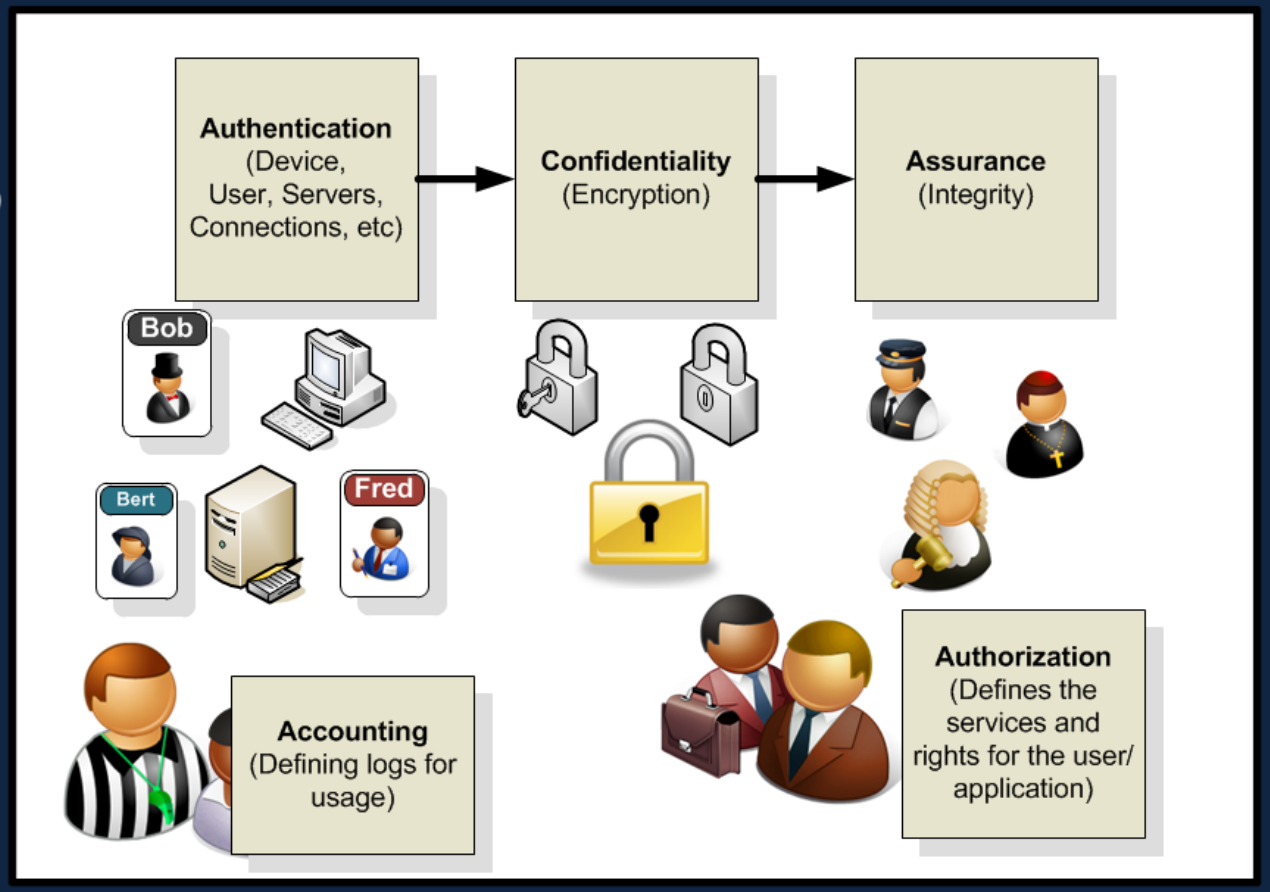
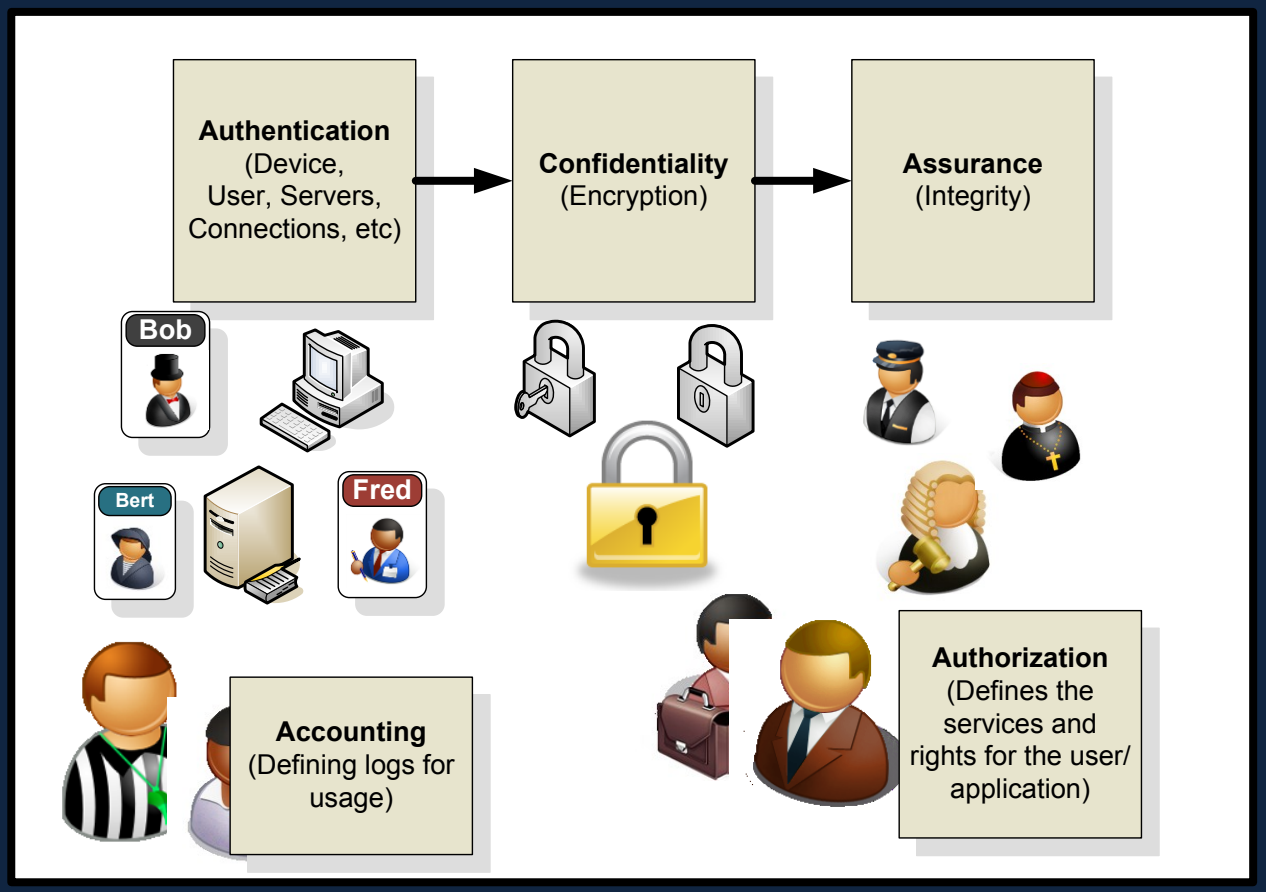
Wireless Security



Prof Bill Buchanan

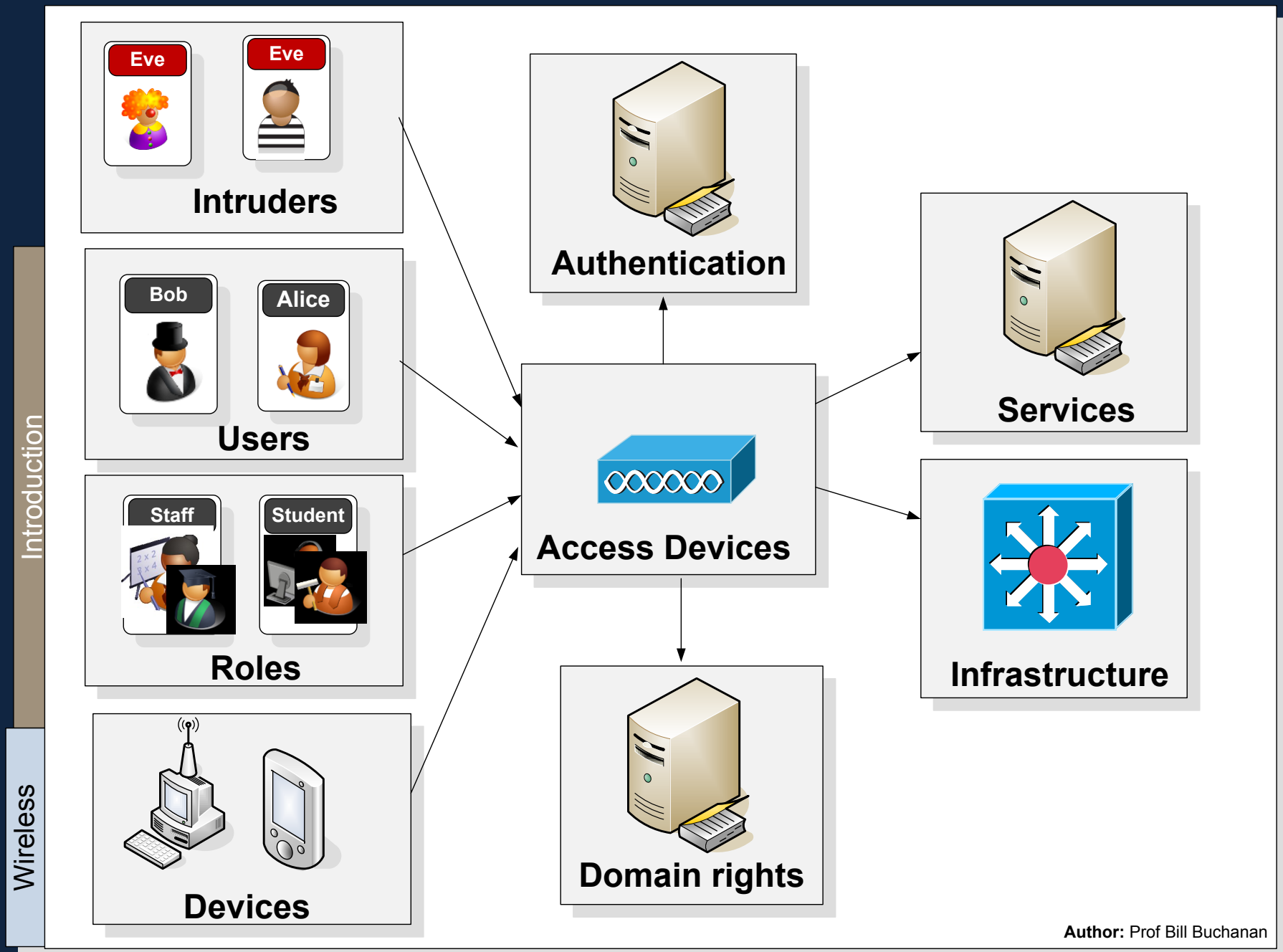
http://onlinevideo.napier.ac.uk/Play.aspx?VideoId=113

Wireless Security



Introduction

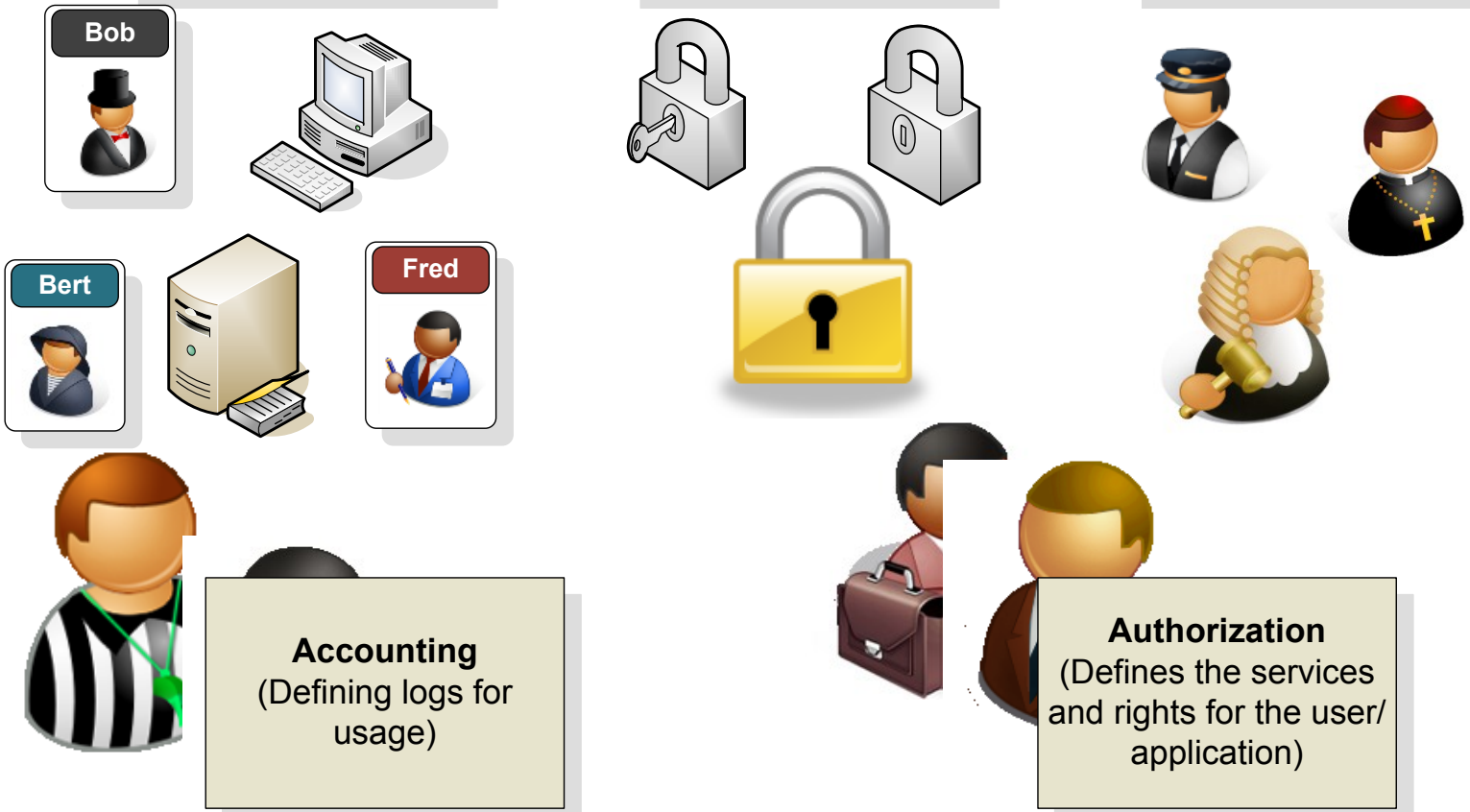
Author: Prof Bill Buchanan


Eve
Eve
Intruders
Bob
Alice
Users
Staff
Student
Roles
Devices
Authentication
Access Devices
Domain rights
Services
Infrastructure
Author: Prof Bill Buchanan

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

Confidentiality
(Encryption)

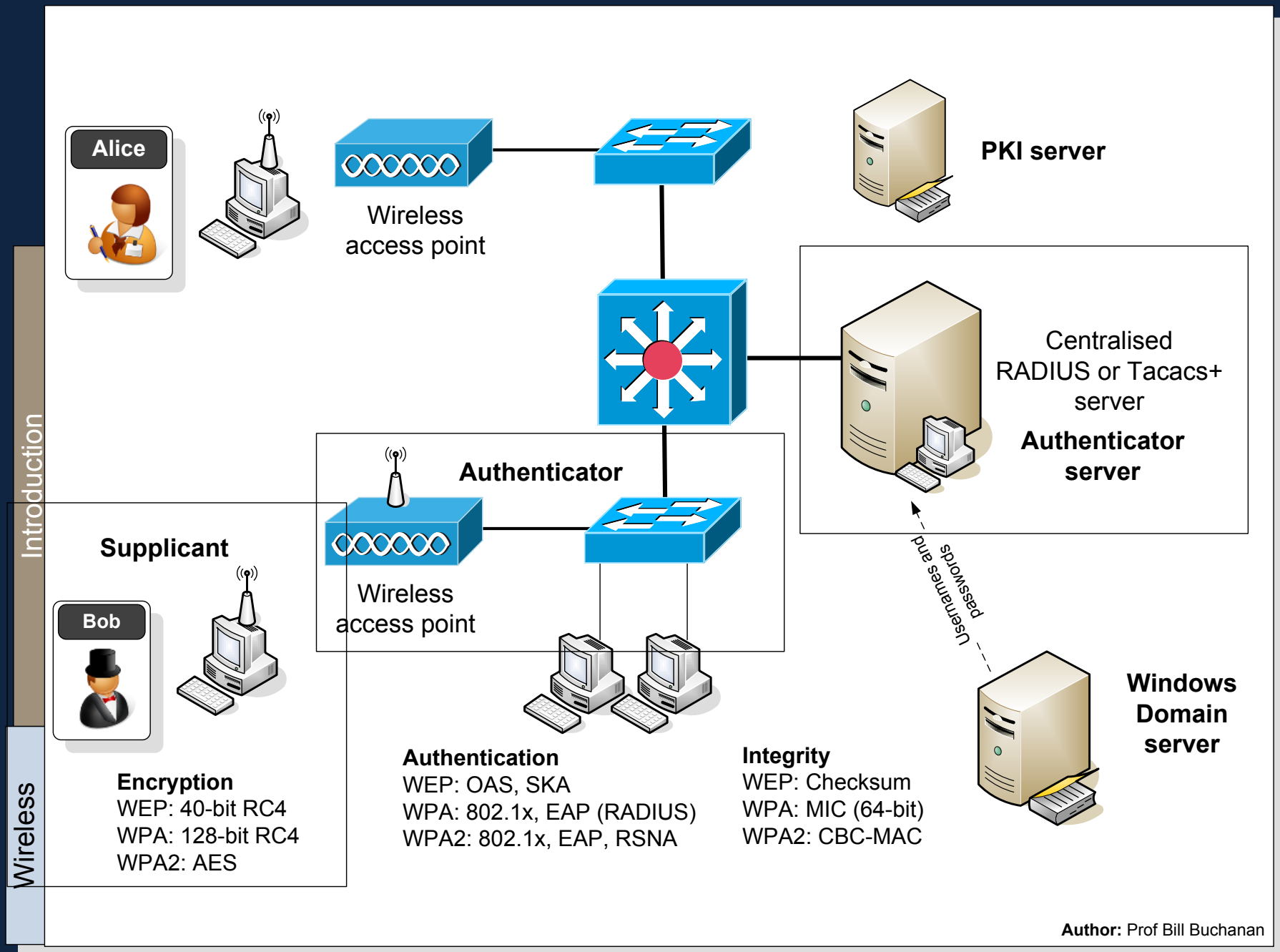
Assurance
(Integrity)



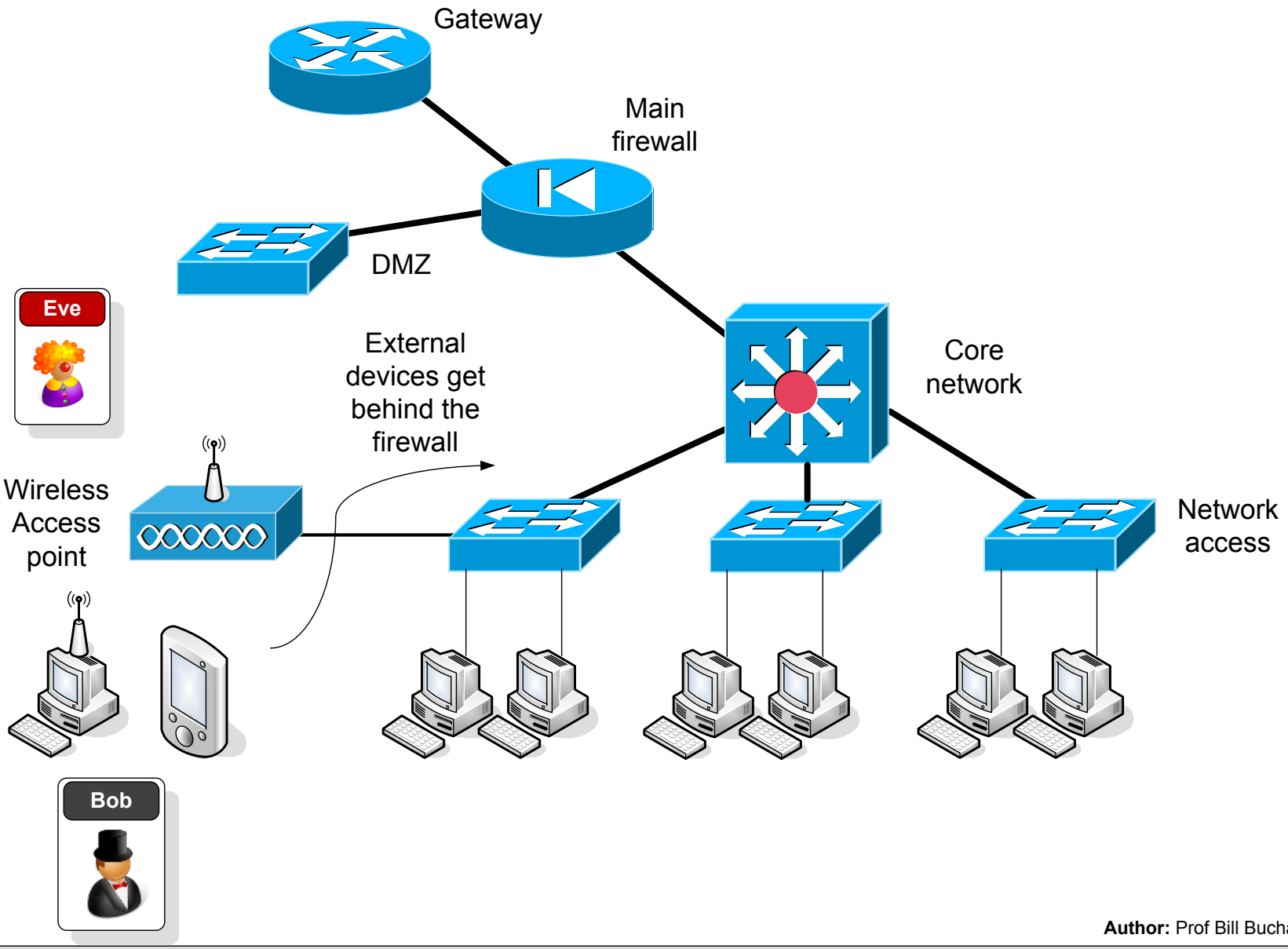
Accounting
(Defining logs for
usage)

Authorization
(Defines the services
and rights for the user/
application)

Author: Prof Bill Buchanan

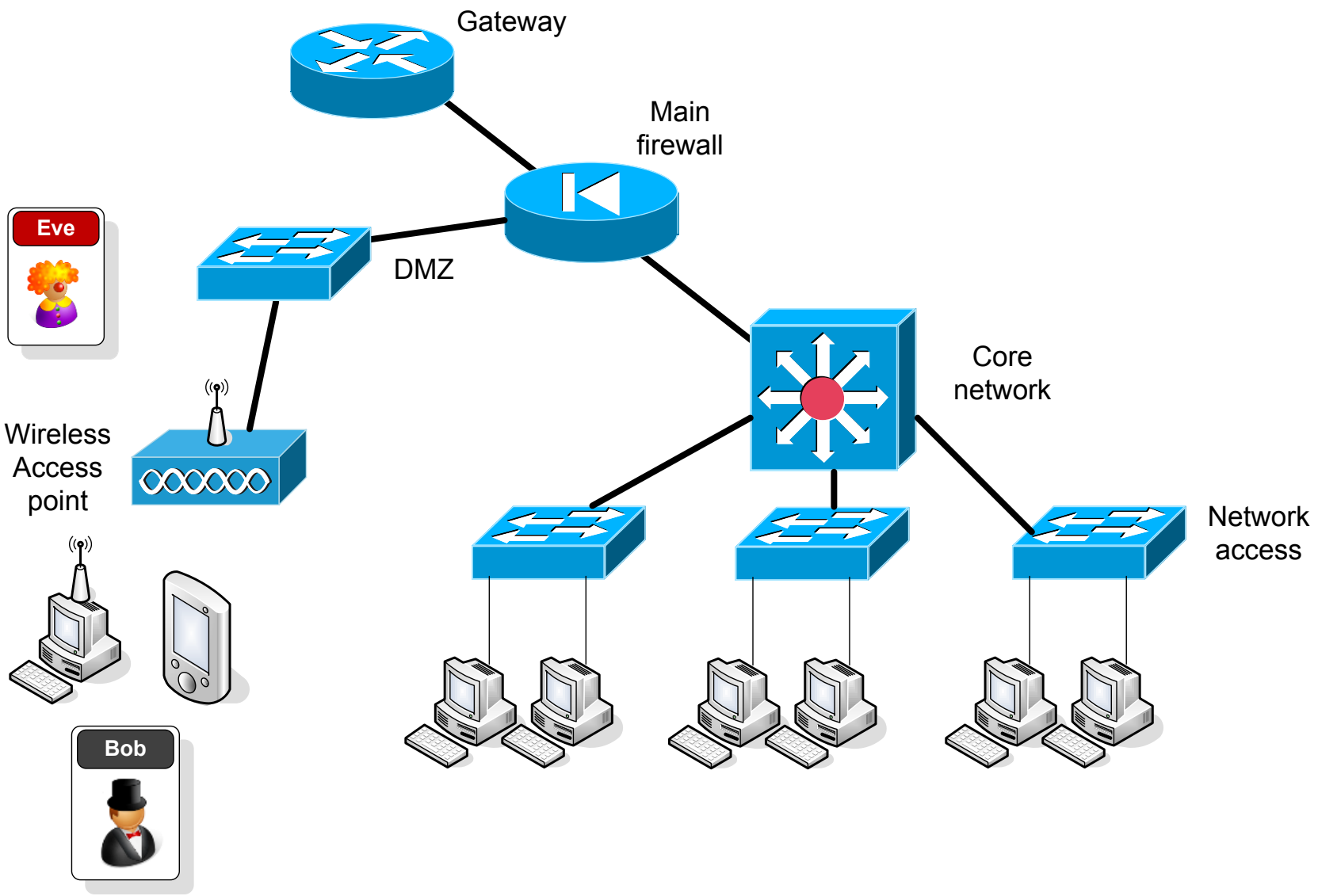


Wireless Infrastructure



Author: Prof Bill Buchanan

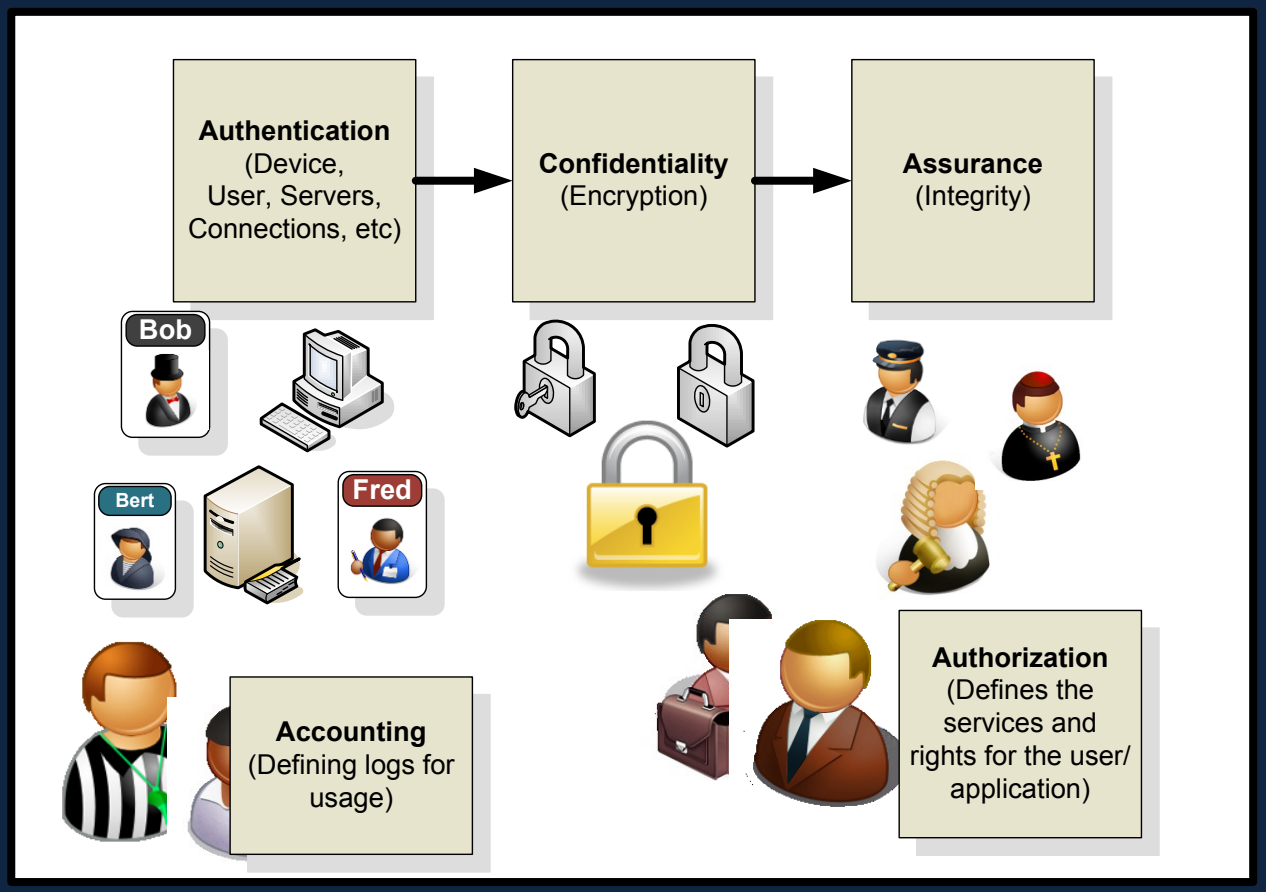
Getting into the core of the network



Author: Prof Bill Buchanan

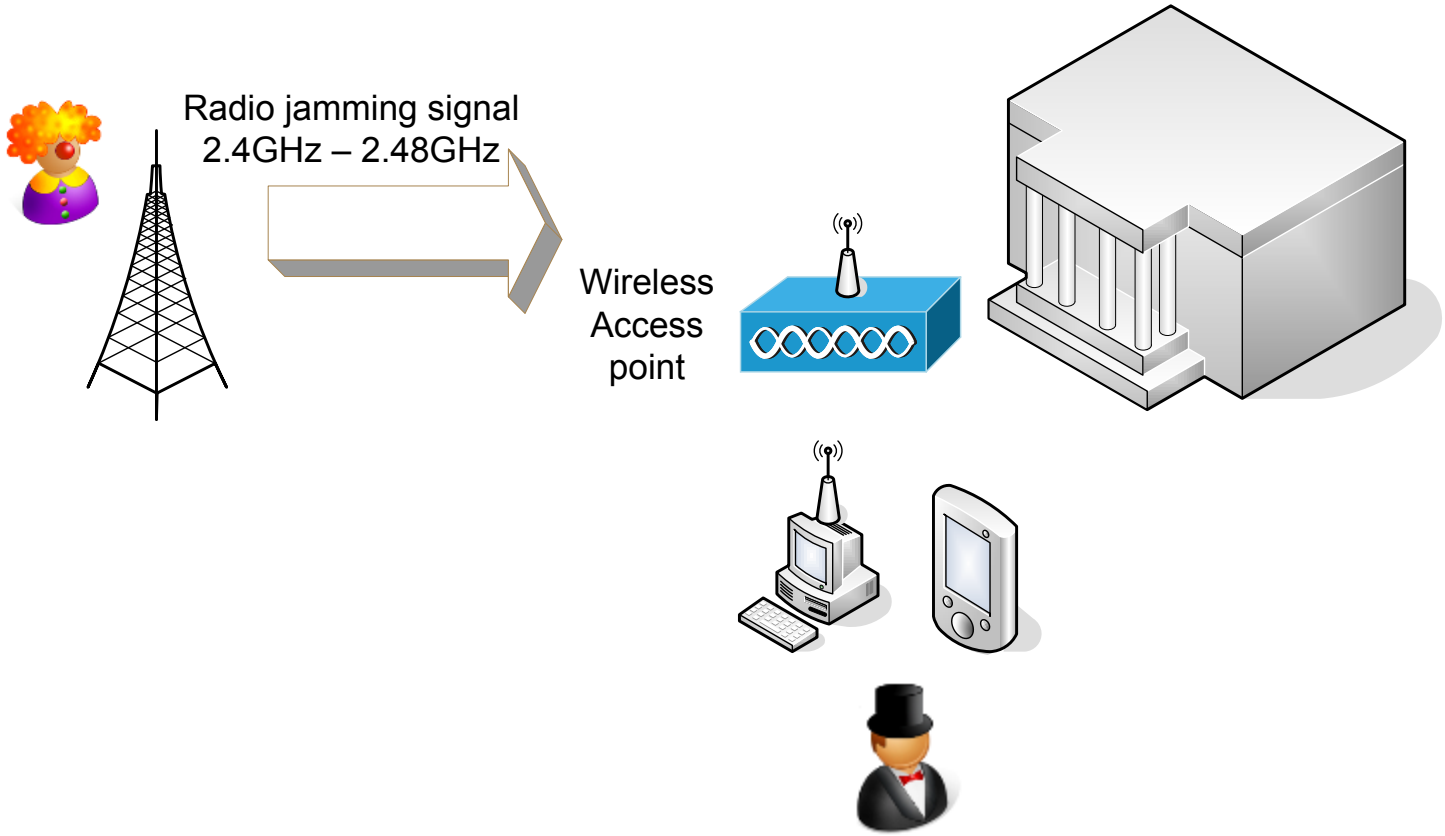
Typical access from the DMZ

Wireless Security



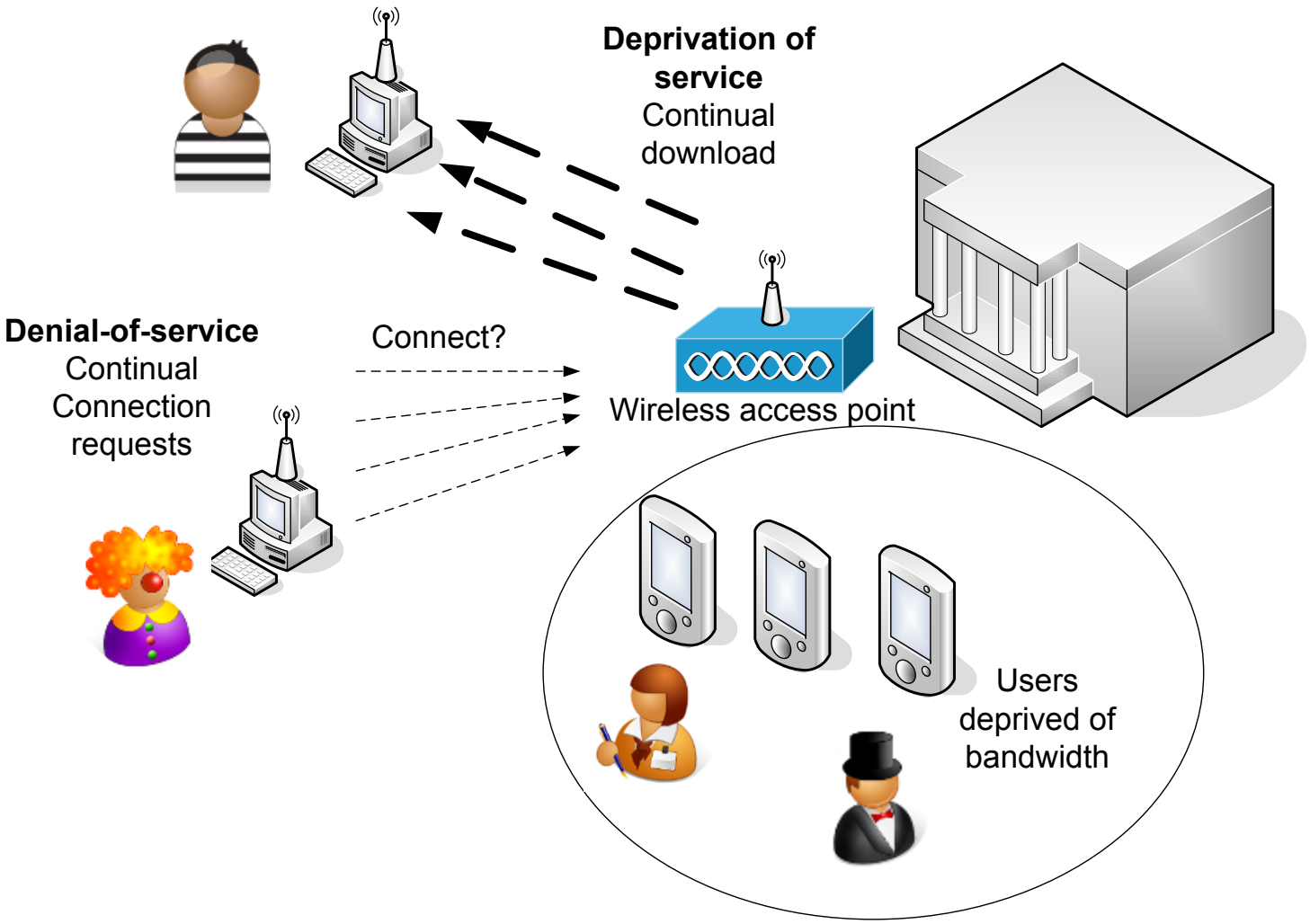
Layer 1 Issues

Author: Prof Bill Buchanan

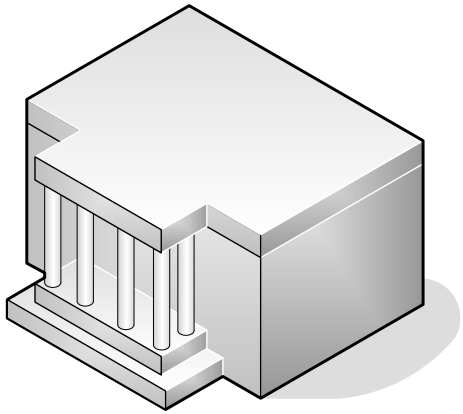


Author: Prof Bill Buchanan

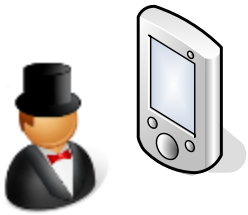
Layer 1 problems: Jamming



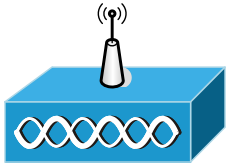
Author: Prof Bill Buchanan

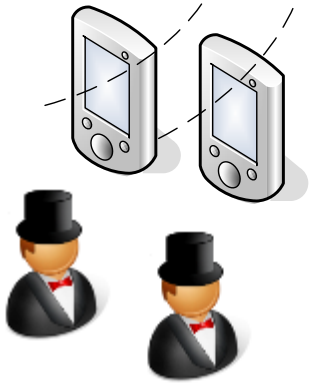


Valid wireless
Access point



Spoof Wireless
access point

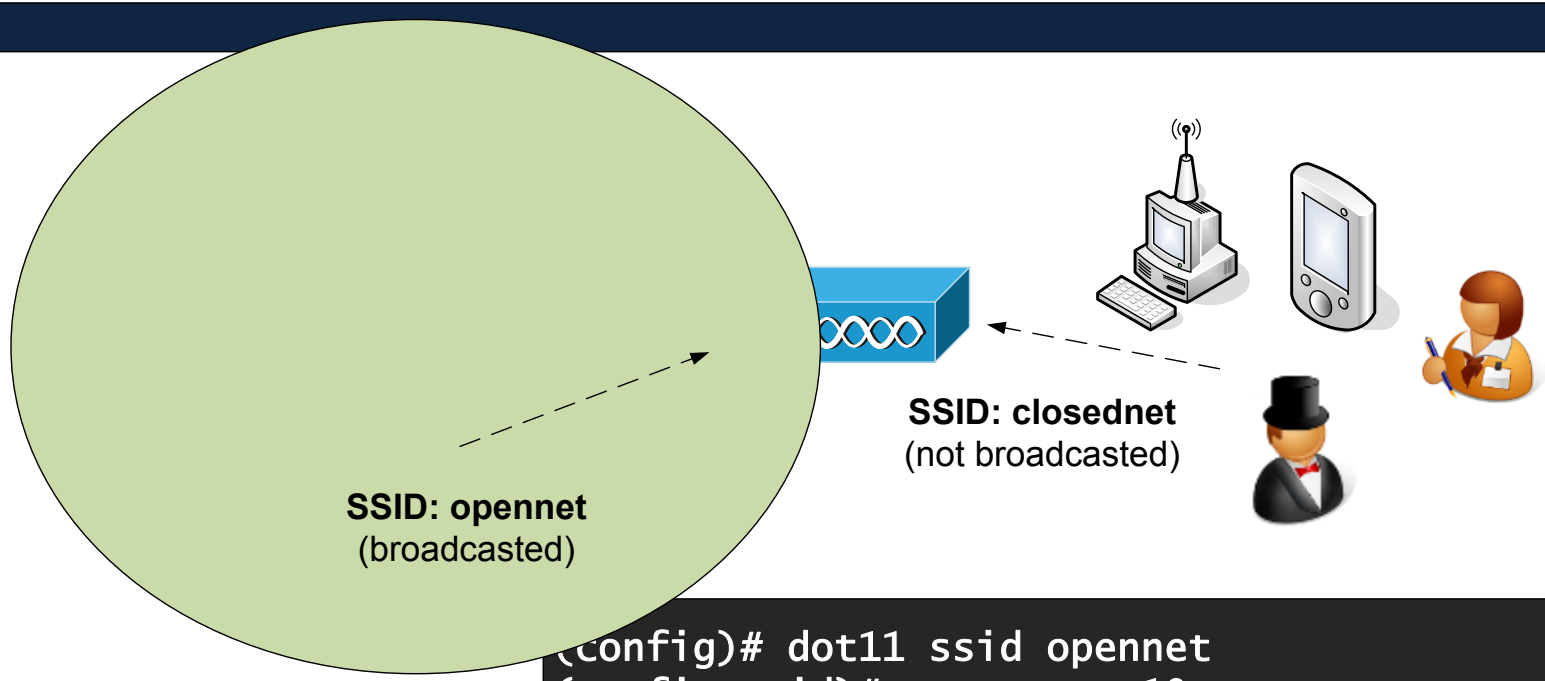




Problems:

- Connecting to strongest access point.
- Valid sounding SSID.

Author: Prof Bill Buchanan



Layer 1 Problems

Wireless

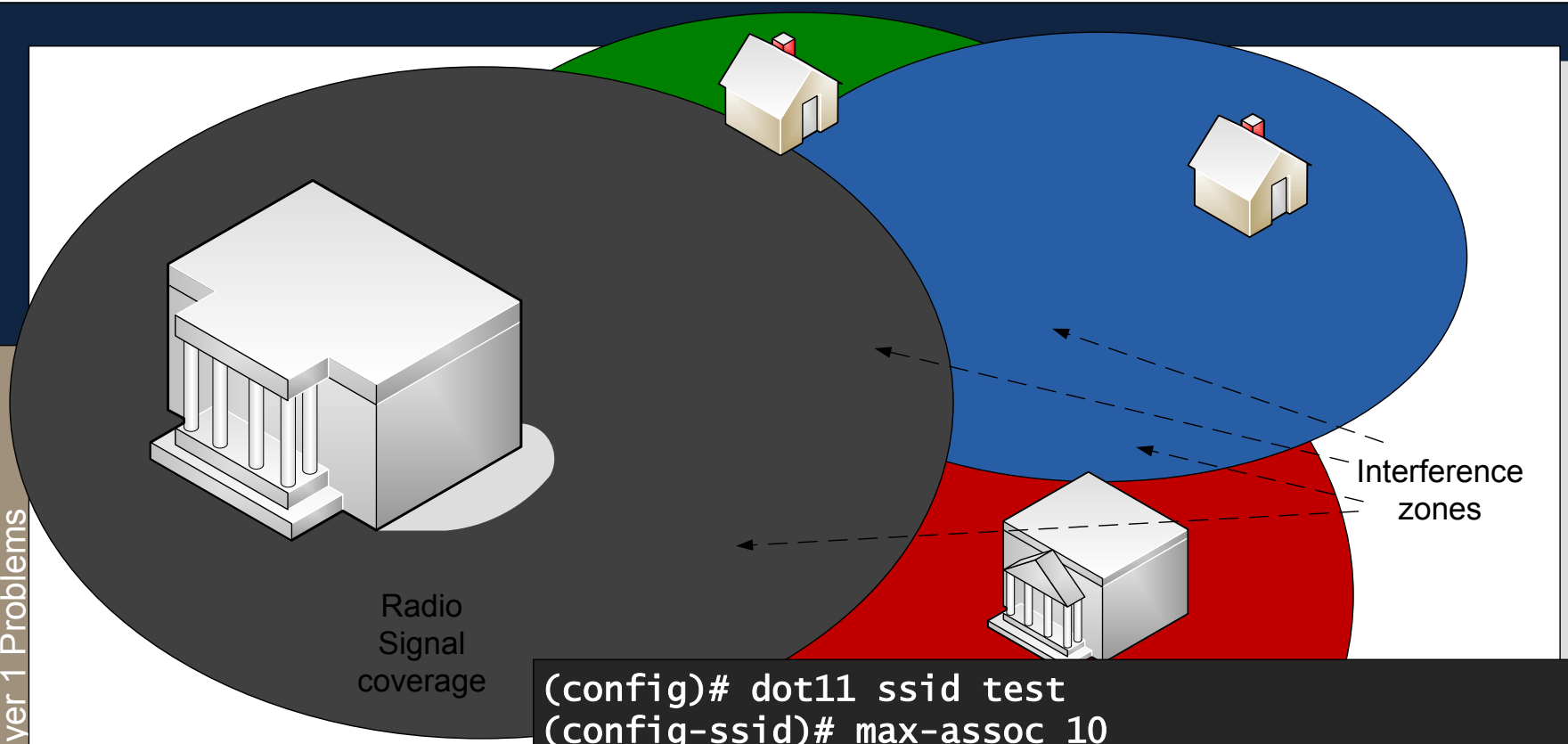
If the SSID is not broadcast, the users must know its name, and manually connect to it

```
(config)# dot11 ssid opennet
(config-ssid)# max-assoc 10
(config-ssid)# mbssid guest-mode
(config-ssid)# exit
(config)# dot11 ssid closednet
(config-ssid)# max-assoc 100
(config-ssid)# exit
(config)# int bvi1
(config-if)# ip address 1.2.3.4 255.255.255.0
(config-if)# exit
(config)# int d0
(config-if)# beacon period 2000 // 2sec
(config-if)# mbssid
(config-if)# ssid opennet
(config-if)# ssid closednet
```

SSID Security

Layer 1 Problems

Wireless



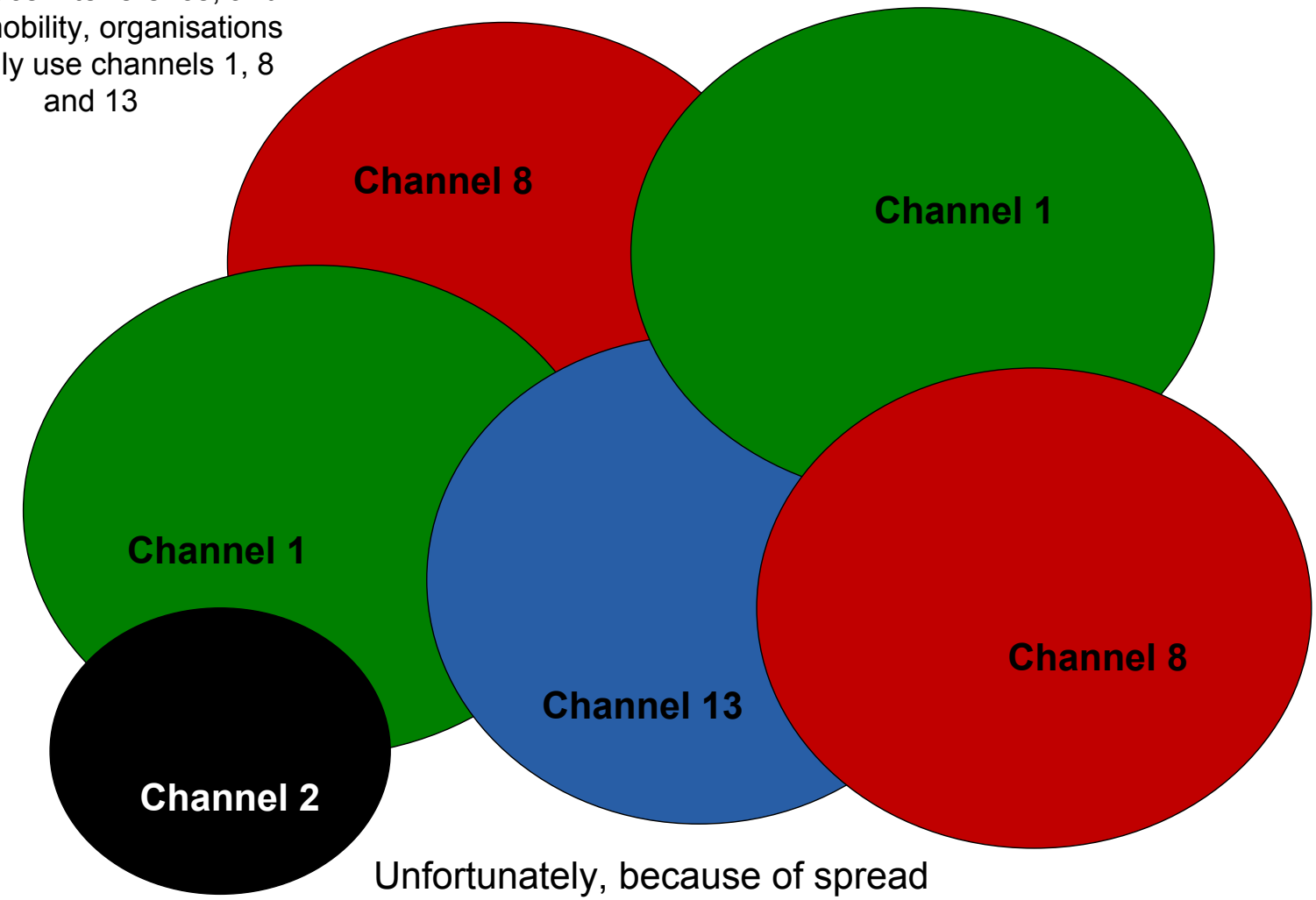
If organisations use the same radio channel (such as Channel 1) it causes interference for others on the same channel

This problem can be reduced with shielding, and by reducing the power levels of the clients and the access point

```
(config)# dot11 ssid test
(config-ssid)# max-assoc 10
(config-ssid)# exit
(config)# int d0
(config-if)# power local ?
  <1-50>   One of: 1 5 20 30 50
  maximum  Set local power to allowed maximum
(config-if)# power local 30
(config-if)# power client ?
  <1-50>   One of: 1 5 20 30 50
  maximum  Set client power to allowed maximum
(config-if)# power client 10
(config-if)# ssid test
```

Layer 1 Problems – Power output

To reduce interference, and allow mobility, organisations normally use channels 1, 8 and 13

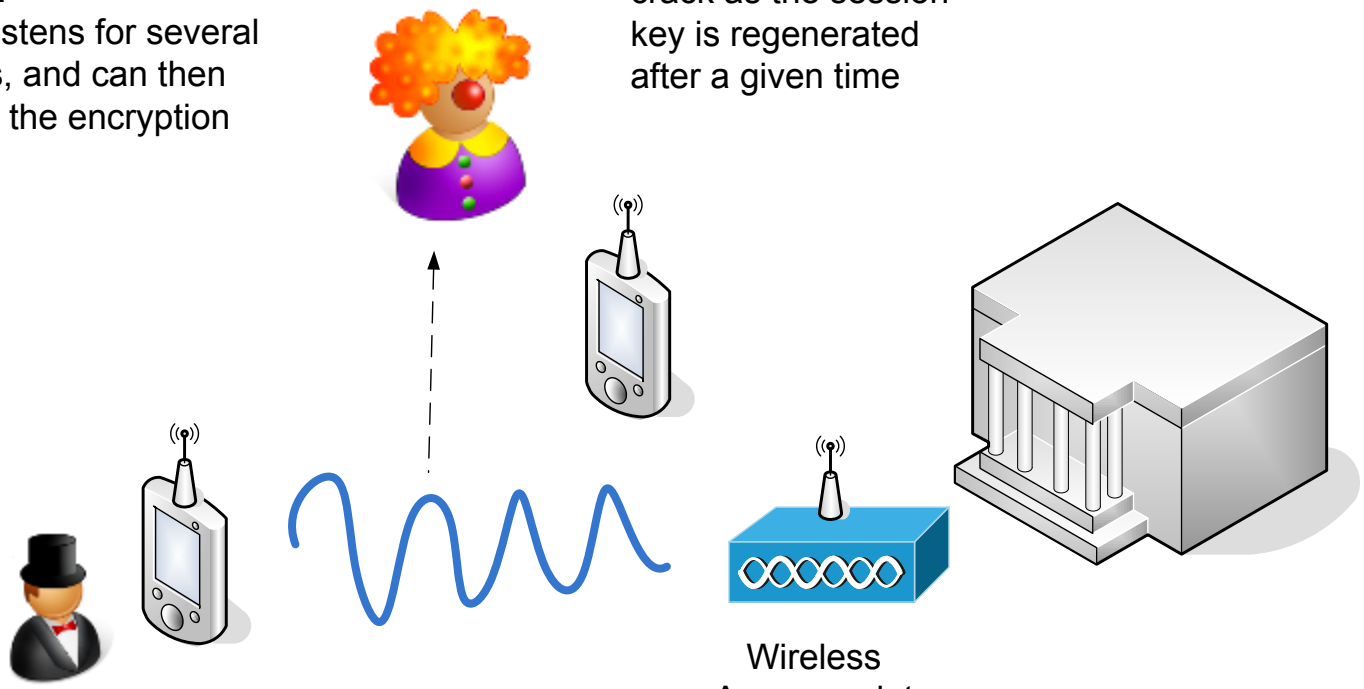


Unfortunately, because of spread spectrum, others channels interfere with these channels, eg channels 2, 3 and 4 interfere with Channel 1

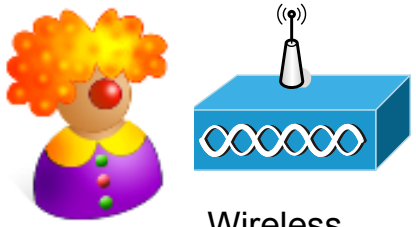
Author: Prof Bill Buchanan

WEP:
Eve listens for several hours, and can then crack the encryption key

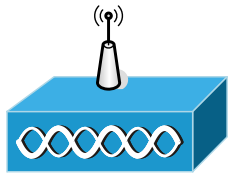
TKIP:
Much more difficult to crack as the session key is regenerated after a given time



Author: Prof Bill Buchanan

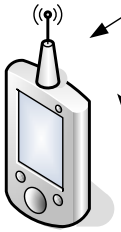


Wireless
Access point

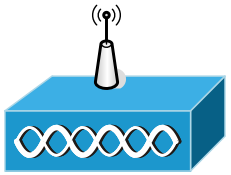


Wireless
Access point

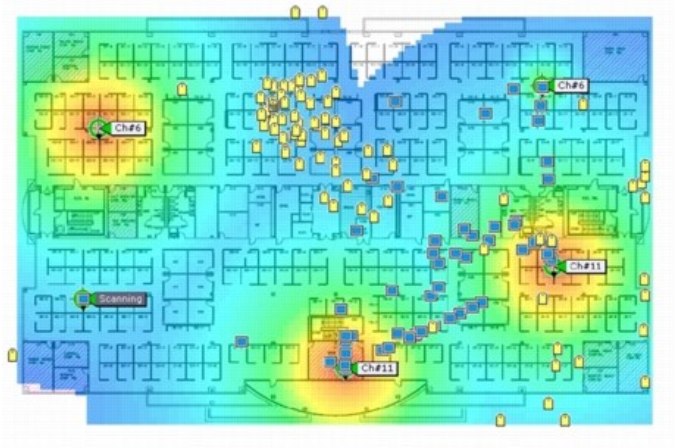
Bob can be tracked when it is known which access point he connects to (**cellular**) or from signal strength/signal delay (**triangulation**)



Time delay or signal strength measured

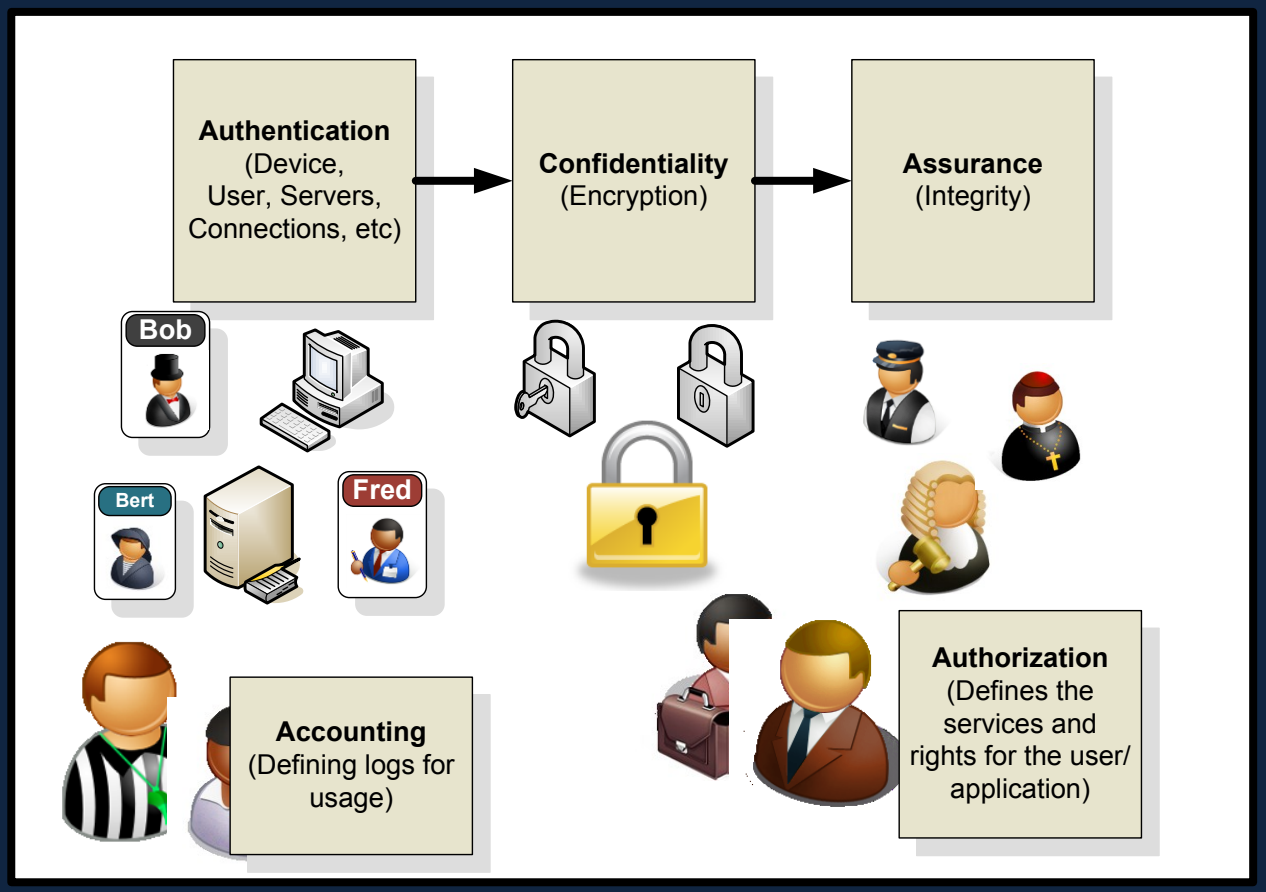


Wireless
Access point



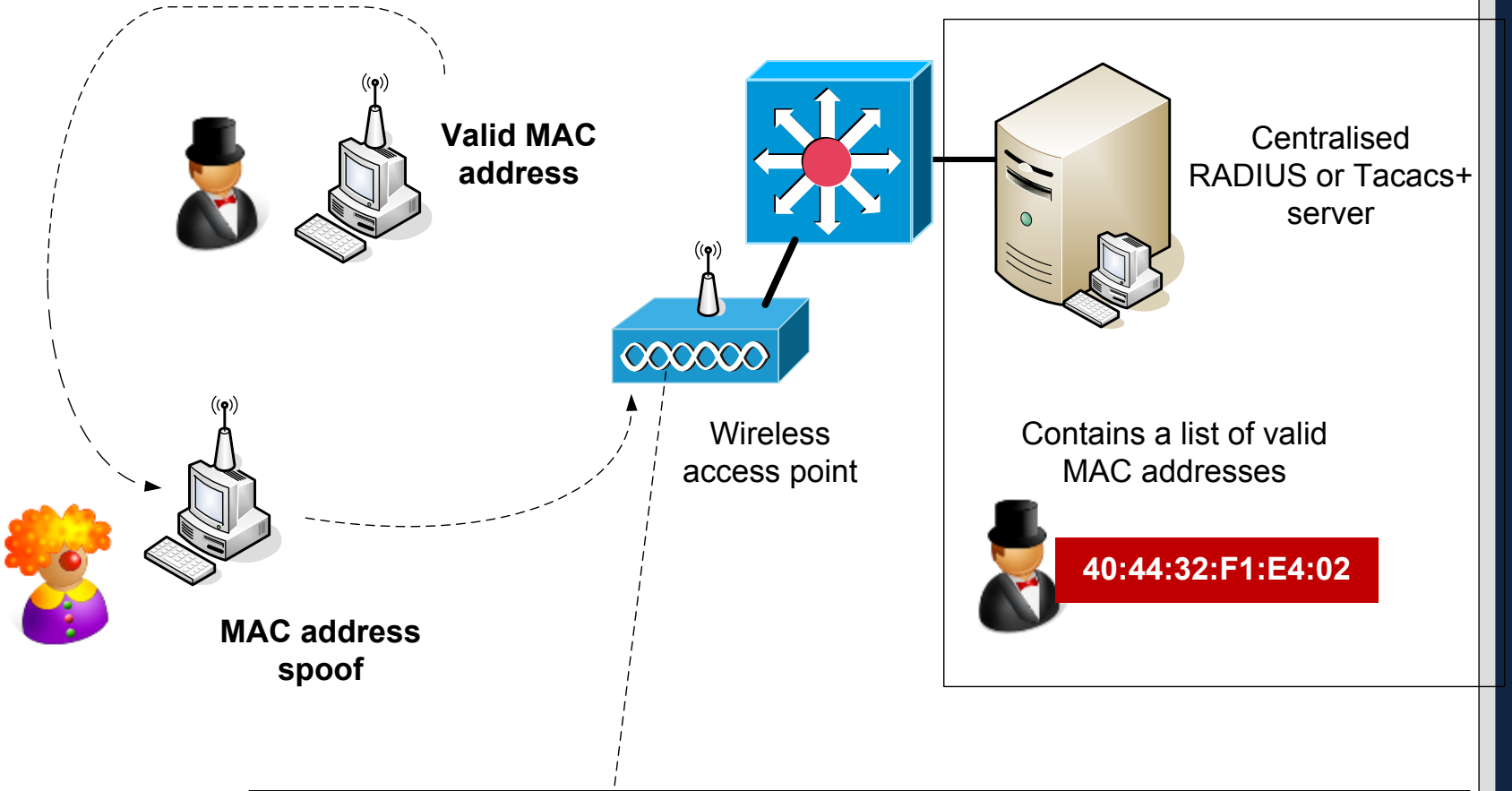
Author: Prof Bill Buchanan

Wireless Security



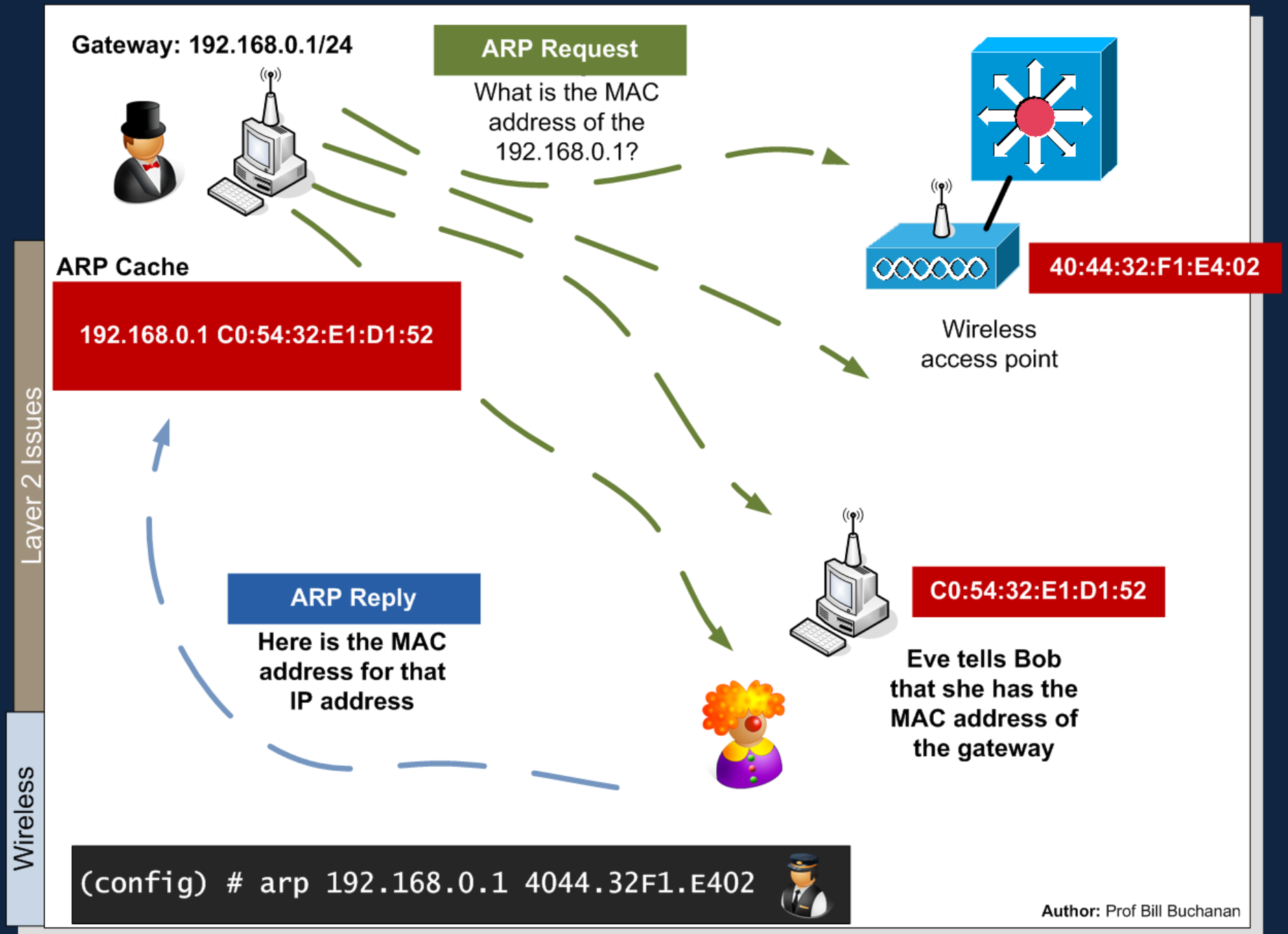
Layer 2 Issues

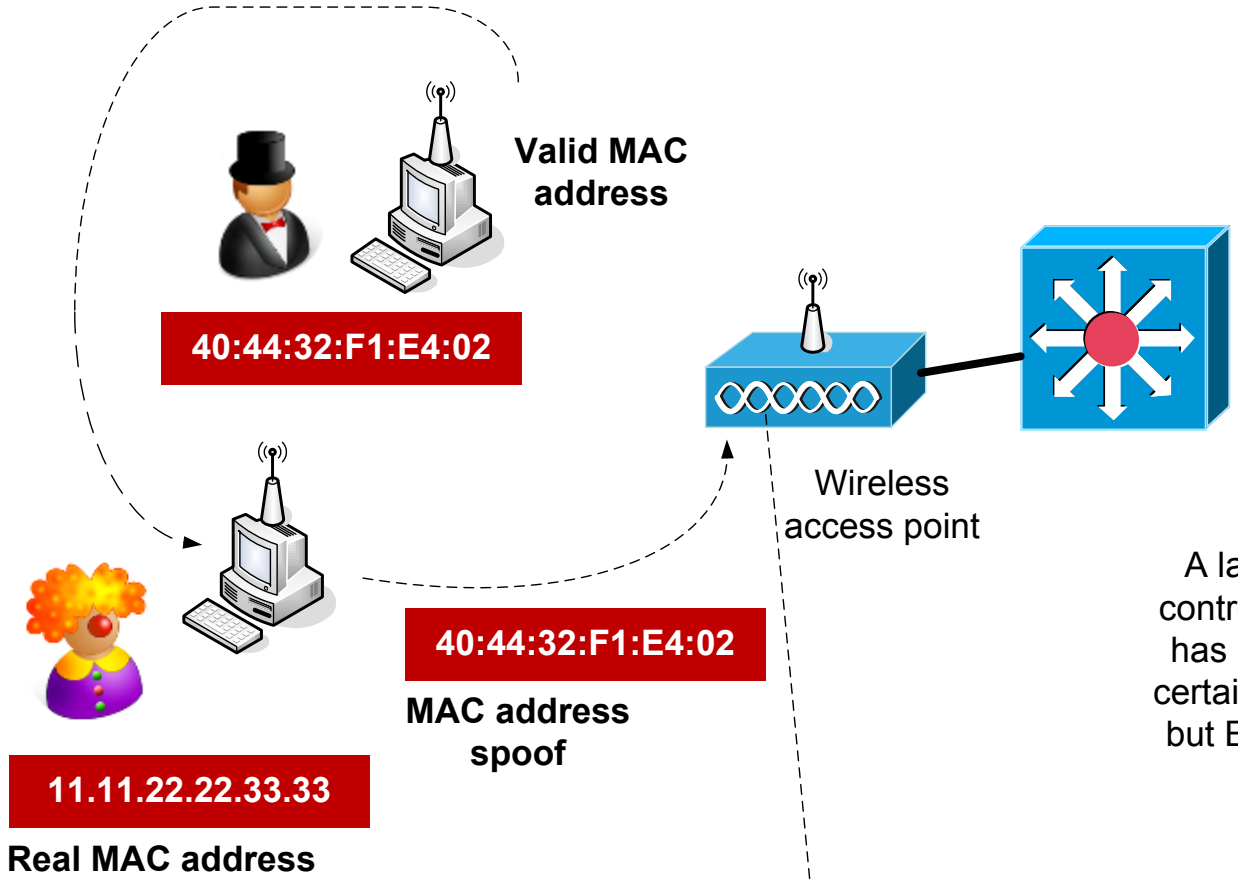
Author: Prof Bill Buchanan




```
# config t
(config)# dot11 ssid fred
(config-ssid)# authentication open mac-address maclist
(config-ssid)# exit
(config)# aaa new-model
(config)# aaa authentication login maclist group radius
```

Author: Prof Bill Buchanan


Gateway: 192.168.0.1/24
ARP Request
What is the MAC address of the 192.168.0.1?
ARP Cache
192.168.0.1 C0:54:32:E1:D1:52
40:44:32:F1:E4:02
Wireless access point
C0:54:32:E1:D1:52
Eve tells Bob that she has the MAC address of the gateway
ARP Reply
Here is the MAC address for that IP address
(config) # arp 192.168.0.1 4044.32F1.E402
Author: Prof Bill Buchanan



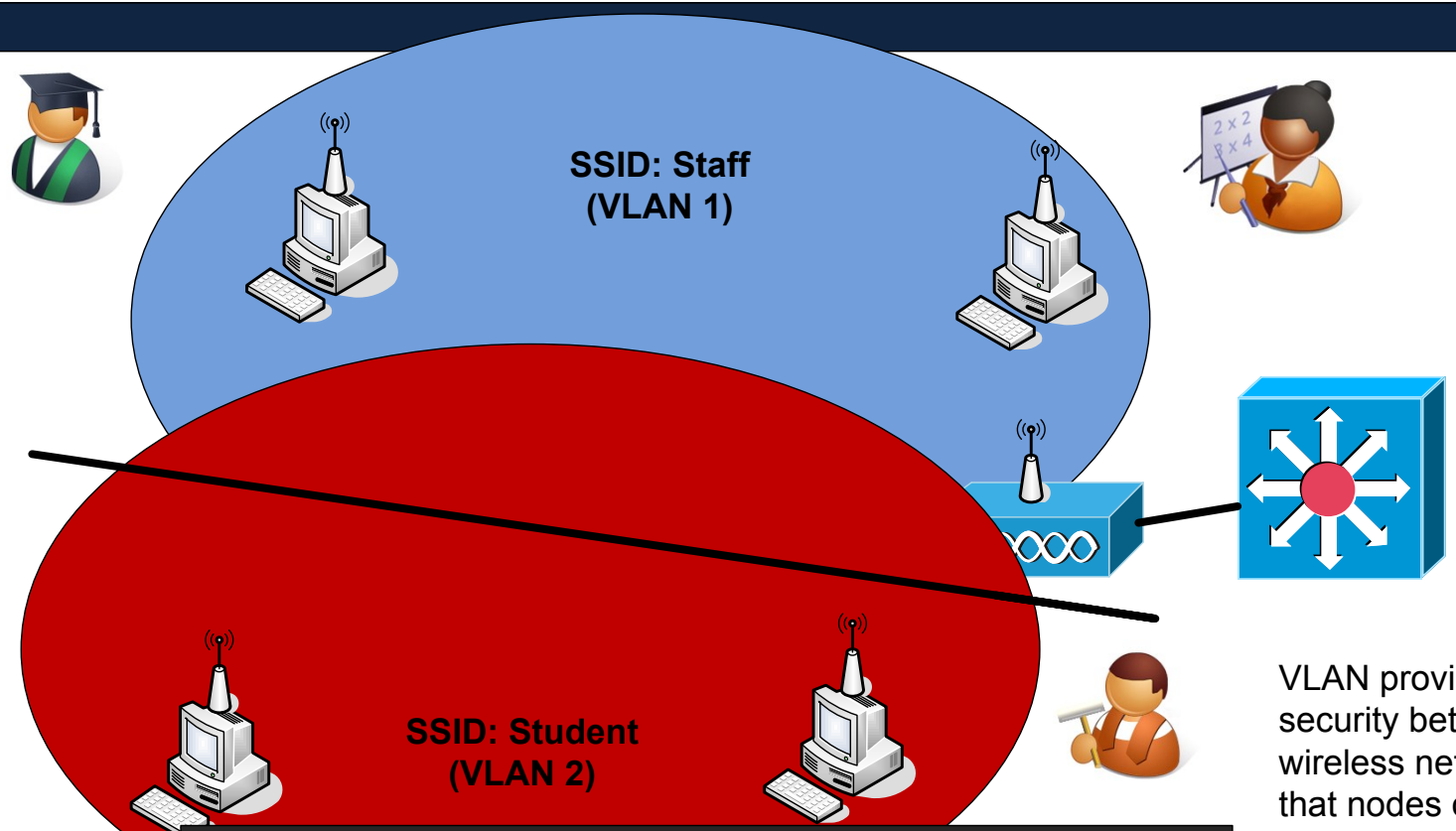
A layer 2 access-list control list (MAC filters) has been setup to bar certain MAC addresses, but Eve selects a valid one

```
(config) # access-list 701 deny 1111.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 2222.3333.4444 ffff.ffff.ffff
(config) # access-list 701 permit 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if) # l2-filter bridge-group-acl
(config-if) # bridge-group 1 output-address-list 701
```

Author: Prof Bill Buchanan

Layer 2 Issues

Wireless



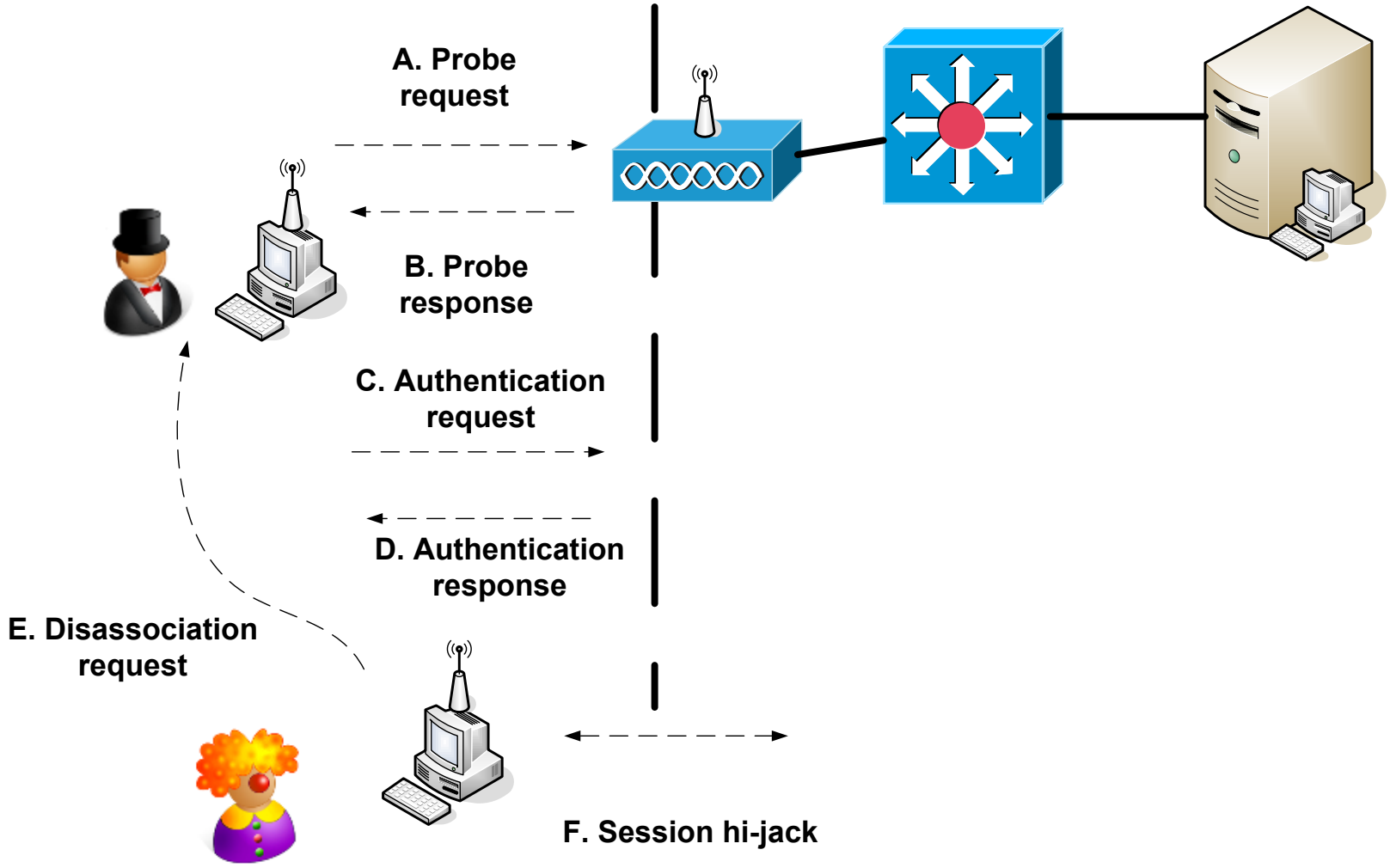

```
(config)# dot11 ssid Staff
(config-ssid)# mbssid guest-mode
(config-ssid)# vlan 1
(config-ssid)# exit
(config)# dot11 ssid Student
(config-ssid)# vlan 2
(config-ssid)# exit
(config)# int d0
(config-if)# mbssid
(config-if)# ssid Staff
(config-if)# ssid Student
```

VLAN provides logical security between the wireless networks, so that nodes on one network cannot directly see nodes on the other VLAN (unless through a router)

Author: Prof Bill Buchanan

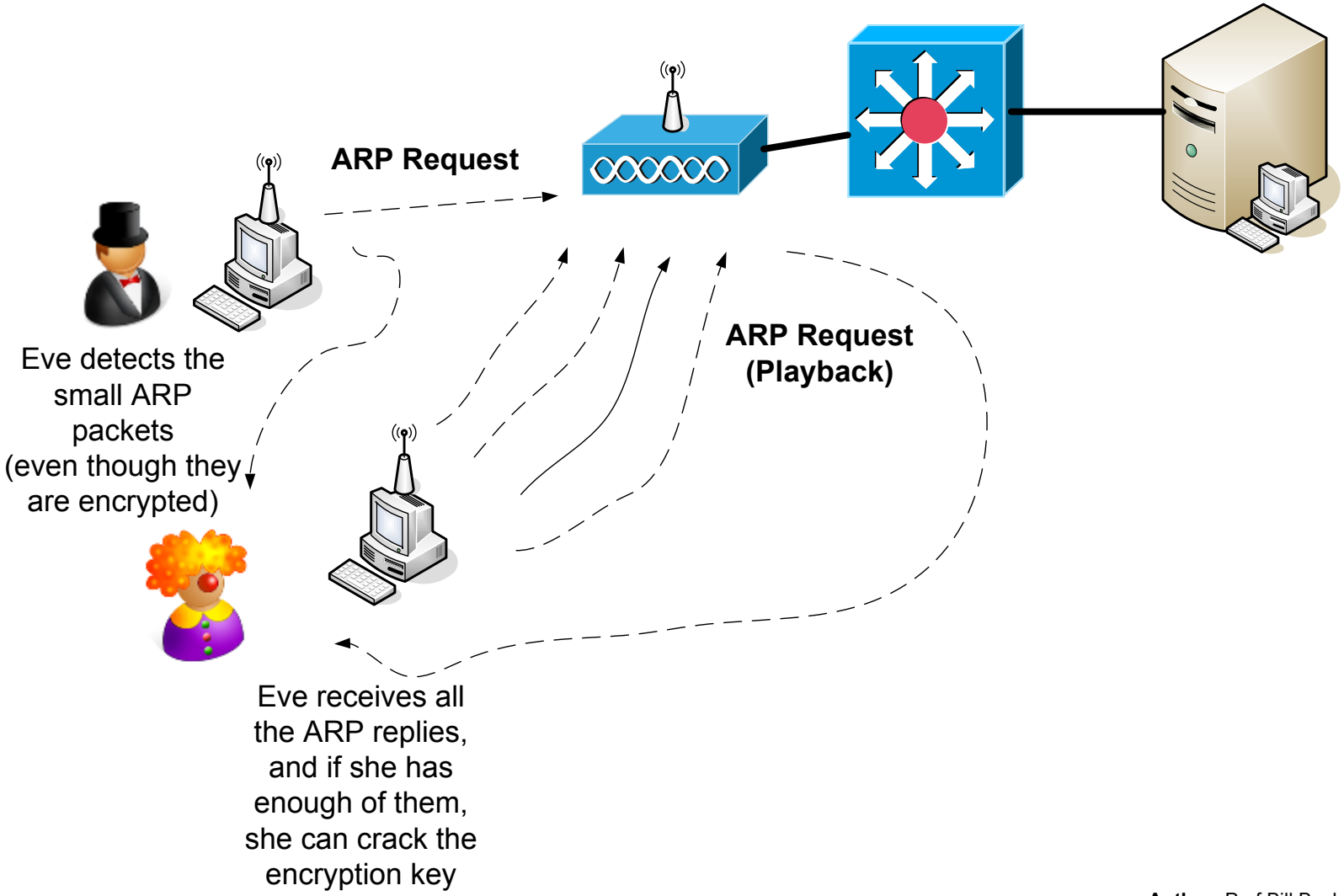
Layer 2 Issues

Wireless



Author: Prof Bill Buchanan

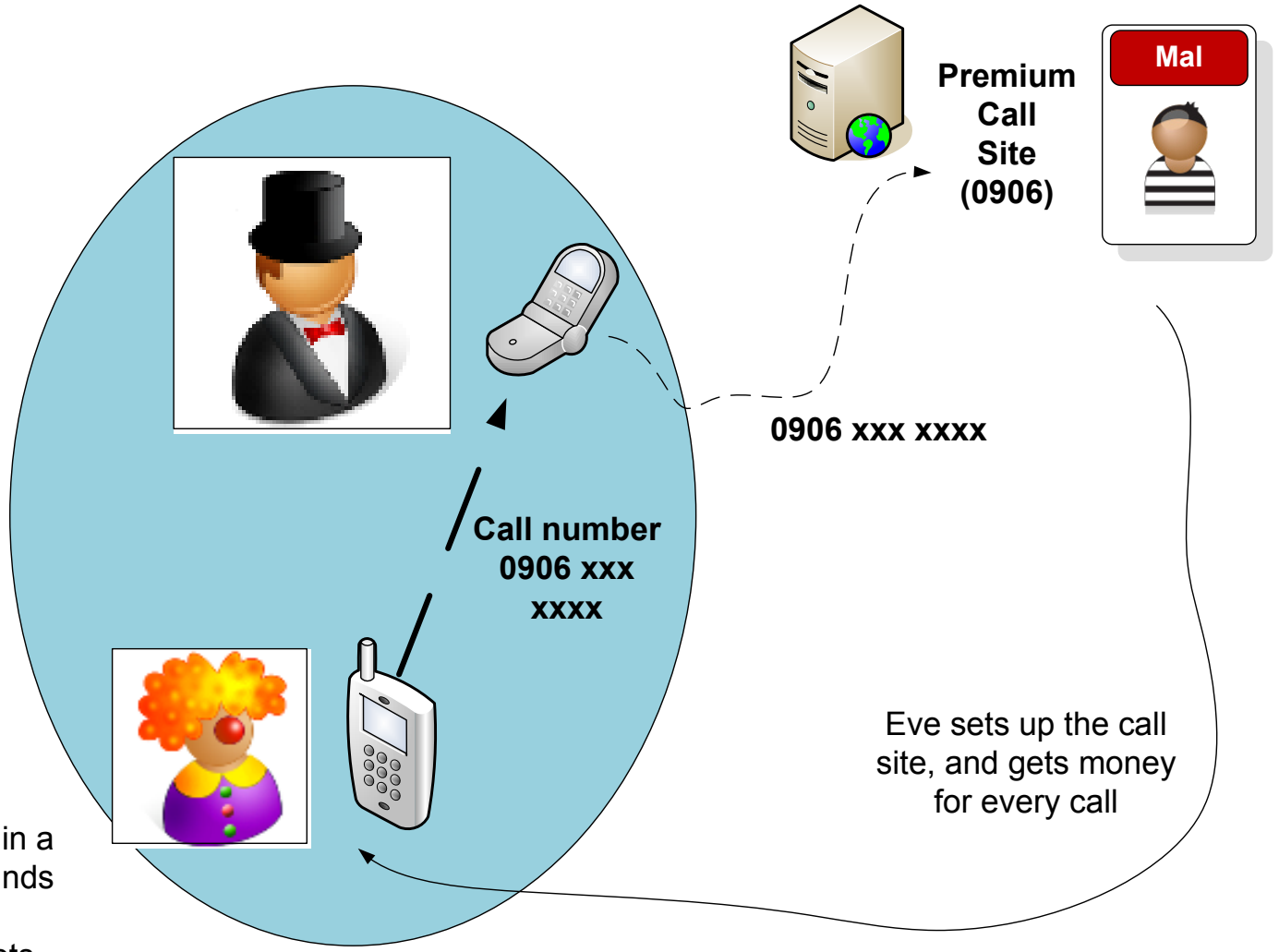
Layer 2 Problems – Session Hi-jack



Author: Prof Bill Buchanan

Layer 2 Issues

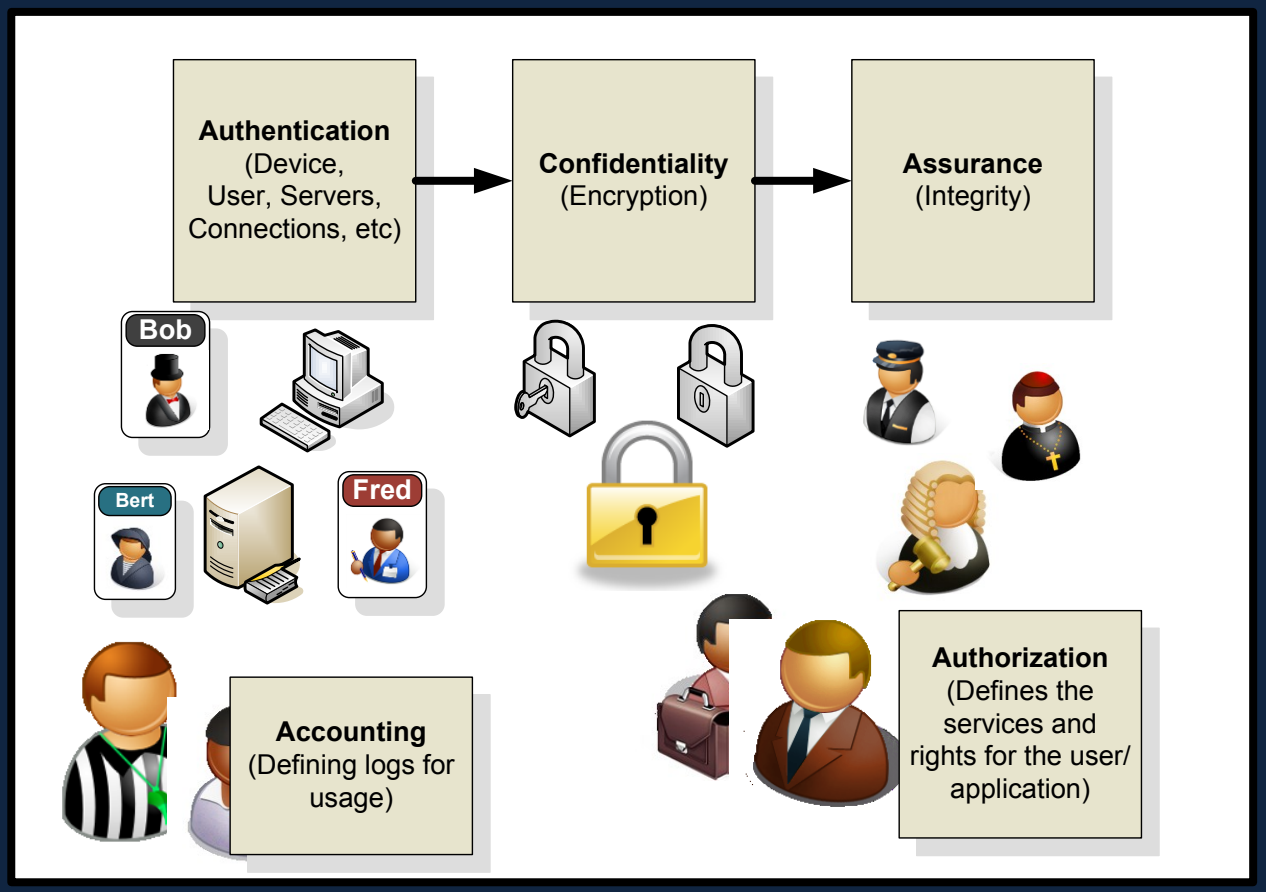
Wireless



Eve sniffs for Bluetooth signals in a public area, and finds a phone with Bluetooth can gets the phone to call a premium rate number

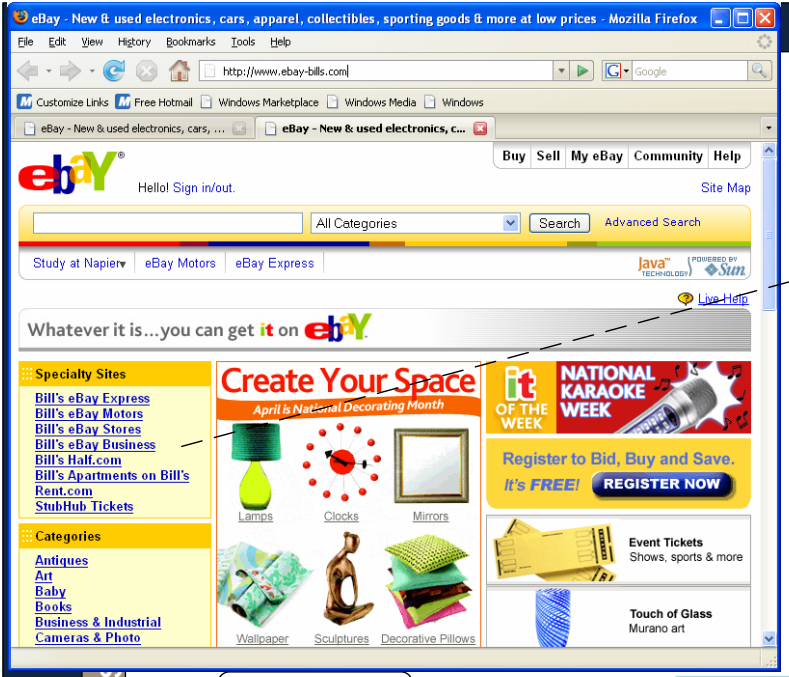
Author: Prof Bill Buchanan

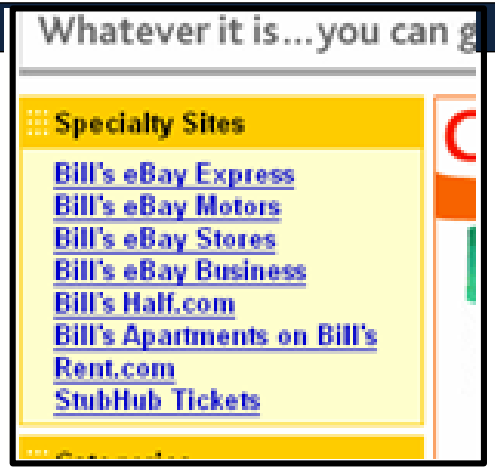
Wireless Security



Layer 3 Issues

Author: Prof Bill Buchanan





Layer 3 Is

Wireless

Public access point

eBay server

Alice

Bob

eBay-bill server

Mal

Eve

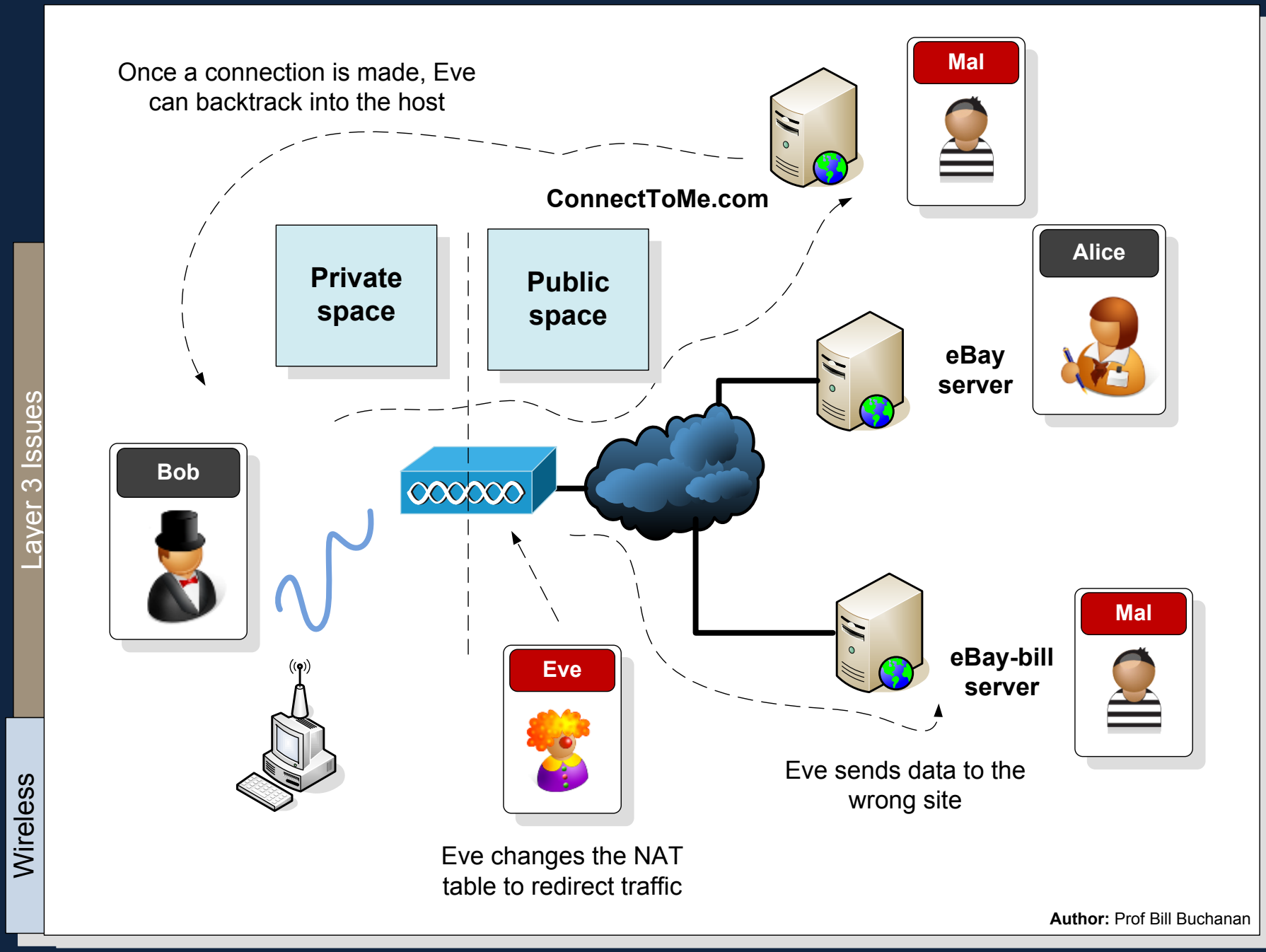
Domain name server

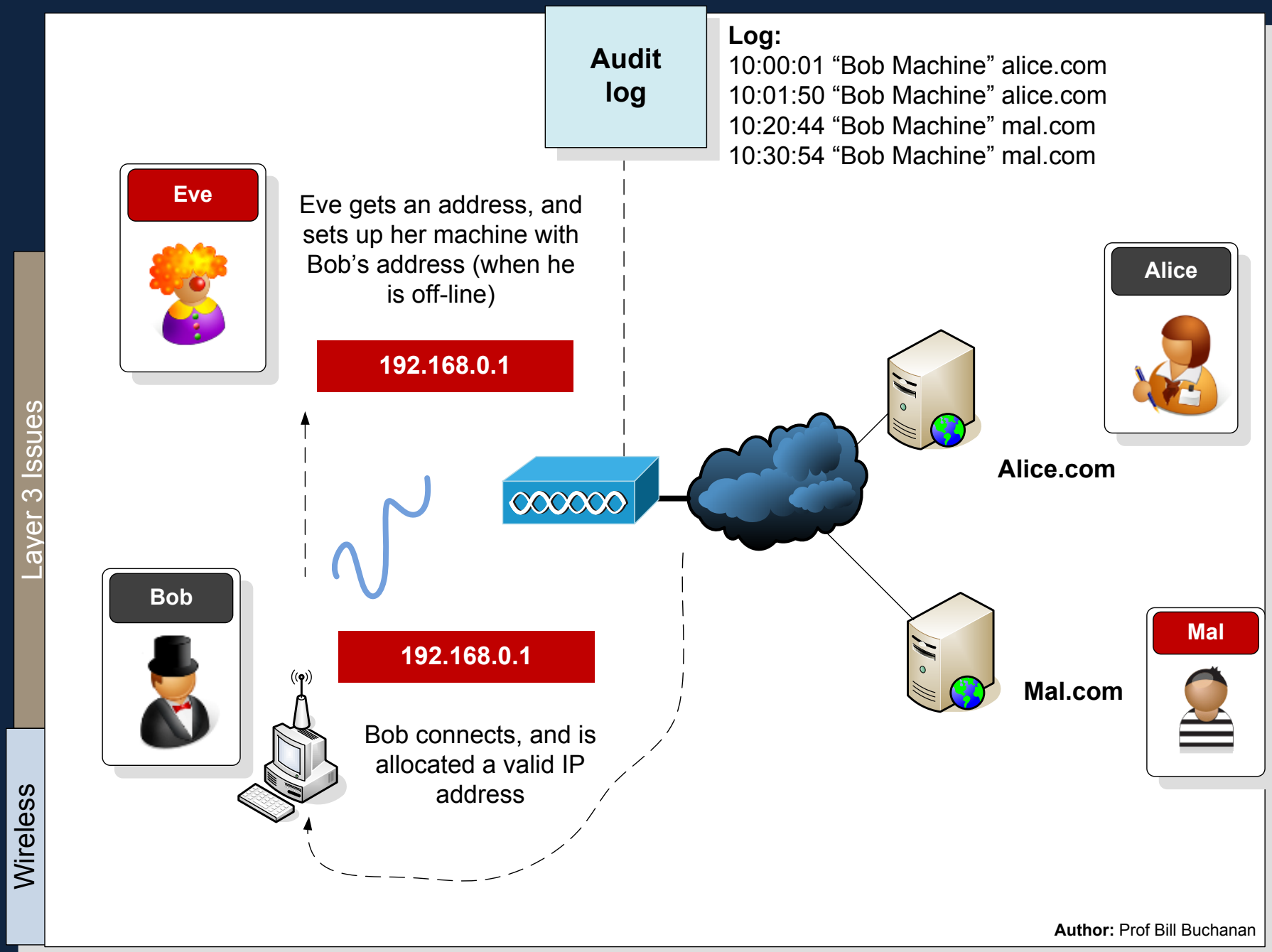
Eve changes to DNS record so that ebay.com points to ebay-bill.com

Eve setups up the access point so that it uses the poisoned DNS

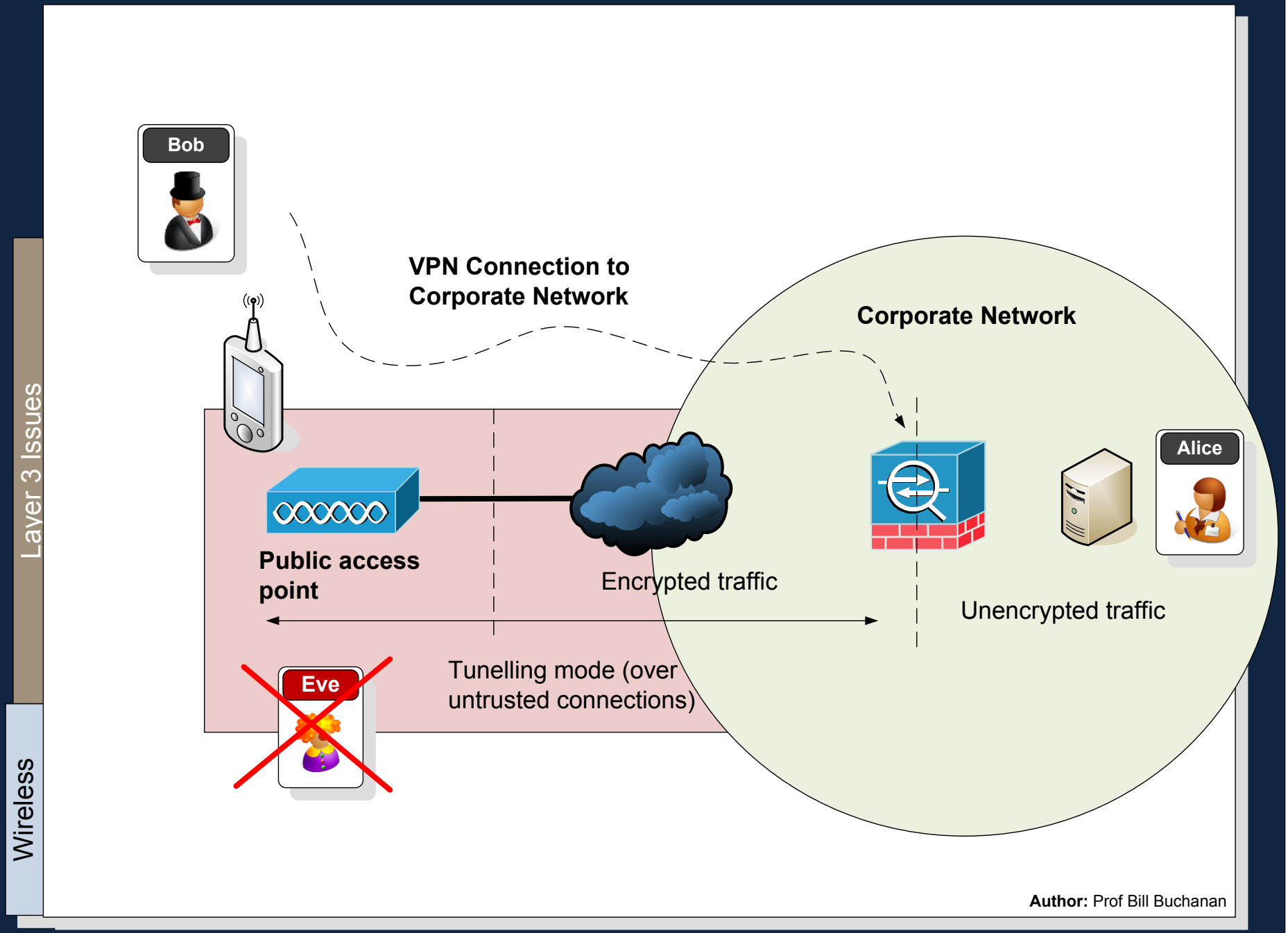
Author: Prof Bill Buchanan

Layer 3 Problems – DNS Poisoning


Layer 3 Issues
Wireless
Once a connection is made, Eve can backtrack into the host
ConnectToMe.com
Mal
Private space
Public space
Alice
eBay server
Bob
Eve
eBay-bill server
Mal
Eve sends data to the wrong site
Eve changes the NAT table to redirect traffic
Author: Prof Bill Buchanan

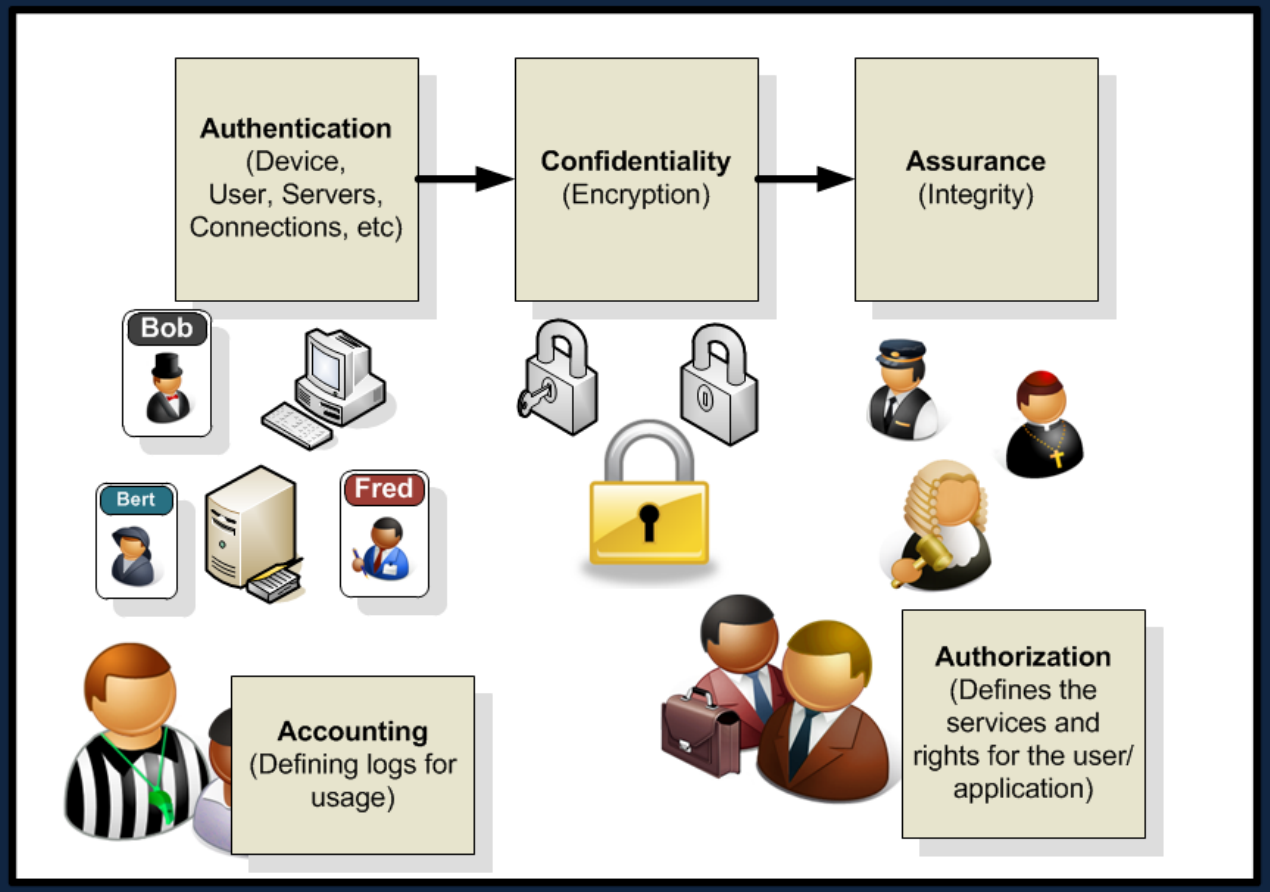


Layer 3 Problems – IP Spoofing



Layer 3 Issues – Tunnelling over Public Networks

Wireles Forensics



Access Point Basics

Author: Prof Bill Buchanan

Wireless Access point

Sky Broadband:
90.192.0.0 - 90.206.255.255
90.207.0.0 - 90.207.223.255
90.208.0.0 - 90.213.255.255

Typical defaults:
192.168.0.x
192.168.1.x

Netgear basics

Wireless

Ethernet Or Phone Line Connection (ASDL)

Public address space

Network Address Translation (NAT)

Firewall/Content Filtering

Web Server (Default: 192.168.1.1)

DHCP Server (Default: 192.168.1.x)

Log/Auditing

SNMP Service

Private address space

SSID beacon
(Channel 1-13)

Author: Prof Bill Buchanan

Wireless Access point

Sky Broadband:
90.192.0.0 - 90.206.255.255
90.207.0.0 - 90.207.223.25
90.208.0.0 - 90.213.255.25

Typical defaults:

Netgear basics

Wireless

Ethernet Or Phone Line Connection (ASDL)

Public address space

Firefox

Query the RIPE Database | NETGEAR Router WNR1000v2

http://www.db.ripe.net/whois?form_type=simple&full_query_string=&sea

dns server for wireless

You are here: Home > Data & Tools > RIPE Database > Whois

Query the RIPE Database

Search for BSKYB-BROADBAND Search Reset Form

By pressing the "Search" button you explicitly express your agreement with the RIPE Database Terms and Conditions.

Advanced Search Form

Switch to the RIPE TEST Database

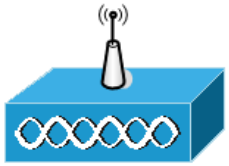
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf


% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.


% Information related to '90.192.0.0 - 90.199.255.255'


inetnum:        90.192.0.0 - 90.199.255.255
netname:        BSKYB-BROADBAND
descr:          Easynet Ltd
descr:          BSkyB Broadband
country:        GB
```

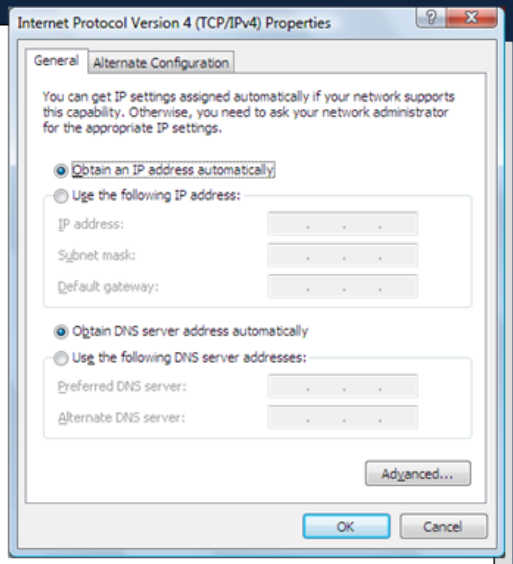
Find: Next Previous Highlight all Match case

Netgear basics

Wireless

Wireless Access point





90.192.1.1

Network Address Translation (NAT)

Firewall/Content Filtering

Web Server (Default: 192.168.1.1)

DHCP Server (Default: 192.168.1.x)

Log/Auditing

SNMP Service

192.168.1.1

IP Address
Subnet mask
Default gateway
DNS Server (Primary)
DNS Server (Secondary)

Public address space

Private address space

Author: Prof Bill Buchanan

Wireless Access point

Sky Broadband
90.192.0.0 - 90.2
90.207.0.0 - 90.2
90.208.0.0 - 90.2

```
> ipconfig /all
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11n Network Adapter
   Physical Address. . . . . . . . . : F8-1E-DF-E8-EC-BC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::44ee:8af7:4a22:be32%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.7(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 27 May 2011 06:13:58
   Lease Expires . . . . . . . . . . : 30 May 2011 06:13:58
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 234364639
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-D1-E3-88-F8-1E-DF-E8-EC-BC

   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Netgear basics

Wireless

Ethernet Or Phone Line Connectio (ASDL)

Public address space

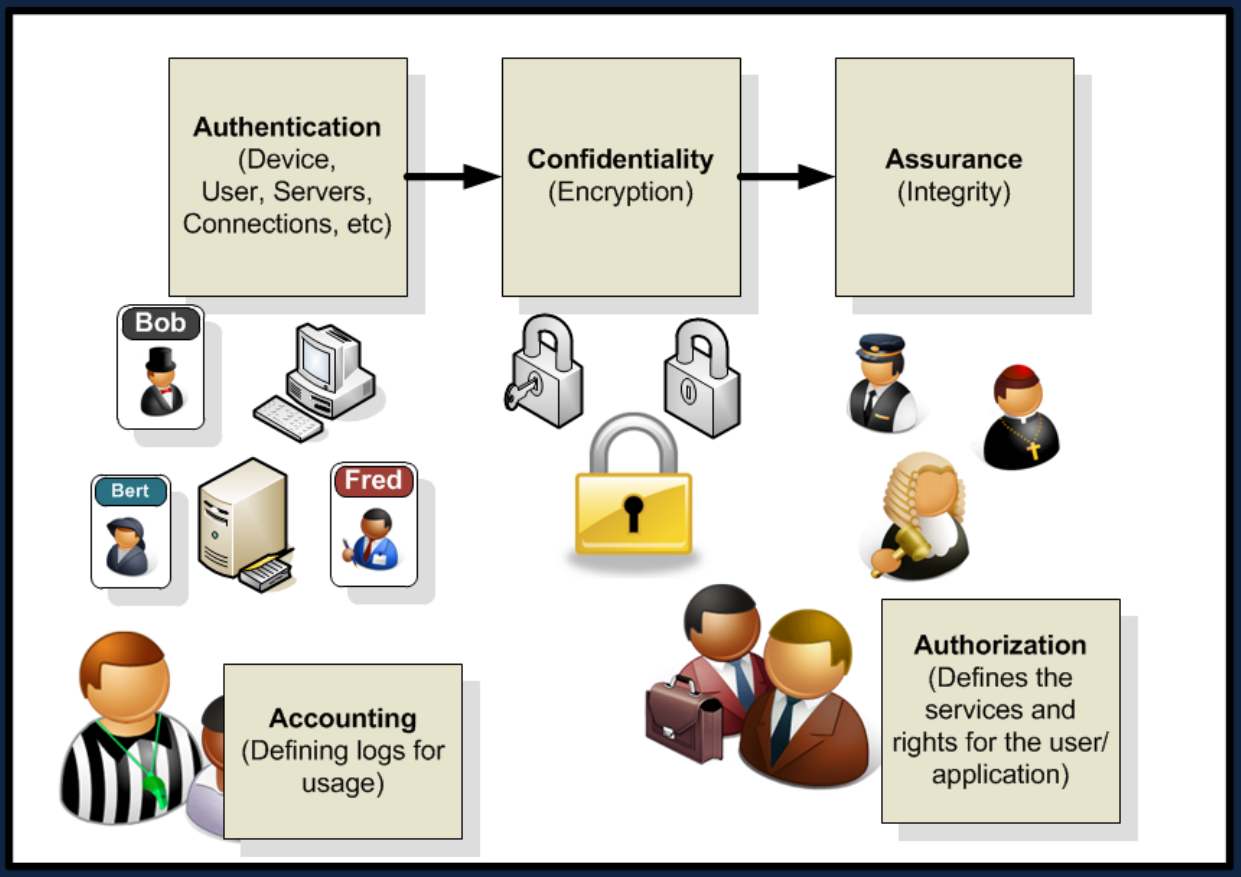
Log/Auditing

SNMP Service

Private address space

Author: Prof Bill Buchanan

Wireles Forensics



Device Configuration

Author: Prof Bill Buchanan

Wireless

Firefox

Query the RIPE Database | NETGEAR Router WNR1000v2

http://192.168.1.1/index.htm

dns server for wireless

NETGEAR SMARTWIZARD™ router manager

N150 Wireless Router model WNR1000v2

Select Language : Auto

Apply

- Setup Wizard
- Add WPS Client

Setup

- Basic Settings
- Wireless Settings

Content Filtering

- Logs
- Block Sites
- Block Services
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Backup Settings
- Set Password
- Router Upgrade

Advanced

- Wireless Settings
- Port Forwarding /

Wireless Settings

Wireless Network

☑ Enable SSID Broadcast

Name (SSID): NETGEAR

Region: Europe

Channel: Auto

Mode: Mbps

Security Options

- None
- WPA2-PSK [AES]
- WPA-PSK [TKIP] + WPA2
- WPA/WPA2 Enterprise

Ap Cancel

Auto, 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13

Wireless Help

NOTE: To ensure proper agency compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the router. For best results, place your router:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf.
- Away from potential sources of interference, such as PCs, microwave ovens, and cordless phones.
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

Find: Next Previous Highlight all Match case

al defaults:
68.0.x
68.1.x

SSID beacon
(Channel 1-13)

Wirele

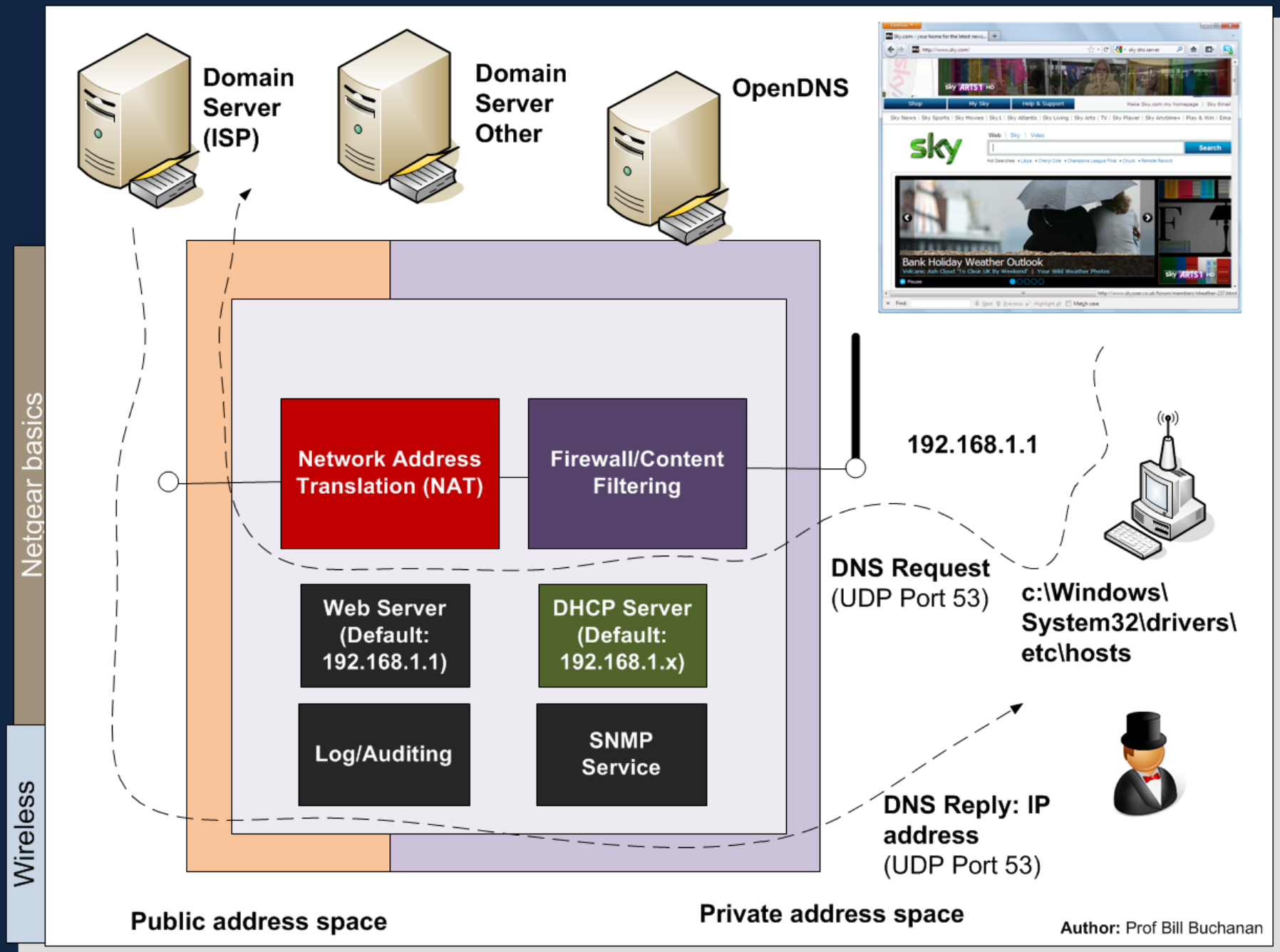
Public address space

Service

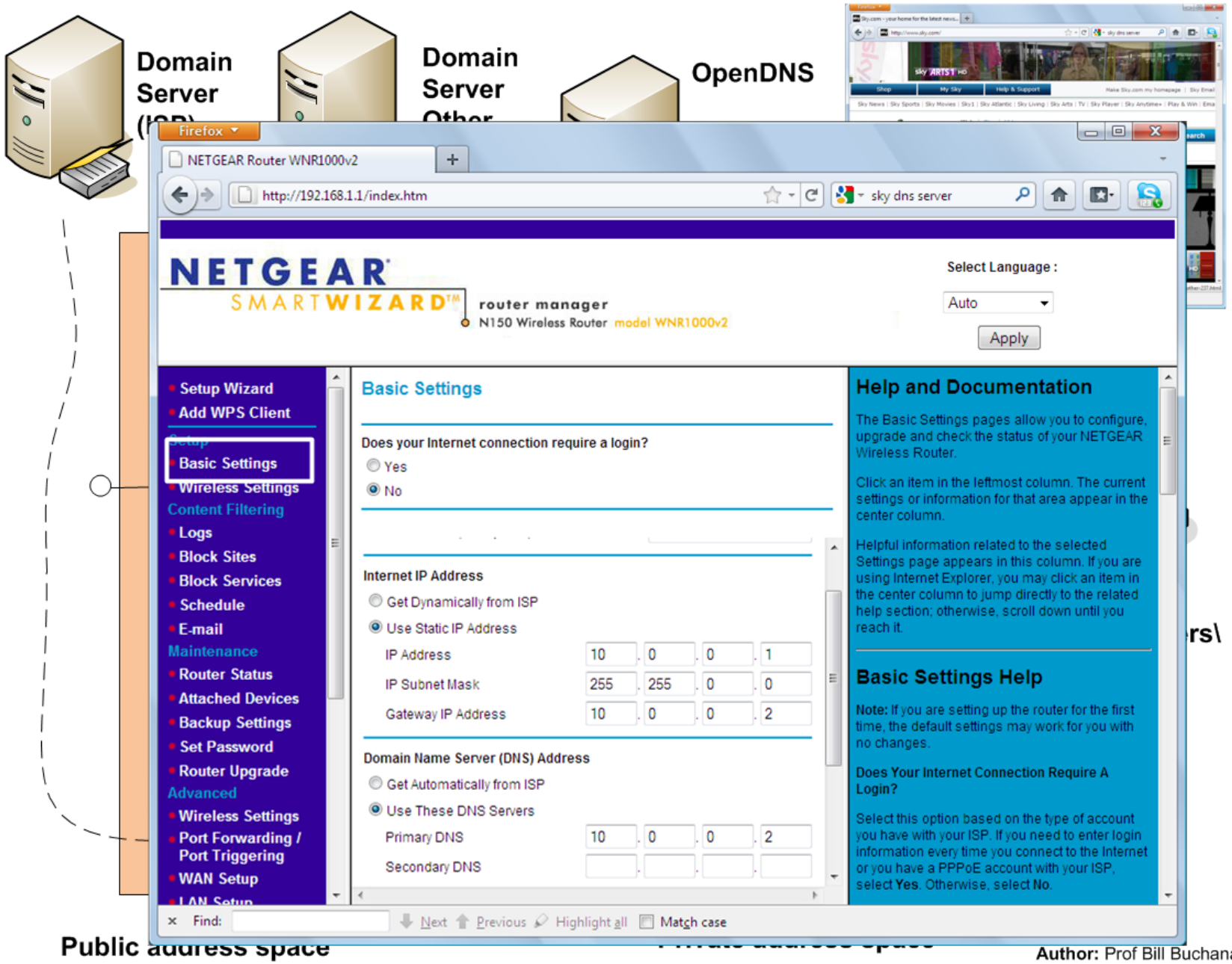
Private address space

Author: Prof Bill Buchanan

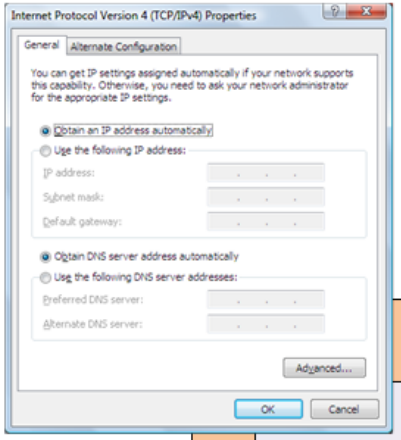
Netgear



Netgear (DNS Settings)

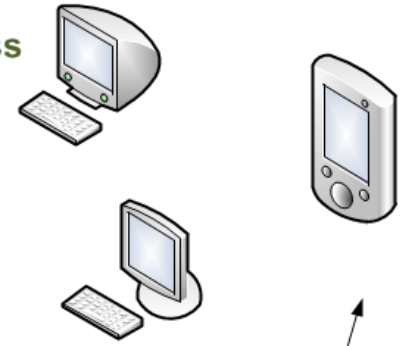


Netgear (DNS Settings)



Static mapping
55:44:33:22:11 -> 192.168.1.3

Static address



Netgear basics

Wireless

Network Address Translation (NAT)

Firewall/Content Filtering

Web Server (Default: 192.168.1.1)

DHCP Server (Default: 192.168.1.x)

Log/Auditing

SNMP Service

Dynamic address

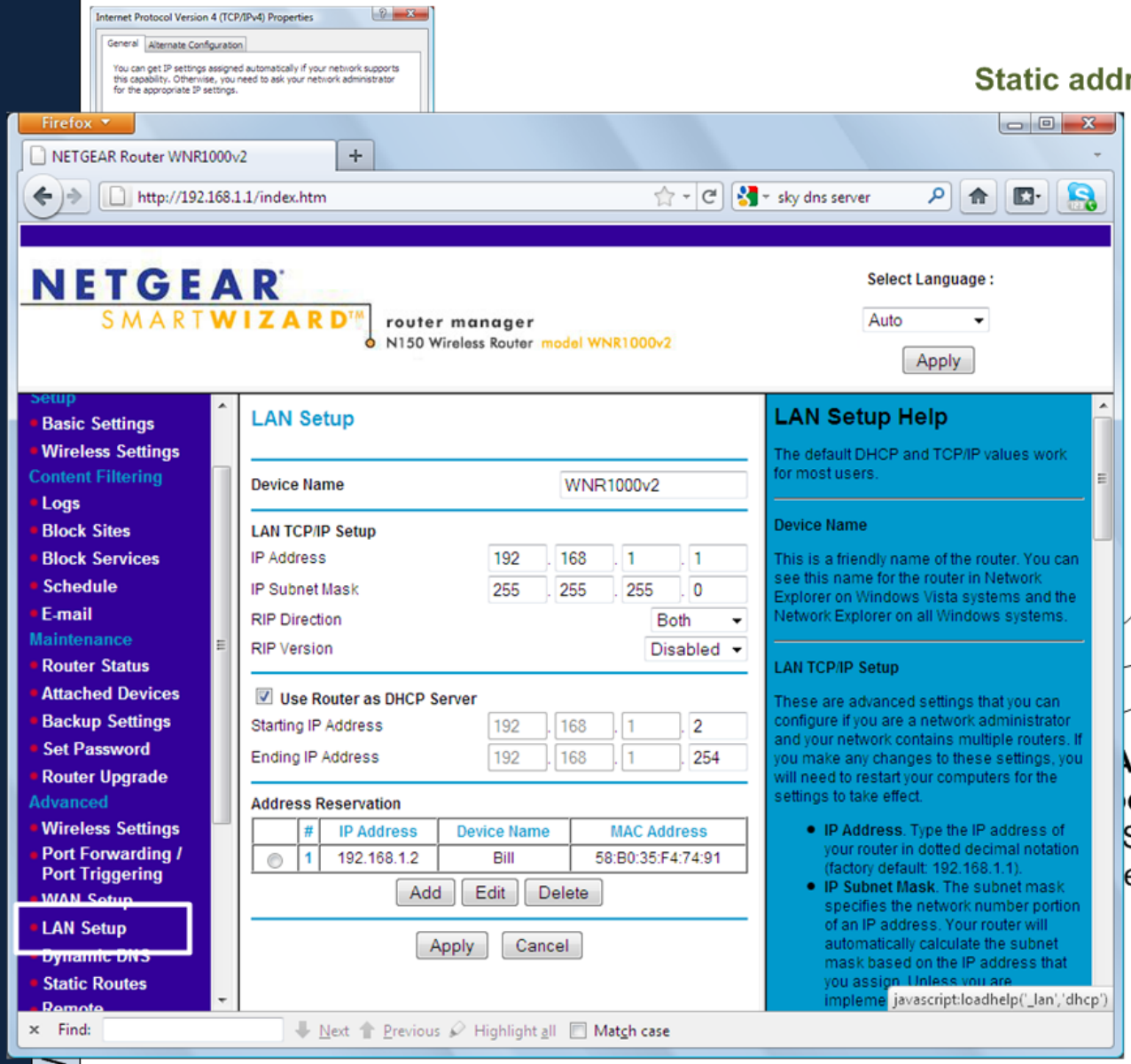
IP Address allocation
(IP/Subnet/DNS/ Gateway)

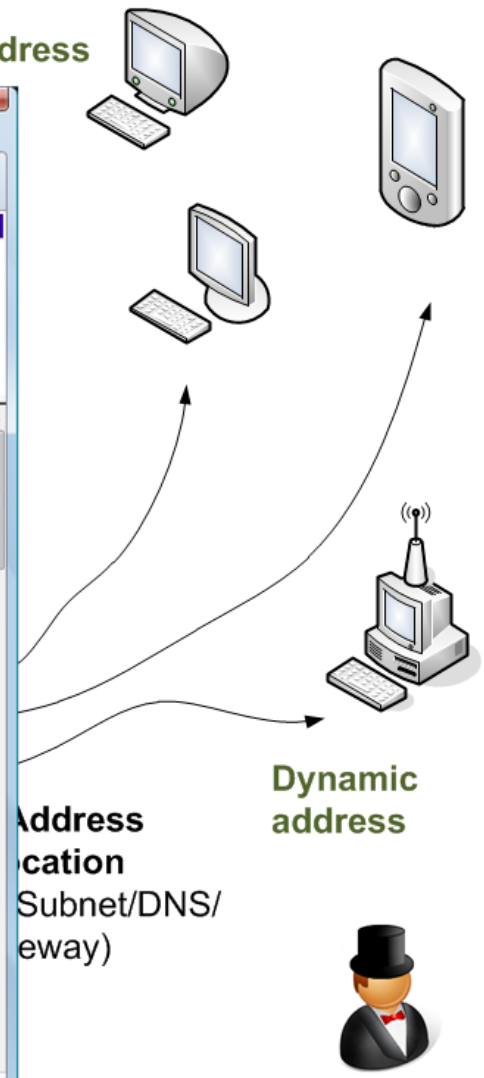
Public address space

Private address space

Author: Prof Bill Buchanan

Netgear (DHCP Settings)





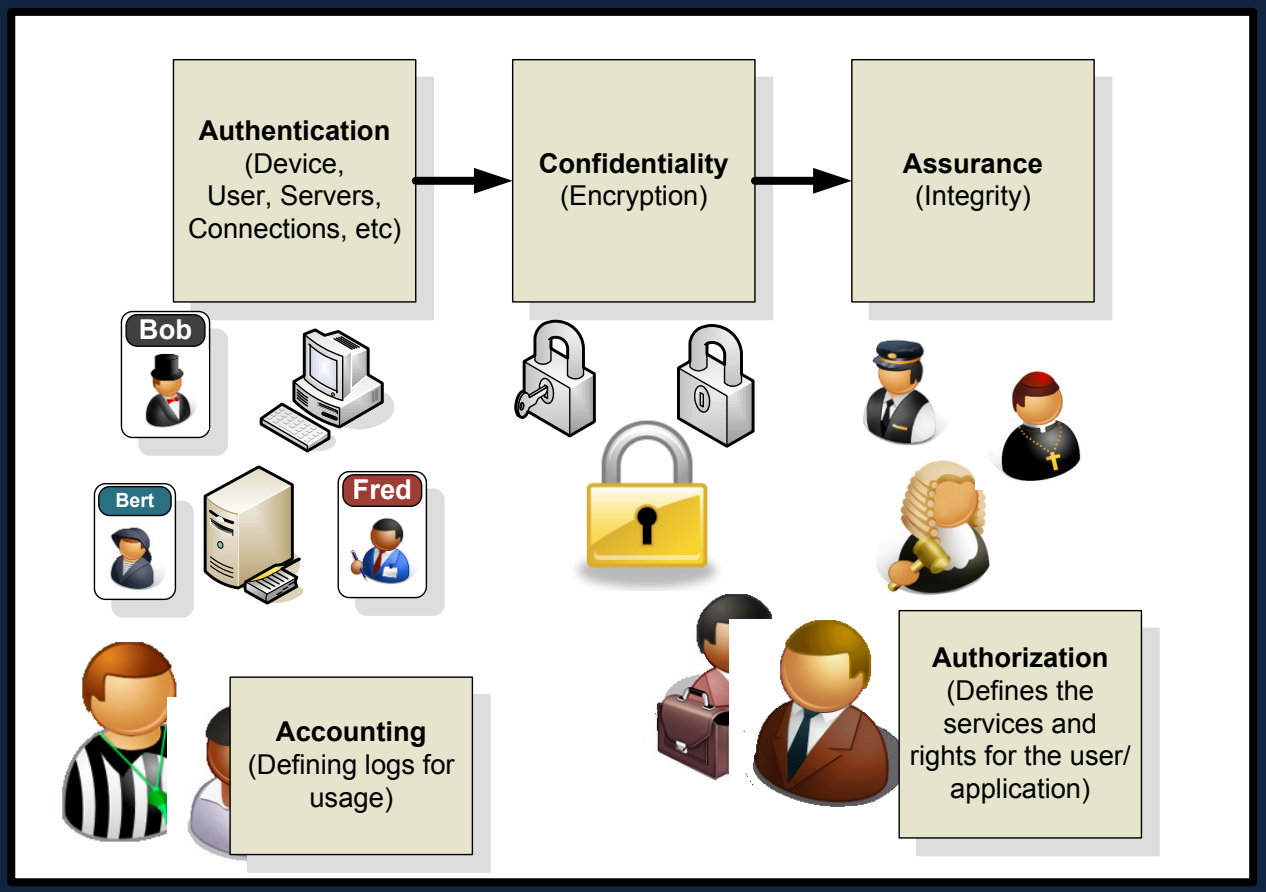
Public address space

Private address space

Author: Prof Bill Buchanan

Netgear (DHCP Settings)

Wireless Security



Security Standards

Author: Prof Bill Buchanan

Security Standards

Wireless

Wireless Security

IPSec standards for VPNs

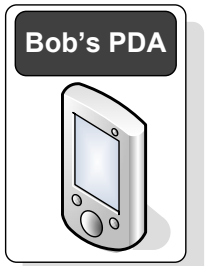
- Limited to IP
- Required for public access systems

Wireless security standards

Encryption

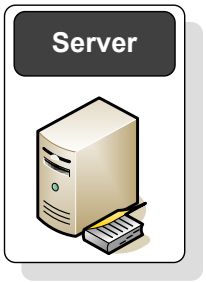
- **WEP** - Wireless Encryption Protocol (RC4)
- **WPA** - Wireless Protected Access (RC4)
- **IEEE 802.11i** (AES)

Authentication

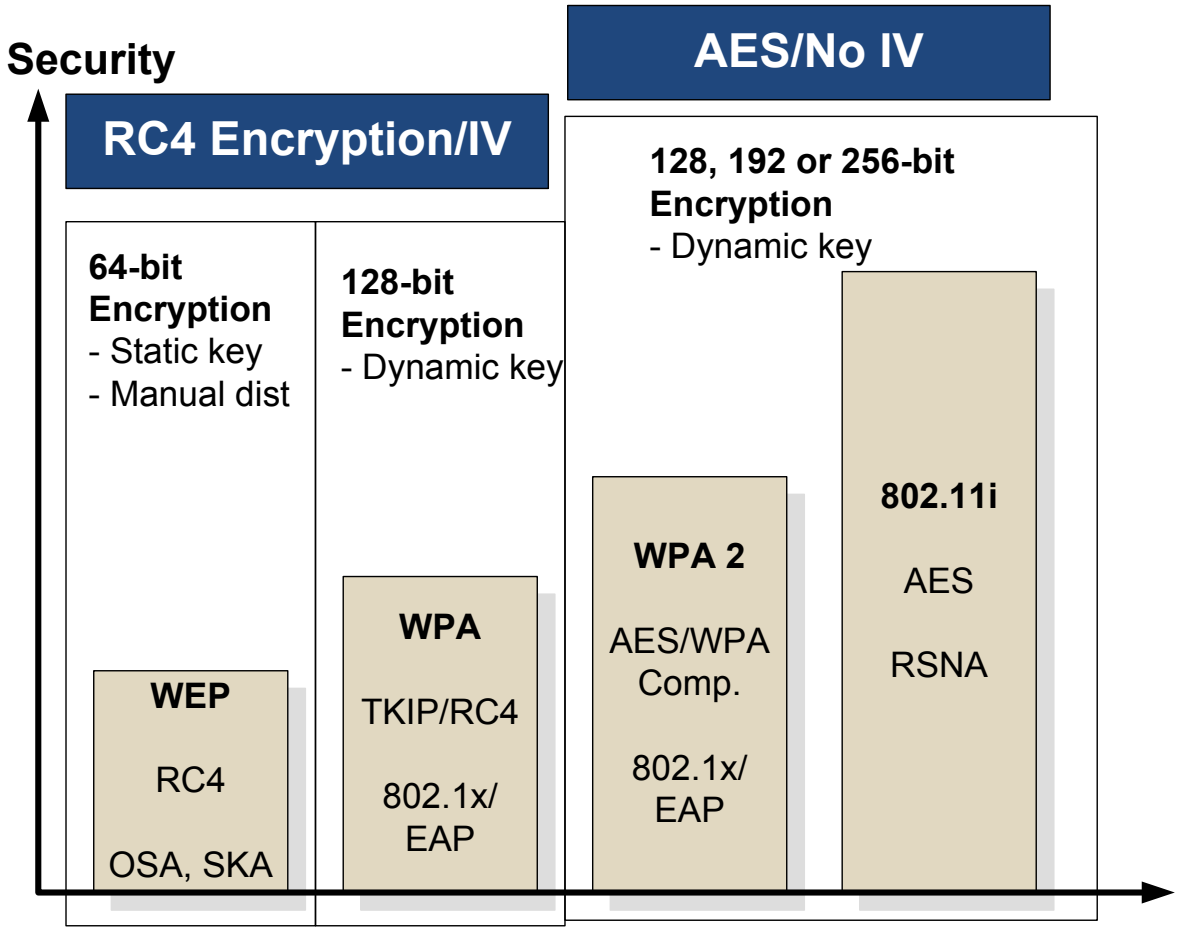


802.1x/EAP:

- **EAPS** - Extensible Authentication Protocol
- **LEAP** - Lightweight EAP
- **EAP-TLS** - EAP - Transport Layer Security
- **EAP-TTLS** - Tunnelled TLS
- **PEAP** - Protected EAP



Author: Prof Bill Buchanan



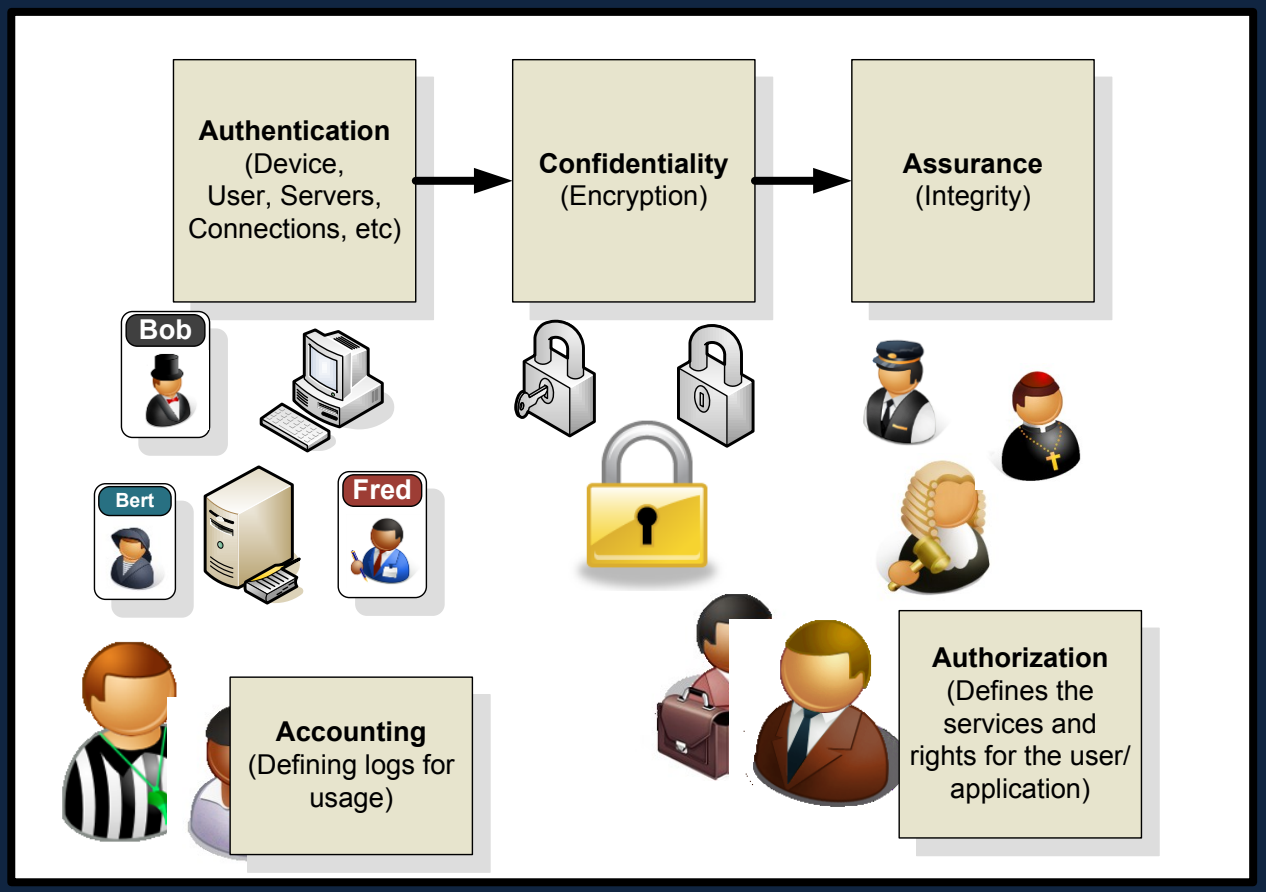
WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard

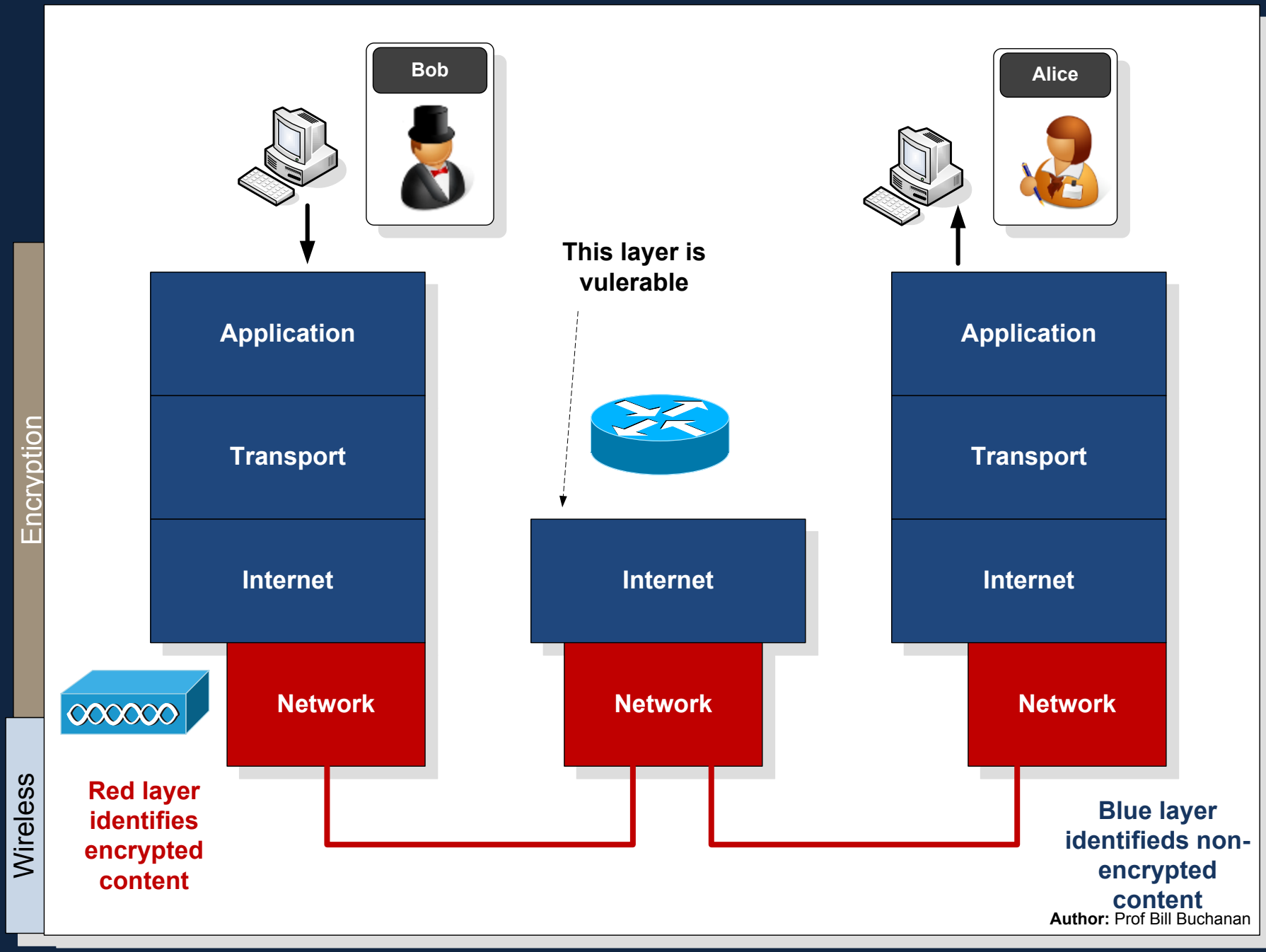
Author: Prof Bill Buchanan

Wireless Security

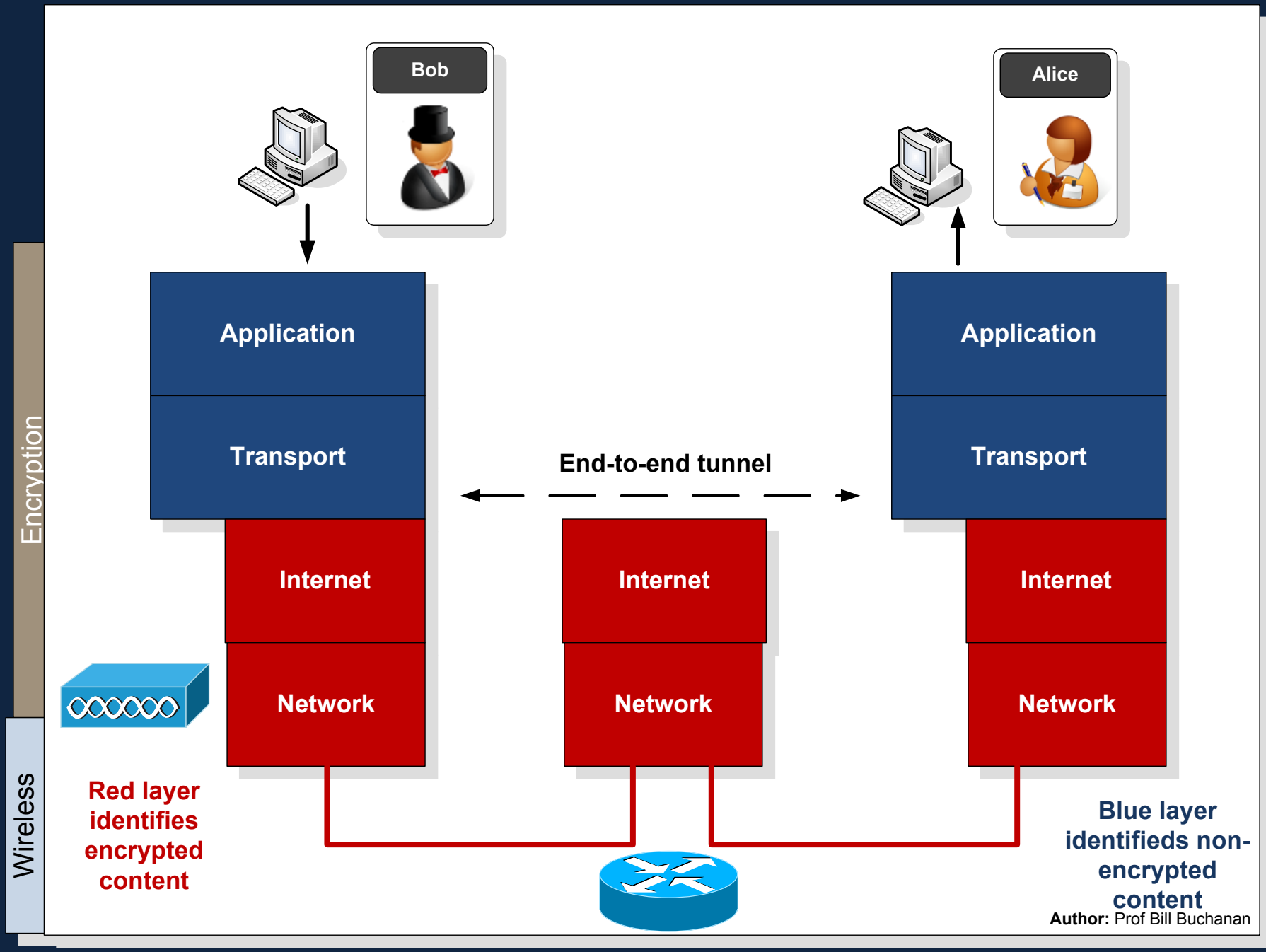


Encryption Scope

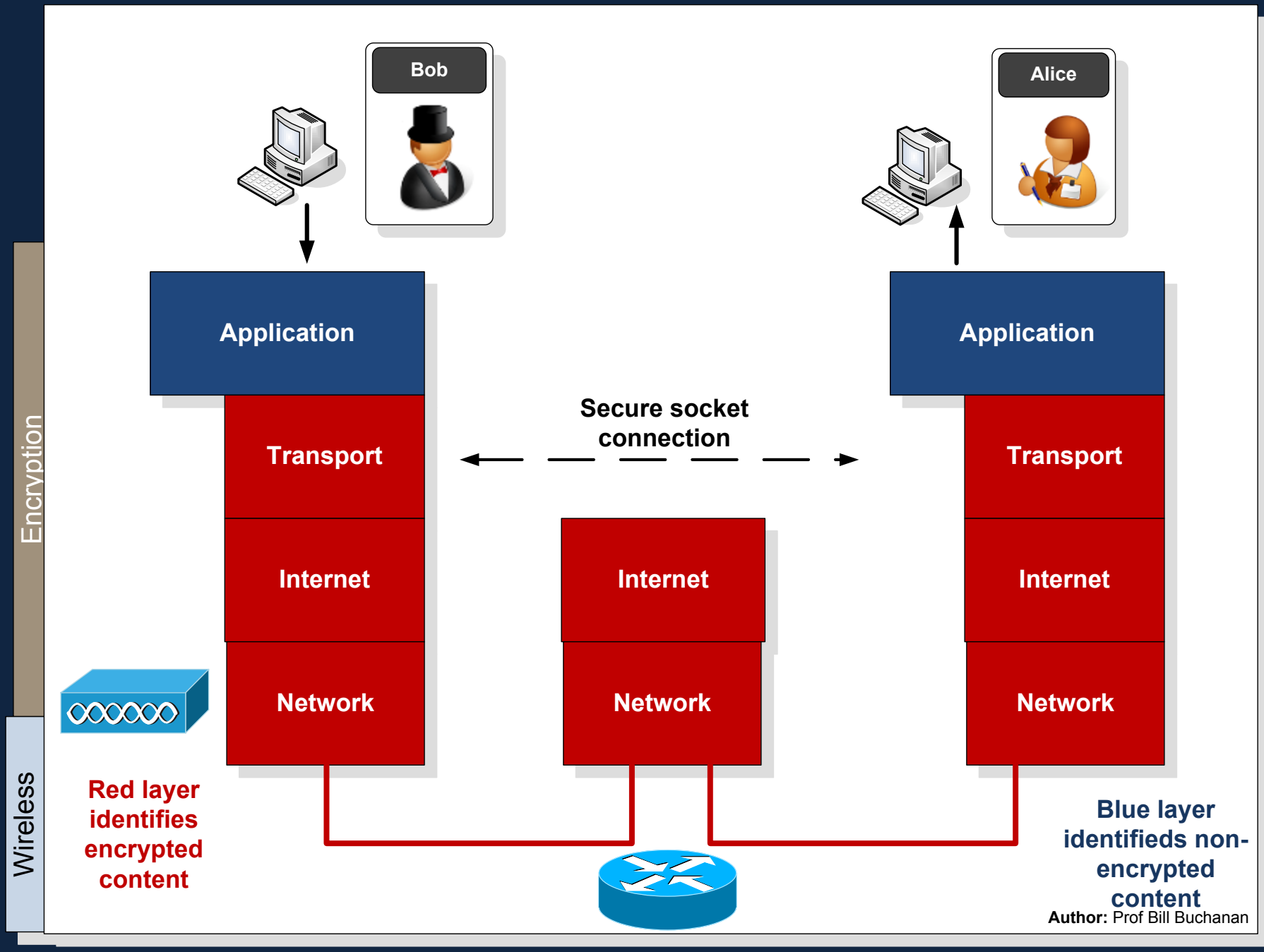
Author: Prof Bill Buchanan



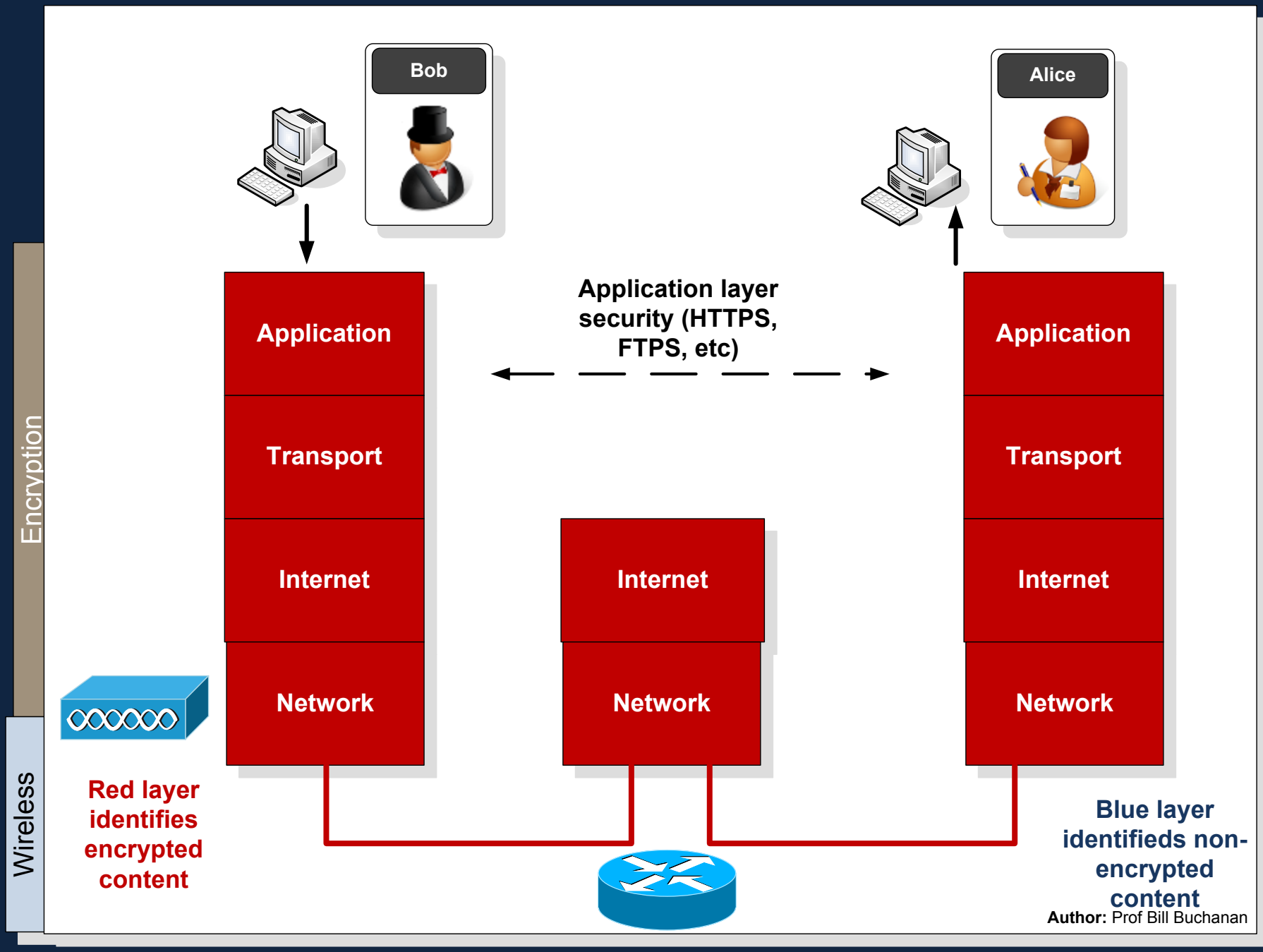
Scope of wireless encryption (Point-to-point encryption)



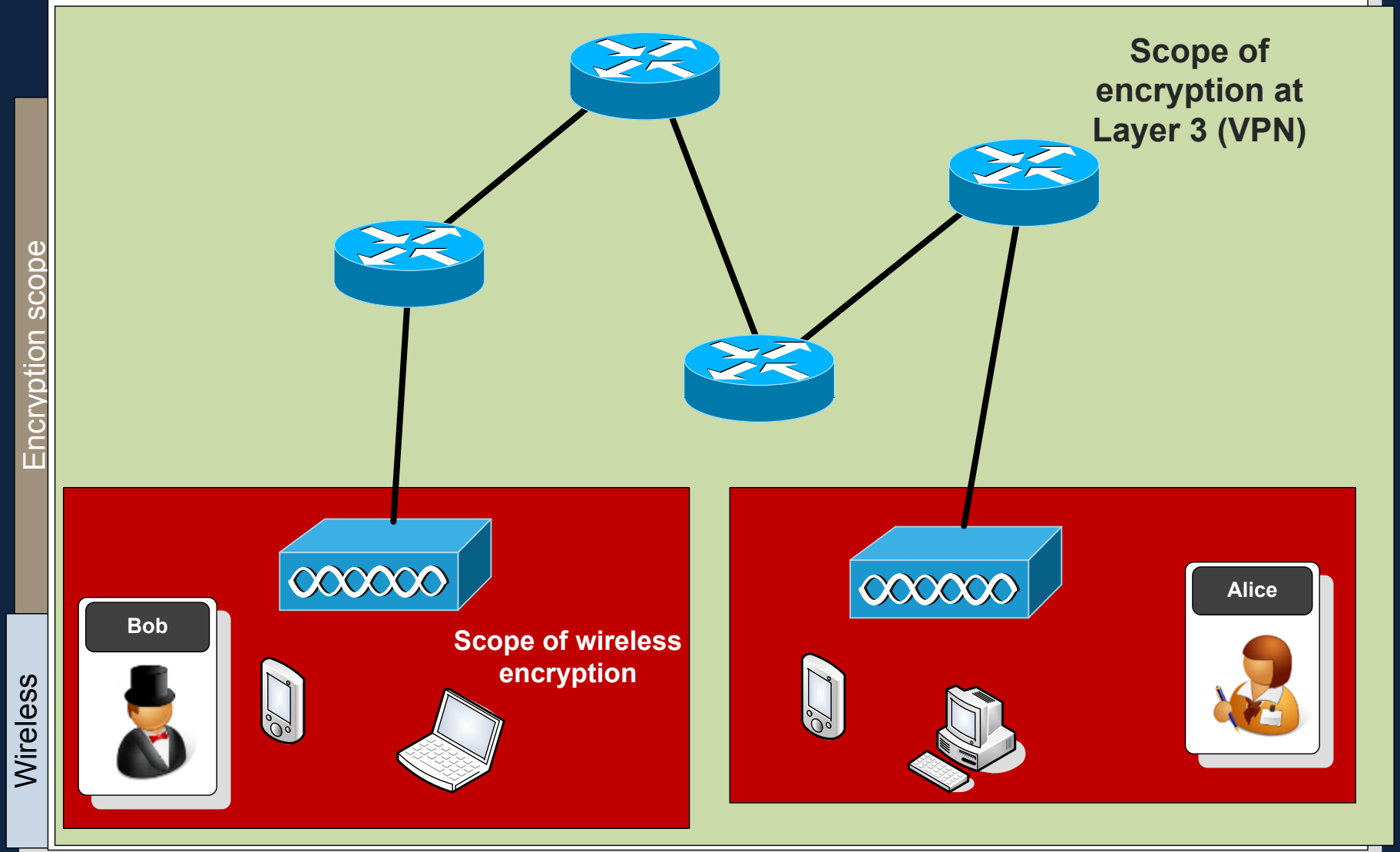
Scope of VPN security



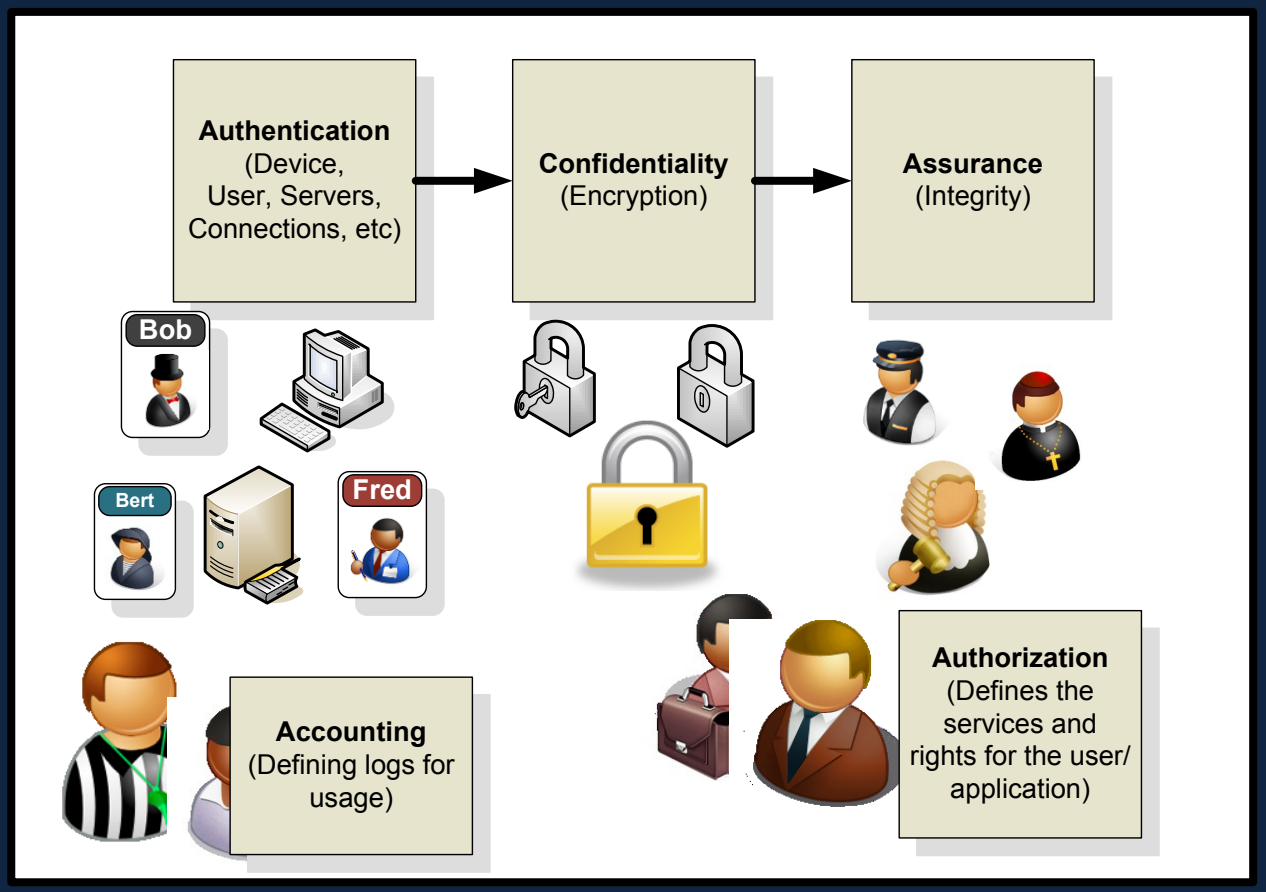
Transport Layer Security (SSL)



Application Layer Security


Encryption scope
Wireless
Scope of encryption at Layer 3 (VPN)
Bob
Scope of wireless encryption
Alice

Wireless Security



WEP

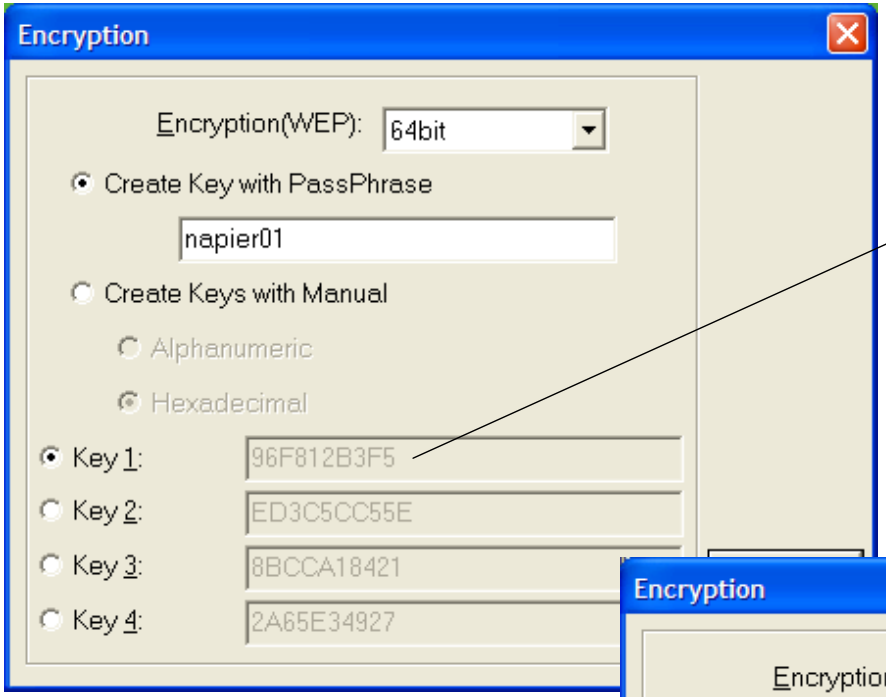
Author: Prof Bill Buchanan

Encryption

Wireless

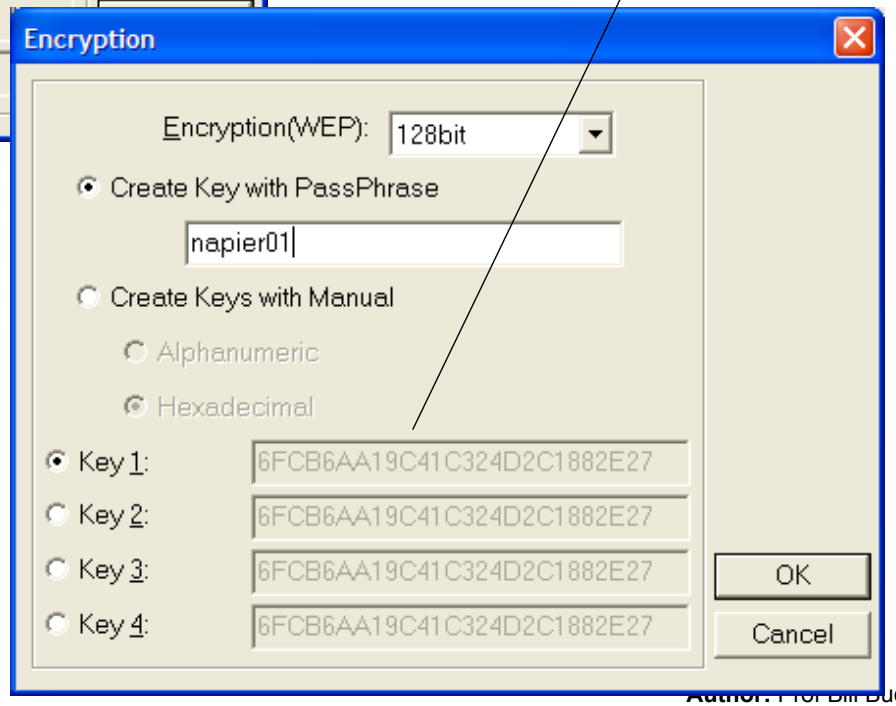
WEP encryption key reduces eavesdropping

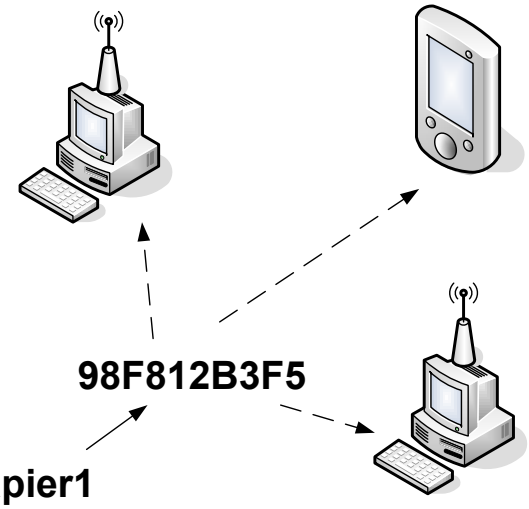
It stops unauthorized access to a Wireless Access Point (along with the SSID, of course)



40-bit Keys (24 bits for IV)

104-bit Keys (24 bits for IV)





Author: Prof Bill Buchanan

Generating the WEP key

Encryption

Wireless

Belkin 802.11g Wireless Card

Status | Configure | Security | Available Networks | Profiles | Statistics

No Encryption

Enable WPA Encryption

Enable WEP Encryption

Create with Passphrase

Passphrase: cisco

Key Length: 64 Bit

Manual Entry

Encryption Key (Hex 0-9 A-F)

		Key Length
Key 1:	D7B338D13D	64 Bit
Key 2:	447C5CCF32	64 Bit
Key 3:	07FE624C78	64 Bit
Key 4:	A7B7A6AB91	64 Bit

BELKIN

Close | Apply

Belkin 802.11g Wireless Card

Status | Configure | Security | Available Networks | Profiles | Statistics

Network SSID	Signal	Encryption	Channel	MAC Address
NapAir	58 %	WPA	1	00:14:69:04:FD:C
C06Air2	70 %	None	3	00:0D:65:72:C1:E
fred	100 %	WEP	6	BE:84:02:72:ED:
Lynksys	84 %	None	6	00:06:25:4B:1C:2
C06Air3	75 %	None	8	00:07:50:D5:BF:4
C06Air	80 %	None	11	00:14:BF:02:79:2
C06Air1	75 %	None	11	00:14:BF:02:79:2

Connect

Site Survey Status

Complete

Re-Scan

BELKIN

Close | Apply

Author: Prof Bill Buchanan

64-bit WEP

Encryption

Wireless

Belkin 802.11g Wireless Card

Status | Configure | Security | Available Networks | Profiles | Statistics

No Encryption

Enable WPA Encryption

Enable WEP Encryption

Create with Passphrase

Key Length

Passphrase: cisco 128 Bit

Manual Entry

Encryption Key (Hex 0-9 A-F)

Key Length

Key 1: 726CFA06B7C17D8F48B6313CE4 128 Bit

Key 2: 726CFA06B7C17D8F48B6313CE4 128 Bit

Key 3: 726CFA06B7C17D8F48B6313CE4 128 Bit

Key 4: 726CFA06B7C17D8F48B6313CE4 128 Bit

BELKIN

Close Apply

Belkin 802.11g Wireless Card

Status | Configure | Security | Available Networks | Profiles | Statistics

Network SSID	Signal	Encryption	Channel	MAC Address
fred	100 %	WEP	6	96:7F:5F:1F:40:D
NapAir	51 %	WPA	1	00:14:69:04:FD:C
C06Air2	70 %	None	3	00:0D:65:72:C1:E
Lynksys	70 %	None	6	00:06:25:4B:1C:2
C06Air3	75 %	None	8	00:07:50:D5:BF:4
C06Air1	72 %	None	11	00:14:BF:02:79:2
C06Air	80 %	None	11	00:14:BF:02:79:2

Connect

Site Survey Status

Complete

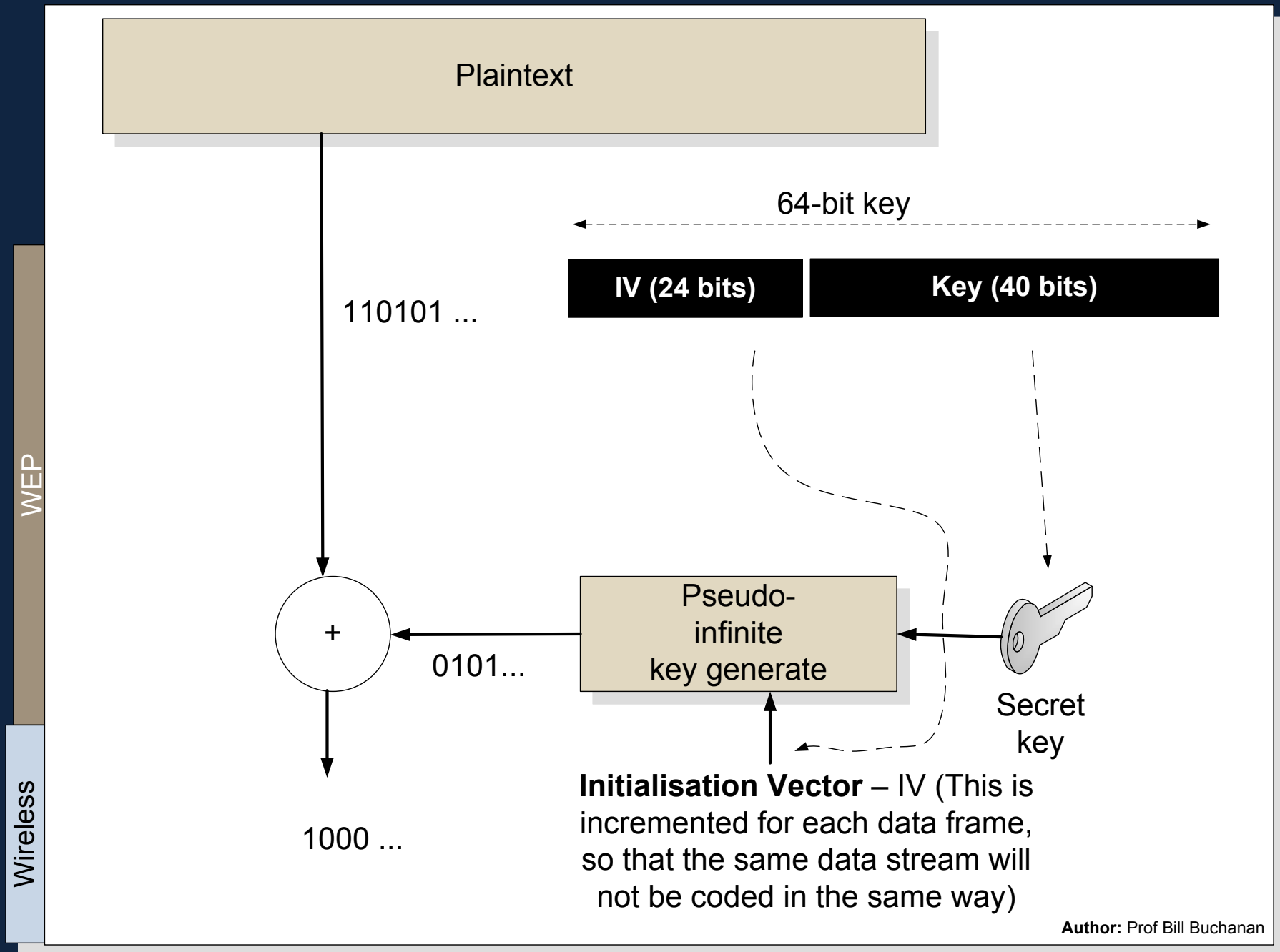
Re-Scan

BELKIN

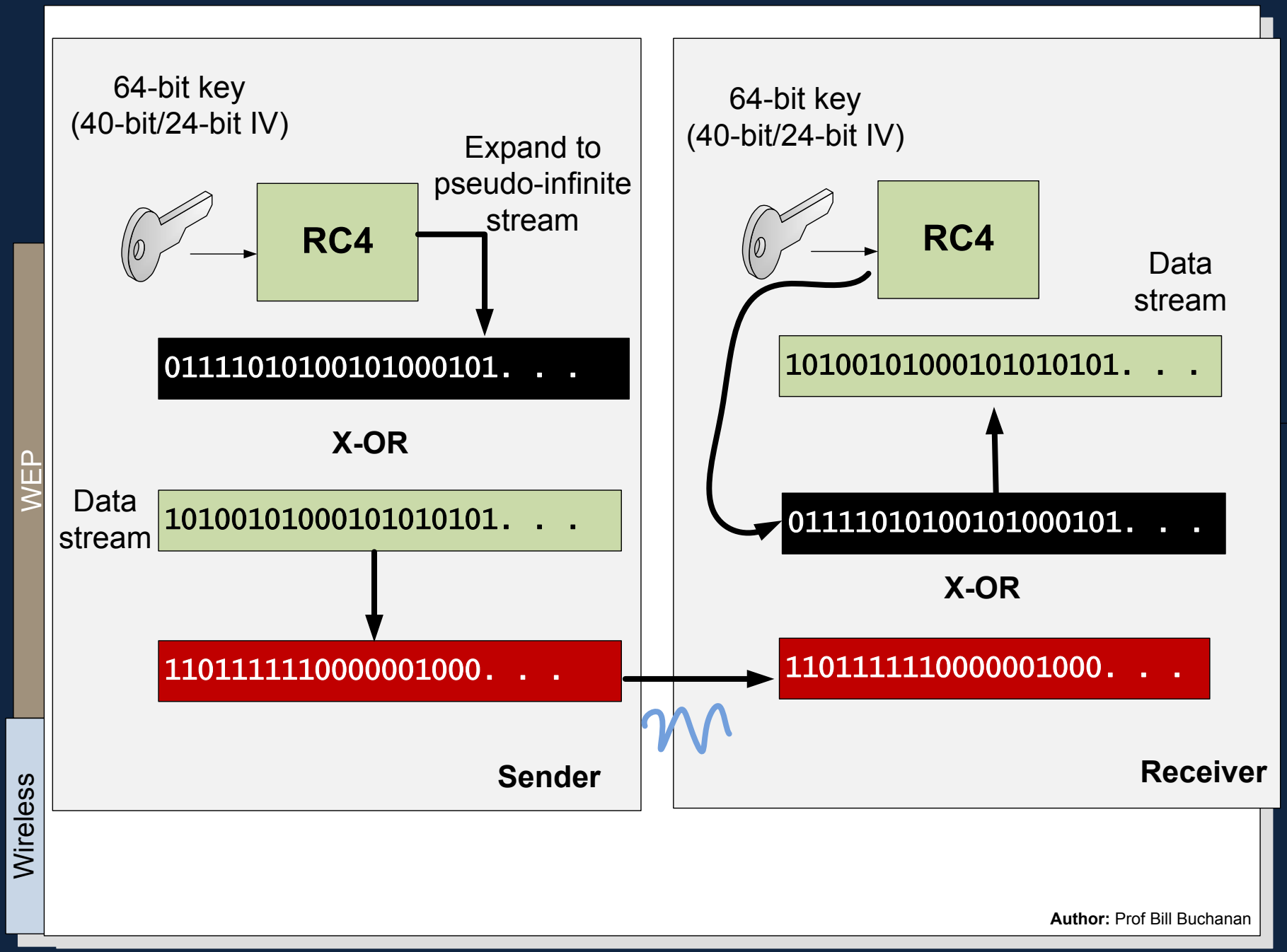
Close Apply

Author: Prof Bill Buchanan

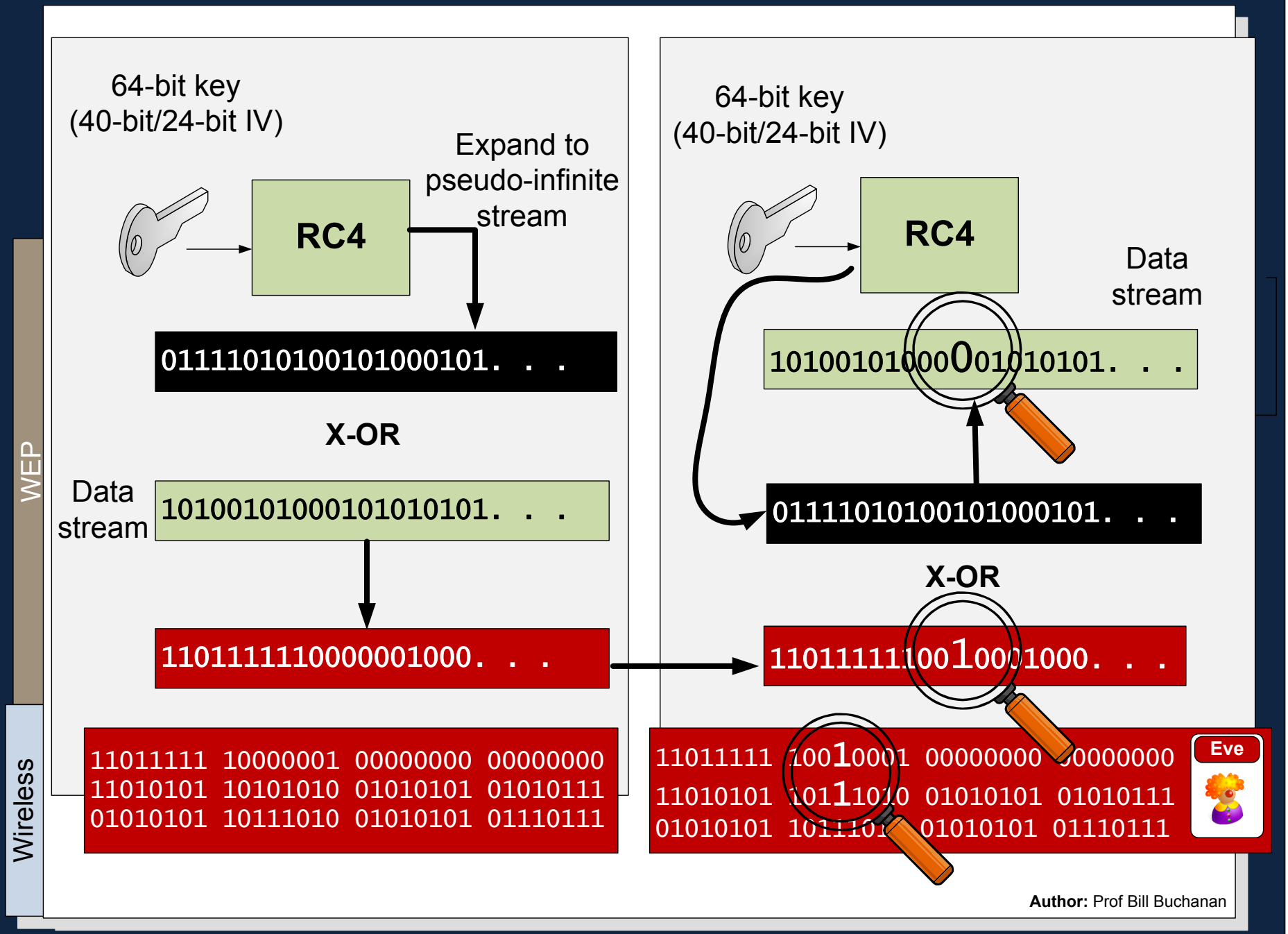
64-bit WEP



WEP - RC4 Encryption



WEP - RC4 Encryption



WEP - RC4 Encryption – Bit flipping

The IV is a 24-bit value, which is sent as **cleartext**.

There can only be 2^{24} vectors (16,777,216)

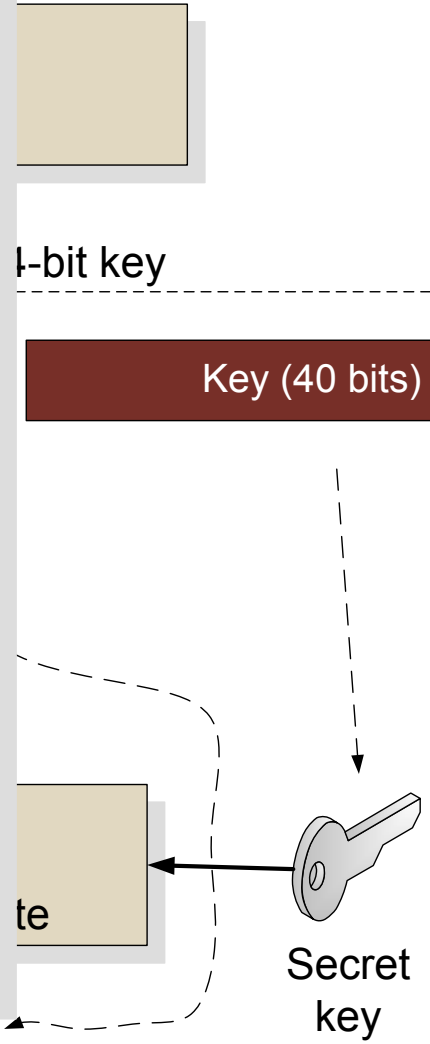
If we use 1500 byte packets, the time to send each packet is 150x8/11e6 = 1.1ms

Thus, if the device is continually sending the same vector will repeat after:

1.1ms 16,777,216 = 18,302.4 seconds

which is **5 hours**

The attacker then takes the two cipertexts which have been encrypted with the same key, and performs a statistical analysis on it.



Wireless

1000 ...

Initialisation Vector – IV (This is incremented for each data frame, so that the same data stream will not be coded in the same way)

Author: Prof Bill Buchanan

WEP

Wireless

IV=0	Ciphertext1
IV=1	Ciphertext2
IV=2	Ciphertext3
IV=16,777,215	Ciphertext1677215
IV=0	Ciphertext1a
IV=1	Ciphertext2a

Eve listens for a reoccurrence of the same IV vector, and then X-OR's the cipher stream, and does a frequency analysis on the result (within five hours it is crackable)

Ciphertext1

X-OR

Ciphertext1a

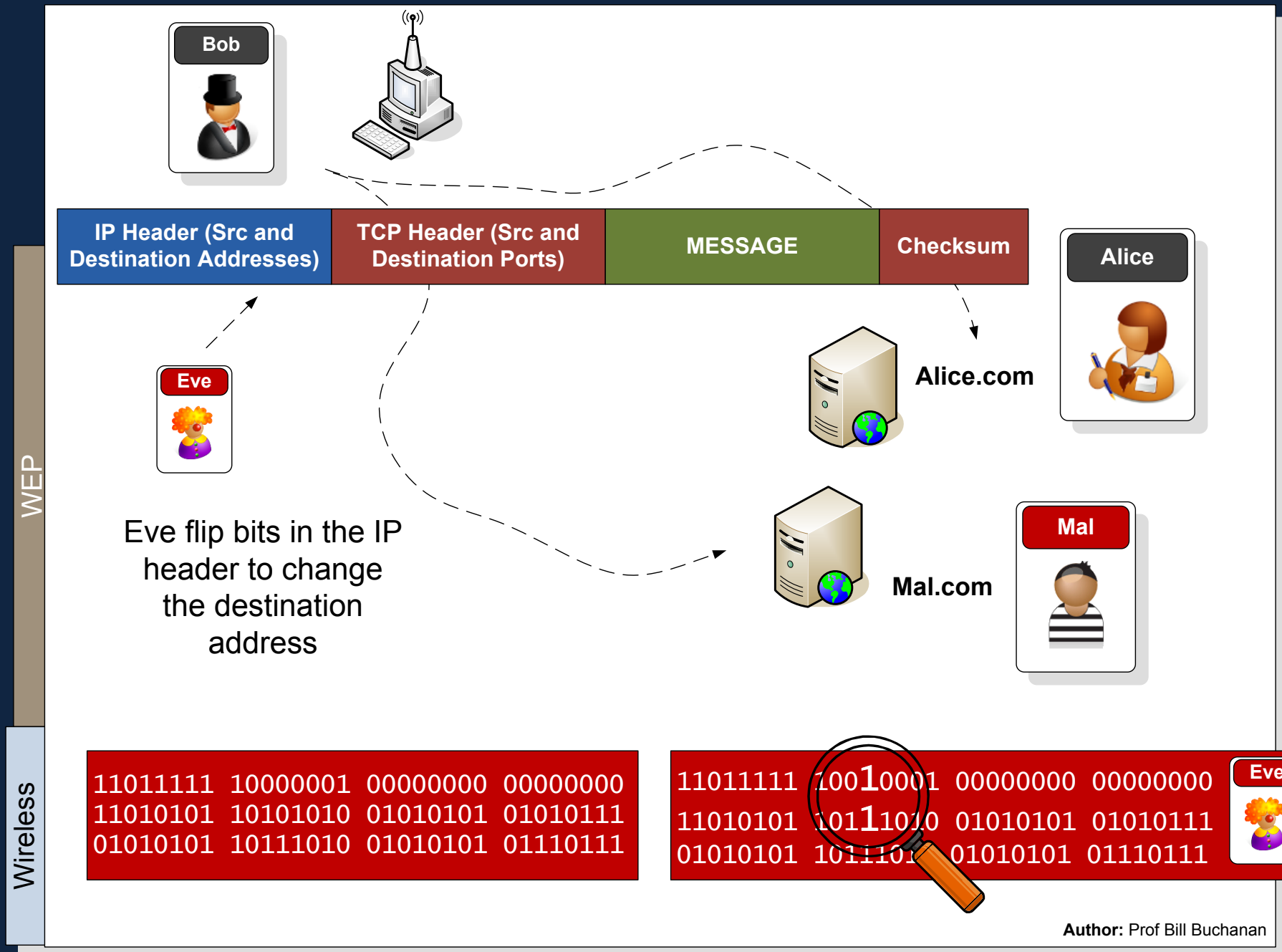
Ciphertext2

X-OR

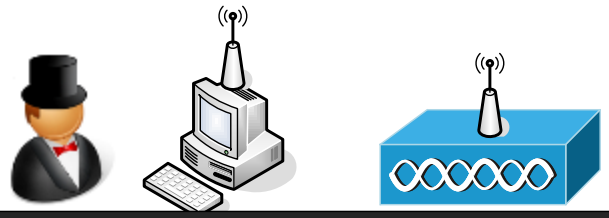
Ciphertext2a

Author: Prof Bill Buchanan

WEP - RC4 Encryption (WEP Cracking)



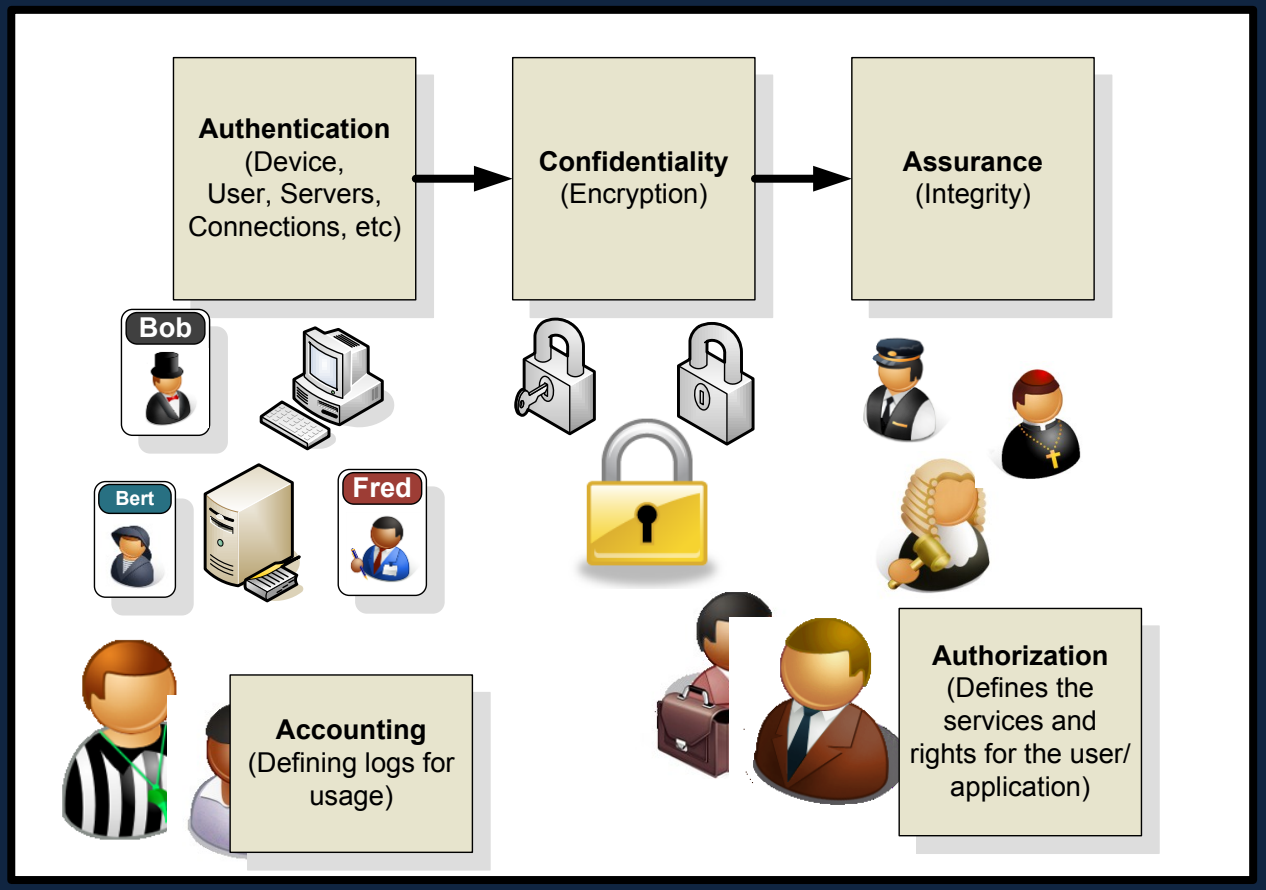
WEP - RC4 Encryption – Bit flipping



```
# config t
(config)# int dot11radio0
(config-if)# encryption ?
  key    Set one encryption key
  mode   encryption mode
  vlan   vlan
(config-if)# encryption mode ?
  ciphers  Optional data ciphers
  wep      Classic 802.11 privacy algorithm
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 40bit 1122334455 transmit-key
(config)# exit
(config)# int dot11radio0
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 128bit 12345678901234567890123456
   transmit-key
(config)# exit
(config)# int dot11radio0
(config-if)# encryption mode cipher tkip wep128
(config-if)# encryption key 3 size 128bit 12345678901234567890123456
transmit-key
```

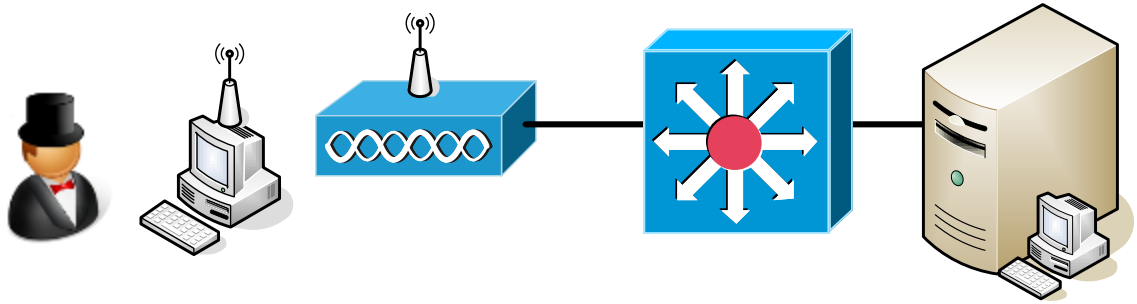

WEP Configuration

Wireless Security



IEEE 802.11i

Author: Prof Bill Buchanan



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.

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.

IEEE 802.1x | **IEEE 802.11i** | **EAP**

Author: Prof Bill Buchanan

Encryption

Wireless

TKIP (Temporal Key Integrity Protocol) which are enhancements to RC4-based WEP. The IV has been increased to 48 bits (rather that 24 bits), and the Integrity Checker has been improved. It uses a **session** key.

AES (Advanced Encryption Standard) – enhanced encryption using block encryption (not based on RC4)

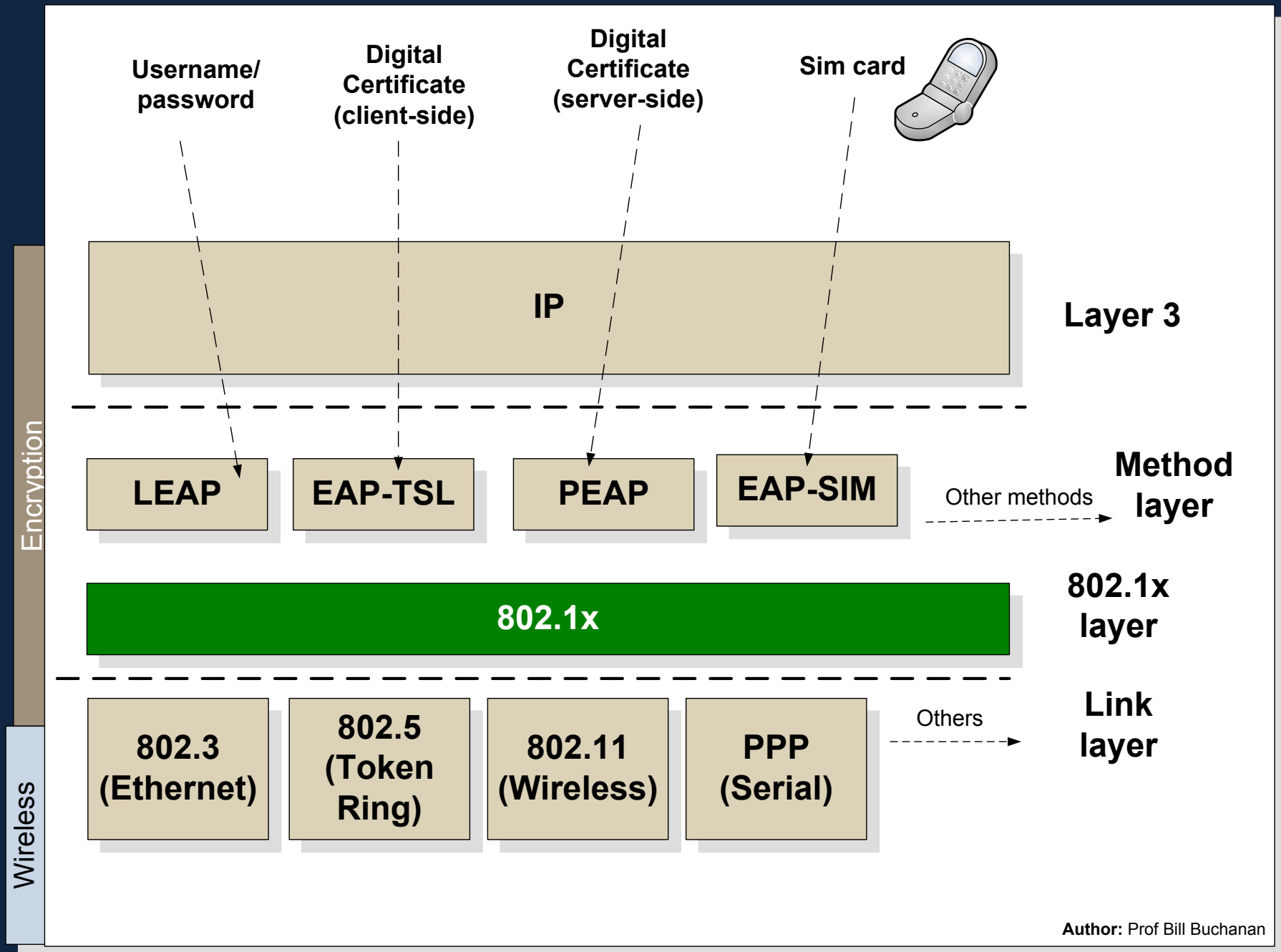
IEEE 802.1x (Authentication of both client and access point) - EAP

WPA

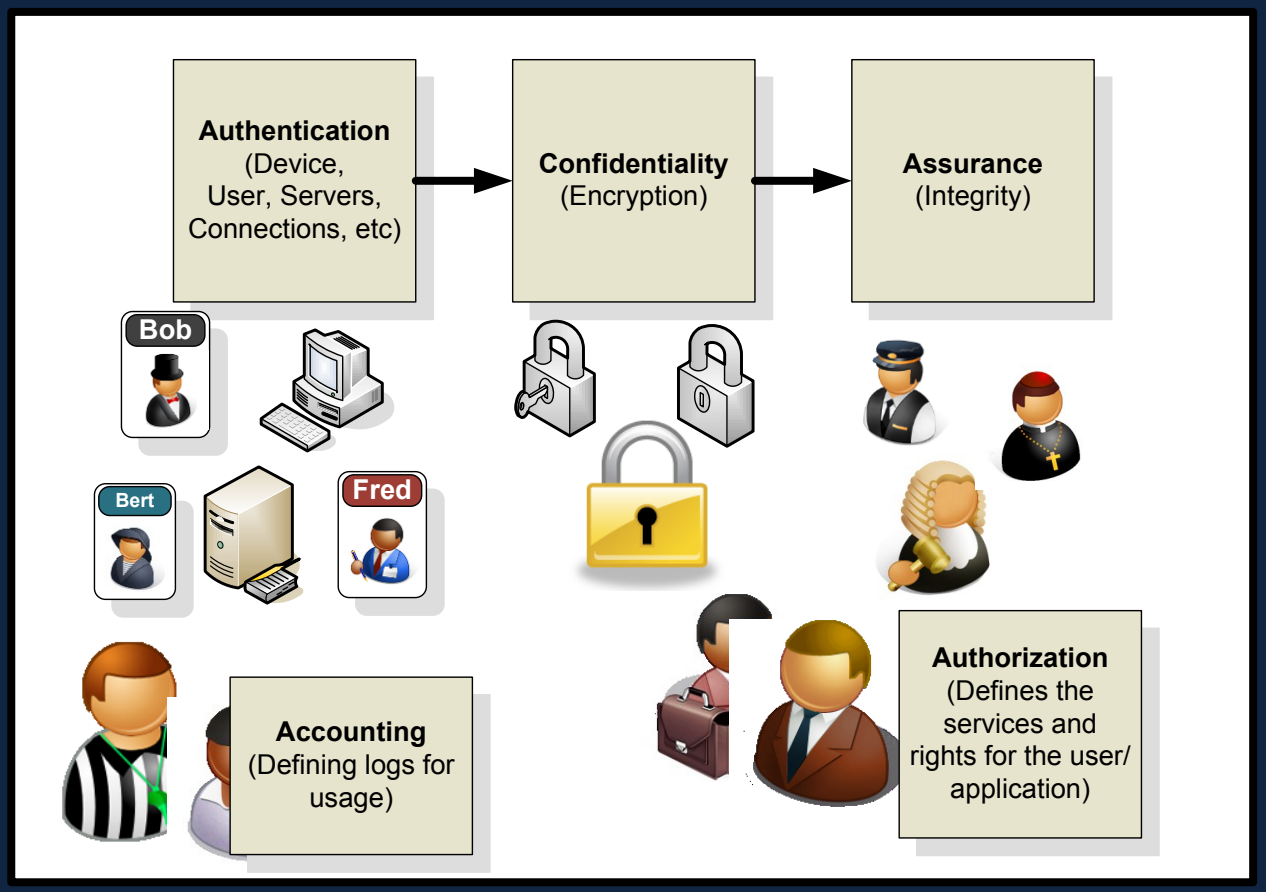
WPA-2

IEEE 802.11i

Author: Prof Bill Buchanan

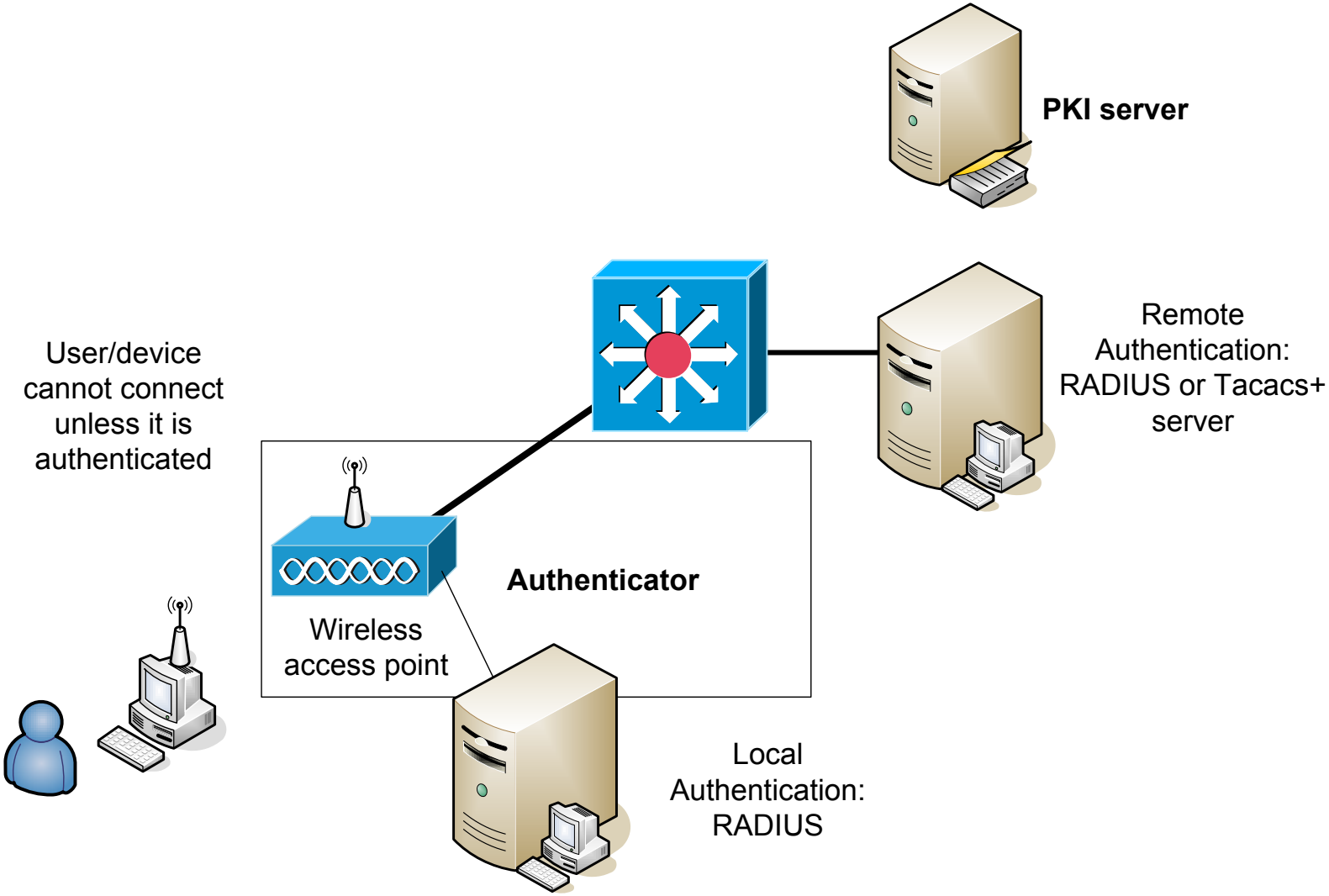

Username/ password
Digital Certificate (client-side)
Digital Certificate (server-side)
Sim card
IP
Layer 3
Encryption
LEAP
EAP-TSL
PEAP
EAP-SIM
Other methods
Method layer
802.1x
802.1x layer
Wireless
802.3 (Ethernet)
802.5 (Token Ring)
802.11 (Wireless)
PPP (Serial)
Others
Link layer
Author: Prof Bill Buchanan

Wireless Security



Authentication

Author: Prof Bill Buchanan



EAP

Wireless

Author: Prof Bill Buchanan

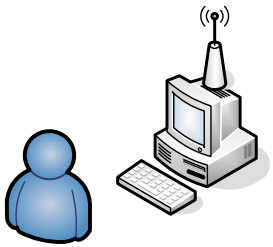
User Authentication:	User ID and digital certificate
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Client Certificate
Open Standard:	Yes
User differentiation:	Group
Certificate:	RADIUS server/WLAN client

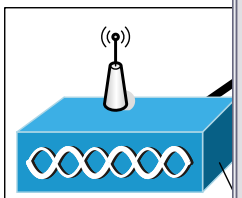
PKI server

Authentication

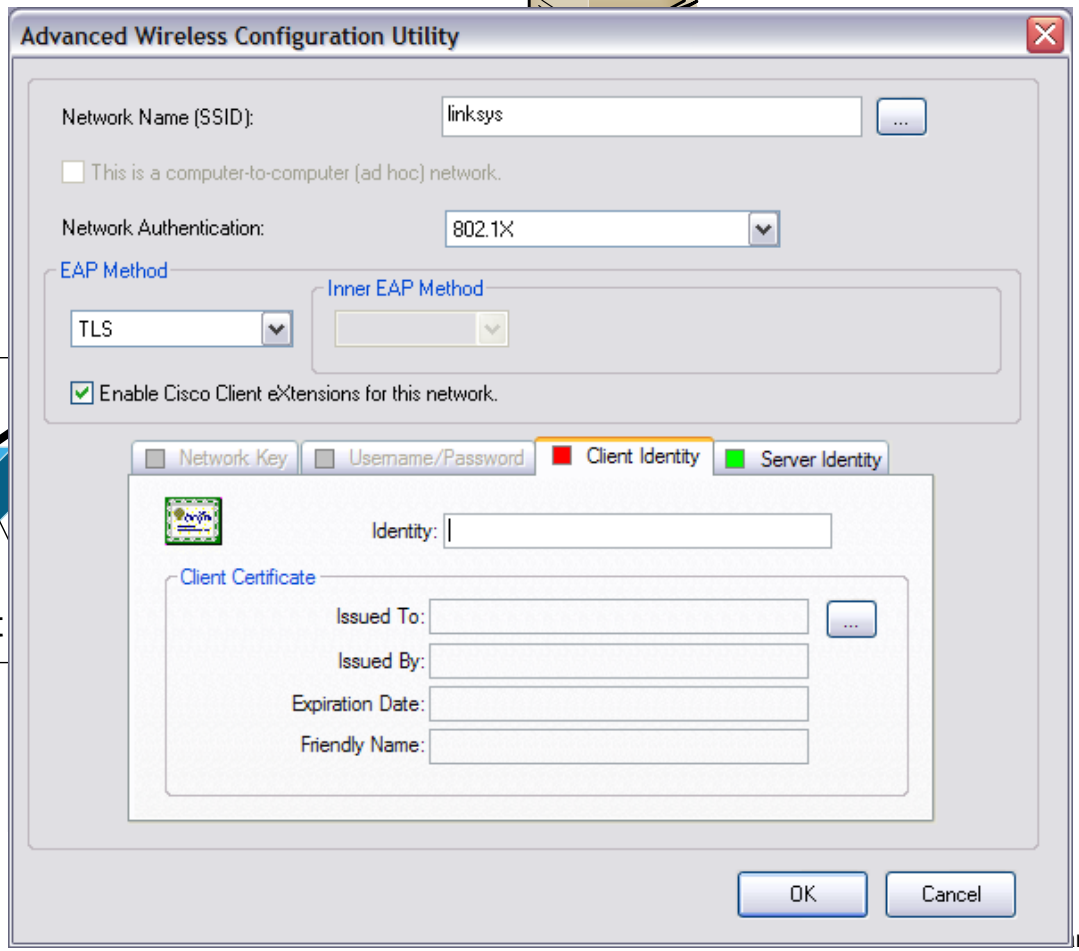
Wireless

User/device cannot connect unless it is authenticated





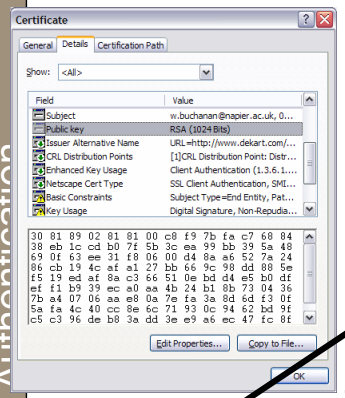
Wireless access point

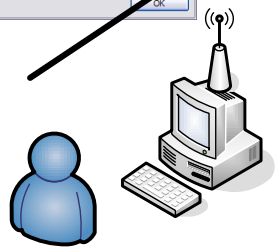


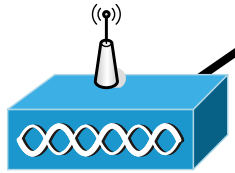
EAP-TLS

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

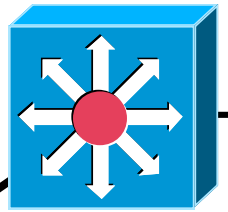


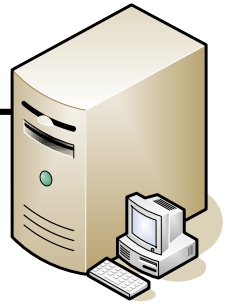




Wireless access point

Authenticator





Centralised RADIUS or Tacacs+ server

Authenticator server

PKI server

Usernames and passwords

Windows Domain server

Strengths: Good security.
Weaknesses: Spoof Access Point

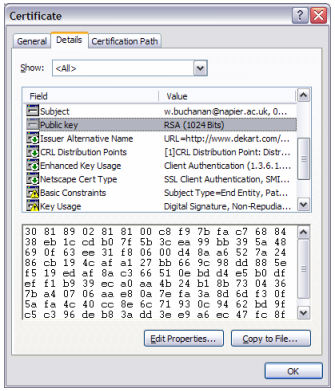
Author: Prof Bill Buchanan

Authentication

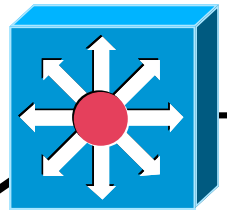
Wireless

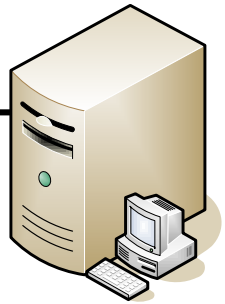
Strengths: Good security.
Weaknesses: Spoof Client

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



PKI server

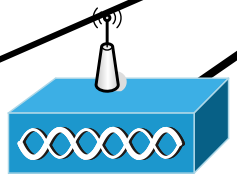




Centralised RADIUS or Tacacs+ server

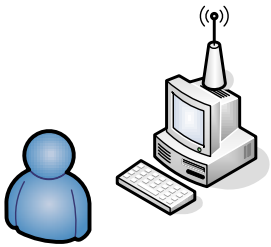
Authenticator server

Do you accept this Certificate (Y/N)?



Authenticator

Wireless access point



Usernames and passwords

Windows Domain server

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

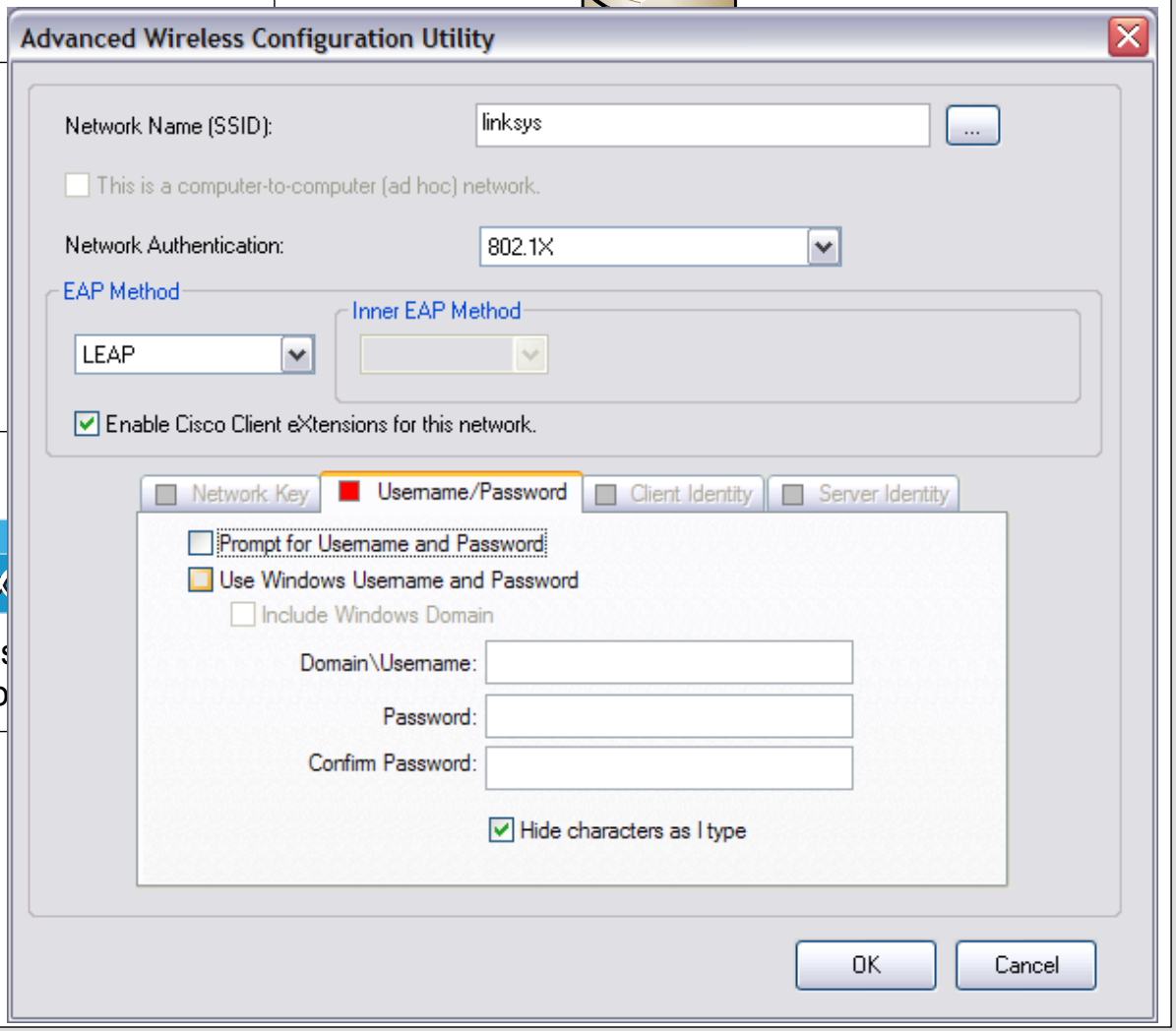
Authentication

Wireless

Author: Prof Bill Buchanan

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

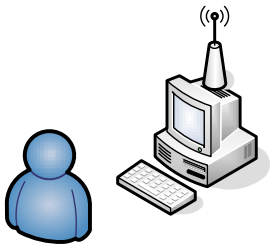
LEAPs is open to attack from a dictionary attack. **Use strong passwords!!!**

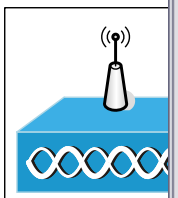


Authentication

Wireless

User/device cannot connect unless it is authenticated





Wireles
access p

LEAP

asleap home page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://asleap.sourceforge.net/

eap-ttls

Extensible Authentication Protocol -... | asleap home page

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)

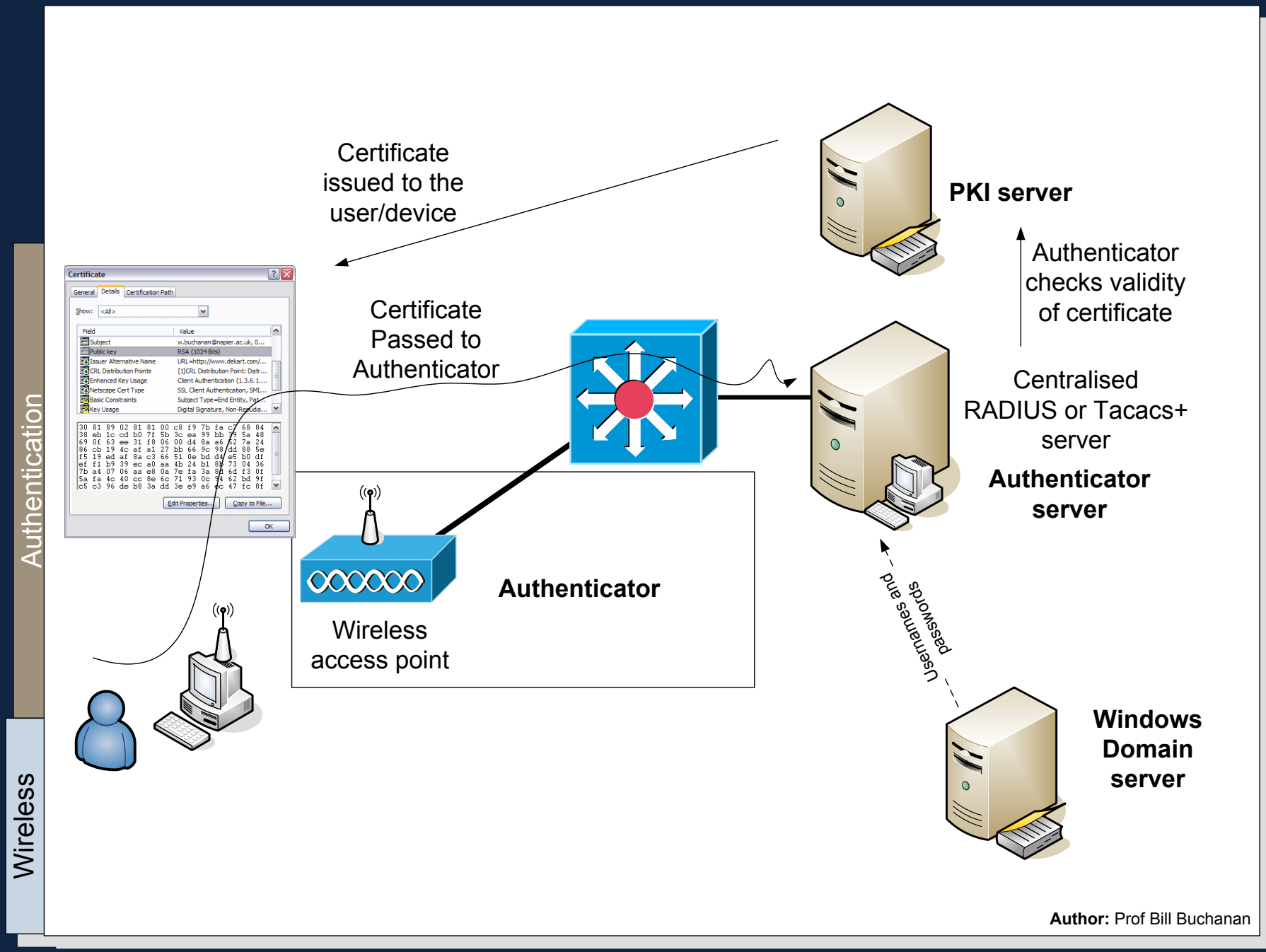
> I'm not one for HTML (as you have have already noticed), so I'm going to keep this simple. I wrote asleap while researching weaknesses in the Cisco proprietary LEAP protocol after I discovered that LEAP uses a modified MS-CHAPv2 exchange to authenticate users. MS-CHAPv2 is very bad.
>
> The first version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

Done

Authentication

Wireless

LEAP

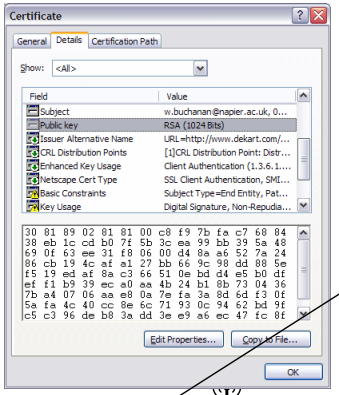


802.11x/EAP with Digital Certificates

Authentication

Wireless

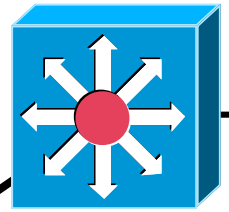
Outer Authentication

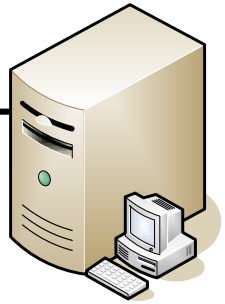


Certificate from network

PKI server

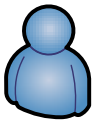
Authenticator checks validity of certificate

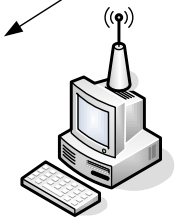


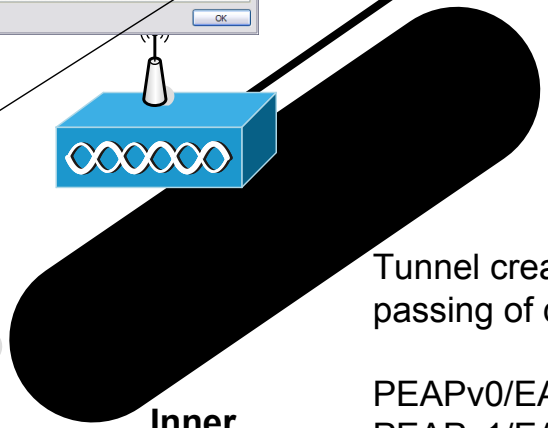


Centralised RADIUS or Tacacs+ server

Authenticator server







Usernames and passwords

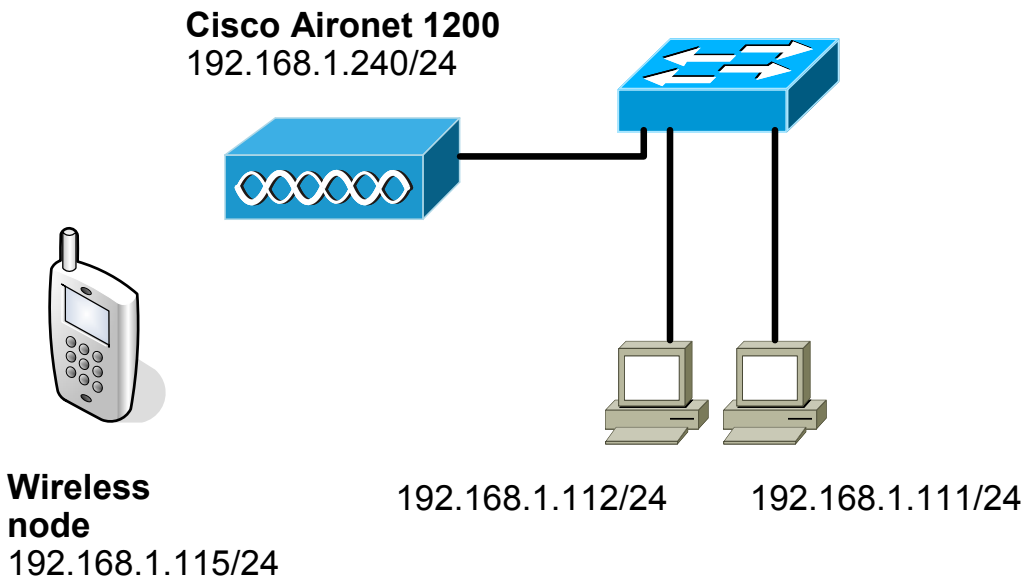
Windows Domain server

Tunnel created for secure passing of details

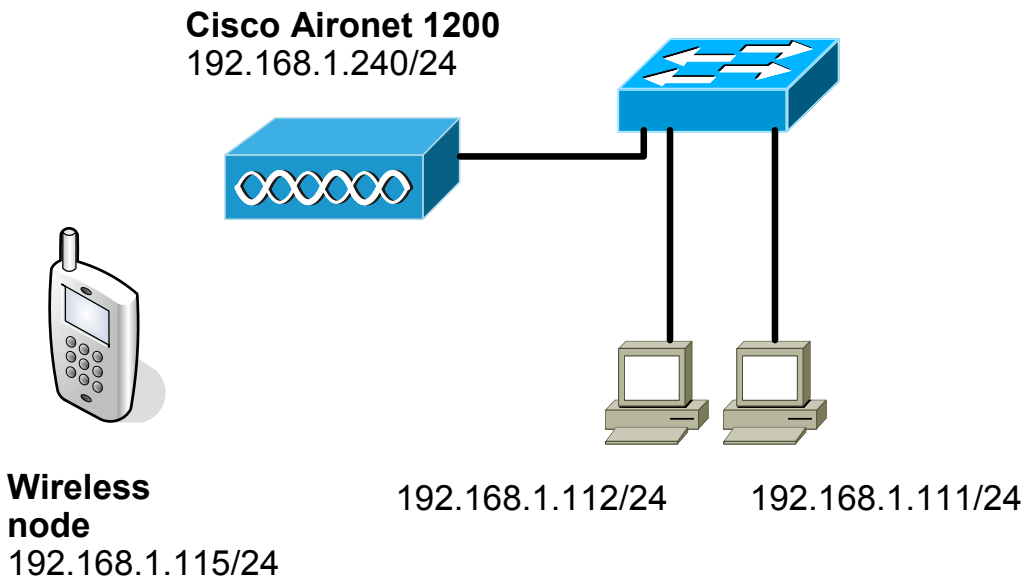
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
(Generic Token Card). No support in Windows.

Inner Authentication

Author: Prof Bill Buchanan



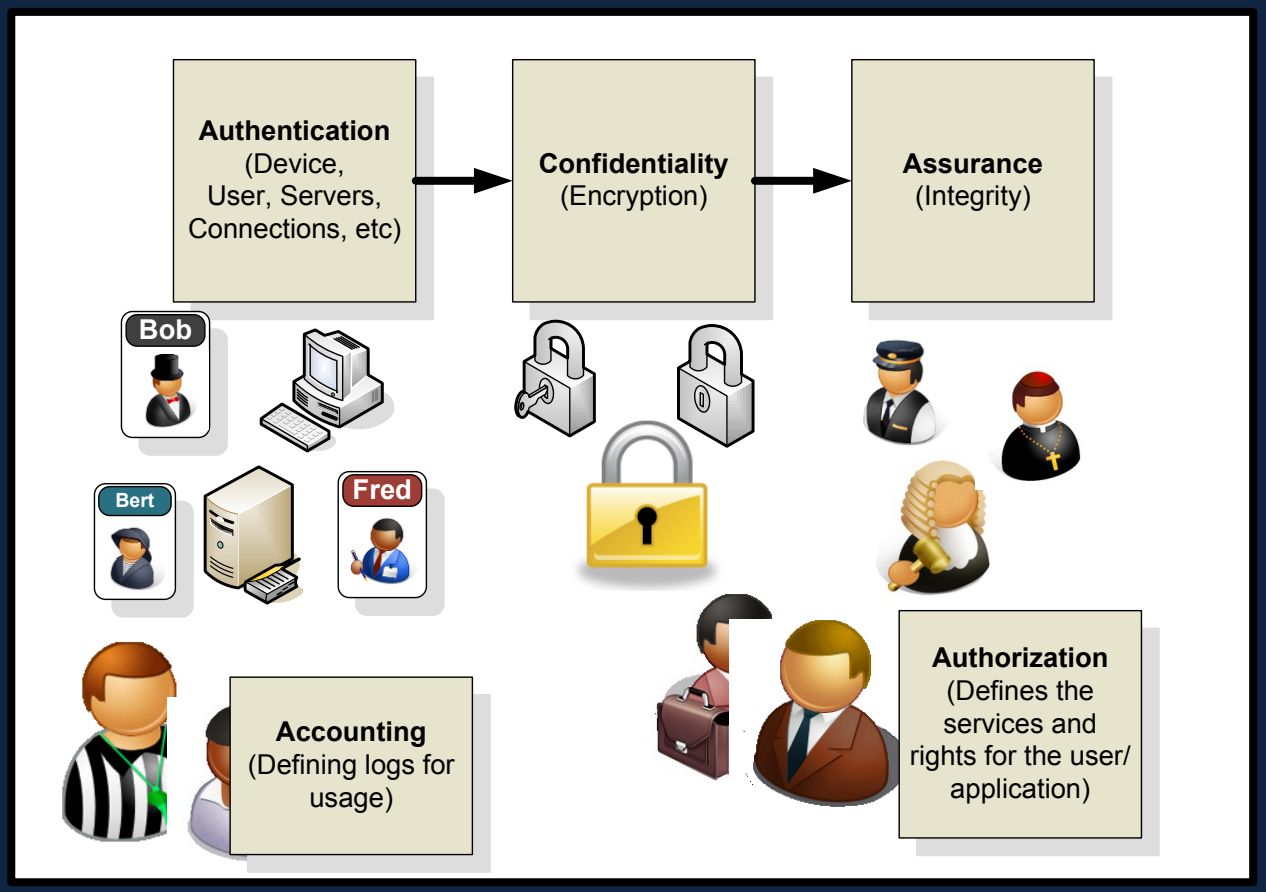

```
(config) # dot11 ssid NapierSSID
(config-ssid) # authentication network-eap eap_methods
(config-ssid) # exit
(config) # interface Dot11Radio0
(config-if) # encryption key 1 size 40bit AAAAAAAAAA transmit-key
(config-if) # encryption mode ciphers wep40
(config-if) # ssid NapierSSID
(config-if) # channel 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
```




```
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)
```

Author: Prof Bill Buchanan

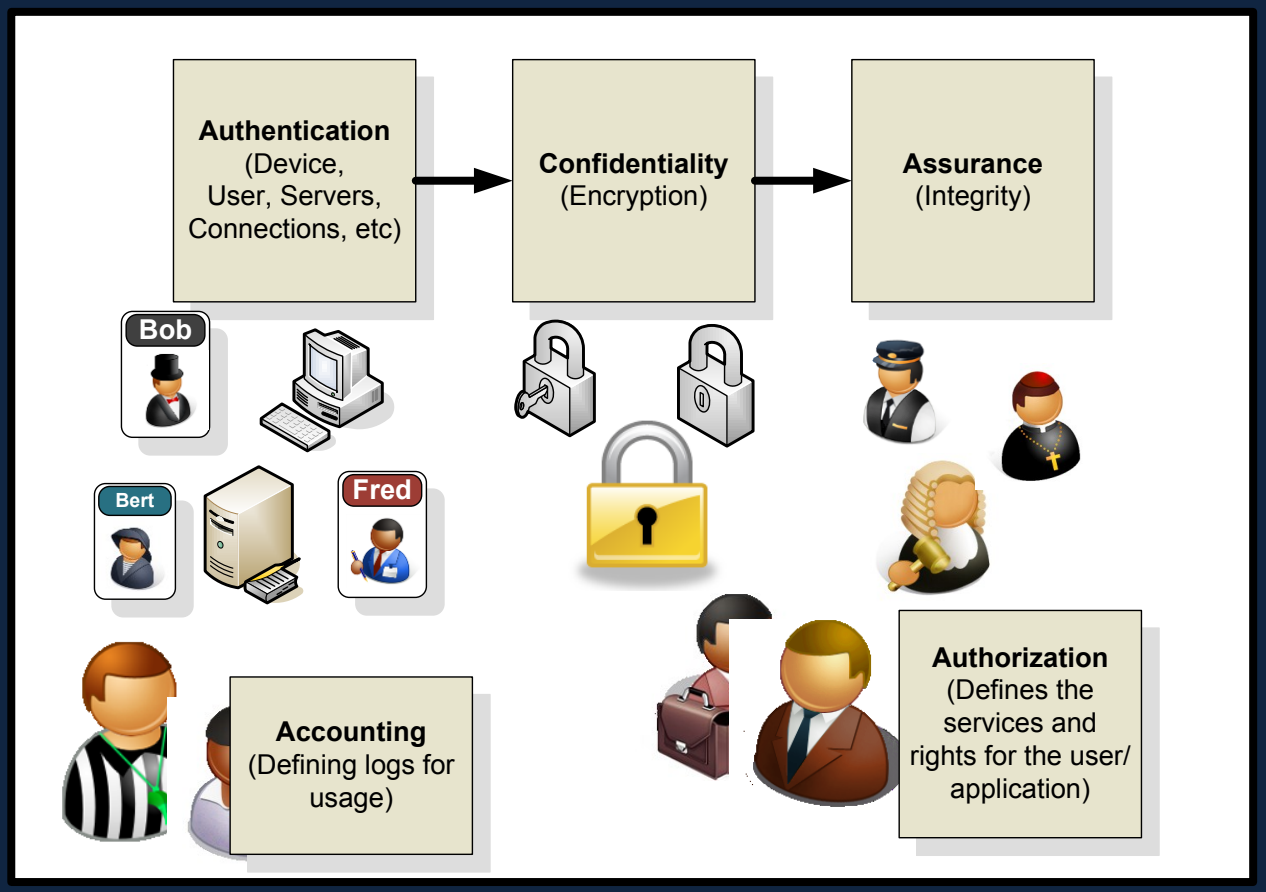
Wireless Security



Conclusions

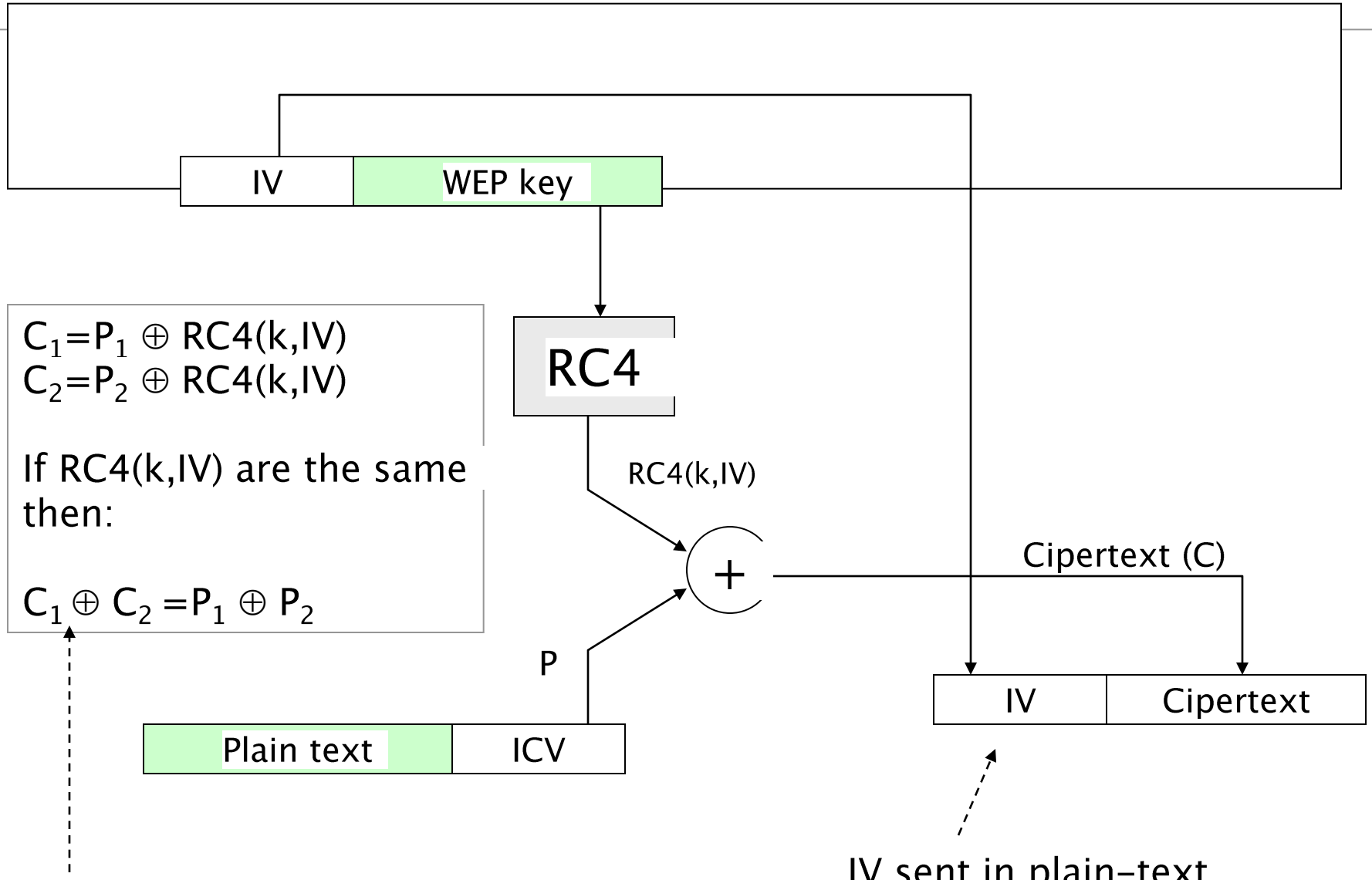
Author: Prof Bill Buchanan

Wireless Security



TKIP

Author: Prof Bill Buchanan



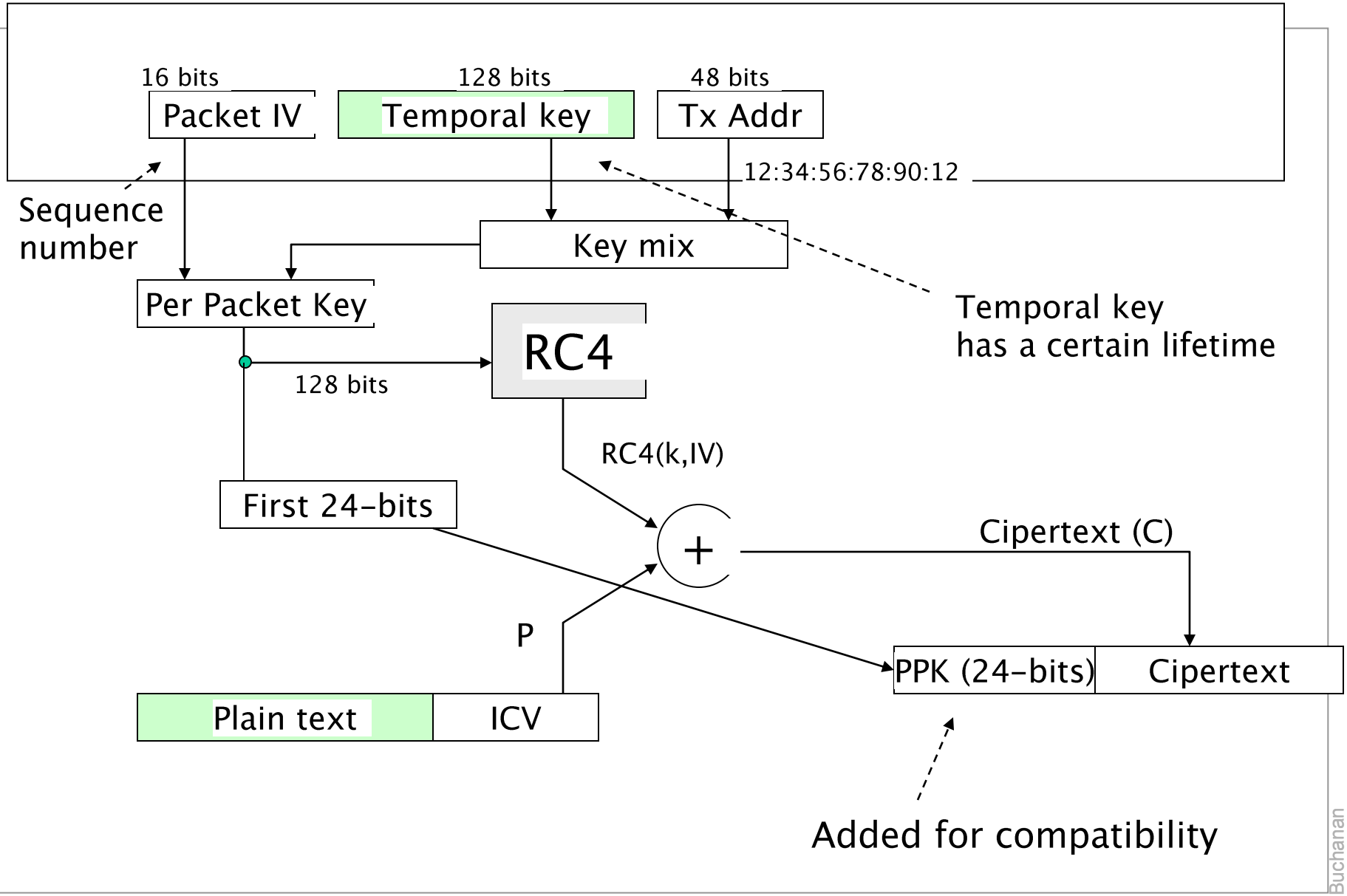
$C_1 = P_1 \oplus RC4(k,IV)$
$C_2 = P_2 \oplus RC4(k,IV)$

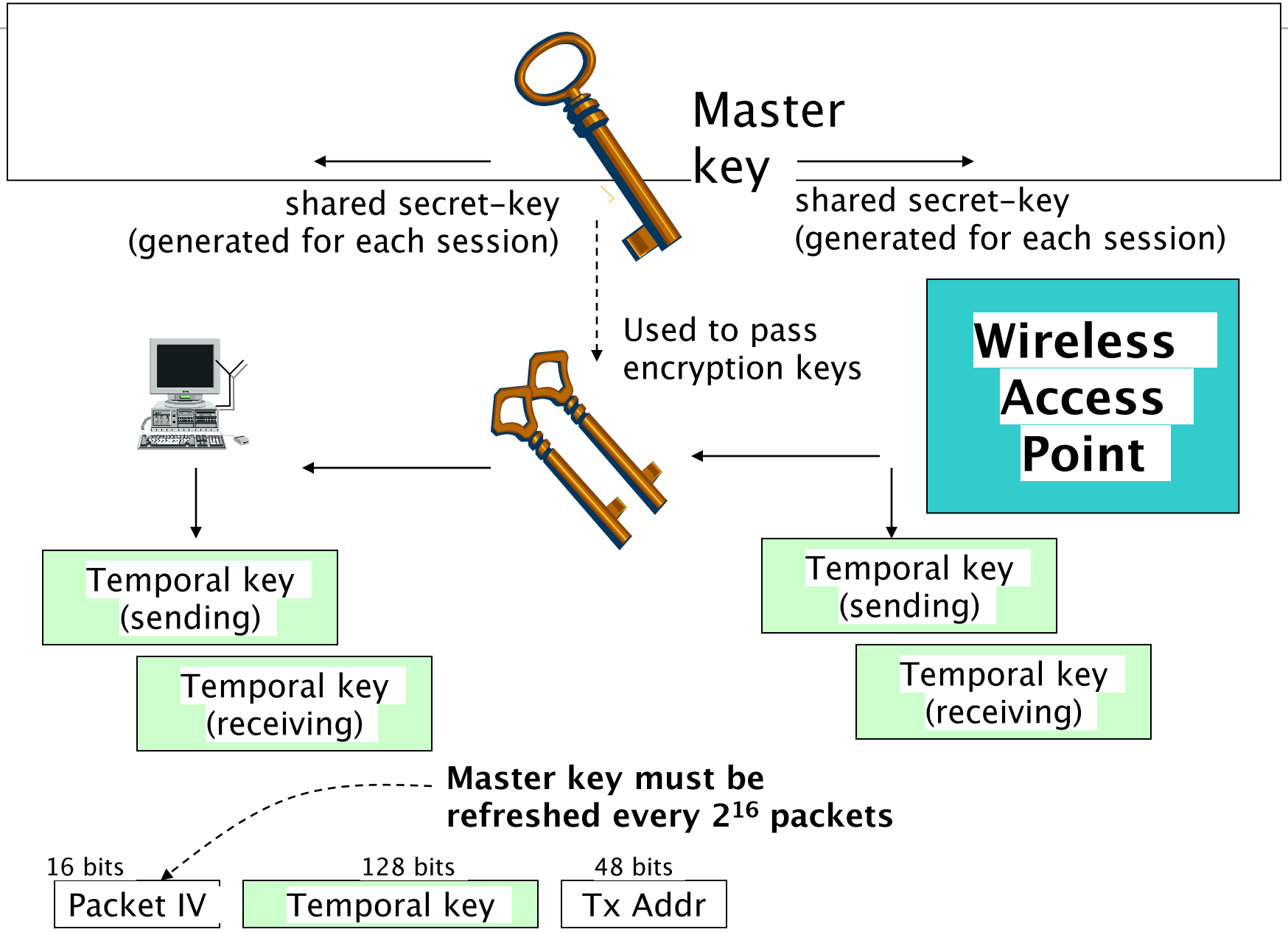
If RC4(k,IV) are the same then:

$C_1 \oplus C_2 = P_1 \oplus P_2$

IV sent in plain-text

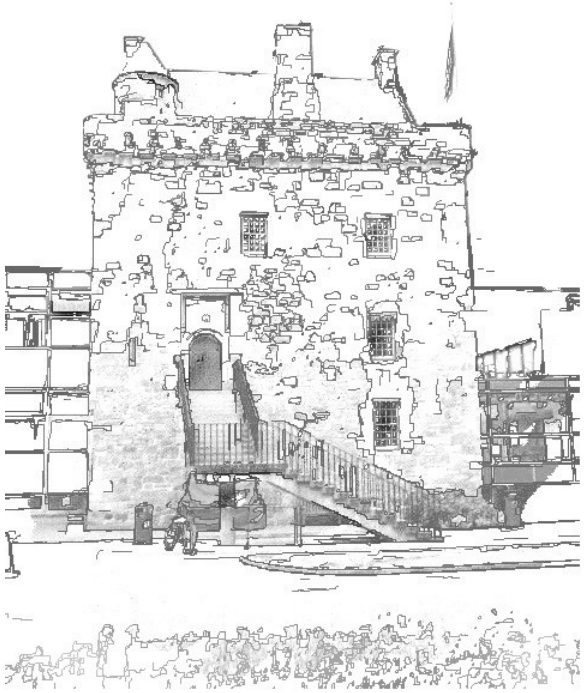
Statistical attack/dictionary attack


16 bits
Packet IV
128 bits
Temporal key
48 bits
Tx Addr
12:34:56:78:90:12
Sequence number
Key mix
Per Packet Key
RC4
128 bits
Temporal key has a certain lifetime
RC4(k,IV)
First 24-bits
+
Cipertext (C)
P
PPK (24-bits)
Cipertext
Plain text
ICV
Added for compatibility



```
(config-if)# encryption mode ?
  ciphers  Optional data ciphers
  wep      Classic 802.11 privacy algorithm
(config-if)# encryption mode ciphers ?
  aes-ccm    WPA AES CCMP
  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)# encryption mode ciphers tkip ?
  aes-ccm  WPA AES CCMP
  wep128   128 bit key
  wep40    40 bit key
  <cr>
(config-if)# encryption key 1 size
        128 12345678901234567890123456 transmit-key
```

WPA-PSK

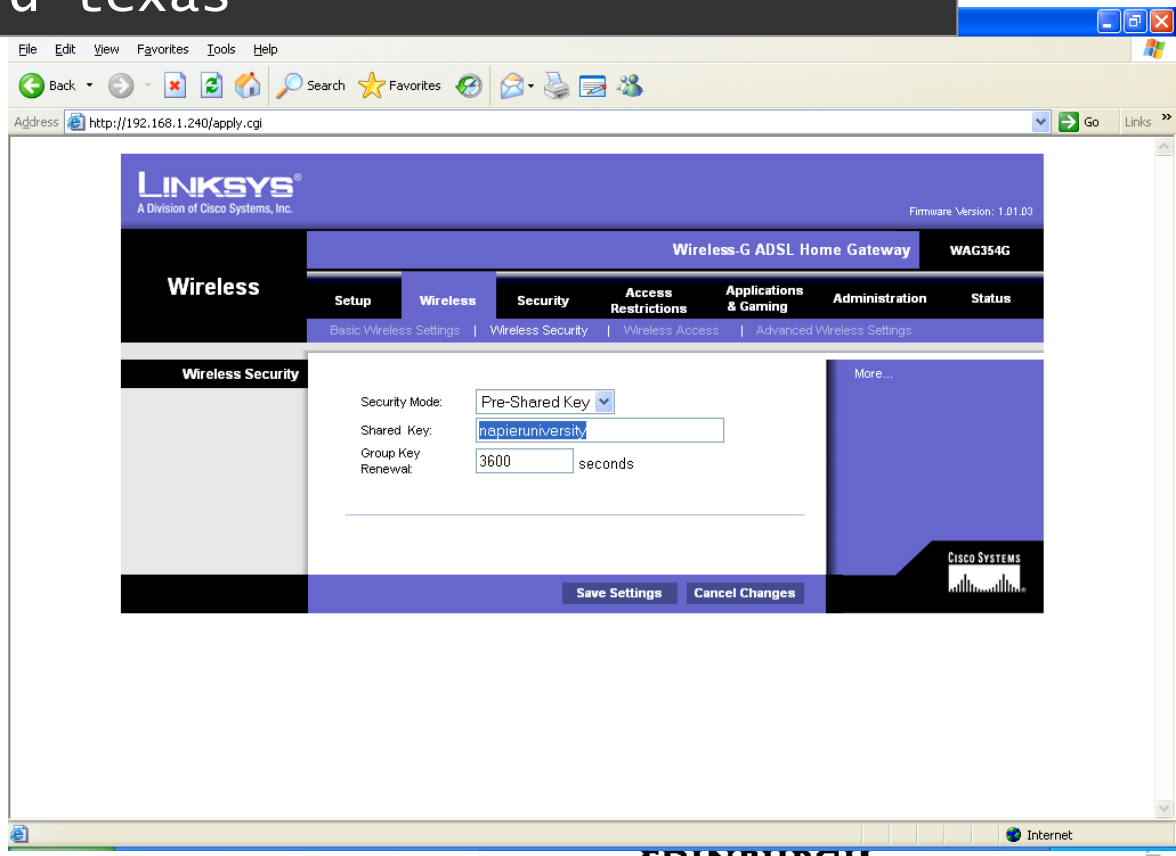


INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```



```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```

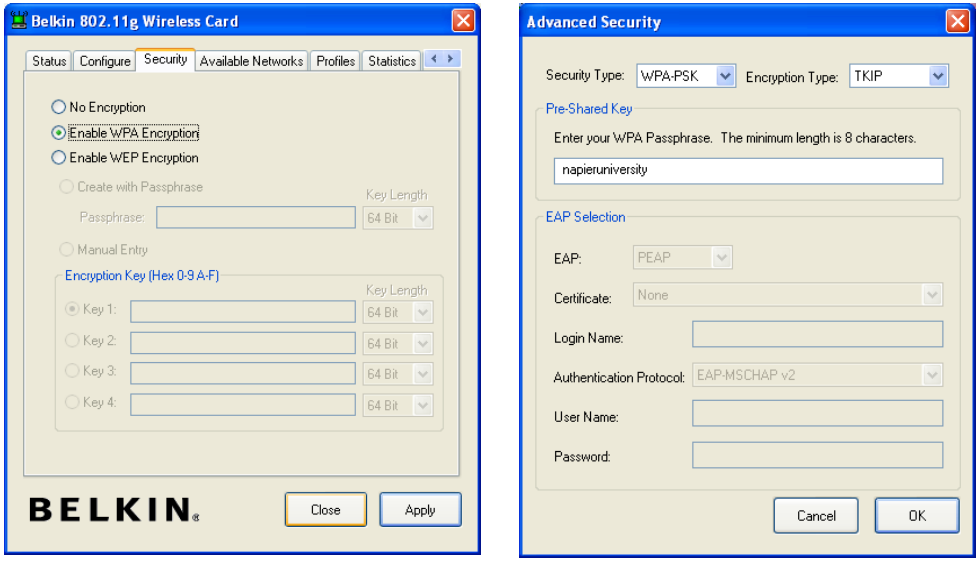
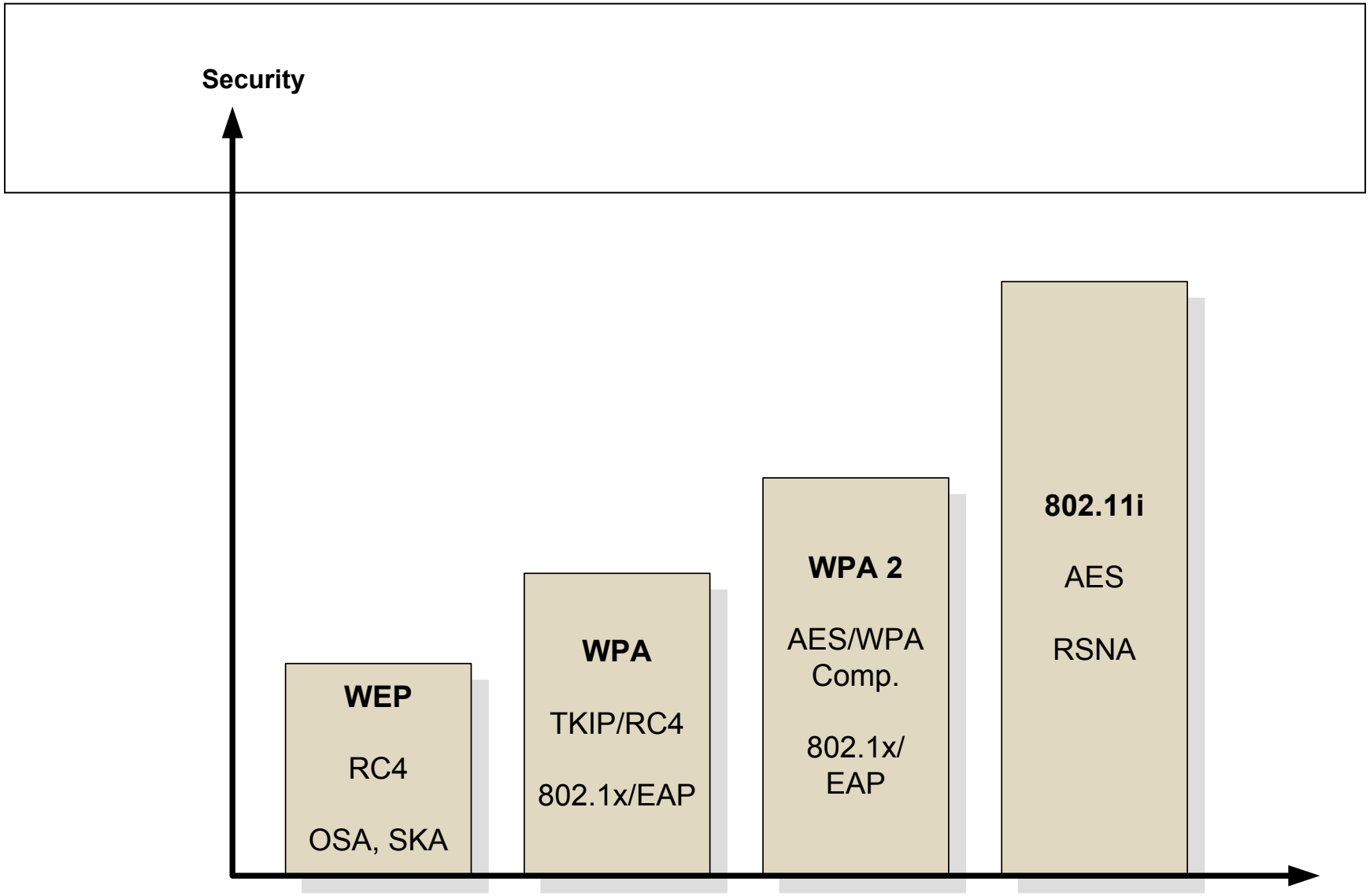


Figure 2: WPA-PSK (client)

```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```

Figure 2:

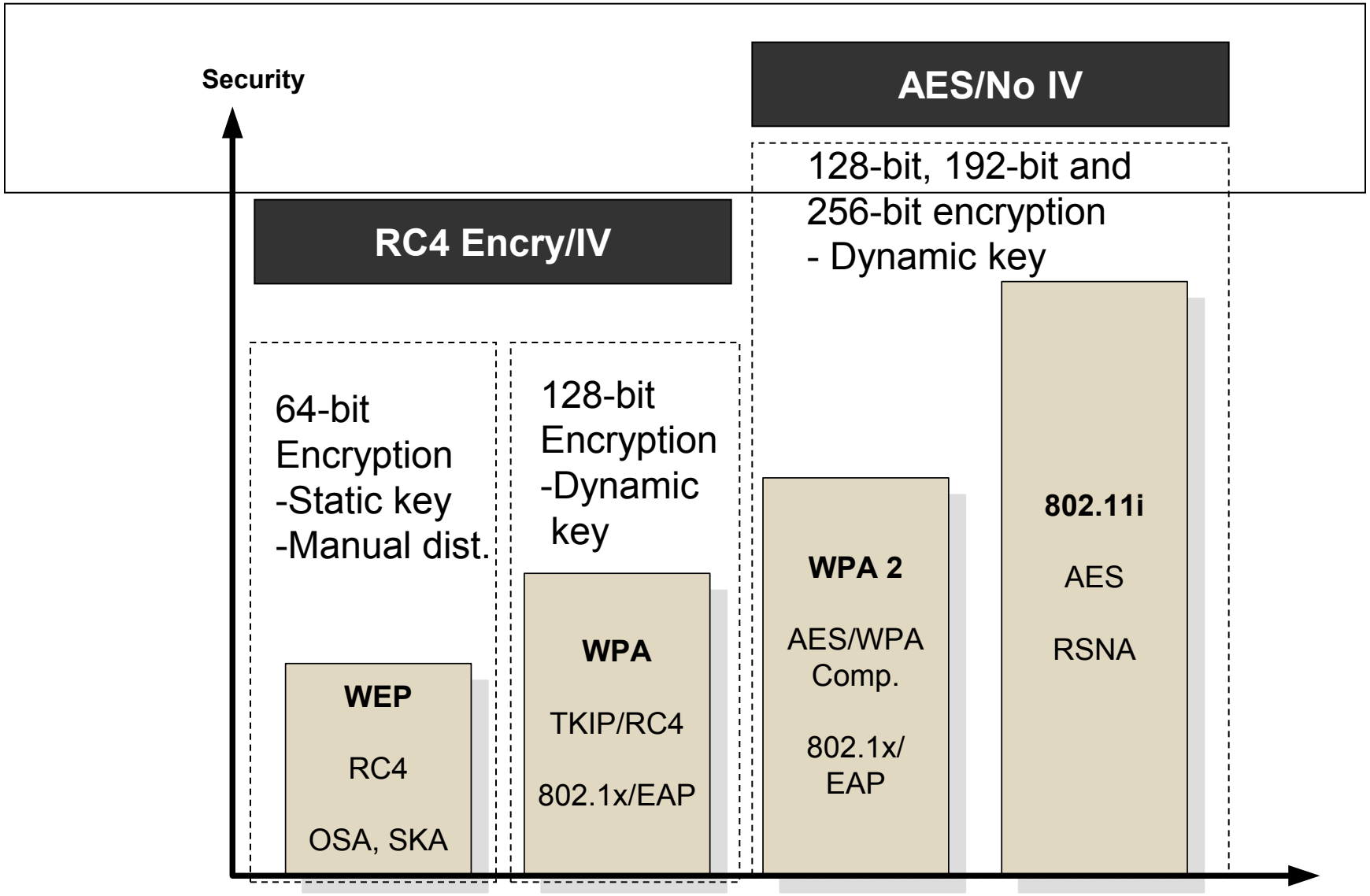
INVESTOR IN PEOPLE



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

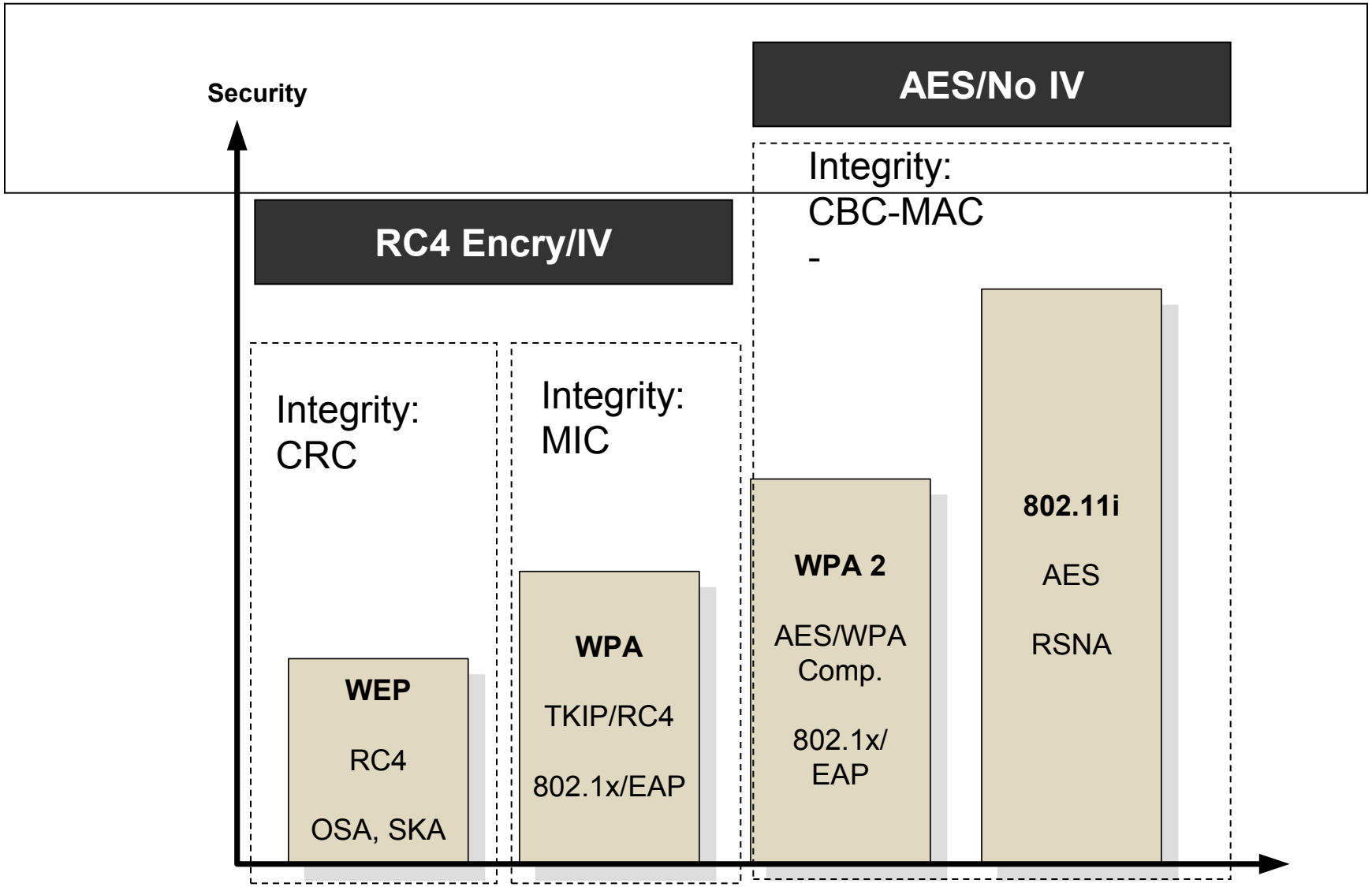
RSNA – Robust Security Network Association
AES – Advanced Encryption Standard



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard

INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

Areas covered:

Authentication methods

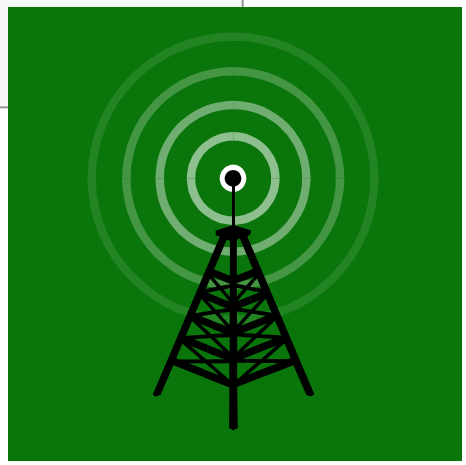
Ways?

LEAP, PEAP, EAP, and so on

Methods and weaknesses.

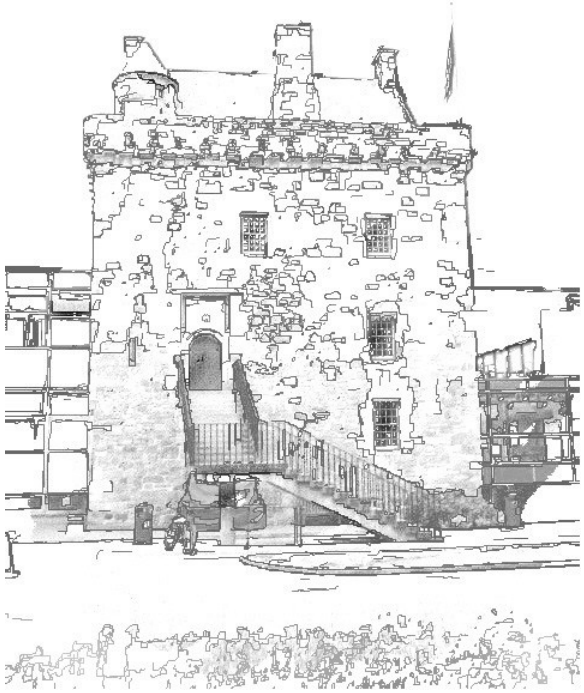
Configurating authentication on an Aironet

A simple example with local Radius

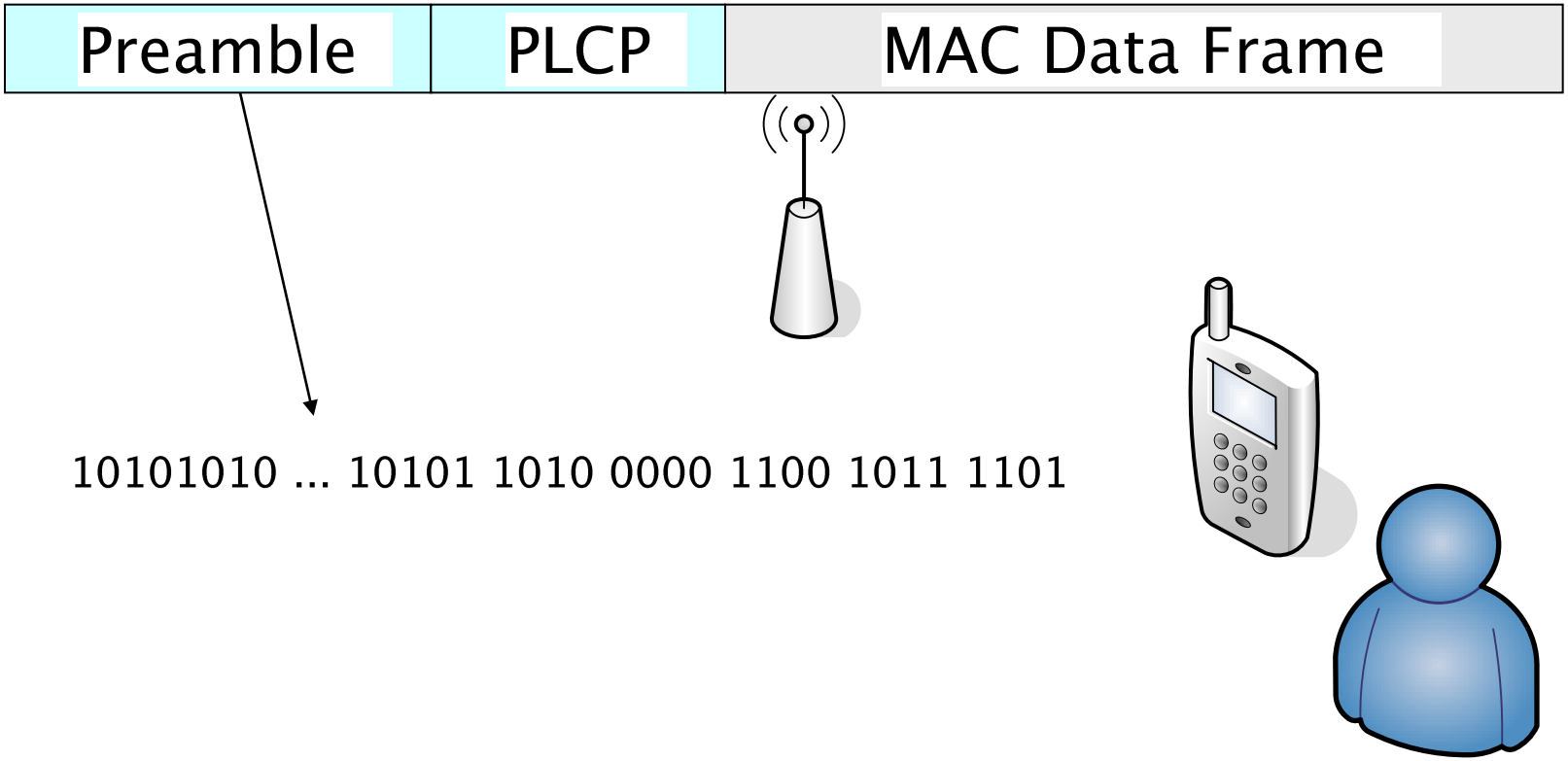


Author: Bill Buchanan

IEEE 802.11 Frame Format



Author: Bill Buchanan



Author: Bill Buchanan

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

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)

XX X X XX XX

Order
0 Not ordered

WEP
0 – No WEP
1 - WEP

MoreData
0 No more data

PowerManagement

Retry

MoreFrag

FromDS

ToDS

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)

MoreFrag

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

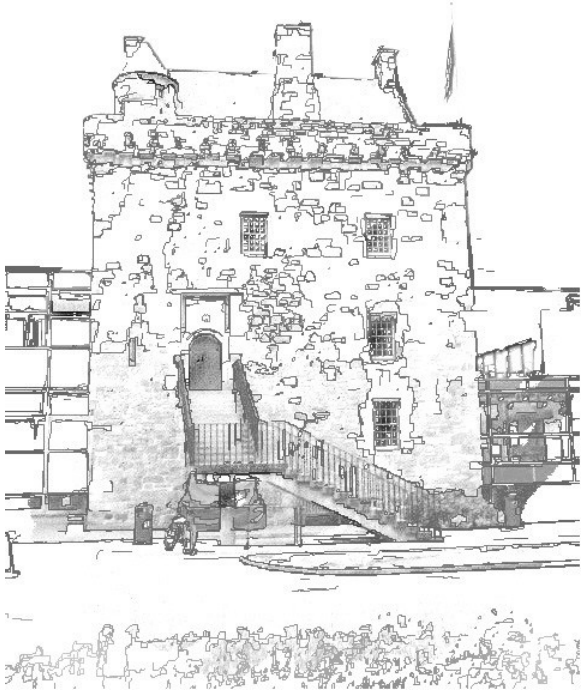
Received: 350 Passed Filter: 350 Memory: 0.7%

- 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

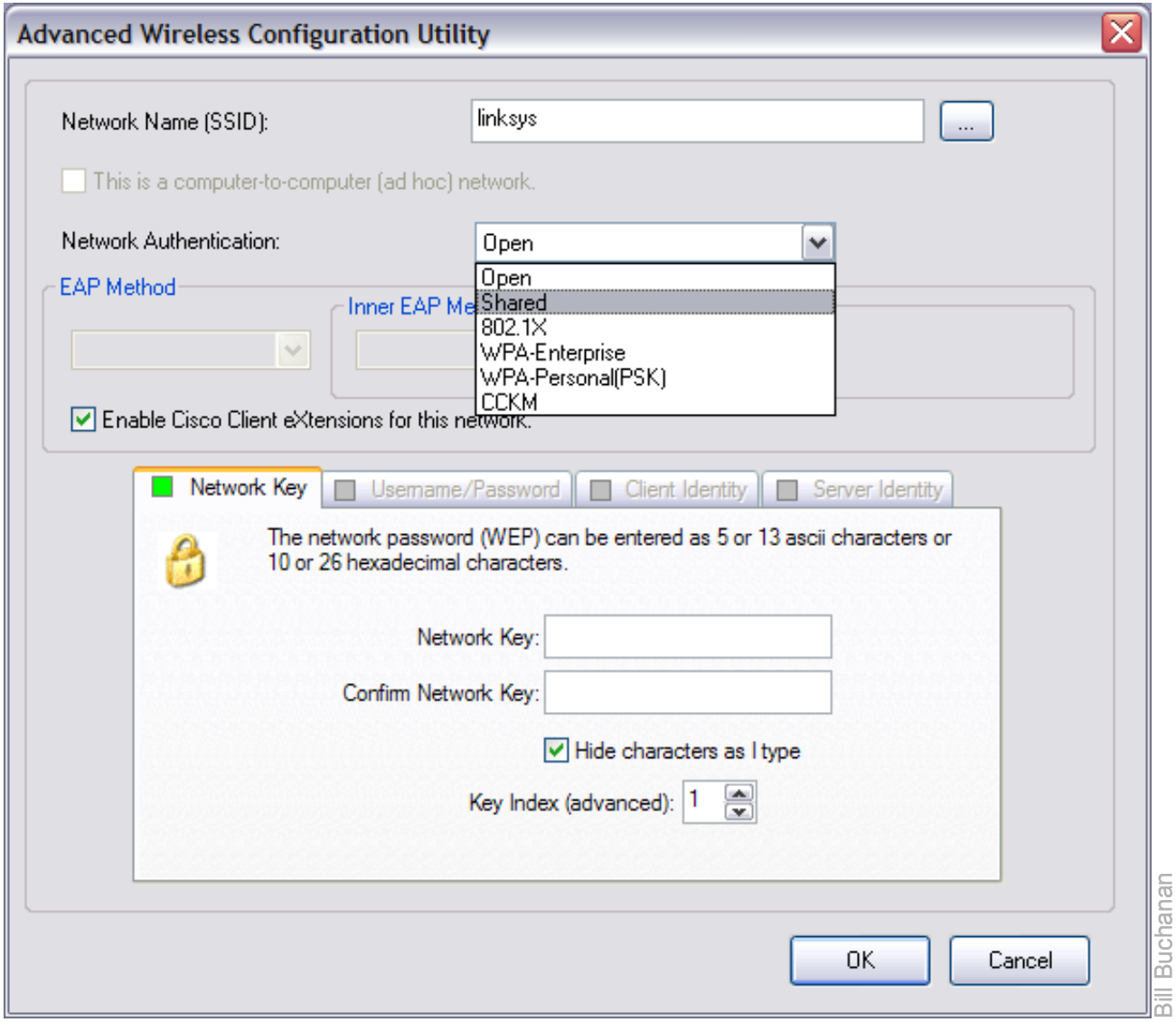
```
0000:  00 C0 A8 B7 5B 5A 00 0C 41 F5 23 D5 24 52 08 02   ....[Z..A.#.$R..
0010:  2C 00 00 C0 A8 B7 5B 5A 00 0C 41 38 9B A4 00 0C   ,.....[Z..A8....
0020:  41 F5 23 D5 10 F5 AA AA 03 00 00 00 08 00 45 00   A.#...........E.
0030:  04 53 40 9D 40 00 35 06 58 9B 50 EF 95 6F C0 A8   .S@.@.5.X.P..o..
0040:  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 E4 B1 03 9D C7 DF 96 BD 02 E8 DA E6 41 FD   ..............A.
```

Wireless Authentication

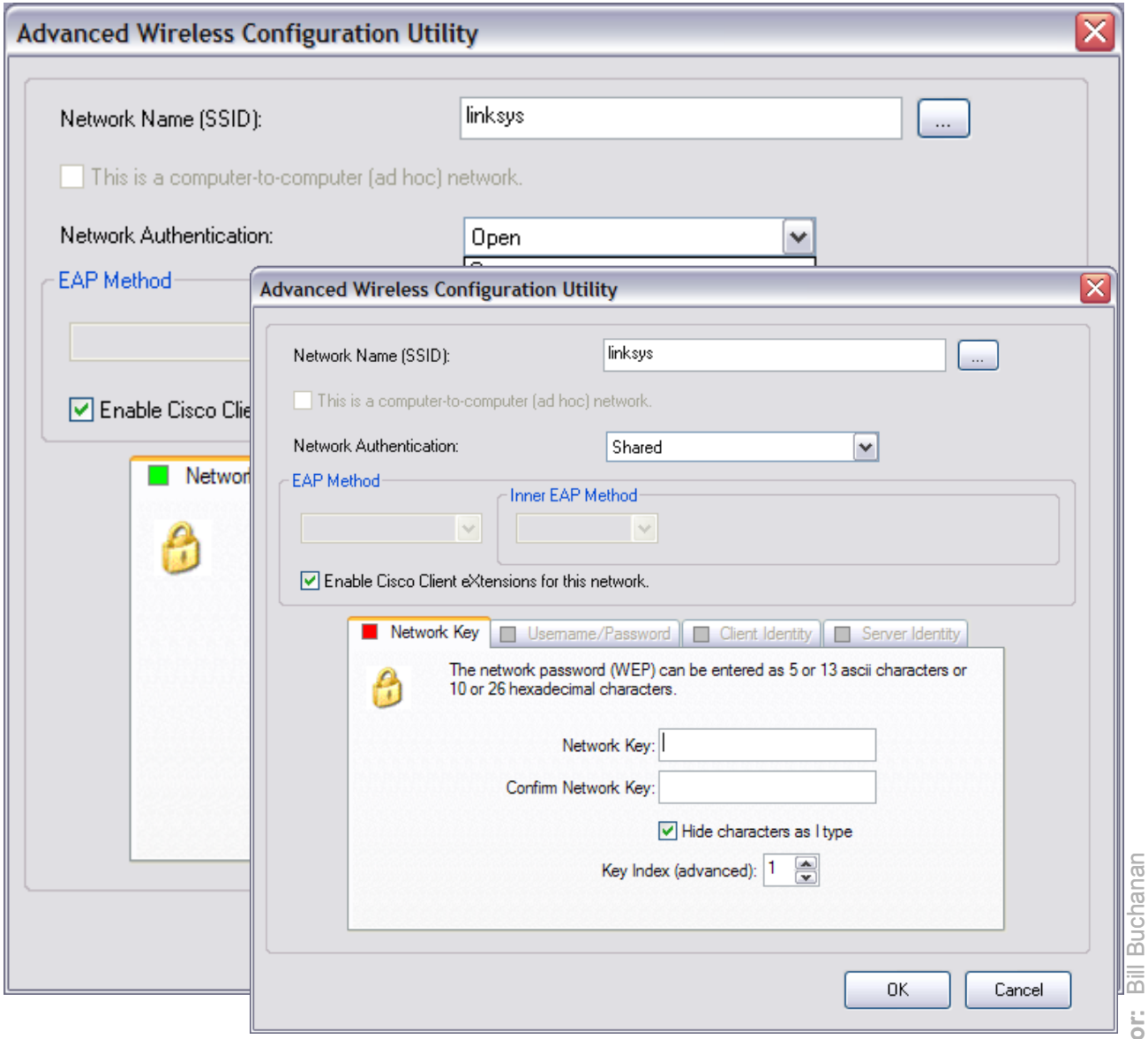


Author: Bill Buchanan

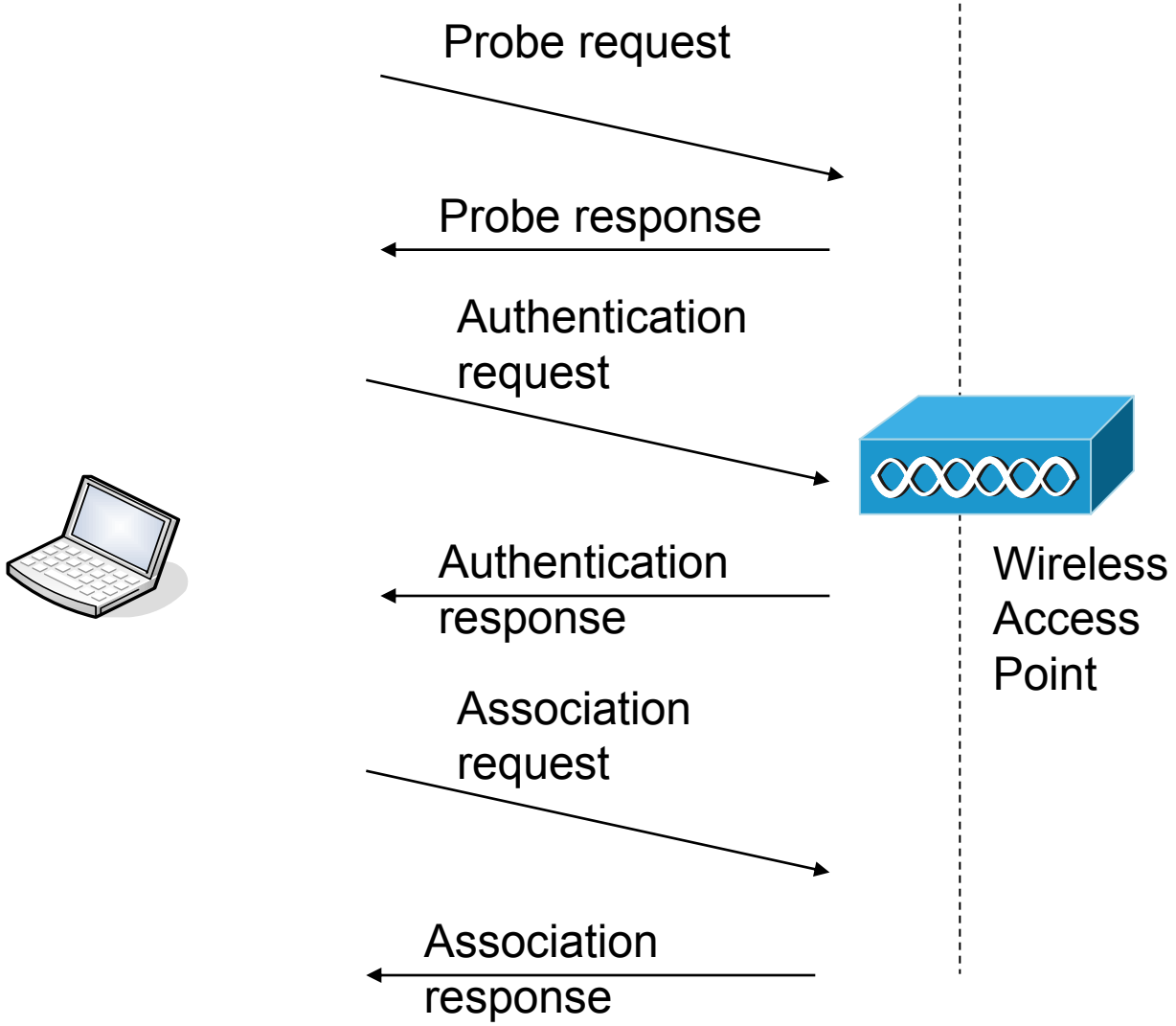
WEP
also allows for authentication using a secret key (shared key) or an open system.



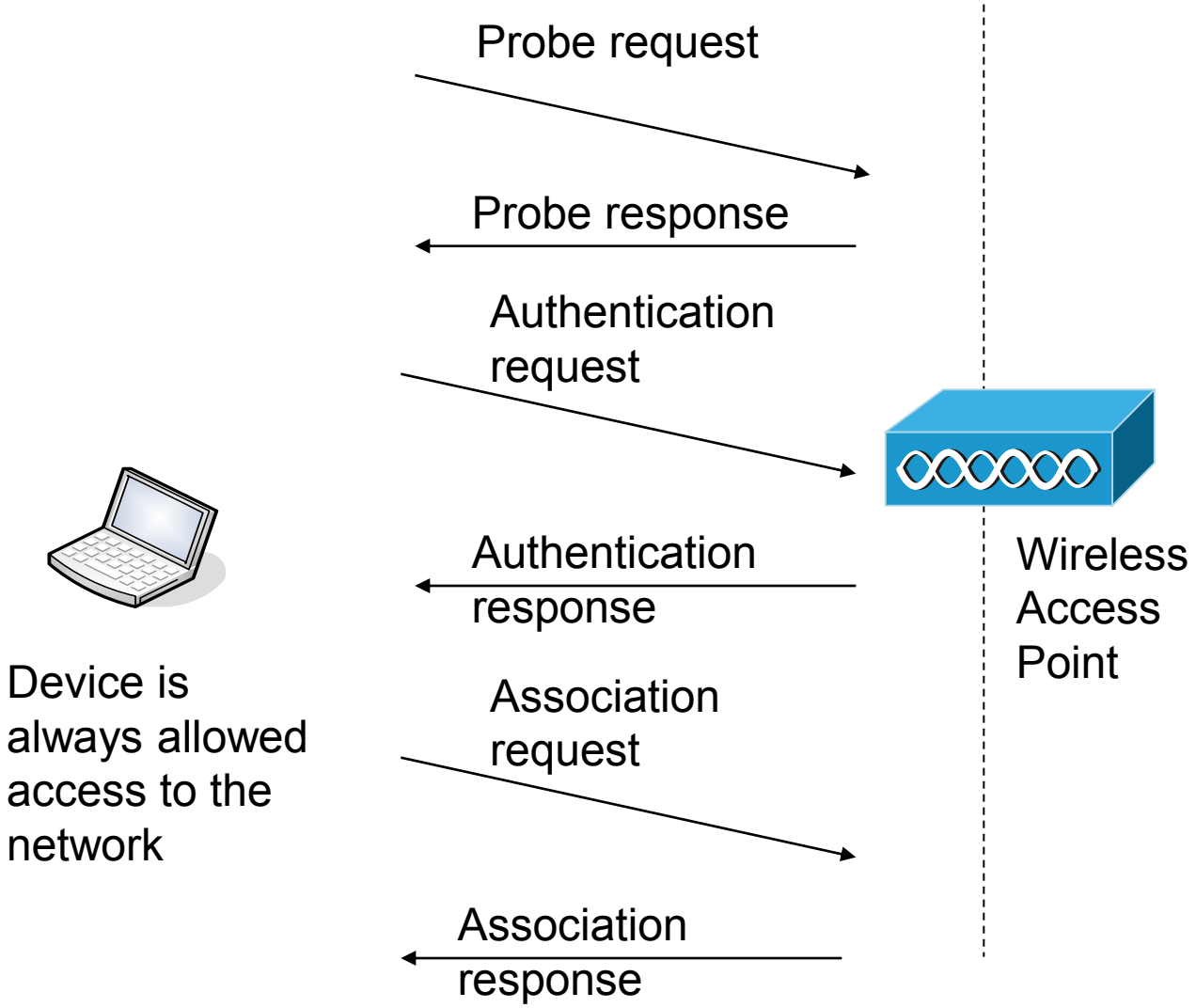
WEP
also allows for authentication using a secret key (shared key) or an open system.



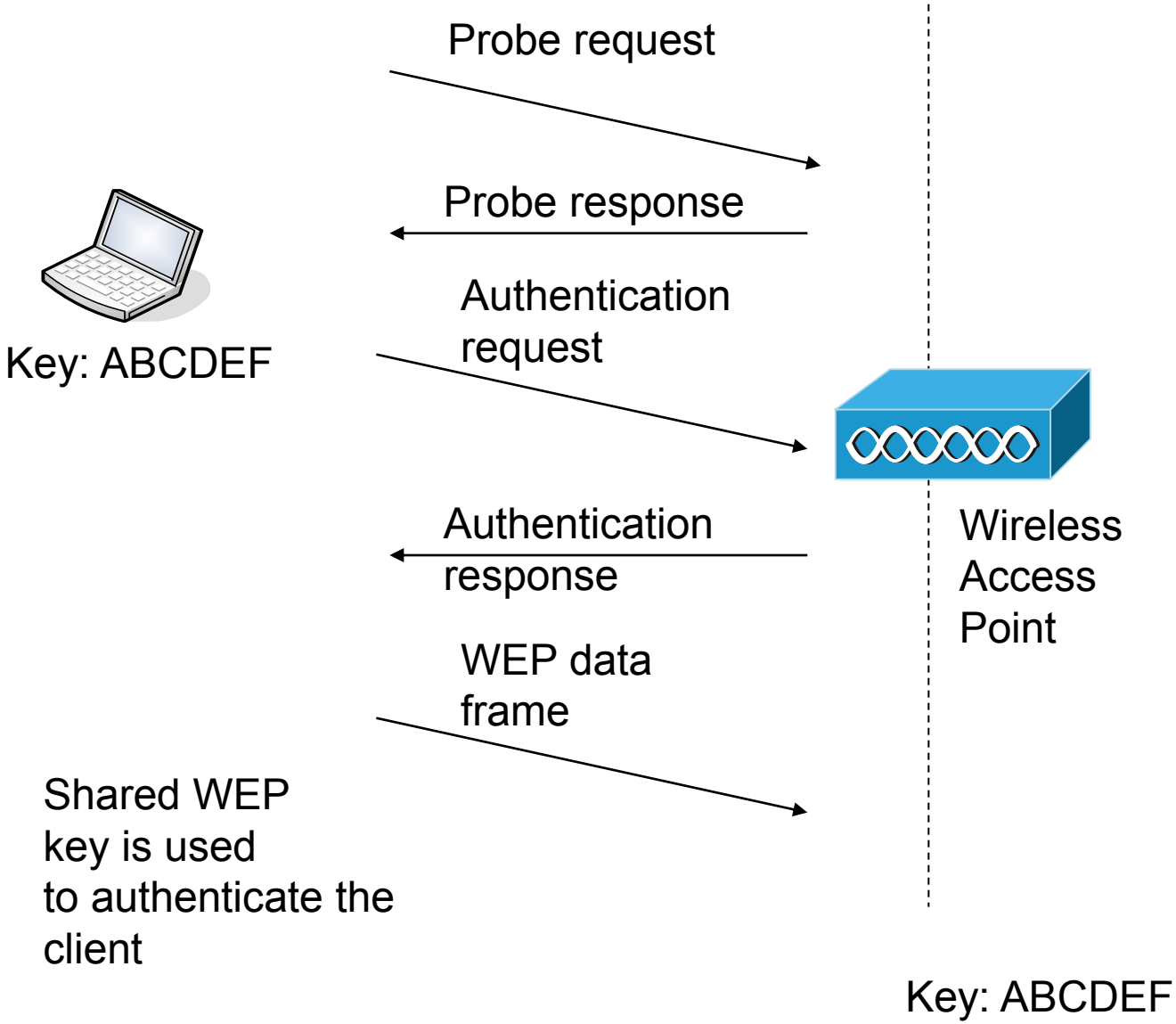
Author: Bill Buchanan

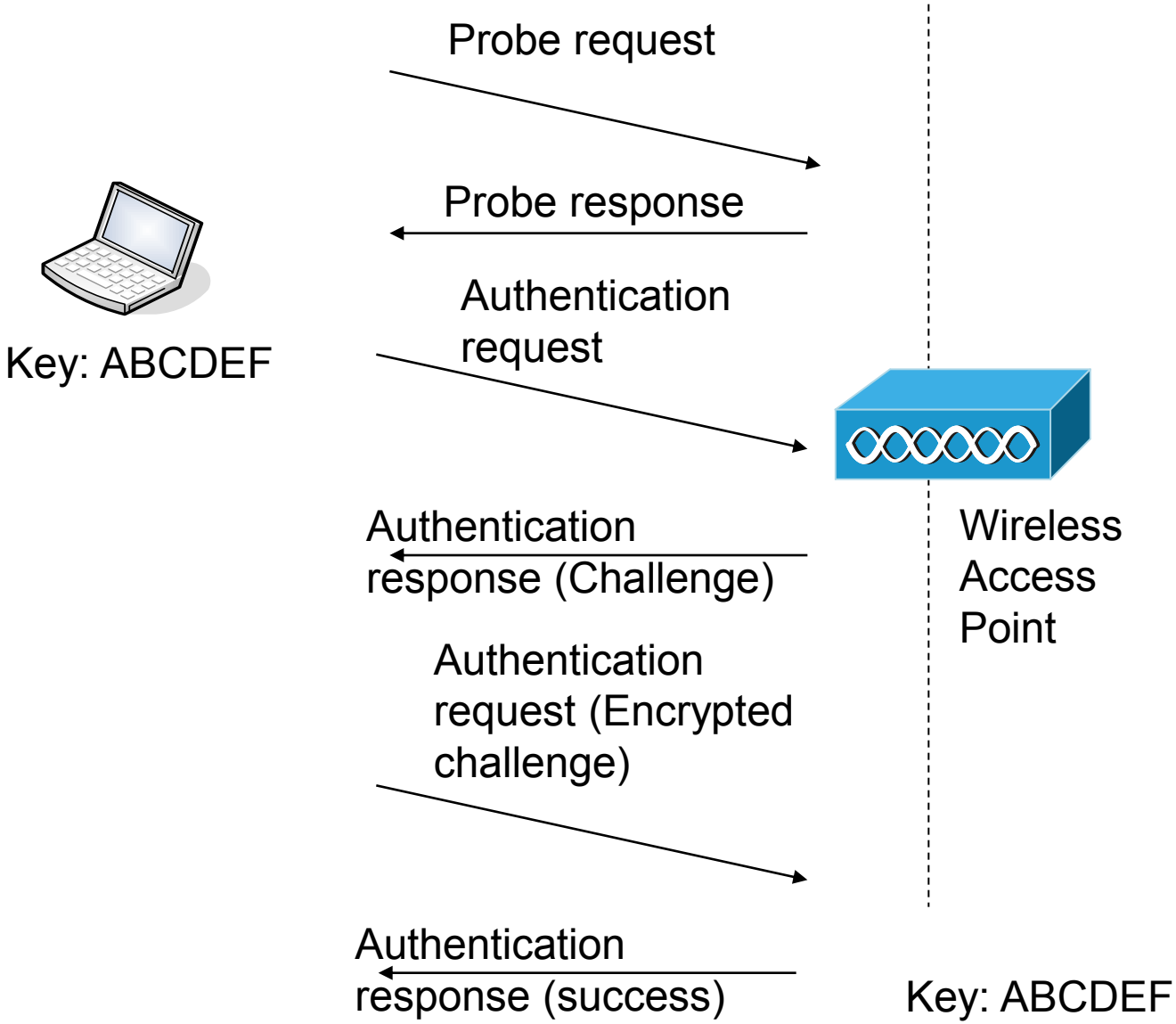


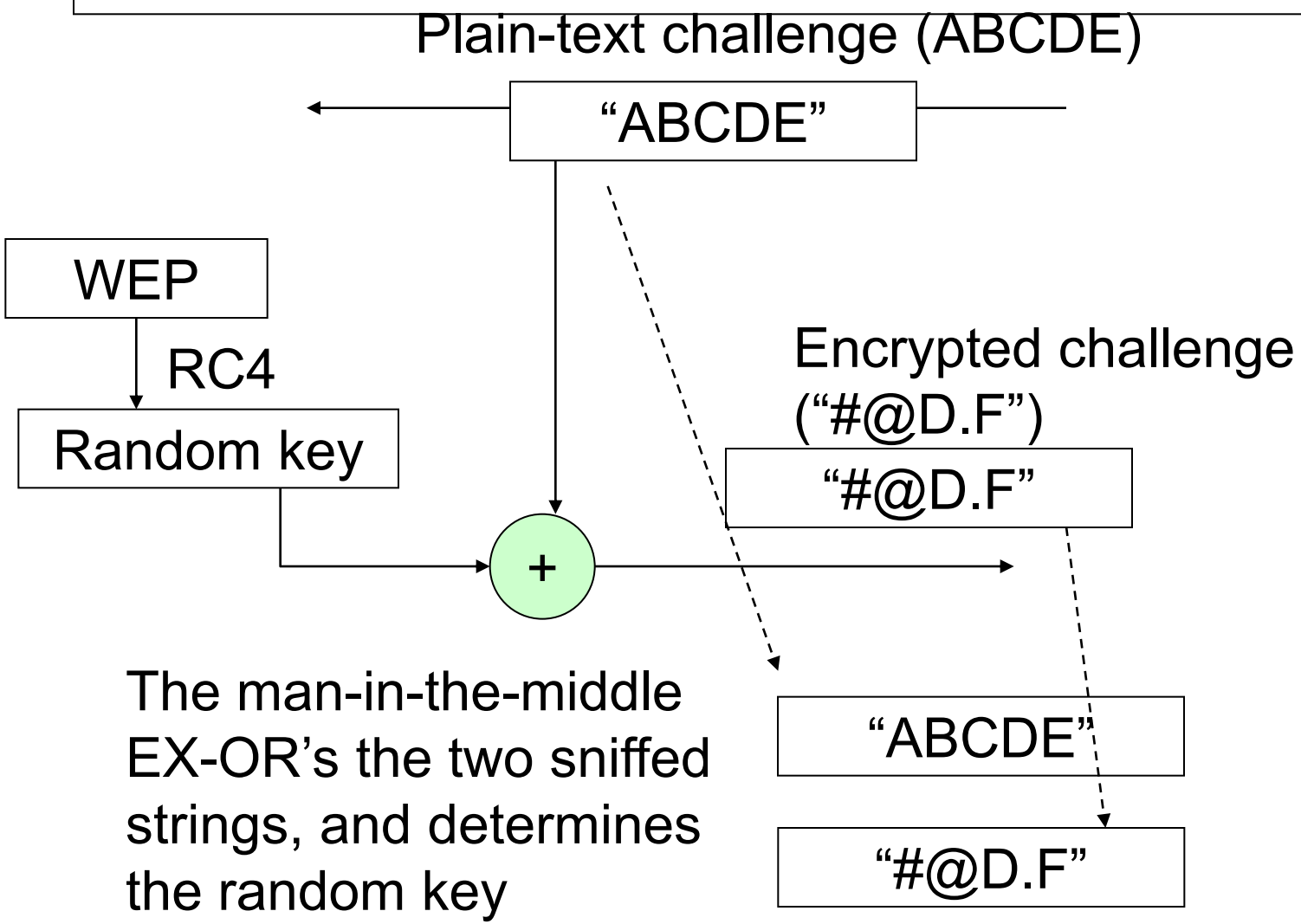
Author: Bill Buchanan



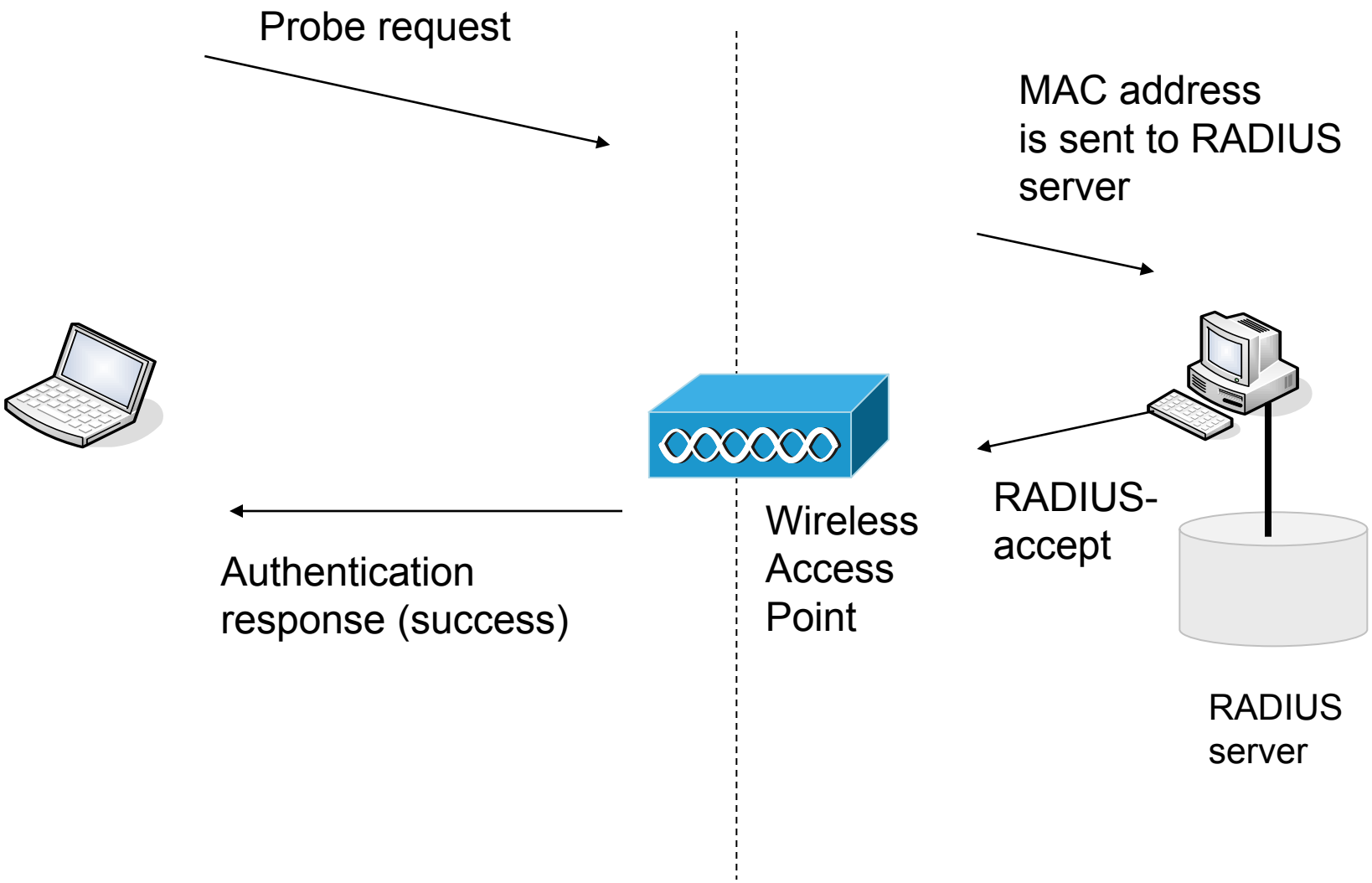
Author: Bill Buchanan

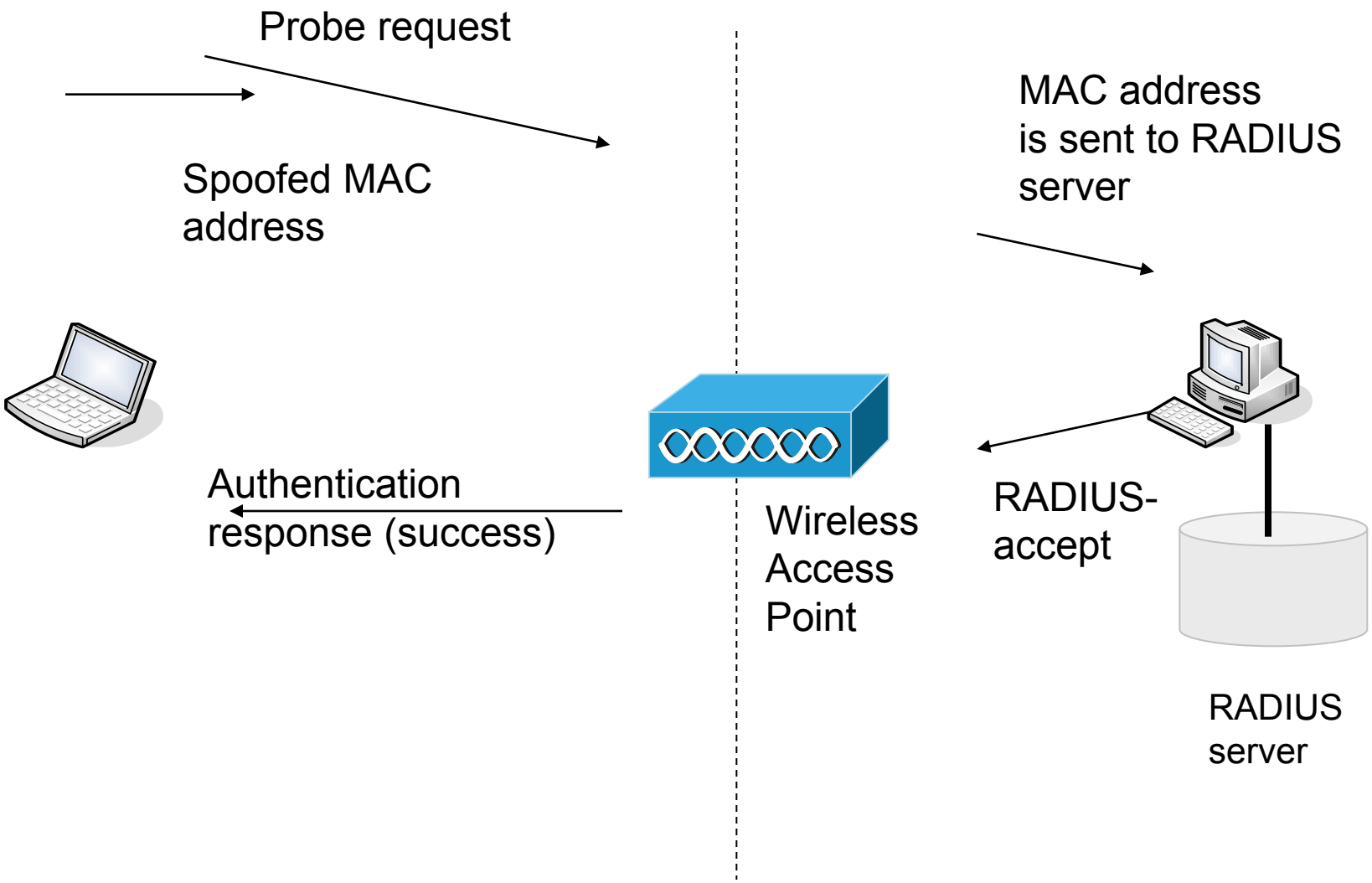


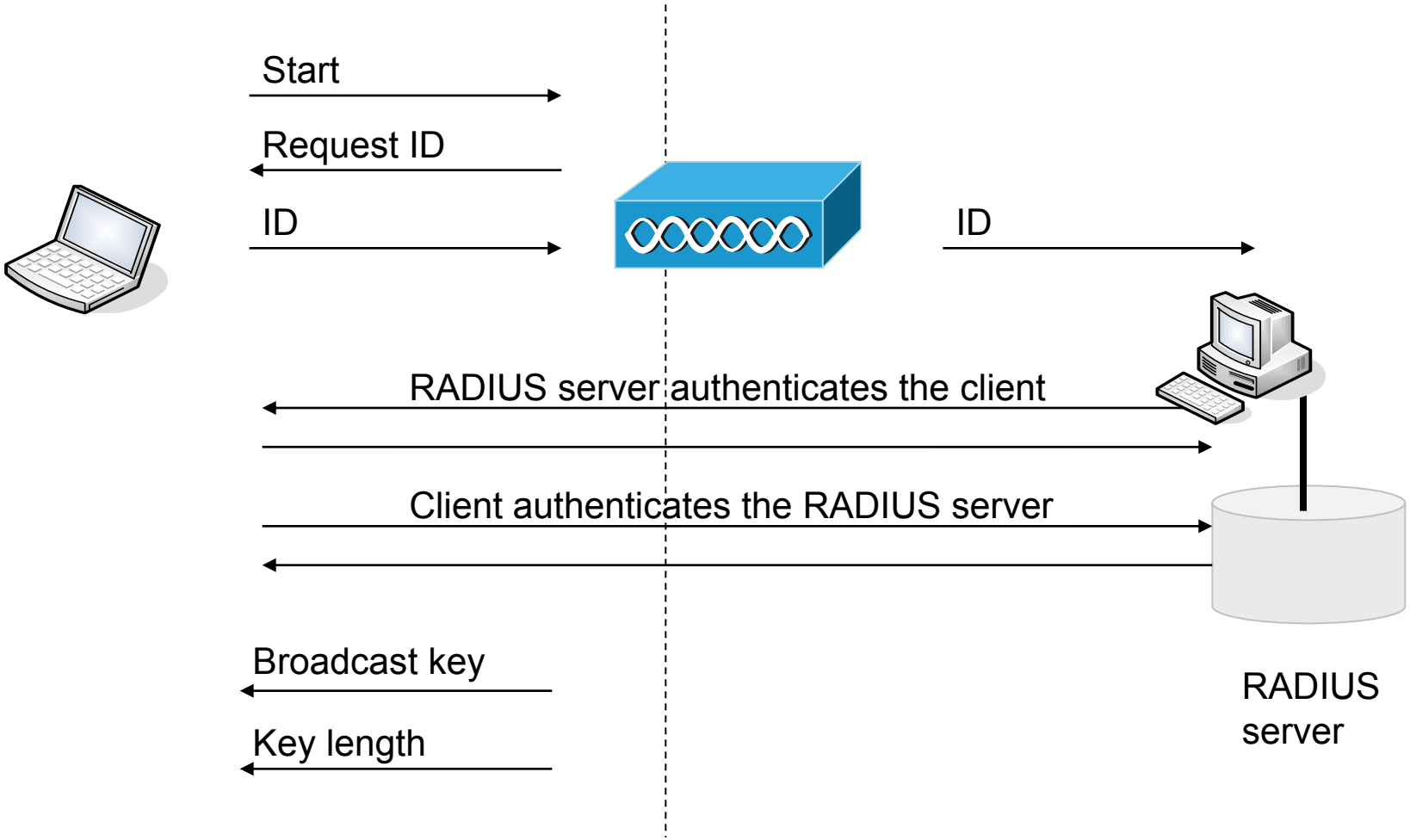




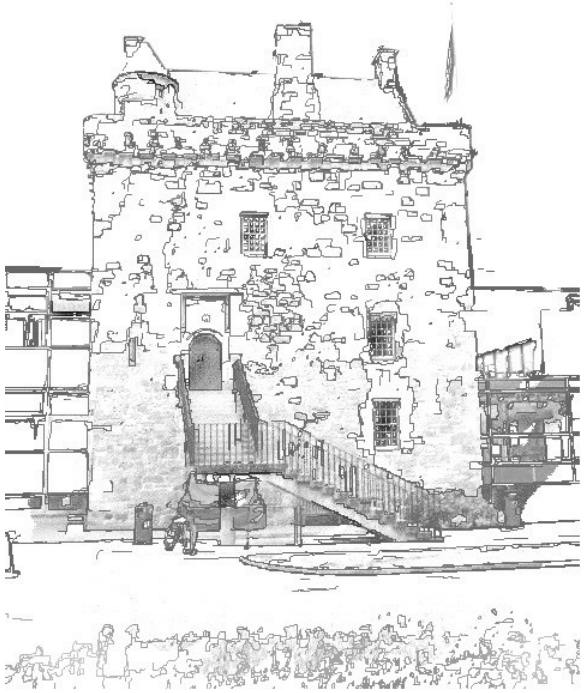
The man-in-the-middle EX-OR’s the two sniffed strings, and determines the random key



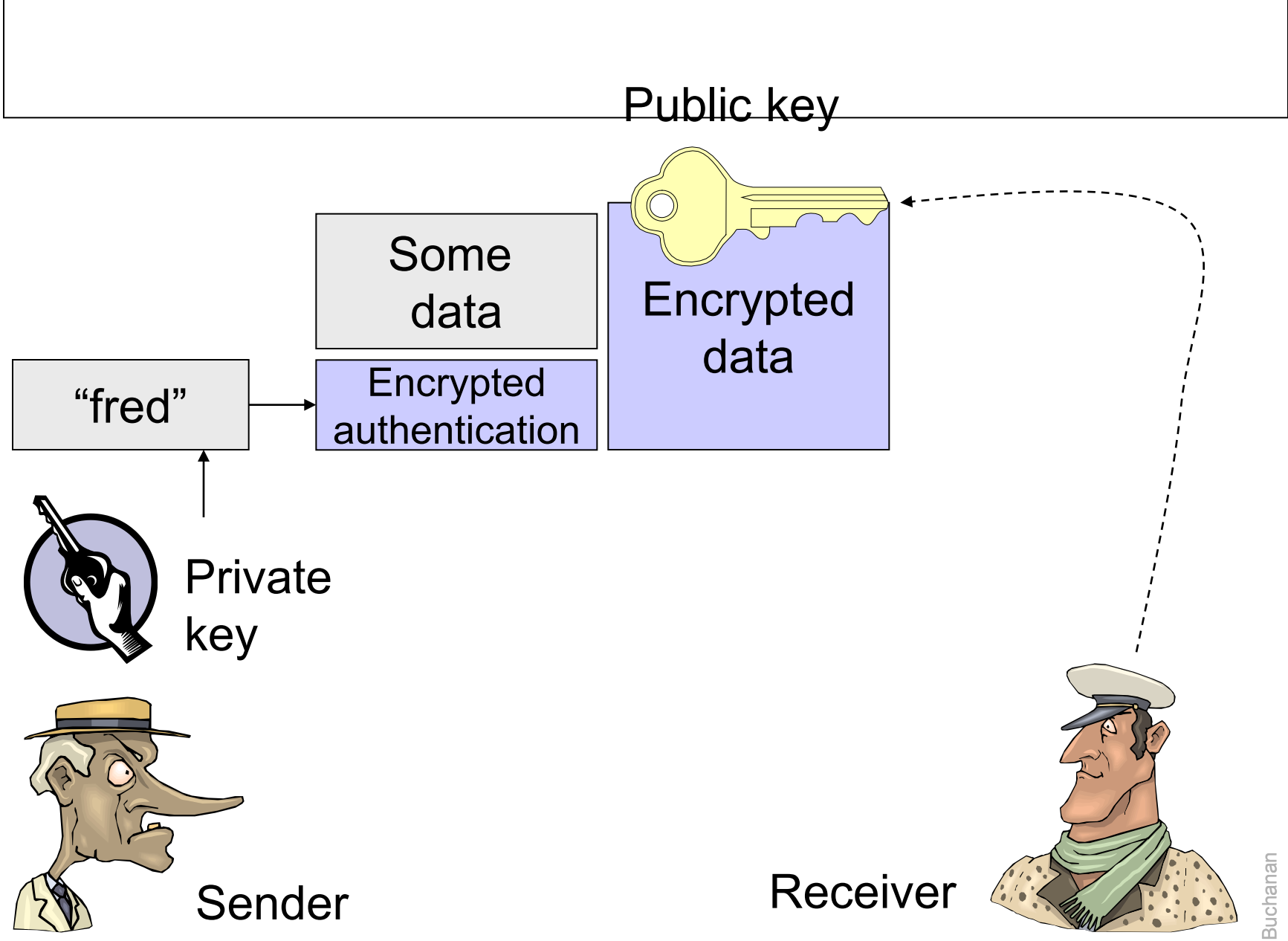




Authenticating using a Digital Certificate



Author: Bill Buchanan



Private key

Encrypted data

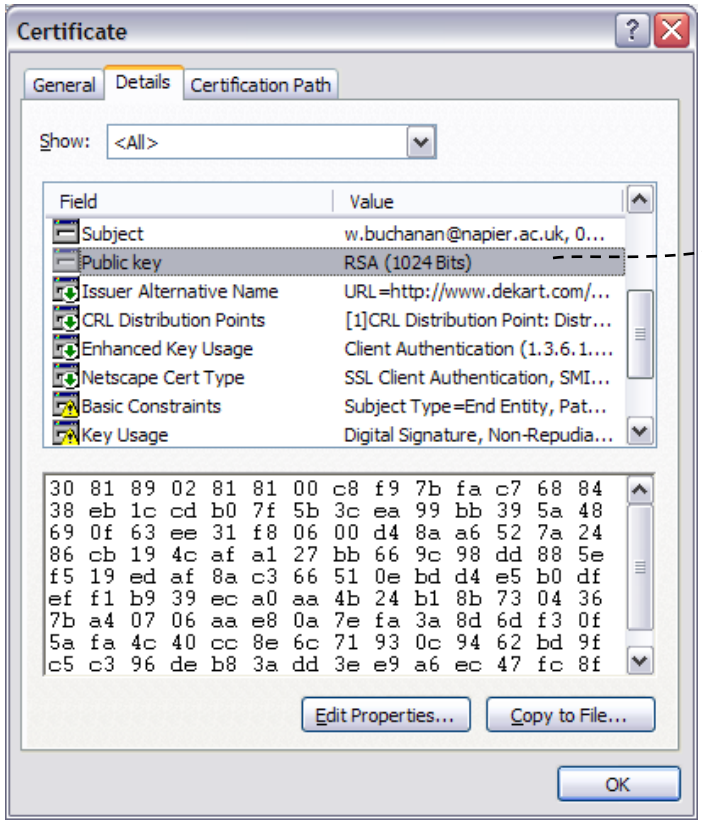
Some data

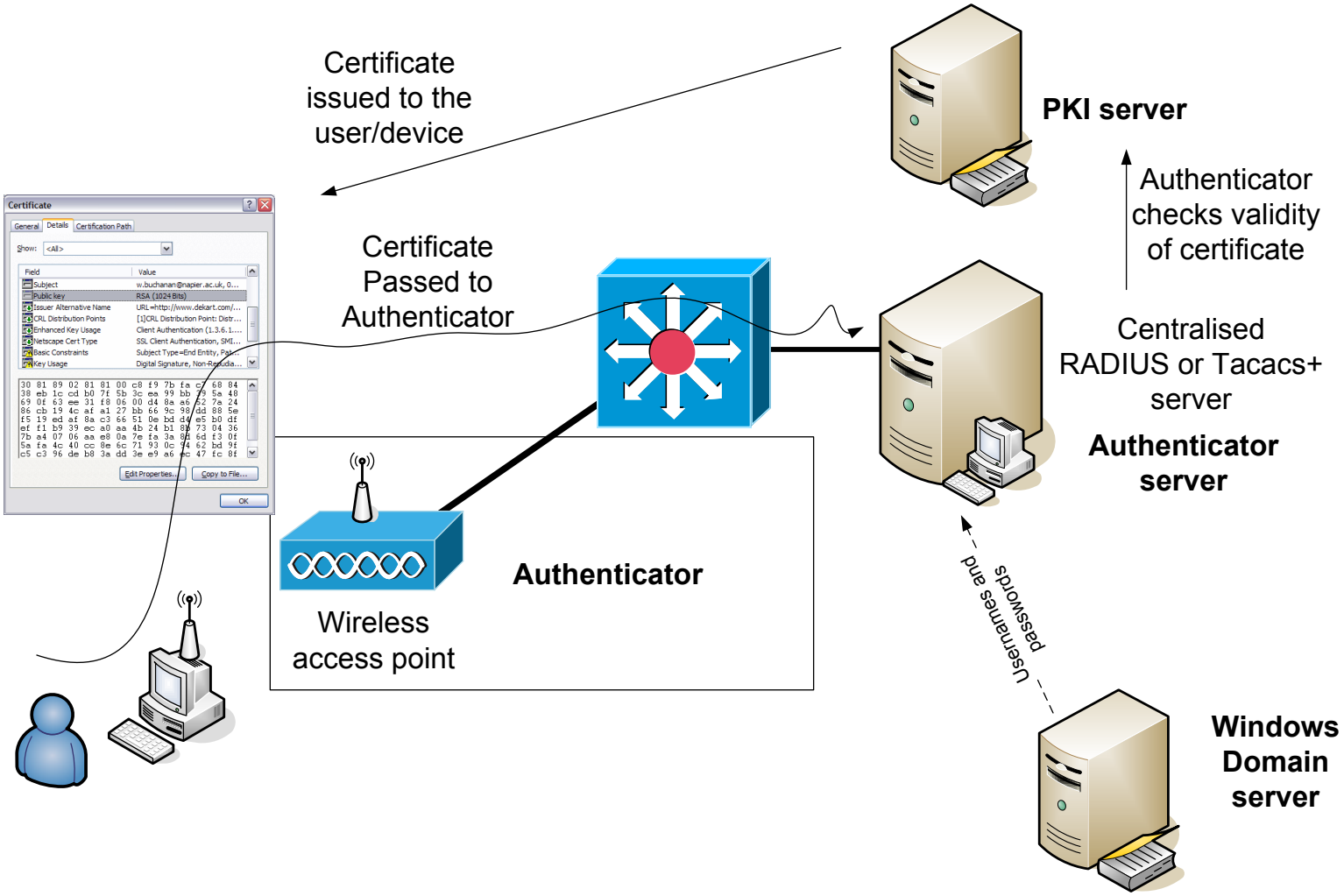
Encrypted authentication

"fred"

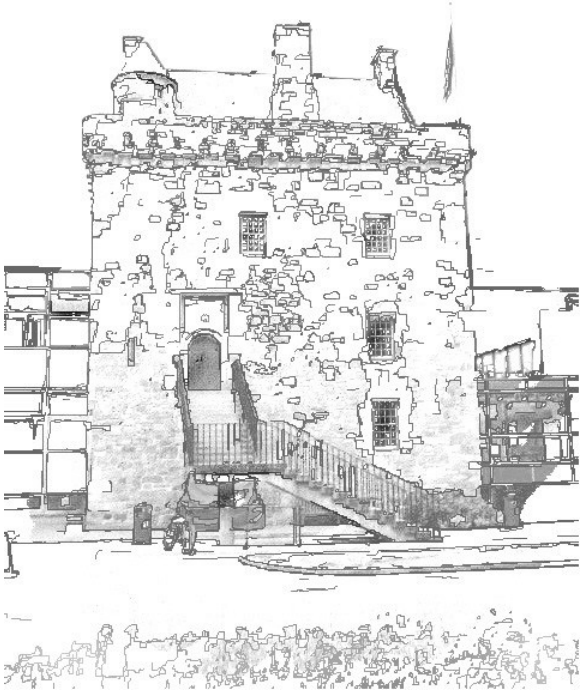
Public key is used to decrypt authentication

Digital certificate





EAP



Author: Bill Buchanan

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.

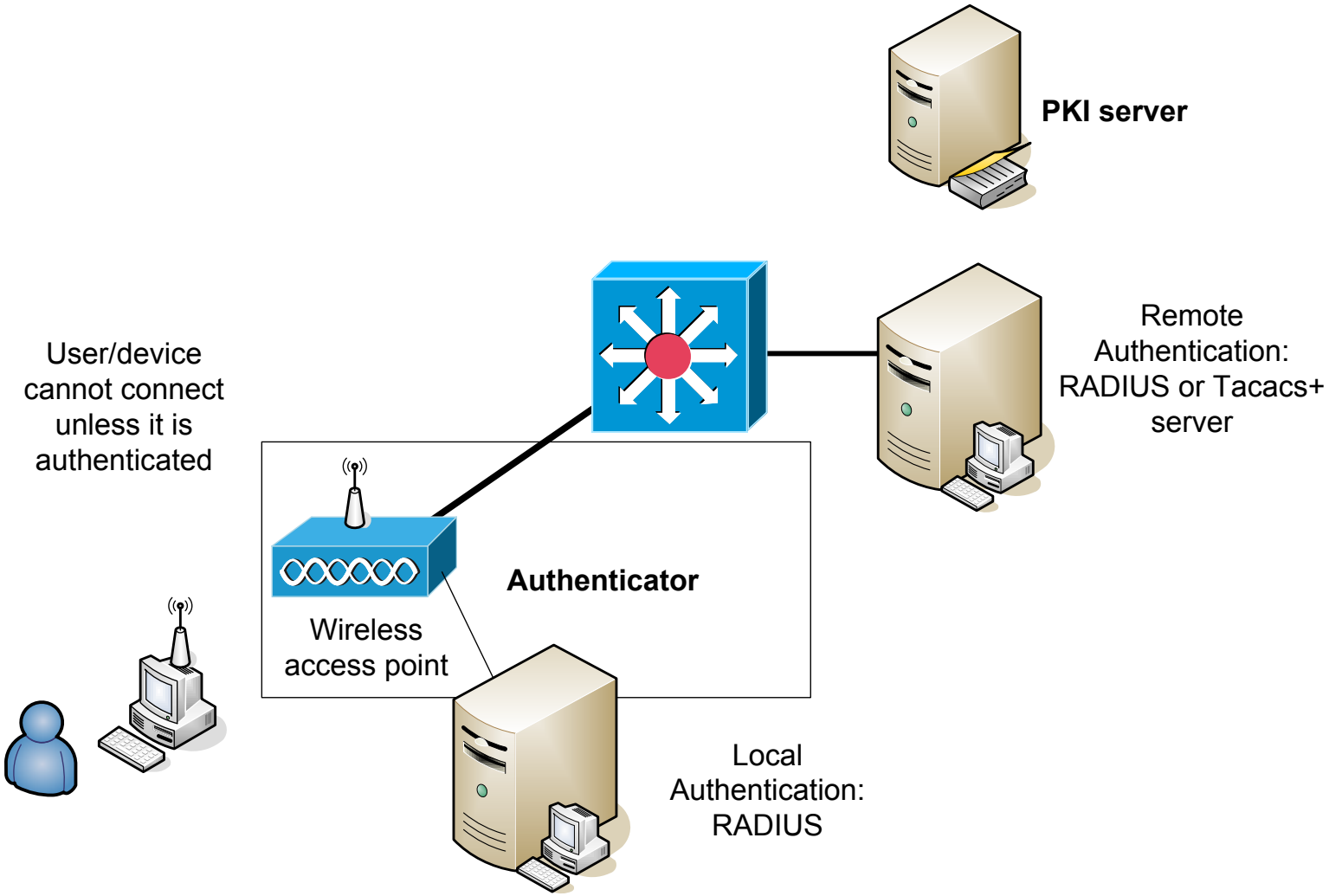
A wireless client cannot gain access to the network, unless it has been authenticated by the access point or a RADIUS server, and has encryption keys.

Author: Bill Buchanan

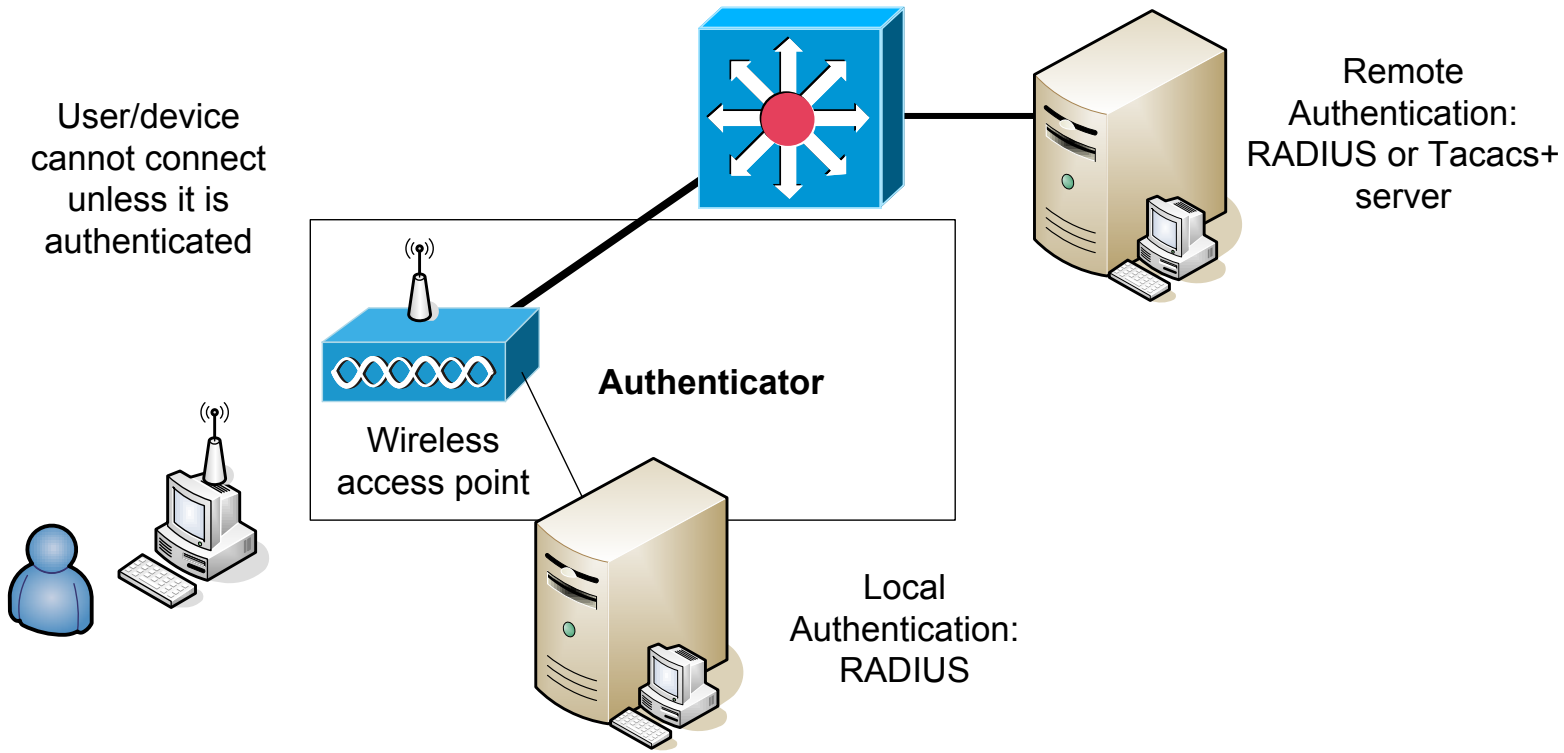
There are many versions of EAP, including:

- **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.

Author: Bill Buchanan



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.



Client details:

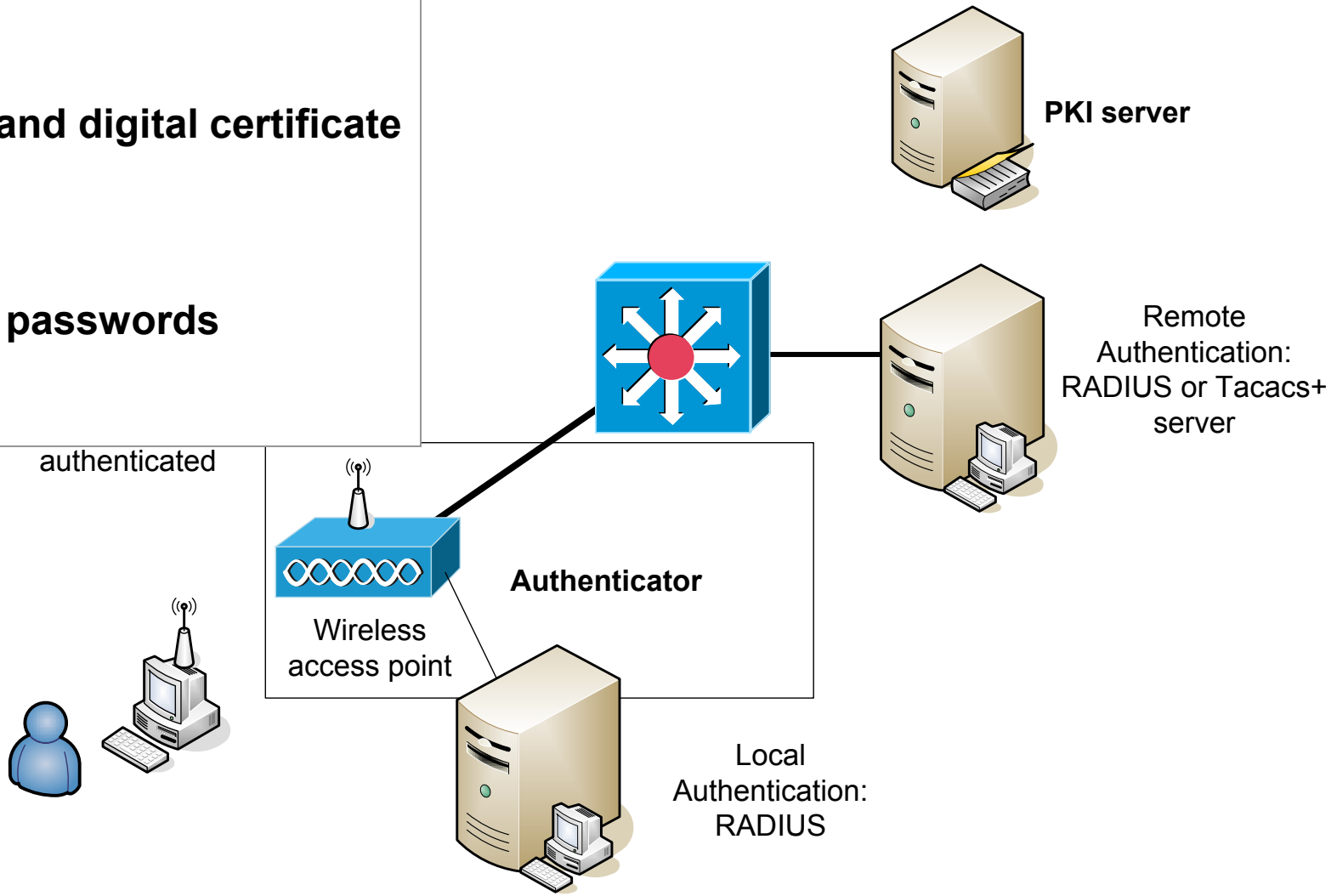
User ID and password.

Or

User ID and digital certificate

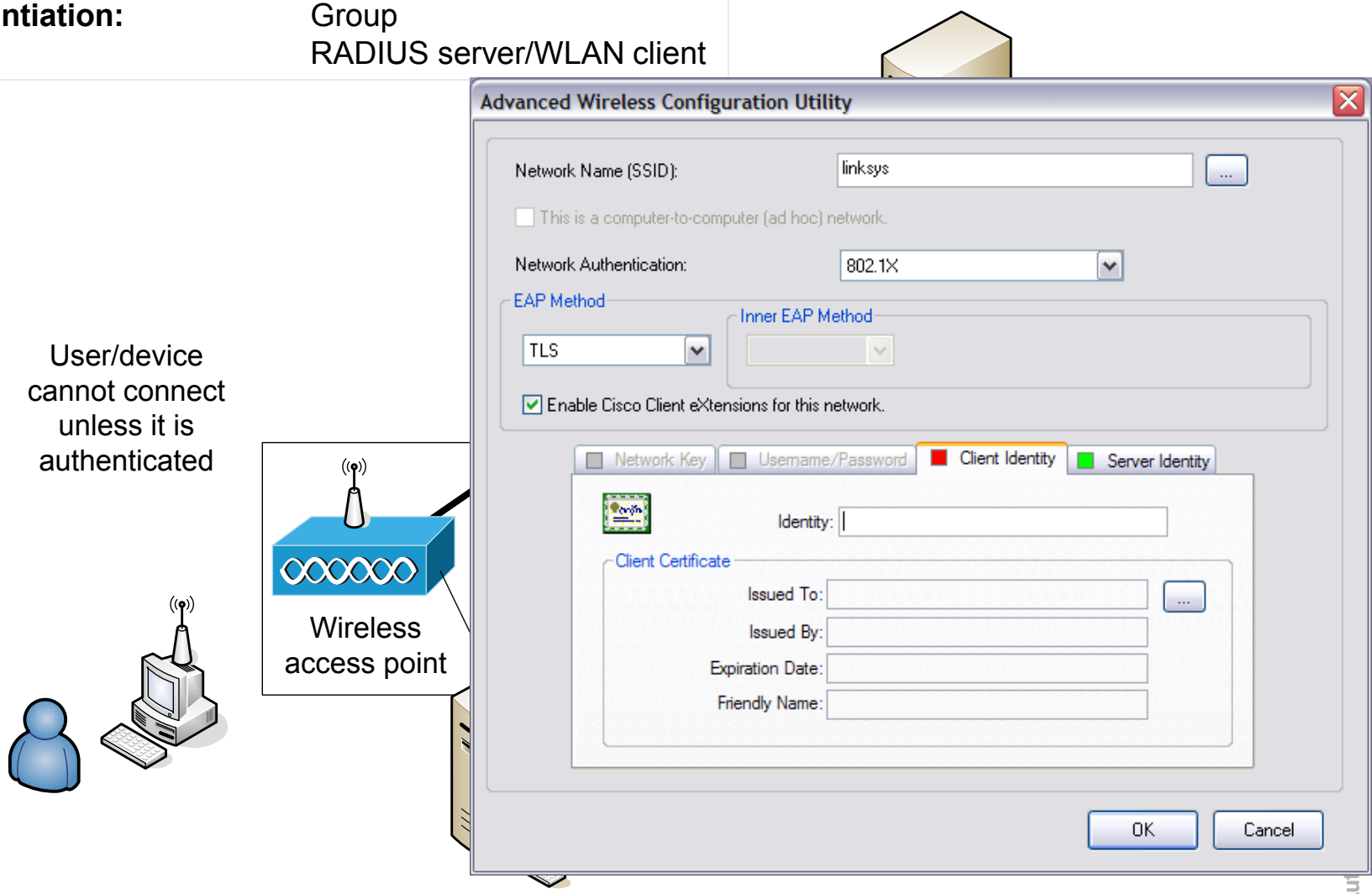
Or

On-time passwords



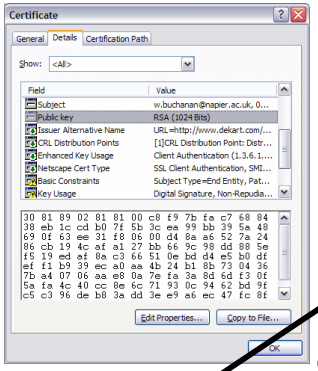
Author: Bill Buchanan

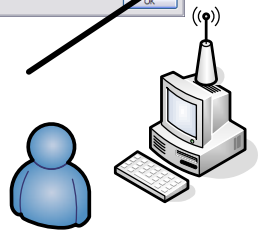
User Authentication:	User ID and digital certificate
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Client Certificate
Open Standard:	Yes
User differentiation:	Group
Certificate:	RADIUS server/WLAN client

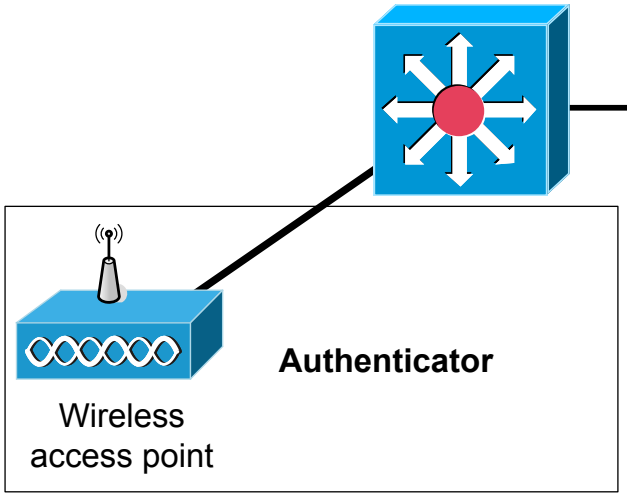


EAP-TLS (EAP-Transport Layer Security):
Digital Certificate is sent to Access Point to authentication the client

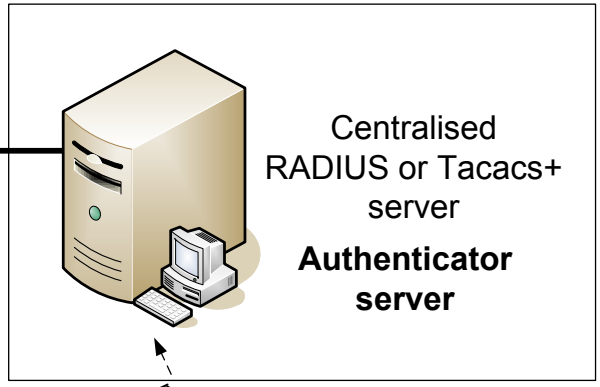
EAP-TLS -> Authenticates client
But certificate required for client

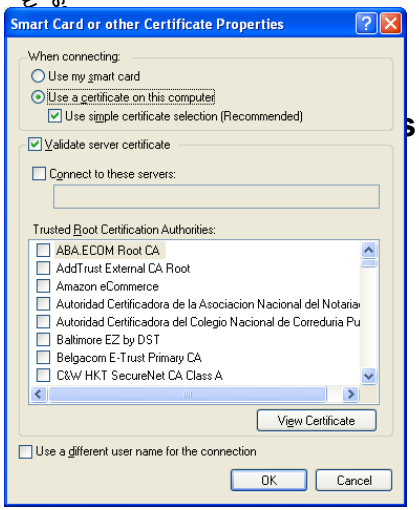






PKI server

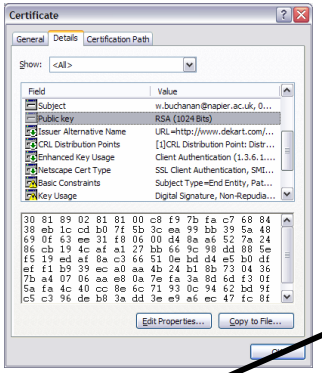




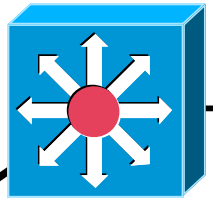
Strengths: Good security.
Weaknesses: Spoof Access Point

Author: Bill Buchanan

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



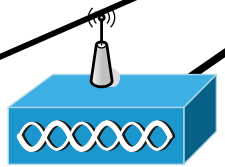
PKI server



Centralised RADIUS or Tacacs+ server

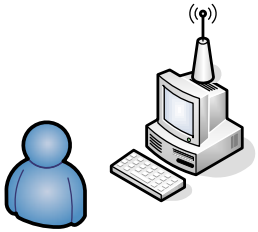
Authenticator server

Do you accept this Certificate (Y/N)?



Authenticator

Wireless access point



Usernames and passwords

Windows Domain server

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

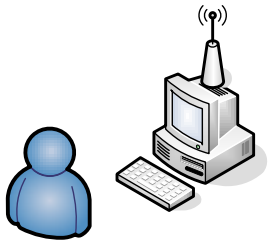
Author: Bill Buchanan

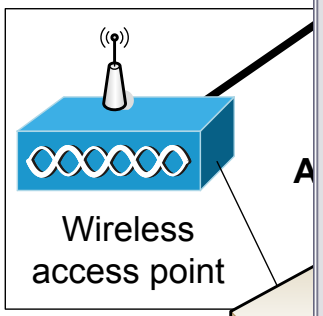
User Authentication:	User ID and password
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Not Supported
Open Standard:	No (Cisco-derived)
User differentiation:	Group
Certificate:	None

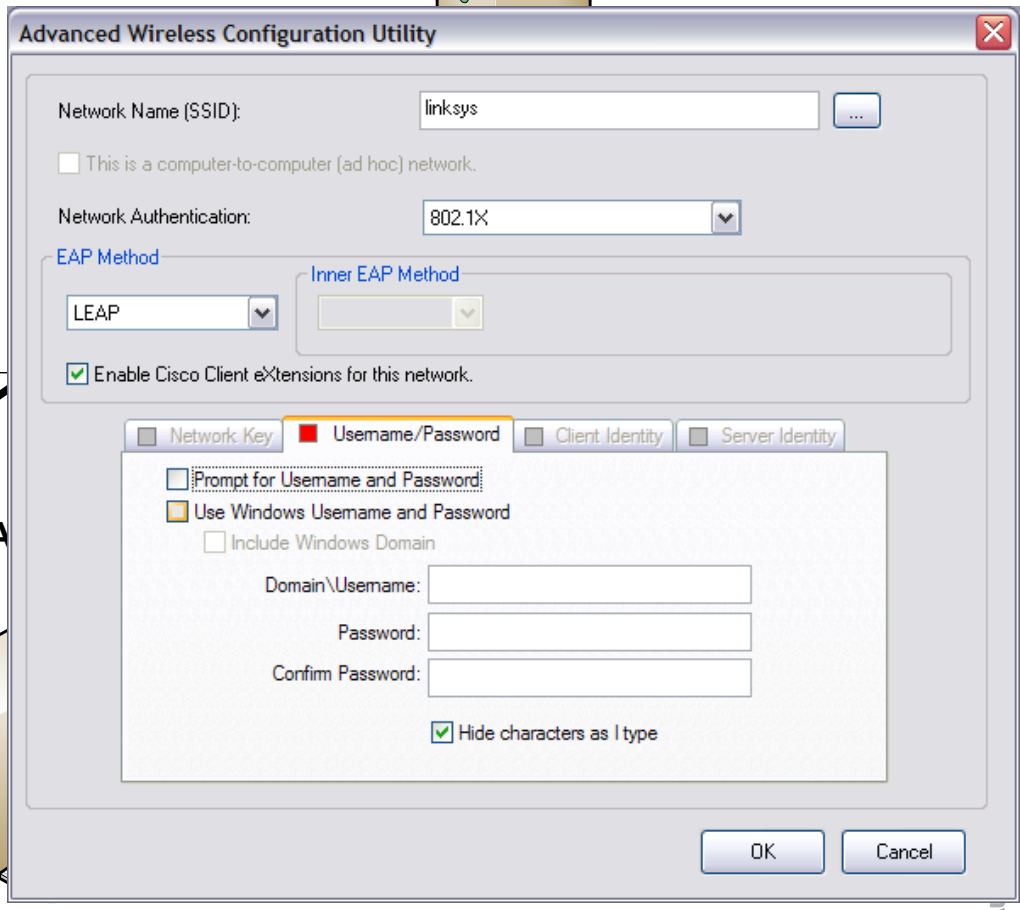
LEAPs is open to attack from a dictionary attack. **Use strong passwords!!!**

PKI server

User/device cannot connect unless it is authenticated







User Auth
Key size:
Encryptio
Device Au
Open Star
User diffe
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

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.

Done

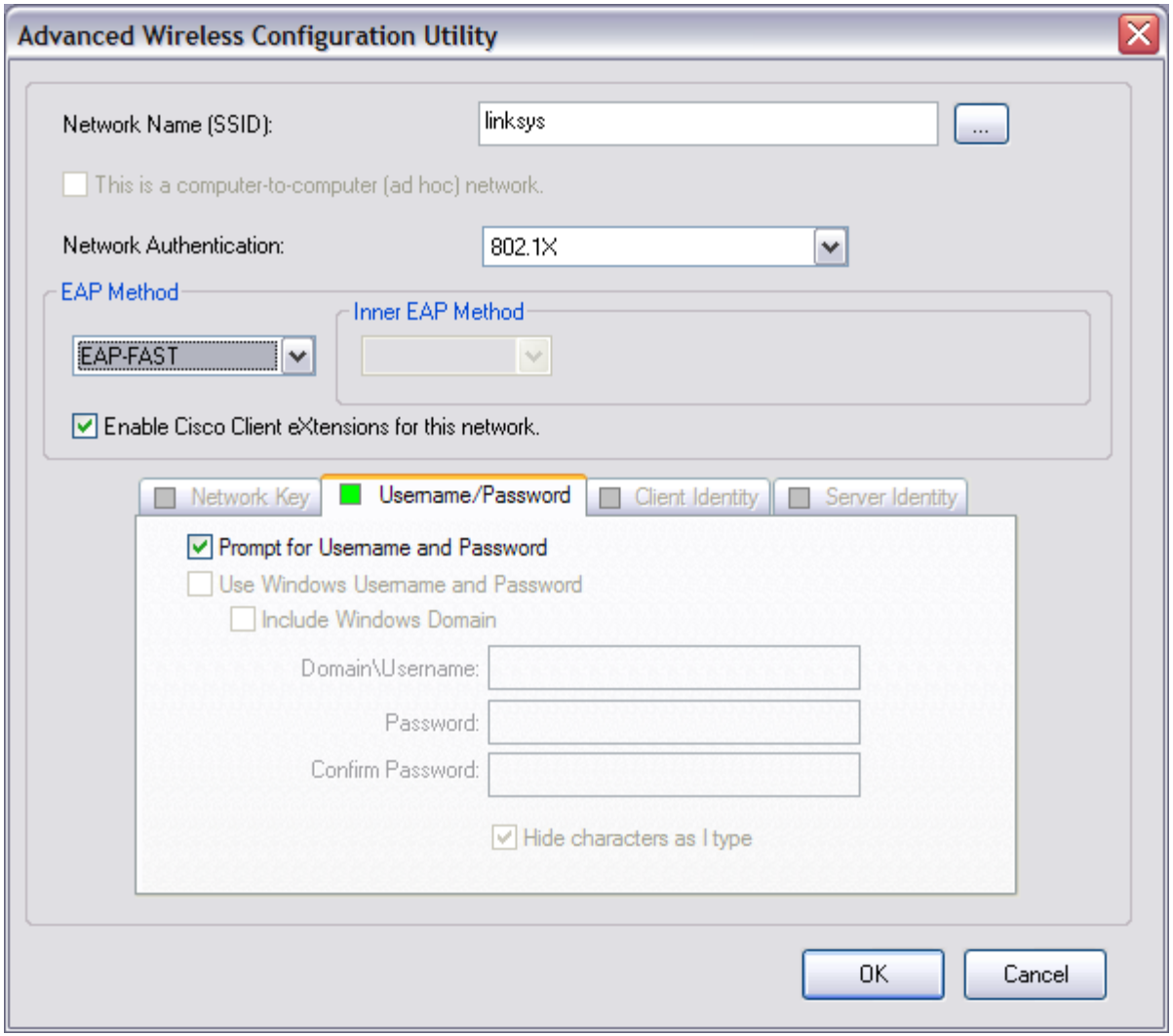
OK Cancel

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.



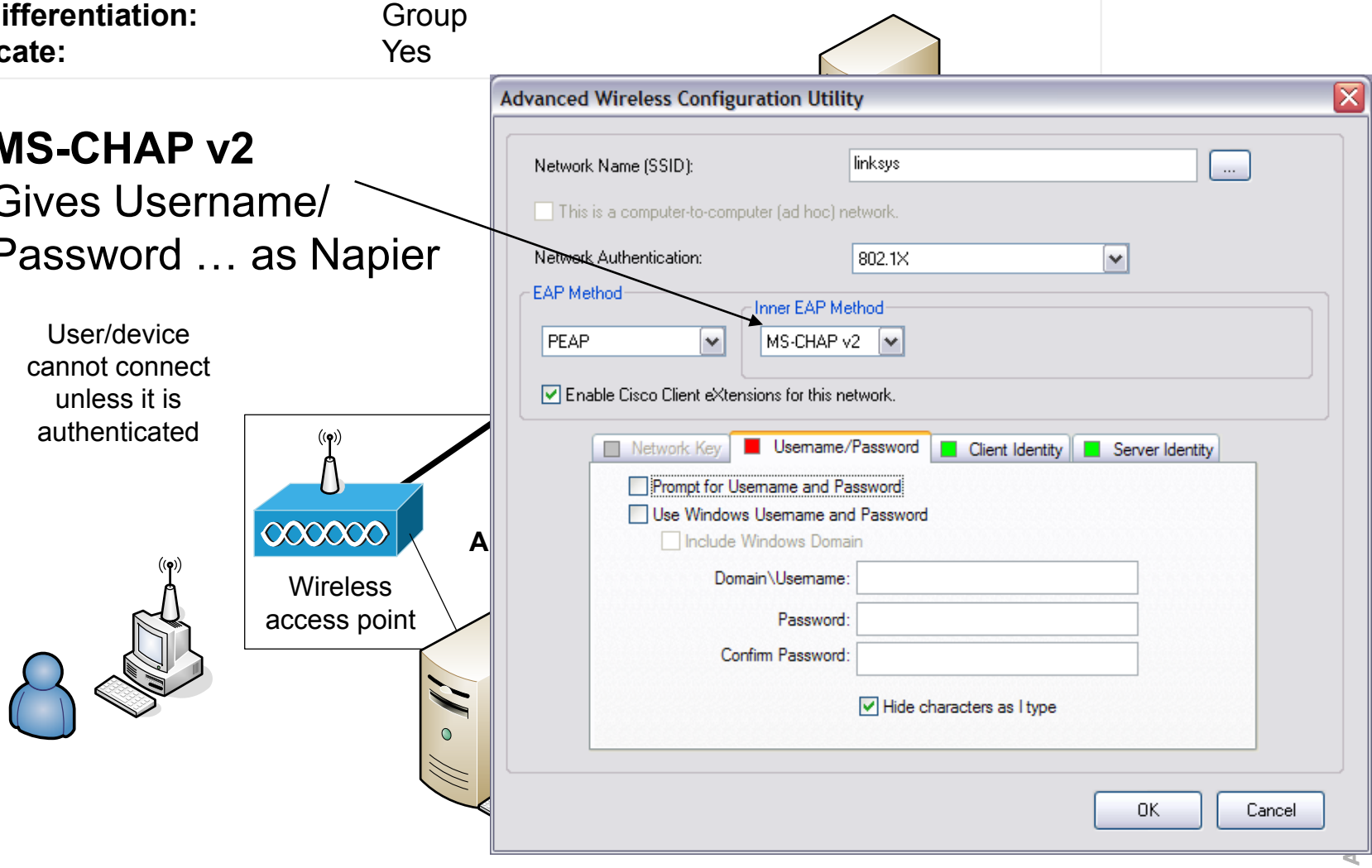
Author: Bill Buchanan

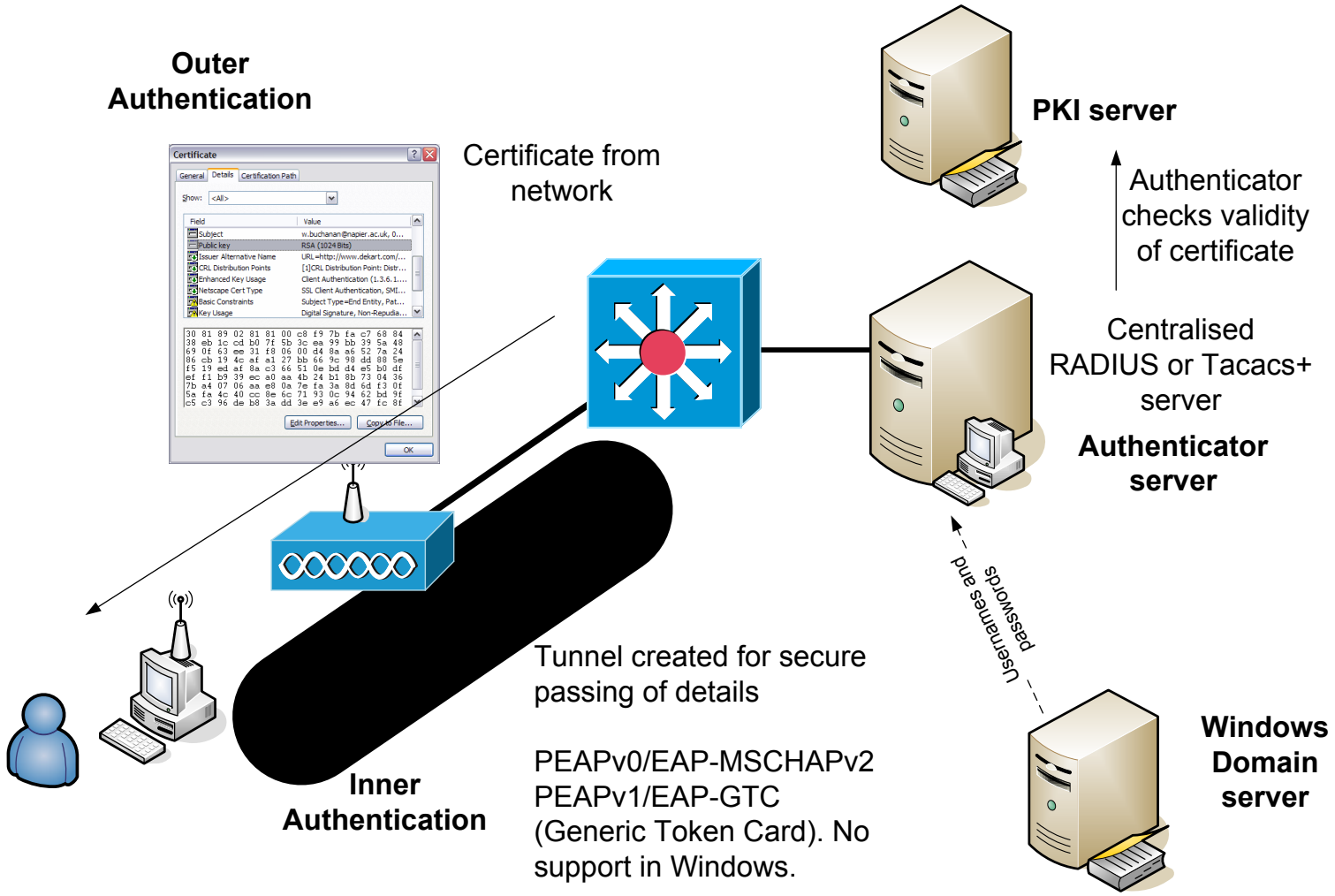
User Authentication:	User ID and password or **OTP** (one-time password)
Key size:	128 bits
Encryption:	RC4
Device Authentication:	Not supported
Open Standard:	Yes (dev… Cisco, Microsoft and RSA Labs)
User differentiation:	Group
Certificate:	Yes

MS-CHAP v2

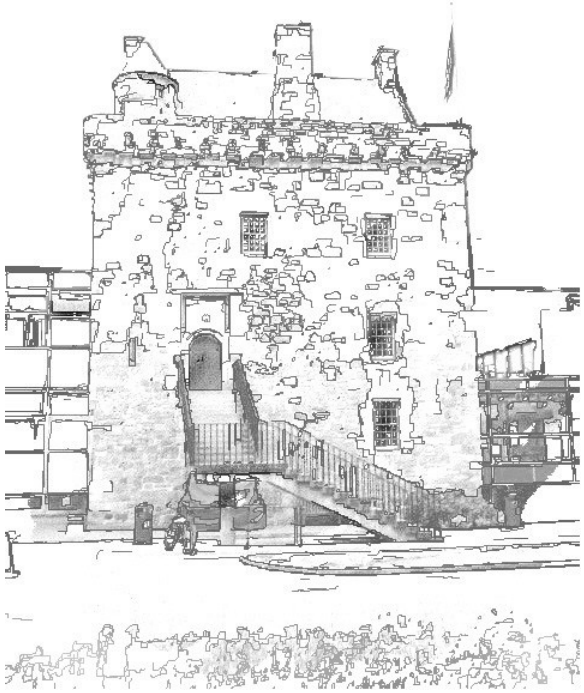
Gives Username/ Password … as Napier

User/device cannot connect unless it is authenticated

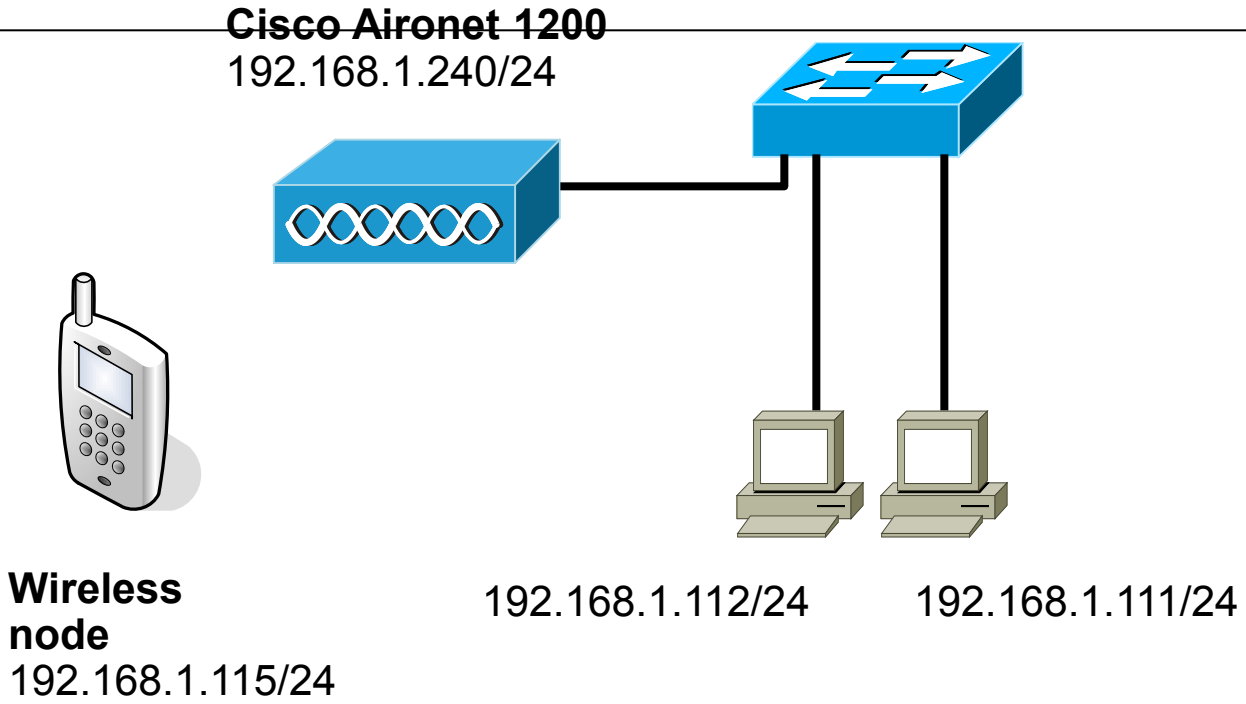




Configuration – Local RADIUS server

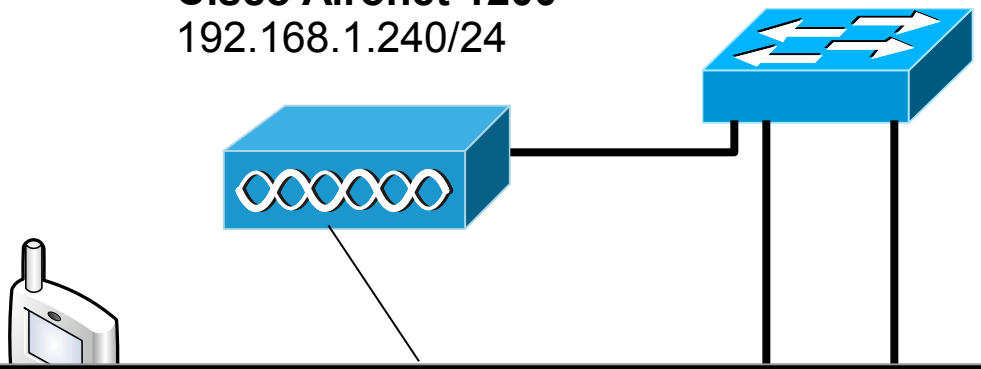


Author: Bill Buchanan



Author: Bill Buchanan

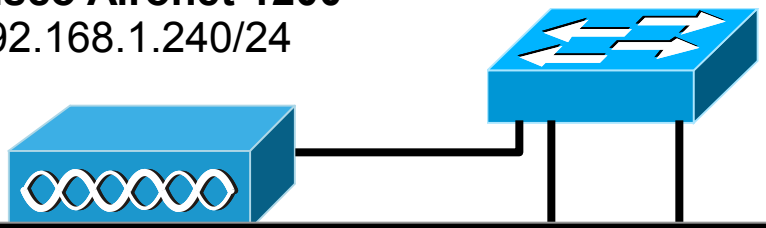
Cisco Aironet 1200
192.168.1.240/24



```
(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
```

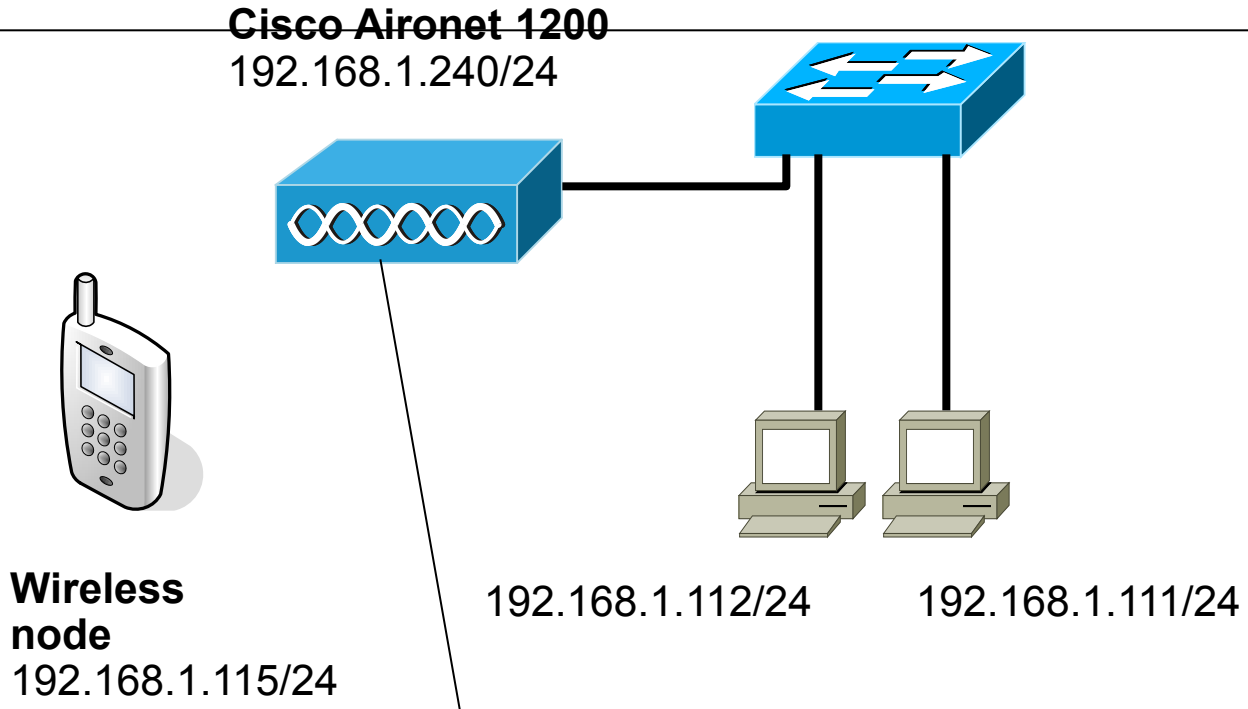
Author: Bill Buchanan

Cisco Aironet 1200
192.168.1.240/24



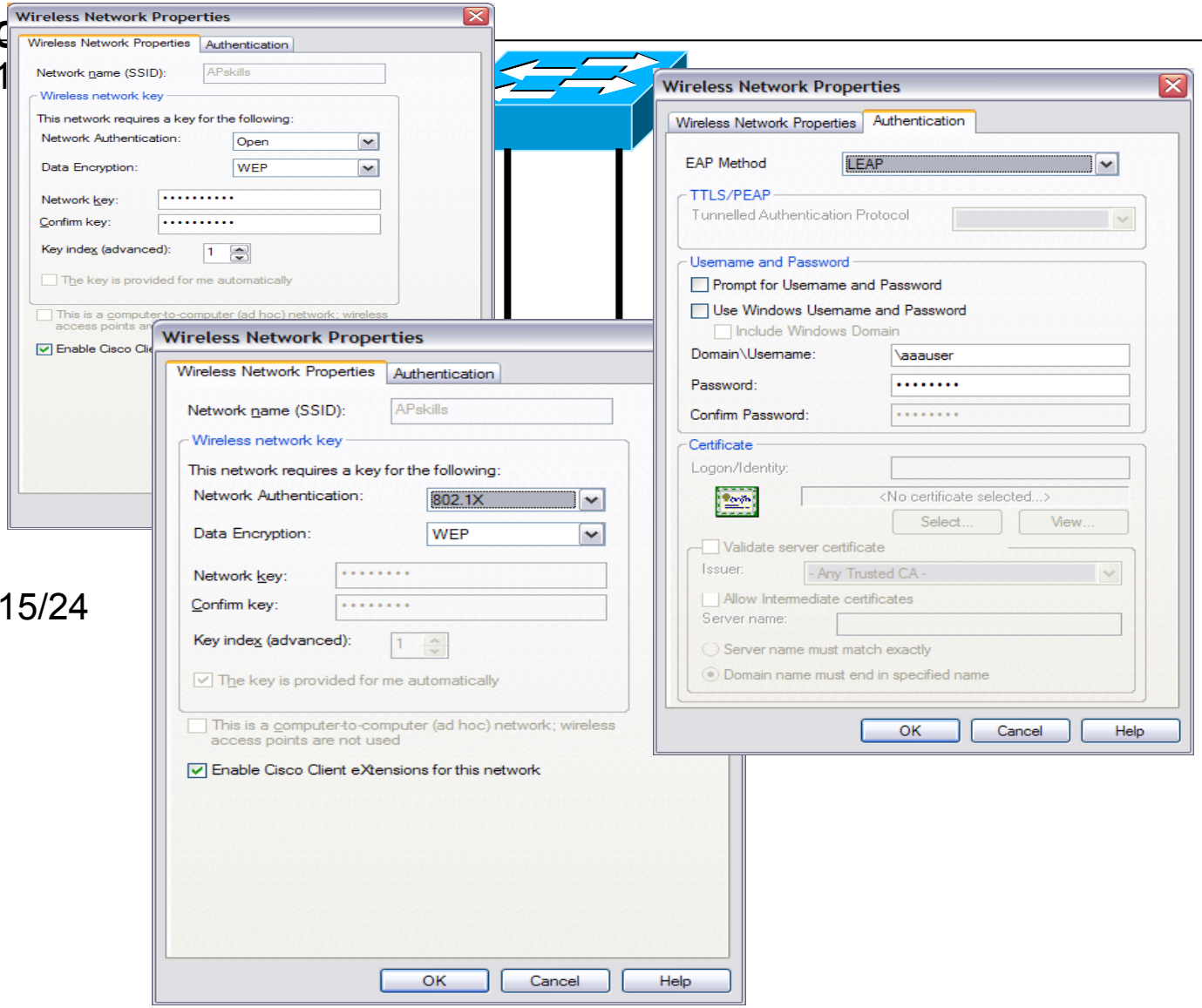
Wirel
node
192.1

```
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
```



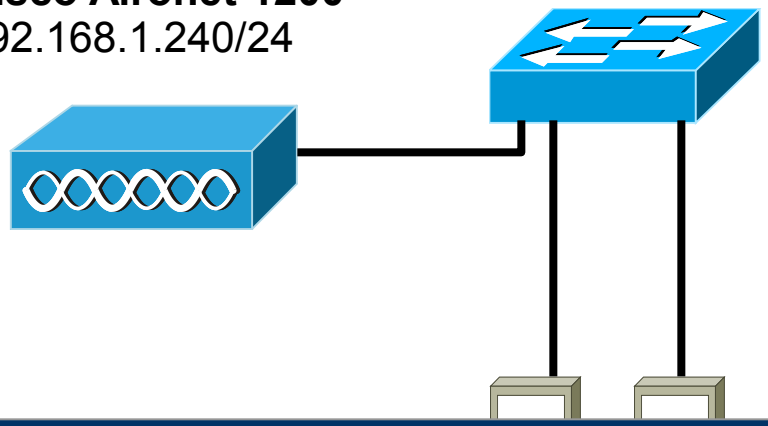

```
(config)# radius-server local
(config-radsrv)# nas 192.168.1.240 key sharedkey
(config-radsrv)# user aaauser password aaapass
(config-radsrv)# user bbbuser password bbbpass
(config-radsrv)# exit
(config)# radius-server host 192.168.1.240 auth-port 1812
                  acct-port 1813 key sharedkey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

Wireless node
192.168.1.115/24



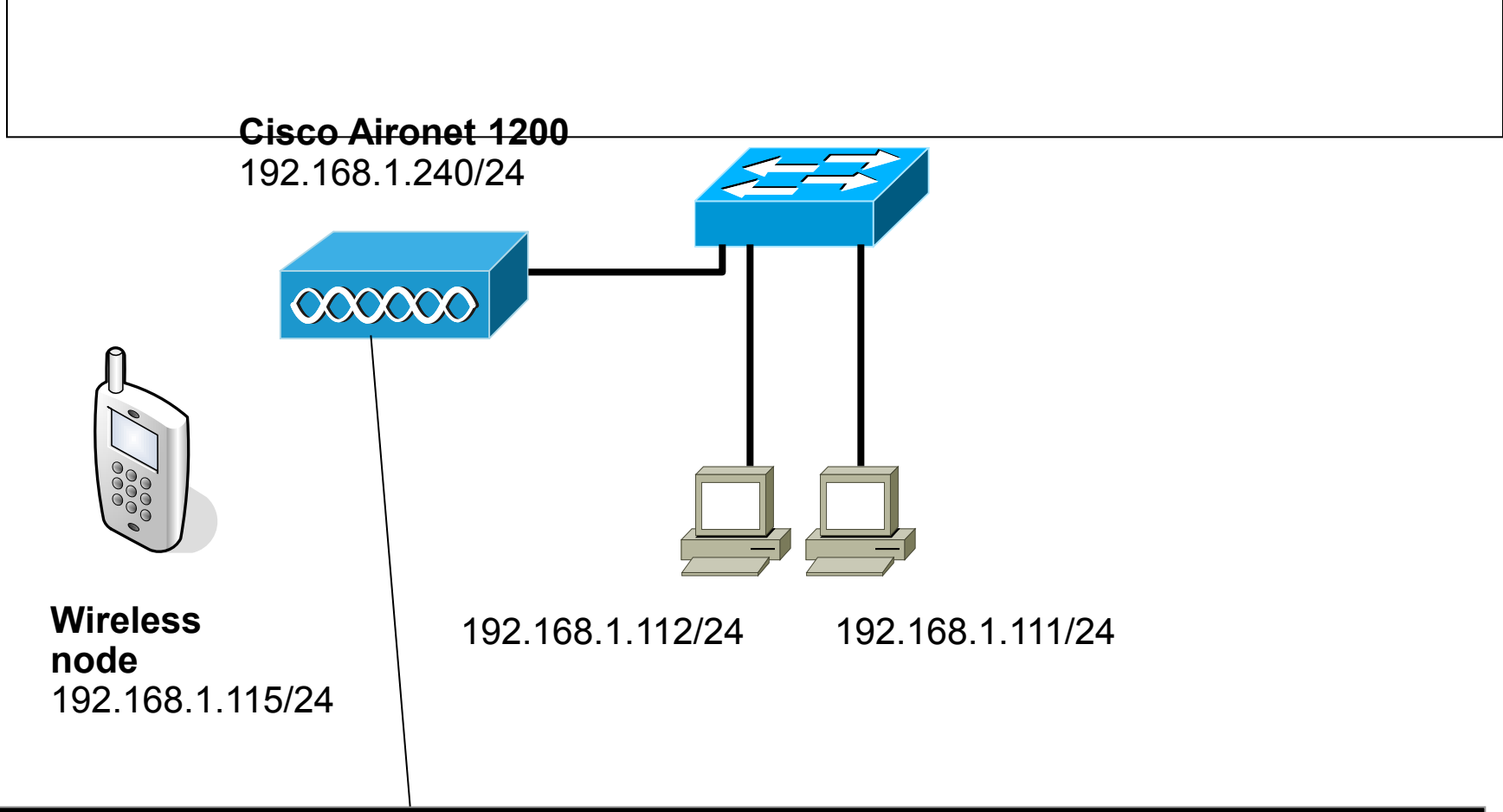
Author: Bill Buchanan

Cisco Aironet 1200
192.168.1.240/24



Wireless node
192.168.1.11

```
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

Wireless node
192.168.1.115/24

Cisco IOS Series AP - Home

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://192.168.1.110/ap_home.htm Go

Close Window

Cisco Systems

Cisco 1200 Access Point

HOME
EXPRESS SET-UP
NETWORK MAP +
ASSOCIATION
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

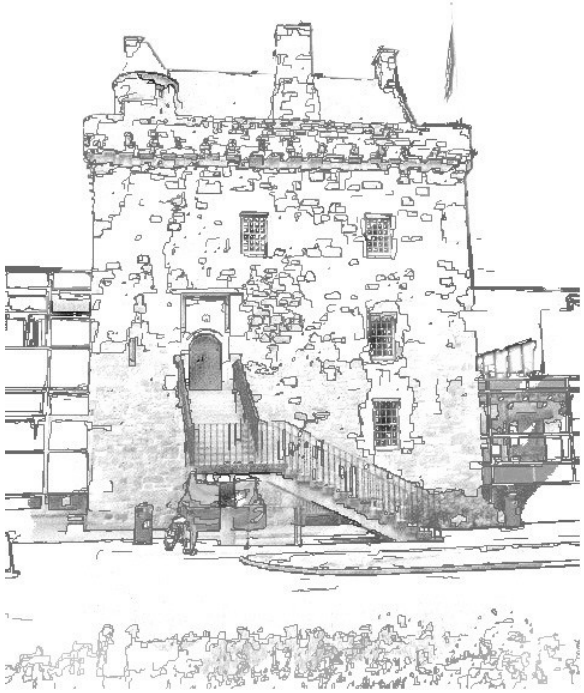
Hostname ap — ap uptime is 2 minutes

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

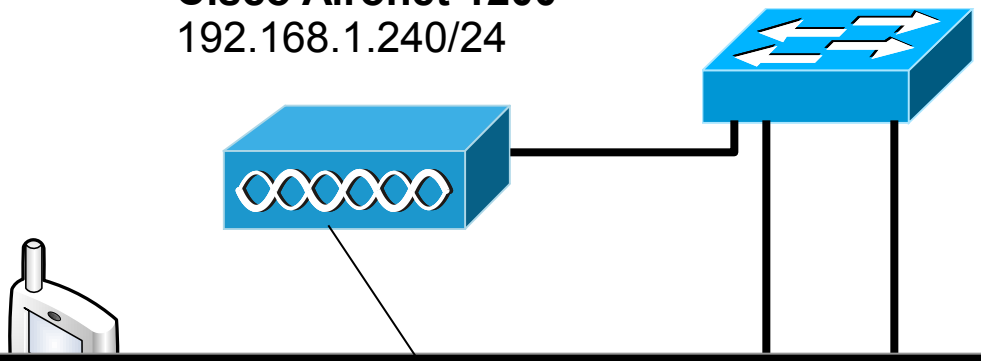
```
ap#show dot11
802.11 Client Stations on Dot11Radio0:
SSID [NapierSSID] :
MAC Address     IP address      Device          Name    Parent State
0090.4b54.d83a 192.168.1.115    4500-radio      -       self    EAP-Assoc
Others:  (not related to any ssid)
```

Configure for Remote TACACS+ Server



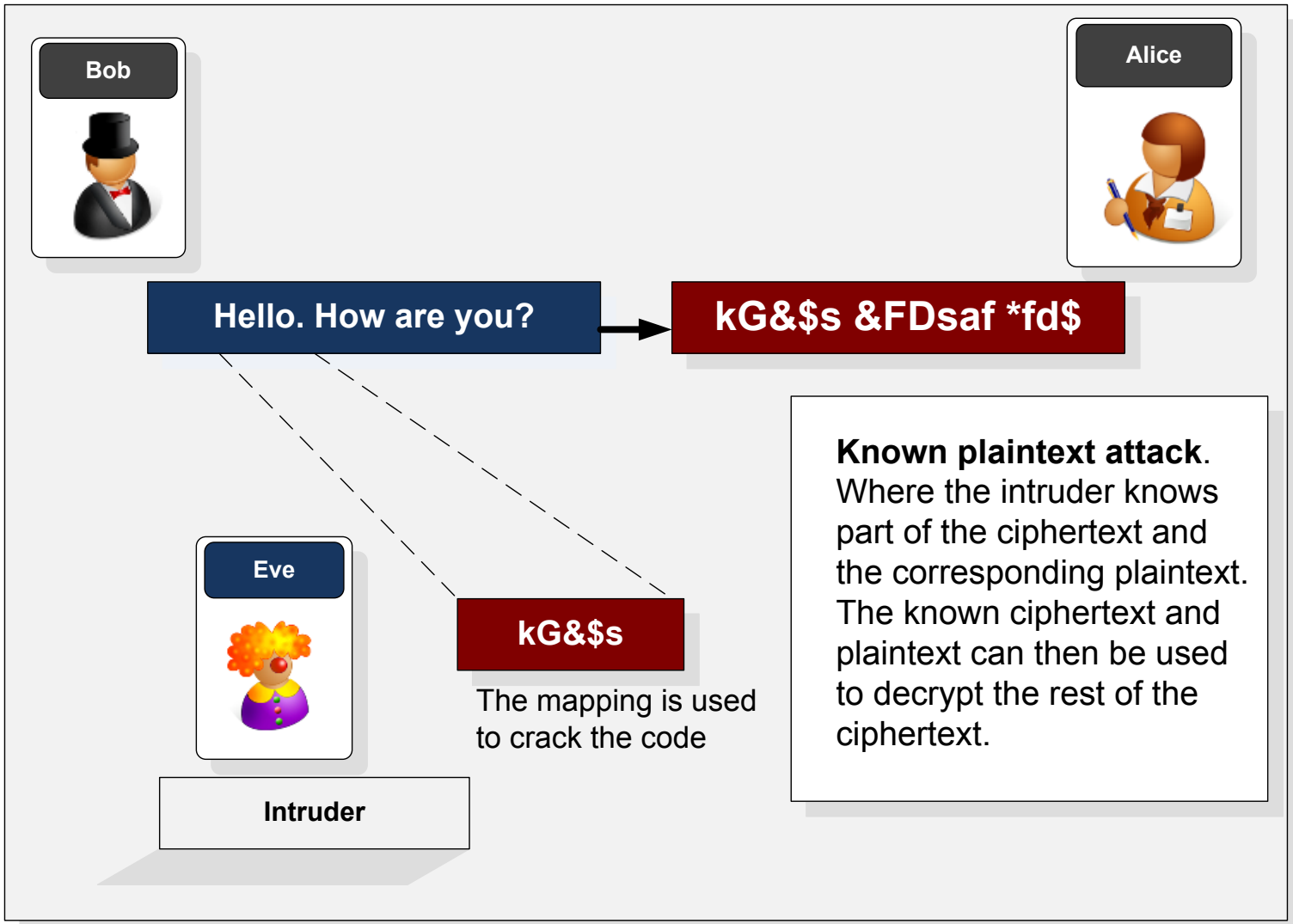
Author: Bill Buchanan

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
```

Author: Bill Buchanan



Known plaintext attack. Where the intruder knows part of the ciphertext and the corresponding plaintext. The known ciphertext and plaintext can then be used to decrypt the rest of the ciphertext.

Author: Prof Bill Buchanan

Hello. How are you? → kG&$s &FDsaf *fd$

kG&$s &FDsaf *fd$

Intruder

000...000 — Zhk& $31 004fX

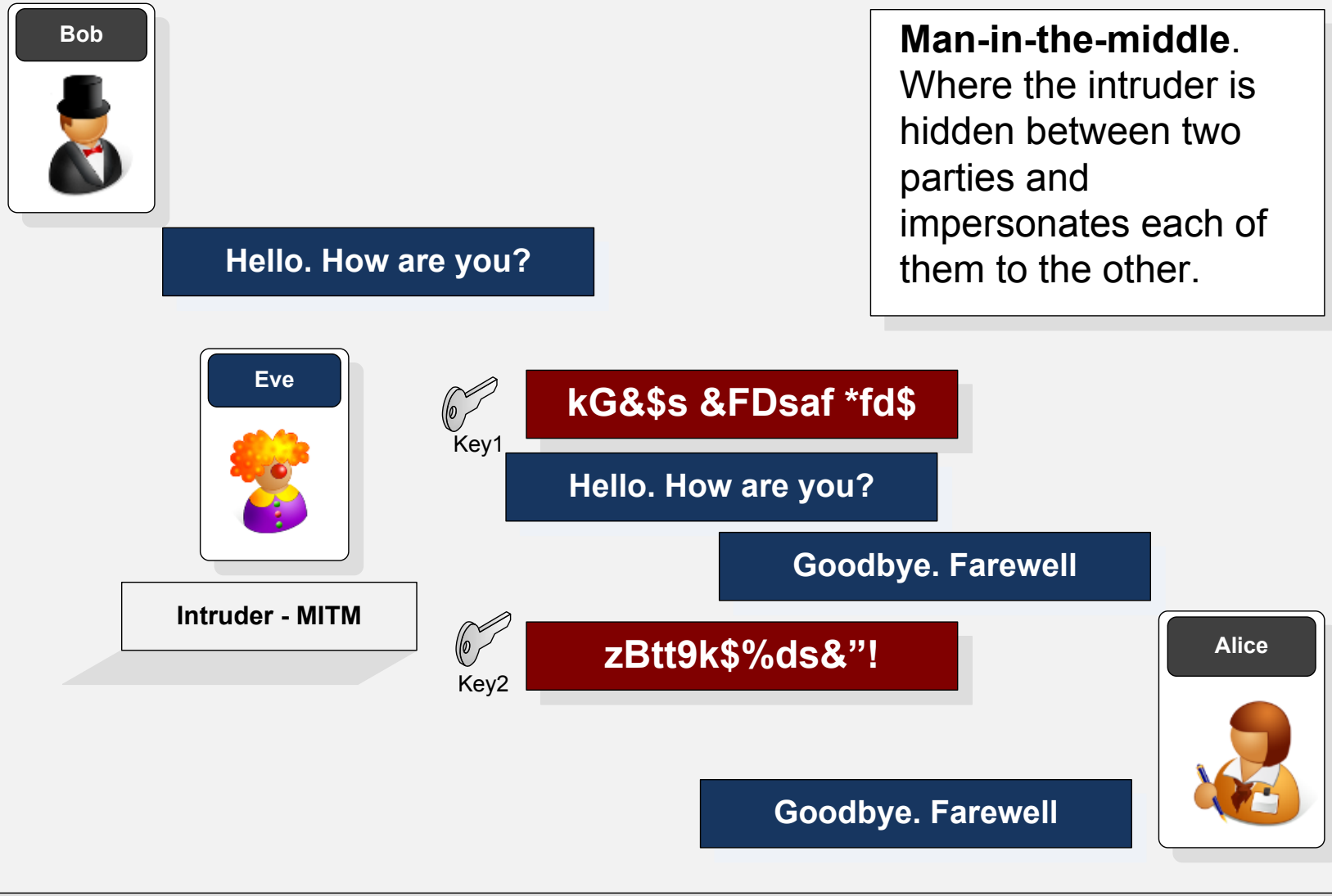
000...001 — kBb 95&$ $23z

001...100 — Hello. How are you?

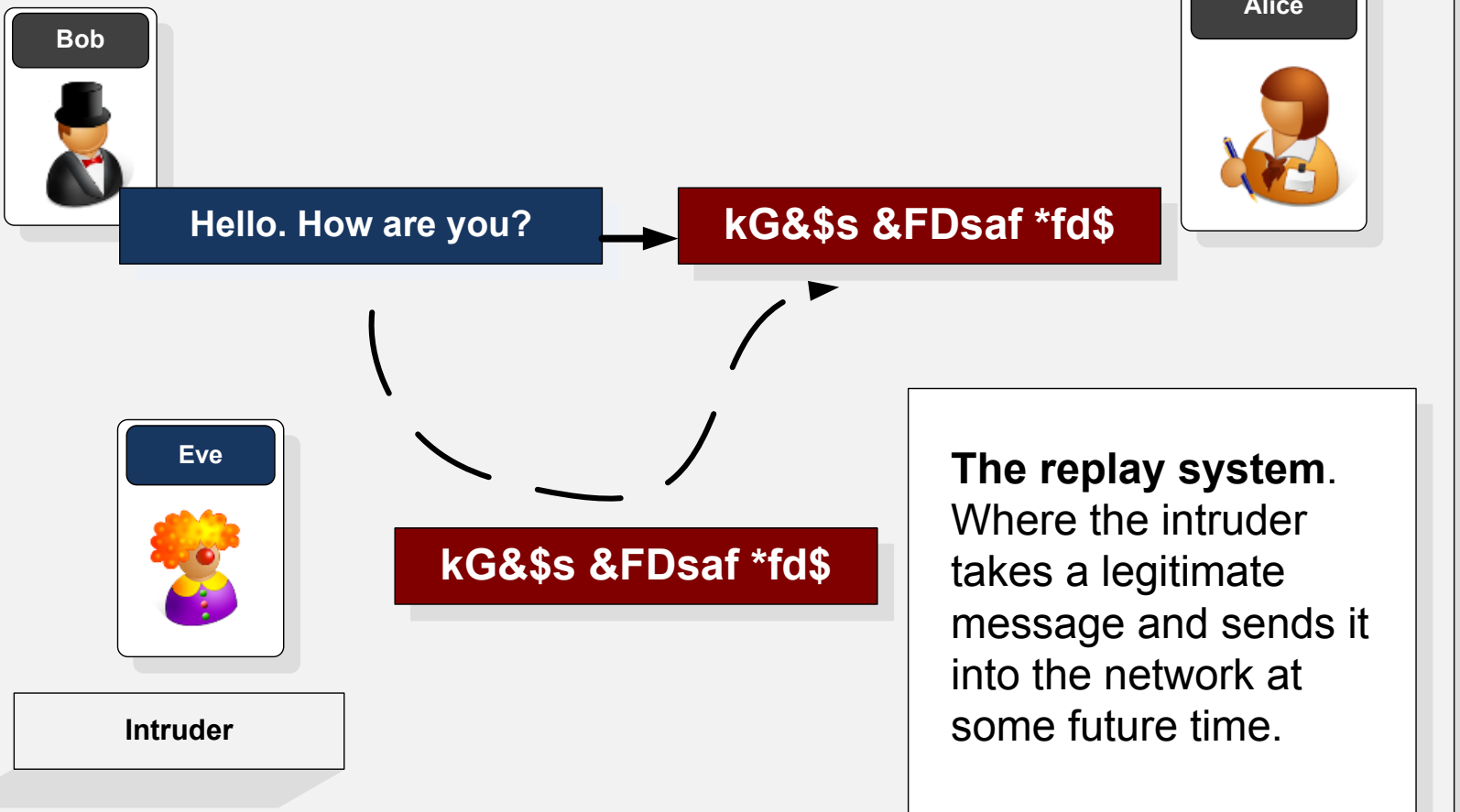
Exhaustive search. Where the intruder uses brute force to decrypt the ciphertext and tries every possible key.

Author: Prof Bill Buchanan

Man-in-the-middle. Where the intruder is hidden between two parties and impersonates each of them to the other.

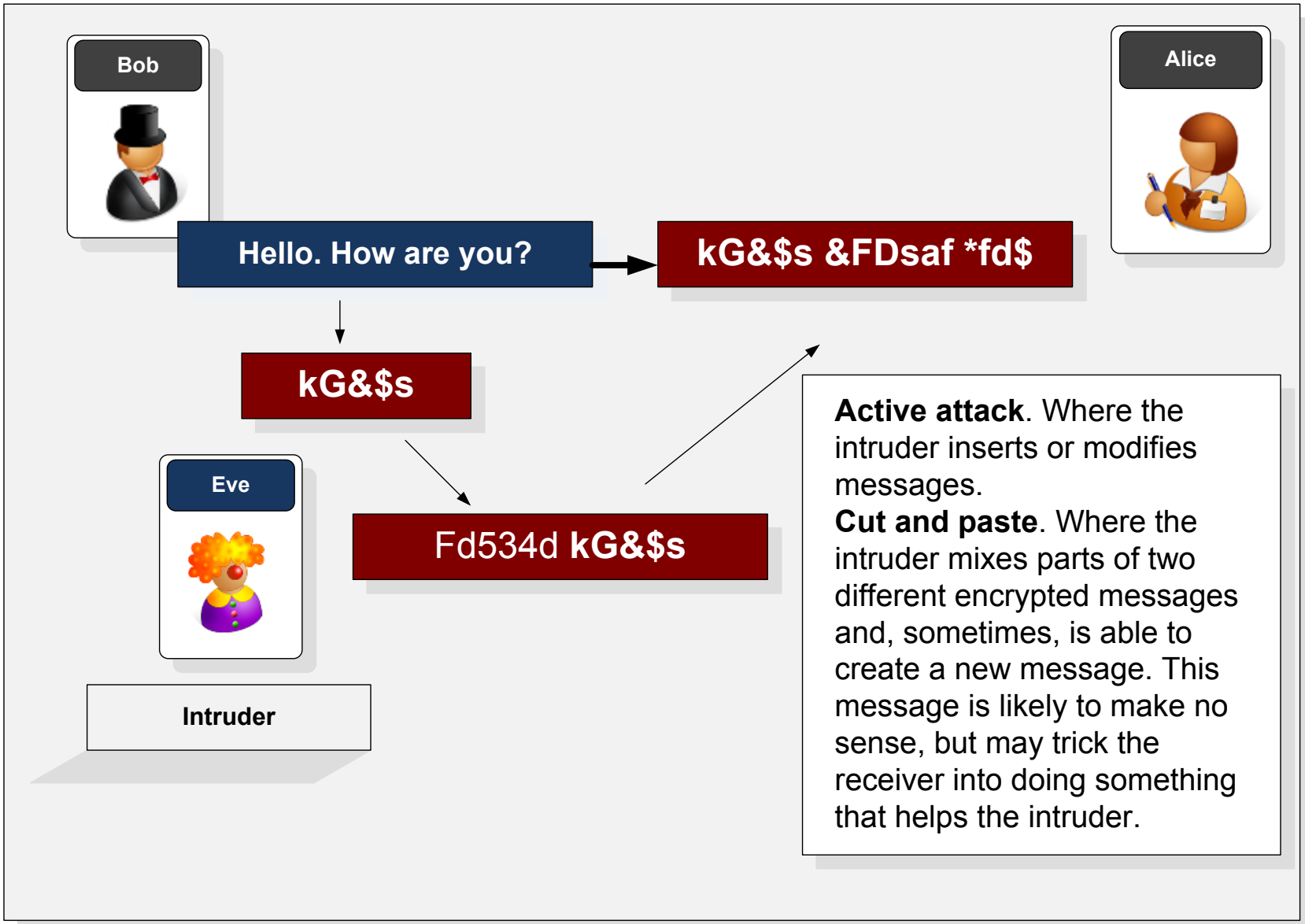


Author: Prof Bill Buchanan



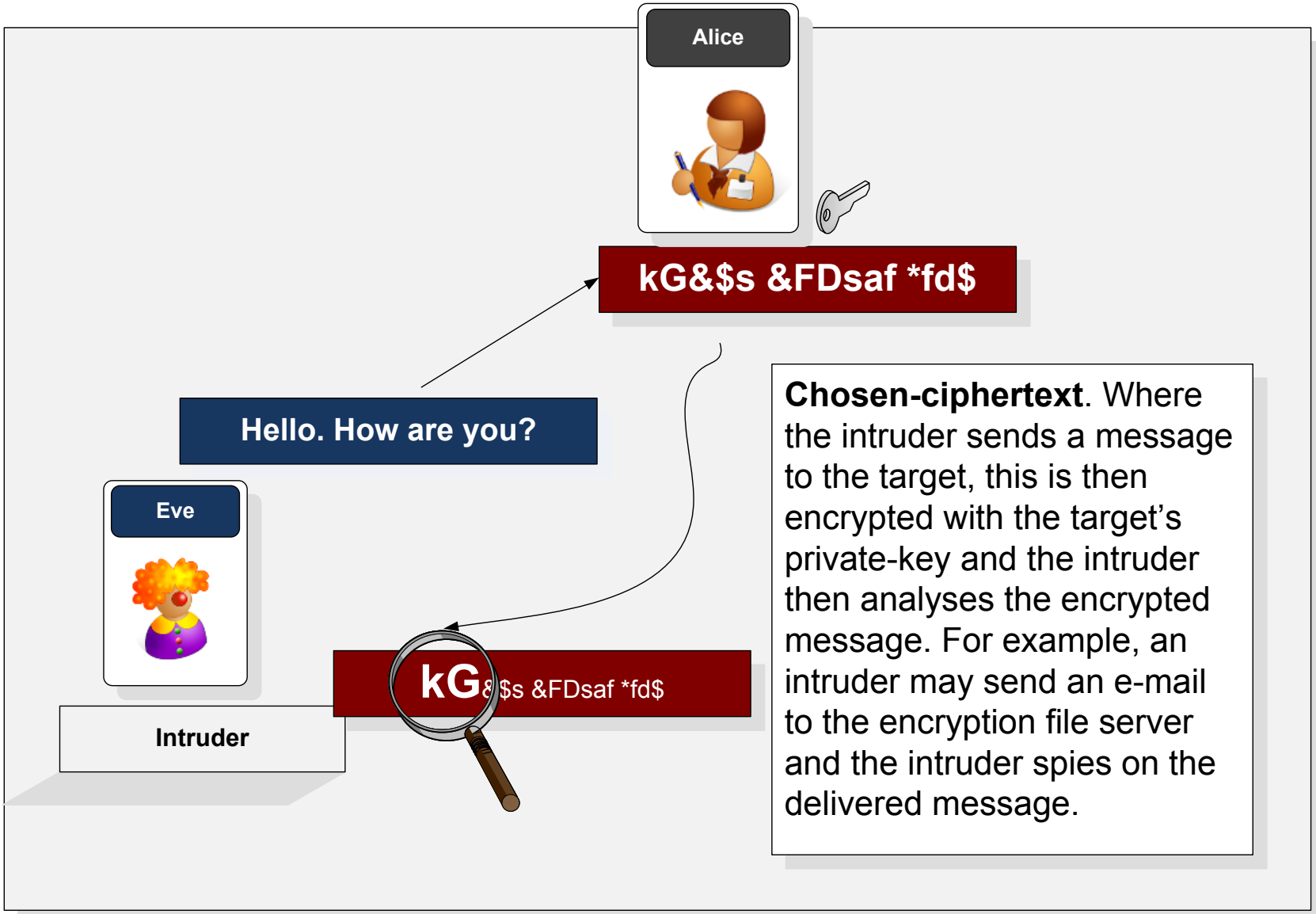
The replay system. Where the intruder takes a legitimate message and sends it into the network at some future time.

Author: Prof Bill Buchanan



Active attack. Where the intruder inserts or modifies messages.
Cut and paste. Where the intruder mixes parts of two different encrypted messages and, sometimes, is able to create a new message. This message is likely to make no sense, but may trick the receiver into doing something that helps the intruder.

Author: Prof Bill Buchanan



Chosen-ciphertext. Where the intruder sends a message to the target, this is then encrypted with the target's private-key and the intruder then analyses the encrypted message. For example, an intruder may send an e-mail to the encryption file server and the intruder spies on the delivered message.

Author: Prof Bill Buchanan