WIRELESS ACCESS POINT SECURITY

Data Security

Lecturer: Mark Gillan

ACCESS ADMIN CONSOLE

To change settings, you must login directly to the router or Wireless Access Point (WAP) firmware.

The Gateway IP: Routers use a default local IP address on the network subnet. The standard address is usually **192.168.1.1** or 192.168.0.1.

Web Browser Access: Connect a laptop/PC via Wi-Fi or Ethernet cable, open any browser, and enter http://192.168.1.1 in the address bar.

Initial Login: Secure routers prompt you with a login screen requesting default administrative credentials (often found on a physical label on the router base).

DEMYSTIFYING SSID CONFIGURATIONS

What is an SSID ?

SSID stands for **Service Set Identifier**. It is simply the user-friendly text name of your wireless network.

Default names contain the ISP brand (e.g., *Sky-WiFi-87B*or *VirginMedia-526*).

Default names tell attackers what hardware/ISP you use, making target discovery easier.

SSID Broadcasting

By default, routers broadcast their SSID so clients can discover and connect to them easily.

Hiding the SSID: Turning this off stops the router from public beaconing.

Note: it can help, but attackers can sniff SSID names from packet handshakes using monitoring software. Changing the SSID name remains beneficial though.

CRITICAL ACCESS SAFEGUARD

Admin Login Key vs. WiFi Security Key

Many beginners confuse the **Wi-Fi connection password** with the **Router Administration Password**. They are completely separate security layers!

The Admin Danger: Default passwords like *admin*, *password*, or blank are globally documented. If an intruder connects, they can easily assume complete control.

Remediation Step: Immediately change the router's administrator password to a custom, long, secure passphrase. Disable "Remote Management" over the WAN.

WIRELESS BANDS & CHANNELS

WiFi Frequency Bands

Band / WiFi version	2.4 GHz	5 GHz
802.11b	√	
802.11g	√	
802.11n	√	√

Wireless networks transmit data using high-frequency radio waves.

To organize this traffic, routers use distinct frequency bands and channels.

2.4 GHz Band: Longer range, better wall penetration, but slower speeds and highly congested (only 3 non-overlapping channels: 1, 6, 11).

5 GHz Band: Extremely fast data rates, less interference, but has a shorter range and struggles to penetrate solid brick walls.

COMPARING SECURITY ENCRYPTION

WEP (Wired Equivalent Privacy) uses vulnerable cyclic redundancy checks and can be cracked in minutes.

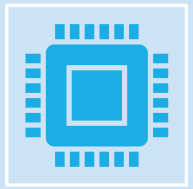
WPA3 introduces **Simultaneous Authentication of Equals (SAE)**, providing heavy immunity against dictionary/offline attacks.

**** Always configure WPA3 or WPA2-AES! ****

IP ADDRESSES VERSUS MAC ADDRESSES

Every device on a wireless network needs two distinct addresses to communicate properly.

IP Address (Logical): Assigned dynamically by the router (DHCP). Represents the device's current location on the network (e.g., 192.168.1.50). Subject to change.



MAC Address (Physical): A unique, 48-bit hexadecimal identifier hardcoded into the network interface card (NIC) by the manufacturer (e.g., A0:B1:C2:3D:4E:5F). It never changes.

GUEST NETWORK

Network Isolation

Creates a secondary broadcast domain. Guest users can access the Internet, but they are fully blocked from viewing primary network files, NAS drives, or printers.

Port Control Rules

Enforces strict access rules by blocking non-essential ports. Guests should only access basic web services, avoiding secure local transfer ports.

Threat Containment

Prevents cross-infection. If a friend's device is infected with network-propagating ransomware, isolation protects your critical devices from exposure.

GUEST NETWORK RESTRICTING PORT ACCESS

Port Number	Protocol	Service Description	Recommended Guest Policy	Security Rationale
80 / 443	TCP	HTTP / HTTPS (Web Browsing)	Allow	Essential for loading modern web pages.
21	TCP	FTP (File Transfer Protocol)	Block	Prevents massive bandwidth usage and unencrypted data transfers.
22	TCP	SSH (Secure Shell Administration)	Block	Blocks remote command-line access to local servers or routers.
23	TCP	Telnet (Legacy Admin Tool)	Block	Completely unencrypted text. Massive security risk.
25 / 110	TCP	SMTP / POP3 (Unencrypted Mail)	Block	Mitigates spam relays and protects sensitive plaintext credentials.

FIREWALL

A firewall is a key security precaution designed to monitor and control network traffic.

Traffic Monitoring: Inspects packets of information crossing the network boundary, checking their source, destination, and payload details.

Access Prevention: SQA Level 5 fundamentals stress that firewalls prevent unauthorized access to systems from hackers, rather than serving as standard antivirus software.

Rule Enforcement: Operates based on strict predefined security rules (opening/closing specific ports, filtering IP addresses and websites).

HARDWARE FIREWALLS

A physical network security device deployed at the network perimeter.

Network Boundary: Sits directly between the local private network and the external Internet connection (ISP gateway).

Blanket Protection: Safeguards every single connected client device (PC, tablet, IoT, server) simultaneously without requiring individual device configuration.

Dedicated Processing: Has its own internal CPU and RAM. Packet filtering does not consume host system resources or cause local performance slowdowns.

This Photo by Unknown Author is licensed under CC BY

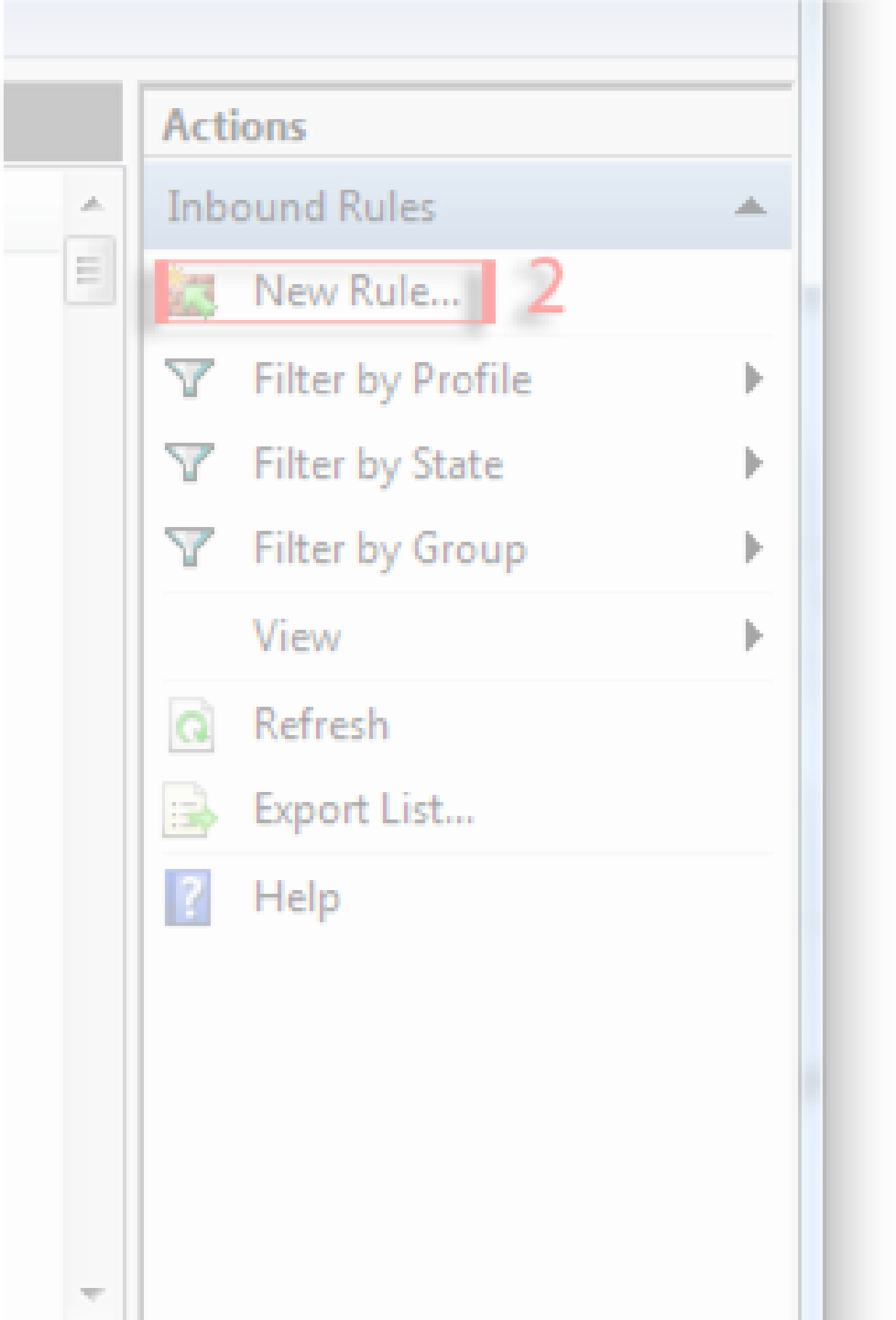
SOFTWARE FIREWALLS

An operating system program protecting a single host device.

Host-Based Security: Installed directly onto individual machines (such as Windows Defender Firewall or macOS Packet Filter) to protect only that specific operating system.

Application Control: Can analyse which specific programs on the machine are attempting to send or receive data, blocking rouge software.

Portable Defence: Keeps protecting laptops and mobile phones even when connecting to unsafe, untrusted external public Wi-Fi networks.



FIREWALL MAC FILTERING RULES

White-Listing (Default DENY - Allow List)

The firewall **BLOCKS ALL** wireless devices except those explicitly registered on the list.

Highly secure: Unlisted devices are instantly refused.

High maintenance: You must manually register every new phone, guest device, or computer.

Black-Listing (Default ALLOW - Deny List)

The firewall **ALLOWS ALL** wireless devices to connect **except** those specifically specified on the block list.

Easy setup: Useful for blocking a known intruder or limiting children's device hours.

Reactive: Offers no protection against new, unknown devices joining your network.

SECURE CONNECTION

Connecting devices securely demands a structured approach rather than raw convenience.

Avoid Open Networks: Unencrypted connections (no password) allow anyone to sniff your traffic using tools like Wireshark.

Disable WPS (Wi-Fi Protected Setup): WPS PINs are vulnerable to brute-force attacks and should be disabled in the router settings.

Use WPA3 Personal: Modern mobile devices automatically look for WPA3 capabilities. Always select this on client device configurations.

CONSIDER SECURITY ENHANCEMENT CHECKS

To help you all think about Hardware and Software changes that can be made to enhance security for Wireless Access Points / Routers

A few points to consider upon the next couple of slides…

HARDWARE

- **CHANGE SSID**: Hiding the SSID (this can cause problems with smart devices such as televisions to automatically locate the network). It means anyone connecting must type in the SSID (network identifier). Change the default name.
  However, hackers might use software that can locate the network anyway
- **DEFAULT PASSWORD:** Change default administrator username and passwords
- **LOCKS:** Physical access to computer equipment restricted and locks placed upon equipment, locating in the middle of the environment of use (to avoid signal spill outside)
- **FILTERING:** MAC address filtering and prohibiting and allocate static IP (Internet Protocol) addresses instead of using DHCP (Dynamic Host Configuration Protocol)
  Note: Hackers can manipulate DHCP to allocate themselves a network address
- **PORT RESTRICTIONS:** Inbound / Outbound port access restrictions (not allowing guests full access to all ports, for example, not allowing FTP or other connections)
- **FIREWALL RULES:** Changing and upgrading Firewall rules (monitoring, blocking certain traffic, changing what is allowed or not allowed for the Firewall)
- **Use a VPN** (Virtual Private Network) to add security and privacy. It replaces initially identifiable IP (Internet Protocol) address with a virtual one
- **Update** firmware for all hardware to latest available

SOFTWARE

- **Authentication:** such as password or PIN requirements for users or tokens for guests, also length of passwords with special characters
- **Activate Encryption** – WEP, WPA, WPA2, WPA3
  Care: WPS is old-fashioned and dangerous, it was designed to facilitate users who are not tech-savvy and make it easier for adding new devices to a network using a PIN or button push (making it easier is not ideal for security)
- **Logging and monitoring** activity
- **BLOCKING:** certain sites (**black list**) or blocking everything except for certain sites (**white list**)
- **Specialist security software:** scanning, surveying, analyse. This can include mobile phone apps.
- **Alert software:** for performance anomalies
- **Mobile Phone App:** Use app on mobile phone to turn off network access when not at home
- **UPDATING:** Purchase and update security software, also keep software up to date and free of known vulnerabilities

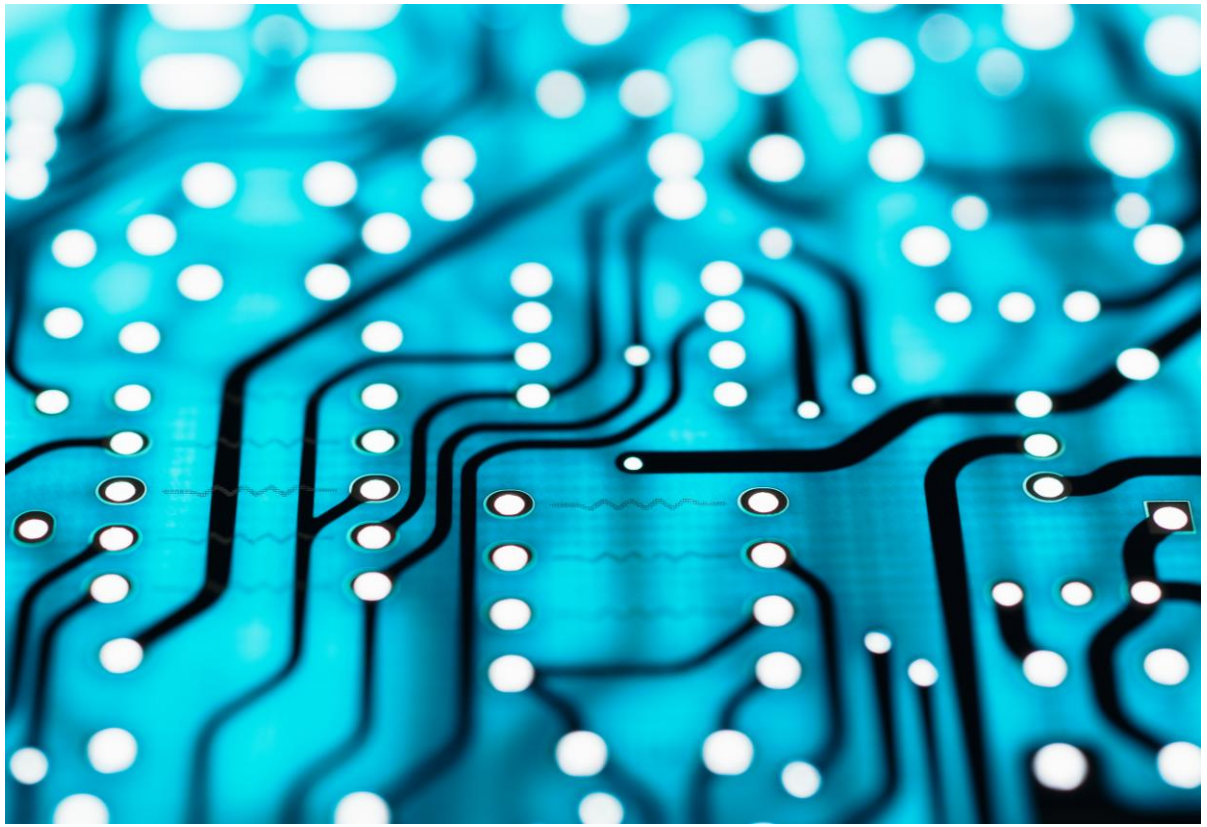
REVIEW AGAIN – KNOW THE LIST

Hardware

- Change SSID name
- Change Default Passwords
- Use Physical Barriers and Locks
- Firewall MAC Address Blocking / Filtering
- Port Restrictions for Guest Network
- Firewall Rules – Blacklist or Whitelisting
- VPN use
- Update Firmware on all devices

Software

- Password Authentication
- Activate Encryption
- Switch off Remote Management
- Logging and monitoring activity
- BLOCKING – Whitelisting or Blacklisting
- Specialist security software for scanning and monitoring
- Alert software for anomalies
- Mobile Phone App
- Update all software and maintain



IMPORTANT NOTE

Investigate and consider your own security.

Make a note of how your settings are prior to any changes and be sure of the changes you make.

Note, I or the college must not be held responsible for any changes or damage in relation to equipment outside of the college campus.

It would be advisable to note everything as working first and make a note on paper as to changes you might propose to enhance security.

The slides in this presentation are only advisory and any changes to your security must be your own responsibility - you take full responsibility therein.

KEEP STUDYING AND RESEARCHING

- Video: Access WiFi Router Settings
- Video: Protecting your Wifi from Hackers
- Video: Guest Wi-Fi and reasons for using
- Video: Protect your Wi-Fi (from Kaspersky)
- Video: 7 steps to Secure your Network
- Web page: NI Cyber Security Centre advice