

HOWTO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant

Version 1.0.1
April 18, 2002

Ken Roser
kroser@pobox.com

TABLE OF CONTENTS

1. INTRODUCTION	3
2. CONFIGURATION	3
2.1 CLIENT NIC SETUP	3
3. OPENSLL AND FREERADIUS SETUP	5
4. GENERATING CERTIFICATES.....	5
4.1 WINDOWS 2000 CERTIFICATION AUTHORITY.....	5
4.2 OPENSLL.....	5
4.4 MICROSOFT MANAGEMENT CONSOLE USE.....	6
4.4.1 <i>Installing CA Root Certificate</i>	10
5. FREERADIUS LOG.....	19
7. ETHEREAL LOG.....	36
8. RFC2716 REFERENCE MESSAGE FLOW	41
9. OPENSLL CERTIFICATE GENERATION SCRIPT	42
10. OPENSLL EXTENSIONS FILE	43
11. REFERENCES.....	43

TABLE OF FIGURES

Figure 1: 802.11b NIC configuration – Wireless Networks.....	3
Figure 2: 802.11b NIC configuration – Authentication.....	4
Figure 3: 802.11b NIC configuration – Authentication – Certificate Properties.....	5
Figure 4: Microsoft Management Console (MMC) - initial.....	6
Figure 5: MMC - Adding a Snap-in.....	7
Figure 6: MMC - Selecting Certificates Snap-in.....	8
Figure 7: MMC - Specifying Certificate Management for User Accounts.....	9
Figure 8: MMC - Specifying Local Computer is to be managed.....	10
Figure 9: Installing CA Root Certificate - Initial Screen.....	11
Figure 10: Installing CA Root Certificate - Selecting Certificate Store, Step 1.....	12
Figure 11: Installing CA Root Certificate - Selecting Certificate Store, Step 2.....	12
Figure 12: Installing CA Root Certificate - Selecting Certificate Store, Step 3.....	13
Figure 13: Installing CA Root Certificate - Success.....	13
Figure 14: Installing CA Root Certificate - Final confirmation.....	14
Figure 15: Installing Client Certificate - Pass phrase prompt.....	14
Figure 16: Installing Client Certificate - Selecting Certificate Store, Step 1.....	15
Figure 17: Display of Client Certificate - General.....	16
Figure 18: Display of Client Certificate - Details.....	17
Figure 19: Display of Client Certificate – Certification Path.....	18

1. Introduction

This document describes what was necessary to set up 802.1x authentication with a Windows XP supplicant and a FreeRADIUS server. An informative tutorial on setting up something very similar but with a Linux client can be found at <http://www.missl.cs.umd.edu/wireless/eaptls/> and was used as a starting point for my implementation and will be referenced occasionally throughout this document.

This document does not have much text, but through the use of the screenshots and examples within, one can easily reproduce a working EAP/TLS setup.

2. Configuration

- Windows XP Supplicant
- Linksys Wireless PCI Card, WMP11, driver version 1.7.29.1032
- Cisco AP340 with software version 11.10T1
- FreeRADIUS server, CVS version 04/15/2002 on Sun Blade 100 with Solaris 8

2.1 Client NIC setup

The following screenshots show how the 802.11b NIC was set up.

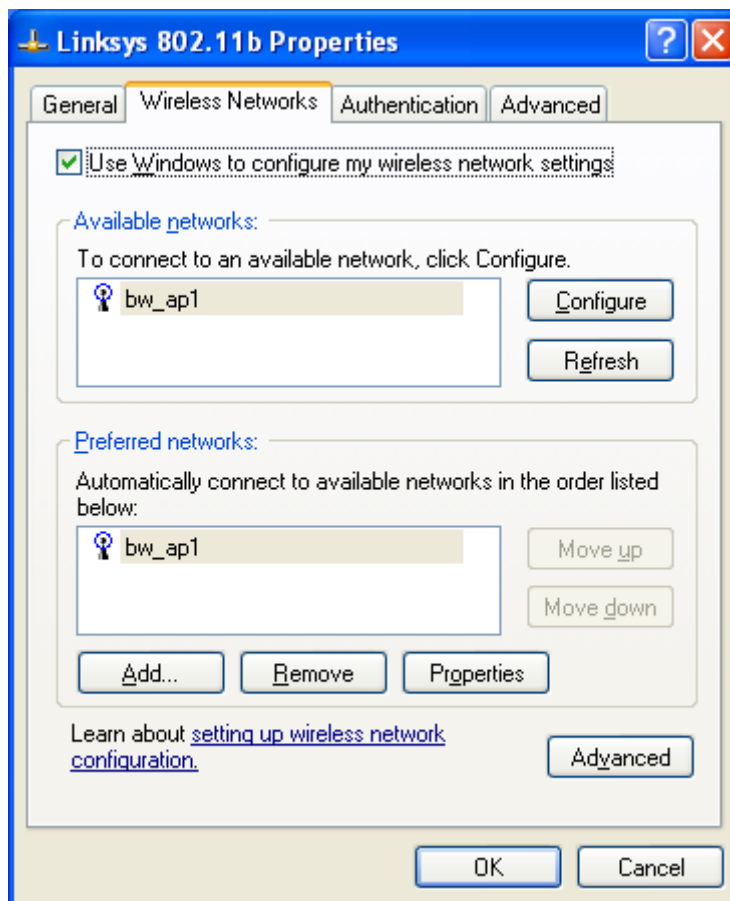


Figure 1: 802.11b NIC configuration – Wireless Networks

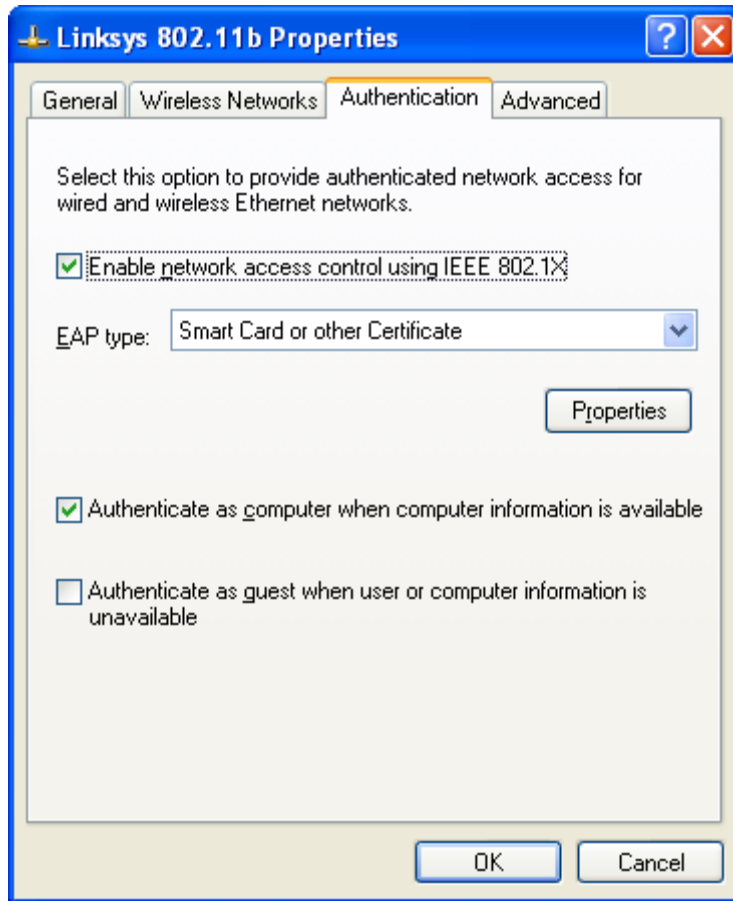


Figure 2: 802.11b NIC configuration – Authentication

Figure 2 shows the authentication setup. Setting the EAP type to “Smart Card or other Certificate” will cause XP to use EAP/TLS for authentication.

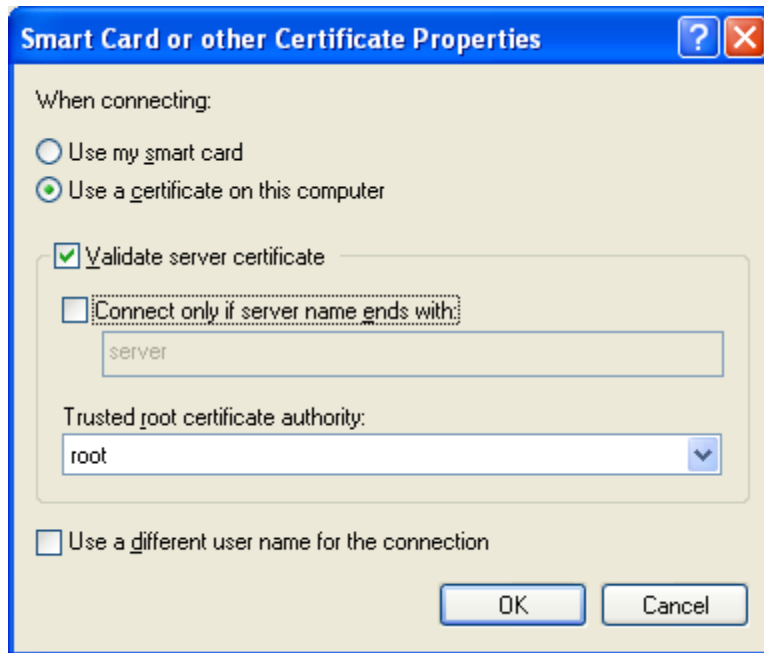


Figure 3: 802.11b NIC configuration – Authentication – Certificate Properties

If you don't populate Trusted root certificate authority, you will get prompted at authentication time with a balloon prompt from the icon in the notification area of the task bar stating, "Click here to process your login information for the network [AP's SSID here]".

3. OpenSSL and FreeRADIUS setup

To configure these two components, please see <http://www.missl.cs.umd.edu/wireless/eaptls/>.

In order to work with XP, the FreeRADIUS version must be equal to or greater than the April 15, 2002 CVS version.

When setting up the FreeRADIUS configuration, I had to make one change from what was stated in [1]. The author suggests to use a `fragment_size` of 1750. I found that I had to set this value to 1024 otherwise the authentication would never complete.

4. Generating Certificates

4.1 Windows 2000 Certification Authority

Ideally if the network has a Windows 2000 server you can use it to issue certificates. I suggest you see [2] as a reference to do this.

4.2 OpenSSL

The server certificate must contain an Enhanced Key Usage (EKU) using the object identifier (OID) of "1.3.6.1.5.5.7.3.1". Similarly the client certificate must contain an EKU of "1.3.6.1.5.5.7.3.2". This wasn't discussed in the EAP/TLS How-to [1]. My usage of OpenSSL to generate certificates takes this into consideration.

After installing OpenSSL, first prepare to run the script by taking the text that's in §10 of this document and placing it in a file called "xpextensions". Take the script text in §9 and write that into a file of any name. To generate the certificates, run the script file you just created. The following generated files must either be copied or be networked to the Windows XP client for certificate installation.

File	Purpose
root.der	CA Root Certificate
cert-clt.p12	Client certificate with private key

Directions for installing these certificates can be found in §4.3.1 and §4.3.2.

4.3 Microsoft Management Console Use

From the Start-Run menu run mmc. The window shown in Figure 4 opens.

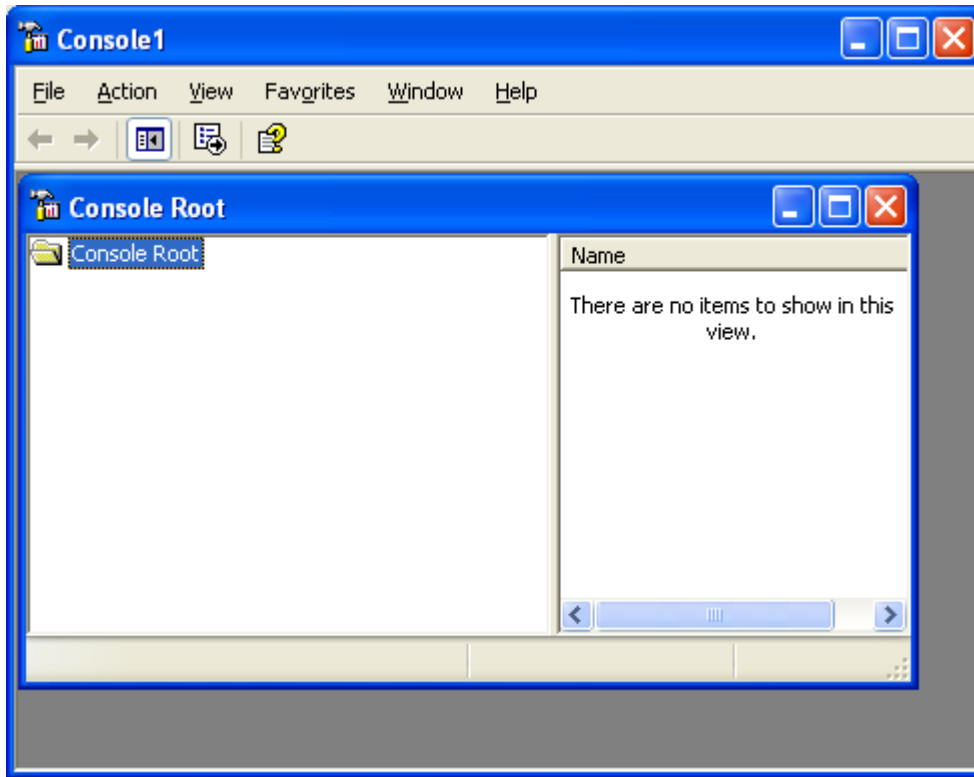


Figure 4: Microsoft Management Console (MMC) - initial

Select "File->Add/Remove Snap-in...". The following dialog will appear.

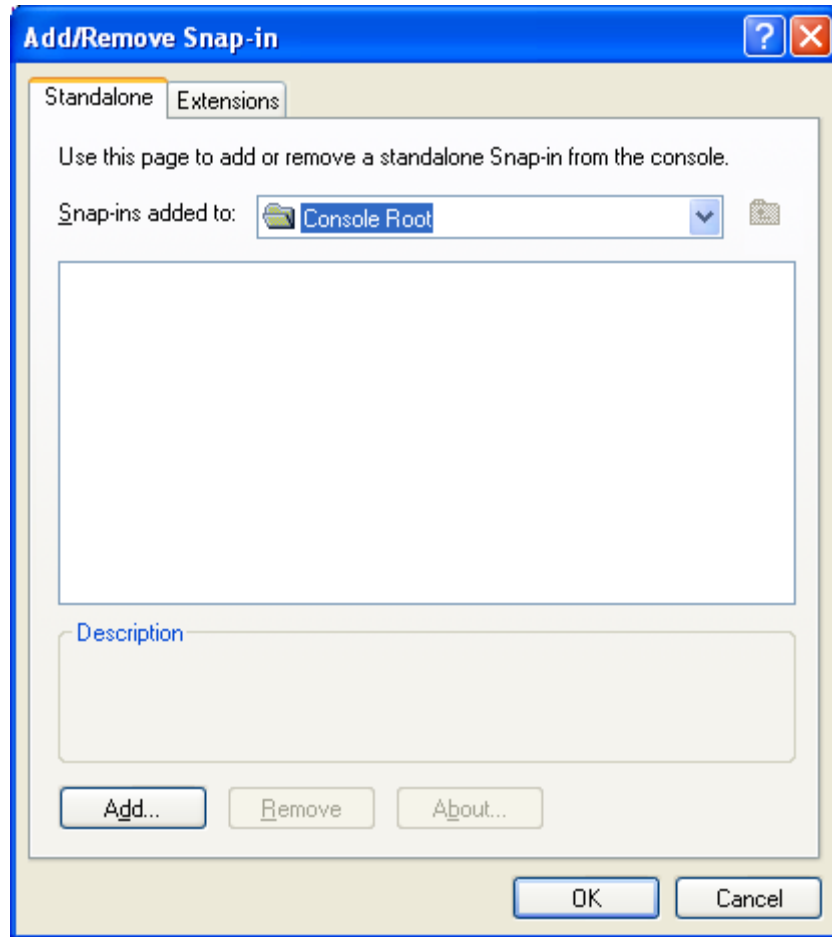


Figure 5: MMC - Adding a Snap-in

Click the "Add" button. The following dialog will appear.

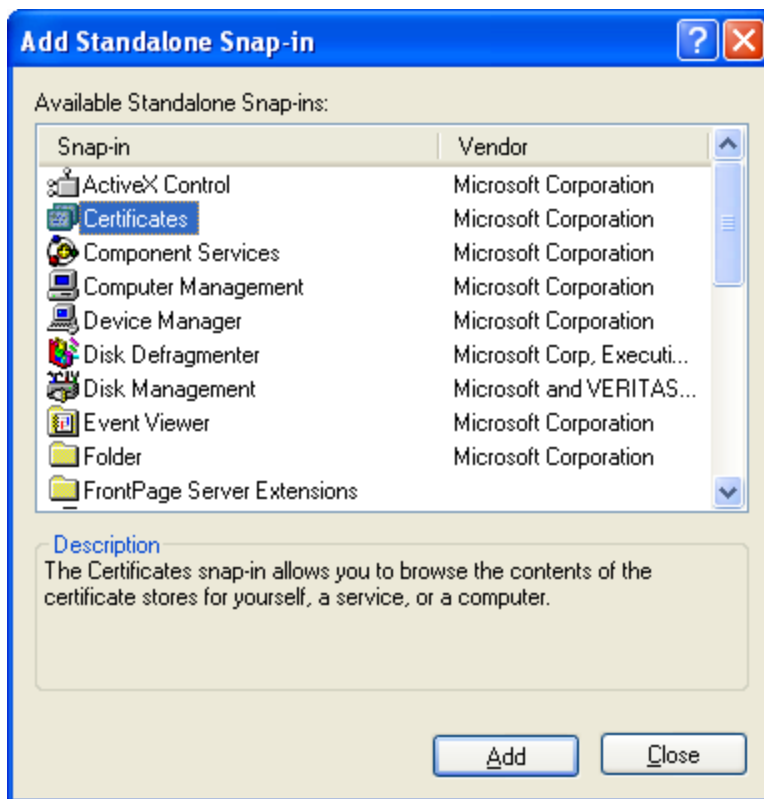


Figure 6: MMC - Selecting Certificates Snap-in

Select the "Certificates" Snap-in and click "Add". The following dialog will appear.

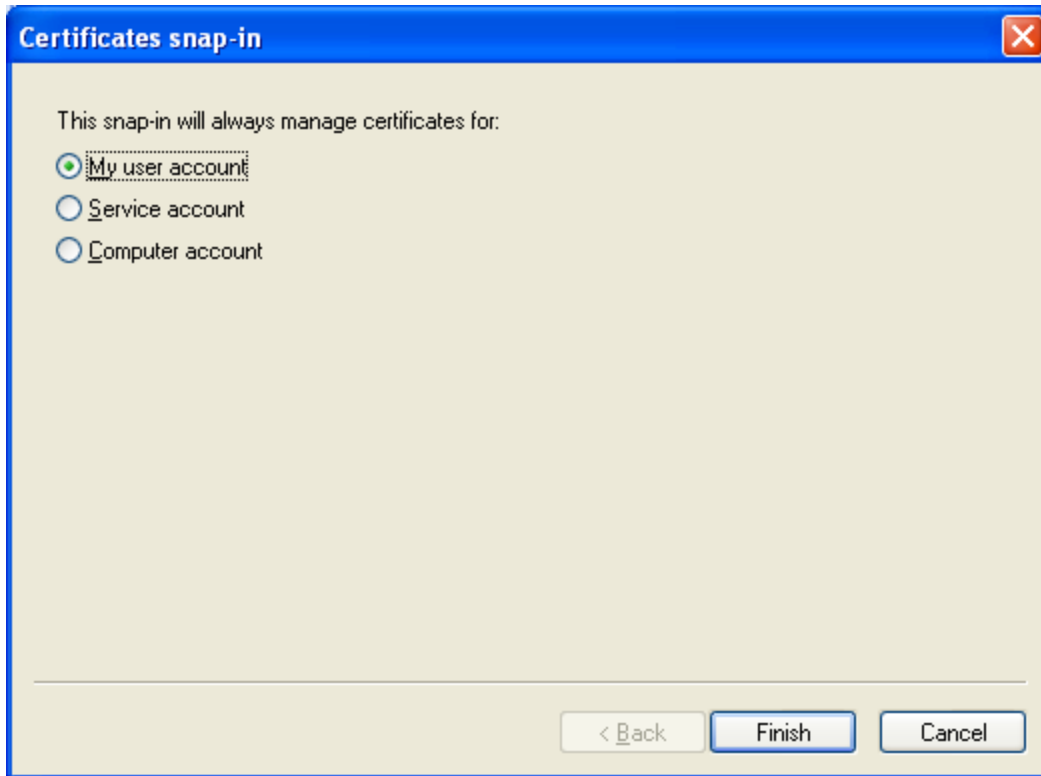


Figure 7: MMC - Specifying Certificate Management for User Accounts

Select "My user account" and click "Finish". The following dialog will appear.

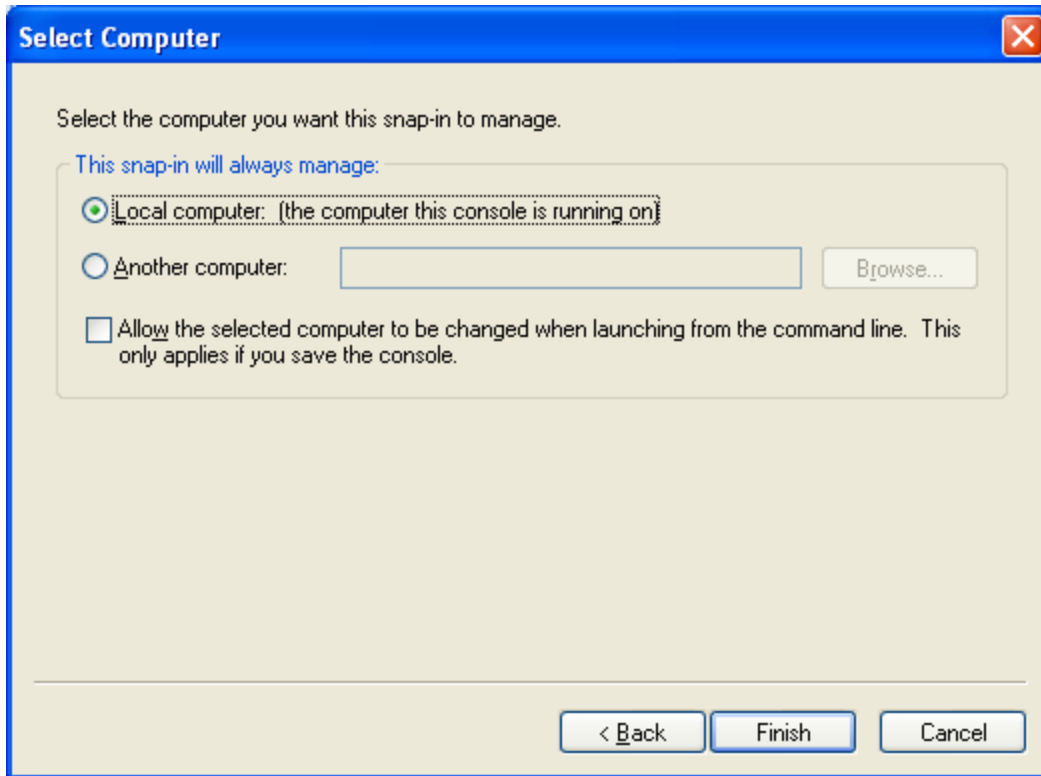


Figure 8: MMC - Specifying Local Computer is to be managed

Select "Local computer" and hit "Finish"

4.3.1 Installing CA Root Certificate

To install the CA Root Certificate, open the "root.der" file created in §4.2. Windows will then display the following dialog. Click "Install Certificate".

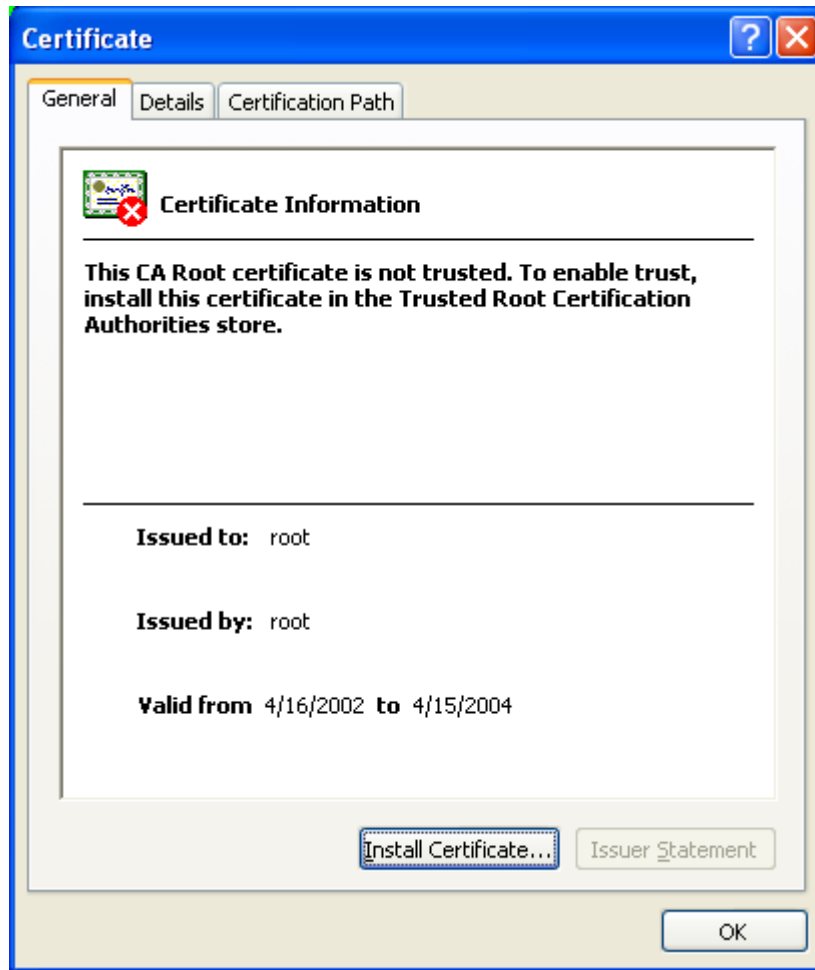


Figure 9: Installing CA Root Certificate - Initial Screen

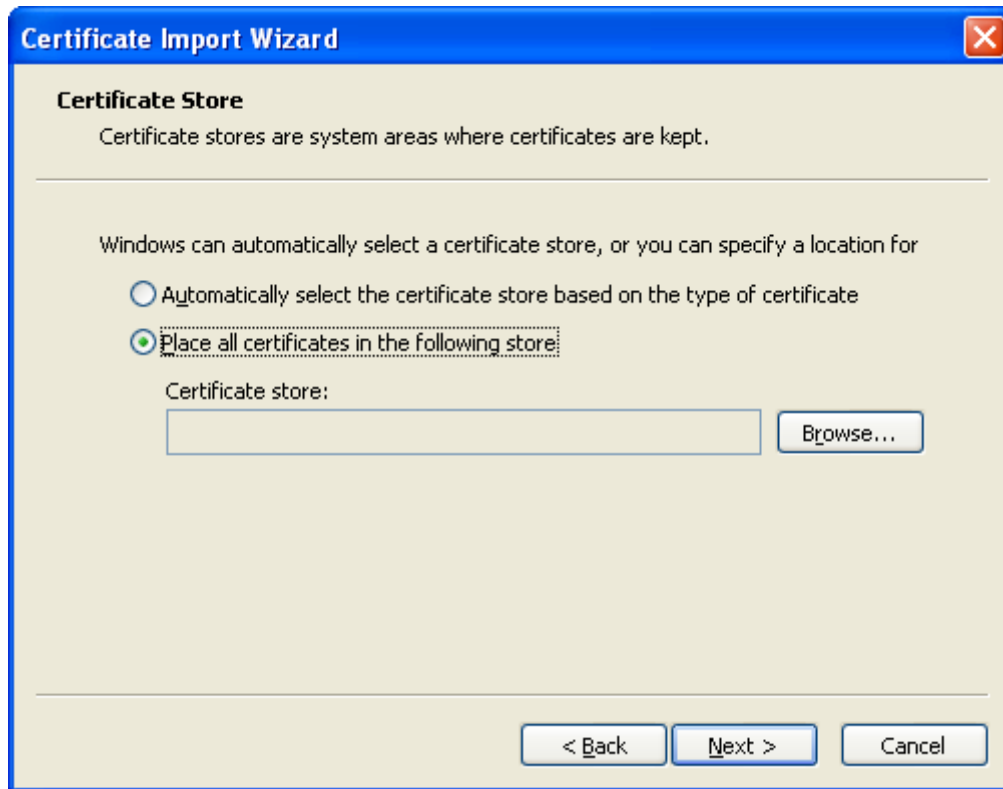


Figure 10: Installing CA Root Certificate - Selecting Certificate Store, Step 1

For the dialog in Figure 10, select "Place all certificates in the following store", then click "Browse...". The following dialog will appear. Select "Trusted Root Certification Authorities" and click "OK".



Figure 11: Installing CA Root Certificate - Selecting Certificate Store, Step 2

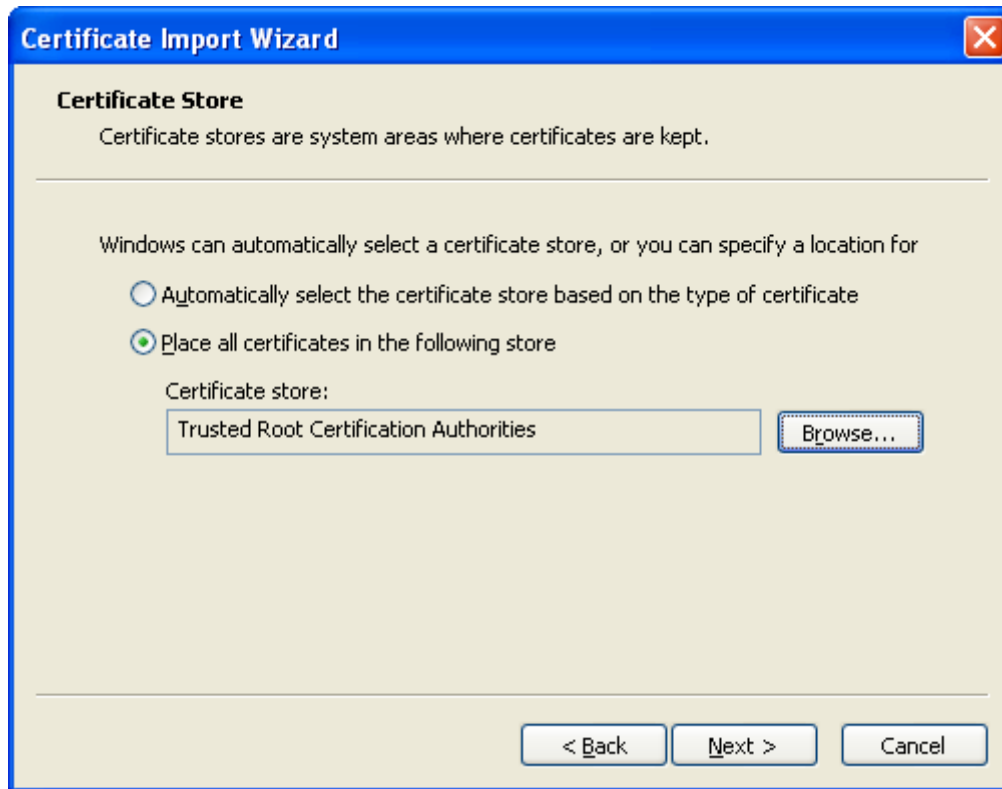


Figure 12: Installing CA Root Certificate - Selecting Certificate Store, Step 3

When the dialog in Figure 12 appears, click "Finish".

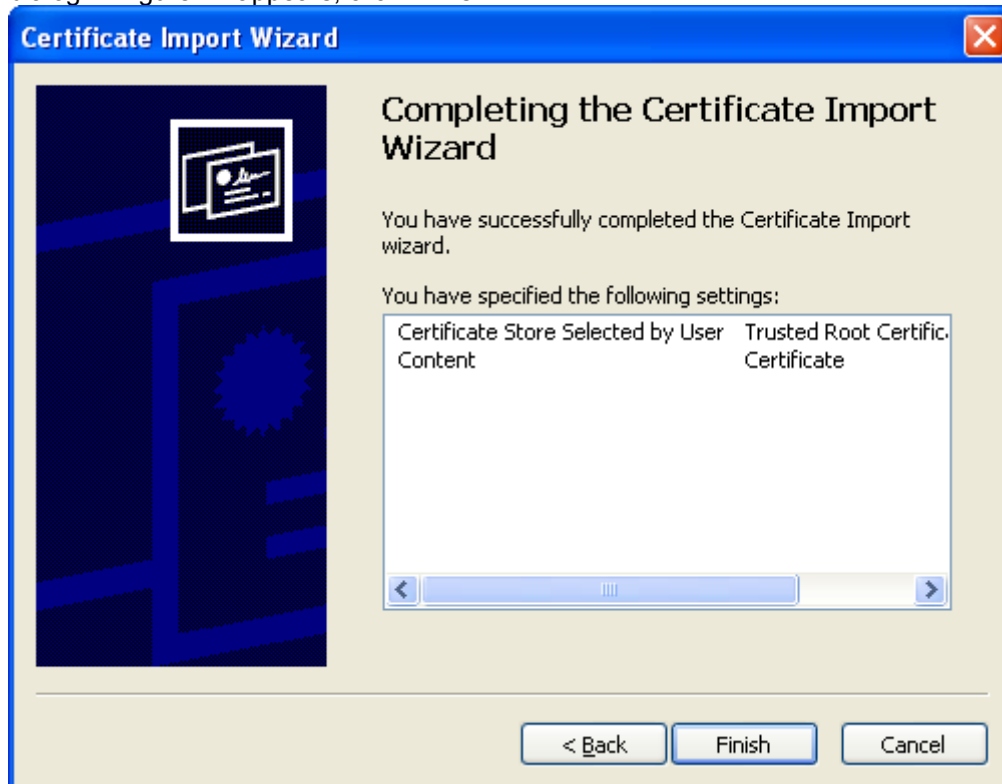


Figure 13: Installing CA Root Certificate - Success

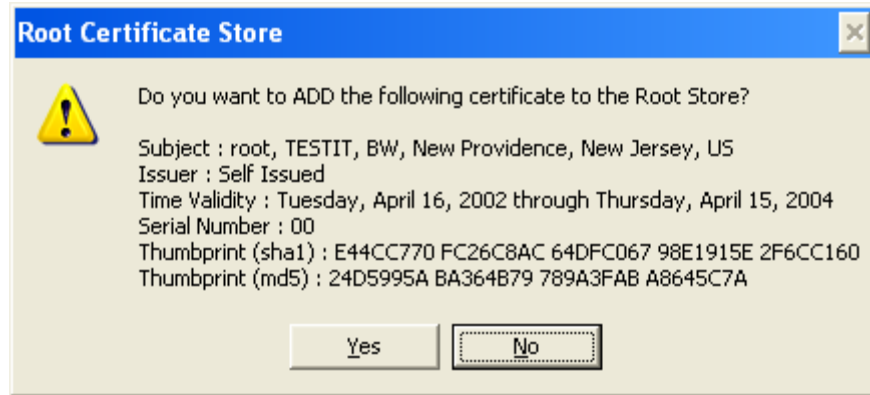


Figure 14: Installing CA Root Certificate - Final confirmation

Click "Yes" at this final dialog box.

4.3.2 Installing Client Certificate

To install the Client (User) Certificate, open the "cert-clt.p12" file created in §4.2. Installation is similar to the CA Root certificate but this time you'll be prompted to enter the password for the private key which is "whatever" if you accepted the default when creating the certificates.



Figure 15: Installing Client Certificate - Pass phrase prompt

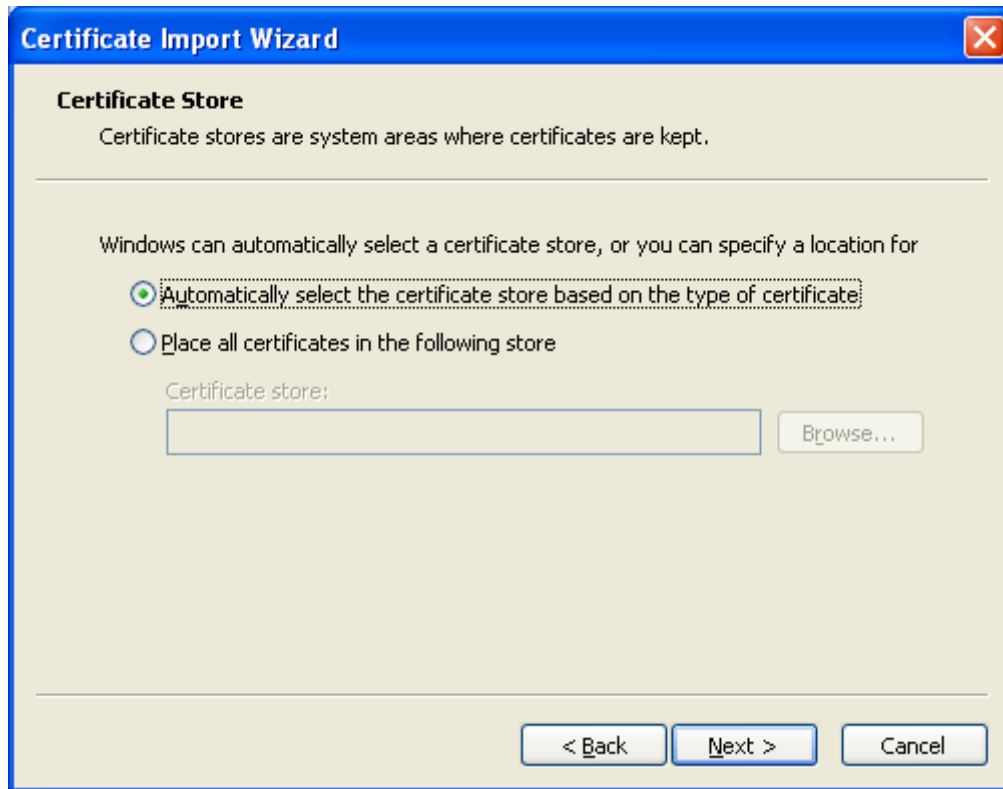


Figure 16: Installing Client Certificate - Selecting Certificate Store, Step 1

Leave the defaults. This will be placed in the User Certificates area.

Open the MMC and the client certificate should look like the following figure.

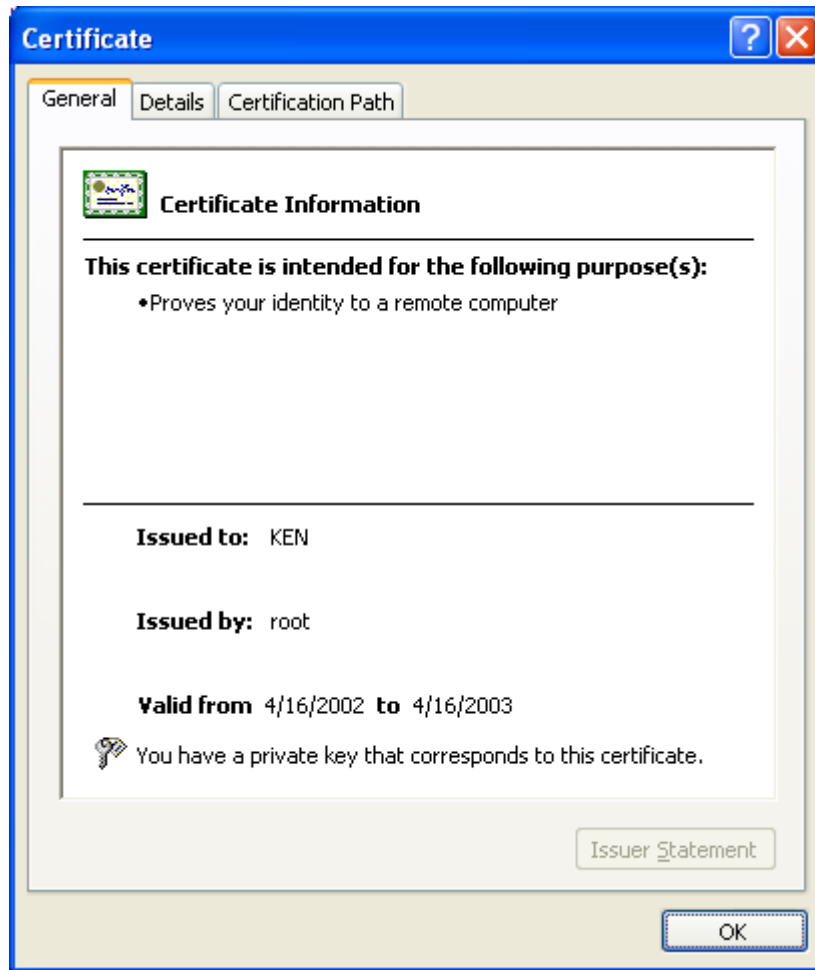


Figure 17: Display of Client Certificate - General

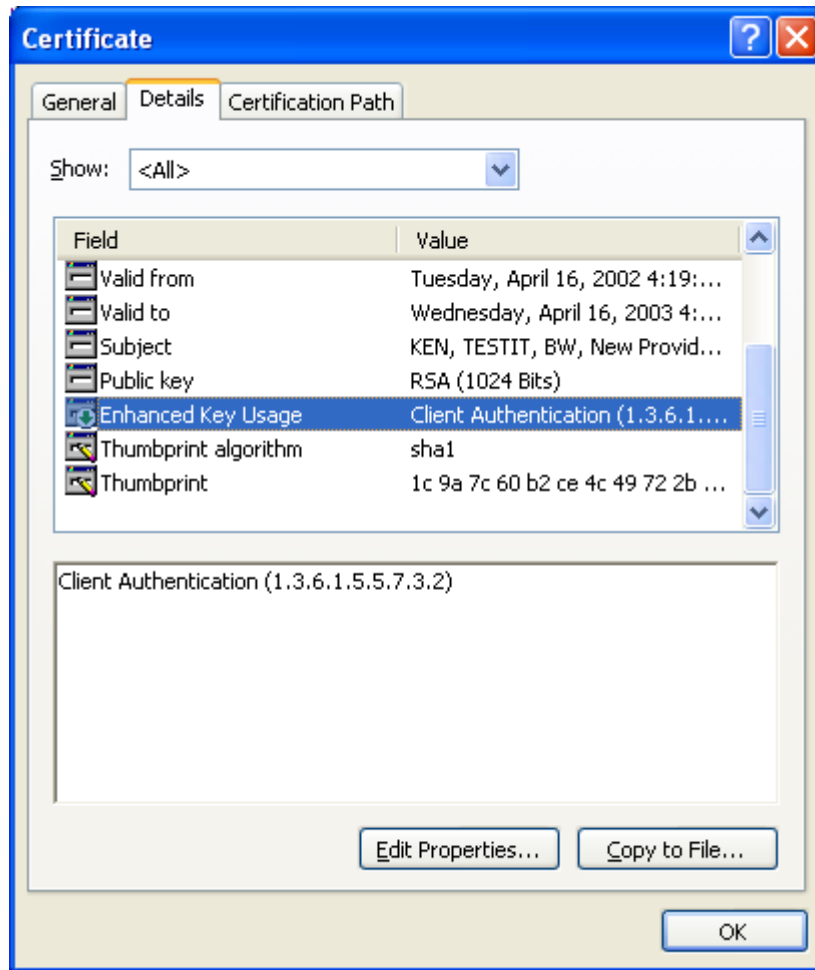


Figure 18: Display of Client Certificate - Details

Be certain the Enhanced Key Usage shows Client Authentication.

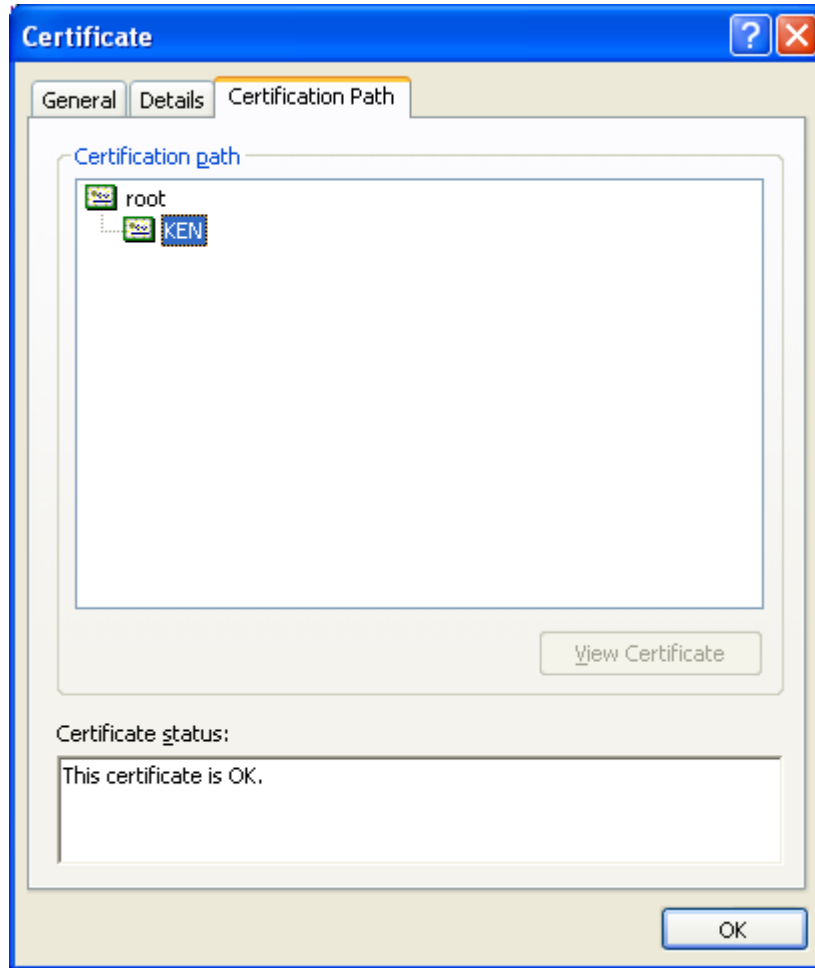


Figure 19: Display of Client Certificate – Certification Path

Certification path should go back to the trusted root certificate you installed previously

5. FreeRADIUS log

The following is a FreeRADIUS log when the XP client is successfully authenticated.

```
$ ./radiusd -X
Starting - reading configuration files ...
reread_config: reading radiusd.conf
Config: including file: /home/freeradius/cvs0415/etc/raddb/proxy.conf
Config: including file: /home/freeradius/cvs0415/etc/raddb/clients.conf
Config: including file: /home/freeradius/cvs0415/etc/raddb/snmp.conf
Config: including file: /home/freeradius/cvs0415/etc/raddb/sql.conf
main: prefix = "/home/freeradius/cvs0415"
main: localstatedir = "/home/freeradius/cvs0415/var"
main: logdir = "/home/freeradius/cvs0415/var/log/radius"
main: libdir = "/home/freeradius/cvs0415/lib"
main: radacctdir = "/home/freeradius/cvs0415/var/log/radius/radacct"
main: hostname_lookups = no
read_config_files: reading dictionary
read_config_files: reading clients
read_config_files: reading realms
read_config_files: reading naslist
main: max_request_time = 30
main: cleanup_delay = 5
main: max_requests = 1024
main: delete_blocked_requests = 0
main: port = 0
main: allow_core_dumps = no
main: log_stripped_names = no
main: log_auth = yes
main: log_auth_badpass = yes
main: log_auth_goodpass = yes
main: pidfile = "/home/freeradius/cvs0415/var/run/radiusd.pid"
main: user = "root"
main: group = "root"
main: usercollide = no
main: lower_user = "no"
main: lower_pass = "no"
main: nospace_user = "no"
main: nospace_pass = "no"
main: proxy_requests = yes
proxy: retry_delay = 5
proxy: retry_count = 3
proxy: synchronous = no
proxy: default_fallback = yes
proxy: dead_time = 120
security: max_attributes = 200
security: reject_delay = 1
main: debug_level = 0
read_config_files: entering modules setup
Module: Library search path is /home/freeradius/cvs0415/lib
Module: Loaded System
unix: cache = no
unix: passwd = "/etc/passwd"
unix: shadow = "(null)"
unix: group = "/etc/group"
unix: radwtmp = "/home/freeradius/cvs0415/var/log/radius/radwtmp"
unix: usegroup = no
unix: cache_reload = 600
Module: Instantiated unix (unix)
Module: Loaded eap
eap: default_eap_type = "tls"
eap: timer_expire = 60
tls: rsa_key_exchange = no
tls: dh_key_exchange = yes
tls: rsa_key_length = 512
tls: dh_key_length = 512
```

```
tls: verify_depth = 0
tls: CA_path = "(null)"
tls: pem_file_type = yes
tls: private_key_file = "/home/ker/certificates/cert-srv.pem"
tls: certificate_file = "/home/ker/certificates/cert-srv.pem"
tls: CA_file = "/home/ker/certificates/demoCA/cacert.pem"
tls: private_key_password = "whatever"
tls: dh_file = "/etc/1x/adamcert/random"
tls: random_file = "/etc/1x/adamcert/dh"
tls: fragment_size = 1024
tls: include_length = yes
rlm_eap_tls: conf N ctx stored
rlm_eap: Loaded and initialized the type tls
Module: Instantiated eap (eap)
Module: Loaded preprocess
preprocess: huntgroups = "/home/freeradius/cvs0415/etc/raddb/huntgroups"
preprocess: hints = "/home/freeradius/cvs0415/etc/raddb/hints"
preprocess: with_ascend_hack = no
preprocess: ascend_channels_per_line = 23
preprocess: with_ntdomain_hack = no
preprocess: with_specialix_jetstream_hack = no
preprocess: with_cisco_vsa_hack = no
Module: Instantiated preprocess (preprocess)
Module: Loaded realm
realm: format = "suffix"
realm: delimiter = "@"
Module: Instantiated realm (suffix)
Module: Loaded files
files: usersfile = "/home/freeradius/cvs0415/etc/raddb/users"
files: acctusersfile = "/home/freeradius/cvs0415/etc/raddb/acct_users"
files: compat = "no"
Module: Instantiated files (files)
Module: Loaded detail
detail: detailfile = "/home/freeradius/cvs0415/var/log/radius/radacct/{Client-IP-Address}/detail"
detail: detailperm = 384
detail: dirperm = 493
Module: Instantiated detail (detail)
Module: Loaded radutmp
radutmp: filename = "/home/freeradius/cvs0415/var/log/radius/radutmp"
radutmp: username = "%{User-Name}"
radutmp: perm = 384
radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
Listening on IP address *, ports 1812/udp and 1813/udp, with proxy on 1814/udp.
Ready to process requests.
rad_recv: Access-Request packet from host 192.168.123.2:4261, id=73, length=119
  User-Name = "KEN"
  NAS-IP-Address = 192.168.123.2
  Called-Station-Id = "004096431d06"
  Calling-Station-Id = "000625039e69"
  NAS-Identifier = "AP340-431d06"
  NAS-Port = 29
  Framed-MTU = 1400
  NAS-Port-Type = Wireless-802.11
  EAP-Message = "\002\003\000\010\001KEN"
  Message-Authenticator = 0xe0589a7549ba0f842260ed300e4e1848
modcall: entering group authorize
  modcall[authorize]: module "preprocess" returns ok
  modcall[authorize]: module "eap" returns updated
    rlm_realm: Looking up realm NULL for User-Name = "KEN"
    rlm_realm: No such realm NULL
  modcall[authorize]: module "suffix" returns noop
    users: Matched KEN at 25
  modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
rad_check_password: Found Auth-Type EAP
```

```
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: processing type tls
  modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Login OK: [KEN/<no User-Password attribute>] (from client 192.168.123.2 port 29 cli
000625039e69)
Sending Access-Challenge of id 73 to 192.168.123.2:4261
  Acct-Interim-Interval = 30
  Idle-Timeout = 7200
  Session-Timeout = 14400
  EAP-Message = "\001\004\000\006\r "
  Message-Authenticator = 0x00000000000000000000000000000000
  State =
0x3506d24e9ac1a05ccfe76d90c4ad606e3cbc5e5a31b74bfc353d8fa4b7dcc2fcb9893813
Finished request 0
Going to the next request
--- Walking the entire request list ---
Waking up in 6 seconds...
rad_recv: Access-Request packet from host 192.168.123.2:4262, id=74, length=229
  User-Name = "KEN"
  NAS-IP-Address = 192.168.123.2
  Called-Station-Id = "004096431d06"
  Calling-Station-Id = "000625039e69"
  NAS-Identifier = "AP340-431d06"
  NAS-Port = 29
  Framed-MTU = 1400
  State =
0x3506d24e9ac1a05ccfe76d90c4ad606e3cbc5e5a31b74bfc353d8fa4b7dcc2fcb9893813
  NAS-Port-Type = Wireless-802.11
  EAP-Message =
"\002\004\000P\r\200\000\000\000F\026\003\001\000A\001\000\000=\003\001<\274^SeE\223\2
55\242\354\213\361\221\3301\027\201\0231\023f\222Qc\267~\3200\216\211\3721\000\000\026
\000\004\000\005\000\n\000\t\000d\000b\000\003\000\006\000\023\000\022\000c\001"
  Message-Authenticator = 0x47abf8cabb646859df38415183adb602
modcall: entering group authorize
  modcall[authorize]: module "preprocess" returns ok
  modcall[authorize]: module "eap" returns updated
    rlm_realm: Looking up realm NULL for User-Name = "KEN"
    rlm_realm: No such realm NULL
  modcall[authorize]: module "suffix" returns noop
    users: Matched KEN at 25
  modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
  rad_check_password: Found Auth-Type EAP
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: Request found, released from the list
rlm_eap: EAP_TYPE - tls
rlm_eap: processing type tls
rlm_eap_tls: Length Included
undefined: before/accept initialization
TLS_accept: before/accept initialization
<<< TLS 1.0 Handshake [length 0041], ClientHello

TLS_accept: SSLv3 read client hello A
>>> TLS 1.0 Handshake [length 004a], ServerHello

TLS_accept: SSLv3 write server hello A
>>> TLS 1.0 Handshake [length 0613], Certificate

TLS_accept: SSLv3 write certificate A
>>> TLS 1.0 Handshake [length 0096], CertificateRequest

TLS_accept: SSLv3 write certificate request A
TLS_accept: SSLv3 flush data
TLS_accept:error in SSLv3 read client certificate A
```

```
rlm_eap_tls: SSL_read Error
  Error code is ..... 2
  SSL Error ..... 2
In SSL Handshake Phase
In SSL Accept mode
  modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Login OK: [KEN/<no User-Password attribute>] (from client 192.168.123.2 port 29 cli
000625039e69)
Sending Access-Challenge of id 74 to 192.168.123.2:4262
  Acct-Interim-Interval = 30
  Idle-Timeout = 7200
  Session-Timeout = 14400
  EAP-Message =
"\001\005\004\n\r\300\000\000\007\002\026\003\001\000J\002\000\000F\003\001<\274^Zn"\0
30\200TW\237?\014\377\300\253\250\330\236e\205\321\343\005\262X5\212\006\311\274\001
\322\353\262\203P'n\273\323\376\226\243\036\274\374j\226\001\325\364\334gK\250,*L\005\
314\275\347L\000\004\000\026\003\001\006\023\013\000\006\017\000\006\014\000\002\2350\
202\002\2310\202\002\002\240\003\002\001\002\002\001\0020\r\006\t*\206H\206\367\r\001\
001\004\005\0000\201\2041\0130\t\006\003U\004\006\023\002US1\0230\021\006\003U\004"
  EAP-Message =
"\367\r\001\t\001\026\013root@bw.com0\036\027\r020416162850Z\027\r030416162850Z0\201\2
061\0130\t\006\003U\004\006\023\002US1\0230\021\006\003U\004\010\023\nNew
Jersey1\0270\025\006\003U\004\007\023\016New
Providence1\0130\t\006\003U\004\n\023\002BW1\0170\r\006\003U\004\013\023\006TESTIT1\01
70\r\006\003U\004\003\023\006server1\0320\030\006\t*\206H\206\367\r\001\t\001\026\013r
oot@bw.com0\201\2370\r\006\t*\206H\206\367\r\001\001\001\005\000\003\201\215\0000\201\
211\002\201\201\000\322H\224j\257e\327\325\327\312"
  EAP-Message =
"\322M!\277\324\r\367\360\203\267\225\036^\007\215\0266\364h\232p\006\rq[\277h\024\321
\332L\0160\371\327\230)\207\031;;\236\317&\202c=\265\253n\302\334\025\001\316*$2\334\2
112P\372<PX.\023Tg\322.\010~\345\320\366\272\021n\333z\214\025\002>\256~|\207U\002\00
3\001\000\001\243\0270\0250\023\006\003U\035%\004\0140\n\006\010+\006\001\005\005\007\
003\0010\r\006\t*\206H\206\367\r\001\001\004\005\000\003\201\201\000\014\330\325q\346\
016{\230\0028X\306\026\300\017.!\320C\320ul\206n\n\340\017\001wf\334\354v\346\216"
  EAP-Message =
"\352\265YJ\217\340\256\257\233=4\330"\222\224\002\021\000\003i0\202\003e0\202\002\316
\240\003\002\001\002\002\001\0000\r\006\t*\206H\206\367\r\001\001\004\005\0000\201\204
1\0130\t\006\003U\004\006\023\002US1\0230\021\006\003U\004\010\023\nNew
Jersey1\0270\025\006\003U\004\007\023\016New
Providence1\0130\t\006\003U\004\n\023\002BW1\0170\r\006\003U\004\013\023\006TESTIT1\r0
\013\006\003U\004\003\023\004root1\0320\030\006\t*\206H\206\367\r\001\t\001\026\013roo
t@bw.com0\036\027\r020416162832Z\027\r040415162832"
  EAP-Message = "sey1\0270\025\006\003U\004\007\023\016New Providen"
  Message-Authenticator = 0x00000000000000000000000000000000
  State =
0x97ef6223ce6bacb1636260ea71f461a23cbc5e5ad72bd01de82881b41d1afe7a051b93db
Finished request 1
Going to the next request
Waking up in 6 seconds...
rad_recv: Access-Request packet from host 192.168.123.2:4263, id=75, length=155
  User-Name = "KEN"
  NAS-IP-Address = 192.168.123.2
  Called-Station-Id = "004096431d06"
  Calling-Station-Id = "000625039e69"
  NAS-Identifier = "AP340-431d06"
  NAS-Port = 29
  Framed-MTU = 1400
  State =
0x97ef6223ce6bacb1636260ea71f461a23cbc5e5ad72bd01de82881b41d1afe7a051b93db
  NAS-Port-Type = Wireless-802.11
  EAP-Message = "\002\005\000\006\r"
  Message-Authenticator = 0xb88e4b53984bccf9f1017f8d8585efa6
modcall: entering group authorize
  modcall[authorize]: module "preprocess" returns ok
  modcall[authorize]: module "eap" returns updated
  rlm_realm: Looking up realm NULL for User-Name = "KEN"
```

```
rlm_realm: No such realm NULL
modcall[authorize]: module "suffix" returns noop
users: Matched KEN at 25
modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: Request found, released from the list
rlm_eap: EAP_TYPE - tls
rlm_eap: processing type tls
rlm_eap tls: Received EAP-TLS ACK message
modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Login OK: [KEN/<no User-Password attribute>] (from client 192.168.123.2 port 29 cli
000625039e69)
Sending Access-Challenge of id 75 to 192.168.123.2:4263
Acct-Interim-Interval = 30
Idle-Timeout = 7200
Session-Timeout = 14400
EAP-Message =
"\001\006\003\014\r\200\000\000\007\002ce1\0130\t\006\003U\004\n\023\002BW1\0170\r\006
\003U\004\013\023\006TESTIT1\r\0\013\006\003U\004\003\023\004root1\0320\030\006\t*\206H
\206\367\r\001\t\001\026\013root@bw.com\201\2370\r\006\t*\206H\206\367\r\001\001\001\
005\000\003\201\215\0000\201\211\002\201\201\000\317\003\215\337he\024i\247\237\220\34
4\001\301g\376\006J\237\201\271\345Nu\027g^u\211\237\203\231\260/\3316M\303\372\033\30
3\353\213yrj\255\017/\005\325\2142mF\217\036h\031$\361m\002\307>\332\037\276?\245"
EAP-Message =
"\3410\035\006\003U\035\016\004\026\004\024\260\347y(\033\371\020\376\014\024\264U~\3
77\223\252(650\201\261\006\003U\035#\004\201\2510\201\246\200\024\260\347y(\033\371\0
20\376\014\024\264U~\377\223\252(65\241\201\212\244\201\2070\201\2041\0130\t\006\003U\
004\006\023\002US1\0230\021\006\003U\004\010\023\nNew
Jersey1\0270\025\006\003U\004\007\023\016New
Providence1\0130\t\006\003U\004\n\023\002BW1\0170\r\006\003U\004\013\023\006TESTIT1\r0
\013\006\003U\004\003\023\004root1\0320\030\006\t*\206H\206\367\r\001"
EAP-Message =
"M$Y\230\353v\205\317\337\252BL4\376\224\372\371v\307\304\263A\334\233=\251\361\333@2
23\2275\345k1I\260\035n9\t9\342\231L\312\353\262\263T\025\360\326\221\272F\033.T\262\0
21\335\365\033ZD\033\031\260\355\017\370j\202M\271d-
N\366\304\253\373j\346\214\346p\031\2539\271\242h\236\241$Vs\306\014\322\236\024.\325o
\032\353=\200)\200zq\345\346s\201\337#\026\003\001\000\226\r\000\000\216\002\001\002\0
00\211\000\2070\201\2041\0130\t\006\003U\004\006\023\002US1\0230\021\006\003U\004\010\
023\nNew Jersey1\0270\025\006"
EAP-Message = "H\206\367\r\001\t\001\026\013root@bw.com\016\000\000"
Message-Authenticator = 0x00000000000000000000000000000000
State =
0x2b773d126657f7639eac84899ec7daf33cbc5e5cf34e6c32feb9278a692cf0dfaf305fd9
Finished request 2
Going to the next request
--- Walking the entire request list ---
Waking up in 4 seconds...
rad_recv: Access-Request packet from host 192.168.123.2:4264, id=76, length=1157
User-Name = "KEN"
NAS-IP-Address = 192.168.123.2
Called-Station-Id = "004096431d06"
Calling-Station-Id = "000625039e69"
NAS-Identifier = "AP340-431d06"
NAS-Port = 29
Framed-MTU = 1400
State =
0x2b773d126657f7639eac84899ec7daf33cbc5e5cf34e6c32feb9278a692cf0dfaf305fd9
NAS-Port-Type = Wireless-802.11
EAP-Message =
"\002\006\003\352\r\200\000\000\003\340\026\003\001\003\260\013\000\002\240\000\002\23
5\000\002\2320\202\002\2260\202\001\377\240\003\002\001\002\002\001\0010\r\006\t*\206H
\206\367\r\001\001\004\005\0000\201\2041\0130\t\006\003U\004\006\023\002US1\0230\021\0
06\003U\004\010\023\nNew Jersey1\0270\025\006\003U\004\007\023\016New
```

Providence1\0130\t\006\003U\004\n\023\002BW1\0170\r\006\003U\004\013\023\006TESTIT1\r0
\013\006\003U\004\003\023\004root1\0320\030\006\t*\206H\206\367\r\001\t\001\026\013root
t@bw.com0\036"

EAP-Message = " Jersey1\0270\025\006\003U\004\007\023\016New
Providence1\0130\t\006\003U\004\n\023\002BW1\0170\r\006\003U\004\013\023\006TESTIT1\01
40\n\006\003U\004\003\023\003KEN1\0320\030\006\t*\206H\206\367\r\001\t\001\026\013root
@bw.com0\201\2370\r\006\t*\206H\206\367\r\001\001\001\005\000\003\201\215\0000\201\211
\002\201\201\000\232E\261S#K\352zx\336@z\304\376^h\376\024V\206\250w\306Y\307+\240\205
\0176\327\317\271xq\242hZ\355A\204\376\345\325\252,\245\210JD\226\213\334y\220I\032\31
7R\r\373\241|\022\301\250\254\340\250"

EAP-Message =
"\216F77N\014\254\253\002\003\001\000\001\243\0270\0250\023\006\003U\035%\004\0140\n\0
06\010+\006\001\005\005\007\003\0020\r\006\t*\206H\206\367\r\001\001\004\005\000\003\2
01\201\000-\016B\245\262\031\032\260\033\336\004\340\230\377-
fm\031k\261\031k\236\360\254\254\247\035\242;X\372u\223i\273\325\007U?\025\327n*\310{h
jW\200~u)\216\2279\316\023\267%\{ \236\311\335\245\366In#\013\000\313\310\234A\261\201[\
315\274\334`)no\006#\347h\353%yLZ\013\244\026\214\227\017\200\0276U\370\224P\230\3356\
336w\304\2646\366\225"

EAP-Message = "\303\365\3316-
rAG\242\3224□r;\025\211k\257L\020& :r\3170\206\017\002\327\234M\213\220\274e\361\330m"
\246f\357\n\244\351\264\360R\$\212\247\213\224\033\026x\202\005\\\231m\202\265b\017\00
0\000\202\000\2005\216\014\360\304{\312\310@255\275\304\325\300o\n9\310aa\376\016\363
\351\236\231\370W\017P\326\214_366_230\2628\326\267\233N\014\237ni\366\243\334"\256\
301\244J"
\000b\245\232\247\306\353\231f\243;\242\241V\342/|\265\232\321X\200\306\277\r`\232\330
□S\366\205\001m\010\377_)bjM\321\031\371"*\230\357FO\354"

Message-Authenticator = 0xd26d6b213424fda43524969796a39031

modcall: entering group authorize
modcall[authorize]: module "preprocess" returns ok
modcall[authorize]: module "eap" returns updated
rlm_realm: Looking up realm NULL for User-Name = "KEN"
rlm_realm: No such realm NULL
modcall[authorize]: module "suffix" returns noop
users: Matched KEN at 25
modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: Multiple EAP_Message attributes found
rlm_eap: Request found, released from the list
rlm_eap: EAP_TYPE - tls
rlm_eap: processing type tls
rlm_eap_tls: Length Included
<<< TLS 1.0 Handshake [length 02a4], Certificate

chain-depth=1,
error=0
--> User-Name = KEN
--> BUF-Name = root
--> subject = /C=US/ST=New Jersey/L=New
Providence/O=BW/OU=TESTIT/CN=root/Email=root@bw.com
--> issuer = /C=US/ST=New Jersey/L=New
Providence/O=BW/OU=TESTIT/CN=root/Email=root@bw.com
--> verify return:1
chain-depth=0,
error=0
--> User-Name = KEN
--> BUF-Name = KEN
--> subject = /C=US/ST=New Jersey/L=New
Providence/O=BW/OU=TESTIT/CN=KEN/Email=root@bw.com
--> issuer = /C=US/ST=New Jersey/L=New
Providence/O=BW/OU=TESTIT/CN=root/Email=root@bw.com
--> verify return:1
TLS accept: SSLv3 read client certificate A
<<< TLS 1.0 Handshake [length 0086], ClientKeyExchange


```
TLS_accept: SSLv3 read client key exchange A
<<< TLS 1.0 Handshake [length 0086], CertificateVerify

TLS_accept: SSLv3 read certificate verify A
<<< TLS 1.0 ChangeCipherSpec [length 0001]

<<< TLS 1.0 Handshake [length 0010], Finished

TLS_accept: SSLv3 read finished A
>>> TLS 1.0 ChangeCipherSpec [length 0001]

TLS_accept: SSLv3 write change cipher spec A
>>> TLS 1.0 Handshake [length 0010], Finished

TLS_accept: SSLv3 write finished A
TLS_accept: SSLv3 flush data
undefined: SSL negotiation finished successfully
rlm_eap_tls: SSL_read Error
  Error code is ..... 2
  SSL Error ..... 2
SSL Connection Established
  modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Login OK: [KEN/<no User-Password attribute>] (from client 192.168.123.2 port 29 cli
000625039e69)
Sending Access-Challenge of id 76 to 192.168.123.2:4264
  Acct-Interim-Interval = 30
  Idle-Timeout = 7200
  Session-Timeout = 14400
  EAP-Message =
"\001\007\0005\r\200\000\000\000+\024\003\001\000\001\001\026\003\001\000
\301\244\215\023\352+\241X^\007P\217\274\302\310\nv\220\343Iiu\224\010x8\353\331\031w\
310?"
  Message-Authenticator = 0x00000000000000000000000000000000
  State =
0x6adc6a53191835de12975988783c5d3cbc5e5e2c781afaaa6fb6942ae8225f89e78868
Finished request 3
Going to the next request
--- Walking the entire request list ---
Waking up in 2 seconds...
rad_recv: Access-Request packet from host 192.168.123.2:4265, id=77, length=155
  User-Name = "KEN"
  NAS-IP-Address = 192.168.123.2
  Called-Station-Id = "004096431d06"
  Calling-Station-Id = "000625039e69"
  NAS-Identifier = "AP340-431d06"
  NAS-Port = 29
  Framed-MTU = 1400
  State =
0x6adc6a53191835de12975988783c5d3cbc5e5e2c781afaaa6fb6942ae8225f89e78868
  NAS-Port-Type = Wireless-802.11
  EAP-Message = "\002\007\000\006\r"
  Message-Authenticator = 0x7e3de717199c91381f3e89126721390d
modcall: entering group authorize
  modcall[authorize]: module "preprocess" returns ok
  modcall[authorize]: module "eap" returns updated
  rlm_realm: Looking up realm NULL for User-Name = "KEN"
  rlm_realm: No such realm NULL
  modcall[authorize]: module "suffix" returns noop
  users: Matched KEN at 25
  modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
  rad_check_password: Found Auth-Type EAP
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: Request found, released from the list
rlm_eap: EAP_TYPE - tls
```

```
rlm_eap: processing type tls
rlm_eap_tls: Received EAP-TLS ACK message
  modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Login OK: [KEN/<no User-Password attribute>] (from client 192.168.123.2 port 29 cli
000625039e69)
Sending Access-Accept of id 77 to 192.168.123.2:4265
  Acct-Interim-Interval = 30
  Idle-Timeout = 7200
  Session-Timeout = 14400
  EAP-Message = "\003\010\000\004"
  Message-Authenticator = 0x00000000000000000000000000000000
Finished request 4
Going to the next request
Waking up in 2 seconds...
--- Walking the entire request list ---
Cleaning up request 0 ID 73 with timestamp 3cbc5e5a
Cleaning up request 1 ID 74 with timestamp 3cbc5e5a
Waking up in 2 seconds...
--- Walking the entire request list ---
Cleaning up request 2 ID 75 with timestamp 3cbc5e5c
Waking up in 2 seconds...
--- Walking the entire request list ---
Cleaning up request 3 ID 76 with timestamp 3cbc5e5e
Cleaning up request 4 ID 77 with timestamp 3cbc5e5e
Nothing to do. Sleeping until we see a request.
```

6. Cisco AP340 EAP log

An EAP log can be obtained on the Cisco AP340 by telnet'ing to the IP address of the AP and typing the following command ":eap_diag2_on". Don't type the quotes, but be sure to type the colon (:). See [4] for full details on troubleshooting techniques with the AP340.

```

4 days, 20:52:15 (Info): Station [192.168.123.7]000625039e69 Authenticated

4 days, 20:52:15 (Info): Station [192.168.123.7]000625039e69 Associated
EAP: Sending Identity Request

00c17a20:      01 00 00 39 01 02 00 39 01 00 6e 65 74 77 *   ..9...9..netw*
00c17a30:  6f 72 6b 69 64 3d 62 72 6f 61 64 77 61 76 65 5f *orkid=broadwave_*
00c17a40:  61 70 31 2c 6e 61 73 69 64 3d 41 50 33 34 30 2d *apl,nasid=AP340-*
00c17a50:  34 33 31 64 30 36 2c 70 6f 72 74 69 64 3d 30 *431d06,portid=0.*

EAP: Received packet from client 192.168.123.7

00c13070:      01 01 00 00 *   .....*

EAP: Type = EAPOL START
EAP: Sending Identity Request

00c18350:      01 00 00 39 01 03 00 39 01 00 *   ..9...9...*
00c18360:  6e 65 74 77 6f 72 6b 69 64 3d 62 72 6f 61 64 77 *networkid=broadw*
00c18370:  61 76 65 5f 61 70 31 2c 6e 61 73 69 64 3d 41 50 *ave_ap1,nasid=AP*
00c18380:  33 34 30 2d 34 33 31 64 30 36 2c 70 6f 72 74 69 *340-431d06,porti*
00c18390:  64 3d 30 *d=0.....*

EAP: Received packet from client 192.168.123.7

00c17a10:      01 00 00 08 02 02 00 08 01 4b 45 4e *   .....KEN*

EAP: Type = Identity Response
EAP: Response not from most recent request. Dropping packet.
EAP: Received packet from client 192.168.123.7

00c17a10:      01 00 00 08 02 03 00 08 01 4b 45 4e *   .....KEN*

EAP: Type = Identity Response
EAP: Forwarding packet to RADIUS server

00albfc0:      01 49 00 77 49 3e a9 96 *   I.wI>..*
00albfd0:  ee 61 b2 c4 7c af f7 e3 a1 f6 99 a4 01 05 4b 45 *.a..|.....KE*
00albfe0:  4e 04 06 c0 a8 7b 02 1e 0e 30 30 34 30 39 36 34 *N....{...0040964*
00albff0:  33 31 64 30 36 1f 0e 30 30 30 36 32 35 30 33 39 *31d06..000625039*
00alc000:  65 36 39 20 0e 41 50 33 34 30 2d 34 33 31 64 30 *e69 .AP340-431d0*
00alc010:  36 05 06 00 00 00 1d 0c 06 00 00 05 78 3d 06 00 *6.....x=..*
00alc020:  00 00 13 4f 0a 02 03 00 08 01 4b 45 4e 50 12 e0 *...O.....KENP..*
00alc030:  58 9a 75 49 ba 0f 84 22 60 ed 30 0e 4e 18 48 *X.uI..."`.0.N.H.*

RADIUS: Received packet for client 192.168.123.7

00977000:  0b 49 00 66 65 55 30 92 0e bc 90 46 d5 f1 3e 00 *.I.feU0....F.>.*
00977010:  5d 51 e6 b3 55 06 00 00 00 1e 1c 06 00 00 1c 20 *]Q..U..... *
00977020:  1b 06 00 00 38 40 4f 08 01 04 00 06 0d 20 50 12 *...8@O..... P.*
00977030:  94 bc 51 14 db a8 a8 2e f1 da e0 f0 97 d9 3a 67 *..Q.....:g*
00977040:  18 26 35 06 d2 4e 9a c1 a0 5c cf e7 6d 90 c4 ad *.&5..N...\.m...*
00977050:  60 6e 3c bc 5e 5a 31 b7 4b fc 35 3d 8f a4 b7 dc *`n<.^Z1.K.5=....*
00977060:  c2 fc b9 89 38 13 *.....8.....*

RADIUS: Received Challenge Request
RADIUS: Received session timeout request of 14400 seconds
RADIUS: Sending EAPOL packet to client 192.168.123.7

00c17a20:      01 00 00 06 01 04 00 06 0d 20 *   ..... *

```

EAP: Received packet from client 192.168.123.7

```

00c18340:                01 00 00 50 02 04 00 50 *          ..P...P*
00c18350: 0d 80 00 00 00 46 16 03 01 00 41 01 00 00 3d 03 *.....F....A...=*
00c18360: 01 3c bc 5e 53 65 45 93 ad a2 ec 8b f1 91 d8 31 *.<.^SeE.....1*
00c18370: 17 81 13 6c 13 66 92 51 63 b7 7e d0 30 8e 89 fa *...l.f.Qc~.0...*
00c18380: 31 00 00 16 00 04 00 05 00 0a 00 09 00 64 00 62 *1.....d.b*
00c18390: 00 03 00 06 00 13 00 12 00 63 01 00 *.....c.....*

```

EAP: Forwarding packet to RADIUS server

```

00albfc0:                01 4a 00 e5 5b 80 0c eb *          J...[...*
00albfd0: 1f 92 67 09 2e 20 ef 7c 86 df 34 8e 01 05 4b 45 *..g...|.4...KE*
00albfe0: 4e 04 06 c0 a8 7b 02 1e 0e 30 30 34 30 39 36 34 *N....{...0040964*
00albff0: 33 31 64 30 36 1f 0e 30 30 30 36 32 35 30 33 39 *31d06..000625039*
00alc000: 65 36 39 20 0e 41 50 33 34 30 2d 34 33 31 64 30 *e69 .AP340-431d0*
00alc010: 36 05 06 00 00 00 1d 0c 06 00 00 05 78 18 26 35 *6.....x.&5*
00alc020: 06 d2 4e 9a c1 a0 5c cf e7 6d 90 c4 ad 60 6e 3c *..N...\.m...n<*
00alc030: bc 5e 5a 31 b7 4b fc 35 3d 8f a4 b7 dc c2 fc b9 *.^Zl.K.5=.....*
00alc040: 89 38 13 3d 06 00 00 00 13 4f 52 02 04 00 50 0d *.8.=.....OR...P.*
00alc050: 80 00 00 00 46 16 03 01 00 41 01 00 00 3d 03 01 *....F....A...=*
00alc060: 3c bc 5e 53 65 45 93 ad a2 ec 8b f1 91 d8 31 17 *<.^SeE.....1.*
00alc070: 81 13 6c 13 66 92 51 63 b7 7e d0 30 8e 89 fa 31 *...l.f.Qc~.0...1*
00alc080: 00 00 16 00 04 00 05 00 0a 00 09 00 64 00 62 00 *.....d.b.*
00alc090: 03 00 06 00 13 00 12 00 63 01 00 50 12 47 ab f8 *.....c..P.G...*
00alc0a0: ca bb 64 68 59 df 38 41 51 83 ad b6 02 *..dhY.8AQ.....*

```

RADIUS: Received packet for client 192.168.123.7

```

00974840:                0b 4a 04 72 6f 3b 54 fc *          J.ro;T.*
00974850: d2 61 56 76 17 a4 ab cc 20 91 f5 bd 55 06 00 00 *.aVv....U...*
00974860: 00 1e 1c 06 00 00 1c 20 1b 06 00 00 38 40 4f fe *.....8@.*
00974870: 01 05 04 0a 0d c0 00 00 07 02 16 03 01 00 4a 02 *.....J.*
00974880: 00 00 46 03 01 3c bc 5e 5a 6e 22 18 80 54 57 9f *..F.<.^Zn"..TW.*
00974890: 3f 0c ff c0 ab a8 d8 9e 65 85 d1 e3 05 b2 58 35 *?...e.....X5*
009748a0: 8a 06 c9 bc 01 20 d2 eb b2 83 50 60 6e bb d3 fe *.....P`n...*
009748b0: 96 a3 1e bc fc 5d 96 01 d5 f4 dc 67 4b a8 2c 2a *.....]....gK.,**
009748c0: 4c 05 cc bd e7 4c 00 04 00 16 03 01 06 13 0b 00 *L....L.....*
009748d0: 06 0f 00 06 0c 00 02 9d 30 82 02 99 30 82 02 02 *.....0...0...*
009748e0: a0 03 02 01 02 02 01 02 30 0d 06 09 2a 86 48 86 *.....0...*H.*
009748f0: f7 0d 01 01 04 05 00 30 81 84 31 0b 30 09 06 03 *.....0...1.0...*
00974900: 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 *U....US1.0...U...*
00974910: 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 17 30 15 *..New Jersey1.0.*
00974920: 06 03 55 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 *.U...New Provi*
00974930: 64 65 6e 63 65 31 0b 30 09 06 03 55 04 0a 13 02 *dence1.0...U...*
00974940: 42 57 31 0f 30 0d 06 03 55 04 0b 13 06 54 45 53 *Bw1.0...U...TES*
00974950: 54 49 54 31 0d 30 0b 06 03 55 04 03 13 04 72 6f *TIT1.0...U...ro*
00974960: 6f 74 31 1a 30 18 06 09 2a 86 48 86 4f fe f7 0d *ot1.0...*H.O...*
00974970: 01 09 01 16 0b 72 6f 6f 74 40 62 77 2e 63 6f 6d *.....root@bw.com*
00974980: 30 1e 17 0d 30 32 30 34 31 36 31 36 32 38 35 30 *0...020416162850*
00974990: 5a 17 0d 30 33 30 34 31 36 31 36 32 38 35 30 5a *Z..030416162850Z*
009749a0: 30 81 86 31 0b 30 09 06 03 55 04 06 13 02 55 53 *0...1.0...U...US*
009749b0: 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a *1.0...U...New J*
009749c0: 65 72 73 65 79 31 17 30 15 06 03 55 04 07 13 0e *ersey1.0...U...*
009749d0: 4e 65 77 20 50 72 6f 76 69 64 65 6e 63 65 31 0b *New Providencel.*
009749e0: 30 09 06 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 *0...U...Bw1.0...*
009749f0: 03 55 04 0b 13 06 54 45 53 54 49 54 31 0f 30 0d *.U...TESTIT1.0.*
00974a00: 06 03 55 04 03 13 06 73 65 72 76 65 72 31 1a 30 *.U...server1.0*
00974a10: 18 06 09 2a 86 48 86 f7 0d 01 09 01 16 0b 72 6f *...*H.....ro*
00974a20: 6f 74 40 62 77 2e 63 6f 6d 30 81 9f 30 0d 06 09 *ot@bw.com0...0...*
00974a30: 2a 86 48 86 f7 0d 01 01 05 00 03 81 8d 00 30 **..H.....0...*
00974a40: 81 89 02 81 81 00 d2 48 94 5d af 40 d7 d5 d7 ca *.....H.]@.....*
00974a50: e9 b9 f0 e8 3f 18 5e 41 cb 3b ff 66 96 c3 01 e9 *....?.^A.;f....*
00974a60: 99 73 fc 5b a4 8c f5 4c ba 40 4f fe d2 4d 21 bf *.s.[...L.@.M!*
00974a70: d4 0d f7 f0 83 b7 95 1e 5e 07 8d 16 36 f4 68 9a *.....^...6.h.*
00974a80: 70 06 0d 71 5b bf 68 14 d1 da 4c 0e 4f f9 d7 98 *p..q[.h...L.O...*

```

```

00974a90: 29 87 19 3b 3b 9e cf 26 82 63 3d b5 ab 6e c2 dc *)...;...&.c=.n..*
00974aa0: 15 01 ce 2a 24 32 dc 89 32 50 fa 3c 50 58 2e 13 *...*$2..2P.<PX..*
00974ab0: 54 67 d2 2e 08 7e e5 d0 f6 ba 7f 11 6e db 7a 8c *Tg...~.....n.z.*
00974ac0: 15 02 3e ae 7e 7c 87 55 02 03 01 00 01 a3 17 30 *...>~|.U.....0*
00974ad0: 15 30 13 06 03 55 1d 25 04 0c 30 0a 06 08 2b 06 *.0...U.%..0...+.*
00974ae0: 01 05 05 07 03 01 30 0d 06 09 2a 86 48 86 f7 0d *.....0...*.H...*
00974af0: 01 01 04 05 00 03 81 81 00 0c d8 d5 71 e6 0e 7b *.....q..{*
00974b00: 98 02 38 58 c6 16 c0 0f 2e 21 d0 43 d0 75 6c 86 *.8X.....!.C.ul.*
00974b10: 6e 0a e0 0f 01 77 66 dc ec 76 e6 8e e9 8c 78 98 *n.....wf..v.....x.*
00974b20: b6 20 50 6a 6e 4c 57 45 5b 77 54 f9 64 3b 54 c3 *. PjnLWE[wT;d;T.*
00974b30: 9a 00 7d f2 e9 04 50 40 2d d0 47 e1 e9 2c 05 6e *..}...P@-.G...n*
00974b40: 11 9b a4 a0 f6 aa b5 0a 82 49 55 08 9d b2 d6 d5 *.....IU.....*
00974b50: 86 5f 45 90 57 1f cf 96 3e fb bf e2 22 65 6e ba *..E.W...>...".en.*
00974b60: 60 09 d0 40 be 06 22 1e 4f fe ea b5 59 4a 8f e0 *`.@...".O...YJ.*
00974b70: ae af 9b 3d 34 d8 22 92 94 02 11 00 03 69 30 82 *...=4.".....i0.*
00974b80: 03 65 30 82 02 ce a0 03 02 01 02 02 01 00 30 0d *.e0.....0.*
00974b90: 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30 81 84 *..*.H.....0...*
00974ba0: 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 *1.0...U....US1.0*
00974bb0: 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 *...U....New Jers*
00974bc0: 65 79 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 *eyl.0...U....New*
00974bd0: 20 50 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 * Providence1.0...*
00974be0: 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 *.U....BW1.0...U.*
00974bf0: 0b 13 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 *...TESTIT1.0...U*
00974c00: 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 *....root1.0....*
00974c10: 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 40 62 77 *H.....root@bw*
00974c20: 2e 63 6f 6d 30 1e 17 0d 30 32 30 34 31 36 31 36 *.com0...02041616*
00974c30: 32 38 33 32 5a 17 0d 30 34 30 34 31 35 31 36 32 *2832Z..040415162*
00974c40: 38 33 32 5a 30 81 84 31 0b 30 09 06 03 55 04 06 *832Z0..1.0...U..*
00974c50: 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e *..US1.0...U....N*
00974c60: 65 77 20 4a 65 72 4f 1c 73 65 79 31 17 30 15 06 *ew JerO.seyl.0...*
00974c70: 03 55 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 64 *.U....New Provid*
00974c80: 65 6e 50 12 4c 73 b8 cc a5 27 c3 65 97 d8 67 84 *enP.Ls...'.e.g.*
00974c90: b9 4a 6e bf 18 26 97 ef 62 23 ce 6b ac b1 63 62 *.Jn...&.b#.k.cb*
00974ca0: 60 ea 71 f4 61 a2 3c bc 5e 5a d7 2b d0 1d e8 28 *`.q.a.<.^Z.+...(*
00974cb0: 81 b4 1d 1a fe 7a 05 1b 93 db *.....z.....*

```

```

RADIUS: Received Challenge Request
RADIUS: Received session timeout request of 14400 seconds
RADIUS: Appending EAP attribute value of length 254
RADIUS: Appending EAP attribute value of length 254
RADIUS: Appending EAP attribute value of length 254
RADIUS: Appending EAP attribute value of length 28
RADIUS: Sending EAPOL packet to client 192.168.123.7

```

```

00c17a20: 01 00 04 0a 01 05 04 0a 0d c0 00 00 07 02 * .....*
00c17a30: 16 03 01 00 04 02 00 00 46 03 01 3c bc 5e 5a 6e *....J...F...<.^Zn*
00c17a40: 22 18 80 54 57 9f 3f 0c ff c0 ab a8 d8 9e 65 85 *"...TW.?.....e.*
00c17a50: d1 e3 05 b2 58 35 8a 06 c9 bc 01 20 d2 eb b2 83 *....X5.....*
00c17a60: 50 60 6e bb d3 fe 96 a3 1e bc fc 5d 96 01 d5 f4 *P`n.....]....*
00c17a70: dc 67 4b a8 2c 2a 4c 05 cc bd e7 4c 00 04 00 16 *.gK.,*L....L....*
00c17a80: 03 01 06 13 0b 00 06 0f 00 06 0c 00 02 9d 30 82 *.....0.*
00c17a90: 02 99 30 82 02 02 a0 03 02 01 02 02 01 02 30 0d *.0.....0.*
00c17aa0: 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30 81 84 *..*.H.....0...*
00c17ab0: 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 *1.0...U....US1.0*
00c17ac0: 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 *...U....New Jers*
00c17ad0: 65 79 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 *eyl.0...U....New*
00c17ae0: 20 50 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 * Providence1.0...*
00c17af0: 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 *.U....BW1.0...U.*
00c17b00: 0b 13 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 *...TESTIT1.0...U*
00c17b10: 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 *....root1.0....*
00c17b20: 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 40 62 77 *H.....root@bw*
00c17b30: 2e 63 6f 6d 30 1e 17 0d 30 32 30 34 31 36 31 36 *.com0...02041616*
00c17b40: 32 38 35 30 5a 17 0d 30 33 30 34 31 36 31 36 32 *2850Z..030416162*
00c17b50: 38 35 30 5a 30 81 86 31 0b 30 09 06 03 55 04 06 *850Z0..1.0...U..*
00c17b60: 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e *..US1.0...U....N*
00c17b70: 65 77 20 4a 65 72 73 65 79 31 17 30 15 06 03 55 *ew Jersey1.0...U*
00c17b80: 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 64 65 6e *....New Providen*

```

```

00c17b90: 63 65 31 0b 30 09 06 03 55 04 0a 13 02 42 57 31 *cel.0...U...BW1*
00c17ba0: 0f 30 0d 06 03 55 04 0b 13 06 54 45 53 54 49 54 *.0...U...TESTIT*
00c17bb0: 31 0f 30 0d 06 03 55 04 03 13 06 73 65 72 76 65 *1.0...U...serve*
00c17bc0: 72 31 1a 30 18 06 09 2a 86 48 86 f7 0d 01 09 01 *r1.0...*.H.....*
00c17bd0: 16 0b 72 6f 6f 74 40 62 77 2e 63 6f 6d 30 81 9f *..root@bw.com0..*
00c17be0: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 *0...*.H.....*
00c17bf0: 81 8d 00 30 81 89 02 81 81 00 d2 48 94 5d af 40 *...0.....H.]@*
00c17c00: d7 d5 d7 ca e9 b9 f0 e8 3f 18 5e 41 cb 3b ff 66 *.....?.^A.;f*
00c17c10: 96 c3 01 e9 99 73 fc 5b a4 8c f5 4c ba 40 d2 4d *.....s.[...L.@.M*
00c17c20: 21 bf d4 0d f7 f0 83 b7 95 1e 5e 07 8d 16 36 f4 *!.....^...6.*
00c17c30: 68 9a 70 06 0d 71 5b bf 68 14 d1 da 4c 0e 4f f9 *h.p..q[.h...L.O.*
00c17c40: d7 98 29 87 19 3b 3b 9e cf 26 82 63 3d b5 ab 6e *..)....;...&.c=.n*
00c17c50: c2 dc 15 01 ce 2a 24 32 dc 89 32 50 fa 3c 50 58 *.....*$2..2P.<PX*
00c17c60: 2e 13 54 67 d2 2e 08 7e e5 d0 f6 ba 7f 11 6e db *..Tg....~.....*
00c17c70: 7a 8c 15 02 3e ae 7e 7c 87 55 02 03 01 00 01 a3 *z...>..~|.U.....*
00c17c80: 17 30 15 30 13 06 03 55 1d 25 04 0c 30 0a 06 08 *.0.0...U.%.0...*
00c17c90: 2b 06 01 05 05 07 03 01 30 0d 06 09 2a 86 48 86 *+.....0...*.H.*
00c17ca0: f7 0d 01 01 04 05 00 03 81 81 00 0c d8 d5 71 e6 *.....*.....*
00c17cb0: 0e 7b 98 02 38 58 c6 16 c0 0f 2e 21 d0 43 d0 75 *.{...8X.....!.C.u*
00c17cc0: 6c 86 6e 0a e0 0f 01 77 66 dc ec 76 e6 8e e9 8c *l.n....wf..v....*
00c17cd0: 78 98 b6 20 50 6a 6e 4c 57 45 5b 77 54 f9 64 3b *x.. PjnLWE[wL;d;*
00c17ce0: 54 c3 9a 00 7d f2 e9 04 50 40 2d d0 47 e1 e9 2c *T...}...P@-.G.,*
00c17cf0: 05 6e 11 9b a4 a0 f6 aa b5 0a 82 49 55 08 9d b2 *.n.....IU...*
00c17d00: d6 d5 86 5f 45 90 57 1f cf 96 3e fb bf e2 22 65 *...E.W...>...e*
00c17d10: 6e ba 60 09 d0 40 be 06 22 1e ea b5 59 4a 8f e0 *n.`..@..".YJ..*
00c17d20: ae af 9b 3d 34 d8 22 92 94 02 11 00 03 69 30 82 *...=4.".....i0.*
00c17d30: 03 65 30 82 02 ce a0 03 02 01 02 02 01 00 30 0d *.e0.....0...*
00c17d40: 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30 81 84 *...*.H.....0...*
00c17d50: 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 *1.0...U...US1.0*
00c17d60: 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 *...U...New Jers*
00c17d70: 65 79 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 *eyl.0...U...New*
00c17d80: 20 50 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 * Providencel.0..*
00c17d90: 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 *.U...BW1.0...U.*
00c17da0: 0b 13 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 *...TESTIT1.0...U*
00c17db0: 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 *...root1.0...*. *
00c17dc0: 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 40 62 77 *H.....root@bw*
00c17dd0: 2e 63 6f 6d 30 1e 17 0d 30 32 30 34 31 36 31 36 *.com0...02041616*
00c17de0: 32 38 33 32 5a 17 0d 30 34 30 34 31 35 31 36 32 *2832Z..040415162*
00c17df0: 38 33 32 5a 30 81 84 31 0b 30 09 06 03 55 04 06 *832Z0..1.0...U..*
00c17e00: 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e *..US1.0...U...N*
00c17e10: 65 77 20 4a 65 72 73 65 79 31 17 30 15 06 03 55 *ew Jersey1.0...U*
00c17e20: 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 64 65 6e *....New Providen*

```

EAP: Received packet from client 192.168.123.7

```

00c18340: 01 00 00 06 02 05 00 06 * .....*
00c18350: 0d 00 *.....*

```

EAP: Forwarding packet to RADIUS server

```

00a1bfc0: 01 4b 00 9b ad 80 64 cc * .....K....d.*
00a1bfd0: be 43 d1 2b 77 53 5f 48 68 5d cc 3c 01 05 4b 45 *.C.+wS_Hh].<..KE*
00a1bfe0: 4e 04 06 c0 a8 7b 02 1e 0e 30 30 34 30 39 36 34 *N....{...0040964*
00a1bff0: 33 31 64 30 36 1f 0e 30 30 30 36 32 35 30 33 39 *31d06..000625039*
00alc000: 65 36 39 20 0e 41 50 33 34 30 2d 34 33 31 64 30 *e69 .AP340-431d0*
00alc010: 36 05 06 00 00 01 d0 0c 06 00 00 05 78 18 26 97 *6.....x.&.*
00alc020: ef 62 23 ce 6b ac b1 63 62 60 ea 71 f4 61 a2 3c *.b#.k..cb`.q.a.<.*
00alc030: bc 5e 5a d7 2b d0 1d e8 28 81 b4 1d 1a fe 7a 05 *.^Z.+...(...z.*
00alc040: 1b 93 db 3d 06 00 00 00 13 4f 08 02 05 00 06 0d *...=.....O.....*
00alc050: 00 50 12 b8 8e 4b 53 98 4b cc f9 f1 01 7f 8d 85 *.P...KS.K.....*
00alc060: 85 ef a6 *.....*

```

RADIUS: Received packet for client 192.168.123.7

```

00977000: 0b 4b 03 72 c3 5d 2d fa 38 31 a8 b2 3e e2 58 fe *.K.r.]-.81..>.X.*
00977010: b0 f1 12 d9 55 06 00 00 00 1e 1c 06 00 00 1c 20 *...U.....*
00977020: 1b 06 00 00 38 40 4f fe 01 06 03 0c 0d 80 00 00 *....8@0.....*

```

```

00977030: 07 02 63 65 31 0b 30 09 06 03 55 04 0a 13 02 42 *..cel.0...U...B*
00977040: 57 31 0f 30 0d 06 03 55 04 0b 13 06 54 45 53 54 *Wl.0...U...TEST*
00977050: 49 54 31 0d 30 0b 06 03 55 04 03 13 04 72 6f 6f *ITl.0...U...roo*
00977060: 74 31 1a 30 18 06 09 2a 86 48 86 f7 0d 01 09 01 *tl.0...*.H.....*
00977070: 16 0b 72 6f 6f 74 40 62 77 2e 63 6f 6d 30 81 9f *..root@bw.com0..*
00977080: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 *0...*.H.....*
00977090: 81 8d 00 30 81 89 02 81 81 00 cf 03 8d df 68 65 *...0.....he*
009770a0: 14 69 a7 9f 90 e4 01 c1 67 fe 06 4a 9f 81 b9 e5 *.i.....g...J...*
009770b0: 4e 75 17 67 5e 75 89 9f 83 99 b0 2f d9 36 4d c3 *Nu.g^u...../.6M.*
009770c0: fa 1b c3 eb 8b 79 72 6a ad 0f 2f 05 d5 8c 32 6d *....yrj../...2m*
009770d0: 46 8f 1e 68 19 24 f1 6d 02 c7 3e da 1f be 3f a5 *F..h.$m.>...?.*
009770e0: 9d 30 69 2d e8 d6 08 0b 81 1f 83 ca 8b 91 63 f5 *.0i-.....c.*
009770f0: 51 c0 4d 4d 46 d6 26 84 79 b9 c2 ce 71 33 b6 21 *Q.MMF.&y...q3!.*
00977100: 35 a5 0c 5c e3 de 1b 4c 50 cb 1d f0 83 d7 b0 1d *5..\...LP.....*
00977110: e5 40 b6 9b e9 42 21 80 b6 83 02 03 01 00 01 a3 *.@...B!.....*
00977120: 81 e4 30 81 4f fe e1 30 1d 06 03 55 1d 0e 04 16 *..0.0.0...U...*
00977130: 04 14 b0 7f e7 79 28 1b f9 10 fe 0c 14 b4 55 7e *....y(.....U~*
00977140: ff 93 aa 28 36 35 30 81 b1 06 03 55 1d 23 04 81 *... (650....U.#.*
00977150: a9 30 81 a6 80 14 b0 7f e7 79 28 1b f9 10 fe 0c *.0.....y(.....*
00977160: 14 b4 55 7e ff 93 aa 28 36 35 a1 81 8a a4 81 87 *.U~... (65.....*
00977170: 30 81 84 31 0b 30 09 06 03 55 04 06 13 02 55 53 *0..1.0...U...US*
00977180: 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a *1.0...U...New J*
00977190: 65 72 73 65 79 31 17 30 15 06 03 55 04 07 13 0e *erseyl.0...U...*
009771a0: 4e 65 77 20 50 72 6f 76 69 64 65 6e 63 65 31 0b *New Providence1.*
009771b0: 30 09 06 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 *0...U...BWl.0..*
009771c0: 03 55 04 0b 13 06 54 45 53 54 49 54 31 0d 30 0b *.U...TESTITl.0.*
009771d0: 06 03 55 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 *.U...rootl.0..*
009771e0: 09 2a 86 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 *.*.H.....root*
009771f0: 40 62 77 2e 63 6f 6d 82 01 00 30 0c 06 03 55 1d *@bw.com...0...U.*
00977200: 13 04 05 30 03 01 01 ff 30 0d 06 09 2a 86 48 86 *...0....0...*.H.*
00977210: f7 0d 01 01 04 05 00 03 81 81 00 c4 57 c3 31 a3 *.....W.1.*
00977220: a8 08 4f fe 4d 24 59 98 eb 76 85 cf df aa 42 4c *.O.M$Y.v...BL*
00977230: 34 fe 94 fa f9 56 c7 c4 b3 41 dc 9b 3d a9 f1 db *4...V...A...=...*
00977240: 40 93 97 35 e5 6b 31 49 b0 1d 6e 39 09 39 e2 99 *@..5.klI..n9.9..*
00977250: 4c ca eb b2 b3 54 15 f0 d6 91 ba 46 1b 2e 54 b2 *L...T.....F..T.*
00977260: 11 dd f5 1b 5a 44 1b 19 b0 ed 0f f8 5d 82 4d b9 *....ZD.....]M.*
00977270: 64 2d 4e f6 c4 ab fb 6a e6 8c e6 70 19 ab 39 b9 *d-N....j....p..9.*
00977280: a2 68 9e a1 24 56 73 c6 0c d2 9e 14 2e d5 6f 1a *.h..$Vs.....o.*
00977290: eb 3d 80 29 80 7a 71 e5 e6 73 81 df 23 16 03 01 *.=.)zq..s..#...*
009772a0: 00 96 0d 00 00 8e 02 01 02 00 89 00 87 30 81 84 *.....0...*
009772b0: 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 *1.0...U...USl.0*
009772c0: 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 *...U...New Jers*
009772d0: 65 79 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 *eyl.0...U...New*
009772e0: 20 50 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 * Providence1.0..*
009772f0: 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 *.U...BWl.0...U.*
00977300: 0b 13 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 *...TESTITl.0...U*
00977310: 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 *....rootl.0...*.
00977320: 4f 1a 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 40 *O.H.....root@*
00977330: 62 77 2e 63 6f 6d 0e 00 00 00 50 12 2d 30 0e c8 *bw.com....P.-0..*
00977340: 9d f5 5b 66 e2 b0 79 6e 9d 6b 95 06 18 26 2b 77 *..[f..yn.k...&+w*
00977350: 3d 12 66 57 f7 63 9e ac 84 89 9e c7 da f3 3c bc *=.fW.c.....<.*
00977360: 5e 5c f3 4e 6c 32 fe b9 27 8a 69 2c f0 df af 30 *^\.Nl2...'i,...0*
00977370: 5f d9 *_.....*

```

```

RADIUS: Received Challenge Request
RADIUS: Received session timeout request of 14400 seconds
RADIUS: Appending EAP attribute value of length 254
RADIUS: Appending EAP attribute value of length 254
RADIUS: Appending EAP attribute value of length 26
RADIUS: Sending EAPOL packet to client 192.168.123.7

```

```

00c18350: 01 00 03 0c 01 06 03 0c 0d 80 *.....*
00c18360: 00 00 07 02 63 65 31 0b 30 09 06 03 55 04 0a 13 *....cel.0...U...*
00c18370: 02 42 57 31 0f 30 0d 06 03 55 04 0b 13 06 54 45 *.BWl.0...U...TE*
00c18380: 53 54 49 54 31 0d 30 0b 06 03 55 04 03 13 04 72 *STITl.0...U...r*
00c18390: 6f 6f 74 31 1a 30 18 06 09 2a 86 48 86 f7 0d 01 *ootl.0...*.H...*
00c183a0: 09 01 16 0b 72 6f 6f 74 40 62 77 2e 63 6f 6d 30 *....root@bw.com0*

```

```

00c183b0: 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 *..0...*.H.....*
00c183c0: 00 03 81 8d 00 30 81 89 02 81 81 00 cf 03 8d df *.....0.....*
00c183d0: 68 65 14 69 a7 9f 90 e4 01 c1 67 fe 06 4a 9f 81 *he.i.....g...J..*
00c183e0: b9 e5 4e 75 17 67 5e 75 89 9f 83 99 b0 2f d9 36 *..Nu.g^u...../.6*
00c183f0: 4d c3 fa 1b c3 eb 8b 79 72 6a ad 0f 2f 05 d5 8c *M.....yrj../...*
00c18400: 32 6d 46 8f 1e 68 19 24 f1 6d 02 c7 3e da 1f be *2mF..h.$m..>...*
00c18410: 3f a5 9d 30 69 2d e8 d6 08 0b 81 1f 83 ca 8b 91 *?...0i-.....*
00c18420: 63 f5 51 c0 4d 4d 46 d6 26 84 79 b9 c2 ce 71 33 *c.Q.MMF.&y...q3*
00c18430: b6 21 35 a5 0c 5c e3 de 1b 4c 50 cb 1d f0 83 d7 *..!5...\...LP.....*
00c18440: b0 1d e5 40 b6 9b e9 42 21 80 b6 83 02 03 01 00 *...@...B!.....*
00c18450: 01 a3 81 e4 30 81 e1 30 1d 06 03 55 1d 0e 04 16 *....0..0...U....*
00c18460: 04 14 b0 7f e7 79 28 1b f9 10 fe 0c 14 b4 55 7e *....y(.....U~*
00c18470: ff 93 aa 28 36 35 30 81 b1 06 03 55 1d 23 04 81 *... (650).....U.#..*
00c18480: a9 30 81 a6 80 14 b0 7f e7 79 28 1b f9 10 fe 0c *.0.....y(.....*
00c18490: 14 b4 55 7e ff 93 aa 28 36 35 a1 81 8a a4 81 87 *.U~... (65).....*
00c184a0: 30 81 84 31 0b 30 09 06 03 55 04 06 13 02 55 53 *0..1.0...U....US*
00c184b0: 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a *1.0...U....New J*
00c184c0: 65 72 73 65 79 31 17 30 15 06 03 55 04 07 13 0e *ersey1.0...U....*
00c184d0: 4e 65 77 20 50 72 6f 76 69 64 65 6e 63 65 31 0b *New Providence1.*
00c184e0: 30 09 06 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 *0...U....BW1.0..*
00c184f0: 03 55 04 0b 13 06 54 45 53 54 49 54 31 0d 30 0b *.U....TESTIT1.0.*
00c18500: 06 03 55 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 *.U....root1.0..*
00c18510: 09 2a 86 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 *.*.H.....root*
00c18520: 40 62 77 2e 63 6f 6d 82 01 00 30 0c 06 03 55 1d *@bw.com...0...U.*
00c18530: 13 04 05 30 03 01 01 ff 30 0d 06 09 2a 86 48 86 *...0....0...*.H.*
00c18540: f7 0d 01 01 04 05 00 03 81 81 00 c4 57 c3 31 a3 *.....W.1.*
00c18550: a8 08 4d 24 59 98 eb 76 85 cf df aa 42 4c 34 fe *.M$Y.v....BL4.*
00c18560: 94 fa f9 56 c7 c4 b3 41 dc 9b 3d a9 f1 db 40 93 *...V...A...=@.*
00c18570: 97 35 e5 6b 31 49 b0 1d 6e 39 09 39 e2 99 4c ca *.5.klI..n9.9..L.*
00c18580: eb b2 b3 54 15 f0 d6 91 ba 46 1b 2e 54 b2 11 dd *...T.....F..T...*
00c18590: f5 1b 5a 44 1b 19 b0 ed 0f f8 5d 82 4d b9 64 2d *.ZD.....]M.d-*
00c185a0: 4e f6 c4 ab fb 6a e6 8c e6 70 19 ab 39 b9 a2 68 *N....j....p..9..h*
00c185b0: 9e a1 24 56 73 c6 0c d2 9e 14 2e d5 6f 1a eb 3d *..$Vs.....o...=*
00c185c0: 80 29 80 7a 71 e5 e6 73 81 df 23 16 03 01 00 96 *.) .zq...s.#.....*
00c185d0: 0d 00 00 8e 02 01 02 00 89 00 87 30 81 84 31 0b *.....0..1.*
00c185e0: 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 *0...U....US1.0..*
00c185f0: 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 *.U....New Jersey*
00c18600: 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 20 50 *1.0...U....New P*
00c18610: 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 03 55 *rovidencel.0...U*
00c18620: 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 0b 13 *....BW1.0...U...*
00c18630: 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 04 03 *.TESTIT1.0...U..*
00c18640: 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 48 86 *.root1.0...*.H.*
00c18650: f7 0d 01 09 01 16 0b 72 6f 6f 74 40 62 77 2e 63 *.....root@bw.c*
00c18660: 6f 6d 0e 00 00 00 *om.....*

```

EAP: Received packet from client 192.168.123.7

```

00c17a10: 01 00 03 ea 02 06 03 ea 0d 80 00 00 *.....*
00c17a20: 03 e0 16 03 01 03 b0 0b 00 02 a0 00 02 9d 00 02 *.....*
00c17a30: 9a 30 82 02 96 30 82 01 ff a0 03 02 01 02 02 01 *.0...0.....*
00c17a40: 01 30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 *.0...*.H.....*
00c17a50: 30 81 84 31 0b 30 09 06 03 55 04 06 13 02 55 53 *0..1.0...U....US*
00c17a60: 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a *1.0...U....New J*
00c17a70: 65 72 73 65 79 31 17 30 15 06 03 55 04 07 13 0e *ersey1.0...U....*
00c17a80: 4e 65 77 20 50 72 6f 76 69 64 65 6e 63 65 31 0b *New Providence1.*
00c17a90: 30 09 06 03 55 04 0a 13 02 42 57 31 0f 30 0d 06 *0...U....BW1.0..*
00c17aa0: 03 55 04 0b 13 06 54 45 53 54 49 54 31 0d 30 0b *.U....TESTIT1.0.*
00c17ab0: 06 03 55 04 03 13 04 72 6f 6f 74 31 1a 30 18 06 *.U....root1.0..*
00c17ac0: 09 2a 86 48 86 f7 0d 01 09 01 16 0b 72 6f 6f 74 *.*.H.....root*
00c17ad0: 40 62 77 2e 63 6f 6d 30 1e 17 0d 30 32 30 34 31 *@bw.com0...02041*
00c17ae0: 36 31 36 32 38 33 39 5a 17 0d 30 33 30 34 31 36 *6162839Z..030416*
00c17af0: 31 36 32 38 33 39 5a 30 81 83 31 0b 30 09 06 03 *162839Z0..1.0...*
00c17b00: 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 *U....US1.0...U..*
00c17b10: 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 17 30 15 *.New Jersey1.0.*
00c17b20: 06 03 55 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 *.U....New Provi*
00c17b30: 64 65 6e 63 65 31 0b 30 09 06 03 55 04 0a 13 02 *dencel.0...U....*
00c17b40: 42 57 31 0f 30 0d 06 03 55 04 0b 13 06 54 45 53 *BW1.0...U....TES*

```



```

00c17b50: 54 49 54 31 0c 30 0a 06 03 55 04 03 13 03 4b 45 *TIT1.0...U....KE*
00c17b60: 4e 31 1a 30 18 06 09 2a 86 48 86 f7 0d 01 09 01 *N1.0...*.H.....*
00c17b70: 16 0b 72 6f 6f 74 40 62 77 2e 63 6f 6d 30 81 9f *.root@bw.com0...*
00c17b80: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 00 03 *0...*.H.....*
00c17b90: 81 8d 00 30 81 89 02 81 81 00 9a 45 b1 53 23 4b *...0.....E.S#K*
00c17ba0: ea 7a 78 de 40 7a c4 fe 5e 68 fe 14 56 86 a8 77 *.zx.@z.^h..V.w*
00c17bb0: c6 59 c7 2b a0 85 0f 36 d7 cf b9 78 71 a2 68 5a *.Y.+...6...xq.hz*
00c17bc0: ed 41 84 fe e5 d5 aa 2c a5 88 4a 44 96 8b dc 79 *.A.....,..JD...y*
00c17bd0: 90 49 1a cf 52 0d fb a1 7c 12 c1 a8 ac e0 a8 7a *.I..R...|.....z*
00c17be0: 98 cd b5 7d 06 21 7d 7e 25 d1 dd 0e a9 f7 78 b4 *...}.!}~%.....x.*
00c17bf0: b7 20 da 88 cb 0f da 51 9e a6 81 4a 89 39 c0 68 *. ....Q...J.9.h*
00c17c00: 48 46 c9 f9 75 51 19 7f c2 80 eb 93 06 0e bb 78 *HF.uuQ.....x*
00c17c10: 75 18 8e 46 37 4e 0c ac ab 02 03 01 00 01 a3 *u..F77N.....*
00c17c20: 17 30 15 30 13 06 03 55 1d 25 04 0c 30 0a 06 08 *.0.0...U.%..0...*
00c17c30: 2b 06 01 05 05 07 03 02 30 0d 06 09 2a 86 48 86 **+.....0...*.H.*
00c17c40: f7 0d 01 01 04 05 00 03 81 81 00 2d 0e 42 a5 b2 *.....-..B...*
00c17c50: 19 1a b0 1b de 04 e0 98 ff 2d 66 6d 19 6b b1 19 *.....-fm.k...*
00c17c60: 6b 9e f0 ac ac a7 1d a2 3b 58 fa 75 93 69 bb d5 *k.....;X.u.i...*
00c17c70: 07 55 3f 15 d7 6e 2a c8 7b 68 6a 57 80 7e 75 29 *.U?.n*.{hjW.~u)*
00c17c80: 8e 97 39 ce 13 b7 25 7b 9e c9 dd a5 f6 49 6e 23 *.9...%{.....In#*
00c17c90: 0b 00 cb c8 9c 41 b1 81 5b cd bc dc 60 29 6e 6f *.....A.[...]no*
00c17ca0: 06 23 e7 68 eb 25 79 4c 5a 0b a4 16 8c 97 0f 80 *.#.h.%yLZ.....*
00c17cb0: 17 36 55 f8 94 50 98 dd 36 de 77 c4 b4 36 f6 95 *.6U..P..6.w..6..*
00c17cc0: e3 0e 79 36 2f 41 6b a4 ed 01 e9 10 00 00 82 00 *.y6/Ak.....*
00c17cd0: 80 cf 71 a3 ca 06 6a 7a 96 cd 33 36 a0 94 5c 6a *.q...jz..36..j*
00c17ce0: ba e4 2c ea d8 b6 fe c6 a6 c4 25 dc 45 df 81 e8 *.,.....%E...*
00c17cf0: 11 22 2c a2 3a 1b 46 ab ee df b5 a8 02 e8 10 d0 *",.:.F.....*
00c17d00: 21 a8 87 03 1d 9f 51 19 62 e3 70 d6 22 a7 f3 c3 *!.....Q.b.p"...*
00c17d10: f5 d9 36 2d 72 41 47 a2 d2 34 7f 72 3b 15 89 6b *.6-rAG..4.r;.k*
00c17d20: af 4c 10 26 5f 3a 72 cf 4f 86 0f 02 d7 9c 4d 8b *.L.&:r.O.....M.*
00c17d30: 90 bc 65 f1 d8 6d 22 a6 7b ef 0a a4 e9 b4 f0 52 *.e.e.m".{.....R*
00c17d40: 24 8a a7 8b 94 7b 1b 16 78 82 05 5c 99 6d 82 b5 *$.....{.x...\.m.*
00c17d50: 62 0f 00 80 82 00 80 35 8e 0c f0 c4 7b ca c8 40 *b.....5.....{.@*
00c17d60: ad bd c4 d5 c0 6f 0a 39 c8 61 61 fe 0e f3 e9 9e *.....o.9.aa.....*
00c17d70: 99 f8 57 0f 50 d6 8c 5f f6 5f 98 b2 38 d6 b7 9b *.W.P..._...8...*
00c17d80: 4e 0c 9f 6e 69 f6 a3 dc 22 ae c1 a4 4a 22 20 00 *N..ni..."..J" ..*
00c17d90: 62 a5 9a a7 c6 eb 99 66 a3 3b a2 a1 56 e2 2f 7c *b.....f;.V./|*
00c17da0: b5 9a d1 58 80 c6 bf 0d 60 9a d8 7f 53 f6 85 01 *.X.....S....*
00c17db0: 6d 08 ff 5f 29 62 6a 4d d1 19 f9 22 2a 98 ef 46 *m.._)bjM..."..F*
00c17dc0: 4f ec 5d 61 bf 97 c4 f0 19 01 61 3b 3c 34 93 d0 *O.]a.....a;<4..*
00c17dd0: 03 c9 c0 6c f3 30 0f 14 03 01 00 01 01 16 03 01 *...l.0.....*
00c17de0: 00 20 dd 31 b8 1f 4e 56 23 7a c2 dd 50 c3 9e 09 *. .1..NV#z..P...*
00c17df0: ca a2 5c 58 5d 80 7f 90 d5 59 c1 e3 41 de 28 df *...X]....Y..A.(*
00c17e00: bc 9c *.....*

```

EAP: Forwarding packet to RADIUS server

```

00977000: 01 4c 04 85 4c 20 a2 fa ec 49 bb b4 78 db ee 7a *.L..L ...I..x.zz*
00977010: ce c6 7d 60 01 05 4b 45 4e 04 06 c0 a8 7b 02 1e *..}`.KEN....{.*
00977020: 0e 30 30 34 30 39 36 34 33 31 64 30 36 1f 0e 30 *.004096431d06..0*
00977030: 30 30 36 32 35 30 33 39 65 36 39 20 0e 41 50 33 *00625039e69 .AP3*
00977040: 34 30 2d 34 33 31 64 30 36 05 06 00 00 1d 0c *.40-431d06.....*
00977050: 06 00 00 05 78 18 26 2b 77 3d 12 66 57 f7 63 9e *.x.&+w=.fW.c.*
00977060: ac 84 89 9e c7 da f3 3c bc 5e 5c f3 4e 6c 32 fe *.....<.\.N12.*
00977070: b9 27 8a 69 2c f0 df af 30 5f d9 3d 06 00 00 00 *.'i,...0_=.***
00977080: 13 4f ff 02 06 03 ea 0d 80 00 00 03 e0 16 03 01 *.O.....*
00977090: 03 b0 0b 00 02 a0 00 02 9d 00 02 9a 30 82 02 96 *.....0...*
009770a0: 30 82 01 ff a0 03 02 01 02 02 01 01 30 0d 06 09 *0.....0...*
009770b0: 2a 86 48 86 f7 0d 01 01 04 05 00 30 81 84 31 0b **H.....0..1.*
009770c0: 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 *0...U...US1.0...*
009770d0: 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 *.U...New Jersey*
009770e0: 31 17 30 15 06 03 55 04 07 13 0e 4e 65 77 20 50 *.1.0...U...New P*
009770f0: 72 6f 76 69 64 65 6e 63 65 31 0b 30 09 06 03 55 *rovidencel.0...U*
00977100: 04 0a 13 02 42 57 31 0f 30 0d 06 03 55 04 0b 13 *...BW1.0...U...*
00977110: 06 54 45 53 54 49 54 31 0d 30 0b 06 03 55 04 03 *.TESTIT1.0...U...*
00977120: 13 04 72 6f 6f 74 31 1a 30 18 06 09 2a 86 48 86 *.root1.0...*.H.*
00977130: f7 0d 01 09 01 16 0b 72 6f 6f 74 40 62 77 2e 63 *.....root@bw.c*

```

```

00977140: 6f 6d 30 1e 17 0d 30 32 30 34 31 36 31 36 32 38 *om0...0204161628*
00977150: 33 39 5a 17 0d 30 33 30 34 31 36 31 36 32 38 33 *39Z..03041616283*
00977160: 39 5a 30 81 83 31 0b 30 09 06 03 55 04 06 13 02 *9Z0..1.0...U...*
00977170: 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 *US1.0...U...New*
00977180: 4f ff 20 4a 65 72 73 65 79 31 17 30 15 06 03 55 *O. Jersey1.0...U*
00977190: 04 07 13 0e 4e 65 77 20 50 72 6f 76 69 64 65 6e *...New Providen*
009771a0: 63 65 31 0b 30 09 06 03 55 04 0a 13 02 42 57 31 *cel.0...U...BW1*
009771b0: 0f 30 0d 06 03 55 04 0b 13 06 54 45 53 54 49 54 *.0...U...TESTIT*
009771c0: 31 0c 30 0a 06 03 55 04 03 13 03 4b 45 4e 31 1a *1.0...U...KEN1.*
009771d0: 30 18 06 09 2a 86 48 86 f7 0d 01 09 01 16 0b 72 *0...*.H.....r*
009771e0: 6f 6f 74 40 62 77 2e 63 6f 6d 30 81 9f 30 0d 06 *oot@bw.com0..0.*
009771f0: 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d 00 *.*.H.....*
00977200: 30 81 89 02 81 81 00 9a 45 b1 53 23 4b ea 7a 78 *0.....E.S#K.zx*
00977210: de 40 7a c4 fe 5e 68 fe 14 56 86 a8 77 c6 59 c7 *.@z..^h..V..w..Y.*
00977220: 2b a0 85 0f 36 d7 cf b9 78 71 a2 68 5a ed 41 84 *+...6...xq.hZ.A.*
00977230: fe e5 d5 aa 2c a5 88 4a 44 96 8b dc 79 90 49 1a *.....,JD...y.I.*
00977240: cf 52 0d fb a1 7c 12 c1 a8 ac e0 a8 7a 98 cd b5 *.R...|.....z...*
00977250: 7d 06 21 7d 7e 25 d1 dd 0e a9 f7 78 b4 b7 20 da *}.!}~%.....x...*
00977260: 88 cb 0f da 51 9e a6 81 4a 89 39 c0 68 48 46 c9 *....Q...J.9.hHF.*
00977270: f9 75 51 19 7f c2 80 eb 93 06 0e bb 78 75 18 4f *.uQ.....xu.O*
00977280: ff 8e 46 37 37 4e 0c ac ab 02 03 01 00 01 a3 17 *.F77N.....*
00977290: 30 15 30 13 06 03 55 1d 25 04 0c 30 0a 06 08 2b *0.0...U.%..0...+*
009772a0: 06 01 05 05 07 03 02 30 0d 06 09 2a 86 48 86 f7 *......0...*.H..*
009772b0: 0d 01 01 04 05 00 03 81 81 00 2d 0e 42 a5 b2 19 *......-B...*
009772c0: 1a b0 1b de 04 e0 98 ff 2d 66 6d 19 6b b1 19 6b *......-fm.k.k*
009772d0: 9e f0 ac ac a7 1d a2 3b 58 fa 75 93 69 bb d5 07 *......;X.u.i...*
009772e0: 55 3f 15 d7 6e 2a c8 7b 68 6a 57 80 7e 75 29 8e *U?.n*.{hJW.~u}.*
009772f0: 97 39 ce 13 b7 25 7b 9e c9 dd a5 f6 49 6e 23 0b *.9...%{.....In#.*
00977300: 00 cb c8 9c 41 b1 81 5b cd bc dc 60 29 6e 6f 06 *....A..[...`no.*
00977310: 23 e7 68 eb 25 79 4c 5a 0b a4 16 8c 97 0f 80 17 *#.h.%yLZ.....*
00977320: 36 55 f8 94 50 98 dd 36 de 77 c4 b4 36 f6 95 e3 *6U..P..6.w..6...*
00977330: 0e 79 36 2f 41 6b a4 ed 01 e9 10 00 00 82 00 80 *.y6/Ak.....*
00977340: cf 71 a3 ca 06 6a 7a 96 cd 33 36 a0 94 5c 6a ba *.q...jz..36..`j.*
00977350: e4 2c ea d8 b6 fe c6 a6 c4 25 dc 45 df 81 e8 11 *.,.....%.E...*
00977360: 22 2c a2 3a 1b 46 ab ee df b5 a8 02 e8 10 d0 21 *",...F.....!*
00977370: a8 87 03 1d 9f 51 19 62 e3 70 d6 22 a7 f3 4f f5 *......Q.b.p."..O.*
00977380: c3 f5 d9 36 2d 72 41 47 a2 d2 34 7f 72 3b 15 89 *...6-rAG..4.r;.*
00977390: 6b af 4c 10 26 5f 3a 72 cf 4f 86 0f 02 d7 9c 4d *k.L.&:r.O.....M*
009773a0: 8b 90 bc 65 f1 d8 6d 22 a6 7b ef 0a a4 e9 b4 f0 *...e..m".{.....*
009773b0: 52 24 8a a7 8b 94 7b 1b 16 78 82 05 5c 99 6d 82 *R$....{.x...\.m.*
009773c0: b5 62 0f 00 00 82 00 80 35 8e 0c f0 c4 7b ca c8 *.b.....5....{..*
009773d0: 40 ad bd c4 d5 c0 6f 0a 39 c8 61 61 fe 0e f3 e9 *@.....o.9.aa...*
009773e0: 9e 99 f8 57 0f 50 d6 8c 5f f6 5f 98 b2 38 d6 b7 *...W.P.....8...*
009773f0: 9b 4e 0c 9f 6e 69 f6 a3 dc 22 ae c1 a4 4a 22 20 *.N..ni...".J" *
00977400: 00 62 a5 9a a7 c6 eb 99 66 a3 3b a2 a1 56 e2 2f *.b.....f.;..V./ *
00977410: 7c b5 9a d1 58 80 c6 bf 0d 60 9a d8 7f 53 f6 85 *|...X.....`S.S.*
00977420: 01 6d 08 ff 5f 29 62 6a 4d d1 19 f9 22 2a 98 ef *.m.._)bjM..."*
00977430: 46 4f ec 5d 61 bf 97 c4 f0 19 01 61 3b 3c 34 93 *FO.]a.....a;<4.*
00977440: d0 03 c9 c0 6c f3 30 0f 14 03 01 00 01 01 16 03 *....l.0.....*
00977450: 01 00 20 dd 31 b8 1f 4e 56 23 7a c2 dd 50 c3 9e *... .l.NV#z..P..*
00977460: 09 ca a2 5c 58 5d 80 7f 90 d5 59 c1 e3 41 de 28 *...X]....Y..A.( *
00977470: df bc 9c 50 12 d2 6d 6b 21 34 24 fd a4 35 24 96 *...P.mk!4$.5$. *
00977480: 97 96 a3 90 31 *....1.....*

```

RADIUS: Received packet for client 192.168.123.7

```

009767f0: 0b 4c 00 95 e1 85 70 8a * L....p.*
00976800: 9f 9b c4 19 fb 5e 86 55 ef 8a 20 9c 55 06 00 00 *.....^..U...U...*
00976810: 00 1e 1c 06 00 00 1c 20 1b 06 00 00 38 40 4f 37 *.....8@07*
00976820: 01 07 00 35 0d 80 00 00 00 2b 14 03 01 00 01 01 *...5.....+.....*
00976830: 16 03 01 00 20 c1 a4 8d 13 ea 2b a1 58 5e 07 50 *....+X^P*
00976840: 8f bc c2 c8 0a 76 90 e3 49 69 75 94 08 78 38 eb *...v..Iiu..x8.*
00976850: d9 19 77 c8 3f 50 12 5d ad 66 b3 d1 a0 2d 34 13 *.w.?P.]f...-4.*
00976860: ed b4 d3 ab f4 a9 59 18 26 6a dc bc 6a 53 19 18 *.....Y.&j..jS..*
00976870: 35 de 12 97 59 88 78 3c 5d 3c bc 5e 5e 2c 78 1a *5...Y.x<]<.^^.x.*
00976880: fa aa 6f b6 94 2a e8 22 5f 89 e7 88 68 *...o...*_...h...*

```

RADIUS: Received Challenge Request
RADIUS: Received session timeout request of 14400 seconds
RADIUS: Sending EAPOL packet to client 192.168.123.7

```
00c17a20:      01 00 00 35 01 07 00 35 0d 80 00 00 00 2b * ..5...5.....+*
00c17a30:  14 03 01 00 01 01 16 03 01 00 20 c1 a4 8d 13 ea *.....*
00c17a40:  2b a1 58 5e 07 50 8f bc c2 c8 0a 76 90 e3 49 69 *+.X^.P.....v..Ii*
00c17a50:  75 94 08 78 38 eb d9 19 77 c8 3f *u..x8...w.?.....*
```

EAP: Received packet from client 192.168.123.7

```
00c18340:      01 00 00 06 02 07 00 06 * .....*
00c18350:  0d 00 *.....*
```

EAP: Forwarding packet to RADIUS server

```
00albfc0:      01 4d 00 9b 48 88 47 fe * M..H.G.*
00albfd0:  1f b6 10 5f 8a 49 ae 7a e0 80 cf 94 01 05 4b 45 *..._.I.z.....KE*
00albfe0:  4e 04 06 c0 a8 7b 02 1e 0e 30 30 34 30 39 36 34 *N...{...0040964*
00albff0:  33 31 64 30 36 1f 0e 30 30 30 36 32 35 30 33 39 *31d06..000625039*
00alc000:  65 36 39 20 0e 41 50 33 34 30 2d 34 33 31 64 30 *e69 .AP340-431d0*
00alc010:  36 05 06 00 00 00 1d 0c 06 00 00 05 78 18 26 6a *6.....x.&j*
00alc020:  dc bc 6a 53 19 18 35 de 12 97 59 88 78 3c 5d 3c *..jS..5...Y.x<]<*
00alc030:  bc 5e 5e 2c 78 1a fa aa 6f b6 94 2a e8 22 5f 89 *.^,x...o..*."_*
00alc040:  e7 88 68 3d 06 00 00 00 13 4f 08 02 07 00 06 0d *..h=.....O.....*
00alc050:  00 50 12 7e 3d e7 17 19 9c 91 38 1f 3e 89 12 67 *..P.~=.....8.>..g*
00alc060:  21 39 0d *!9.....*
```

RADIUS: Received packet for client 192.168.123.7

```
00977000:  02 4d 00 3e a7 54 3e 0d 47 66 ee d9 3d 2f af cb *.M.>.T>.Gf..=/...*
00977010:  ea 88 58 0c 55 06 00 00 00 1e 1c 06 00 00 1c 20 *..X.U.....*
00977020:  1b 06 00 00 38 40 4f 06 03 08 00 04 50 12 ea 05 *....8@O.....P...*
00977030:  b6 ef b2 44 55 f7 4c ca d0 de 38 c5 12 b1 *...DU.L...8.....*
```

RADIUS: Received session timeout request of 14400 seconds
RADIUS: Sending EAPOL packet to client 192.168.123.7

```
00c18350:      01 00 00 04 03 08 00 04 * .....*
```

RADIUS: ACCEPT for 192.168.123.7

4 days, 20:52:20 (Info): Station 000625039e69, User "KEN" EAP-Authenticated

7. Ethereal log

This log was captured with Ethereal version 0.9.3, available at <http://www.ethereal.com>.

```
Frame 1 (161 on wire, 161 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.123.2 (192.168.123.2), Dst Addr: bw.tzo.com
(192.168.123.1)
User Datagram Protocol, Src Port: 4261 (4261), Dst Port: radius (1812)
Radius Protocol
  Code: Access Request (1)
  Packet identifier: 0x49 (73)
  Length: 119
  Authenticator
  Attribute value pairs
    t:User Name(1) l:5, Value:"KEN"
    t:NAS IP Address(4) l:6, Value:192.168.123.2
    t:Called Station Id(30) l:14, Value:"004096431d06"
    t:Calling Station Id(31) l:14, Value:"000625039e69"
    t:NAS identifier(32) l:14, Value:"AP340-431d06"
    t:NAS Port(5) l:6, Value:29
    t:Framed MTU(12) l:6, Value:1400
    t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11
    t:EAP-Message(79) l:10
      Extensible Authentication Protocol
        Code: Response (2)
        Id: 3
        Length: 8
        Type: Identity [RFC2284] (1)
        Identity (3 bytes): KEN
    t:Message Authenticator(80) l:18,
Value:"\224X\154uI\186\015\132"\2370\014N\024H"

Frame 2 (144 on wire, 144 captured)
Ethernet II
Internet Protocol, Src Addr: bw.tzo.com (192.168.123.1), Dst Addr: 192.168.123.2
(192.168.123.2)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 4261 (4261)
Radius Protocol
  Code: Access challenge (11)
  Packet identifier: 0x49 (73)
  Length: 102
  Authenticator
  Attribute value pairs
    t:Unknown Type(85) l:6, Unknown Value Type
    t:Idle Timeout(28) l:6, Value:7200
    t:Session Timeout(27) l:6, Value:14400
    t:EAP-Message(79) l:8
      Extensible Authentication Protocol
        Code: Request (1)
        Id: 4
        Length: 6
        Type: EAP-TLS [RFC2716] [Aboba] (13)
        Flags(0x20): Start
    t:Message Authenticator(80) l:18,
Value:"\148\188Q\020\219\168\168.\241\218\224\240\151\217:g"
    t:State(24) l:38,
Value:"5\006\210N\154\193\160\207\231m\144\196\173`n<\188^Z1\183K\2525=\143\164\183\2
20\194\252\185\1378\019"

Frame 3 (271 on wire, 271 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.123.2 (192.168.123.2), Dst Addr: bw.tzo.com
(192.168.123.1)
User Datagram Protocol, Src Port: 4262 (4262), Dst Port: radius (1812)
Radius Protocol
```

```
Code: Access Request (1)
Packet identifier: 0x4a (74)
Length: 229
Authenticator
Attribute value pairs
  t:User Name(1) 1:5, Value:"KEN"
  t:NAS IP Address(4) 1:6, Value:192.168.123.2
  t:Called Station Id(30) 1:14, Value:"004096431d06"
  t:Calling Station Id(31) 1:14, Value:"000625039e69"
  t:NAS identifier(32) 1:14, Value:"AP340-431d06"
  t:NAS Port(5) 1:6, Value:29
  t:Framed MTU(12) 1:6, Value:1400
  t:State(24) 1:38,
Value:"5\006\210N\154\193\160\207\231m\144\196\173`n<\188^z1\183K\2525=\143\164\183\2
20\194\252\185\1378\019"
  t:NAS Port Type(61) 1:6, Value:Wireless IEEE 802.11
  t:EAP-Message(79) 1:82
    Extensible Authentication Protocol
      Code: Response (2)
      Id: 4
      Length: 80
      Type: EAP-TLS [RFC2716] [Aboba] (13)
      Flags(0x80): Length
      Length: 70
      Secure Socket Layer
  t:Message Authenticator(80) 1:18,
Value:"G\171\248\202\187dhY\2238AQ\131\173\182\002"
```

```
Frame 4 (1180 on wire, 1180 captured)
Ethernet II
Internet Protocol, Src Addr: bw.tzo.com (192.168.123.1), Dst Addr: 192.168.123.2
(192.168.123.2)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 4262 (4262)
Radius Protocol
```

```
Code: Access challenge (11)
Packet identifier: 0x4a (74)
Length: 1138
Authenticator
Attribute value pairs
  t:Unknown Type(85) 1:6, Unknown Value Type
  t:Idle Timeout(28) 1:6, Value:7200
  t:Session Timeout(27) 1:6, Value:14400
  t:EAP-Message(79) 1:254
    EAP fragment
  t:EAP-Message(79) 1:254
    EAP fragment
  t:EAP-Message(79) 1:254
    EAP fragment
  t:EAP-Message(79) 1:254
    EAP fragment
  t:EAP-Message(79) 1:28
    EAP fragment
    Extensible Authentication Protocol
      Code: Request (1)
      Id: 5
      Length: 1034
      Type: EAP-TLS [RFC2716] [Aboba] (13)
      Flags(0xC0): Length More
      Length: 1794
      EAP-TLS Fragments
      Secure Socket Layer
  t:Message Authenticator(80) 1:18,
Value:"Ls\184\204\165'\195e\151\216g\132\185Jn\191"
  t:State(24) 1:38,
Value:"\151\239b#\206k\172\177cb`\234q\244a\162<\188^z\215+\208\029\232(\129\180\029\0
26\254z\005\027\147\219"
```

```
Frame 5 (197 on wire, 197 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.123.2 (192.168.123.2), Dst Addr: bw.tzo.com
(192.168.123.1)
User Datagram Protocol, Src Port: 4263 (4263), Dst Port: radius (1812)
Radius Protocol
  Code: Access Request (1)
  Packet identifier: 0x4b (75)
  Length: 155
  Authenticator
  Attribute value pairs
    t:User Name(1) 1:5, Value:"KEN"
    t:NAS IP Address(4) 1:6, Value:192.168.123.2
    t:Called Station Id(30) 1:14, Value:"004096431d06"
    t:Calling Station Id(31) 1:14, Value:"000625039e69"
    t:NAS identifier(32) 1:14, Value:"AP340-431d06"
    t:NAS Port(5) 1:6, Value:29
    t:Framed MTU(12) 1:6, Value:1400
    t:State(24) 1:38,
Value:"\151\239b#\206k\172\177cb`\234q\244a\162<\188^Z\215+\208\029\232(\129\180\029\0
26\254z\005\027\147\219"
    t:NAS Port Type(61) 1:6, Value:Wireless IEEE 802.11
    t:EAP-Message(79) 1:8
      Extensible Authentication Protocol
        Code: Response (2)
        Id: 5
        Length: 6
        Type: EAP-TLS [RFC2716] [Aboba] (13)
        Flags(0x0):
    t:Message Authenticator(80) 1:18,
Value:"\184\142KS\152K\204\249\241\001\127\141\133\133\239\166"
```

```
Frame 6 (924 on wire, 924 captured)
Ethernet II
Internet Protocol, Src Addr: bw.tzo.com (192.168.123.1), Dst Addr: 192.168.123.2
(192.168.123.2)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 4263 (4263)
Radius Protocol
  Code: Access challenge (11)
  Packet identifier: 0x4b (75)
  Length: 882
  Authenticator
  Attribute value pairs
    t:Unknown Type(85) 1:6, Unknown Value Type
    t:Idle Timeout(28) 1:6, Value:7200
    t:Session Timeout(27) 1:6, Value:14400
    t:EAP-Message(79) 1:254
      EAP fragment
    t:EAP-Message(79) 1:254
      EAP fragment
    t:EAP-Message(79) 1:254
      EAP fragment
    t:EAP-Message(79) 1:26
      EAP fragment
    Extensible Authentication Protocol
      Code: Request (1)
      Id: 6
      Length: 780
      Type: EAP-TLS [RFC2716] [Aboba] (13)
      Flags(0x80): Length
      Length: 1794
      EAP-TLS Fragments
      Secure Socket Layer
    t:Message Authenticator(80) 1:18, Value:"-
0\014\200\157\245[f\226\176yn\157k\149\006"
```

t:State(24) 1:38,
Value:"+w=\018fW\247c\158\172\132\137\158\199\218\243<\188^\243N12\254\185'\138i,\240
\223\1750_\217"

Frame 7 (1199 on wire, 1199 captured)

Ethernet II

Internet Protocol, Src Addr: 192.168.123.2 (192.168.123.2), Dst Addr: bw.tzo.com
(192.168.123.1)

User Datagram Protocol, Src Port: 4264 (4264), Dst Port: radius (1812)

Radius Protocol

Code: Access Request (1)

Packet identifier: 0x4c (76)

Length: 1157

Authenticator

Attribute value pairs

t:User Name(1) 1:5, Value:"KEN"

t:NAS IP Address(4) 1:6, Value:192.168.123.2

t:Called Station Id(30) 1:14, Value:"004096431d06"

t:Calling Station Id(31) 1:14, Value:"000625039e69"

t:NAS identifier(32) 1:14, Value:"AP340-431d06"

t:NAS Port(5) 1:6, Value:29

t:Framed MTU(12) 1:6, Value:1400

t:State(24) 1:38,

Value:"+w=\018fW\247c\158\172\132\137\158\199\218\243<\188^\243N12\254\185'\138i,\240
\223\1750_\217"

t:NAS Port Type(61) 1:6, Value:Wireless IEEE 802.11

t:EAP-Message(79) 1:255

EAP fragment

t:EAP-Message(79) 1:255

EAP fragment

t:EAP-Message(79) 1:255

EAP fragment

t:EAP-Message(79) 1:245

EAP fragment

Extensible Authentication Protocol

Code: Response (2)

Id: 6

Length: 1002

Type: EAP-TLS [RFC2716] [Aboba] (13)

Flags(0x80): Length

Length: 992

Secure Socket Layer

t:Message Authenticator(80) 1:18,

Value:"\210mk!4\$\253\1645\$\150\151\150\163\1441"

Frame 8 (191 on wire, 191 captured)

Ethernet II

Internet Protocol, Src Addr: bw.tzo.com (192.168.123.1), Dst Addr: 192.168.123.2
(192.168.123.2)

User Datagram Protocol, Src Port: radius (1812), Dst Port: 4264 (4264)

Radius Protocol

Code: Access challenge (11)

Packet identifier: 0x4c (76)

Length: 149

Authenticator

Attribute value pairs

t:Unknown Type(85) 1:6, Unknown Value Type

t:Idle Timeout(28) 1:6, Value:7200

t:Session Timeout(27) 1:6, Value:14400

t:EAP-Message(79) 1:55

Extensible Authentication Protocol

Code: Request (1)

Id: 7

Length: 53

Type: EAP-TLS [RFC2716] [Aboba] (13)

Flags(0x80): Length

Length: 43

Secure Socket Layer
t:Message Authenticator(80) l:18, Value:"]\173f\179\209\160-4\019\237\180\211\171\244\169Y"
t:State(24) l:38,
Value:"j\220\188js\025\0245\222\018\151Y\136x<]\188^^,x\026\250\170o\182\148*\232"_\137\231\136h"

Frame 9 (197 on wire, 197 captured)

Ethernet II

Internet Protocol, Src Addr: 192.168.123.2 (192.168.123.2), Dst Addr: bw.tzo.com (192.168.123.1)

User Datagram Protocol, Src Port: 4265 (4265), Dst Port: radius (1812)

Radius Protocol

Code: Access Request (1)

Packet identifier: 0x4d (77)

Length: 155

Authenticator

Attribute value pairs

t:User Name(1) l:5, Value:"KEN"

t:NAS IP Address(4) l:6, Value:192.168.123.2

t:Called Station Id(30) l:14, Value:"004096431d06"

t:Calling Station Id(31) l:14, Value:"000625039e69"

t:NAS identifier(32) l:14, Value:"AP340-431d06"

t:NAS Port(5) l:6, Value:29

t:Framed MTU(12) l:6, Value:1400

t:State(24) l:38,

Value:"j\220\188js\025\0245\222\018\151Y\136x<]\188^^,x\026\250\170o\182\148*\232"_\137\231\136h"

t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11

t:EAP-Message(79) l:8

Extensible Authentication Protocol

Code: Response (2)

Id: 7

Length: 6

Type: EAP-TLS [RFC2716] [Aboba] (13)

Flags(0x0):

t:Message Authenticator(80) l:18,

Value:"~=\231\023\025\156\1458\031>\137\018g!9\013"

Frame 10 (104 on wire, 104 captured)

Ethernet II

Internet Protocol, Src Addr: bw.tzo.com (192.168.123.1), Dst Addr: 192.168.123.2 (192.168.123.2)

User Datagram Protocol, Src Port: radius (1812), Dst Port: 4265 (4265)

Radius Protocol

Code: Access Accept (2)

Packet identifier: 0x4d (77)

Length: 62

Authenticator

Attribute value pairs

t:Unknown Type(85) l:6, Unknown Value Type

t:Idle Timeout(28) l:6, Value:7200

t:Session Timeout(27) l:6, Value:14400

t:EAP-Message(79) l:6

Extensible Authentication Protocol

Code: Success (3)

Id: 8

Length: 4

t:Message Authenticator(80) l:18,

Value:"\234\005\182\239\178DU\247L\202\208\2228\197\018\177"

8. RFC2716 Reference Message Flow

This is extracted from RFC2716 [3] and shows the EAP/TLS message flow in a nice concise format:

In the case where the EAP-TLS mutual authentication is successful, and fragmentation is required, the conversation will appear as follows:

```
Authenticating Peer      Authenticator
-----
PPP LCP ACK-EAP
auth ->                  <- PPP LCP Request-EAP
                           auth

PPP EAP-Response/
Identity (MyID) ->      <- PPP EAP-Request/
                           Identity

PPP EAP-Response/
EAP-Type=EAP-TLS
(TLS client_hello)->   <- PPP EAP-Request/
                           EAP-Type=EAP-TLS
                           (TLS Start, S bit set)

PPP EAP-Response/
EAP-Type=EAP-TLS
(TLS client_hello)->   <- PPP EAP-Request/
                           EAP-Type=EAP-TLS
                           (TLS server_hello,
                           TLS certificate,
                           [TLS server_key_exchange,]
                           [TLS certificate_request,]
                           TLS server_hello_done)
                           (Fragment 1: L, M bits set)

PPP EAP-Response/
EAP-Type=EAP-TLS ->    <- PPP EAP-Request/
                           EAP-Type=EAP-TLS
                           (Fragment 2: M bit set)

PPP EAP-Response/
EAP-Type=EAP-TLS ->    <- PPP EAP-Request/
                           EAP-Type=EAP-TLS
                           (Fragment 3)

PPP EAP-Response/
EAP-Type=EAP-TLS
(TLS certificate,
 TLS client_key_exchange,
 [TLS certificate_verify,]
 TLS change_cipher_spec,
 TLS inished) (Fragment 1:
 L, M bits set)->     <- PPP EAP-Request/
                           EAP-Type=EAP-TLS

PPP EAP-Response/
EAP-Type=EAP-TLS
(Fragment 2)->        <- PPP EAP-Request/
                           EAP-Type=EAP-TLS
                           (TLS change_cipher_spec,
                           TLS finished)

PPP EAP-Response/
EAP-Type=EAP-TLS ->   <- PPP EAP-Success

PPP Authentication
Phase complete,
NCP Phase starts

ECP negotiation
CCP negotiation
```

9. OpenSSL certificate generation script

```
#!/bin/ksh
SSL=/usr/local/openssl

export PATH=${SSL}/bin/:${SSL}/ssl/misc:${PATH}
export LD_LIBRARY_PATH=${SSL}/lib

# needed if you need to start from scratch otherwise the CA.pl -newca command doesn't copy the
new
# private key into the CA directories
rm -rf demoCA

echo "*****"
echo "Creating self-signed private key and certificate"
echo "When prompted override the default value for the Common Name field"
echo "*****"
echo

# Generate a new self-signed certificate.
# After invocation, newreq.pem will contain a private key and certificate
# newreq.pem will be used in the next step
openssl req -new -x509 -keyout newreq.pem -out newreq.pem -days 730 \
    -passin pass:whatever -passout pass:whatever

echo "*****"
echo "Creating a new CA hierarchy (used later by the \"ca\" command) with the certificate"
echo "and private key created in the last step"
echo "*****"
echo

echo "newreq.pem" | CA.pl -newca >/dev/null

echo "*****"
echo "Creating ROOT CA"
echo "*****"
echo

# Create a PKCS#12 file, using the previously created CA certificate/key
# The certificate in demoCA/cacert.pem is the same as in newreq.pem. Instead of
# using "-in demoCA/cacert.pem" we could have used "-in newreq.pem" and then omitted
# the "-inkey newreq.pem" because newreq.pem contains both the private key and certificate
openssl pkcs12 -export -in demoCA/cacert.pem -inkey newreq.pem -out root.p12 -cacerts \
    -passin pass:whatever -passout pass:whatever

# parse the PKCS#12 file just created and produce a PEM format certificate and key in root.pem
openssl pkcs12 -in root.p12 -out root.pem -passin pass:whatever -passout pass:whatever

# Convert root certificate from PEM format to DER format
openssl x509 -inform PEM -outform DER -in root.pem -out root.der

echo "*****"
echo "Creating client private key and certificate"
echo "When prompted enter the client name in the Common Name field. This is the same"
echo " used as the Username in FreeRADIUS"
echo "*****"
echo

# Request a new PKCS#10 certificate.
# First, newreq.pem will be overwritten with the new certificate request
openssl req -new -keyout newreq.pem -out newreq.pem -days 730 \
    -passin pass:whatever -passout pass:whatever

# Sign the certificate request. The policy is defined in the openssl.cnf file.
# The request generated in the previous step is specified with the -infile option and
# the output is in newcert.pem
# The -extensions option is necessary to add the OID for the extended key for client
authentication
openssl ca -policy policy_anything -out newcert.pem -passin pass:whatever \
    -key whatever -extensions xpclient_ext -extfile xpeextensions \
    -infile newreq.pem

# Create a PKCS#12 file from the new certificate and its private key found in newreq.pem
# and place in file cert-clt.p12
```

```
openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out cert-clt.p12 -clcerts \  
-passin pass:whatever -passout pass:whatever  
  
# parse the PKCS#12 file just created and produce a PEM format certificate and key in cert-  
clt.pem  
openssl pkcs12 -in cert-clt.p12 -out cert-clt.pem -passin pass:whatever -passout pass:whatever  
  
# Convert certificate from PEM format to DER format  
openssl x509 -inform PEM -outform DER -in cert-clt.pem -out cert-clt.der  
  
echo "*****"  
echo "Creating server private key and certificate"  
echo "When prompted enter the server name in the Common Name field."  
echo "*****"  
echo  
  
# Request a new PKCS#10 certificate.  
# First, newreq.pem will be overwritten with the new certificate request  
openssl req -new -keyout newreq.pem -out newreq.pem -days 730 \  
-passin pass:whatever -passout pass:whatever  
  
# Sign the certificate request. The policy is defined in the openssl.cnf file.  
# The request generated in the previous step is specified with the -infile option and  
# the output is in newcert.pem  
# The -extensions option is necessary to add the OID for the extended key for server  
authentication  
openssl ca -policy policy_anything -out newcert.pem -passin pass:whatever -key whatever \  
-extensions xpserver_ext -extfile xextensions -infile newreq.pem  
  
# Create a PKCS#12 file from the new certificate and its private key found in newreq.pem  
# and place in file cert-srv.p12  
openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out cert-srv.p12 -clcerts \  
-passin pass:whatever -passout pass:whatever  
  
# parse the PKCS#12 file just created and produce a PEM format certificate and key in cert-  
srv.pem  
openssl pkcs12 -in cert-srv.p12 -out cert-srv.pem -passin pass:whatever -passout pass:whatever  
  
# Convert certificate from PEM format to DER format  
openssl x509 -inform PEM -outform DER -in cert-srv.pem -out cert-srv.der  
  
#clean up  
rm newcert.pem newreq.pem
```

10. OpenSSL extensions file

```
[ xpclient_ext]  
extendedKeyUsage = 1.3.6.1.5.5.7.3.2  
  
[ xpserver_ext ]  
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

11. References

- [1] Adam Sulmicki, *HOWTO on EAP/TLS authentication between FreeRADIUS and Xsupplicant*, <http://www.missl.cs.umd.edu/wireless/eaptls/>, April 2002
- [2] Joseph Davies, Microsoft Corporation, *Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000 Internet Authentication Service*, <http://www.microsoft.com/WindowsXP/pro/techinfo/deployment/wireless/80211corp.doc>, March 2002
- [3] B. Aboba, D. Simon, Microsoft, *RFC 2716: PPP EAP TLS Authentication Protocol*, October 1999
- [4] Cisco Systems, *Cisco Aironet Access Point Software Configuration Guide- Diagnostics and Troubleshooting*, http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accspts/ap350scg/ap350ch9.htm

