Networks: Hardware Components

Unit 11: Cybersecurity and Incident Management

BTech Level 3

Table of Contents

Lesson Objectives

By the end of this session, you will be able to:

1. **Define** end user computing devices and explain their role in network architecture
2. **Describe** the various connectivity devices used in networks and their specific functions
3. **Evaluate** which connection media best suits different network scenarios
4. **Compare** the security implications of wired versus wireless connection media

Learning Outcomes

LO1: Understand the fundamental hardware components required to establish a functional network

LO2: Identify and explain the purpose of different connectivity devices within network infrastructures

LO3: Analyse the characteristics and applications of various connection media types

LO4: Evaluate and justify the selection of appropriate network hardware for specific scenarios

Introduction to Network Hardware

Time: 5 minutes

Three Primary Categories:

1. **End User Devices** - Interface between users and network
2. **Connectivity Devices** - Enable network communication
3. **Connection Media** - Physical/wireless data transmission pathways

Key Point: Each component represents both a functional necessity and a potential security vulnerability

> Proper hardware selection forms the foundation of effective network security

End User Computing Devices

Time: 8 minutes

Definition: Computing systems that individuals utilise to access network resources and services

Common End User Devices:

- **Desktop PCs** - Stationary systems with superior processing power
- **Laptop Computers** - Portable devices with integrated components
- **Workstations** - High-performance systems for specialised tasks

These devices serve as the interface between human users and network infrastructure

End User Device Connectivity

```
+------------------+     +------------------+     +------------------+
|   Wi-Fi (IEEE    |     |  Ethernet Cable  |     |    Bluetooth     |
|    802.11ax)     |     |   (Cat5e/Cat6)   |     |  (IEEE 802.15)   |
+------------------+     +------------------+     +------------------+
| Speed: Up to     |     | Speed: Up to     |     | Speed: Up to     |
| 9.6 Gbps         |     | 10 Gbps          |     | 50 Mbps          |
|                  |     |                  |     |                  |
| Range: 30-50m    |     | Range: 100m      |     | Range: 10-100m   |
|                  |     |                  |     |                  |
| Security: WPA3   |     | Security: High   |     | Security: Medium |
| Moderate-High    |     | (Physical)       |     | (Limited range)  |
+------------------+     +------------------+     +------------------+
```

Selection factors: Bandwidth requirements, mobility needs, security considerations

Network Switches

Time: 12 minutes

Function: Connect multiple devices within a LAN and intelligently forward data packets

Operation: Layer 2 (Data Link Layer) of OSI model

```
Network Switch Architecture:

         [Port 1] ---- PC 1 (MAC: AA:BB:CC:DD:EE:01)
         [Port 2] ---- PC 2 (MAC: AA:BB:CC:DD:EE:02)
[Switch] [Port 3] ---- PC 3 (MAC: AA:BB:CC:DD:EE:03)
         [Port 4] ---- Server (MAC: AA:BB:CC:DD:EE:04)
         [Port 5] ---- Printer (MAC: AA:BB:CC:DD:EE:05)
```

Key Feature: Maintains MAC address table mapping devices to specific ports

Switch Types and Features

Unmanaged Switches

- Basic plug-and-play devices - Suitable for small networks - Minimal configuration

Managed Switches

- VLAN support - Quality of Service (QoS) - Security features (port security, ACLs)

Layer 3 Switches

- Combine switching and routing - Enable inter-VLAN routing - Improved network segmentation

Network Routers - Router Network Topology

Function: Forward data packets between different networks

Operation: Layer 3 (Network Layer) - uses IP addresses

```
LAN 1 (192.168.1.0/24)          LAN 2 (192.168.2.0/24)
       |                              |
  [Switch 1]                     [Switch 2]
       |                              |
+------+------+                +------+------+
|   Router 1  |----------------|   Router 2  |
+-------------+                +-------------+
       |                              |
    [WAN]                          [WAN]
       |                              |
+-------------+                       |
|  Internet   |<----------------------+
|   (ISP)     |
+-------------+
```

Routing Protocols

Static Routing

- Manually configured routes
- Suitable for small, stable networks

Dynamic Routing

- Automated route discovery
- Protocols: OSPF, BGP
- Adapts to network changes

Default Gateway

- Router serves as default path for external traffic
- Essential for Internet connectivity

Wireless Access Points - Time: 10 minutes

Function: Extend network connectivity to wireless devices by creating WLANs

Configuration: Connect to wired infrastructure via Ethernet, broadcast wireless signals

```
Wireless Network Architecture:

                    Internet
                       |
                   [Router]
                       |
        +--------------+--------------+
        |                             |
    [Switch]                   [Access Point]
        |                      /    |    \
   [Wired PC]            [Laptop] [Phone] [Tablet]
```

Wireless Standards Evolution

```
+------------+------------+---------------+------------------+
| Standard   | Max Speed  | Frequency     | Year Introduced  |
+------------+------------+---------------+------------------+
| 802.11a    | 54 Mbps    | 5 GHz         | 1999            |
| 802.11b    | 11 Mbps    | 2.4 GHz       | 1999            |
| 802.11g    | 54 Mbps    | 2.4 GHz       | 2003            |
| 802.11n    | 600 Mbps   | 2.4/5 GHz     | 2009            |
| 802.11ac   | 3.5 Gbps   | 5 GHz         | 2014            |
| 802.11ax   | 9.6 Gbps   | 2.4/5/6 GHz   | 2019            |
+------------+------------+---------------+------------------+
```

Security Requirement: WPA3 encryption, strong authentication, regular updates

Modems

Function: Convert signals between different transmission media formats

Primary Role: Connect local networks to Internet Service Providers (ISPs)

Modem Types:

- **DSL Modems** - Utilise telephone lines
- **Cable Modems** - Leverage coaxial cable infrastructure
- **Fibre Modems (ONTs)** - Connect to fibre-optic networks (highest speeds)
- **Cellular Modems** - Use 4G/5G mobile networks

Note: Often integrated with routers in residential deployments

Multifunctional Network Devices

Time: 8 minutes

Modern Trend: Multiple functions combined into single physical device

Benefits:

- Reduced equipment costs
- Simplified management
- Decreased physical space requirements

Typical Home Router Integration:

Router + Switch + Wireless AP + Modem + Firewall + DHCP Server

Integrated Home Router Functions

```
+----------------------------------------------------------+
|                   Integrated Home Router                  |
|                                                          |
|  +----------+  +----------+  +--------------+  +------+ |
|  |  Modem   |--| Router   |--|   Switch     |--|DHCP  | |
|  | Function |  | Function |  | (4-8 ports)  |  |Server| |
|  +----------+  +----------+  +--------------+  +------+ |
|                     |                                    |
|                     |         +--------------+           |
|                     +---------| Access Point |           |
|                     |         | (Wi-Fi)      |           |
|                     |         +--------------+           |
|                     |                                    |
|                     |         +--------------+           |
|                     +---------| Firewall     |           |
|                               | (NAT/SPI)    |           |
|                               +--------------+           |
+----------------------------------------------------------+
```

Enterprise vs Consumer Equipment

Enterprise Networks:

- Dedicated, specialised devices for each function
- Higher performance and capacity
- Built-in redundancy and fault tolerance
- Centralised management capabilities - Higher initial cost, lower operational costs

Residential Networks:

- Integrated multifunctional devices
- Adequate performance for home use
- Single point of failure
- Consumer-friendly interfaces - Lower initial costs

Wired Connection Media

Time: 10 minutes

Ethernet Cables - Twisted Pair

Two primary variants:

Unshielded Twisted Pair (UTP)

- Most common and cost-effective
- Suitable for standard office environments

Shielded Twisted Pair (STP)

- Additional shielding against electromagnetic interference
- Used in electrically noisy environments

Structure: Pairs of insulated copper wires twisted together to reduce interference

Ethernet Cable Categories

Category	Maximum Speed	Maximum Distance	Typical Application
Cat5e	1 Gbps	100 metres	Standard office networks
Cat6	10 Gbps (55m) / 1 Gbps (100m)	100 metres	High-performance networks
Cat6a	10 Gbps	100 metres	Data centres, enterprise
Cat7	10 Gbps	100 metres	Specialised applications
Cat8	40 Gbps (30m)	30 metres	Data centre interconnections

Selection Criteria: Balance performance requirements against cost

Fibre Optic Cables

Technology: Transmit data as pulses of light through glass/plastic fibres

Advantages:

- **Speed:** 10 Gbps to 100+ Gbps
- **Distance:** Up to 100km+ without repeaters
- **Electromagnetic Immunity:** No interference from electrical sources
- **Security:** Difficult to tap without detection
- **Bandwidth:** Significantly higher than copper

Types:

- **Single-Mode Fibre (SMF)** - Long distances, laser light
- **Multi-Mode Fibre (MMF)** - Shorter distances, LED light

Wired Connection Security Benefits

Inherent Security Advantages:

1. **Physical Access Requirements**
    - Attackers need physical access to intercept data
2. **No Broadcast**
    - Data transmitted only between directly connected devices
3. **Predictable Topology**
    - Easier monitoring and control of connected devices
4. **Strong Physical Security**
    - Reduces reliance on encryption (though still recommended)

Wireless Technologies

Time: 10 minutes

Wi-Fi (IEEE 802.11) - **Latest Std.:** 802.11ax (Wi-Fi 6/6E) - up to 9.6 Gbps

Advantages:

- Mobility - users move freely whilst maintaining connectivity
- Reduced infrastructure costs
- Rapid deployment and expansion - Support for temporary and guest access

Disadvantages:

- Reduced security (broadcast signals)
- Potential interference
- Variable performance - Increased susceptibility to DoS attacks

Bluetooth Technology

Purpose: Short-range, low-power wireless connections for Personal Area Networks (PANs)

Characteristic	Specification
Range	10-100 metres (class dependent)
Speed	Up to 50 Mbps (Bluetooth 5.0)
Frequency	2.4 GHz ISM band
Power	Low (battery-powered devices)
Uses	Keyboards, mice, headphones, speakers, trackers

Key Point: Unsuitable for high-bandwidth or backbone connections

Li-Fi (Light Fidelity)

Emerging Technology: Data transmission using visible light from LED bulbs

Advantages:

- Exceptional speeds (theoretical maximum up to 224 Gbps)
- No radio frequency interference
- Enhanced security through light confinement - Uses existing lighting infrastructure

Challenges:

- Requires line of sight
- Cannot penetrate walls
- Dependent on active lighting
- Limited commercial availability - Evolving standardisation

Wireless Security Considerations

Key Threats:

1. **Eavesdropping** - Signals intercepted within range
2. **Unauthorised Access** - Attackers connect without proper authentication
3. **Rogue Access Points** - Deployed to intercept traffic
4. **Denial of Service** - Jamming and interference attacks

Security Mitigations:

- Implement WPA3 encryption
- Deploy 802.1X with RADIUS authentication
- Regular firmware updates - Periodic wireless security audits
- Network segmentation using VLANs - Continuous traffic monitoring

Comparative Analysis

Time: 7 minutes

Wired vs Wireless Comparison Matrix:

```
+------------------+------------------+------------------+
| Criterion        | Wired (Ethernet) | Wireless (Wi-Fi) |
+------------------+------------------+------------------+
| Speed            | Up to 100 Gbps   | Up to 9.6 Gbps   |
| Reliability      | Very High        | Moderate         |
| Security         | High             | Moderate         |
| Installation     | Complex          | Simple           |
| Cost             | Higher Initial   | Lower Initial    |
| Mobility         | None             | Excellent        |
| Range            | 100m per segment | 30-50m per AP    |
| Interference     | Minimal          | Susceptible      |
| Latency          | Very Low         | Low-Moderate     |
+------------------+------------------+------------------+
```

Key Concepts Summary

End User Devices

Computing systems (PCs, laptops, workstations) enabling human interaction with network resources

Connectivity Devices

- **Switches** - Connect devices within LANs (MAC addresses)
- **Routers** - Connect different networks (IP addresses)
- **Access Points** - Provide wireless connectivity
- **Modems** - Interface between network types

Connection Media

- **Wired** - Ethernet cables and fibre optics (high performance & security)
- **Wireless** - Wi-Fi, Bluetooth, Li-Fi (mobility & flexibility)

Security Implications

Wired Connections:

- Superior physical security
- Require physical access to intercept - Minimal broadcast exposure

Wireless Technologies:

- Convenience and mobility - Broadcast signals (interception risk)
- Require robust encryption and authentication

Essential Requirements:

- Proper security configuration
- Regular updates - Ongoing monitoring - Defence-in-depth strategies

Conclusion

Key Takeaways:

1. Network hardware components form the foundation of modern digital infrastructure
2. Understanding roles, characteristics, and applications enables effective network design
3. Balance required between:
    - Performance vs Cost - Security vs Convenience - Current capabilities vs Future scalability
4. Each hardware component represents both functional necessity and potential security vulnerability
5. Cybersecurity professionals must appreciate security implications of all hardware

Looking Forward

Future Considerations:

- Continued evolution of networking technology
- Multifunctional devices combining capabilities
- Emerging technologies (Li-Fi) reshaping connectivity
- Fundamental principles remain constant

Professional Responsibility:

- Understand security implications of each component
- Balance wired security/performance with wireless flexibility
- Make informed decisions as technology evolves

Remember: Foundation knowledge explored today enables future decision-making in evolving network environments