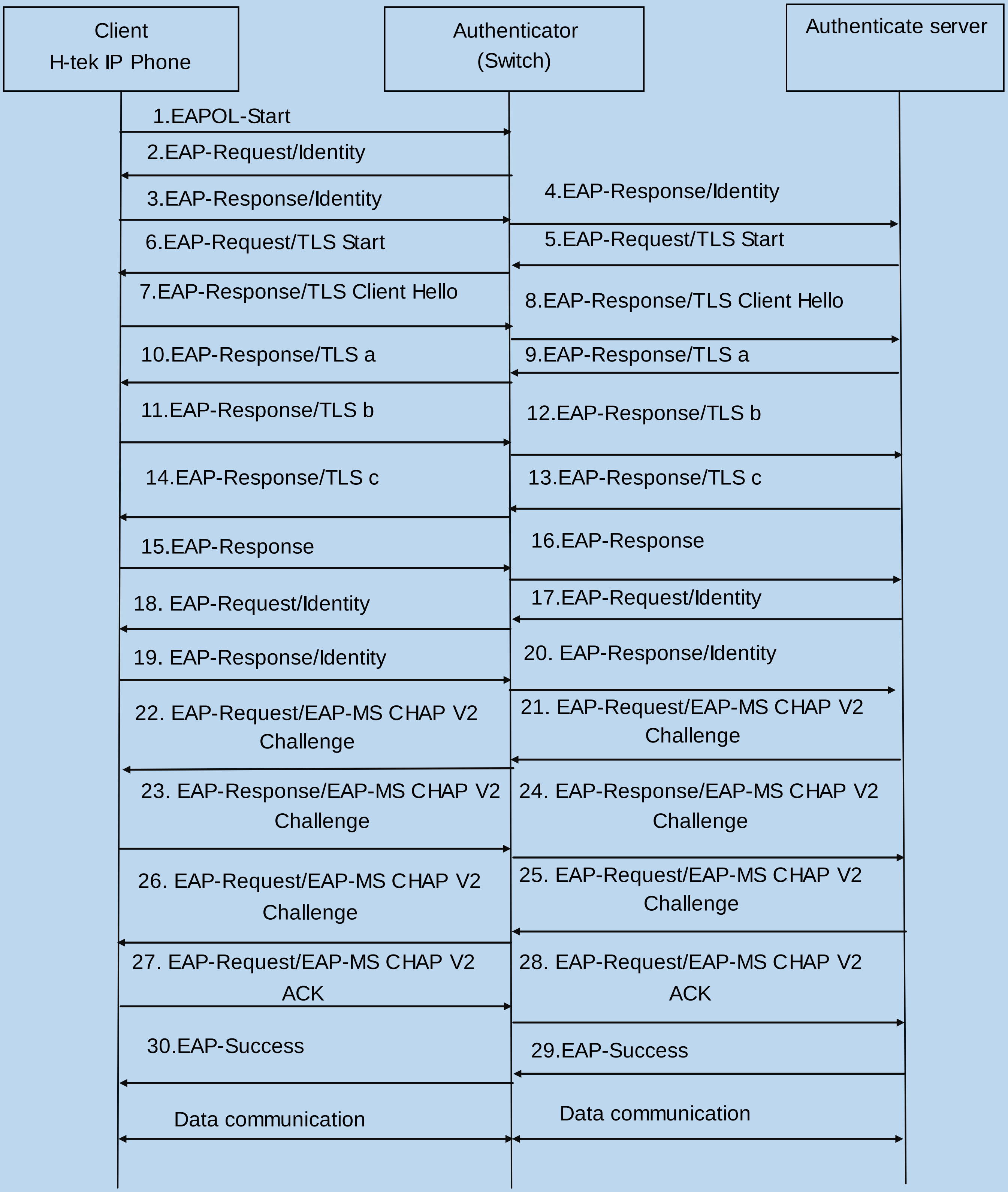
17. The authentication server responds with a success message indicating the supplicant and the authentication server have successfully authenticated each other.

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.

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.



a: Server Hello, Serve Certificate, Certificate Request, Server Hello Done

b: Client Certificate, Client Key Exchange, Certificate verify, Change Cipher Spec

c: Change Cipher Spec, Finished Handshake message

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.

A Successful Authentication Using other Protocols

The **EAP-TTLS/EAP-MSCHAPv2**, **EAP-PEAP/GTC**, **EAP-TTLS/EAP-GTC**, **EAP-FAST** protocol authentication process is similar to the **EAP-PEAP/EAP-MSCHAPv2**. 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 support@Htek.com.