5 Wireless Authentication

Ref: http://www.asecuritysite.com/wireless/wireless05

5.1 Introduction

The key elements of security are confidentially, integrity and assurance (CIA), where the sensitive data must be kept securely using encryption. A key factor though is the ownership and the access rights of the data. Thus some form of authentication must be applied to make sure that the users and/or devices that are accessing the data have the correct rights. Authentication is thus important from many aspects, as it can be used to identify users and devices. Normally this authentication is used to grant access for the user and/or the device to the wireless network. The first generation of wireless networks tended not to use authentication, and tended to use the MAC address of the device to authenticate. Unfortunately this method is open of MAC and IP address spoofing, where valid MAC and IP addresses are used to connect to the wireless network. Along with this an authentication scheme based purely on the device does not properly authenticate the user, thus many authentication schemes have some form of user identification and verification. The main methods used for verification include:

- **Network/physical addresses**. These are simple method of verifying a device. The network address, such as the IP address can be easily spoofed, but the physical address is less easy and is a more secure implementation. Unfortunately the physical address can also be spoofed, either through software modifications of the wireless data frame, or by reprogramming the network interface card. Methods include DHCP.
- **Username and password**. The use is usernames and passwords are well known but are open to security breaches, especially from dictionary attacks on passwords, and from social engineering attacks. Methods include PEAP, EAP-FAST and EAP-SRP.
- **Authentication certificate**. This certificate verifies a user or a device by providing a digital certificate which can be verified by a reputable source. Methods include EAP-TLS.
- **Tokens/Smart cards**. With this method a user can only gain access to the system after they have inserted their personal smart card into the computer and then entered their PIN code. Methods include RSA SecurID Token Card and Smartcard EAP.
- **Pre-shared keys**. This uses a pre-defined secret key. Methods include EAP-Archie.
- **Biometrics**. This is a better method than a smart card where a physical feature of the user is scanned. The scanned parameter requires to be unchanging, such as fingerprints or retina images.

Normally the level of security applied depends on the security requirements. In a highly secure network, smart cards and biometrics are likely to be used to authenticate users, while in a less secure network, usernames and passwords may be sufficient.

5.2 802.11 frame format

The 802.11 frame format includes a 12-byte preamble (10101 … 1010 0000 1100 1011 1101), followed by a PLCP header (which contains information used by the physical layer) and then by the MAC data frame (Figure 1).

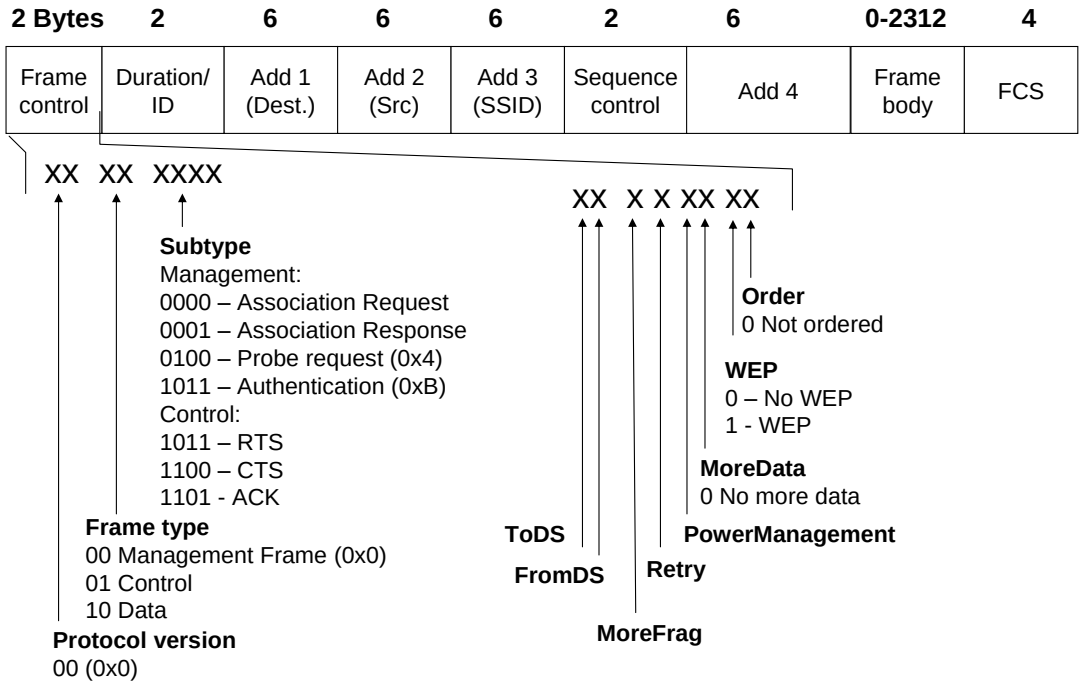

Figure 1 IEEE 802.11 frame format

There are three types of data frames (defined in the frame type bits);

- **Management frame**. Used for management purposes, such as associating with the access point, and in authentication.
- **Control frame**. Used for control purposes, such as using RTS, CTS and ACK.
- **Data frame.** Used to transmit data.

The types of management frames are:

0000 Association Request
0001 Association Response
0010 Reassociation Request
0011 Reassociation Response
0100 Probe Request
0101 Probe Response
1000 Beacon
1010 Disassociation
1011 Authentication
1100 Deauthentication

For a control frame:

1011 RTS

1100 CTS
1101 ACK

A DS (Distributed System) defines whether the data frame is forwarded. If it is not to be forwarded the **ToDS** and **FromDS** bits are set to zero. The **MoreFrag** bit defines whether the data frame has been fragmented, and the **Retry** bit is set when the same data frame has already been sent. A client can define that it has power management by setting the **PowerManagement** bit. The **MoreData** bit is used by an access point to define that there are more data frames that have been buffered for a client. If the **Order** bit is set it defines that the data frames are ordered, while the **WEP** bit defines if WEP is used, or not. The main phases of the connection between a station client and a wireless access point is **probe request**, **authentication**, and **association**.

5.3.1 Probe request

When a client station starts sends out a probe request on each channel for a specified SSID. All the access points which match the SSID respond with a probe response. If it does not know the name of the SSID it will use the BROADCAST address (FF FF FF FF FF FF). As it will not know the MAC address of the access point it sends out a BROADCAST address (FF FF FF FF FF FF) for the destination address.

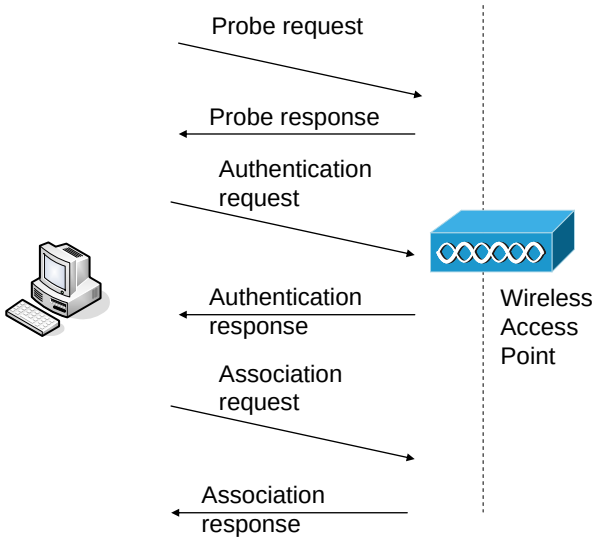

Figure 2 Station operations

5.3.2 Authentication phase

The authentication method used typically depends on the application, and the range of devices currently available. Figure 3 shows some of these methods for a client. The authentication phase either uses:

- **Open authentication**. In this type the station client is always accepted. The open authentication is typically used where it does not matter whether the devices are to be authenticated or where there are devices which cannot support complex authentication, such as in hand-held devices. If open authentication is used, any device can gain access to the network.

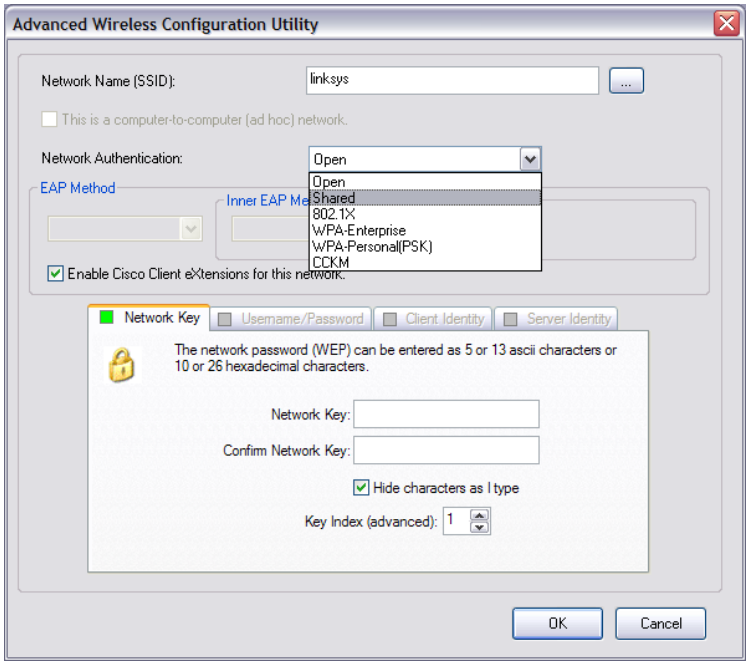

Figure 3 Authentication methods

- **Based on WEP**. If WEP is used, the WEP key can be used to authenticate the client to the access point. If it does not have the correct WEP key it will not be allowed access to the network.
- **Shared-key**. With this method, the access point and the client have the same shared key. The access point then sends an authentication response which has a challenge text. The client then encrypts the challenges with the shared WEP key, and sends it back to the access point. If it has been correctly encrypted, the access point sends back an authentication response (success), as illustrated in Figure 4. The major problem with shared-key authentication is that it is venerable to a Man-in-the-middle attack, where an intruder can capture both the plain-text challenge and the cipertext, and XOR them together to generate the key stream, as illustrated in Figure 5. With the data stream, the man-in-the-middle does not need the shared-key as they can send a message which is XOR'ed with the random key.
- **802.1x**. This method implements a whole range of authentication methods, such as TLS, LEAP, EAP-FAST, and so on.
- **MAC address-based**. This is not a standard method used in 802.11, but is implemented by many vendors. Initially, as illustrated in Figure 6, the station client sends an association request to the access point, which then sends the MAC address to the RADIUS server, which then checks the devices in its database. If it is successful, it sends a RADIUS-ACCEPT message to the access point, after which the access point will send an associated response (Success) message to the station client. The MAC address-based method can be defeated with a network interface card which can be set to a MAC address which is valid on the network.

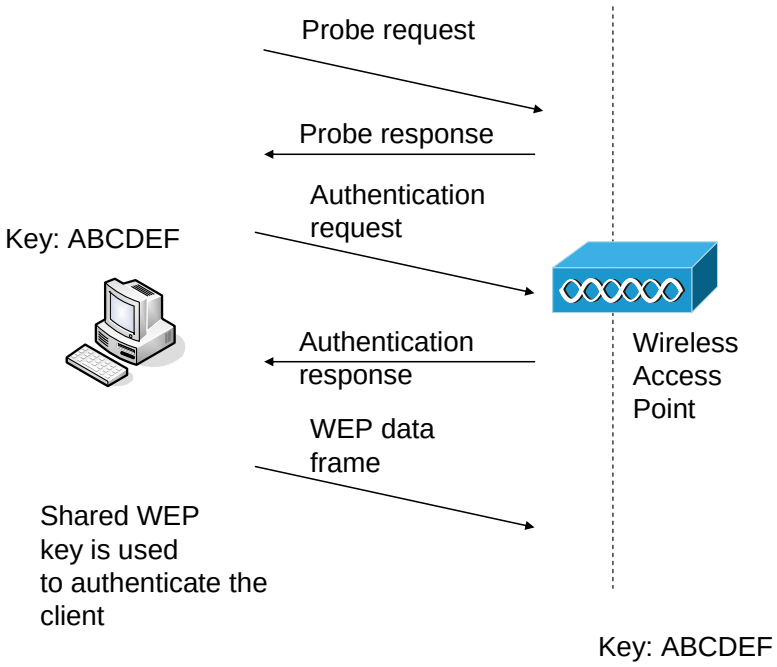

Figure 4 Shared-key authentication

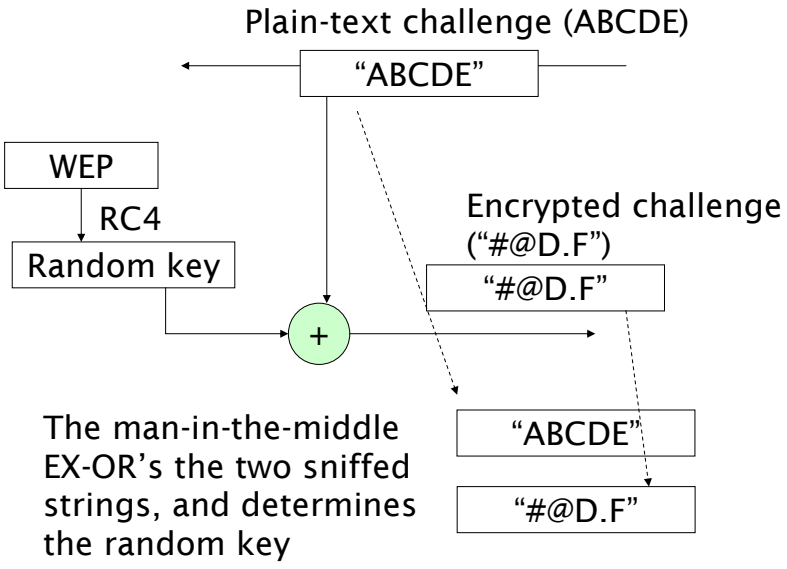

Figure 5 Man-in-the-middle attack

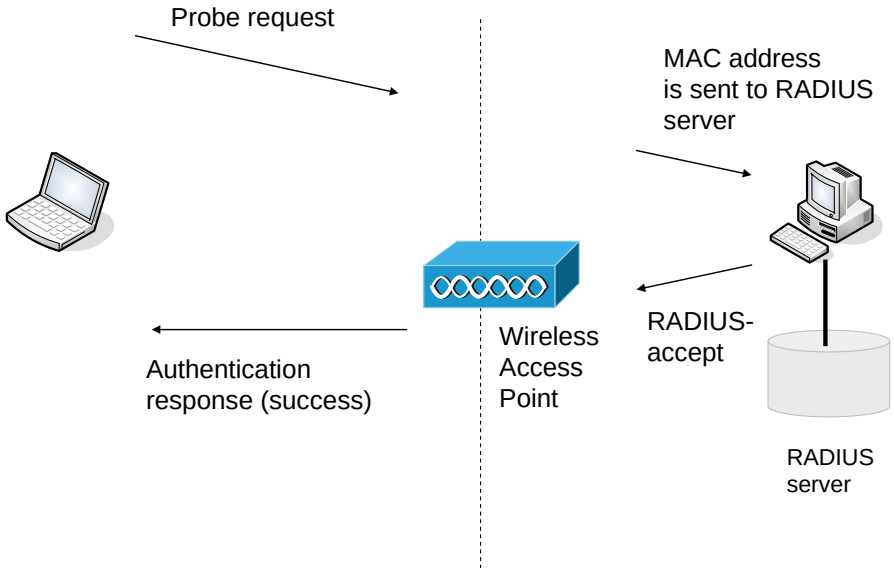

Figure 6 MAC address-based authentication

5.3 Authentication techniques

It has been seen that standard 802.11 authentication methods can be easily overcome. There are several standard authentication methods, some of which have been developed by vendors, such as Cisco Systems, while others are international standards. Basically authentication consists of an authentication framework, an authentication algorithm and an encryption technique. The proposed authentication tries to split these up with:

- **801.1x authentication**. This defines the authentication framework which can support many authentication types. Ethernet network have developed so that it is now the standard method of connecting to a wired network. The IEEE 802.1X standard aims to extend Ethernet onto wireless networks and dialup connections. It uses a port authentication method that could be used on a range of networks, including 802.3 (Ethernet), 802.11 (wireless) and PPP (serial connections). IEEE 802.1X thus defines authentication and key management, while 802.11i defines extended security. At the present the WiFi Alliance (WFA) has drafted the 802.11 security specification, which is now known as Wi-fi Protected Access (WPA).
- **EAP** (Extensible Authentication Protocol). This defines the actual implementation of the authentication method. It thus provides centralized authentication and dynamic key distribution. It has been developed by the IEEE 802.11i Task Group as an end-to-end framework and uses 802.1X. It uses:
    - **Authentication**. This is of both the client and the authentication server (such as a RADIUS server).
    - **Encryption keys**. These are dynamically created after authentication. They are not common to the whole network.
    - **Centralized policy control**. A session time-out generates a reauthentication and the generation of new encryption keys.
- **Encryption**. This replaces WEP with TKIP (Temporal Key Integrity Protocol), which is based on WEP but which overcomes its major weaknesses.

Figure 7 shows that the 802.1X framework provides an interface between many different network types a number of differing authentication methods (such as LEAP, EAP-TLS, and so on). The 802.1X method uses three main entities:

- **Supplicant**. This operates on the station client.
- **Authenticator**. This operates on the access point.
- **Authenticator server**. This operates on a RADIUS server.

Figure 8 shows the basic message flow for 802.1X authentication, where the supplicant sends its identity to the access point, which is then forwarded to a RADIUS server. The RADIUS server then authenticates the client, and vice-versa. If these are successful the RADIUS server sends a RADIUS-ACCEPT message to the access point, which then allows the client to join the network.

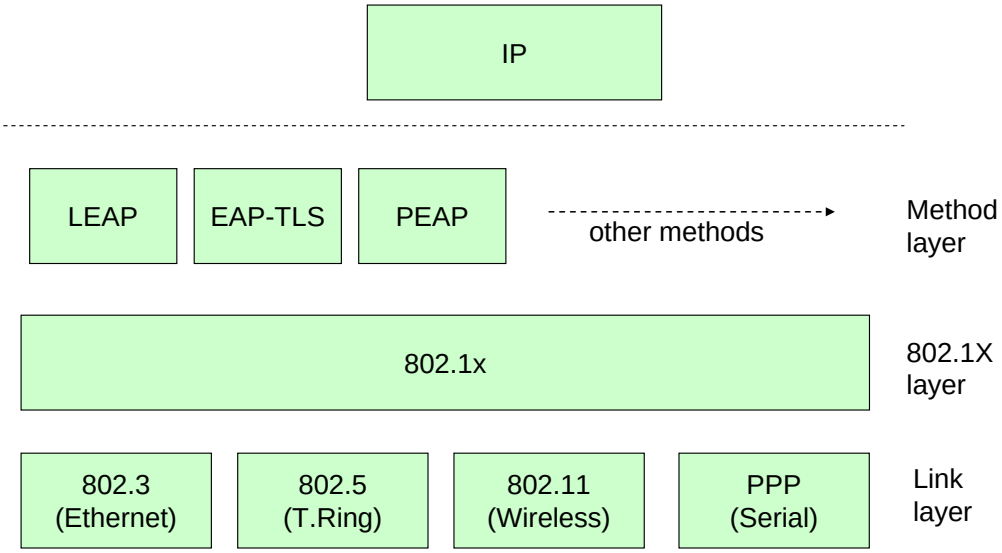

Figure 7 802.1X layers

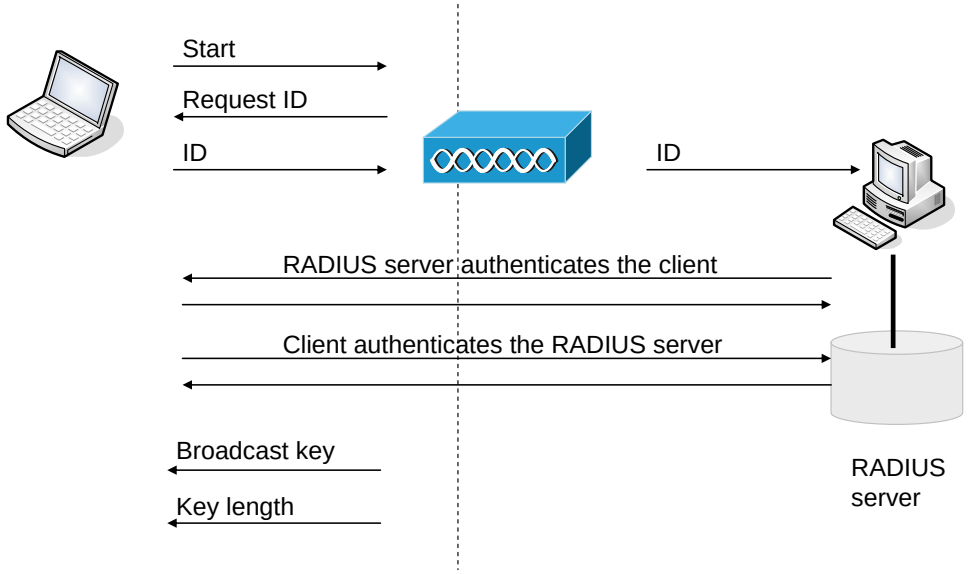

Figure 8 Basic message flow for 802.1X

5.3.1 EAP

A wireless client cannot gain access to the network, unless it has been authenticated by the access point or a RADIUS server, and has encryption keys (Figure 9). The main versions of EAP are:

- LEAP - Lightweight EAP.
- EAP-TLS - EAP-Transport Layer Security.
- PEAP - Protected EAP.
- EAP-TTLS - EAP-Tunnelled TLS.
- EAP-SIM - EAP-Subscriber Identity Module.

The operation of EAPs is:

1. Client associates with the access point.
2. Client provides authentication details. The client detail can be either UserID and password, or UserID and digital certification, or an on-time password.
3. RADIUS server authenticates the user.
4. User authenticates the RADIUS server.
5. Client and RADIUS server derive unicast WEP key.
6. RADIUS server gives broadcast WEP key to access point.
7. Access point sends broadcast WEP key to client using unicast WEP key.

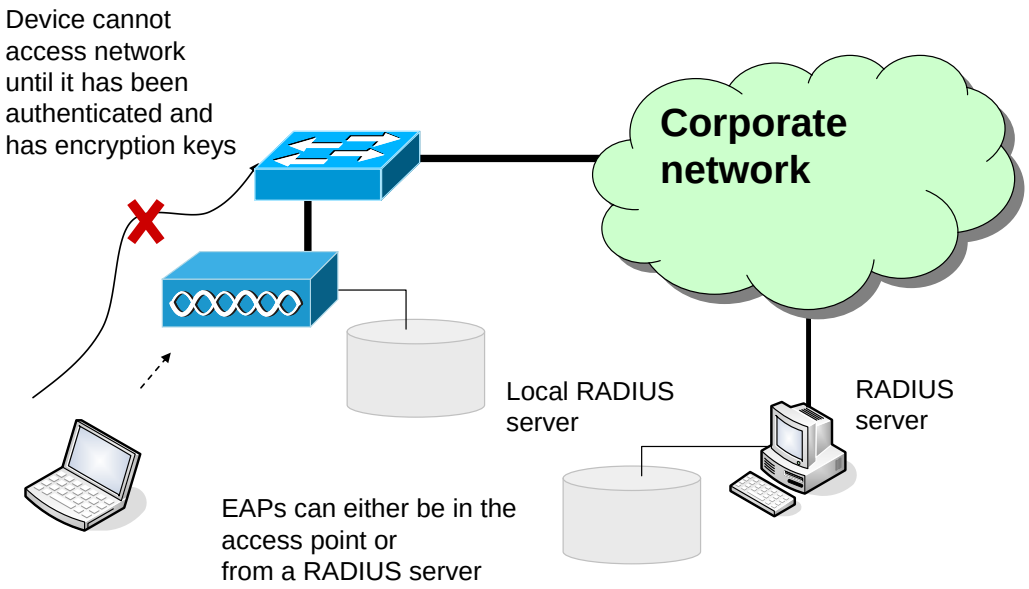

Figure 9 EAP authentication

5.3.2 EAP-TLS

This is based on a UserID and a digital certificate.

User Authentication:	User ID and digital certificate
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Certificate
Open Standard:	Yes

User differentiation:	Group
Certificate:	RADIUS server/WLAN client

5.3.3 LEAPs

This is based on UserID and password.

User Authentication:	User ID and password
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Not Supported
Open Standard:	No (Cisco-derived)
User differentiation:	Group
Certificate:	None

LEAP uses MS-CHAP (Microsoft Handshake Authentication Protocol) to continually challenge the device for its ID. It uses a challenge-response, mutual authentication protocol using Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating device challenges the client and vice-versa. If either challenge is incorrect, the connection is rejected. The password is converted into password hash[1] using MD4. It is thus not possible for an intruder to listen to the password.

The hashed password is then converted into a Windows NT key, which has the advantage of being compatible with Microsoft Windows systems. Normally authentication is achieved using the Microsoft login screen, where the user name and the Windows NT key are passed from the client to the access point.

LEAPs is open to attack from a dictionary attack, thus strong passwords should be used. There are also many programs which can search for passwords and determine their hash function.

5.3.4 Protected EAPS (PEAPs)

This uses a UserID and a one-time password.

User Authentication:	User ID and password or **OTP** (one-time password)
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Not supported
Open Standard:	Yes
User differentiation:	Group
Certificate:	Yes

[1] A hash function is a one-way encryption process, and thus the original data cannot be recovered.

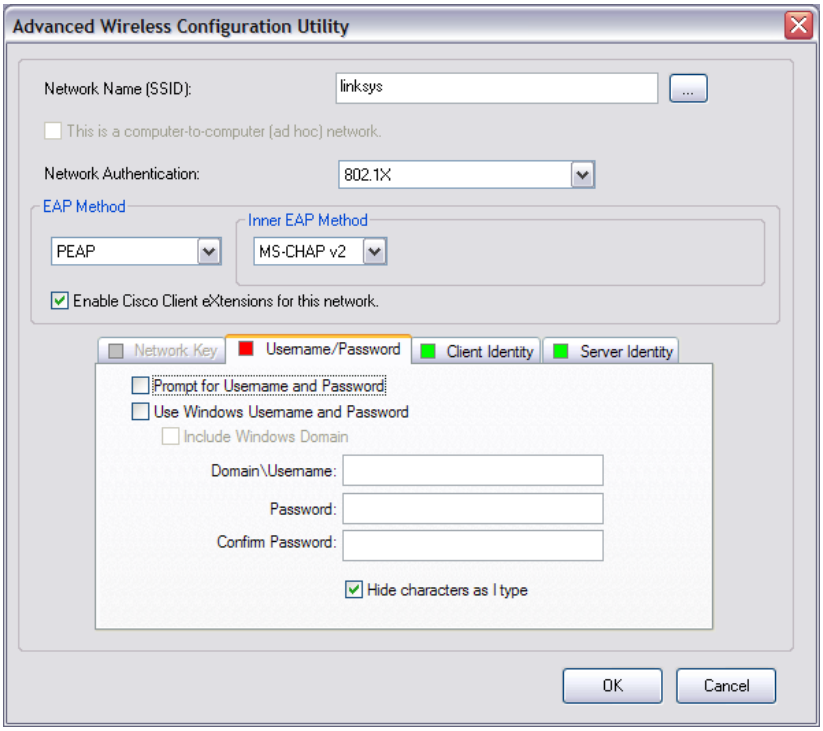

Figure 10 PEAP authentication

5.4 Digital Certificates

One of the most secure methods of authentication is to use digital certificates which are granted from a reputable source. Figure 11 shows the first part of the authentication process where the sender encrypts a known message with their private encryption key, and then, possibly, encrypts this and the data with the recipient's public key. When the encrypted message is then received by the recipient, it will be decrypted by the recipient's private key, and then the encrypted authentication is then decrypted by reading the senders public key which it reads from the digital certificate, as illustrated in Figure 12.

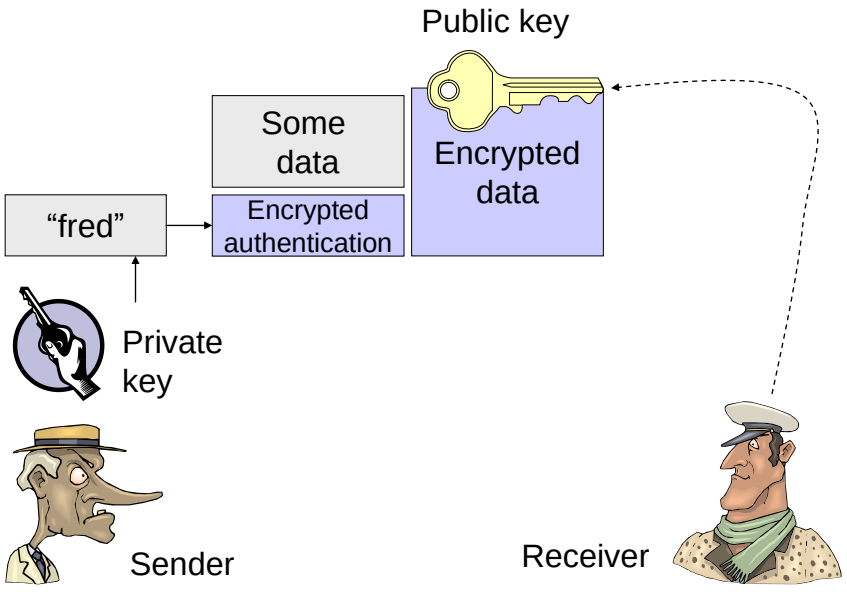

Figure 11 Adding authentication

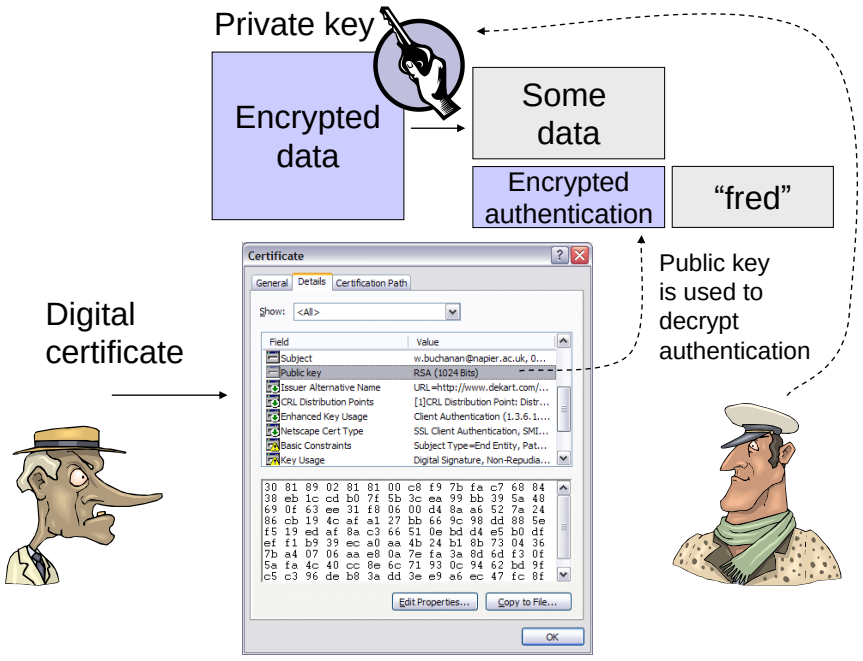

Figure 12 Authenticating

5.5 Cisco Access Point configuration

The authentication of the radio interface is defined within SSID configuration. To set the authentication to LEAP we must define a **user ID and a password**:

```
# config t
(config)# dot11 ssid ohio
(config-ssid)# dot11 ssid ohio
(config-ssid)# authentication ?
  client           LEAP client information
  key-management   key management
  network-eap      leap method
  open             open method
  shared           shared method
(config-ssid)# authentication network-eap ?
  WORD  leap list name (1 -- 31 characters)
(config-ssid)# auth net newhampshire ?
  mac-address  mac-address authentication method
  <cr>
(config-ssid)# authentication network-eap newhampshire
(config-ssid)# exit

(config)# int bvi1
(config-if)# ip address 143.224.21.9 255.240.0.0
(config-if)# int d0
(config-if)# encry ?
  key   Set one encryption key
  mode  encryption mode
  vlan  vlan
(config-if)# encry key ?
  <1-4>  key number 1-4
(config-if)# encry key 1
  size  Key size
(config-if)# encry key 1 size ?
  128bit  128-bit key
  40bit   40-bit key
(config-if)# encry key 1 size 128bit ?
  0         Specifies an UNENCRYPTED key will follow
  7         Specifies a HIDDEN key will follow
```

```
  Hex-data  26 hexadecimal digits
(config-if)# encry key 1 size 128bit fffffffffffffffffffffffffff
(config-if)# encryp mode ?
  ciphers  Optional data ciphers
  wep      Classic 802.11 privacy algorithm
(config-if)# encryp mode ciphers ?
  ckip       Cisco Per packet key hashing
  ckip-cmic  Cisco Per packet key hashing and MIC (MMH)
  cmic       Cisco MIC (MMH)
  tkip       WPA Temporal Key encryption
  wep128     128 bit key
  wep40      40 bit key
(config-if)# encryp mode ciphers ckip
(config-if)# ssid ohio
```

5.6 LEAP and RADIUS

This section contains a practical setup of LEAP and RADIUS running on an Aironet device, and use LEAP authentication. The parameters to set on the Aironet device are (Figure 13):

SSID: NapierSSID
IP address: 192.168.1.240/24
WEP key: AAAAAAAAAA (64-bit WEP key)
Authentication: LEAP

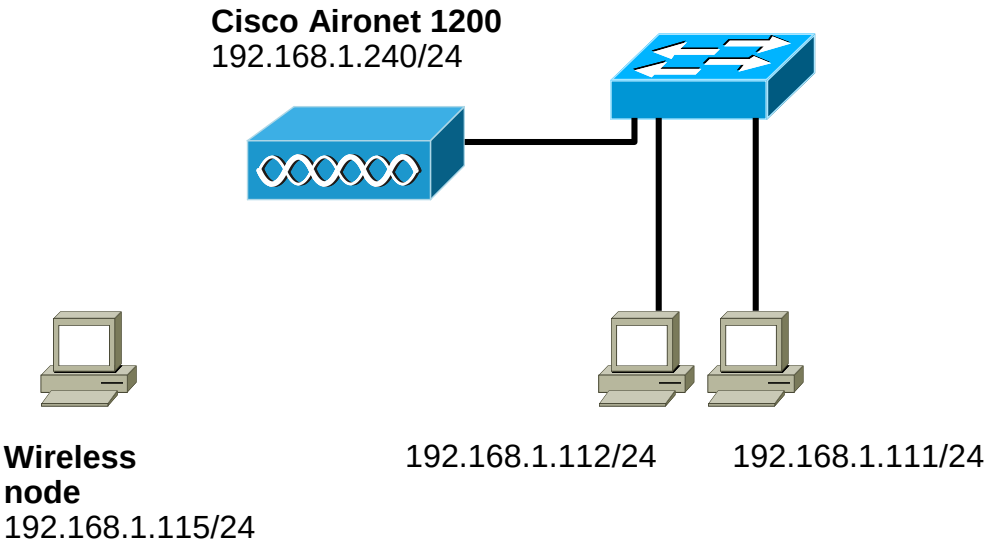

Figure 13

Step 1.

To setup a WEP key of AAAAAAAAAA, and IP address of 192.168.1.240, and open authentication.

A connection is made with the Access Point, and its SSID (NapierSSID), IP address and subnet mask can be set. This can be done either with the CLI of:

```
interface Dot11Radio0
      encryption key 1 size 40bit AAAAAAAAAA transmit-key
```

```
      encryption mode ciphers wep40
      no ssid tsunami
      ssid NapierSSID
            authentication network-eap eap_methods
      exit
      channel 1
      guest-mode
      station-role root
exit
interface BVI1
      ip address 192.168.1.240 255.255.255.0
exit
ip http server
```

2. After which the AAA can be setup with:

```
hostname ap
aaa new-model
aaa group server radius rad_eap
      server 192.168.1.240 auth-port 1812 acct-port 1813
exit
aaa group server radius rad_mac
aaa group server radius rad_acct
aaa group server radius rad_admin
aaa group server radius dummy
      server 192.168.1.240 auth-port 1812 acct-port 1813
exit
aaa group server radius rad_pmip
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
```

3. Next RADIUS is setup as the local server with (using a shared key of sharedkey):

```
radius-server local
      nas 192.168.1.240 key sharedkey
      user aaauser password aaapass
      user bbbuser password bbbpass
exit
radius-server host 192.168.1.240 auth-port 1812 acct-port 1813 key
sharedkey
exit
```

4. Next the wireless client can be setup by first setting the WEP key (Figure 14).

5. Next authentication is defined with LEAP (Figure 15), where the username is defined as **aaauser** and the password is **aaapass**.

6. The wireless device should be about to ping itself and the access point, such as:

```
C:\>ping 192.168.1.240

Pinging 192.168.1.240 with 32 bytes of data:

Reply from 192.168.1.240: bytes=32 time=2ms TTL=255
```

```
Reply from 192.168.1.240: bytes=32 time=1ms TTL=255
Reply from 192.168.1.240: bytes=32 time=1ms TTL=255
Reply from 192.168.1.240: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.1.115

Pinging 192.168.1.115 with 32 bytes of data:
Reply from 192.168.1.115: bytes=32 time<1ms TTL=128
Reply from 192.168.1.115: bytes=32 time<1ms TTL=128
Reply from 192.168.1.115: bytes=32 time<1ms TTL=128
Reply from 192.168.1.115: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.115:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6. The wireless access point should also be able to show the association such as:

```
ap#show dot11 assoc

802.11 Client Stations on Dot11Radio0:

SSID [NapierSSID] :

MAC Address    IP address      Device         Name            Parent
State
0090.4b54.d83a 192.168.1.115   4500-radio     -               self
EAP-Assoc

Others:  (not related to any ssid)
```

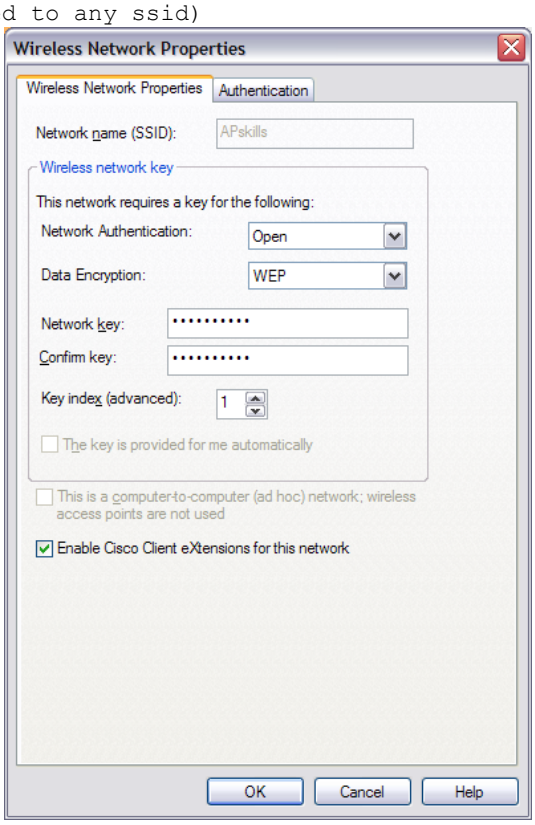

Figure 14

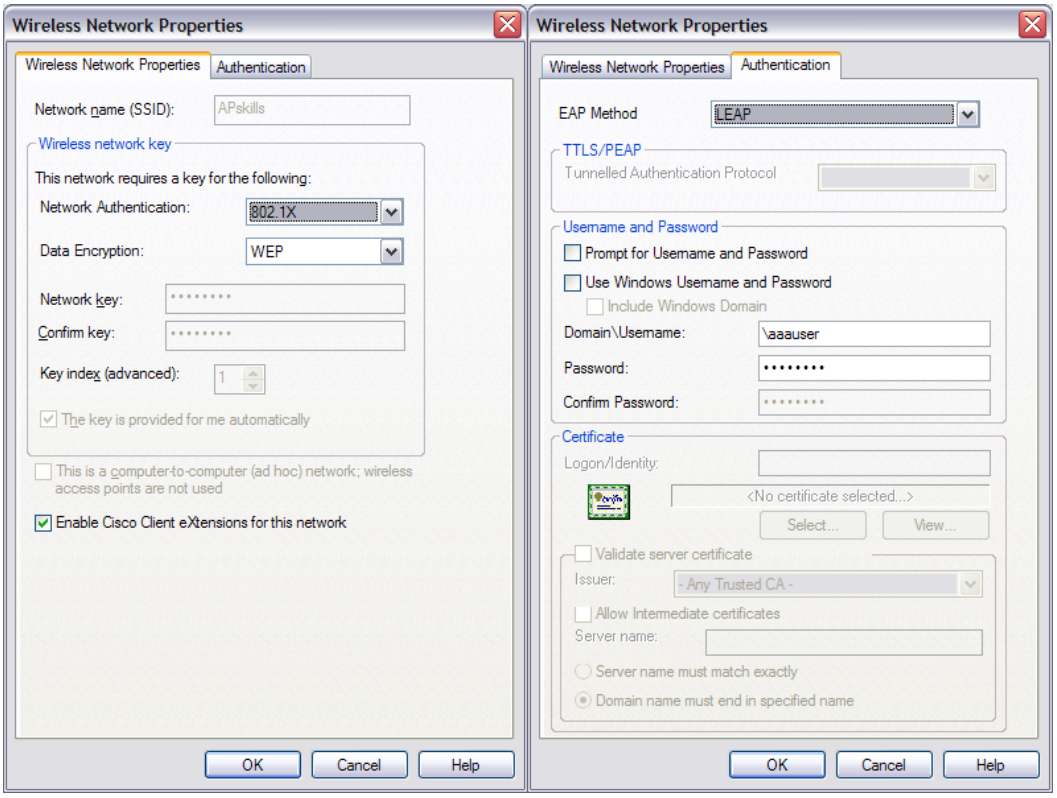
Wireless Network Properties
Wireless Network Properties
Authentication
Network name (SSID):
APskills
Wireless network key
This network requires a key for the following:
Network Authentication:
802.1X
Data Encryption:
WEP
Network key:
Confirm key:
Key index (advanced):
1
The key is provided for me automatically
This is a computer-to-computer (ad hoc) network; wireless access points are not used
Enable Cisco Client eXtensions for this network
OK
Cancel
Help
Wireless Network Properties
Wireless Network Properties
Authentication
EAP Method
LEAP
TTLS/PEAP
Tunnelled Authentication Protocol
Username and Password
Prompt for Username and Password
Use Windows Username and Password
Include Windows Domain
Domain\Username:
\aaauser
Password:
Confirm Password:
Certificate
Logon/Identity:
<No certificate selected...>
Select...
View...
Validate server certificate
Issuer:
- Any Trusted CA -
Allow Intermediate certificates
Server name:
Server name must match exactly
Domain name must end in specified name
OK
Cancel
Help

Figure 15