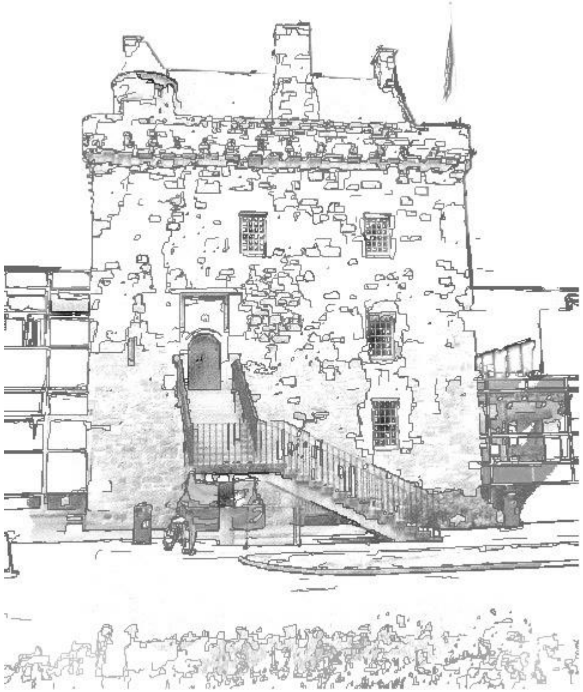
Wireless LAN

Unit 5: Wireless Authentication



Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

Author: Bill Buchanan

Wireless connections … which technology?

Areas covered:

Authentication methods

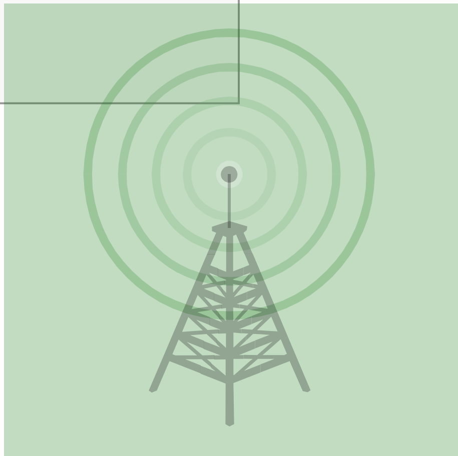
Ways?

LEAP, PEAP, EAP, and so on

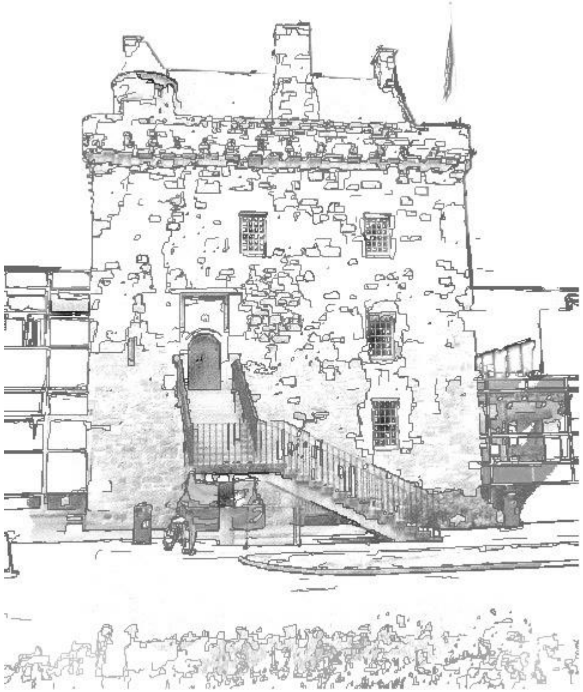
Methods and weaknesses.

Configurating authentication on an Aironet

A simple example with local Radius



Security



Fundamental Elements of Security

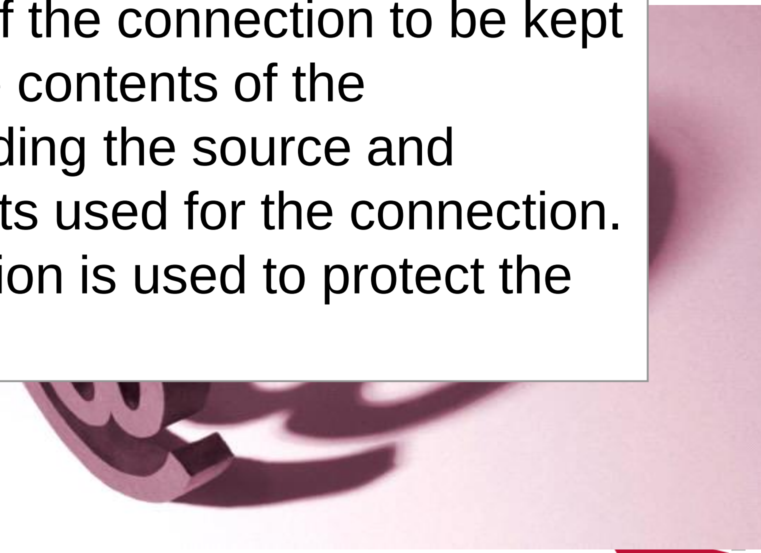
Authentication. This is used to identify the user, the wireless client and the wireless access point.

Authorization. This is used to determine that users and wireless devices have the authorization to connect to the network.

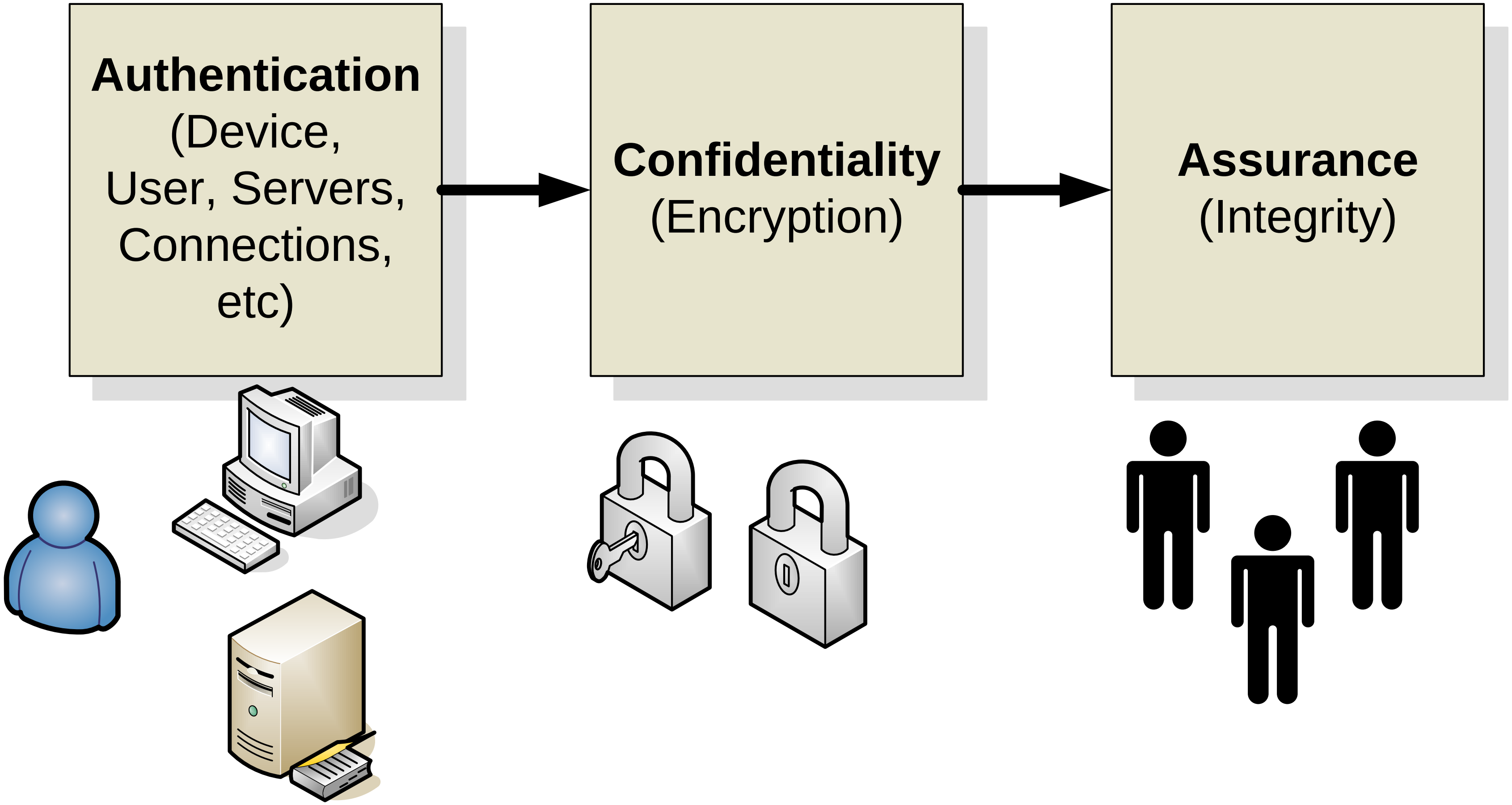
Accounting. This is used to log information on the usage of the network, and may set restrictions of the access.

Assurance. This defines that the data that is received and transmitted has not been changed in any way. This is often known as Integrity.

Confidentiality. This allows the details of the connection to be kept secret. It typically involves preserving the contents of the transmitted data, but may also include hiding the source and destinations addresses, and the TCP ports used for the connection. Most often, in wireless networks, encryption is used to protect the confidentiality.



Fundamental Principles of Security



Authentication (Device, User, Servers, Connections, etc)

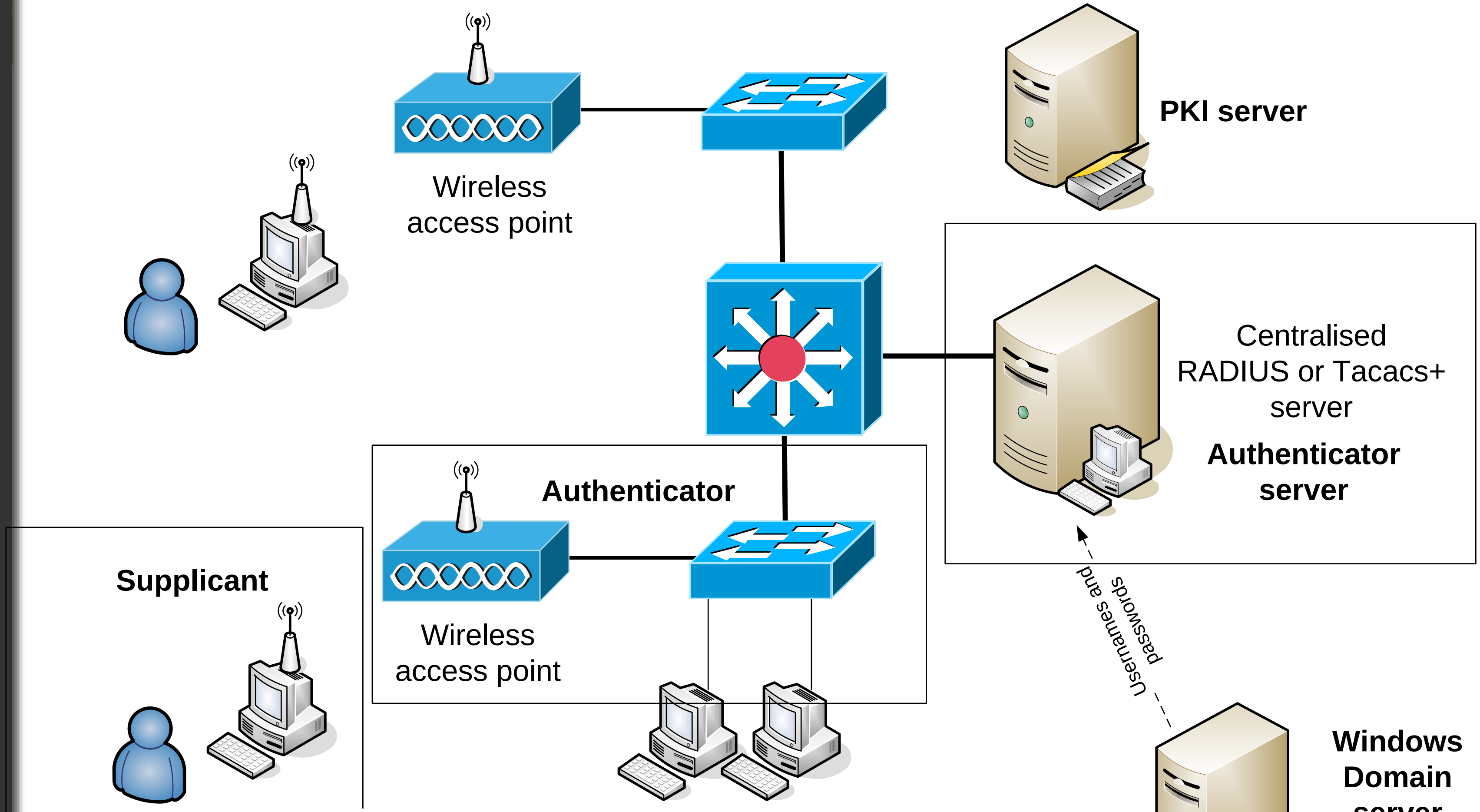
Confidentiality (Encryption)

Assurance (Integrity)

Wireless LAN

Centre for Dist. Computing and Security

Prof W Buchanan



Encryption
WEP: 40-bit RC4
WPA: 128-bit RC4
WPA2: AES

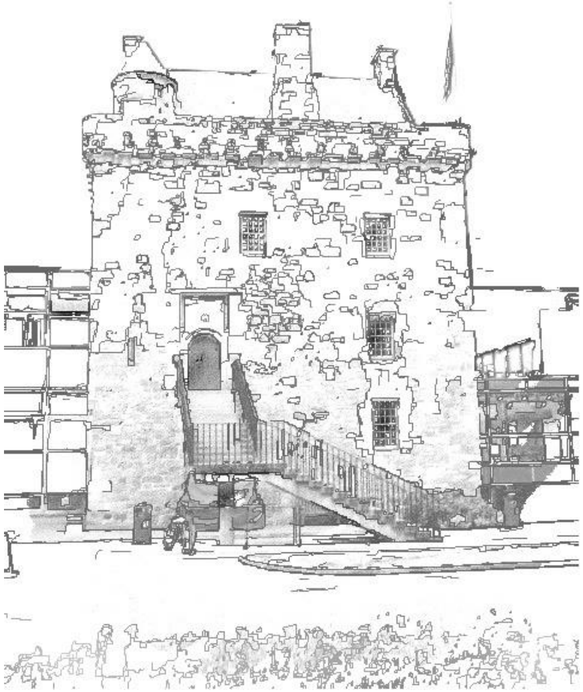
Authentication
WEP: OAS, SKA
WPA: 802.1x, EAP (RADIUS)
WPA2: 802.1x, EAP, RSNA

Integrity
WEP: Checksum
WPA: MIC (64-bit)
WPA2: CBC-MAC

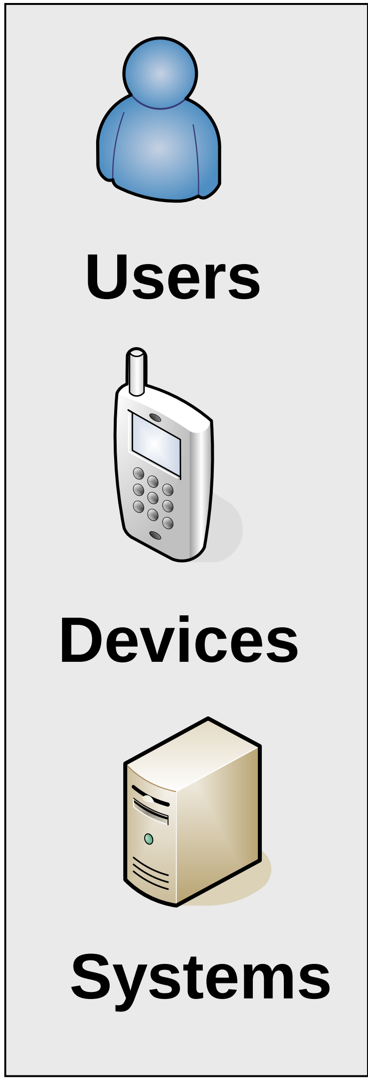
Edinburgh Napier
UNIVERSITY

Author: Bill Buchanan

Ways to Authenticate



Authentication methods



Users

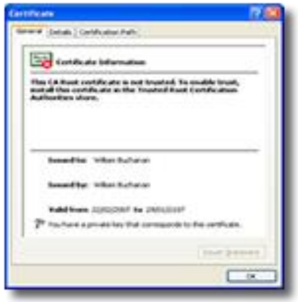
Devices

Systems

Authentication methods

Username/
password

Network/
physical
address



Certificate

General | Details | Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: William Buchanan

Issued by: William Buchanan

Valid from [illegible] to [illegible]

You have a private key that corresponds to this certificate.

Issuer Statement

OK

Digital
certificate

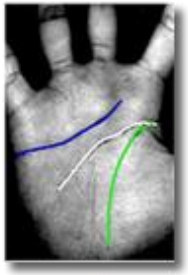
Retina
scan

Finger
print

Smart
card

RFID
tags

Palm
print



Retina
scan

USB stick
with encrypyion
keys

Users

Devices

Systems

Author: Bill Bu

Authentication methods

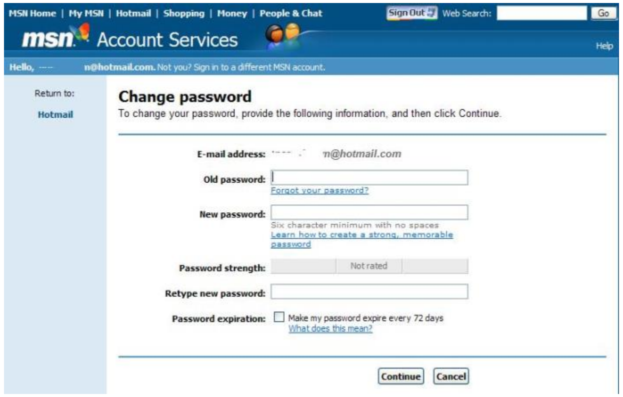
Network/physical addresses. These are simple method of verifying a device. The network address, such as the IP address can be easily spoofed, but the physical address is less easy and is a more secure implementation. Unfortunately the physical address can also be spoofed, either through software modifications 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.

Users

Devices

Systems



MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat
Sign Out
Web Search:
Go
msn Account Services
Help

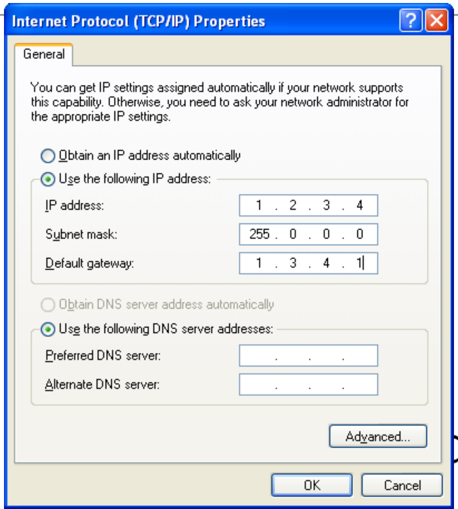
Hello, ---- n@hotmail.com. Not you? Sign in to a different MSN account.

Return to: Hotmail

Change password

To change your password, provide the following information, and then click Continue.

E-mail address:	n@hotmail.com
Old password:	Forgot your password?
New password:	Six character minimum with no spaces Learn how to create a strong, memorable password
Password strength:	Not rated
Retype new password:	
Password expiration:	☐ Make my password expire every 72 days What does this mean?



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	1 . 2 . 3 . 4
Subnet mask:	255 . 0 . 0 . 0
Default gateway:	1 . 3 . 4 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

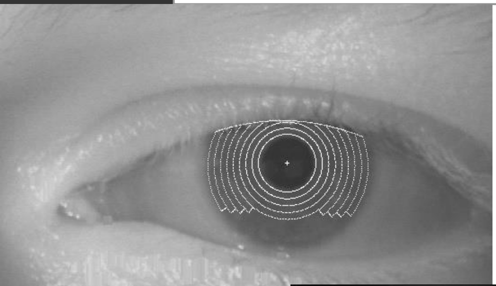
Preferred DNS server:	. . .
Alternate DNS server:	. . .

dinburgh Napier
UNIVERSITY

Authentication methods

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.



Users

Devices

Systems

Authentication methods

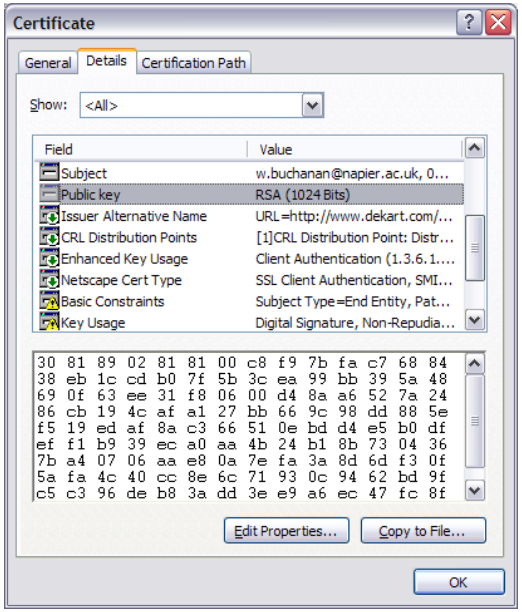
Authentication certificate. This certificate verifies a user or a device by providing a digital certificate which can be verified by a reputable source. Methods include EAP-TLS.

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.

Users

Devices

Systems



Show: <All>

Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

Authentication methods

Physical port connection. Maps users to ports, so that they cannot connect to any other port.

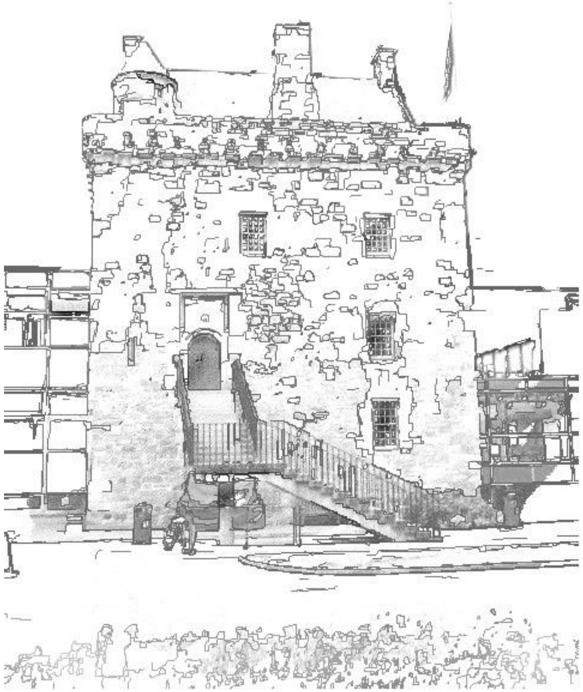
Mobile Phone SIM Cards. Maps mobile phones to users.

Users

Devices

Systems

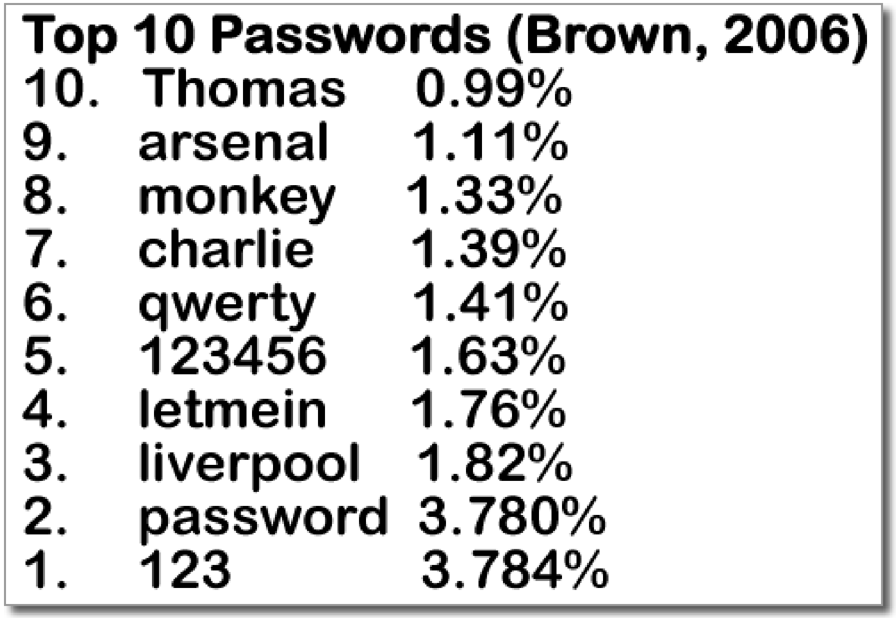
Usernames and passwords



Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

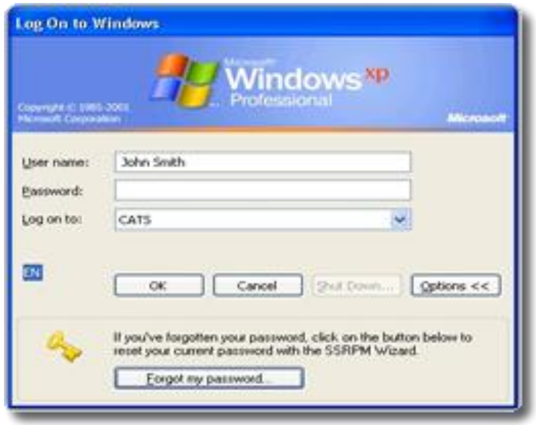
Author: Bill Buchanan

The problem with passwords is ...



Top 10 Passwords (Brown, 2006)

10.	Thomas	0.99%
9.	arsenal	1.11%
8.	monkey	1.33%
7.	charlie	1.39%
6.	qwerty	1.41%
5.	123456	1.63%
4.	letmein	1.76%
3.	liverpool	1.82%
2.	password	3.780%
1.	123	3.784%



Log On to Windows

Copyright © 1985-2001 Microsoft Corporation

User name: John Smith

Password:

Log on to: CATS

If you've forgotten your password, click on the button below to reset your current password with the SSRPM Wizard.

Brown, http://www.modernlifeisrubbish.co.uk/article/top-10-most-common-passwords, 2006.

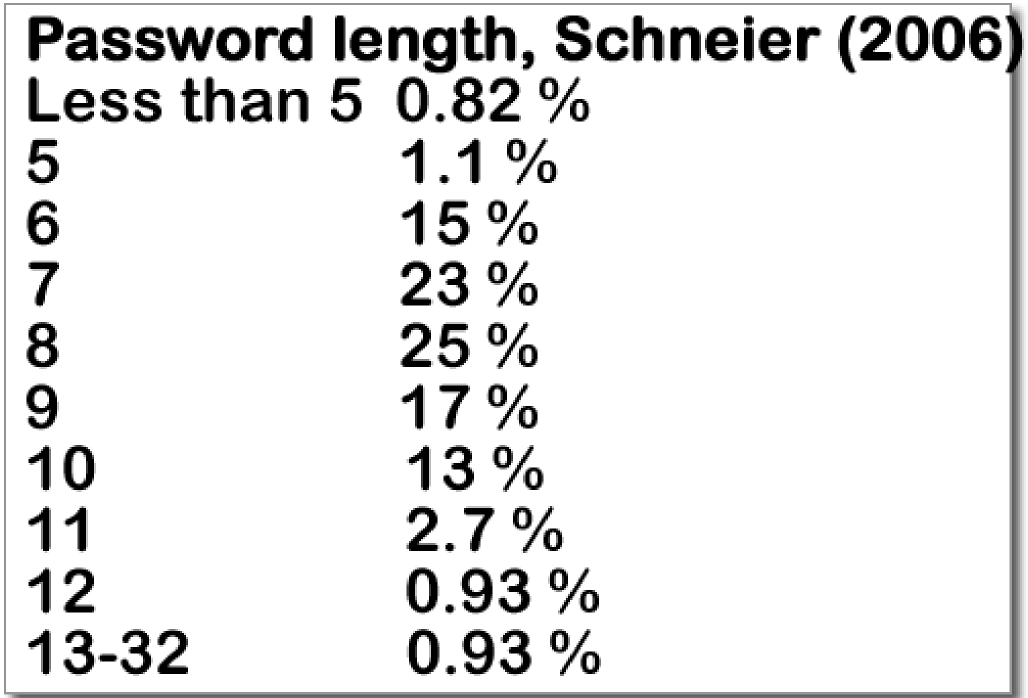
Usernames and passwords are used by many systems as a way of authenticating users.

Suffer from many problems, especially that the full range of available passwords is hardly ever used.

For example a 10 character password has 8 bits per character, thus it there should be up to 80 bits used for the password, which gives 1,208,925,819,614,629,174,706,176 possible permutations.

Unfortunately the actual number of useable passwords is typically less than 1.3 bits per character, such as the actual bit size is less than **13 bits** (8192).

The problem with passwords is ...



Password length, Schneier (2006)

Less than 5	0.82 %
5	1.1 %
6	15 %
7	23 %
8	25 %
9	17 %
10	13 %
11	2.7 %
12	0.93 %
13-32	0.93 %

Log On to Windows

User name: John Smith
Password:
Log on to: CATS

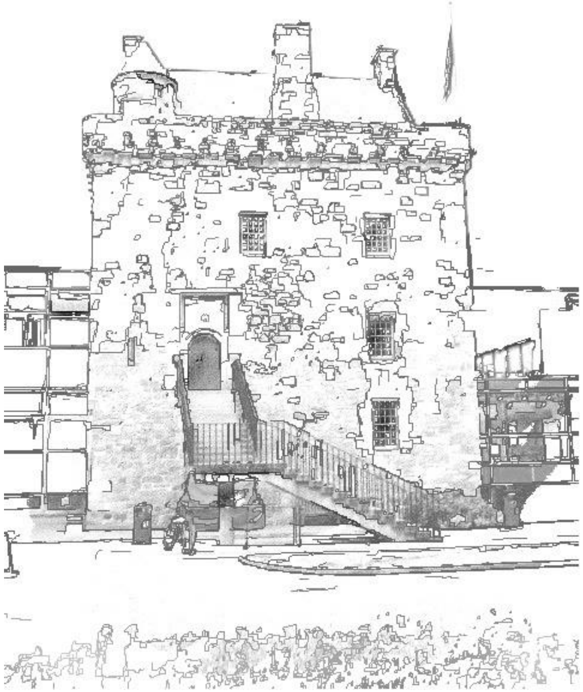
If you've forgotten your password, click on the button below to reset your current password with the SSRPM Wizard.

He also found 81% used a mixture of alphanumeric characters, whereas only 9.6% used only letters, and 1.3% used just numbers.

Also his Top 10 was: password1, abc123, myspace1, password, blink182, qwerty1, #uck$ou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey. The MySpace password was popular as the survey was done over the MySpace domain.

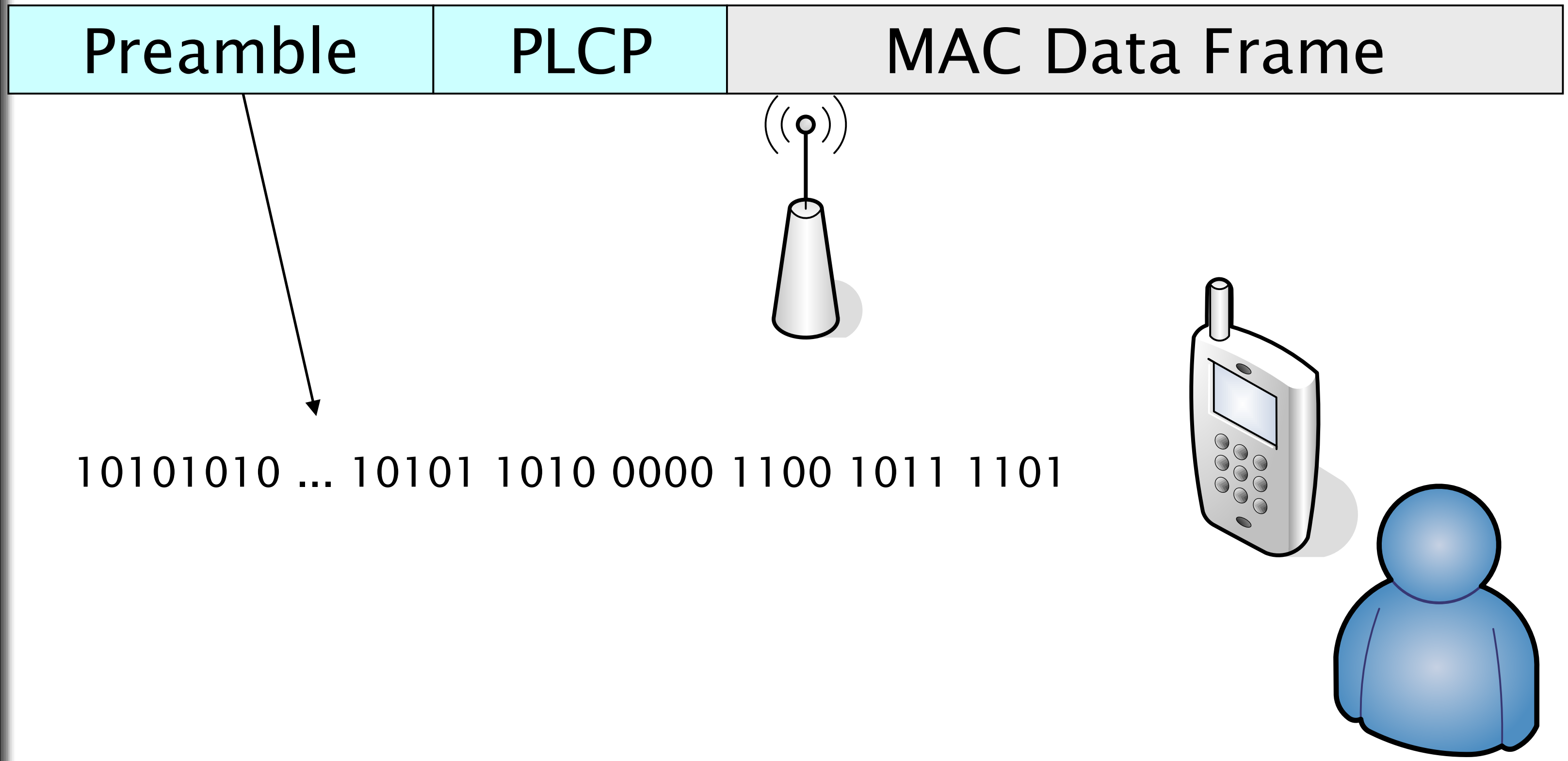
Schneier, http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

IEEE 802.11 Frame Format



Edinburgh Napier
UNIVERSITY

Transmitted frame



Preamble

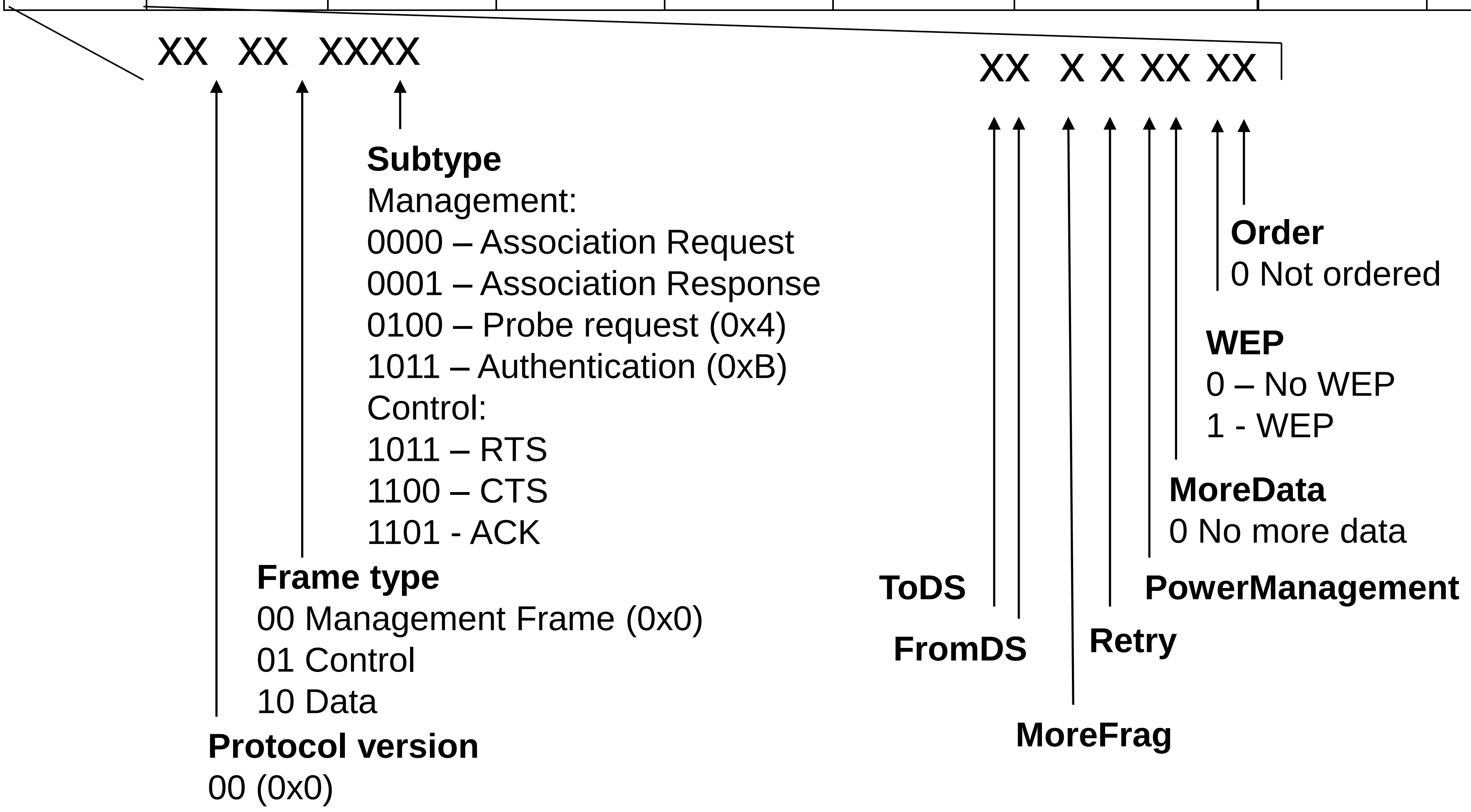
PLCP

MAC Data Frame

10101010 ... 10101 1010 0000 1100 1011 1101

IEEE 802.11 data frame

2 Bytes	2	6	6	6	2	6	0-2312	4
Frame control	Duration/ ID	Add 1 (Dest.)	Add 2 (Src)	Add 3 (SSID)	Sequence control	Add 4	Frame body	FCS



XX XX XXXX

XX X X XX XX

Subtype
Management:
0000 – Association Request
0001 – Association Response
0100 – Probe request (0x4)
1011 – Authentication (0xB)
Control:
1011 – RTS
1100 – CTS
1101 - ACK

Frame type
00 Management Frame (0x0)
01 Control
10 Data

Protocol version
00 (0x0)

Order
0 Not ordered

WEP
0 – No WEP
1 - WEP

MoreData
0 No more data

PowerManagement

ToDS

FromDS

Retry

MoreFrag

IEEE 802.11 data frame

2 Bytes	2	6	6	6	2	6	0-2312	4
Frame control	Duration/ ID	Add 1 (Dest.)	Add 2 (Src)	Add 3 (SSID)	Sequence control	Add 4	Frame body	FCS

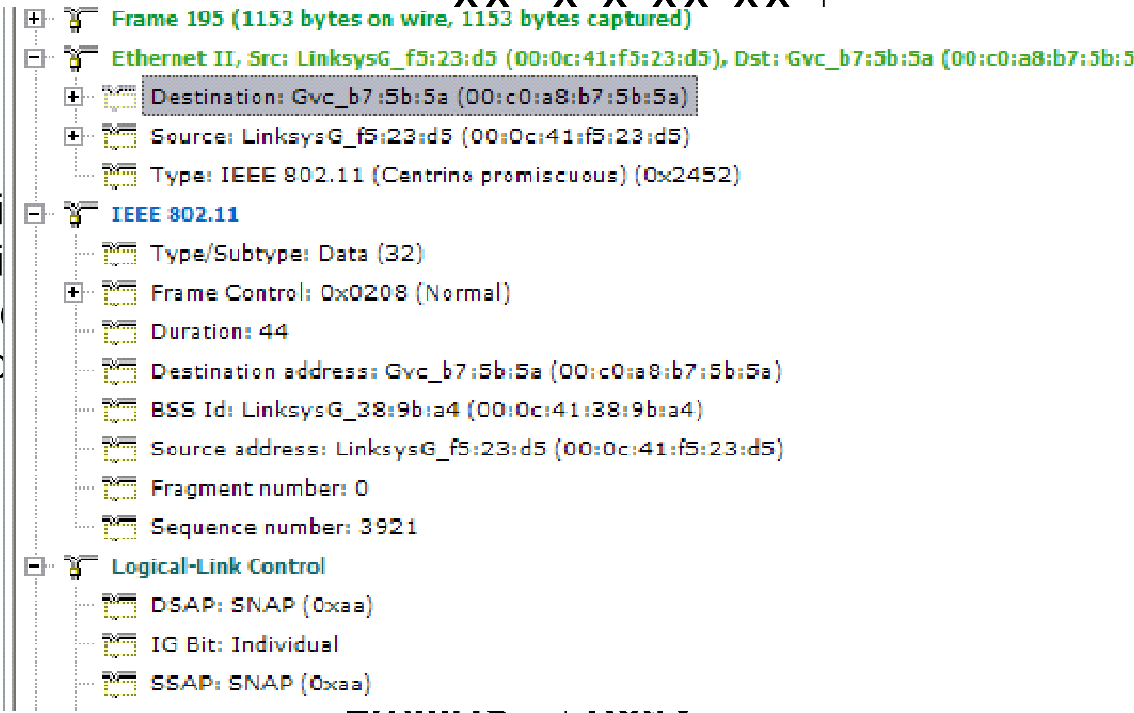
XX XX XXXX

XX X X XX XX

Subtype
Management:
0000 – Associati
0001 – Associati
0100 – Probe re
1011 – Authentic
Control:
1011 – RTS
1100 – CTS
1101 - ACK

Frame type
00 Management Frame
01 Control
10 Data

Protocol version
00 (0x0)



```
⊞ Frame 195 (1153 bytes on wire, 1153 bytes captured)
⊟ Ethernet II, Src: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5), Dst: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5
   ⊞ Destination: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5a)
   ⊞ Source: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5)
     Type: IEEE 802.11 (Centrino promiscuous) (0x2452)
⊟ IEEE 802.11
     Type/Subtype: Data (32)
   ⊞ Frame Control: 0x0208 (Normal)
     Duration: 44
     Destination address: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5a)
     BSS Id: LinksysG_38:9b:a4 (00:0c:41:38:9b:a4)
     Source address: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5)
     Fragment number: 0
     Sequence number: 3921
⊟ Logical-Link Control
     DSAP: SNAP (0xaa)
     IG Bit: Individual
     SSAP: SNAP (0xaa)
```

FromDS

Retry

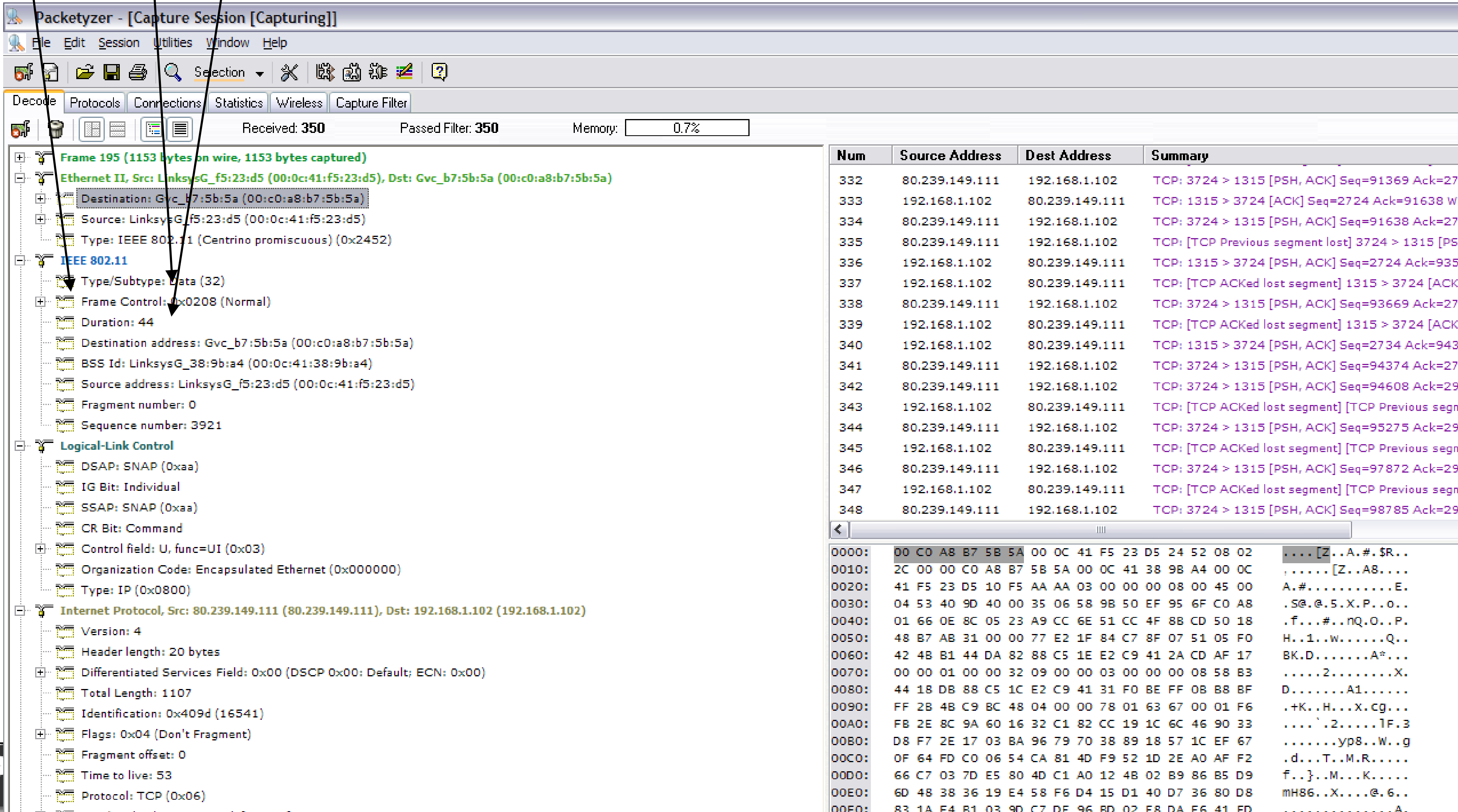
MoreFrag

IEEE 802.11 data frame

Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Frame body	FCS
2 Bytes	**2**	**6**	**6**	**6**	**2**	**6**	**0-2312**	**4**

Frame control. This contains control information.
Duration/ID. This contains information on how long the data frame will last.
Address fields. This contains different types of address, such as an individual address of group addresses. The two main types of group addresses are broadcast and multicast.
Sequence control. This identifies the sequence number of the data frames, and allows the recipient to check for missing or duplicate data frames.
Frame body. This part contains the actual data. The maximum amount is 2312 bytes, but most implementations use up to 1500 bytes.
FCS (Frame Check Sequence). This is a strong error detection code.

Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Frame body	FCS
2 Bytes	2	6	6	6	2	6	0-2312	4



Packetyzer - [Capture Session [Capturing]]
File Edit Session Utilities Window Help
Selection
Decode
Protocols
Connections
Statistics
Wireless
Capture Filter

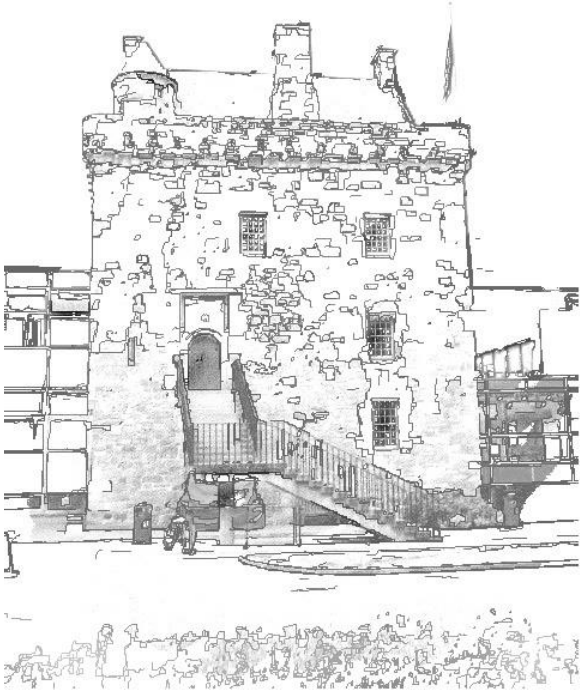
Received: 350 Passed Filter: 350 Memory: 0.7%

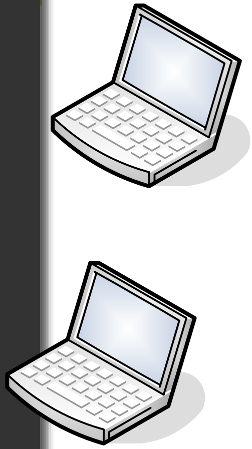
```
Frame 195 (1153 bytes on wire, 1153 bytes captured)
Ethernet II, Src: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5), Dst: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5a)
    Destination: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5a)
    Source: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5)
    Type: IEEE 802.11 (Centrino promiscuous) (0x2452)
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208 (Normal)
    Duration: 44
    Destination address: Gvc_b7:5b:5a (00:c0:a8:b7:5b:5a)
    BSS Id: LinksysG_38:9b:a4 (00:0c:41:38:9b:a4)
    Source address: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5)
    Fragment number: 0
    Sequence number: 3921
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func=UI (0x03)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IP (0x0800)
Internet Protocol, Src: 80.239.149.111 (80.239.149.111), Dst: 192.168.1.102 (192.168.1.102)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1107
    Identification: 0x409d (16541)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 53
    Protocol: TCP (0x06)
```

Num	Source Address	Dest Address	Summary
332	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=91369 Ack=27
333	192.168.1.102	80.239.149.111	TCP: 1315 > 3724 [ACK] Seq=2724 Ack=91638 W
334	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=91638 Ack=27
335	80.239.149.111	192.168.1.102	TCP: [TCP Previous segment lost] 3724 > 1315 [PS
336	192.168.1.102	80.239.149.111	TCP: 1315 > 3724 [PSH, ACK] Seq=2724 Ack=935
337	192.168.1.102	80.239.149.111	TCP: [TCP ACKed lost segment] 1315 > 3724 [ACK
338	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=93669 Ack=27
339	192.168.1.102	80.239.149.111	TCP: [TCP ACKed lost segment] 1315 > 3724 [ACK
340	192.168.1.102	80.239.149.111	TCP: 1315 > 3724 [PSH, ACK] Seq=2734 Ack=943
341	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=94374 Ack=27
342	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=94608 Ack=29
343	192.168.1.102	80.239.149.111	TCP: [TCP ACKed lost segment] [TCP Previous segn
344	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=95275 Ack=29
345	192.168.1.102	80.239.149.111	TCP: [TCP ACKed lost segment] [TCP Previous segn
346	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=97872 Ack=29
347	192.168.1.102	80.239.149.111	TCP: [TCP ACKed lost segment] [TCP Previous segn
348	80.239.149.111	192.168.1.102	TCP: 3724 > 1315 [PSH, ACK] Seq=98785 Ack=29

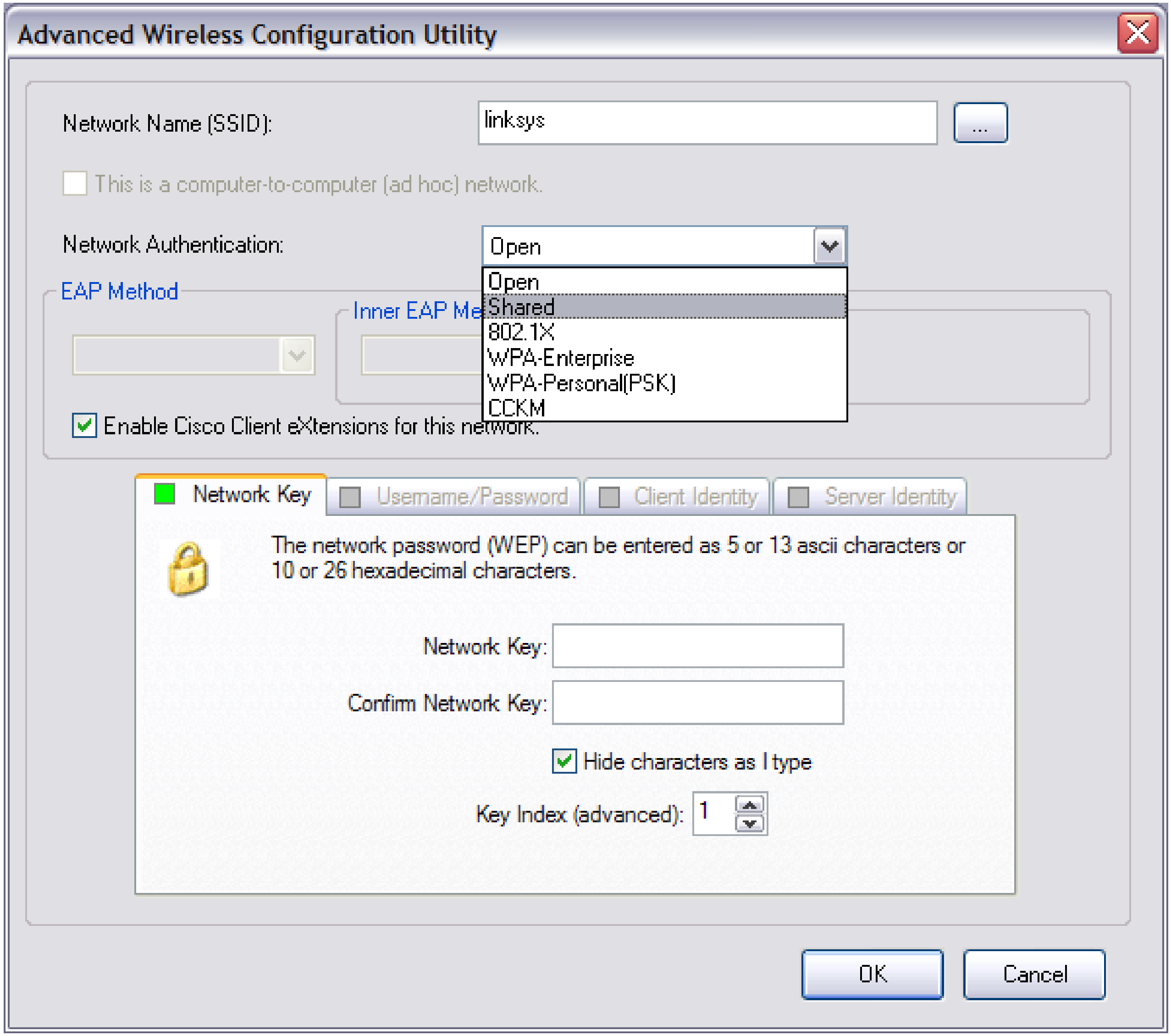
```
0000:   00 C0 A8 B7 5B 5A 00 0C 41 F5 23 D5 24 52 08 02   ....[Z..A.#.$R..
0010:   2C 00 00 C0 A8 B7 5B 5A 00 0C 41 38 9B A4 00 0C   ,.....[Z..A8....
0020:   41 F5 23 D5 10 F5 AA AA 03 00 00 00 08 00 45 00   A.#...........E.
0030:   04 53 40 9D 40 00 35 06 58 9B 50 EF 95 6F C0 A8   .S@.@.5.X.P..o..
0040:   01 66 0E 8C 05 23 A9 CC 6E 51 CC 4F 8B CD 50 18   .f...#..nQ.O..P.
0050:   48 B7 AB 31 00 00 77 E2 1F 84 C7 8F 07 51 05 F0   H..1..w......Q..
0060:   42 4B B1 44 DA 82 88 C5 1E E2 C9 41 2A CD AF 17   BK.D.......A*...
0070:   00 00 01 00 00 32 09 00 00 03 00 00 00 08 58 B3   .....2........X.
0080:   44 18 DB 88 C5 1C E2 C9 41 31 F0 BE FF 0B B8 BF   D.......A1......
0090:   FF 2B 4B C9 BC 48 04 00 00 78 01 63 67 00 01 F6   .+K..H...x.cg...
00A0:   FB 2E 8C 9A 60 16 32 C1 82 CC 19 1C 6C 46 90 33   ....`.2.....lF.3
00B0:   D8 F7 2E 17 03 BA 96 79 70 38 89 18 57 1C EF 67   .......yp8..W..g
00C0:   0F 64 FD C0 06 54 CA 81 4D F9 52 1D 2E A0 AF F2   .d...T..M.R.....
00D0:   66 C7 03 7D E5 80 4D C1 A0 12 4B 02 B9 86 B5 D9   f..}..M...K.....
00E0:   6D 48 38 36 19 E4 58 F6 D4 15 D1 40 D7 36 80 D8   mH86..X....@.6..
00F0:   83 1A F4 B1 03 9D C7 DF 96 BD 02 E8 DA F6 41 FD   ..............A.
```

Wireless Authentication





WEP also allows for authentication using a secret key (shared key) or an open system.



Advanced Wireless Configuration Utility

Network Name (SSID): linksys

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: Open

☑ Enable Cisco Client eXtensions for this network.

The network password (WEP) can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

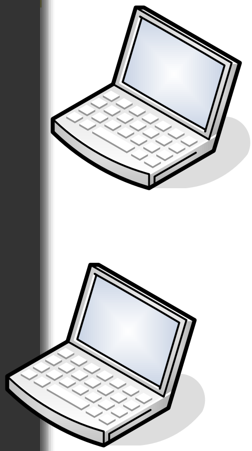
Network Key:

Confirm Network Key:

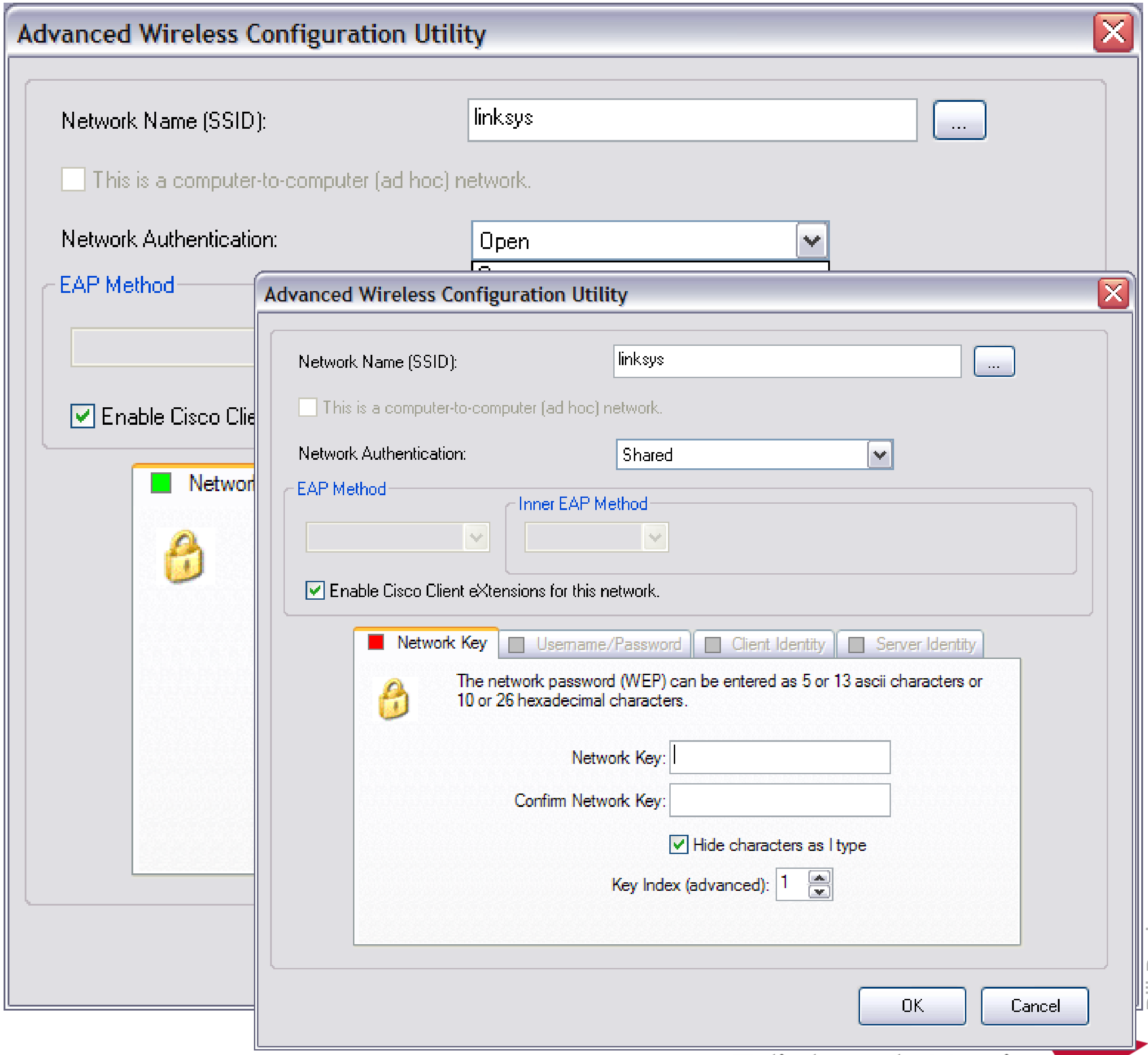
☑ Hide characters as I type

Key Index (advanced): 1

Edinburgh Napier
UNIVERSITY



WEP
also allows for authentication using a secret key (shared key) or an open system.



Advanced Wireless Configuration Utility

Network Name (SSID): linksys

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: Open

EAP Method

☑ Enable Cisco Clie

🟩 Networ

Advanced Wireless Configuration Utility

Network Name (SSID): linksys

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: Shared

EAP Method

Inner EAP Method

☑ Enable Cisco Client eXtensions for this network.

🟥 Network Key | Username/Password | Client Identity | Server Identity

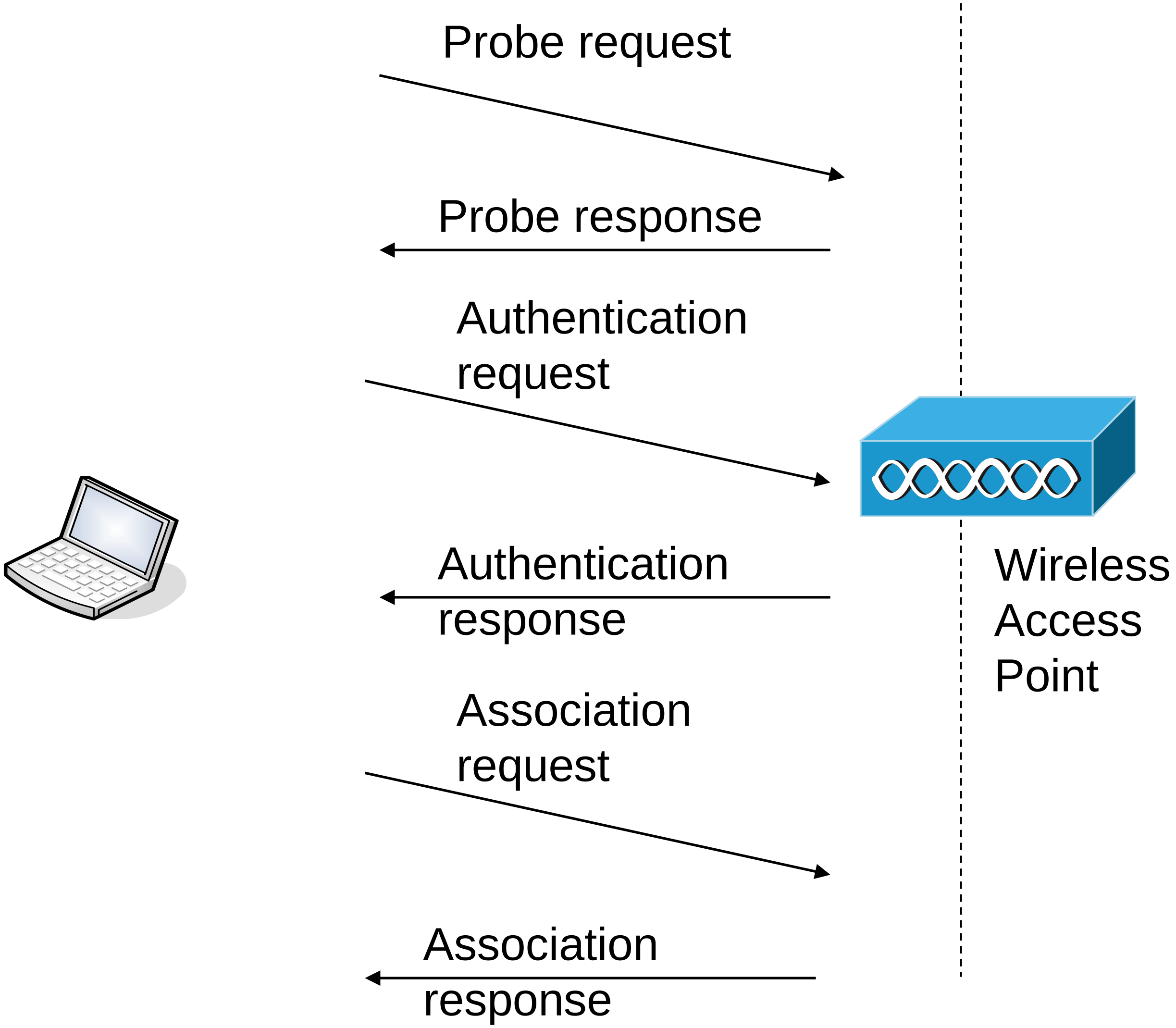
The network password (WEP) can be entered as 5 or 13 ascii characters or 10 or 26 hexadecimal characters.

Network Key:

Confirm Network Key:

☑ Hide characters as I type

Key Index (advanced): 1



Probe request

Probe response

Authentication request

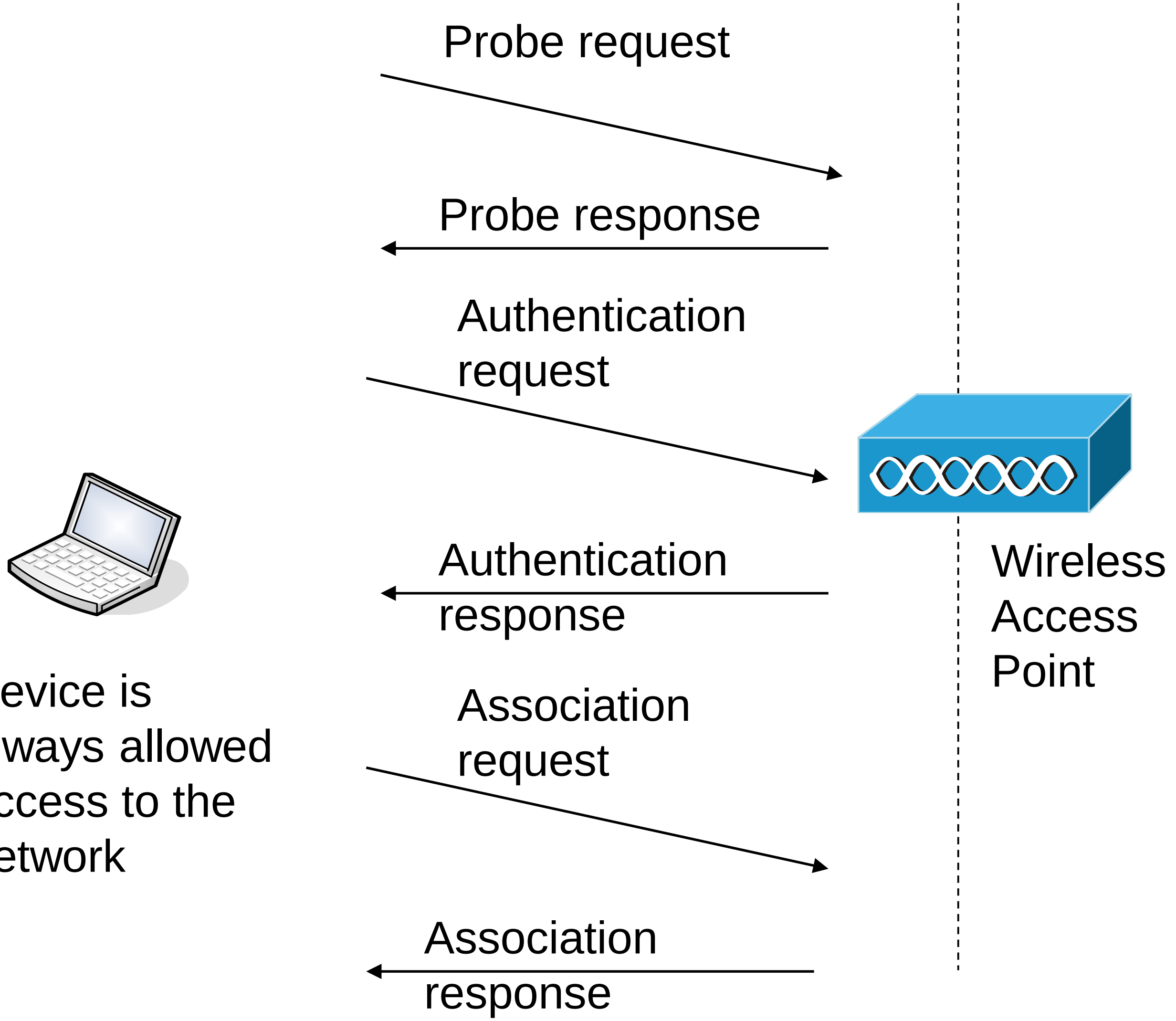
Authentication response

Association request

Association response

Wireless Access Point

Open authentication



Probe request

Probe response

Authentication request

Authentication response

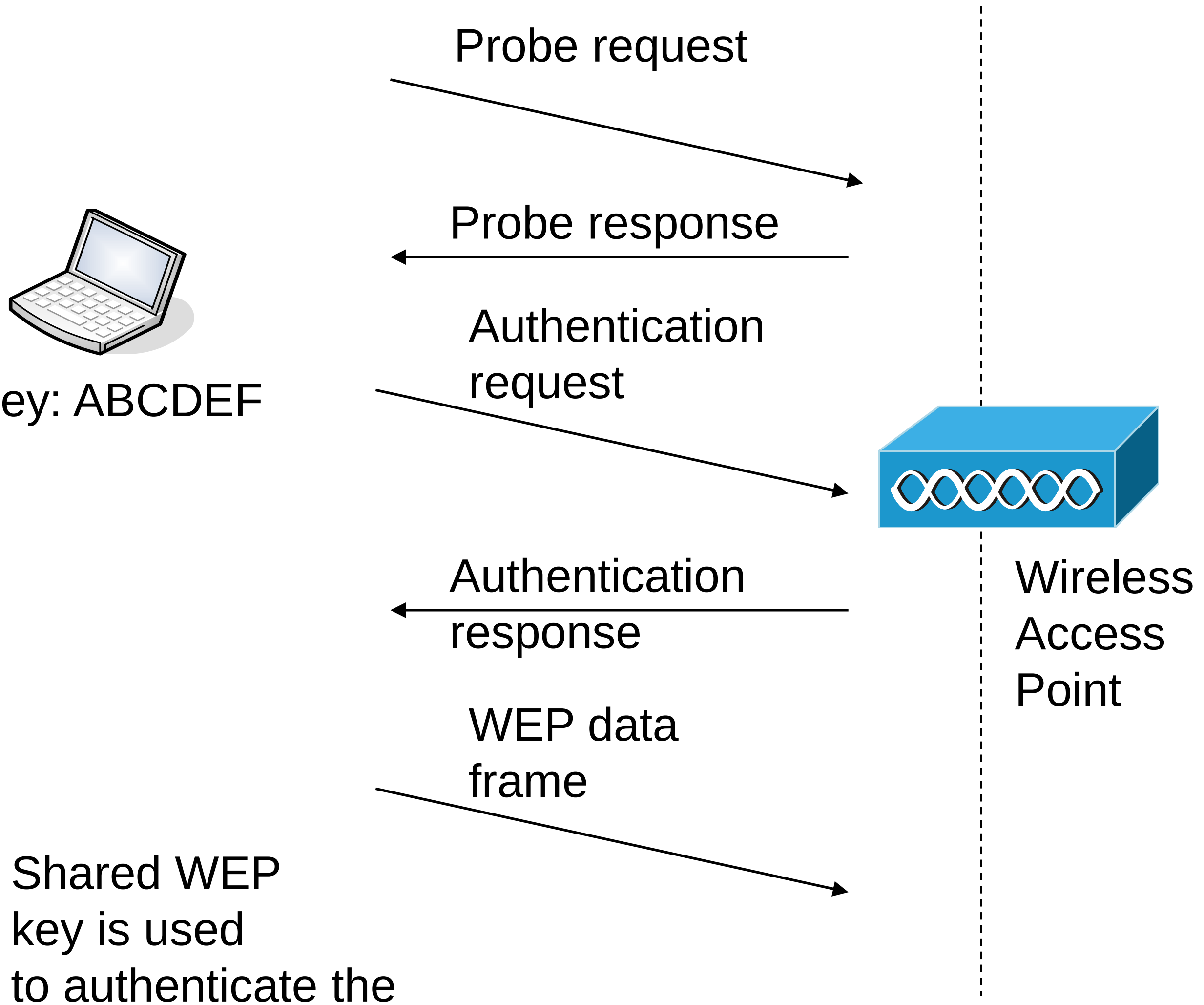
Association request

Association response

Wireless Access Point

Device is always allowed access to the network

Open authentication (based on WEP)



Probe request

Probe response

Authentication request

Authentication response

WEP data frame

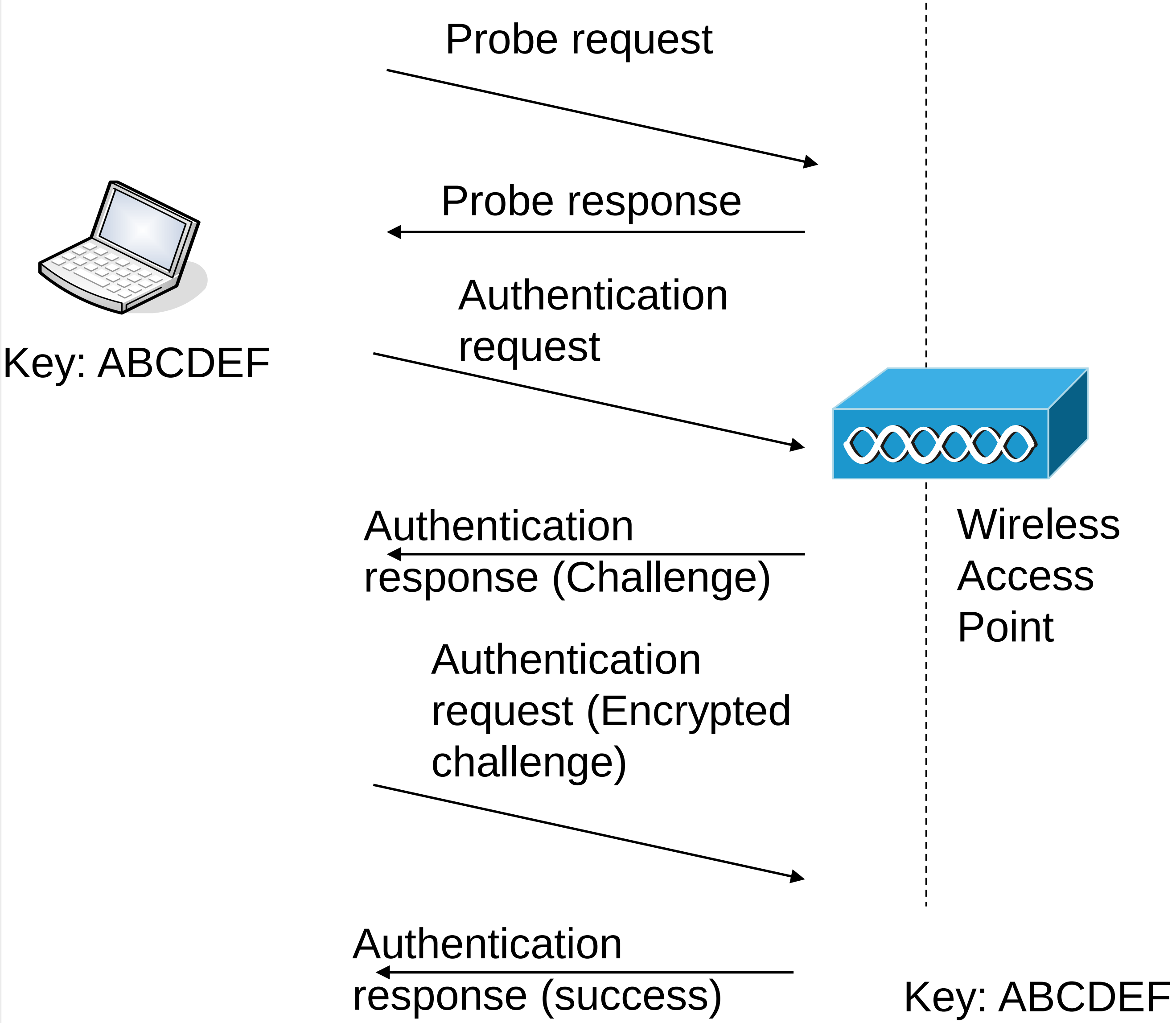
Key: ABCDEF

Wireless Access Point

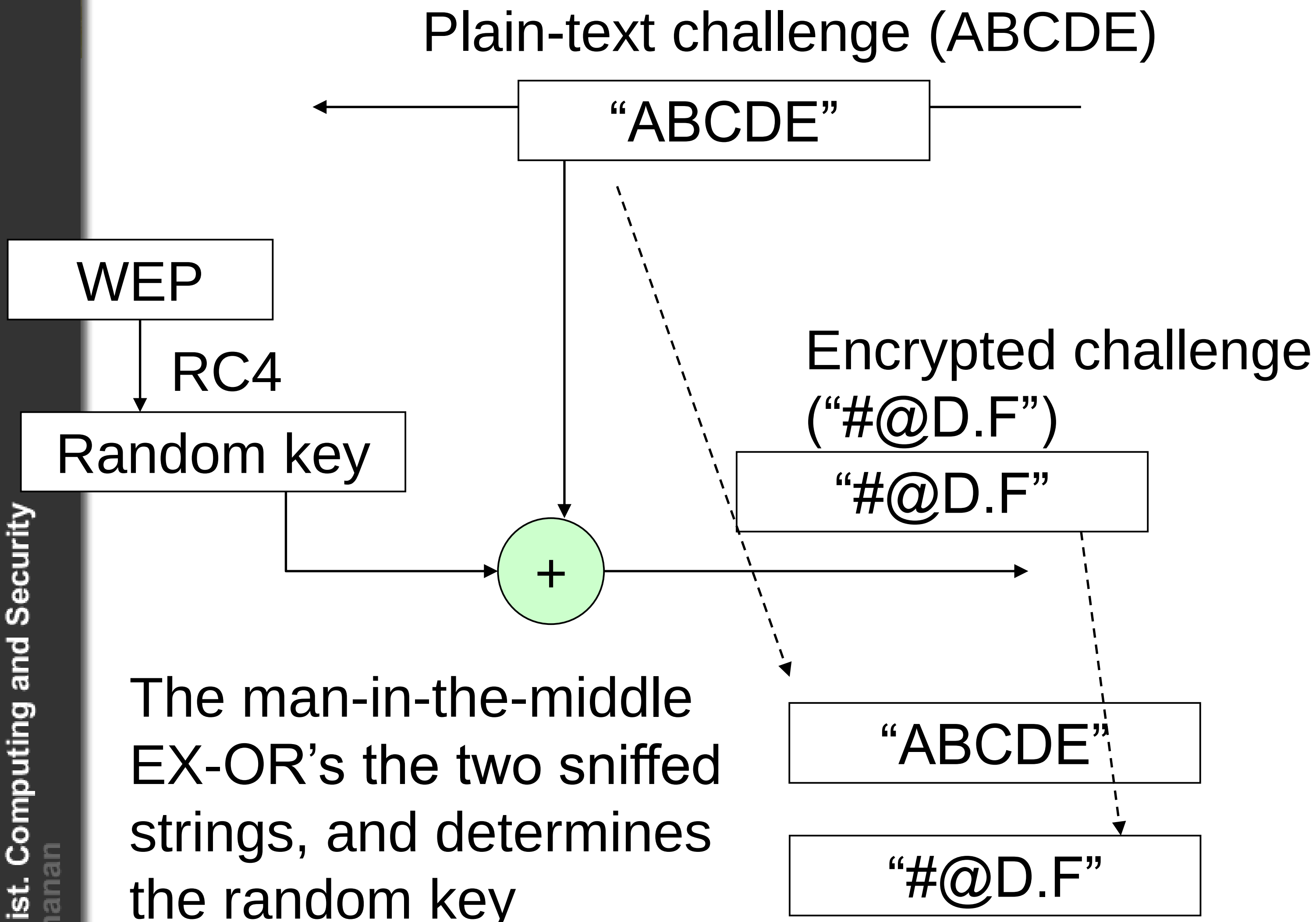
Shared WEP key is used to authenticate the client

Key: ABCDEF

Shared-key authentication

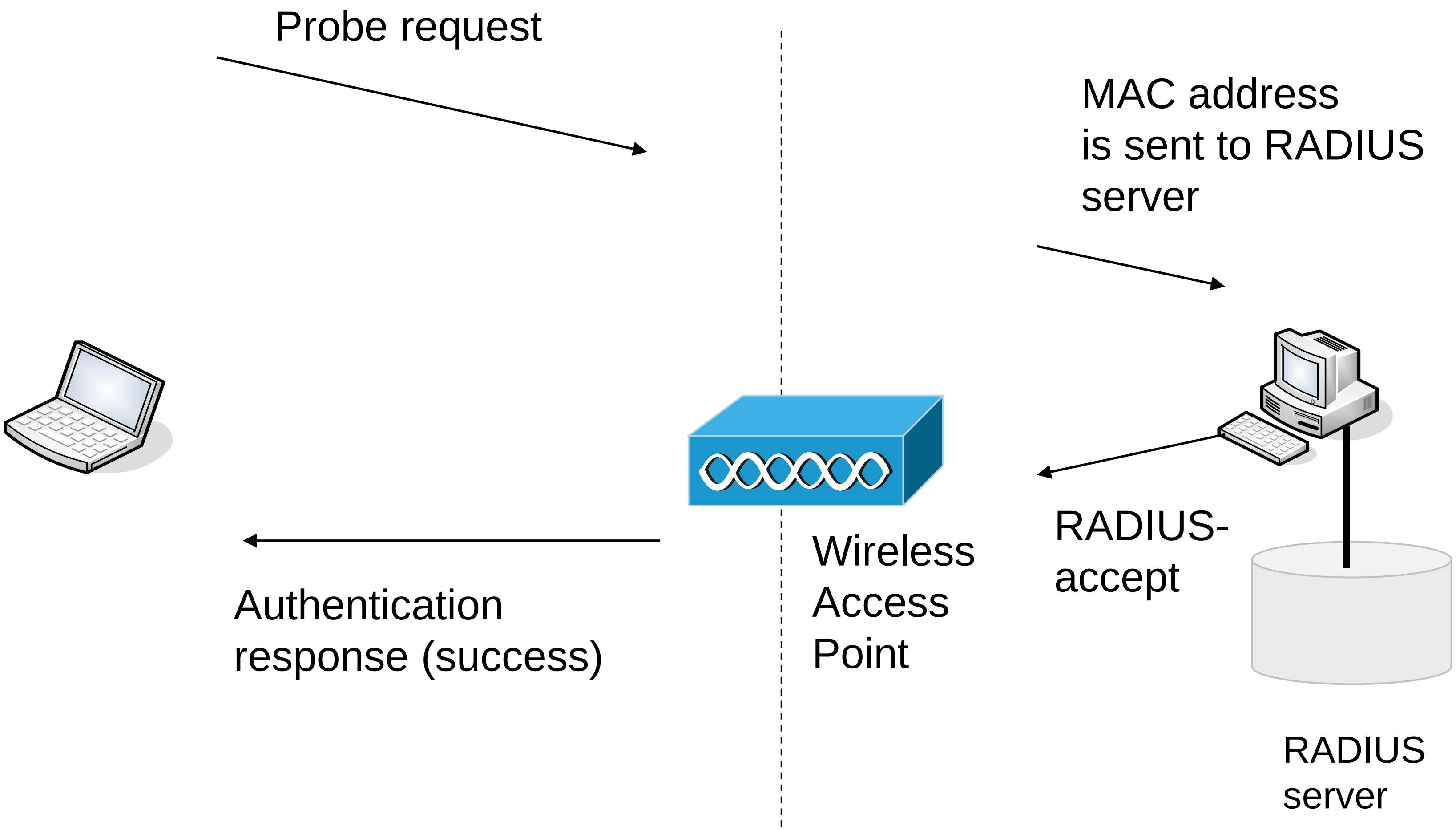

Probe request
Probe response
Authentication request
Key: ABCDEF
Authentication response (Challenge)
Wireless Access Point
Authentication request (Encrypted challenge)
Authentication response (success)
Key: ABCDEF

Weakness of shared-key authentication



The man-in-the-middle EX-OR's the two sniffed strings, and determines the random key

MAC address-based authentication



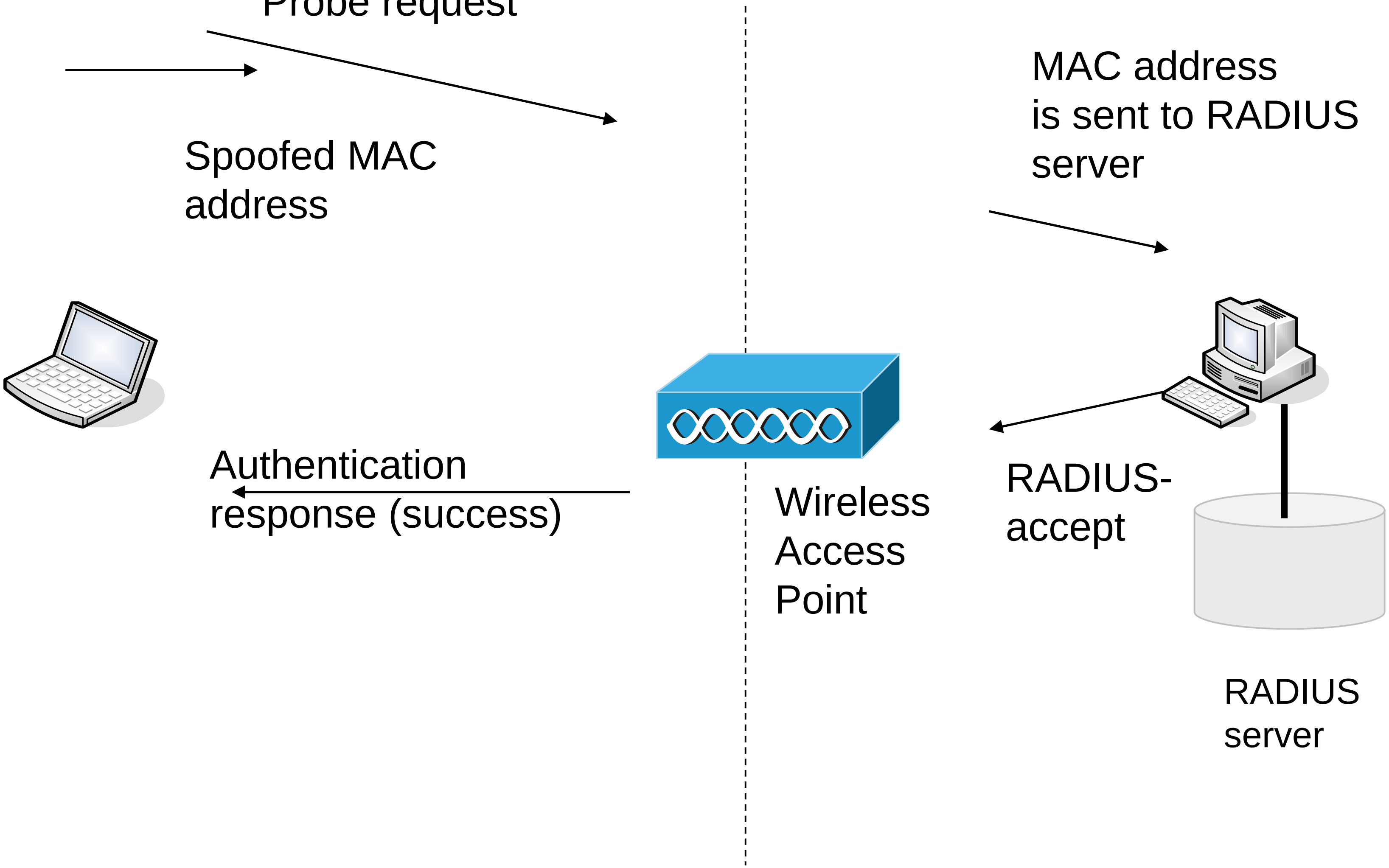
Probe request

MAC address
is sent to RADIUS
server

RADIUS-
accept

Authentication
response (success)

MAC address-based authentication (weakness)



Probe request

Spoofed MAC address

MAC address is sent to RADIUS server

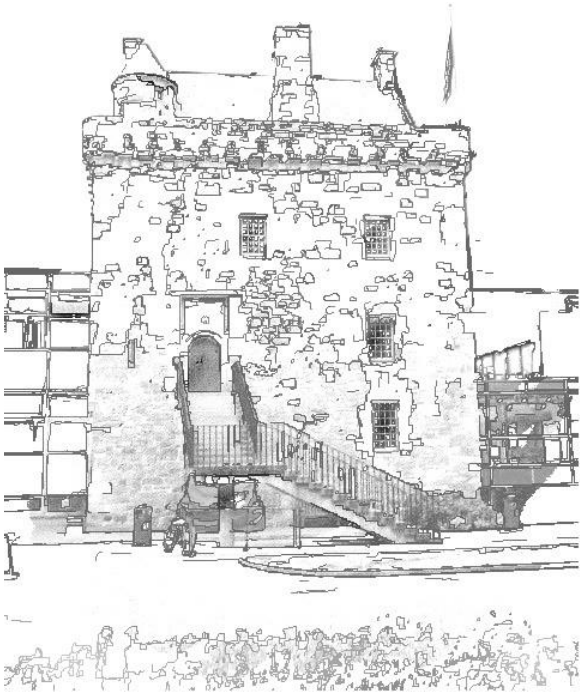
Authentication response (success)

Wireless Access Point

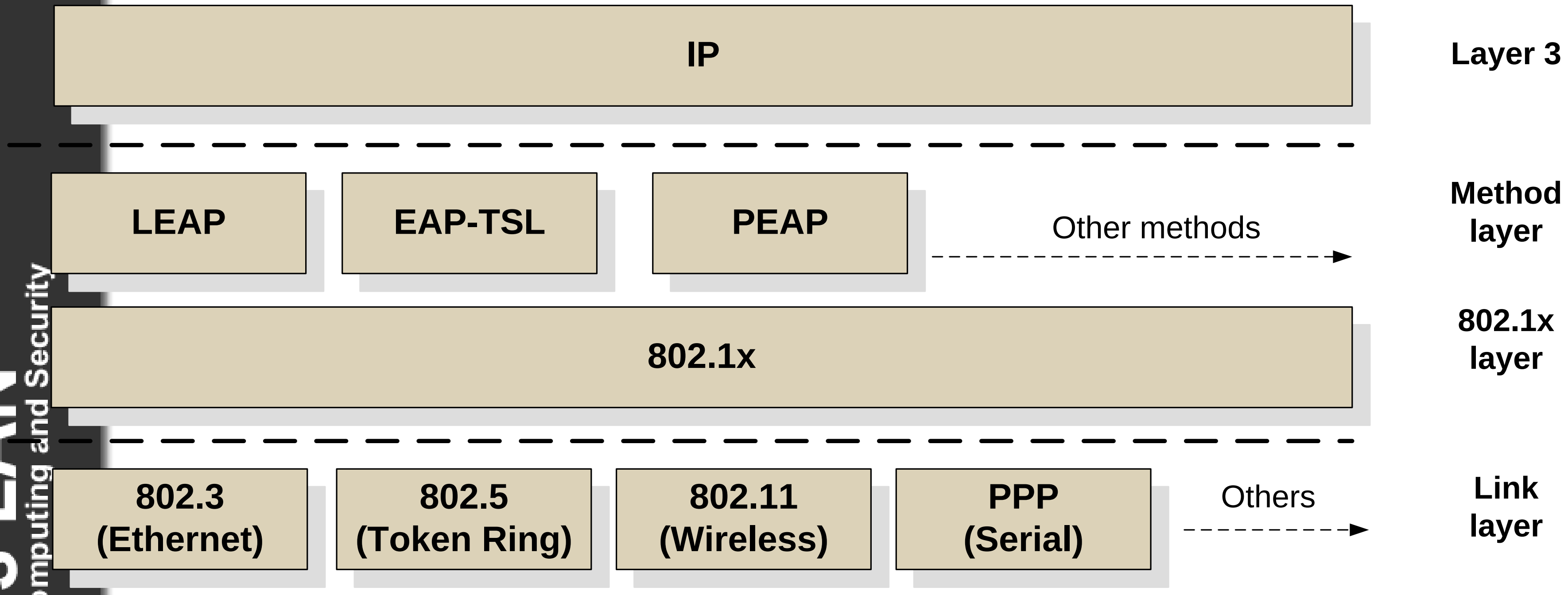
RADIUS-accept

RADIUS server

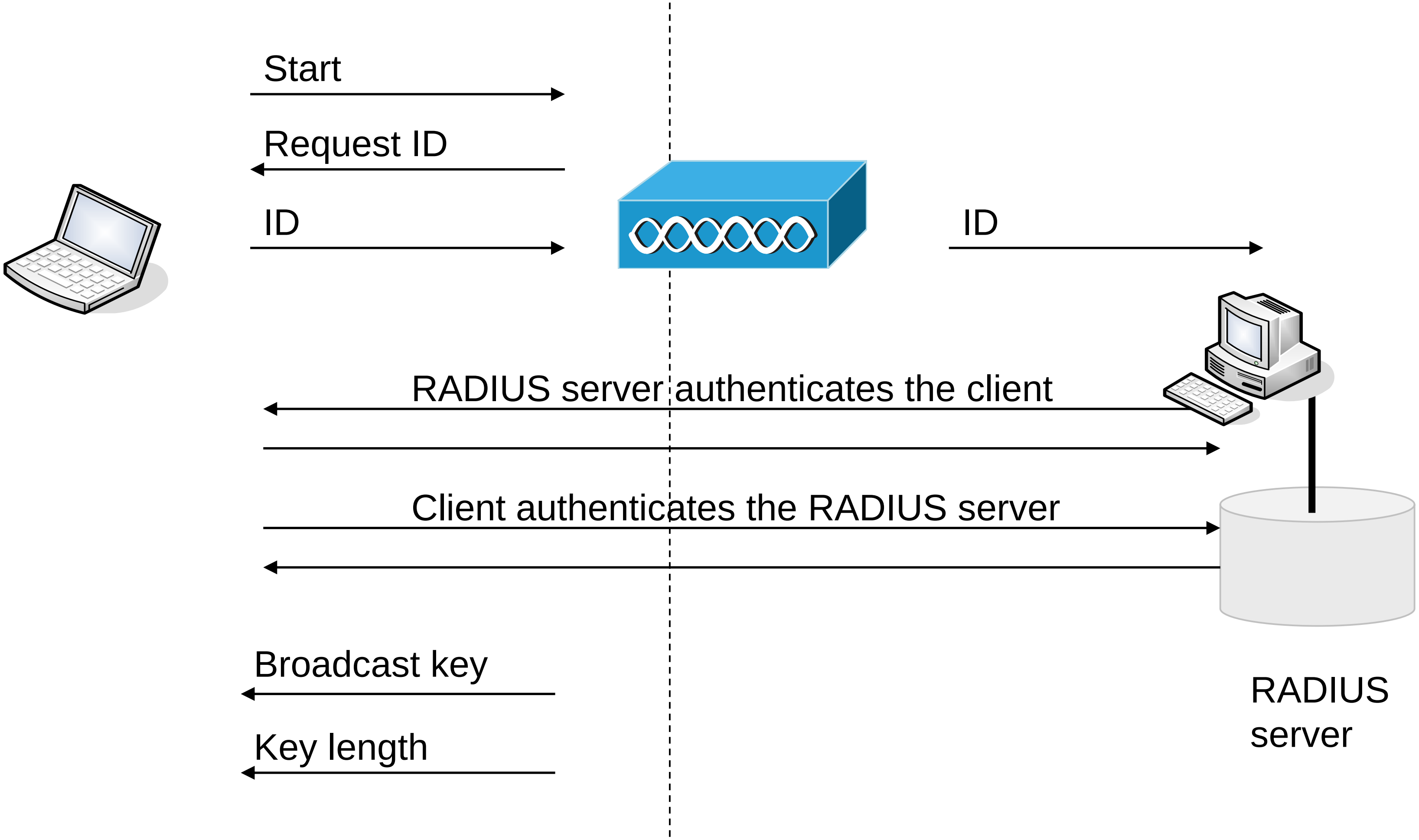
Enhanced Security



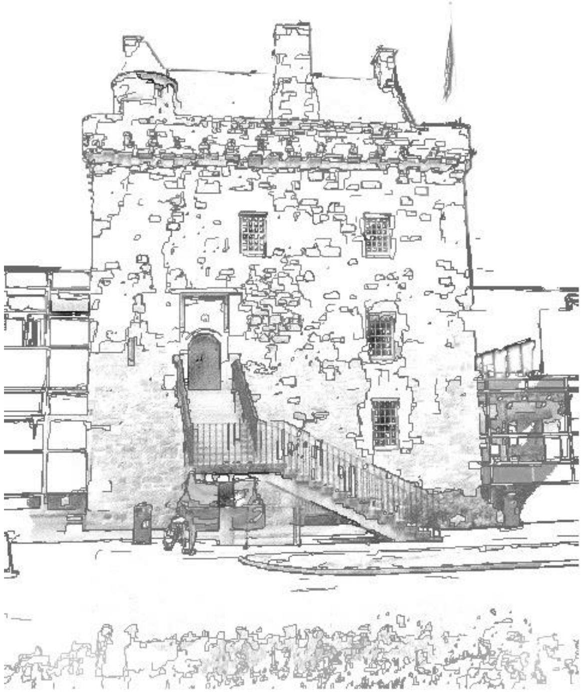
802.1x Framework



802.1X framework


Start
Request ID
ID
ID
RADIUS server authenticates the client
Client authenticates the RADIUS server
Broadcast key
Key length
RADIUS server

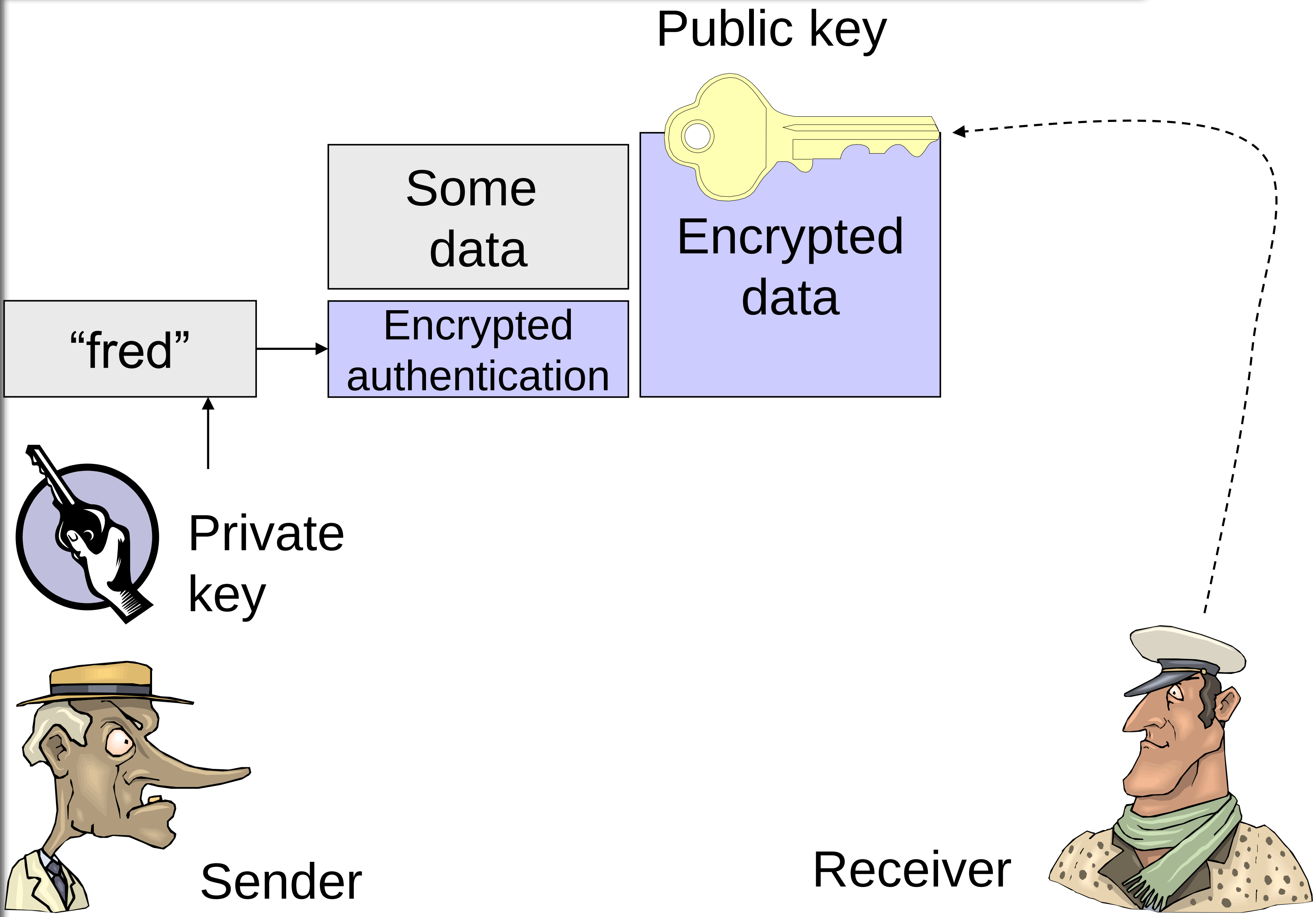
Authenticating using a Digital Certificate

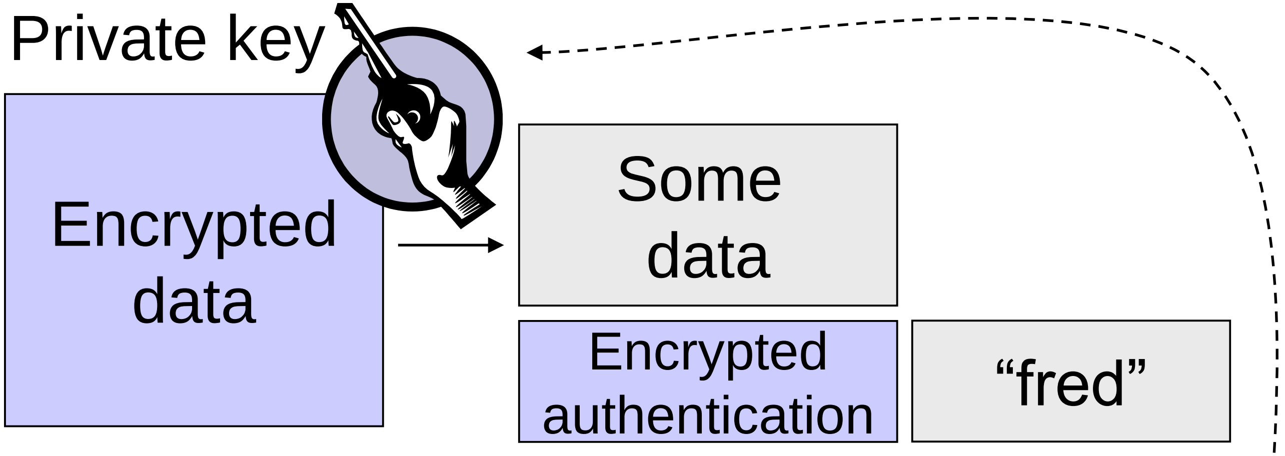


Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

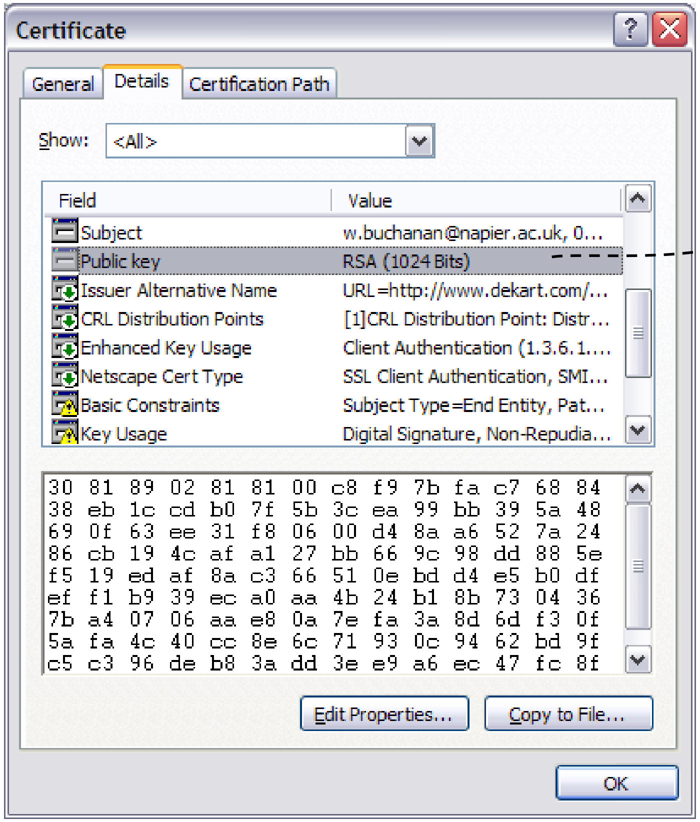
Author: Bill Buchanan

Edinburgh Napier UNIVERSITY


Public key
Some data
Encrypted data
"fred"
Encrypted authentication
Private key
Sender
Receiver



Digital certificate

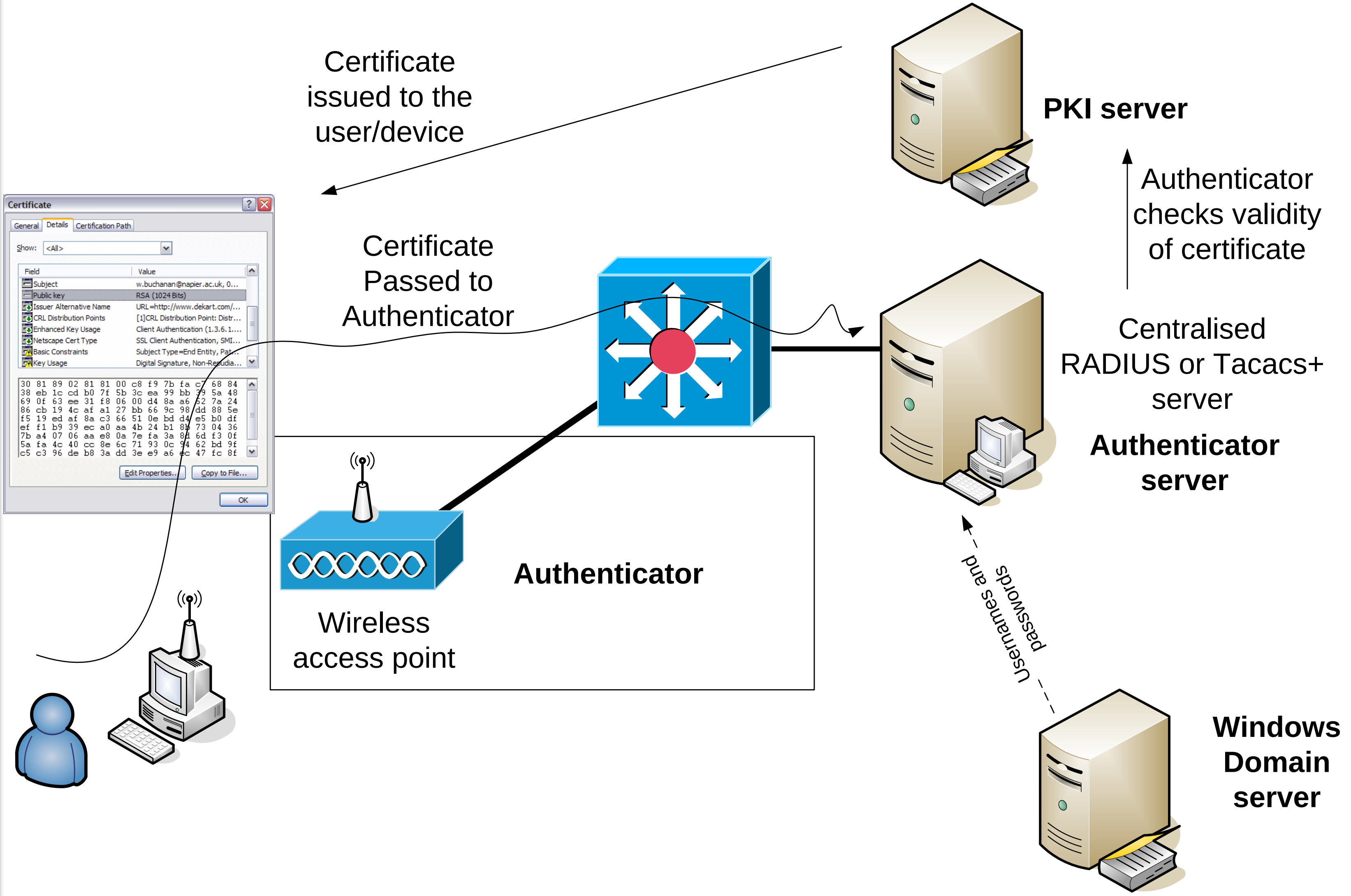

Certificate

Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

Public key is used to decrypt authentication

Edinburgh Napier UNIVERSITY



Certificate issued to the user/device
PKI server
Authenticator checks validity of certificate
Certificate Passed to Authenticator
Centralised RADIUS or Tacacs+ server
Authenticator server
Authenticator
Wireless access point
Usernames and passwords
Windows Domain server

Certificate

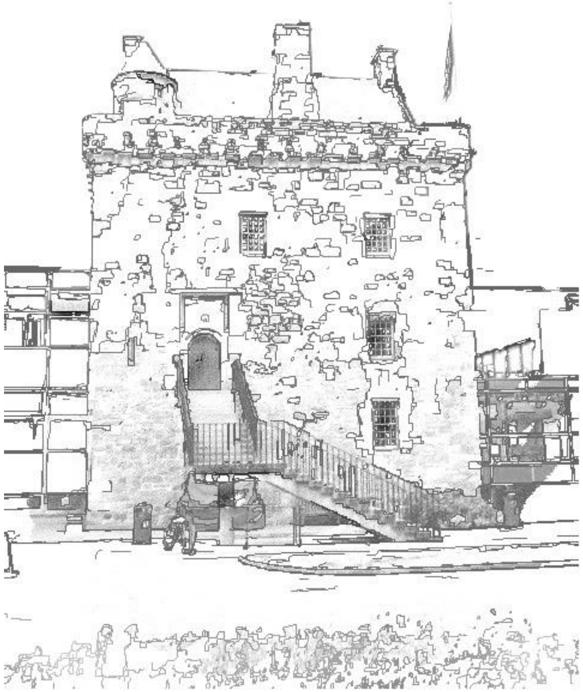
General | Details | Certification Path

Show: <All>

Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

EAP



EAP - Efficient Application Protocols

EAP 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 and EAP.

This is:

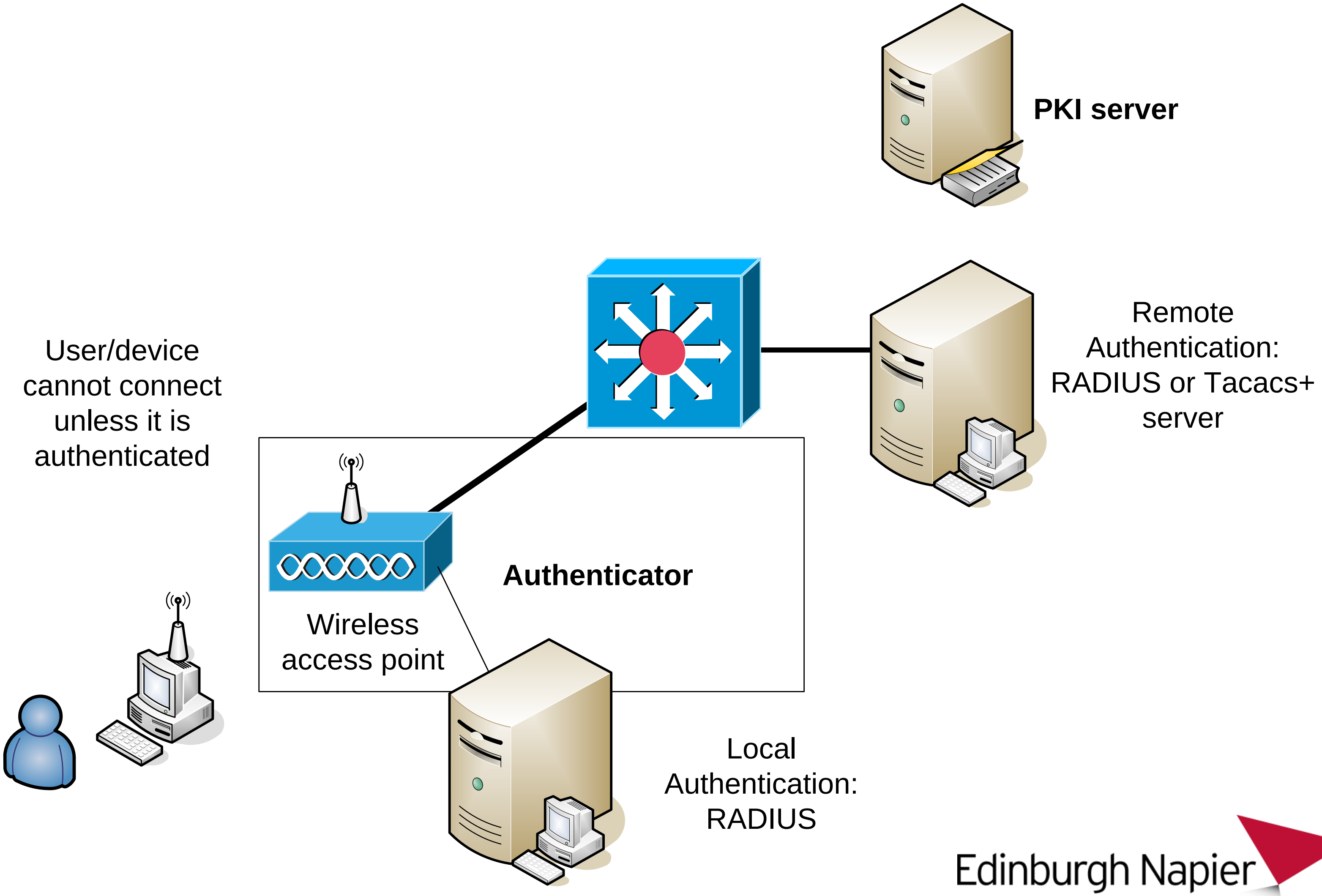
Authentication. This is of both the client and the authentication server (such as a RADIUS server).
Encryption keys. These are dynamically created after authentication. They are not common to the whole network.
Centralized policy control. A session time-out generates a reauthentication and the generation of new encryption keys.

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.

There are many versions of EAP, including:

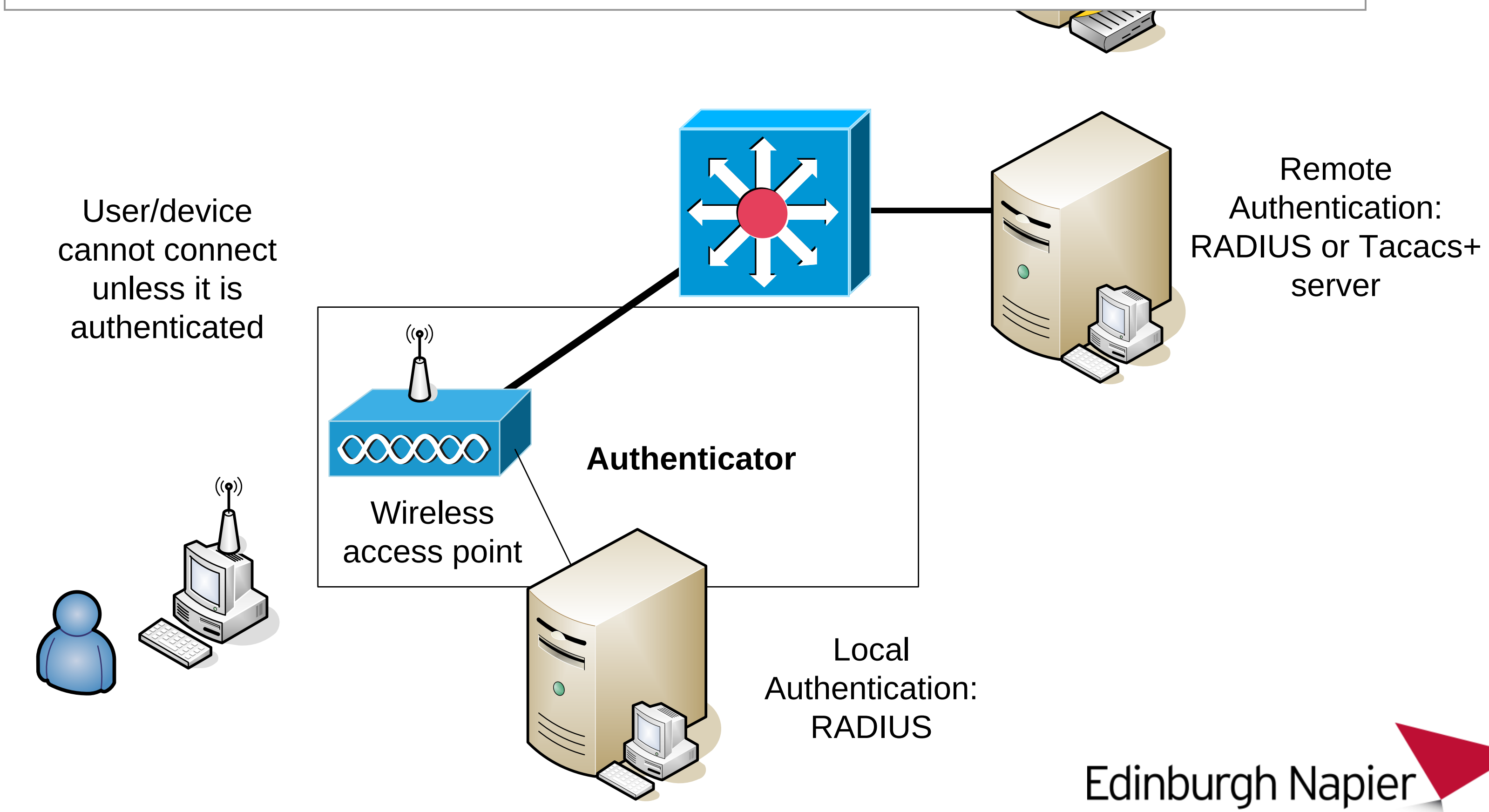
- **LEAP** - Lightweight EAP … EAP-FAST (Flexible Authentication Secure Tunnelling).
- **EAP-TLS** - EAP-Transport Layer Security.
- **PEAP** - Protected EAP.
- **EAP-TTLS** - EAP-Tunnelled TLS.
- **EAP-SIM** - EAP-Subscriber Identity Module.
- **EAP-MD5** – Simple authentication.

EAPs


PKI server
Remote Authentication: RADIUS or Tacacs+ server
User/device cannot connect unless it is authenticated
Authenticator
Wireless access point
Local Authentication: RADIUS

EAPs

1. Client associates with the access point.
2. Client provides authentication details.
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.



User/device cannot connect unless it is authenticated

Authenticator

Wireless access point

Remote Authentication: RADIUS or Tacacs+ server

Local Authentication: RADIUS

EAPs

Client details:

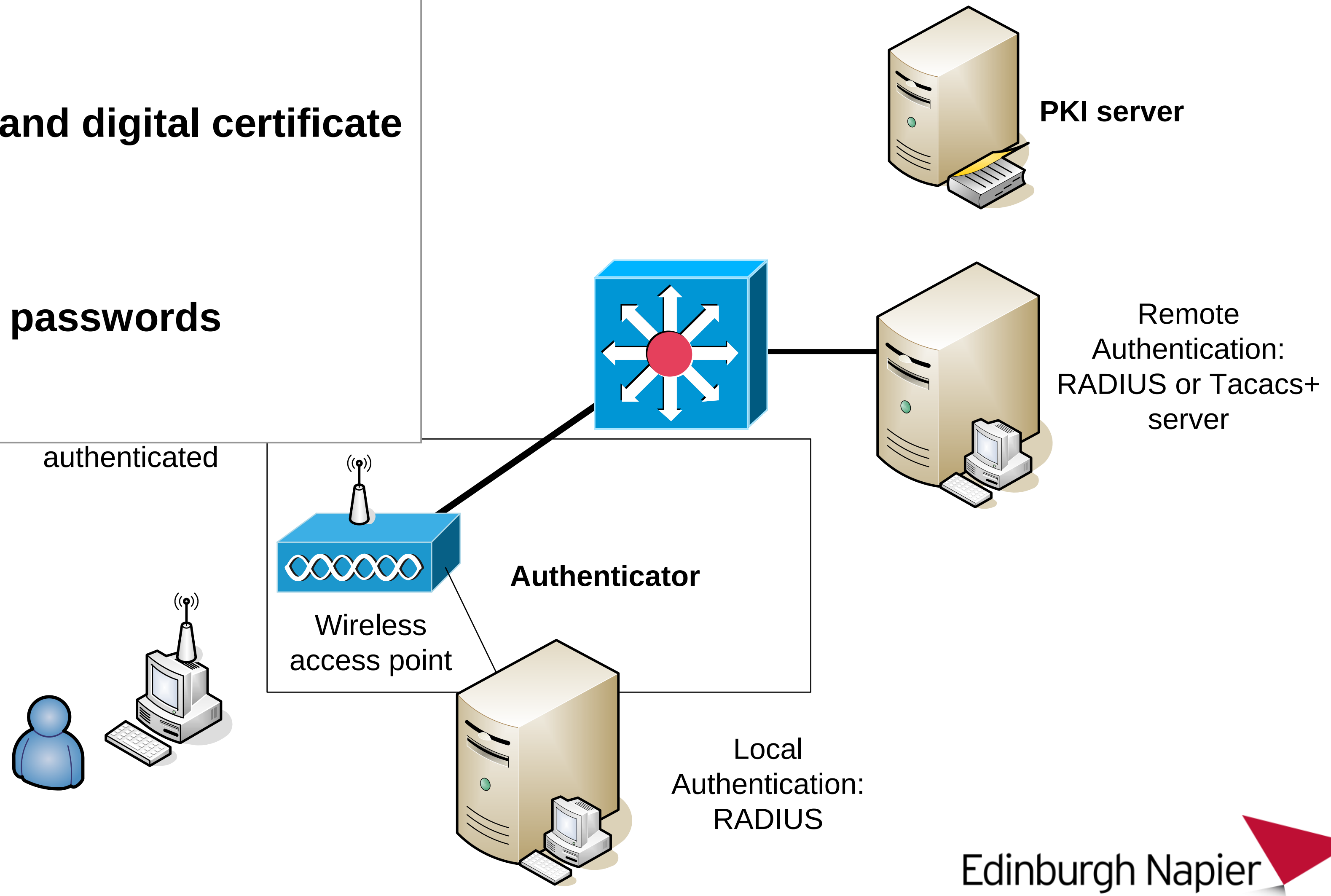
User ID and password.

Or

User ID and digital certificate

Or

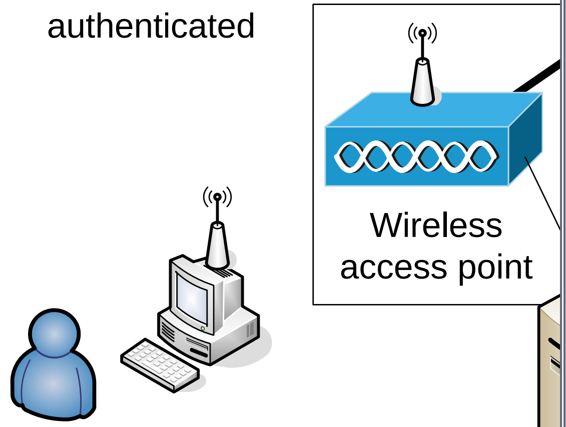
On-time passwords

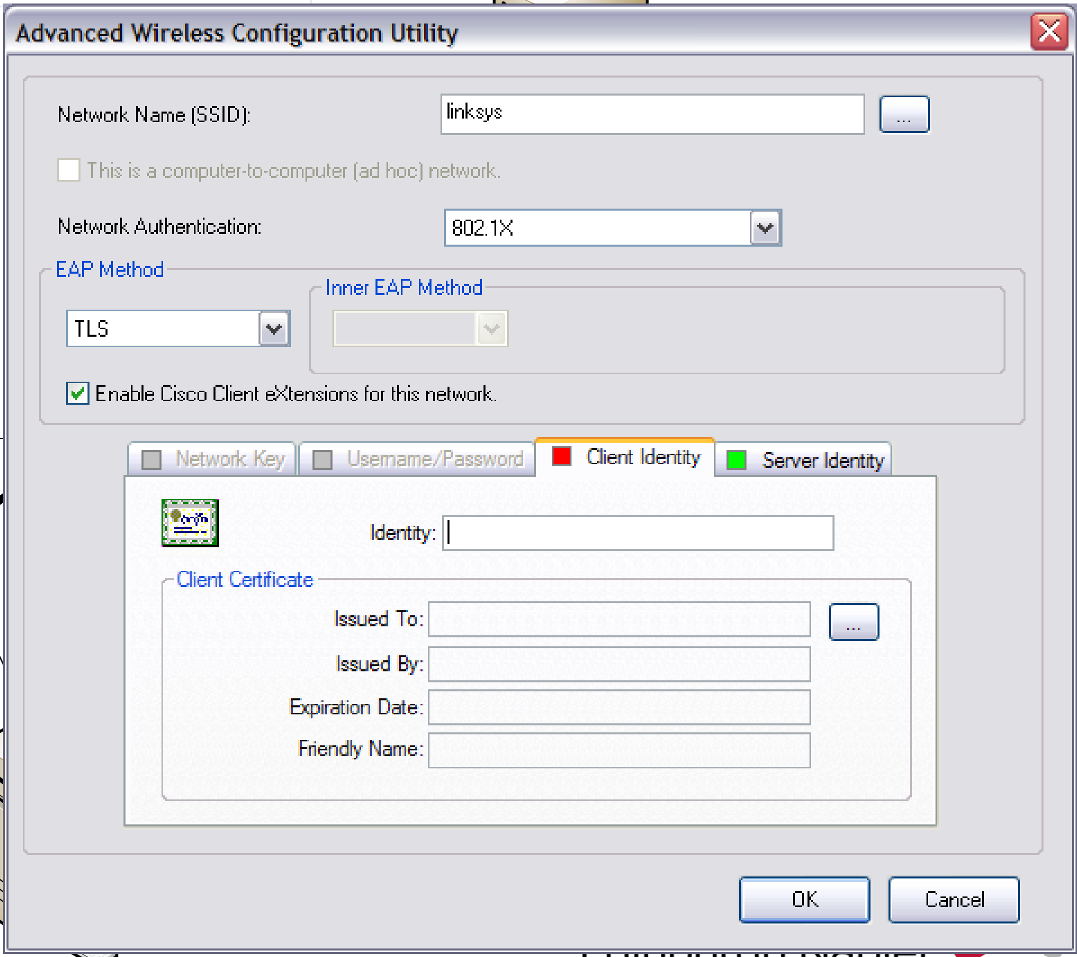

authenticated
PKI server
Remote Authentication: RADIUS or Tacacs+ server
Authenticator
Wireless access point
Local Authentication: RADIUS

EAP-TLS

User Authentication:	User ID and digital certificate
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Client Certificate
Open Standard:	Yes
User differentiation:	Group
Certificate:	RADIUS server/WLAN client

User/device cannot connect unless it is authenticated




Advanced Wireless Configuration Utility

Network Name (SSID): linksys

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: 802.1X

EAP Method: TLS

Inner EAP Method:

☑ Enable Cisco Client eXtensions for this network.

Identity:

Client Certificate

Issued To:

Issued By:

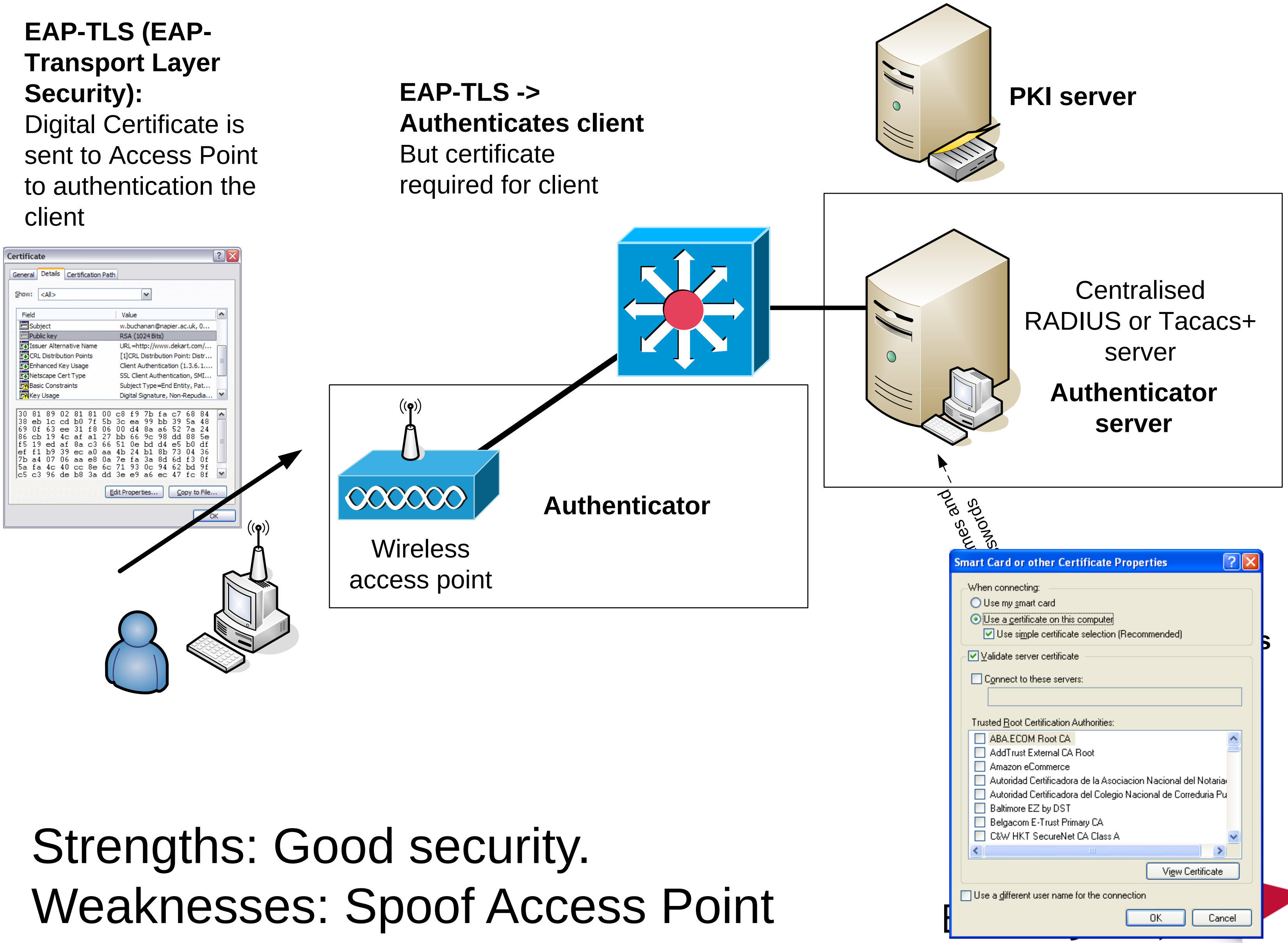
Expiration Date:

Friendly Name:

EAP-TLS

EAP-TLS (EAP-Transport Layer Security): Digital Certificate is sent to Access Point to authentication the client

EAP-TLS -> Authenticates client
But certificate required for client



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

Edit Properties... | Copy to File... | OK

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card
● Use a certificate on this computer
☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ AddTrust External CA Root
□ Amazon eCommerce
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A

View Certificate

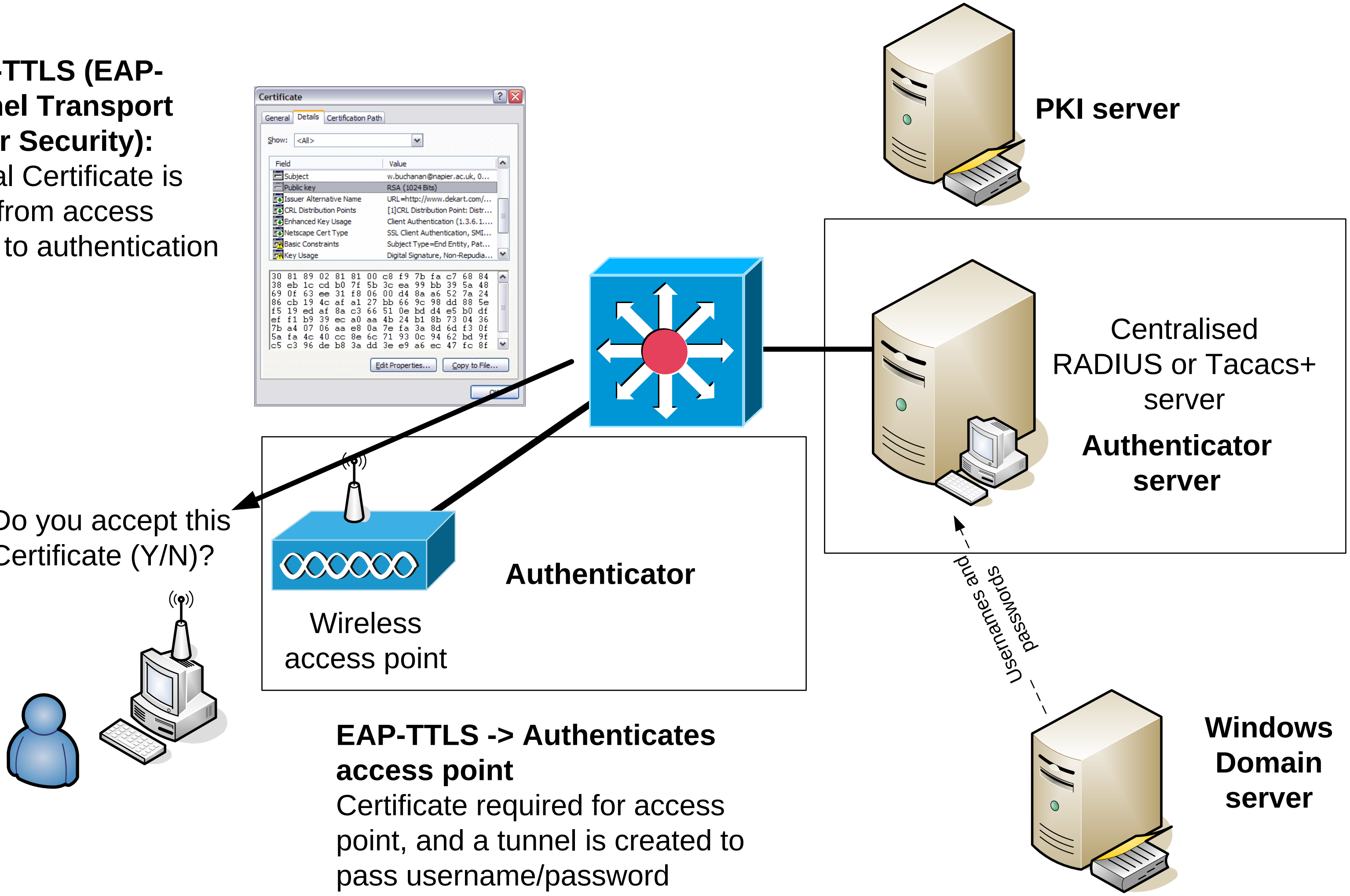
□ Use a different user name for the connection

OK | Cancel

Strengths: Good security.
Weaknesses: Spoof Access Point

EAP-TTLS

EAP-TTLS (EAP-Tunnel Transport Layer Security): Digital Certificate is sent from access point to authentication itself



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

EAP-TTLS -> Authenticates access point
Certificate required for access point, and a tunnel is created to pass username/password

Strengths: Good security.
Weaknesses: Spoof Client

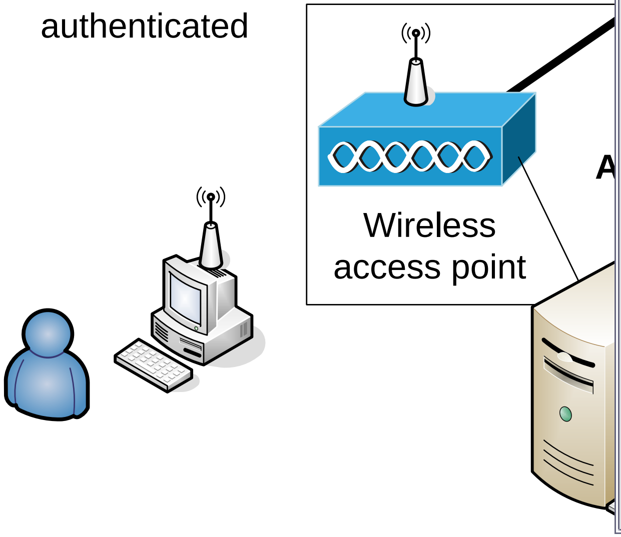
LEAP

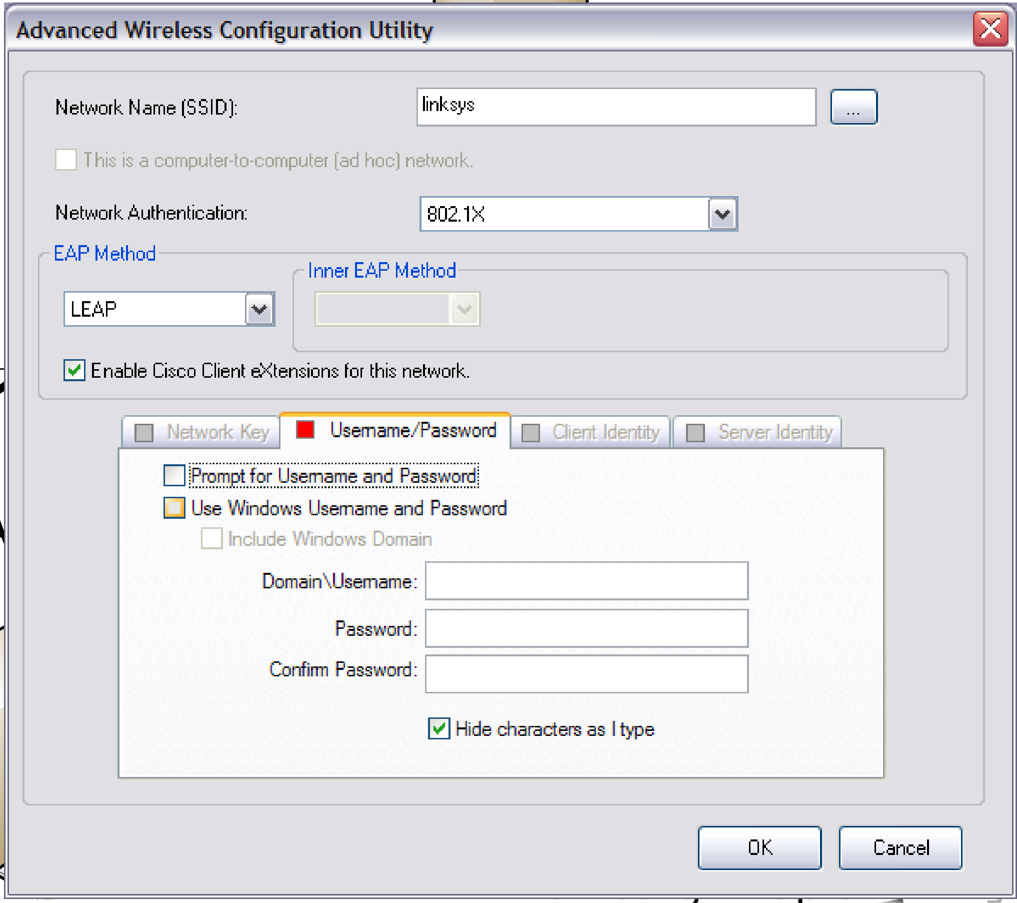
User Authentication:	User ID and password
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Not Supported
Open Standard:	No (Cisco-derived)
User differentiation:	Group
Certificate:	None

LEAPs is open to attack from a dictionary attack. **Use strong passwords!!!**

PKI server

User/device cannot connect unless it is authenticated




Advanced Wireless Configuration Utility

Network Name (SSID): linksys

☐ This is a computer-to-computer (ad hoc) network.

Network Authentication: 802.1X

EAP Method: LEAP

Inner EAP Method:

☑ Enable Cisco Client eXtensions for this network.

☐ Prompt for Username and Password

☐ Use Windows Username and Password

☐ Include Windows Domain

Domain\Username:

Password:

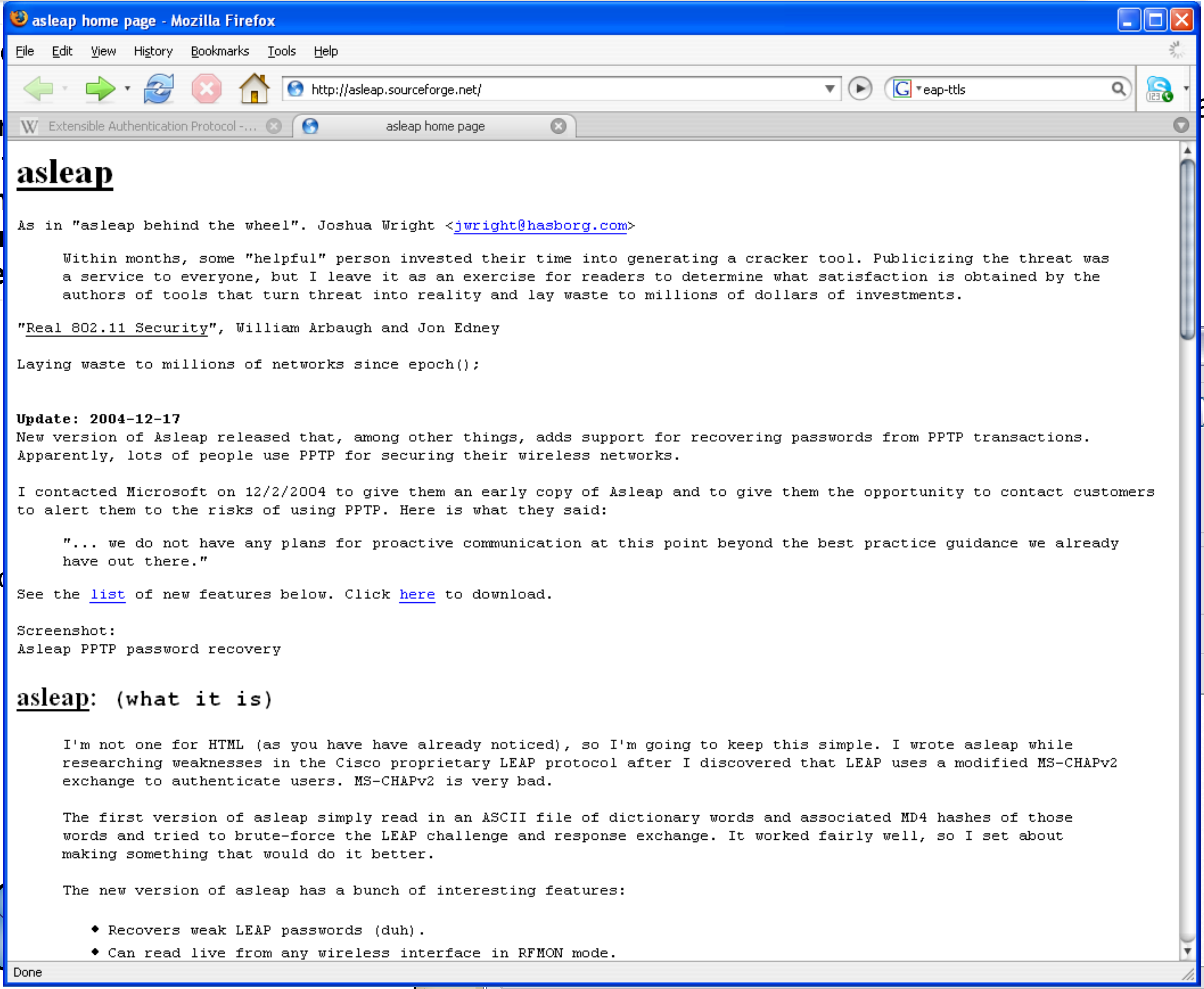
Confirm Password:

☑ Hide characters as I type

LEAP … ASLEAP

User Auth
Key size:
Encryption
Device Au
Open Star
User differ
Certificate

ack.



asleap home page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://asleap.sourceforge.net/
eap-ttls
Extensible Authentication Protocol -...
asleap home page
Done

asleap

As in "asleap behind the wheel". Joshua Wright <jwright@hasborg.com>

> Within months, some "helpful" person invested their time into generating a cracker tool. Publicizing the threat was a service to everyone, but I leave it as an exercise for readers to determine what satisfaction is obtained by the authors of tools that turn threat into reality and lay waste to millions of dollars of investments.

"Real 802.11 Security", William Arbaugh and Jon Edney

Laying waste to millions of networks since epoch();

Update: 2004-12-17
New version of Asleap released that, among other things, adds support for recovering passwords from PPTP transactions. Apparently, lots of people use PPTP for securing their wireless networks.

I contacted Microsoft on 12/2/2004 to give them an early copy of Asleap and to give them the opportunity to contact customers to alert them to the risks of using PPTP. Here is what they said:

> "... we do not have any plans for proactive communication at this point beyond the best practice guidance we already have out there."

See the list of new features below. Click here to download.

Screenshot:
Asleap PPTP password recovery

asleap: (what it is)

I'm not one for HTML (as you have have already noticed), so I'm going to keep this simple. I wrote asleap while researching weaknesses in the Cisco proprietary LEAP protocol after I discovered that LEAP uses a modified MS-CHAPv2 exchange to authenticate users. MS-CHAPv2 is very bad.

The first version of asleap simply read in an ASCII file of dictionary words and associated MD4 hashes of those words and tried to brute-force the LEAP challenge and response exchange. It worked fairly well, so I set about making something that would do it better.

The new version of asleap has a bunch of interesting features:

- Recovers weak LEAP passwords (duh).
- Can read live from any wireless interface in RFMON mode.

OK Cancel

UNIVERSITY

LEAP

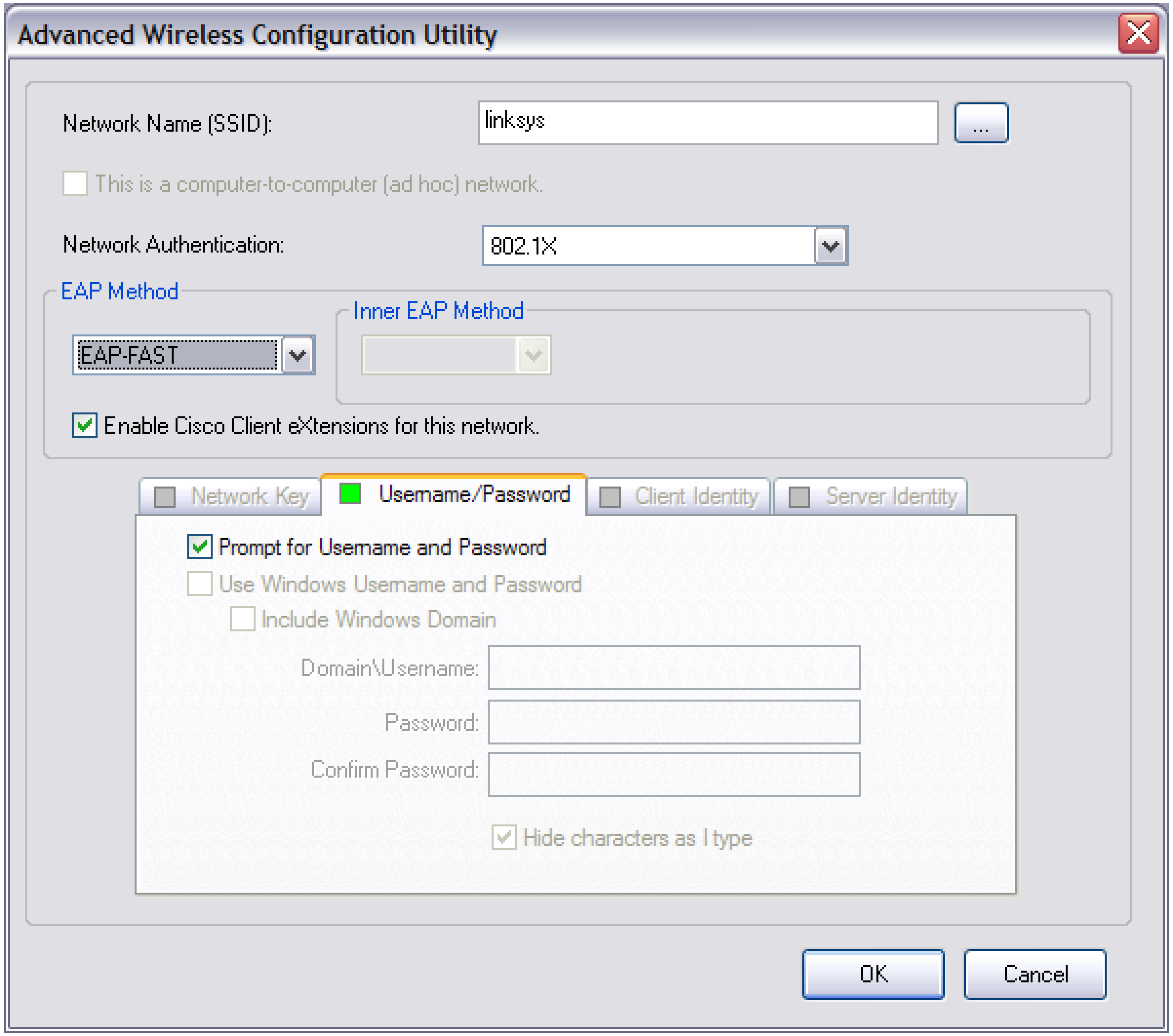
LEAPs uses MS-CHAP (Microsoft Handshake Authentication Protocol) to continually challenge the device for its ID. It uses a challenge-response, mutual authentication protocol using Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating device challenges the client and vice-versa. If either challenge is incorrect, the connection is rejected. The password is converted into password hash 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.

… upated by Cisco with … EAP-FAST (Flexible Authorization Secure Tunnel) so that details are passed through a tunnel.

EAP-FAST



Advanced Wireless Configuration Utility

Network Name (SSID): linksys

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: 802.1X

EAP Method: EAP-FAST

Inner EAP Method:

☑ Enable Cisco Client eXtensions for this network.

☑ Prompt for Username and Password

□ Use Windows Username and Password

□ Include Windows Domain

Domain\Username:

Password:

Confirm Password:

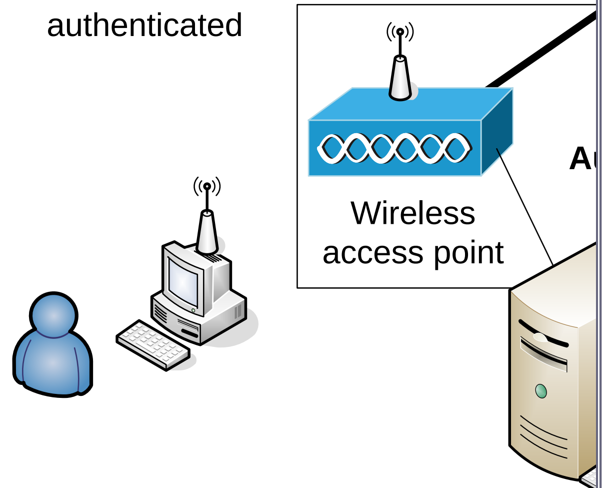
☑ Hide characters as I type

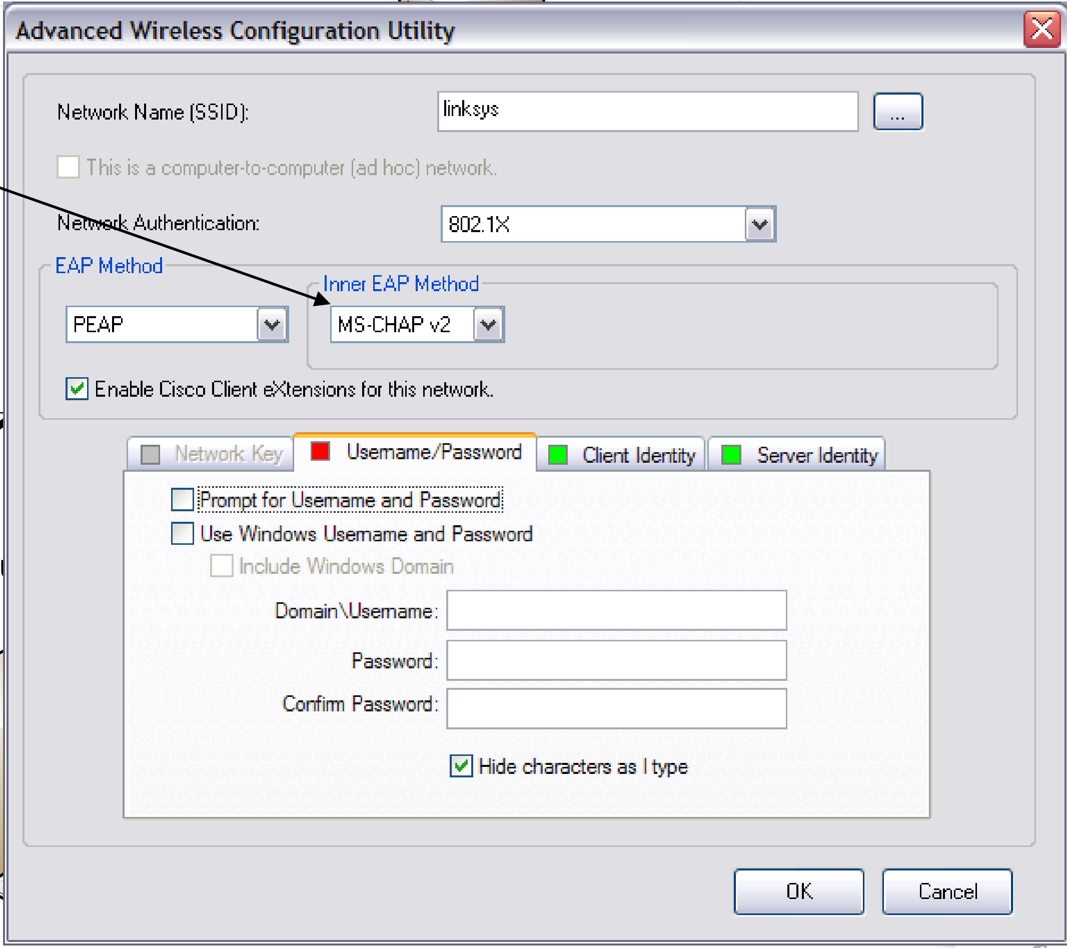
EAP - PEAP

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

MS-CHAP v2
Gives Username/
Password … as Napier

User/device cannot connect unless it is authenticated




Advanced Wireless Configuration Utility

Network Name (SSID): linksys

☐ This is a computer-to-computer (ad hoc) network.

Network Authentication: 802.1X

EAP Method: PEAP

Inner EAP Method: MS-CHAP v2

☑ Enable Cisco Client eXtensions for this network.

▨ Network Key | 🟥 Username/Password | 🟩 Client Identity | 🟩 Server Identity

☐ Prompt for Username and Password

☐ Use Windows Username and Password

☐ Include Windows Domain

Domain\Username:

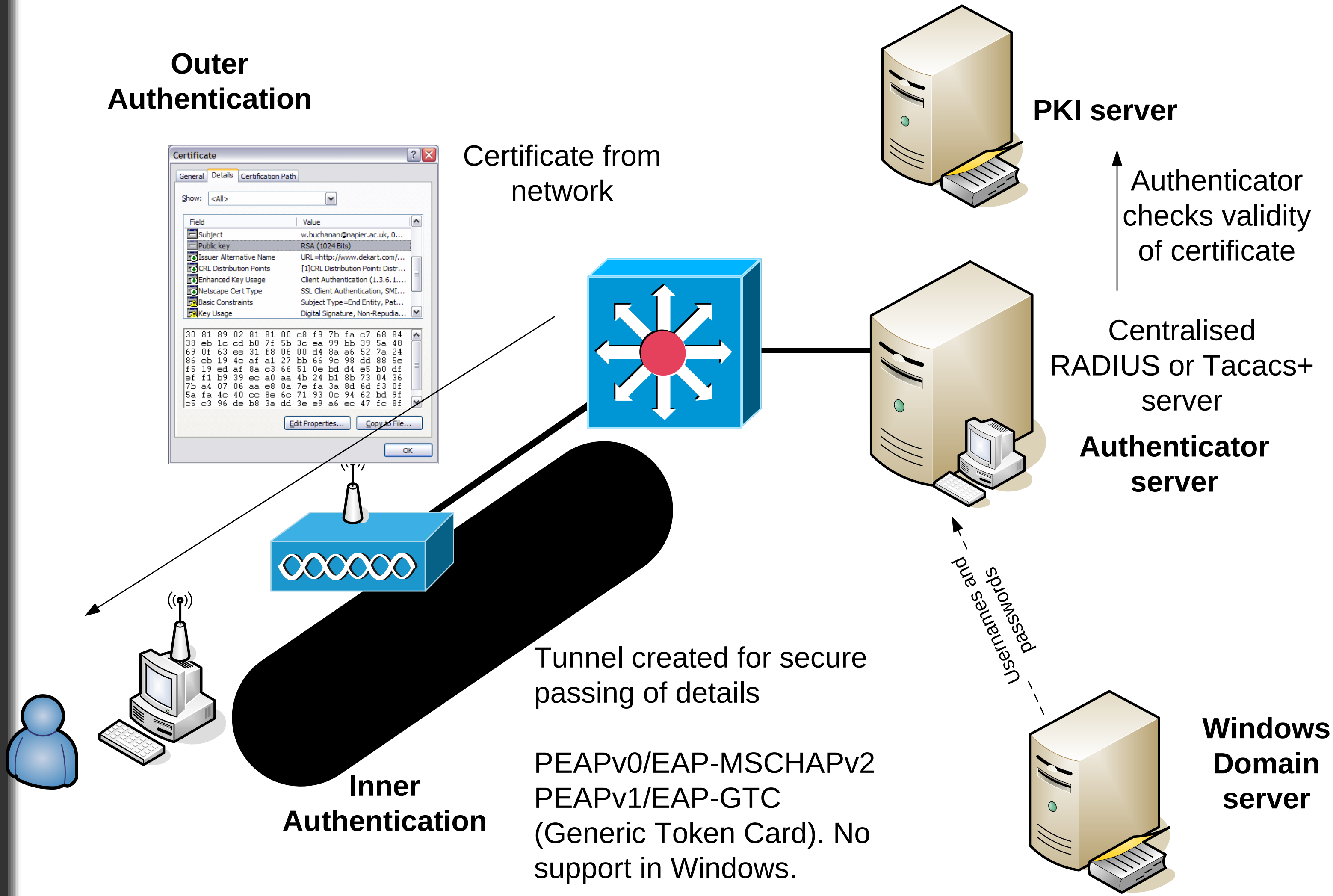
Password:

Confirm Password:

☑ Hide characters as I type

Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

EAP- PEAP



Show: <All>

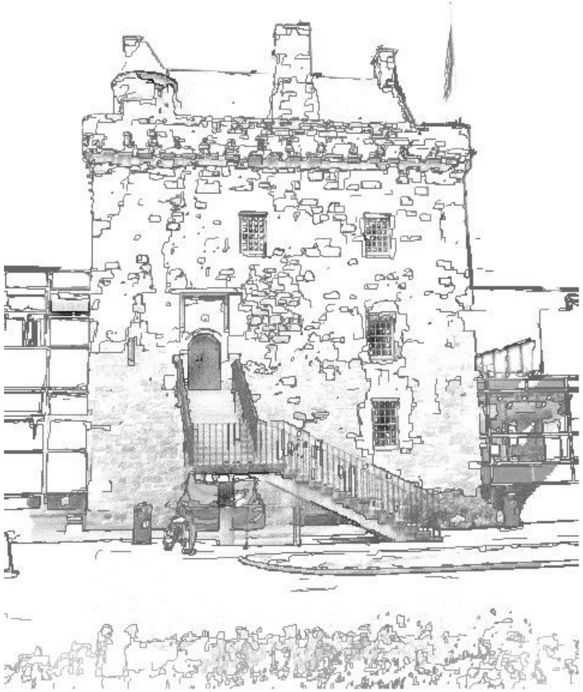
Field	Value
Subject	w.buchanan@napier.ac.uk, 0...
Public key	RSA (1024 Bits)
Issuer Alternative Name	URL=http://www.dekart.com/...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Cert Type	SSL Client Authentication, SMI...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Non-Repudia...

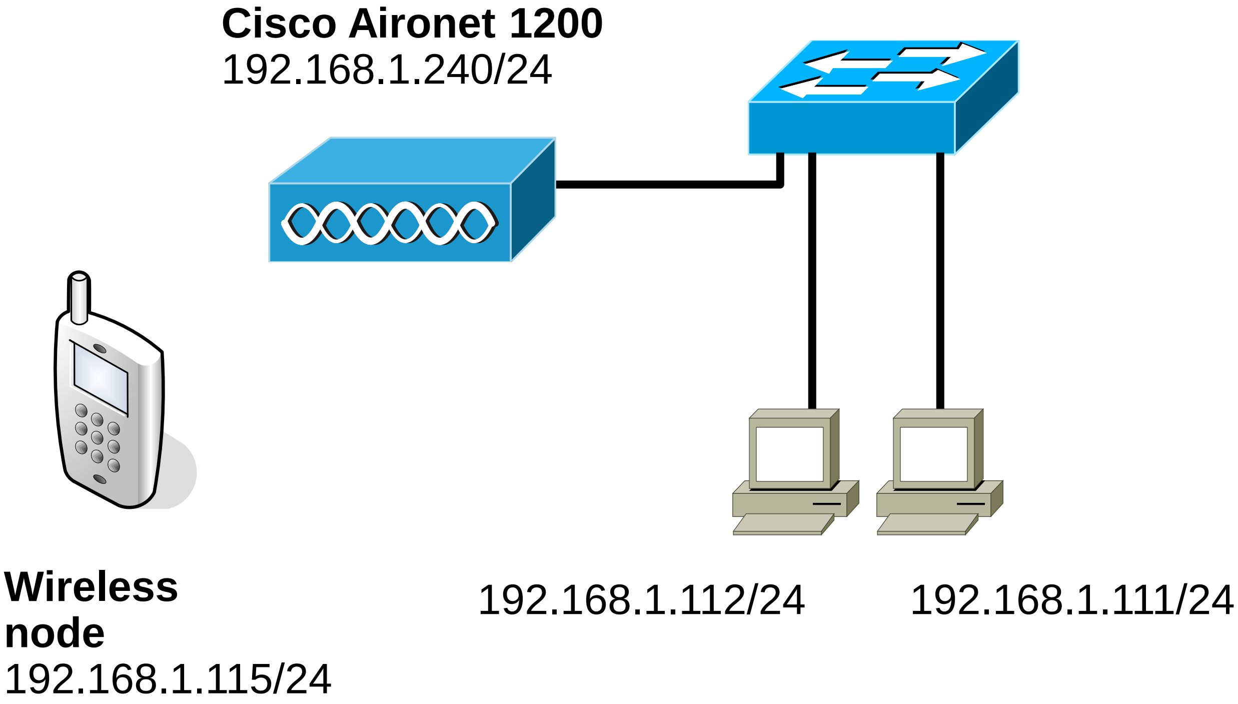
```
30 81 89 02 81 81 00 c8 f9 7b fa c7 68 84
38 eb 1c cd b0 7f 5b 3c ea 99 bb 39 5a 48
69 0f 63 ee 31 f8 06 00 d4 8a a6 52 7a 24
86 cb 19 4c af a1 27 bb 66 9c 98 dd 88 5e
f5 19 ed af 8a c3 66 51 0e bd d4 e5 b0 df
ef f1 b9 39 ec a0 aa 4b 24 b1 8b 73 04 36
7b a4 07 06 aa e8 0a 7e fa 3a 8d 6d f3 0f
5a fa 4c 40 cc 8e 6c 71 93 0c 94 62 bd 9f
c5 c3 96 de b8 3a dd 3e e9 a6 ec 47 fc 8f
```

Tunnel created for secure passing of details

PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC (Generic Token Card). No support in Windows.

Configuration – Local RADIUS server



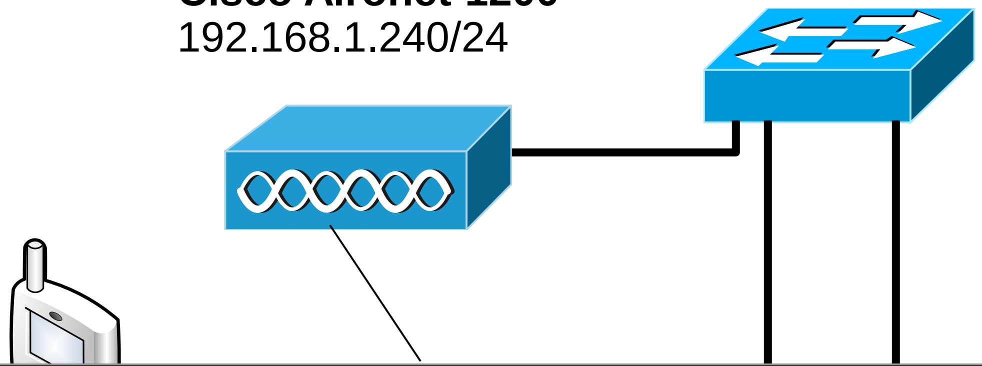


Cisco Aironet 1200
192.168.1.240/24

Wireless node
192.168.1.115/24

192.168.1.112/24

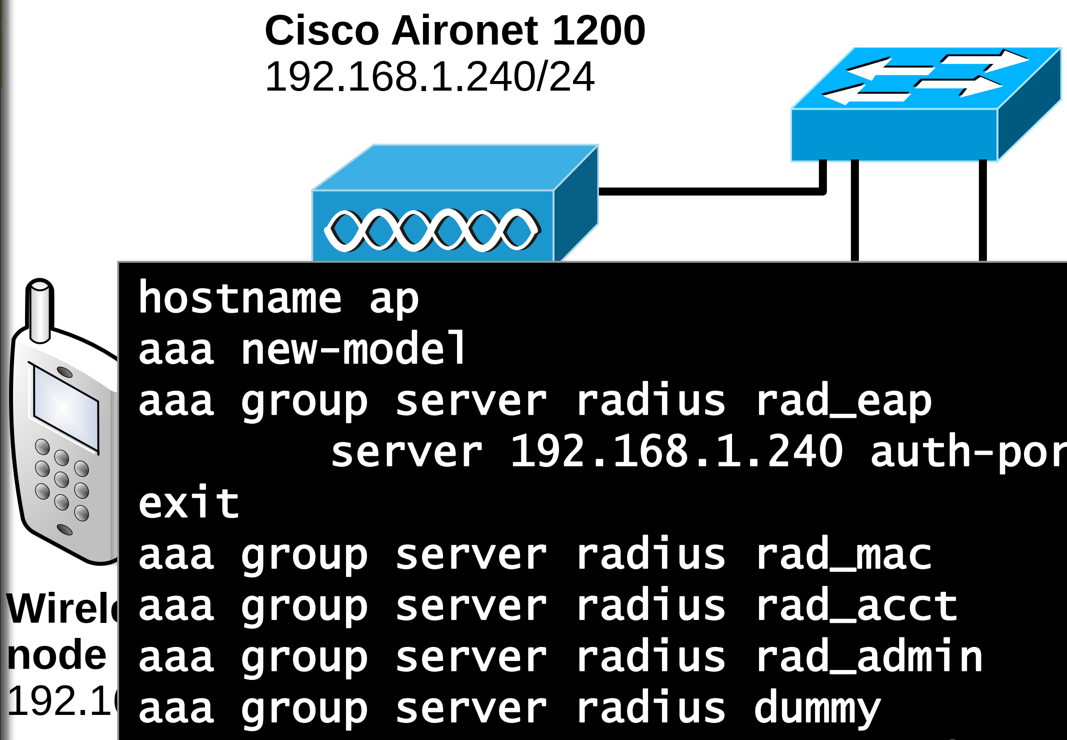
192.168.1.111/24



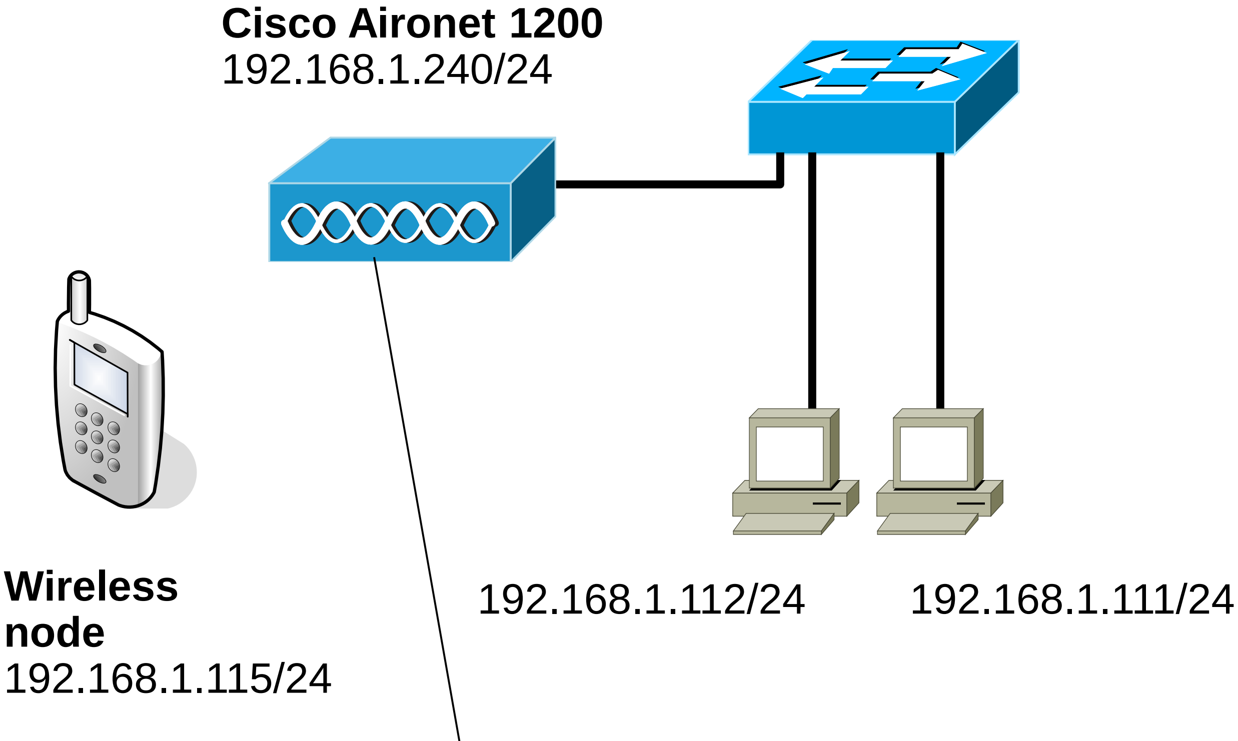
Cisco Aironet 1200
192.168.1.240/24

```
(config) # dot11 ssid NapierSSID
(config-ssid) # authentication network-eap eap_methods
(config-ssid) # exit

(config) # interface Dot11Radio0
(config-if) # encryption key 1 size 40bit AAAAAAAAAA transmit-key
(config-if) # encryption mode ciphers wep40
(config-if) # no ssid tsunami
(config-if) # ssid NapierSSID
(config-if) # channel 1
(config-if) # guest-mode
(config-if) # station-role root
(config-if) # exit
(config) # interface BVI1
(config-if) # ip address 192.168.1.240 255.255.255.0
(config-if) # exit
(config) # ip http server
```



```
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
```



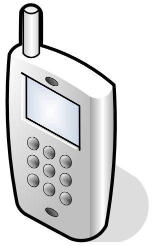
Cisco Aironet 1200
192.168.1.240/24

Wireless node
192.168.1.115/24

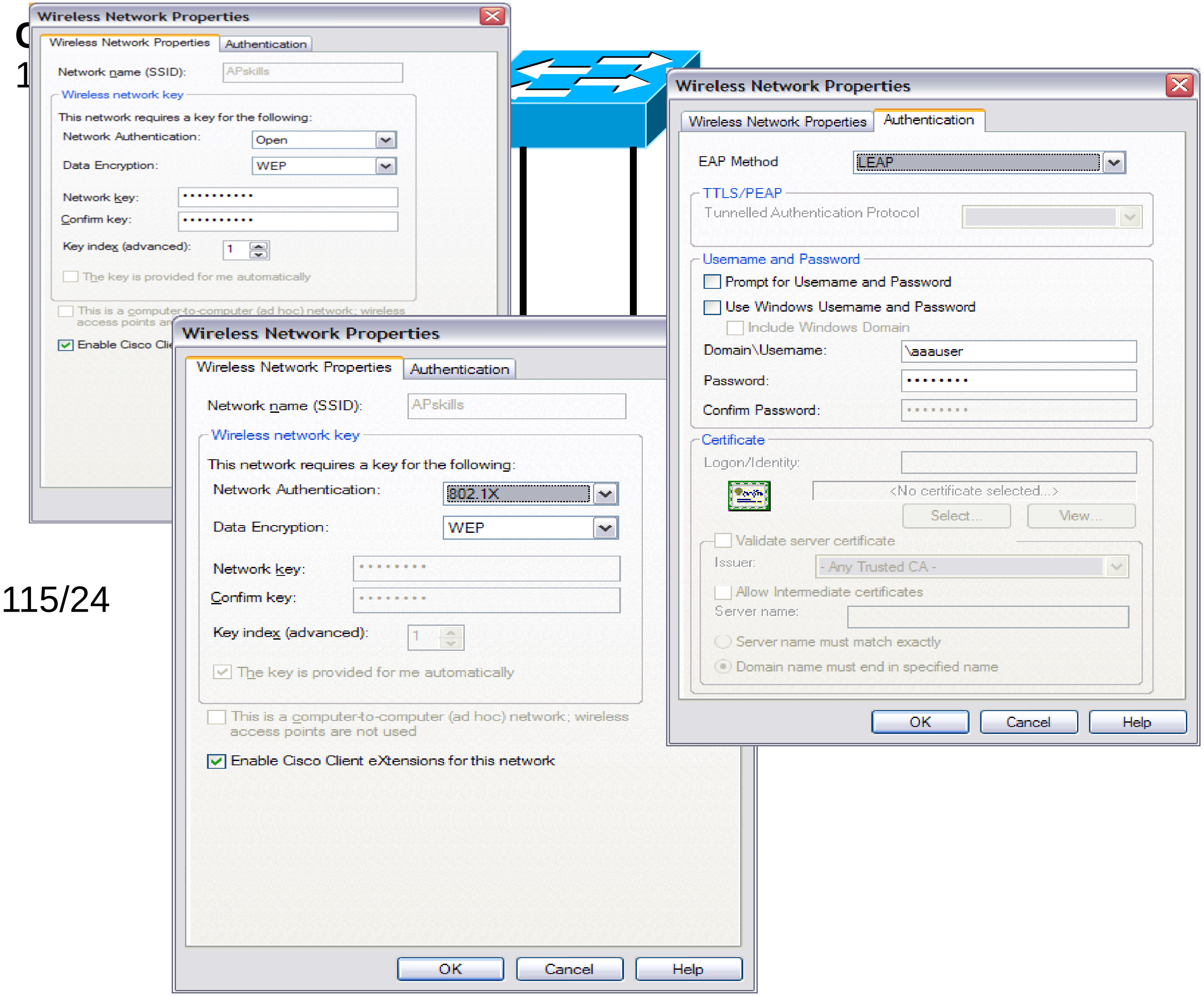
192.168.1.112/24

192.168.1.111/24

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



Wireless node
192.168.1.115/24



Wireless Network Properties

Wireless Network Properties | Authentication

Network name (SSID): APskills

Wireless network key

This network requires a key for the following:

Network Authentication: Open

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 ar

☑ Enable Cisco Clie

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

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...>

□ Validate server certificate

Issuer: - Any Trusted CA -

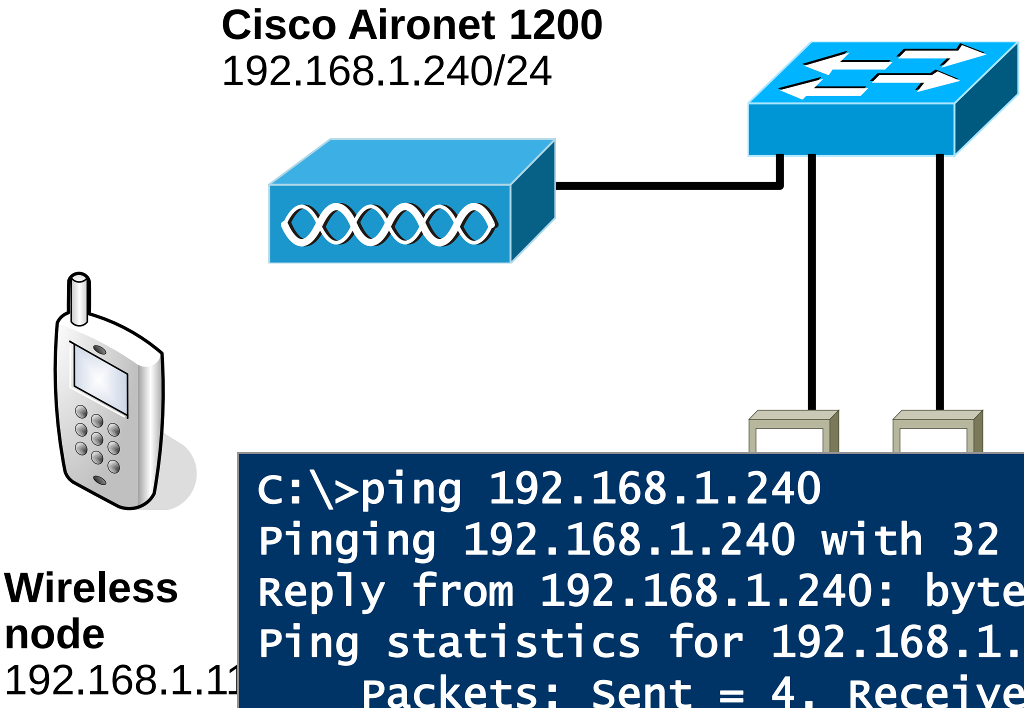
□ Allow Intermediate certificates

Server name:

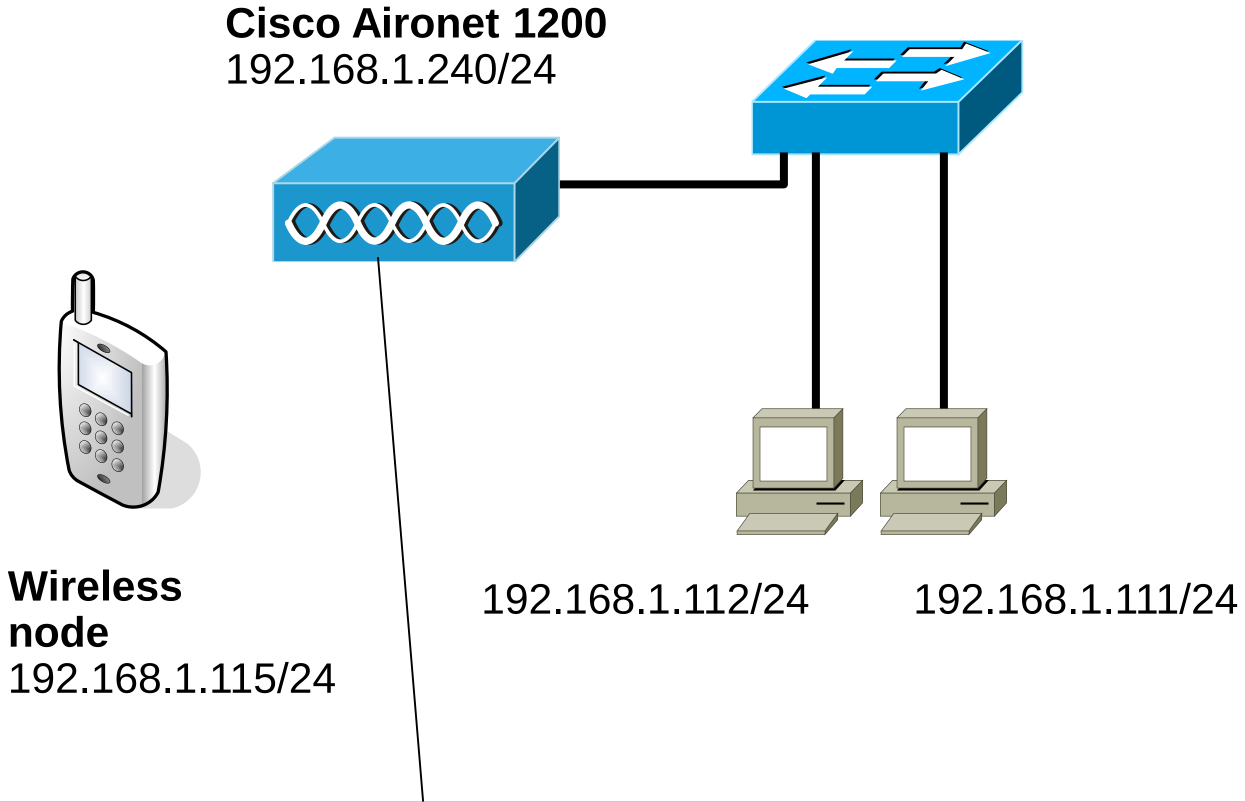
○ Server name must match exactly

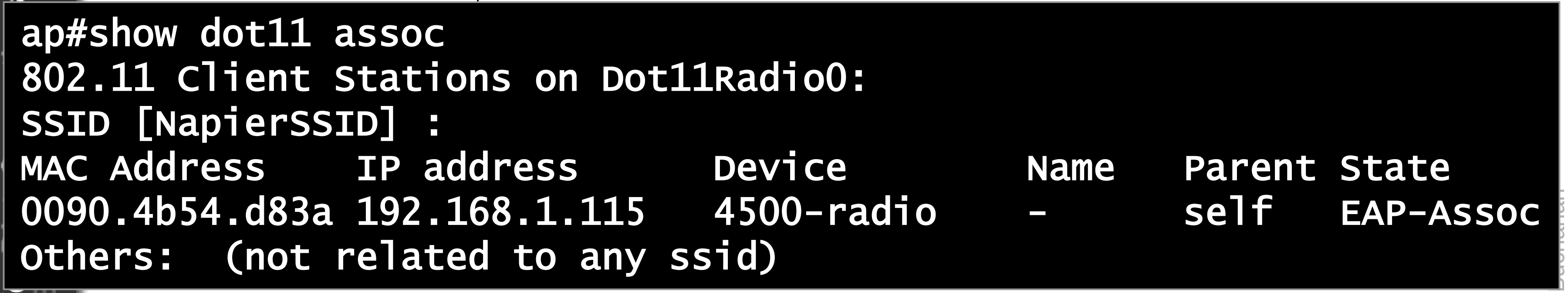
● Domain name must end in specified name

Edinburgh Napier
UNIVERSITY



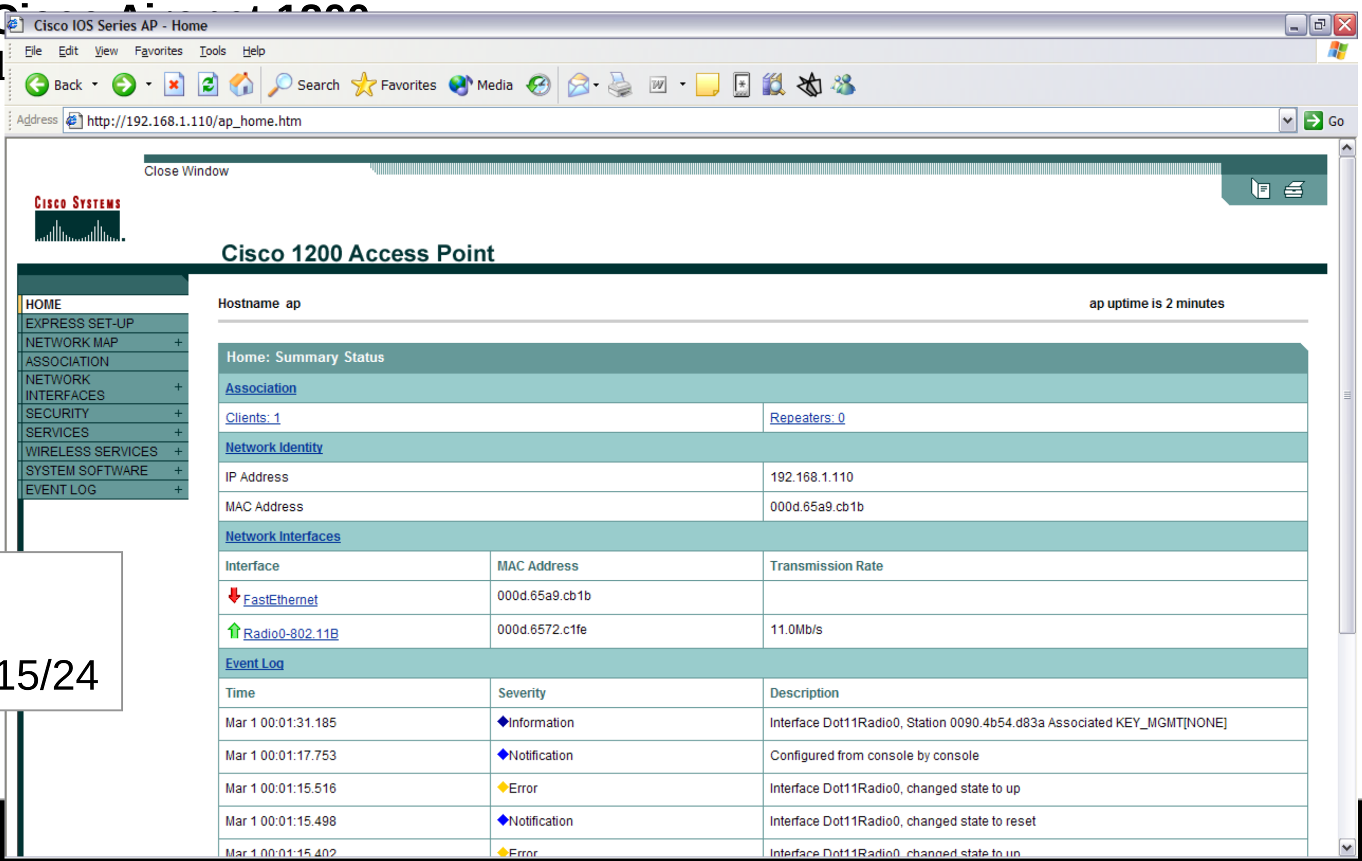
```
C:\>ping 192.168.1.240
Pinging 192.168.1.240 with 32 bytes of data:
Reply from 192.168.1.240: bytes=32 time=2ms TTL=255
Ping statistics for 192.168.1.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 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
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
```





```
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)
```

Cisco Aironet 1200
1



Cisco 1200 Access Point

Hostname ap

ap uptime is 2 minutes

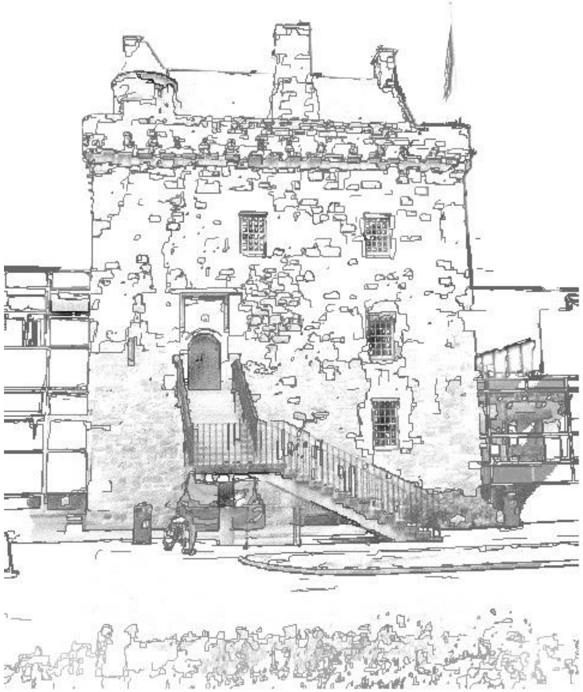
Home: Summary Status

Association		
Clients: 1		Repeaters: 0
Network Identity		
IP Address		192.168.1.110
MAC Address		000d.65a9.cb1b
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	000d.65a9.cb1b	
Radio0-802.11B	000d.6572.c1fe	11.0Mb/s
Event Log		
Time	Severity	Description
Mar 1 00:01:31.185	Information	Interface Dot11Radio0, Station 0090.4b54.d83a Associated KEY_MGMT[NONE]
Mar 1 00:01:17.753	Notification	Configured from console by console
Mar 1 00:01:15.516	Error	Interface Dot11Radio0, changed state to up
Mar 1 00:01:15.498	Notification	Interface Dot11Radio0, changed state to reset
Mar 1 00:01:15.402	Error	Interface Dot11Radio0, changed state to up

Wireless node
192.168.1.115/24

```
ap#show dot11
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)
```

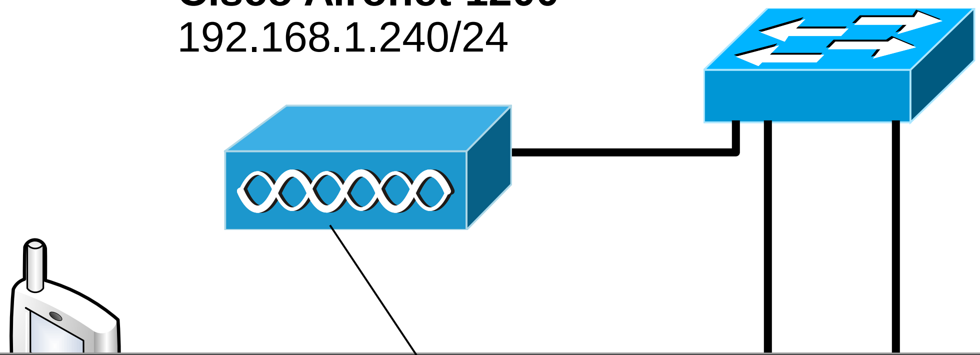
Configure for Remote TACACS+ Server



Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

Author: Bill Buchanan

Edinburgh Napier UNIVERSITY



Cisco Aironet 1200
192.168.1.240/24

```
> en
# config t
(config)# hostname test
(config)# aaa new-model
(config)# tacacs-server host 39.100.234.1
(config)# tacacs-server key krinkle
(config)# aaa authentication login default group tacacs
(config)# aaa authentication ppp default group tacacs
(config)# aaa authorization network default group tacacs
(config)# aaa authorization exec default group tacacs
```