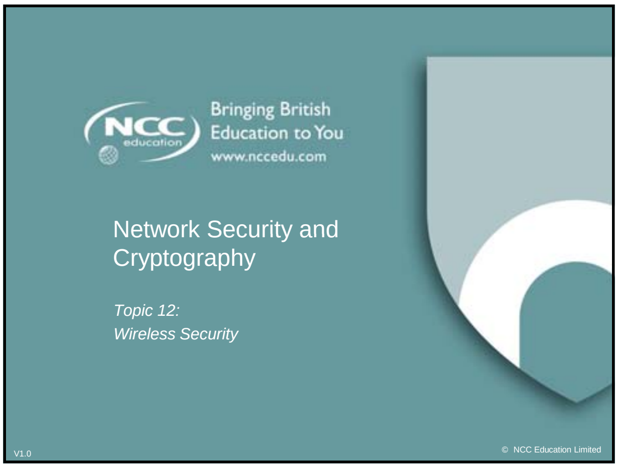
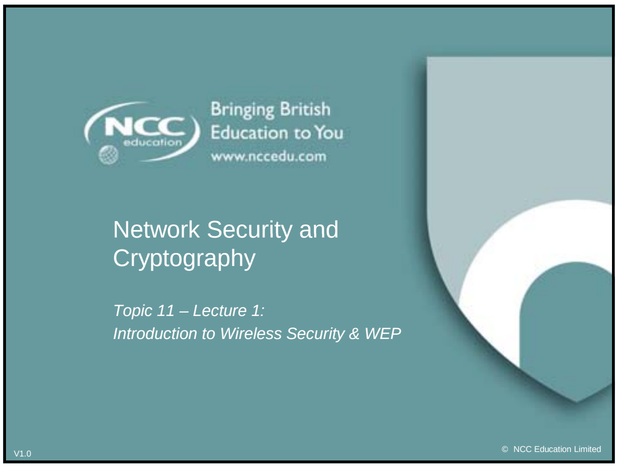


Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 12:
Wireless Security

V1.0

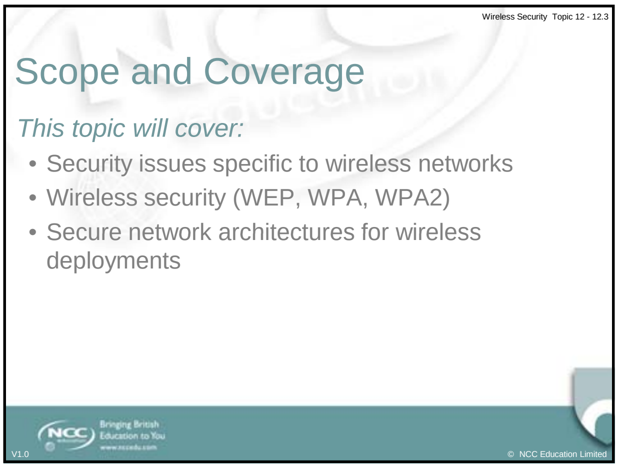


Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 11 – Lecture 1:
Introduction to Wireless Security & WEP

V1.0



Wireless Security Topic 12 - 12.3

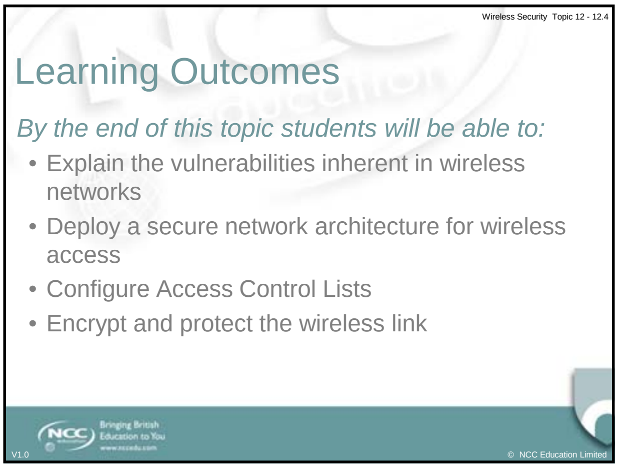
Scope and Coverage

This topic will cover:

- Security issues specific to wireless networks
- Wireless security (WEP, WPA, WPA2)
- Secure network architectures for wireless deployments

Bringing British Education to You
www.nccedu.com

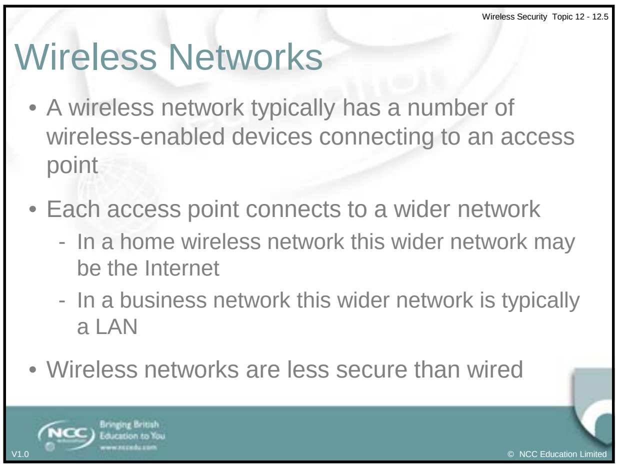
V1.0



Learning Outcomes

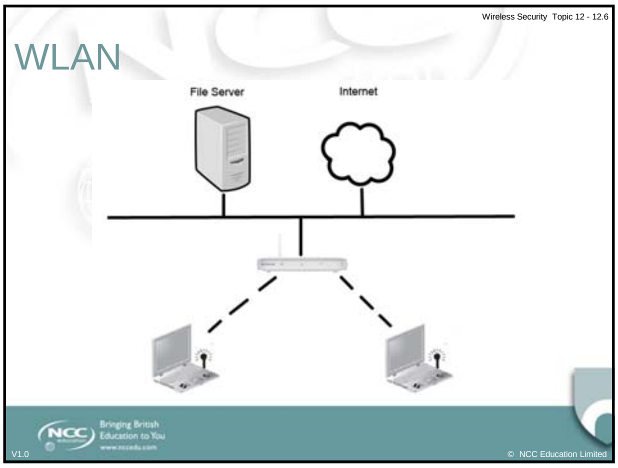
By the end of this topic students will be able to:

- Explain the vulnerabilities inherent in wireless networks
- Deploy a secure network architecture for wireless access
- Configure Access Control Lists
- Encrypt and protect the wireless link

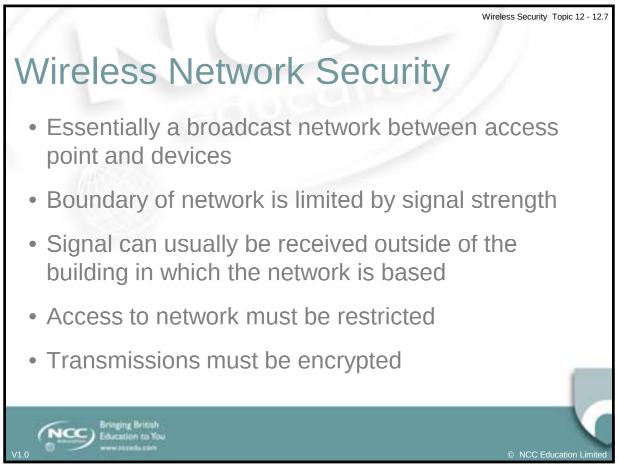


Wireless Networks

- A wireless network typically has a number of wireless-enabled devices connecting to an access point
- Each access point connects to a wider network
  - In a home wireless network this wider network may be the Internet
  - In a business network this wider network is typically a LAN
- Wireless networks are less secure than wired



WLAN

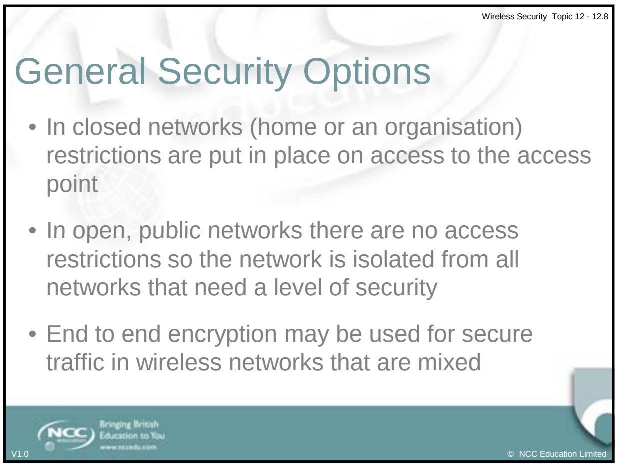


Wireless Security Topic 12 - 12.7

Wireless Network Security

- Essentially a broadcast network between access point and devices
- Boundary of network is limited by signal strength
- Signal can usually be received outside of the building in which the network is based
- Access to network must be restricted
- Transmissions must be encrypted

V1.0 © NCC Education Limited

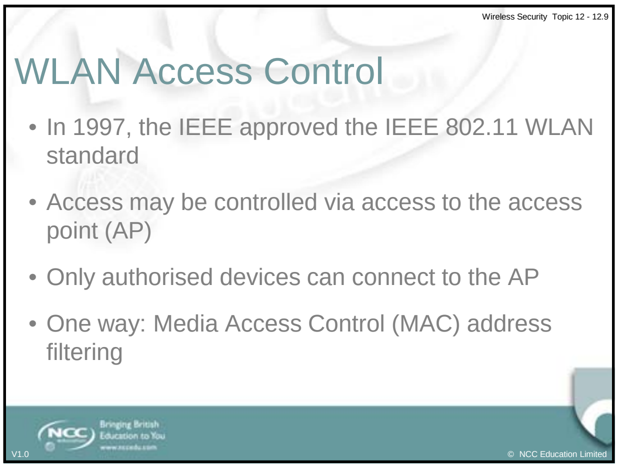


Wireless Security Topic 12 - 12.8

General Security Options

- In closed networks (home or an organisation) restrictions are put in place on access to the access point
- In open, public networks there are no access restrictions so the network is isolated from all networks that need a level of security
- End to end encryption may be used for secure traffic in wireless networks that are mixed

V1.0 © NCC Education Limited



Wireless Security Topic 12 - 12.9

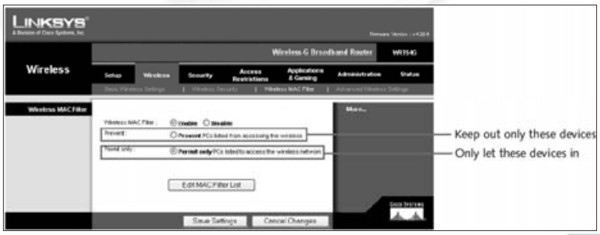
WLAN Access Control

- In 1997, the IEEE approved the IEEE 802.11 WLAN standard
- Access may be controlled via access to the access point (AP)
- Only authorised devices can connect to the AP
- One way: Media Access Control (MAC) address filtering

V1.0 © NCC Education Limited

MAC Address Filtering

- Usually implemented to permit rather than prevent



Wireless MAC Filter : ● Enable ○ Disable

Prevent : ○ Prevent PCs listed from accessing the wireless — Keep out only these devices

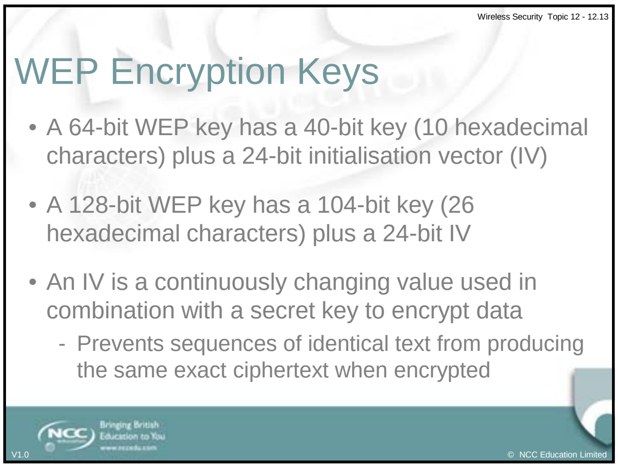
Permit only : ● Permit only PCs listed to access the wireless network — Only let these devices in

Wired Equivalent Privacy (WEP)

- Original security component of 802.11
- Aim: only authorized parties can view transmitted wireless information
- Uses encryption to protect traffic
- Designed as an efficient and reasonably strong security
- Has numerous security flaws and has been superseded by Wi-Fi Protected Access (WPA)

WEP Encryption

- Uses the RC4 stream cipher for confidentiality
- Uses the CRC-32 checksum for integrity
- Secret keys can be 64 or 128 bits long
  - Some vendors do supply 256-bit key version
- Can hold up to four shared secret keys
  - One key is designated as the default key
- Key size is one of the security limitations in WEP

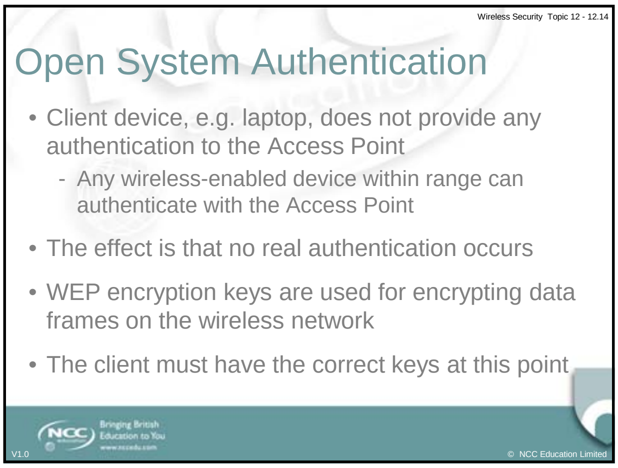


Wireless Security Topic 12 - 12.13

WEP Encryption Keys

- A 64-bit WEP key has a 40-bit key (10 hexadecimal characters) plus a 24-bit initialisation vector (IV)
- A 128-bit WEP key has a 104-bit key (26 hexadecimal characters) plus a 24-bit IV
- An IV is a continuously changing value used in combination with a secret key to encrypt data
  - Prevents sequences of identical text from producing the same exact ciphertext when encrypted

V1.0 © NCC Education Limited

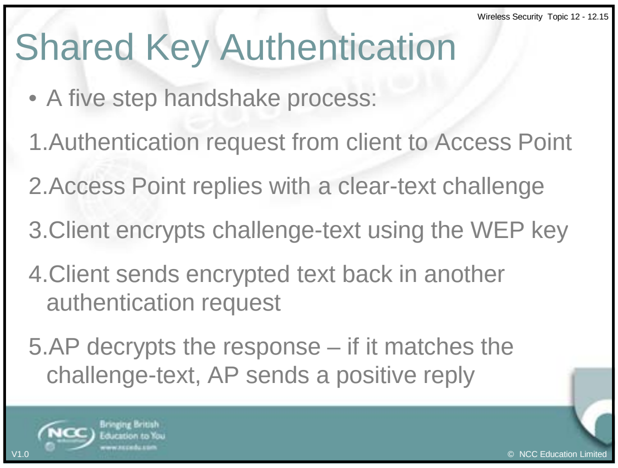


Wireless Security Topic 12 - 12.14

Open System Authentication

- Client device, e.g. laptop, does not provide any authentication to the Access Point
  - Any wireless-enabled device within range can authenticate with the Access Point
- The effect is that no real authentication occurs
- WEP encryption keys are used for encrypting data frames on the wireless network
- The client must have the correct keys at this point

V1.0 © NCC Education Limited



Wireless Security Topic 12 - 12.15

Shared Key Authentication

- A five step handshake process:

1.Authentication request from client to Access Point

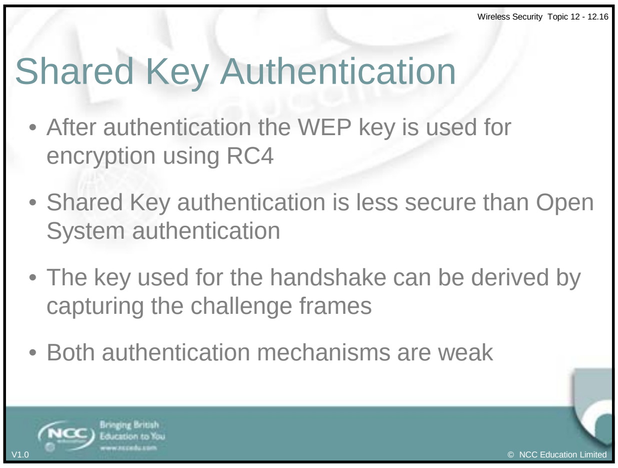
2.Access Point replies with a clear-text challenge

3.Client encrypts challenge-text using the WEP key

4.Client sends encrypted text back in another authentication request

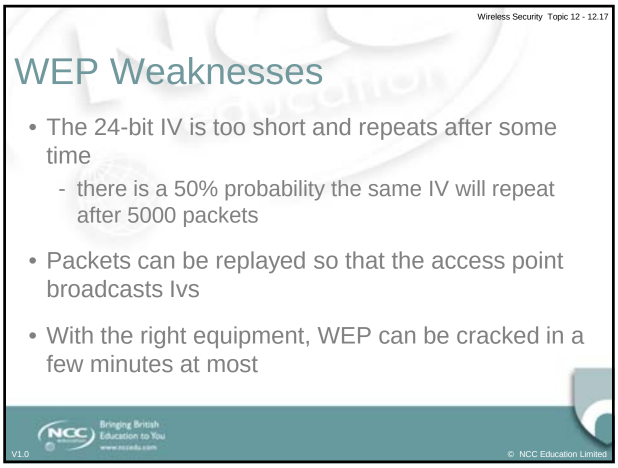
5.AP decrypts the response – if it matches the challenge-text, AP sends a positive reply

V1.0 © NCC Education Limited



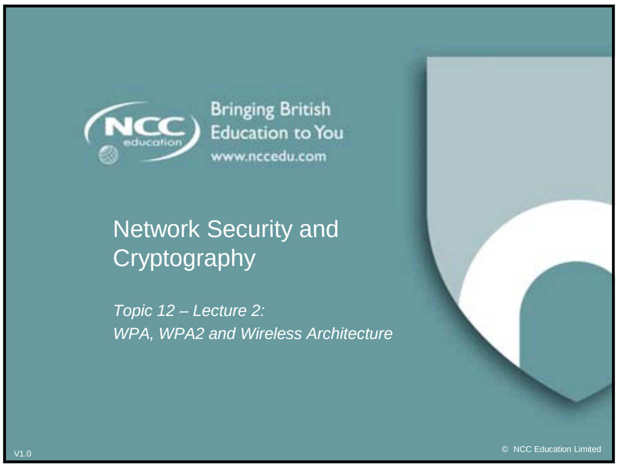
Shared Key Authentication

- After authentication the WEP key is used for encryption using RC4
- Shared Key authentication is less secure than Open System authentication
- The key used for the handshake can be derived by capturing the challenge frames
- Both authentication mechanisms are weak



WEP Weaknesses

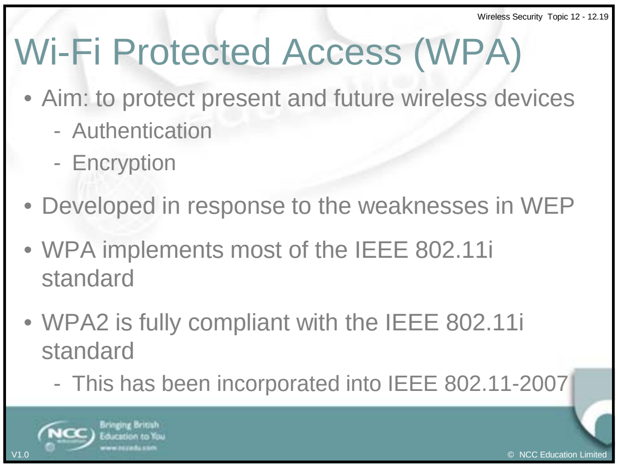
- The 24-bit IV is too short and repeats after some time
  - there is a 50% probability the same IV will repeat after 5000 packets
- Packets can be replayed so that the access point broadcasts Ivs
- With the right equipment, WEP can be cracked in a few minutes at most



Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 12 – Lecture 2:
WPA, WPA2 and Wireless Architecture

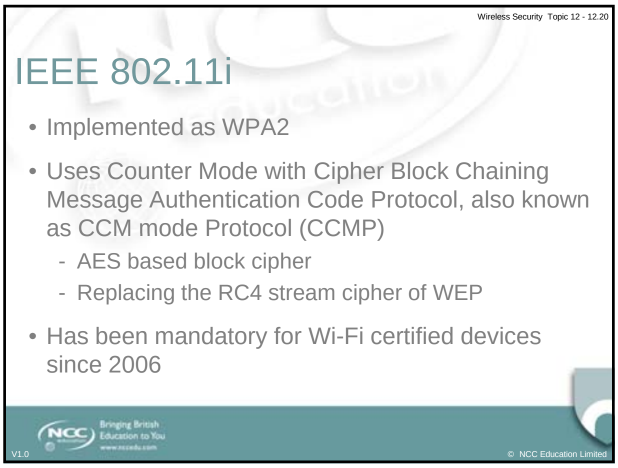


Wireless Security Topic 12 - 12.19

Wi-Fi Protected Access (WPA)

- Aim: to protect present and future wireless devices
  - Authentication
  - Encryption
- Developed in response to the weaknesses in WEP
- WPA implements most of the IEEE 802.11i standard
- WPA2 is fully compliant with the IEEE 802.11i standard
  - This has been incorporated into IEEE 802.11-2007

V1.0

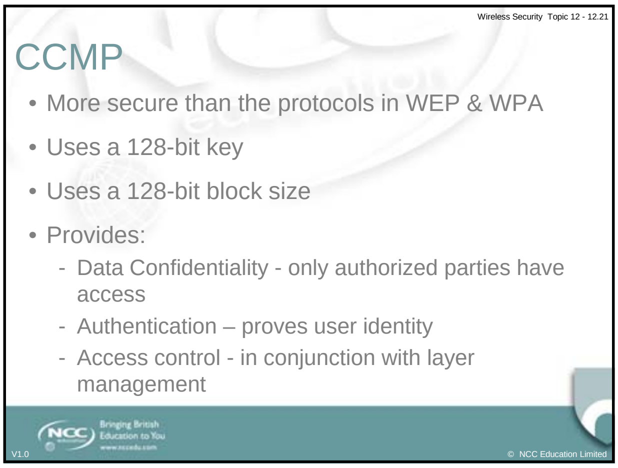


Wireless Security Topic 12 - 12.20

IEEE 802.11i

- Implemented as WPA2
- Uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, also known as CCM mode Protocol (CCMP)
  - AES based block cipher
  - Replacing the RC4 stream cipher of WEP
- Has been mandatory for Wi-Fi certified devices since 2006

V1.0

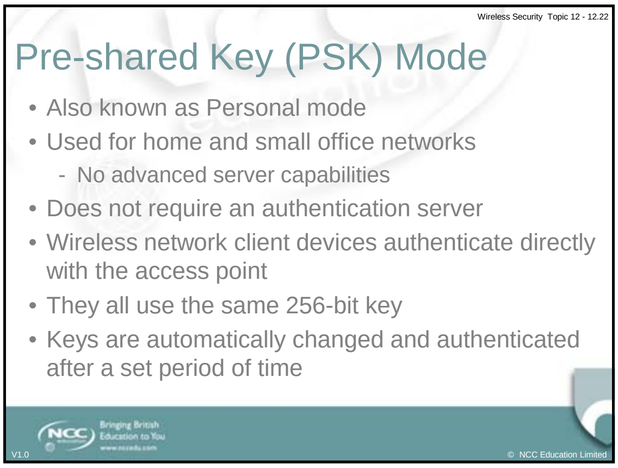


Wireless Security Topic 12 - 12.21

CCMP

- More secure than the protocols in WEP & WPA
- Uses a 128-bit key
- Uses a 128-bit block size
- Provides:
  - Data Confidentiality - only authorized parties have access
  - Authentication – proves user identity
  - Access control - in conjunction with layer management

V1.0

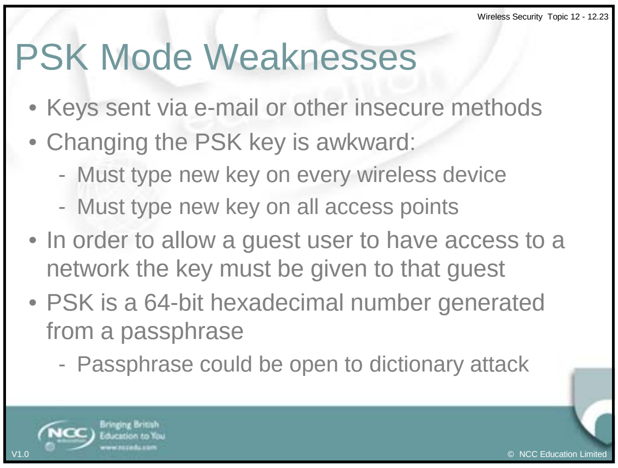


Wireless Security Topic 12 - 12.22

Pre-shared Key (PSK) Mode

- Also known as Personal mode
- Used for home and small office networks
  - No advanced server capabilities
- Does not require an authentication server
- Wireless network client devices authenticate directly with the access point
- They all use the same 256-bit key
- Keys are automatically changed and authenticated after a set period of time

V1.0 © NCC Education Limited

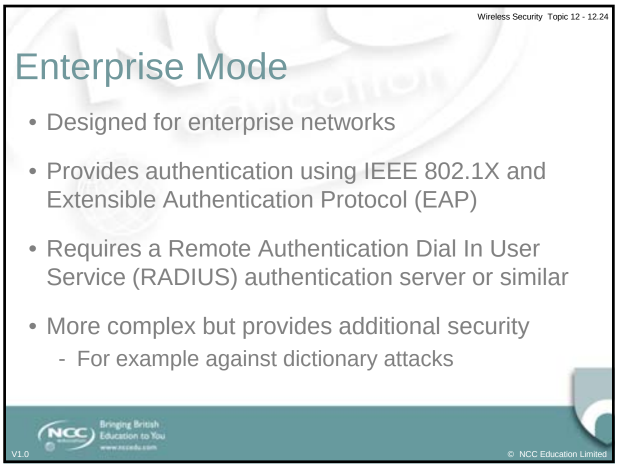


Wireless Security Topic 12 - 12.23

PSK Mode Weaknesses

- Keys sent via e-mail or other insecure methods
- Changing the PSK key is awkward:
  - Must type new key on every wireless device
  - Must type new key on all access points
- In order to allow a guest user to have access to a network the key must be given to that guest
- PSK is a 64-bit hexadecimal number generated from a passphrase
  - Passphrase could be open to dictionary attack

V1.0 © NCC Education Limited

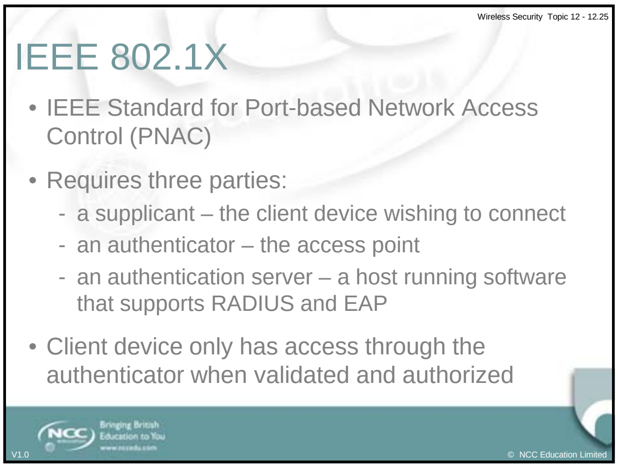


Wireless Security Topic 12 - 12.24

Enterprise Mode

- Designed for enterprise networks
- Provides authentication using IEEE 802.1X and Extensible Authentication Protocol (EAP)
- Requires a Remote Authentication Dial In User Service (RADIUS) authentication server or similar
- More complex but provides additional security
  - For example against dictionary attacks

V1.0 © NCC Education Limited

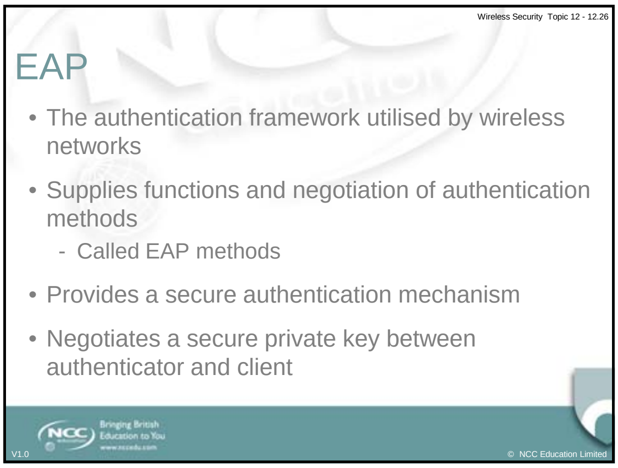


Wireless Security Topic 12 - 12.25

IEEE 802.1X

- IEEE Standard for Port-based Network Access Control (PNAC)
- Requires three parties:
  - a supplicant – the client device wishing to connect
  - an authenticator – the access point
  - an authentication server – a host running software that supports RADIUS and EAP
- Client device only has access through the authenticator when validated and authorized

V1.0 © NCC Education Limited

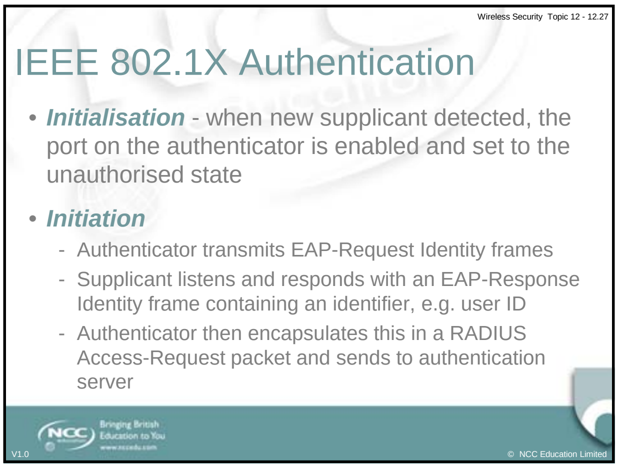


Wireless Security Topic 12 - 12.26

EAP

- The authentication framework utilised by wireless networks
- Supplies functions and negotiation of authentication methods
  - Called EAP methods
- Provides a secure authentication mechanism
- Negotiates a secure private key between authenticator and client

V1.0 © NCC Education Limited

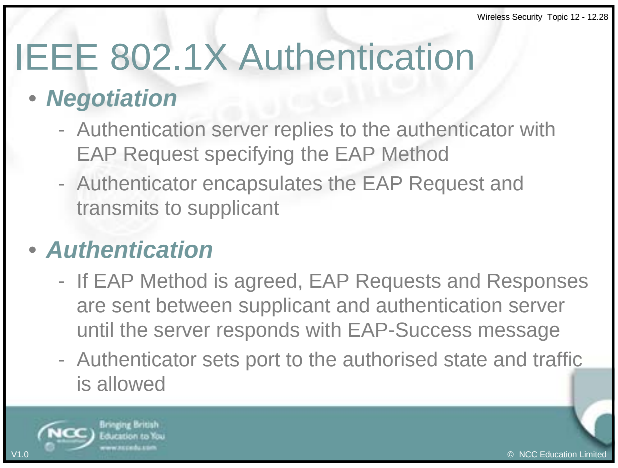


Wireless Security Topic 12 - 12.27

IEEE 802.1X Authentication

- ***Initialisation*** - when new supplicant detected, the port on the authenticator is enabled and set to the unauthorised state
- ***Initiation***
  - Authenticator transmits EAP-Request Identity frames
  - Supplicant listens and responds with an EAP-Response Identity frame containing an identifier, e.g. user ID
  - Authenticator then encapsulates this in a RADIUS Access-Request packet and sends to authentication server

V1.0 © NCC Education Limited

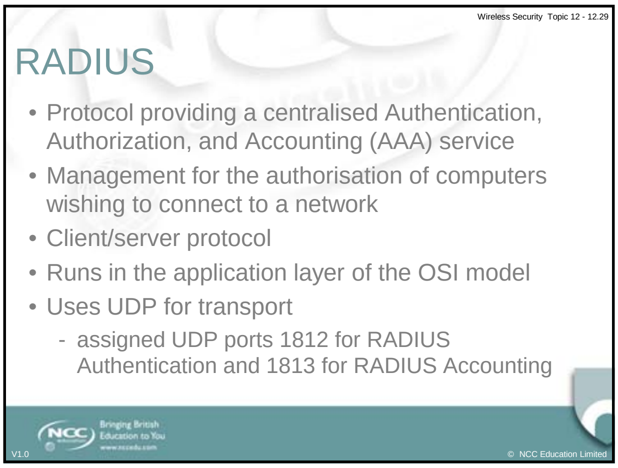


Wireless Security Topic 12 - 12.28

IEEE 802.1X Authentication

- ***Negotiation***
  - Authentication server replies to the authenticator with EAP Request specifying the EAP Method
  - Authenticator encapsulates the EAP Request and transmits to supplicant
- ***Authentication***
  - If EAP Method is agreed, EAP Requests and Responses are sent between supplicant and authentication server until the server responds with EAP-Success message
  - Authenticator sets port to the authorised state and traffic is allowed

V1.0 © NCC Education Limited

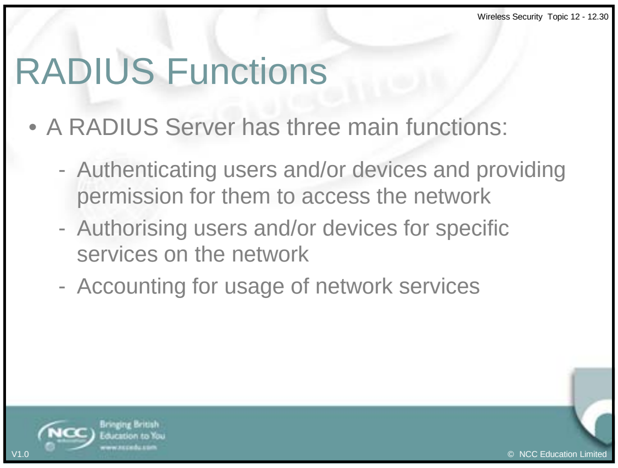


Wireless Security Topic 12 - 12.29

RADIUS

- Protocol providing a centralised Authentication, Authorization, and Accounting (AAA) service
- Management for the authorisation of computers wishing to connect to a network
- Client/server protocol
- Runs in the application layer of the OSI model
- Uses UDP for transport
  - assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting

V1.0 © NCC Education Limited

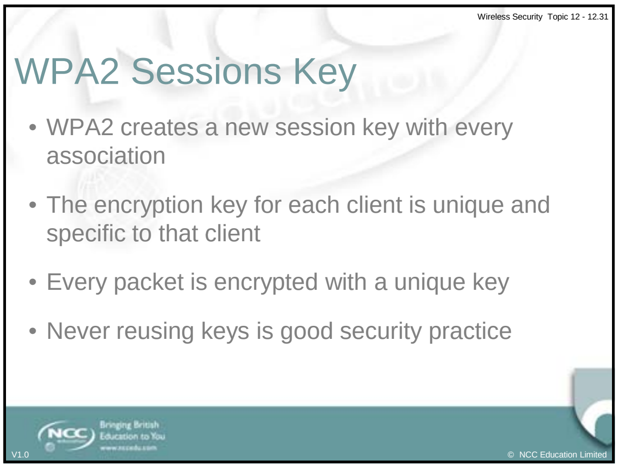


Wireless Security Topic 12 - 12.30

RADIUS Functions

- A RADIUS Server has three main functions:
  - Authenticating users and/or devices and providing permission for them to access the network
  - Authorising users and/or devices for specific services on the network
  - Accounting for usage of network services

V1.0 © NCC Education Limited

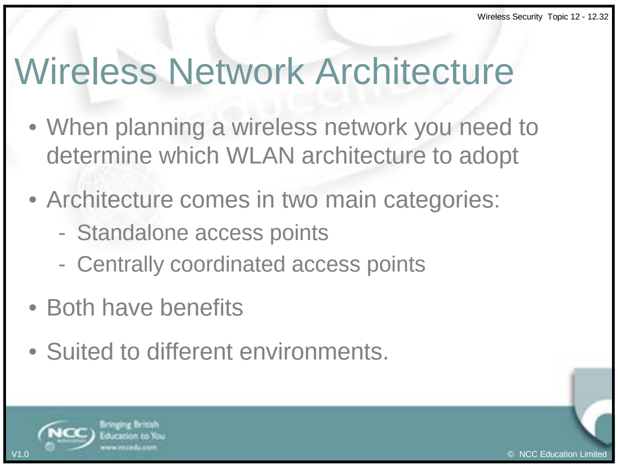


Wireless Security Topic 12 - 12.31

WPA2 Sessions Key

- WPA2 creates a new session key with every association
- The encryption key for each client is unique and specific to that client
- Every packet is encrypted with a unique key
- Never reusing keys is good security practice

V1.0 © NCC Education Limited

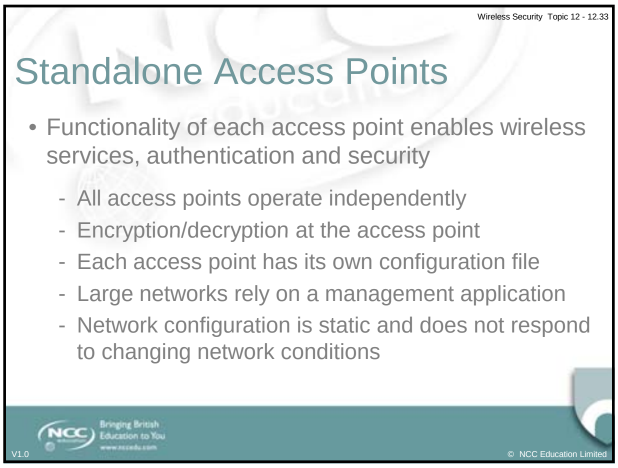


Wireless Security Topic 12 - 12.32

Wireless Network Architecture

- When planning a wireless network you need to determine which WLAN architecture to adopt
- Architecture comes in two main categories:
  - Standalone access points
  - Centrally coordinated access points
- Both have benefits
- Suited to different environments.

V1.0 © NCC Education Limited

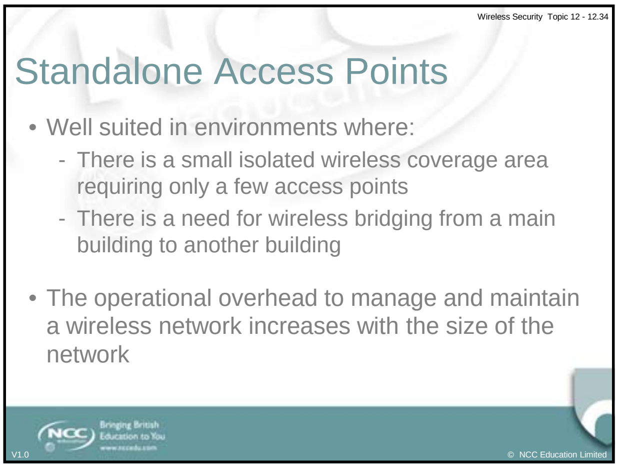


Wireless Security Topic 12 - 12.33

Standalone Access Points

- Functionality of each access point enables wireless services, authentication and security
  - All access points operate independently
  - Encryption/decryption at the access point
  - Each access point has its own configuration file
  - Large networks rely on a management application
  - Network configuration is static and does not respond to changing network conditions

V1.0 © NCC Education Limited



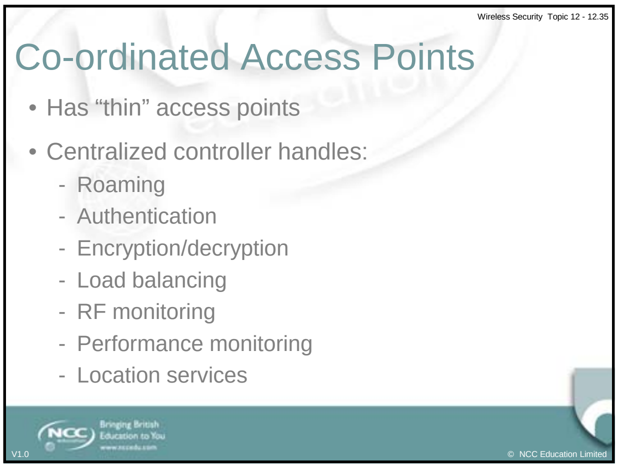
Wireless Security Topic 12 - 12.34

Standalone Access Points

- Well suited in environments where:
  - There is a small isolated wireless coverage area requiring only a few access points
  - There is a need for wireless bridging from a main building to another building
- The operational overhead to manage and maintain a wireless network increases with the size of the network

V1.0

© NCC Education Limited



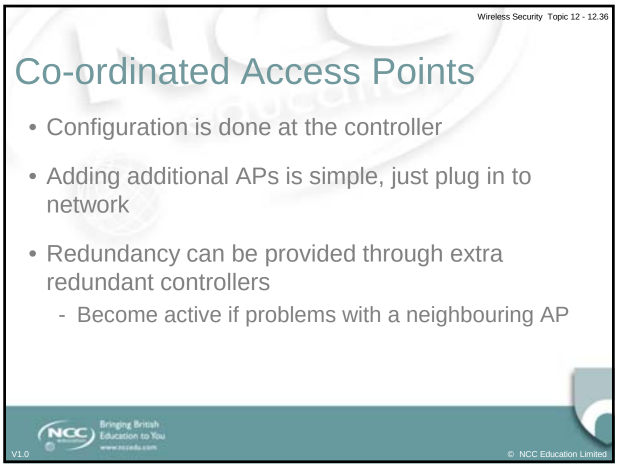
Wireless Security Topic 12 - 12.35

Co-ordinated Access Points

- Has “thin” access points
- Centralized controller handles:
  - Roaming
  - Authentication
  - Encryption/decryption
  - Load balancing
  - RF monitoring
  - Performance monitoring
  - Location services

V1.0

© NCC Education Limited



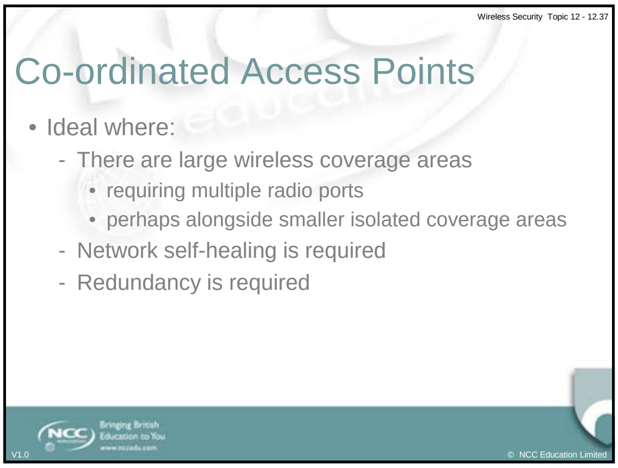
Wireless Security Topic 12 - 12.36

Co-ordinated Access Points

- Configuration is done at the controller
- Adding additional APs is simple, just plug in to network
- Redundancy can be provided through extra redundant controllers
  - Become active if problems with a neighbouring AP

V1.0

© NCC Education Limited

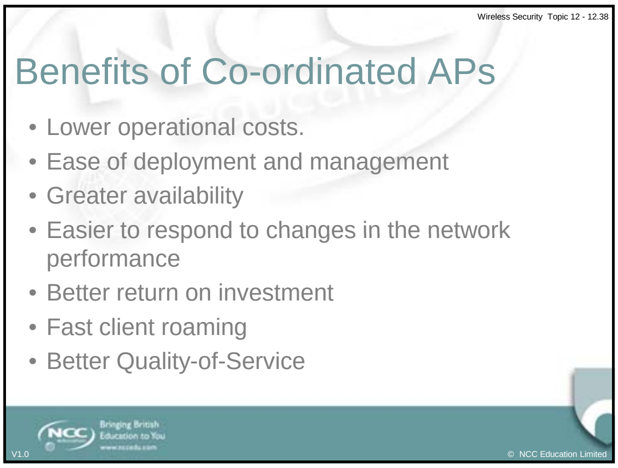


Wireless Security Topic 12 - 12.37

Co-ordinated Access Points

- Ideal where:
  - There are large wireless coverage areas
    - requiring multiple radio ports
    - perhaps alongside smaller isolated coverage areas
  - Network self-healing is required
  - Redundancy is required

V1.0 © NCC Education Limited

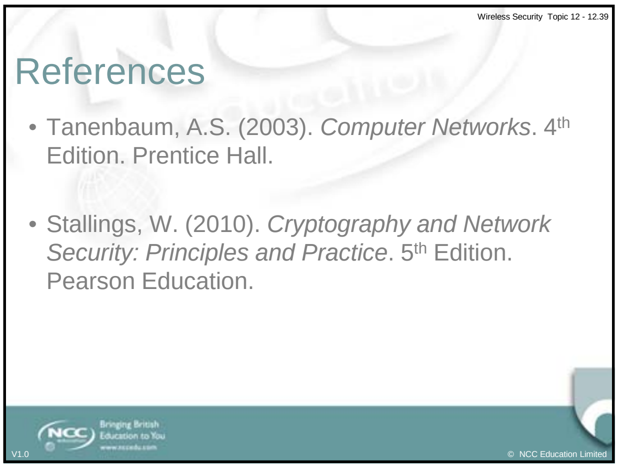


Wireless Security Topic 12 - 12.38

Benefits of Co-ordinated APs

- Lower operational costs.
- Ease of deployment and management
- Greater availability
- Easier to respond to changes in the network performance
- Better return on investment
- Fast client roaming
- Better Quality-of-Service

V1.0 © NCC Education Limited



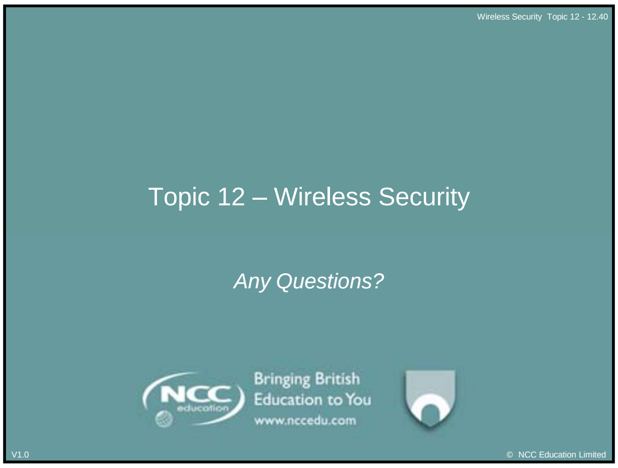
Wireless Security Topic 12 - 12.39

References

- Tanenbaum, A.S. (2003). *Computer Networks*. 4th Edition. Prentice Hall.

- Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. 5th Edition. Pearson Education.

V1.0 © NCC Education Limited



Wireless Security Topic 12 - 12.40

Topic 12 – Wireless Security

Any Questions?

Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited