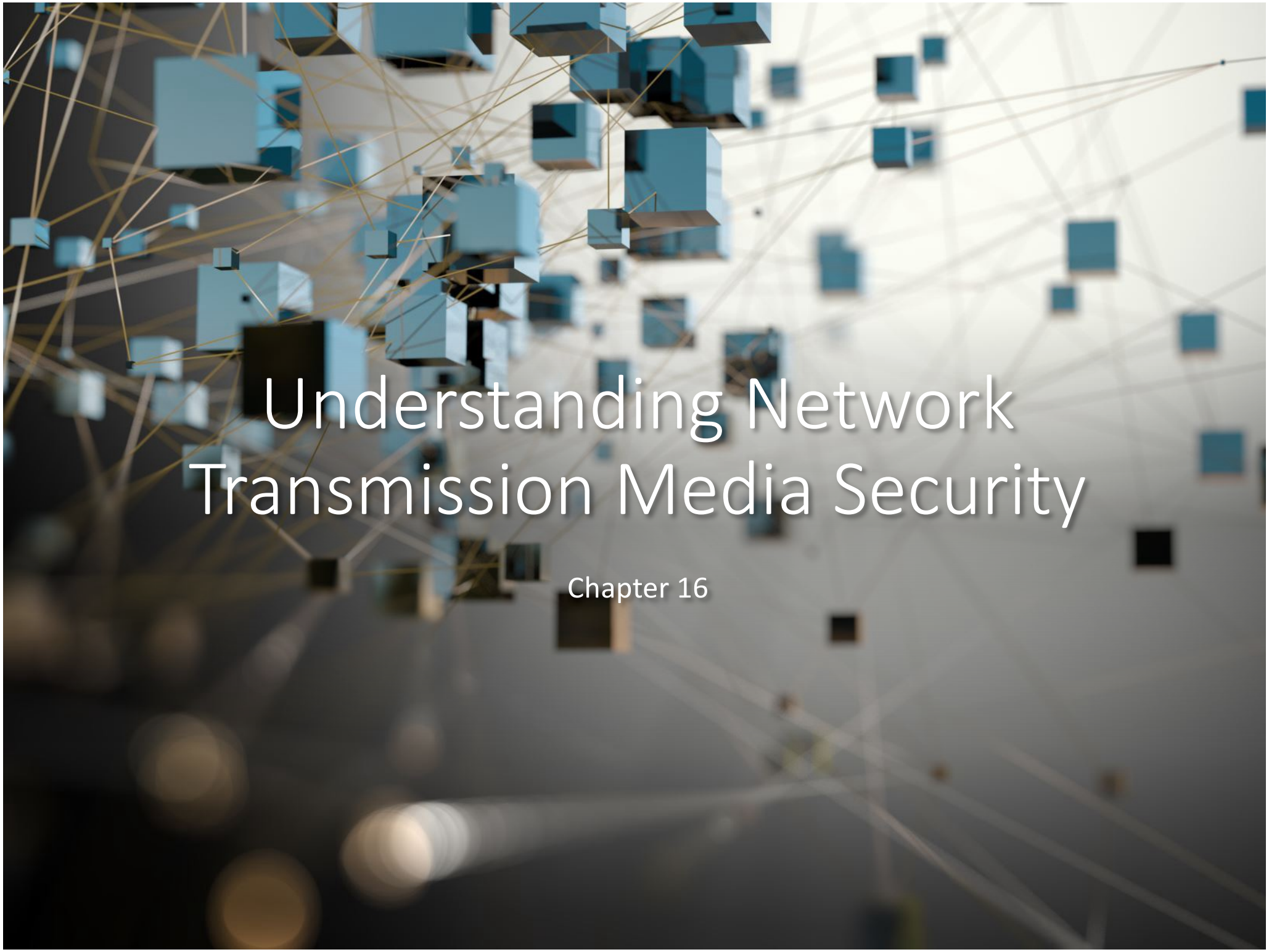


Understanding Network Transmission Media Security

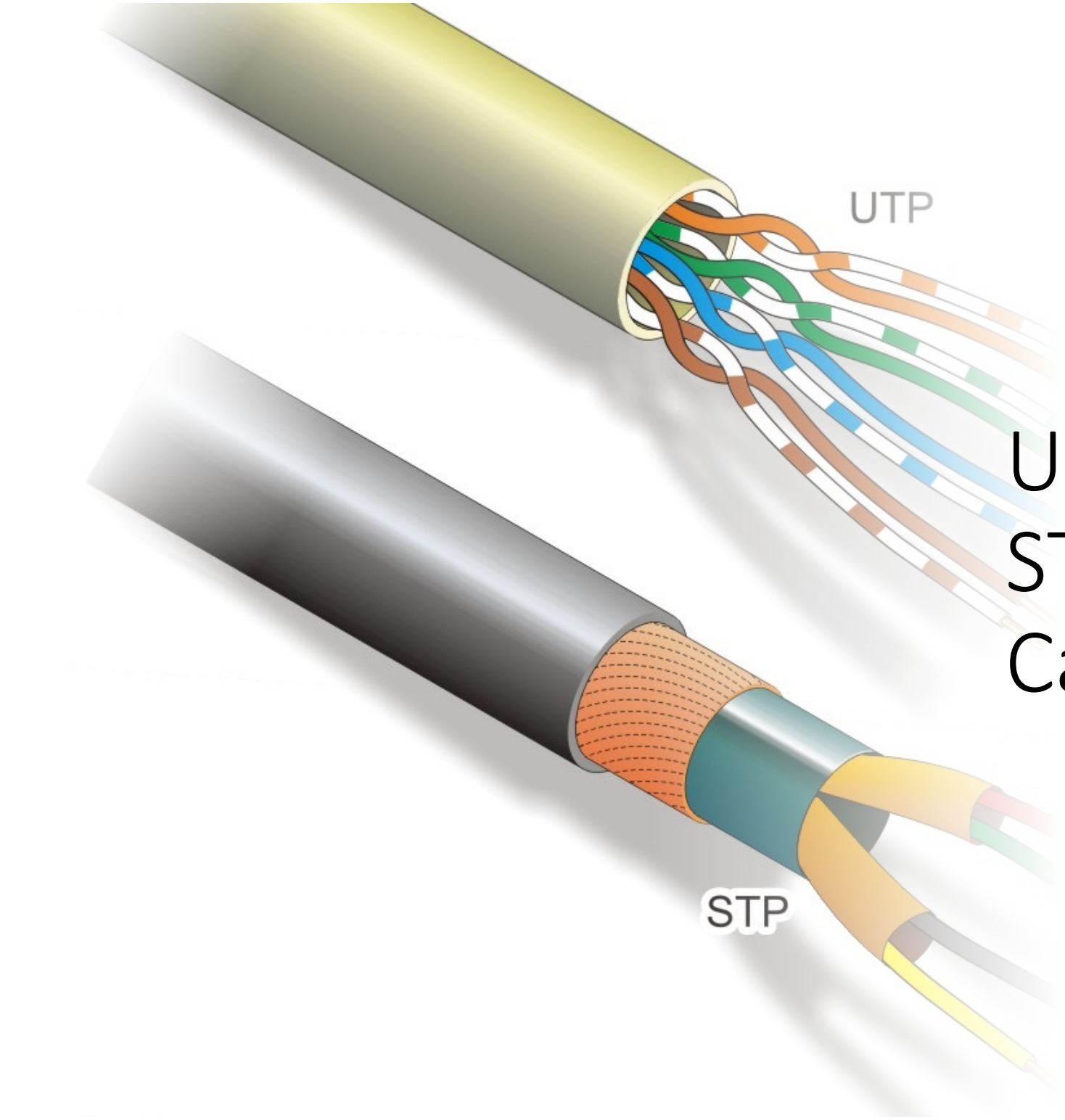
Chapter 16

In this chapter, you'll learn to:

- Understand twisted-pair cabling and coaxial cabling
- Understand fiber-optic cabling
- Understand Bluetooth and WiMAX
- Understand transmission media vulnerabilities
- Understand wireless network vulnerabilities

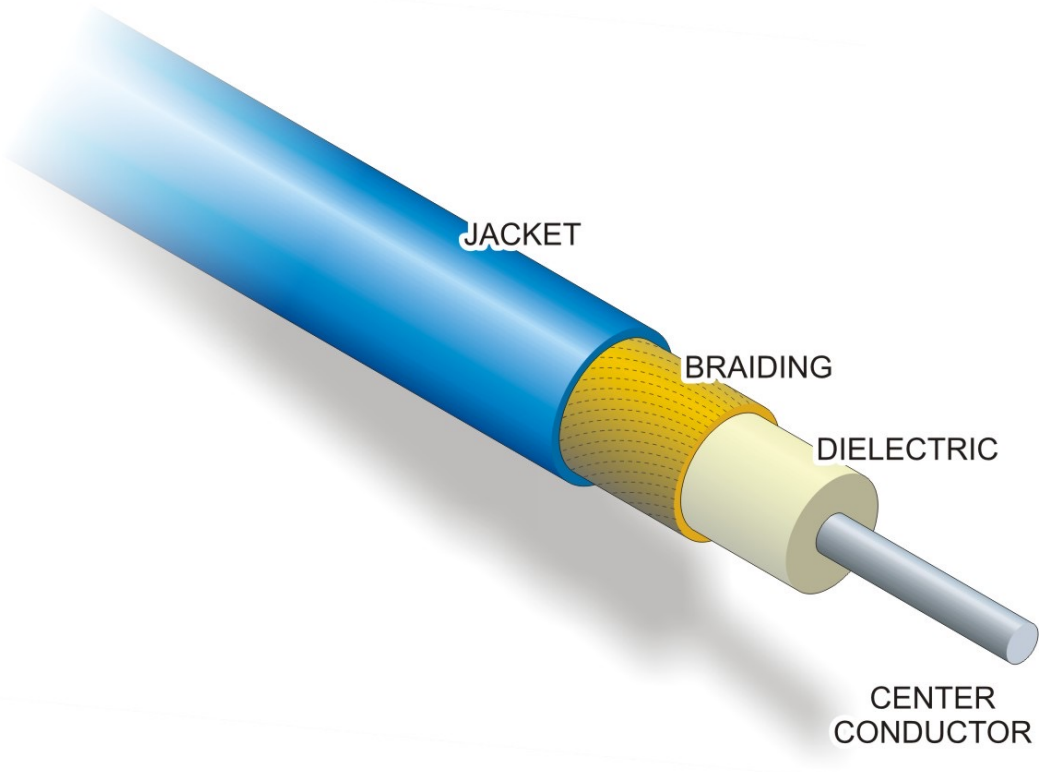
Digital data travels using three types of transmission media

- Copper wire(twisted copper cabling or coaxial cabling)
- Light waves (fiber-optic cabling or infrared light)
- Wireless radio frequency (RF) signals (Wi-Fi, WiMAX, Bluetooth, ZigBee, or Z-Wave)

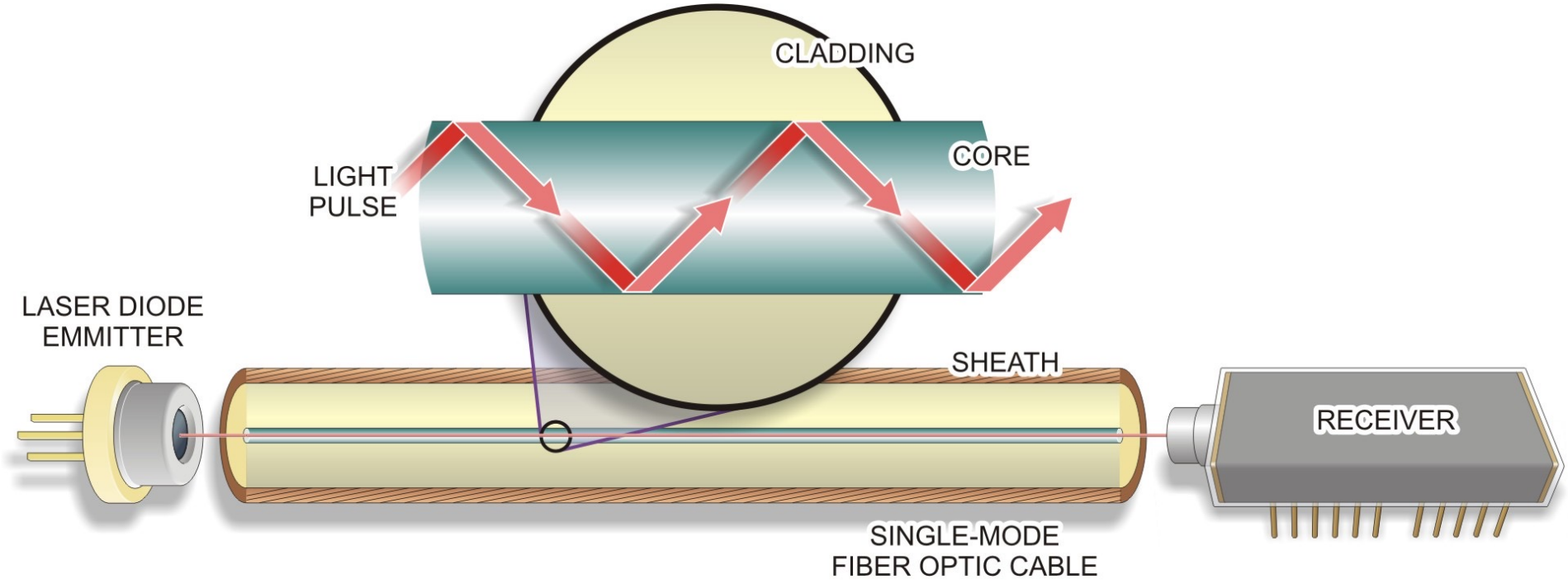


UTP and STP Cabling

Coaxial Cable



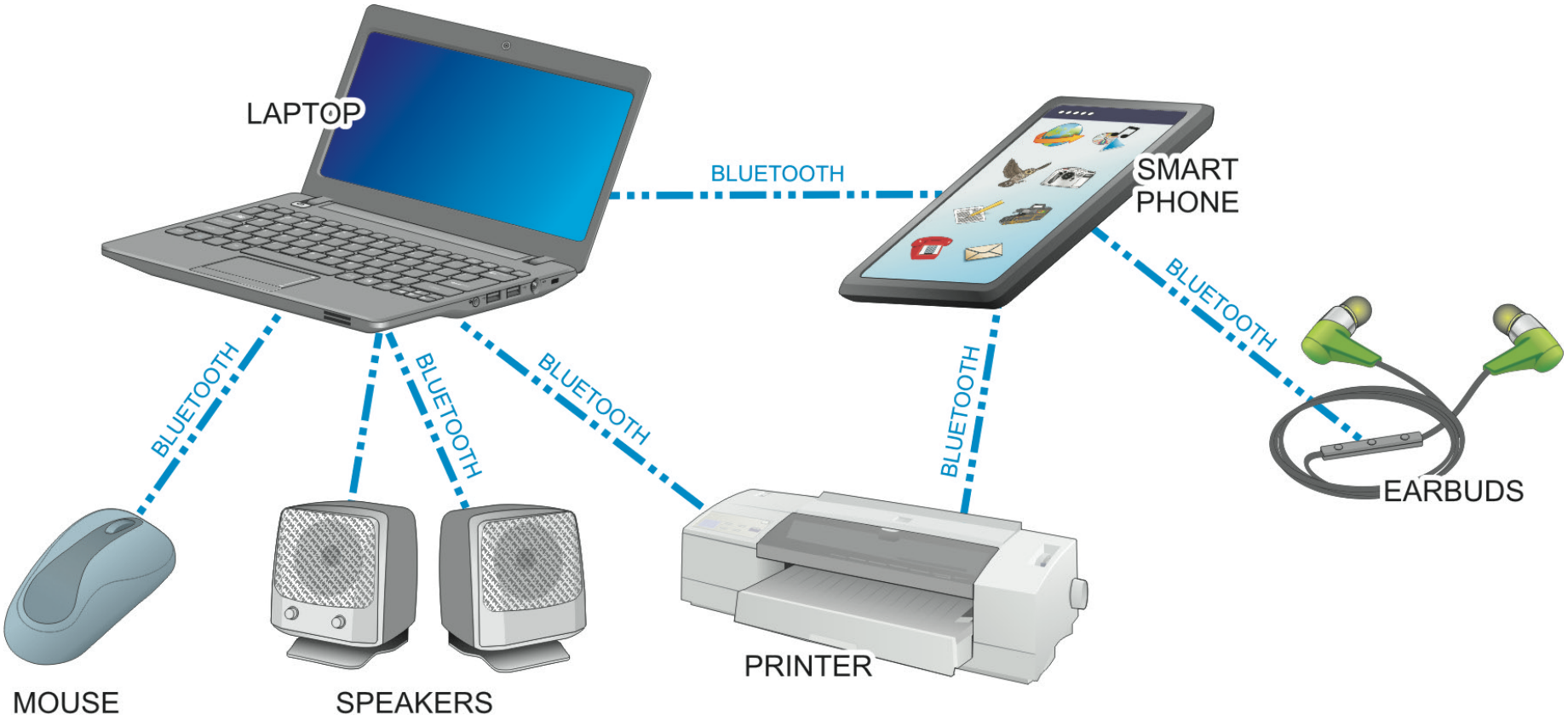
Transmitting Over Fiber-Optic Cable



A Fiber-Optic World Speed Record

- Researchers from the United States and the Netherlands have broken a world speed record by using a single, multicored piece of glass fiber. They were able to push 255 terabits per second, roughly equivalent to 32 terabytes per second.

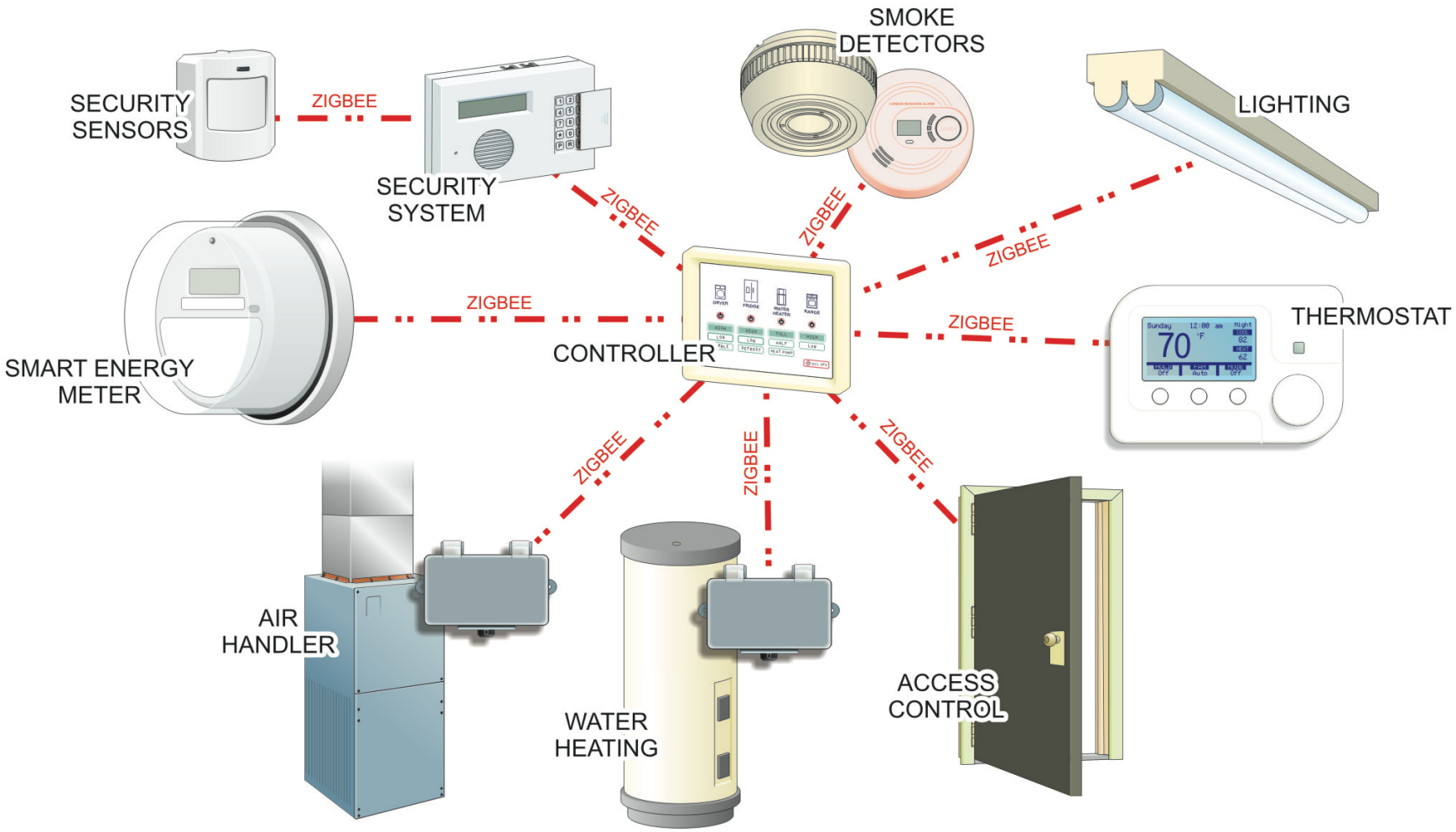
Bluetooth PAN



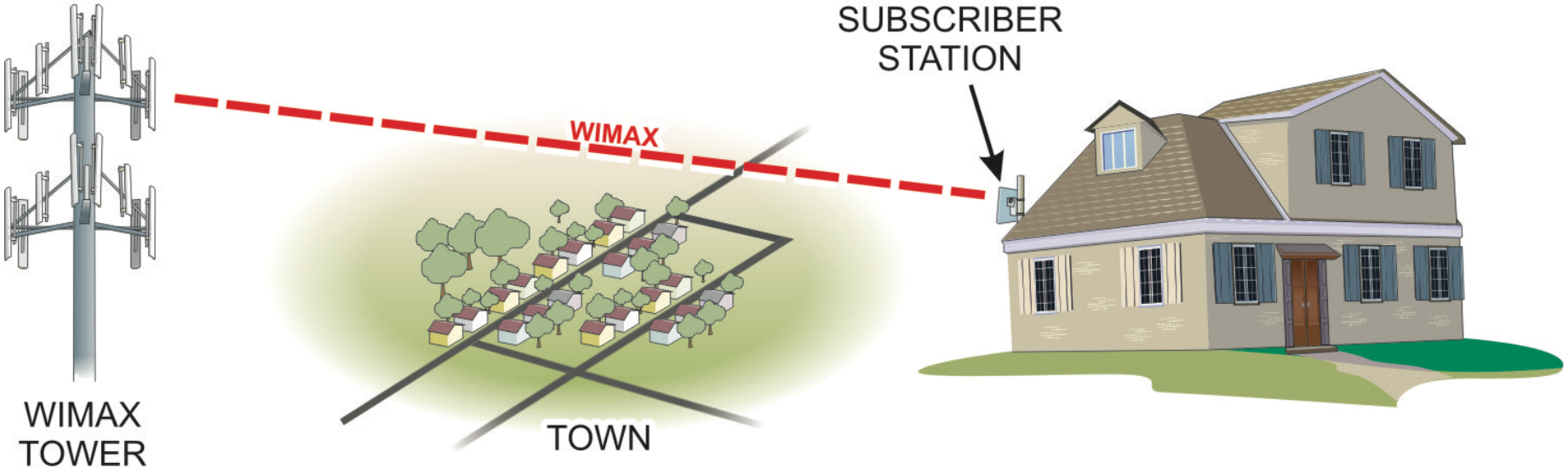
Bluetooth Parameters

Class	Maximum Power	Operating Range
Class 1	100 mW (20 dBm)	100 meters
Class 2	2.5 mW (4 dBm)	10 meters
Class 3	1 mW (0 dBm)	1 meter

ZigBee PAN


SECURITY SENSORS
ZIGBEE
SECURITY SYSTEM
SMOKE DETECTORS
LIGHTING
ZIGBEE
ZIGBEE
ZIGBEE
SMART ENERGY METER
ZIGBEE
CONTROLLER
ZIGBEE
THERMOSTAT
ZIGBEE
ZIGBEE
ZIGBEE
AIR HANDLER
WATER HEATING
ACCESS CONTROL

WiMAX



Local Network Security: Review Questions

Chapter 17

Summary Point

- The most widely discussed hierarchical networking initiative is the *open systems interconnection (OSI) model* put forward by the International Standards Organization.

Summary Point

- Every networking course examines the OSI model in terms of what types of devices, protocols, and functions exist at each level. However, different cybersecurity challenges may be present at each level.

Summary Point

- Network topologies are Layer 1 – physical or logical – connection strategies that fall into four basic types of configurations: star, bus, ring, and mesh.

Summary Point

- Most networks employ connectivity devices, such as hubs, switches and routers, which alter the appearance of the actual connection scheme. Therefore, the logical topology will not match the appearance of the physical topology. The particulars of the connection scheme are hidden inside the connecting device.

Summary Point

- A *network protocol* is a set of rules that governs how communications are conducted across a network. In order for devices to communicate with each other on the network, they must all use the same network protocol.

Summary Point

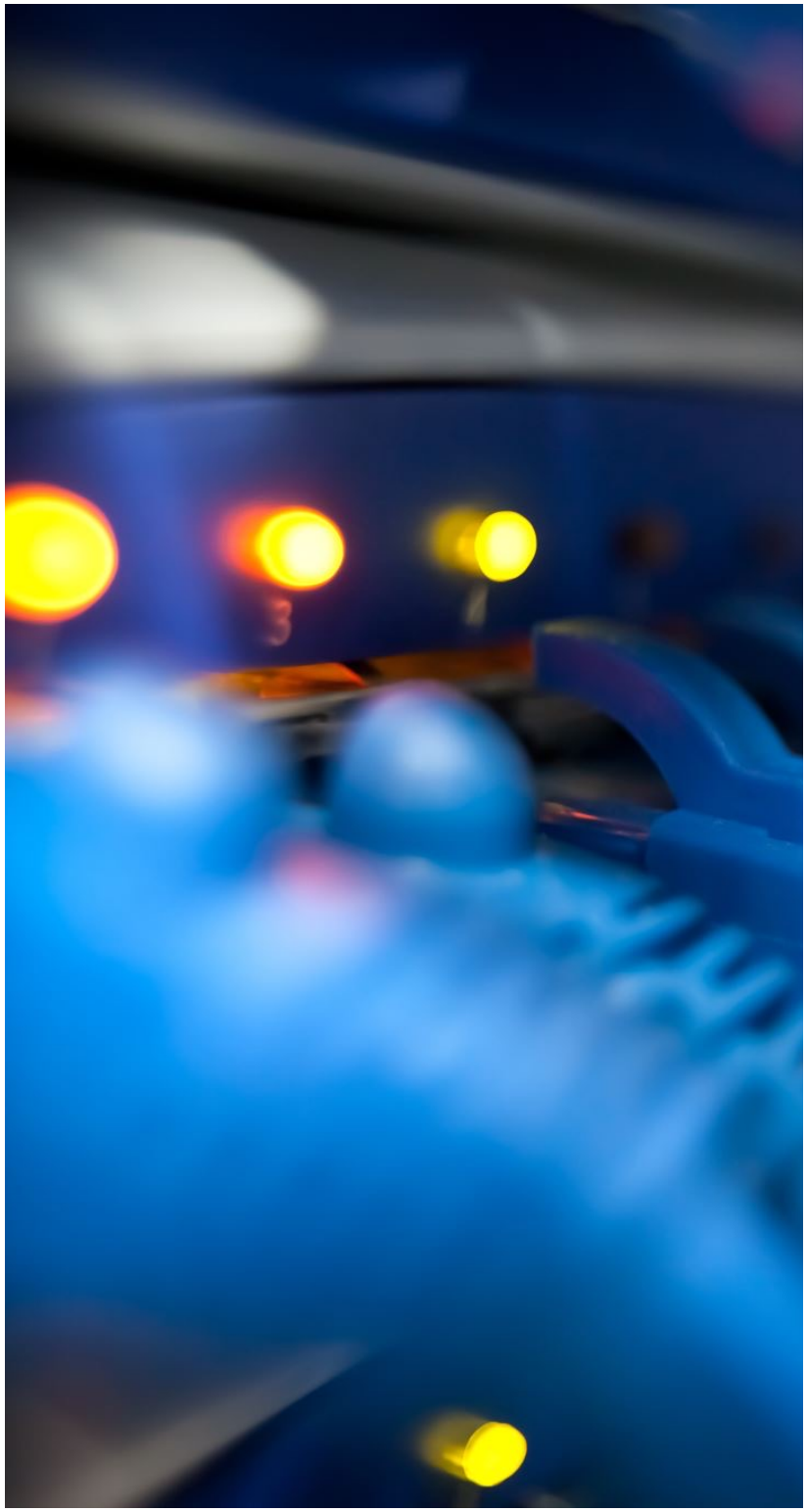
- The most basic address in networking operations is the Media Access Control address (*MAC address*) that serves as a unique identifier for every device attached to a network. These addresses are typically assigned to the devices by their manufacturers and stored in their firmware.

Summary Point

- There are two common types of attacks typically aimed at the MAC layer of a network: MAC Spoofing and MAC Broadcast Flooding.

Summary Point

- *MAC spoofing* involves changing the device's MAC address to change its identity.



Summary Point

- A *MAC broadcast flood attack* can be launched against a Layer 2 device, such as a network switch, from a device connected to one of its ports. The attack software on the controlled device is designed to flood a high volume of different MAC addresses into the switch's CAM table causing it to fill up. When this state is reached the switch will run out of room to map the new MAC addresses to its ports. Because all of the MAC addresses in the CAM are now new addresses that have not been mapped, the switch will be forced to broadcast all of the frames it receives to all of its ports.

Summary Point

- The TCP/IP (Transmission control protocol/Internet protocol) suite of protocols form the most popular network protocol currently in use.

Summary Point

- With the proper tools, it is fairly easy to manipulate the IP headers of TCP/IP packets to falsify addresses to hide an attacker's identity. This manipulation process is known as *IP spoofing* and is the basis for many types of network and internetwork attacks.

Summary Point

- A *SYN flood* that exploits the three-way handshake TCP/IP employs to initiate connections between network nodes. In this type of attack, the attacker sends the SYN request to the server, but manipulates the handshake to either spoof a different IP address in the SYN packet or simply withhold the ACK packet from the server.

Summary Point

- An IP address is required to make a device a valid member of the Internet. This is how individual users are identified to receive file transfers, email, and file requests. Two versions of IP addressing are currently in use: IPv4 and IPv6. IPv4 is the Internet protocol version typically referenced because it has been around longer and is simpler to understand.

Summary Point

- Sections of the network can be grouped together into subnets that share a range of IP addresses. A protective *gateway* is employed to act as an entry and exit point for the segmented subnet. These groups are referred to as *intranets*. An intranet requires that each segment have a protective gateway to act as an entry and exit point for the segment. In most cases, the gateway is a device called a *router* or a *switch*.

Summary Point

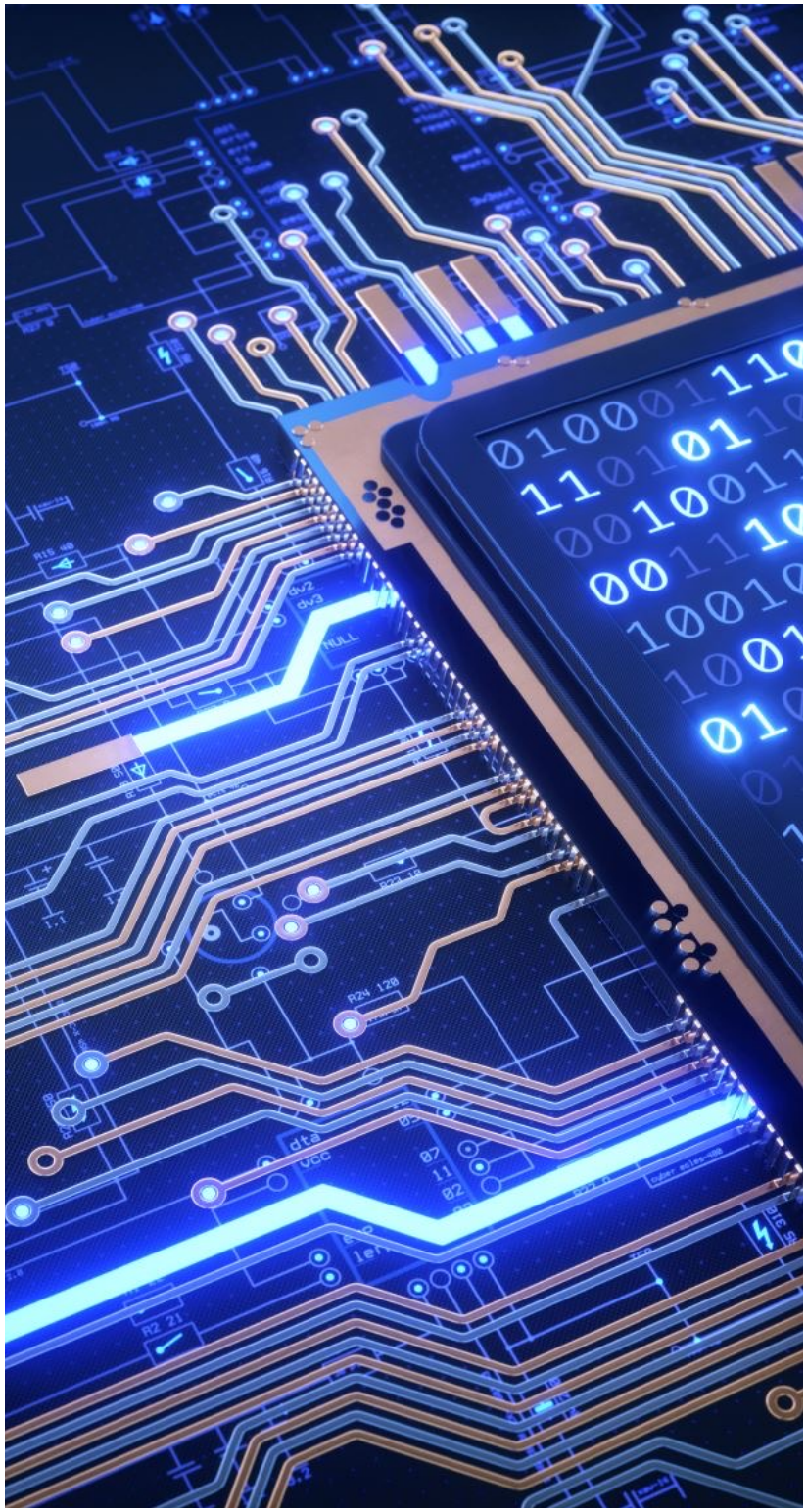
- Alongside TCP/IP being the dominant data packaging and transfer protocol suite, the Ethernet family of standards has become the dominant force in hardware and electrical signaling interfacing as well as for providing media access control.

Summary Point

- Under the Ethernet standard, information is collected into a package called a frame. An Ethernet *frame* brings together many pieces of information required to navigate a network: the source and destination MAC addresses, as well as the IP packet header and data. In addition, the Ethernet frame adds an error-checking and correcting section, which enables the receiver at the destination to check what it receives for correctness.

Summary Point

- The Ethernet protocol is classified as a bus topology that has been implemented across several different network media, including:
  - Coaxial cable (IEEE 802.3 – 10BASE-2 or -5)
  - Twisted-pair copper cable (IEEE 802.3 – 10/100/1000BASE-T)
  - Fiber-optic cable (IEEE 802.3 – 10/100/1000BASE-Fx, Lx or Sx)
  - Wireless RF (IEEE 802.11a-h)



Summary Point

- *Network servers* are specialized computers designed to operate efficiently in a multiuser, multiprocessor, multitasking environment.

Summary Point

- While all servers perform the basic functions described so far, in practice servers may vary significantly in the primary application they are designed to perform for the network's clients.

Summary Point

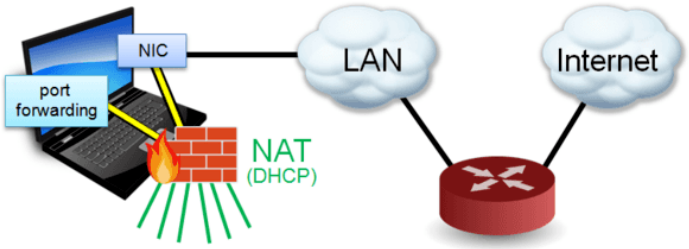
- Access to a server’s shared resources should be limited to users who have both a need and the proper authorization to gain such access. Care should to be taken to make sure that unauthorized employees do not gain access to confidential materials.

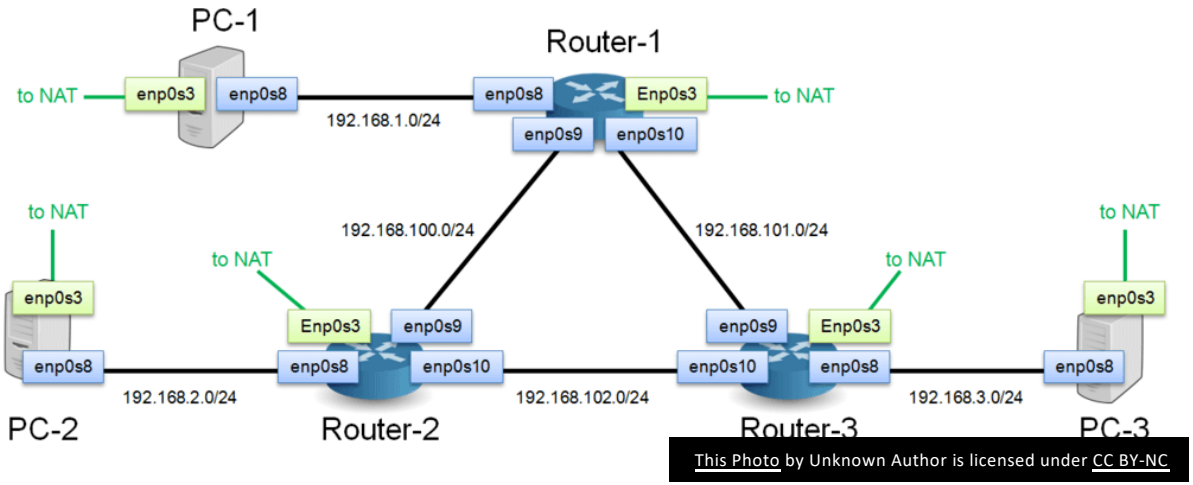
Summary Point

- Network access to servers should typically be protected by one or more firewalls.

Subnets or routers may be used to create a network segment for some network servers.

Summary Point





Summary Point

- Because servers are frequently used for user authentication, the server's password should be hashed as a preventative measure. This is typically done by the operating system.

```
string|false password_hash (
    string $password ,
    int $algo
    [, array $options ]
)
```

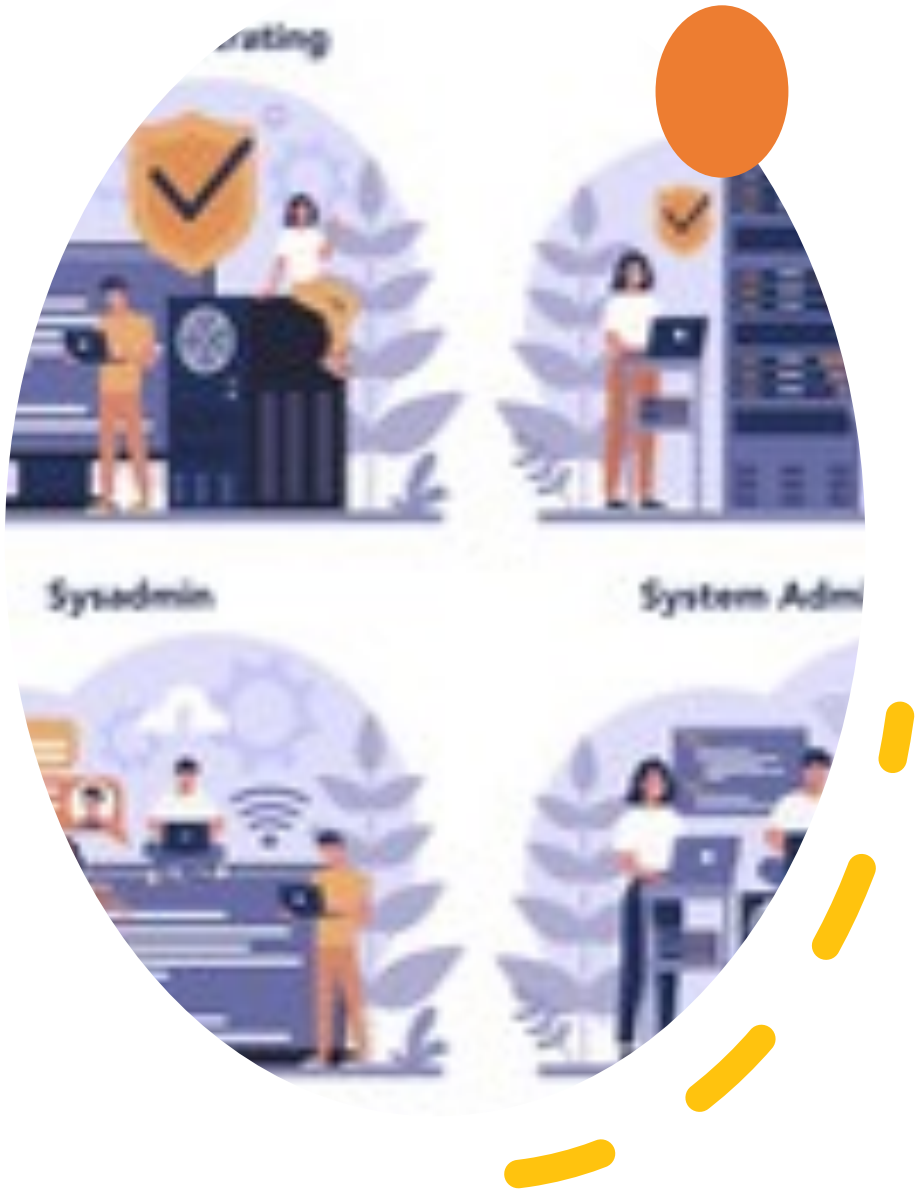
```
$algo = PASSWORD_DEFAULT (=== PASSWORD_BCRYPT)

$options = ['cost' => 10]
```

Summary Point

- In network environments administrators are responsible for implementing the organization's security policies. These policies should be designed to reflect the three objectives associated with the classical model of information security: confidentiality, integrity and availability (CIA).

Summary Point

- The server admin is responsible for the design, implementation, and maintenance of the server computers, while the network administrator provides the same functions for the network and its media and connectivity devices.



Summary Point

- Division of administrative duties may also involve a special security administrator who is responsible for performing information security tasks for the servers, hosts and connectivity devices in the network.

Summary Point

- Network administrators must have control over their physical server environment to provide a comprehensive security setting. This is accomplished by strictly limiting physical access to the servers – most commonly by placing them in protected server rooms that have automatic locks on the door and computer chassis.

Summary Point

- After the operating system and the desired applications have been installed, steps need to be taken to harden the security configuration of the entire server software environment. This involves closing as many known vulnerabilities, while still offering acceptable usability to the network's users/customers.

Summary Point

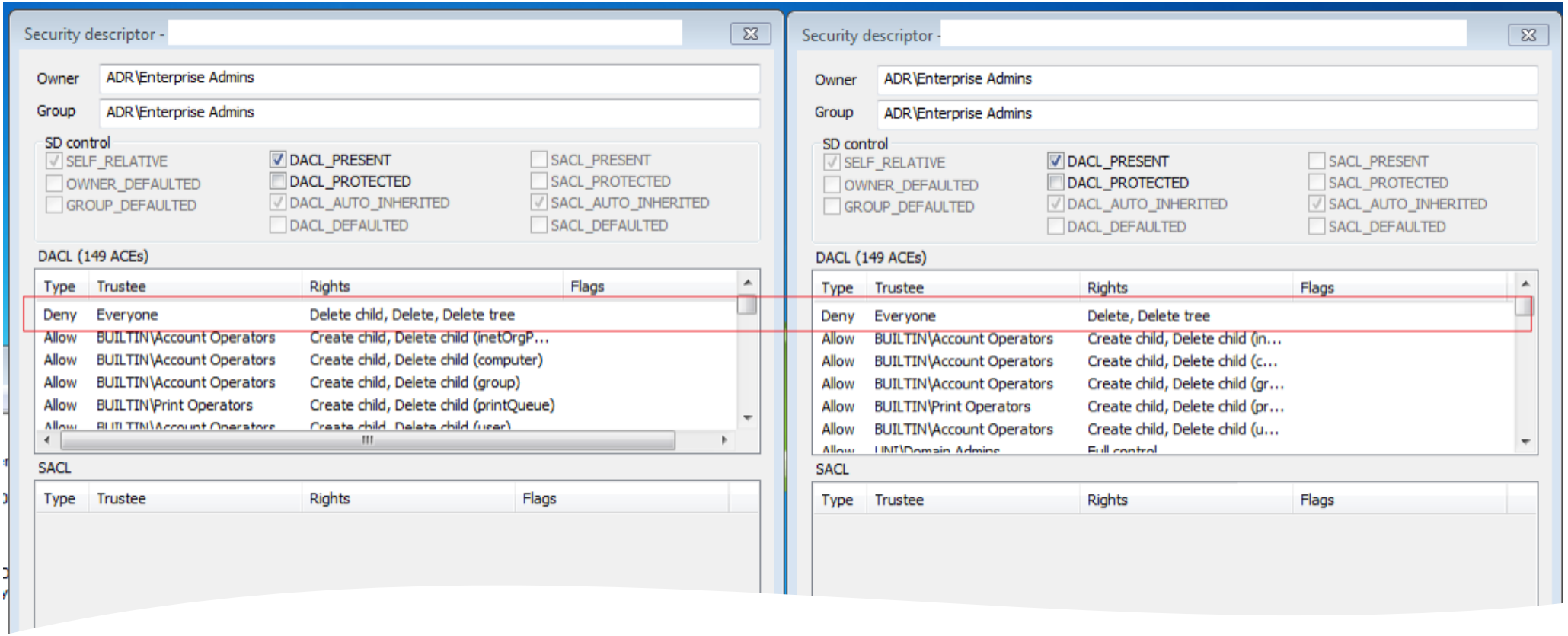
- The *Mandatory Access Control (MAC) system* establishes which users or groups may access files, folders, and other resources.

Summary Point

- With Discretionary Access Control (DAC) strategies and configurations, the user has the discretion to decide who has access to their objects and to what extent.

Summary Point

- *Non-Discretionary, Role-Based Access Control (RBAC)* is based on job roles each user has within the organization.

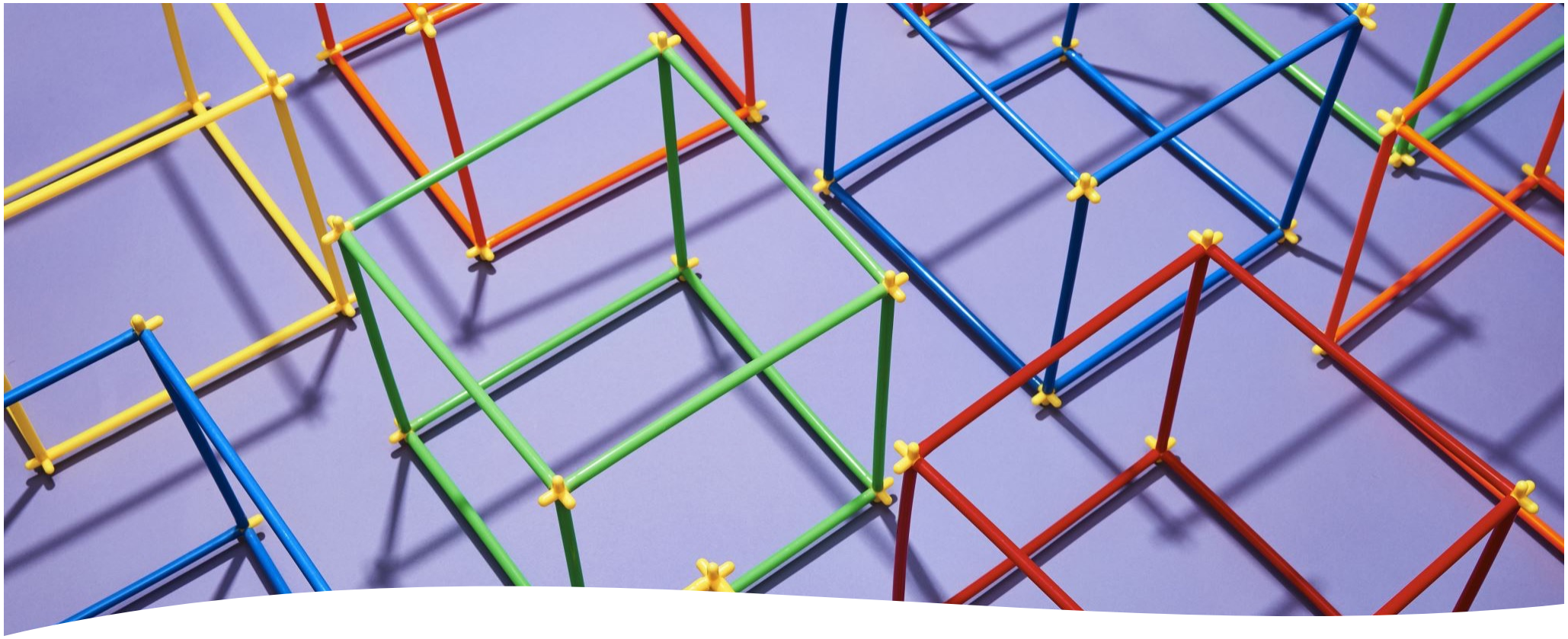


Summary Point

- The domain's server is responsible for maintaining an *access control list (ACL)* database that tracks each user account, including which group accounts they may be assigned to, as well as what rights and permission they have to different objects.

Summary Point

- In each strategy type, the *principle of least privilege* should be implemented when providing users with access to objects through rights and permissions assignments. Under this rule, each user is granted only the levels of access required to perform their job rolls. This principle limits the damage that can be inflicted by a security breech to the initial task, process, or user.



Summary Point

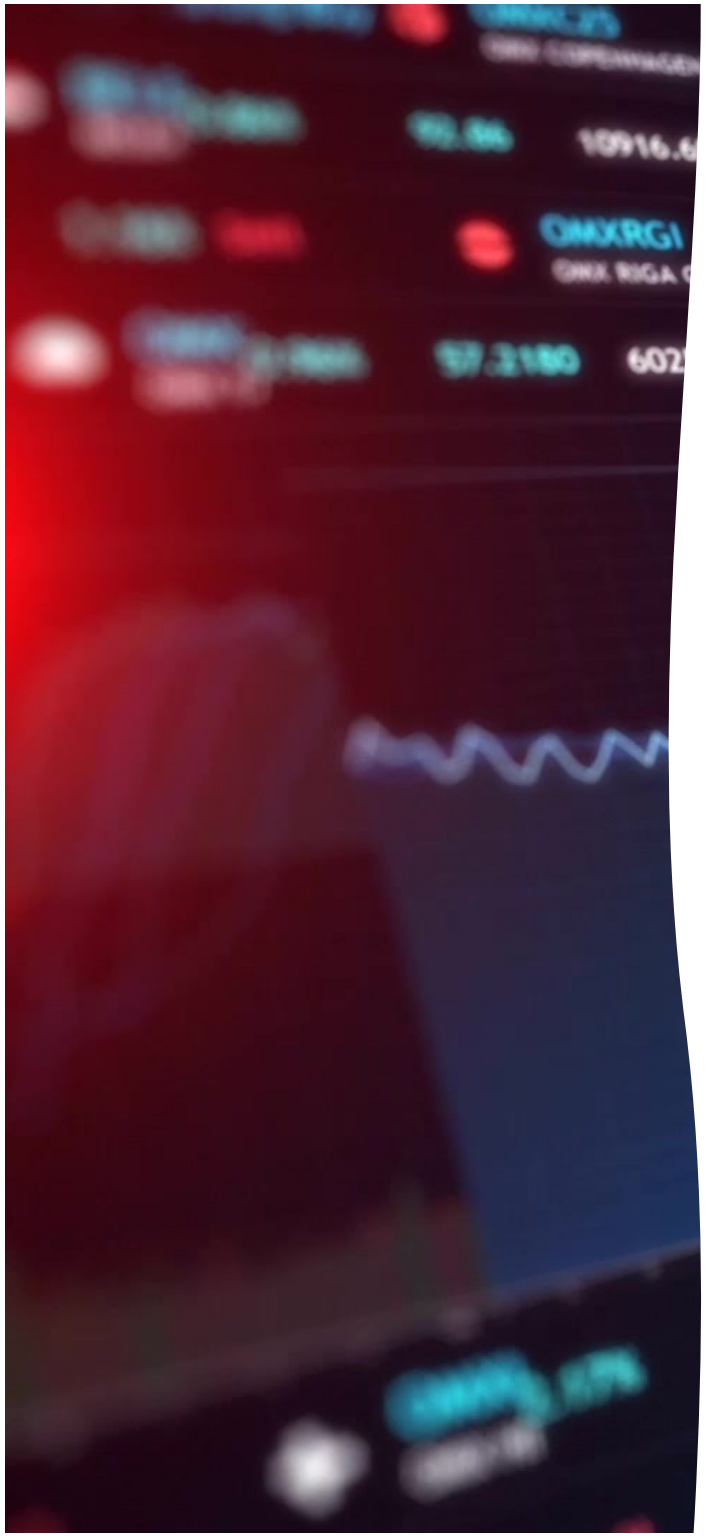
- There are two classes of users in a network: administrators and users. These classes may also exist at two different levels: in local accounts databases located on the individual client devices and in network accounts databases located on network servers.

Summary Point

- Administrators create user and group accounts for network clients that include specific access rights and permissions to the network's resources. Network users are allowed or denied access to read, modify, and examine files and folders based upon the access control policy that has been established for them either as individuals or by their position in different network groups.

Summary Point

- An important part of an administrator's tasks and the overall network security plan is auditing. *Auditing* is a pre-planned monitoring method to evaluate or determine if problems exist within the area being evaluated or audited.



Summary Point

- Some firewalls, Intrusion Detection Systems, and auditing software can be configured to provide immediate alerts or notifications to administrators when unusual patterns or events are recognized.

Summary Point

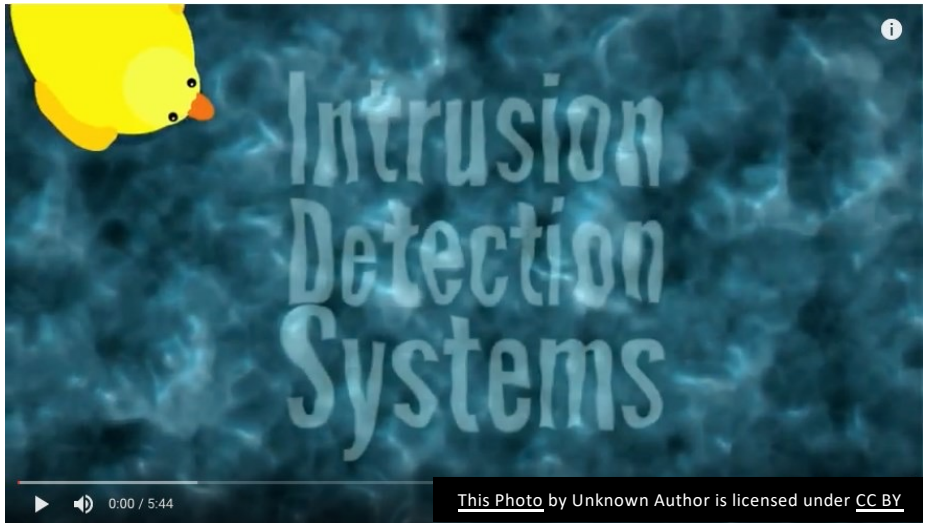
- Auditing user privileges is a useful technique for identifying whether a user's computer has picked up a virus that escalates the user's privileges.

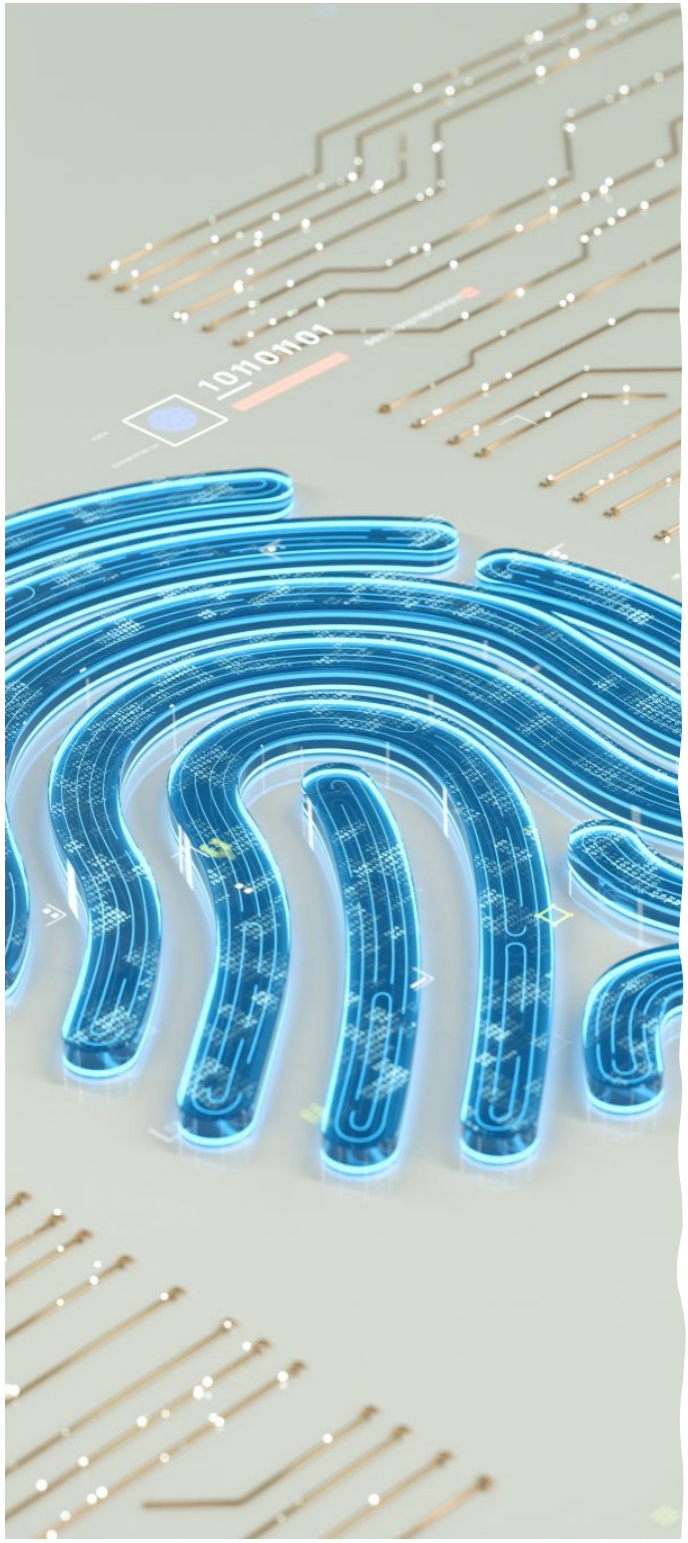
Summary Point

- *Privilege escalation* refers to users who are able to execute a program with embedded code that gives them administrative privileges after logging onto the server.

Summary Point

- Local host Intrusion Detection Systems have been the dominant implementation choice. However, similar systems are available for network-wide implementation. Ultimately, the most effective IDS/IDPS defense is a combination of the two types of systems working together in what are referred to as *distributed IDS systems*.



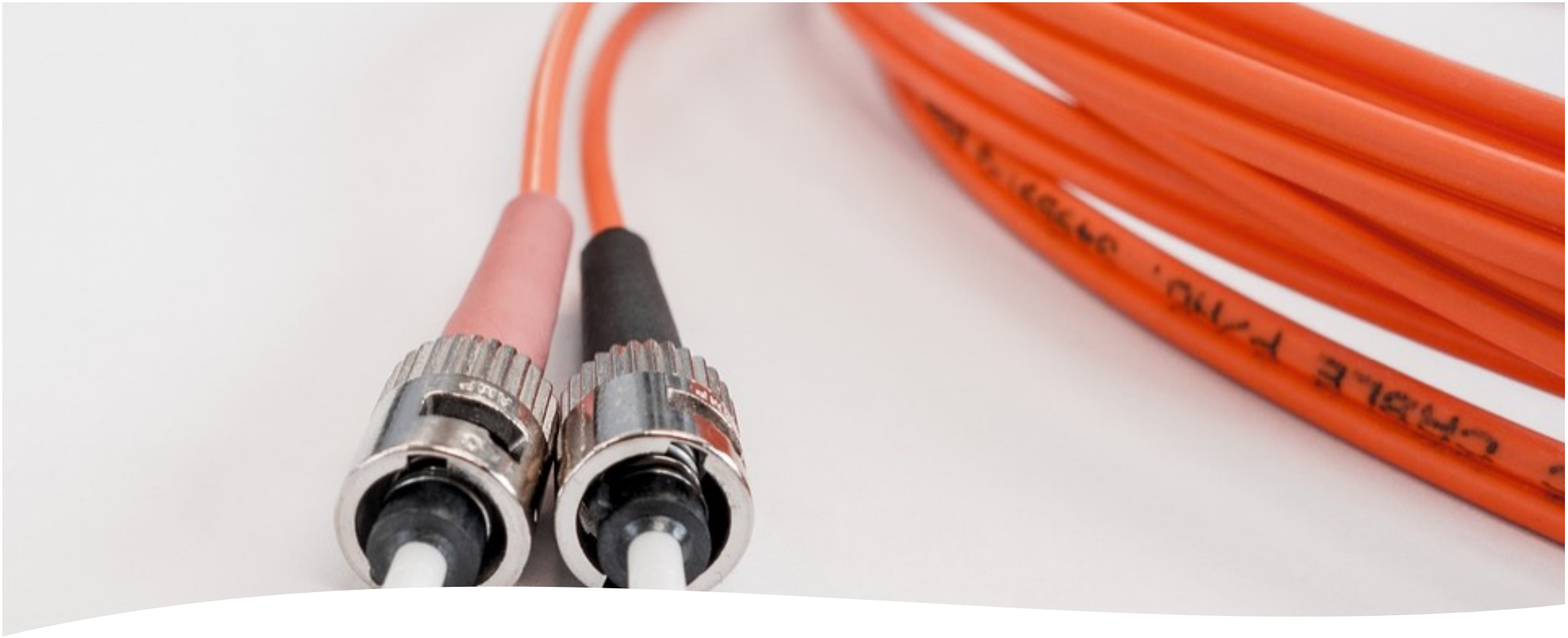


Summary Point

- Several vulnerability scanners are available to test the system and identify vulnerabilities and misconfigurations of computing devices in a network environment.

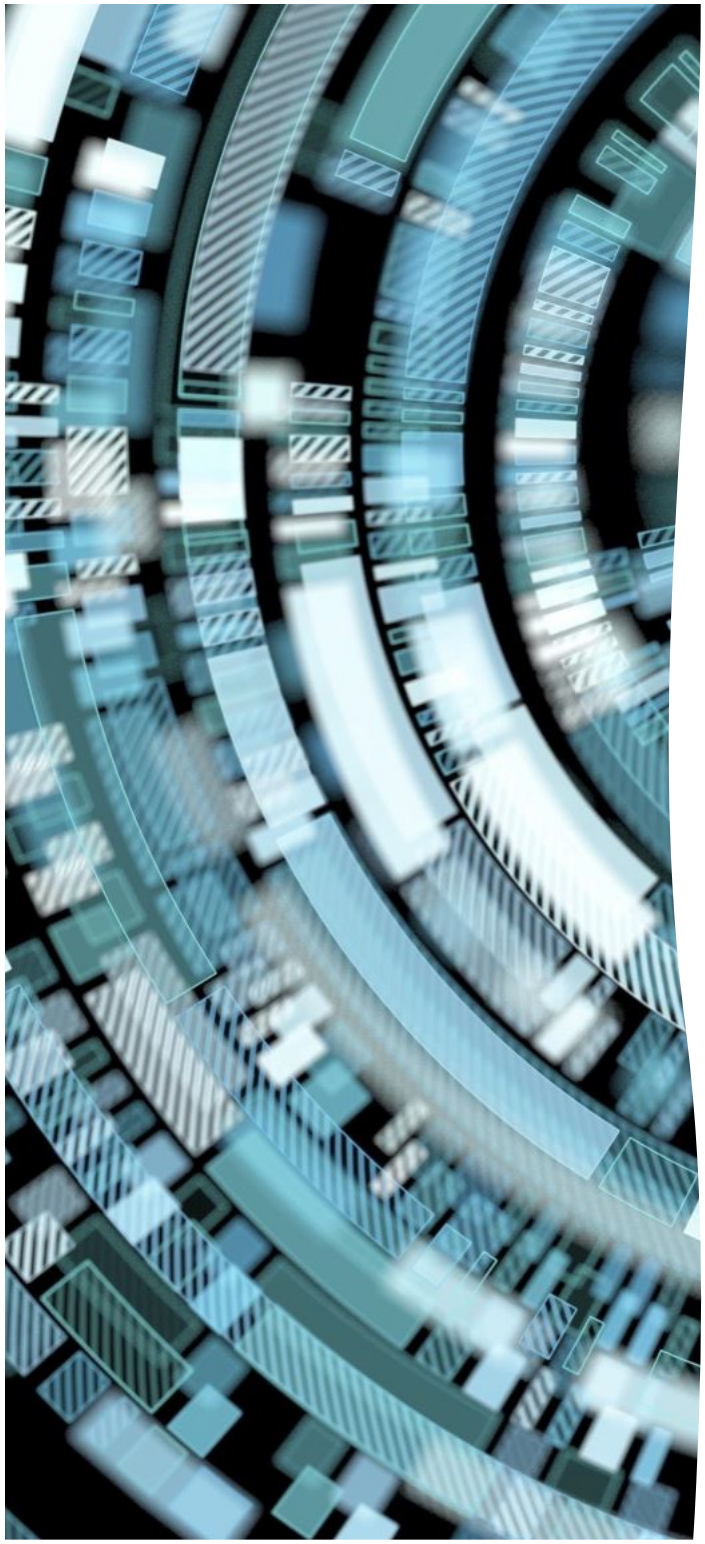
Summary Point

- When physical media leaves the confines of the private facility, the information they carry becomes vulnerable to interception and capture along their route or at the receiving port of the message.



Summary Point

- Fiber-optic cable provides a much more secure data-transmission medium than copper cable, because it cannot be tapped without physically breaking the conductor.

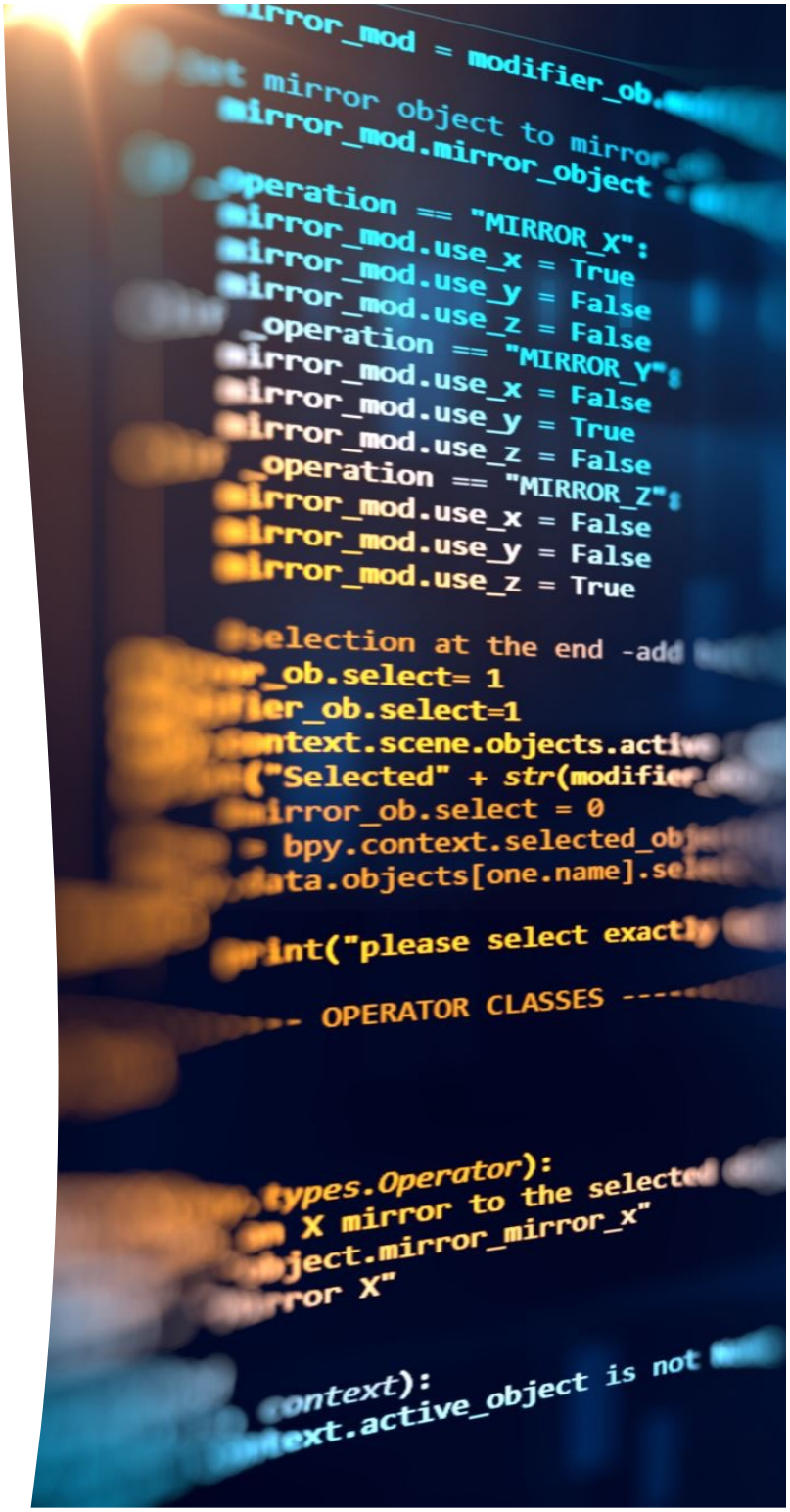


Summary Point

- The IEEE 802.11x wireless standards (also known as Wireless Fidelity or Wi-Fi) have gained wide acceptance as the preferred wireless networking technology for both business and residential network applications.

Summary Point

- Wired Equivalent Privacy (WEP) provides a basic encryption scheme for encrypting data transmissions and authenticating each computer on the network using a 128-bit mathematical key.

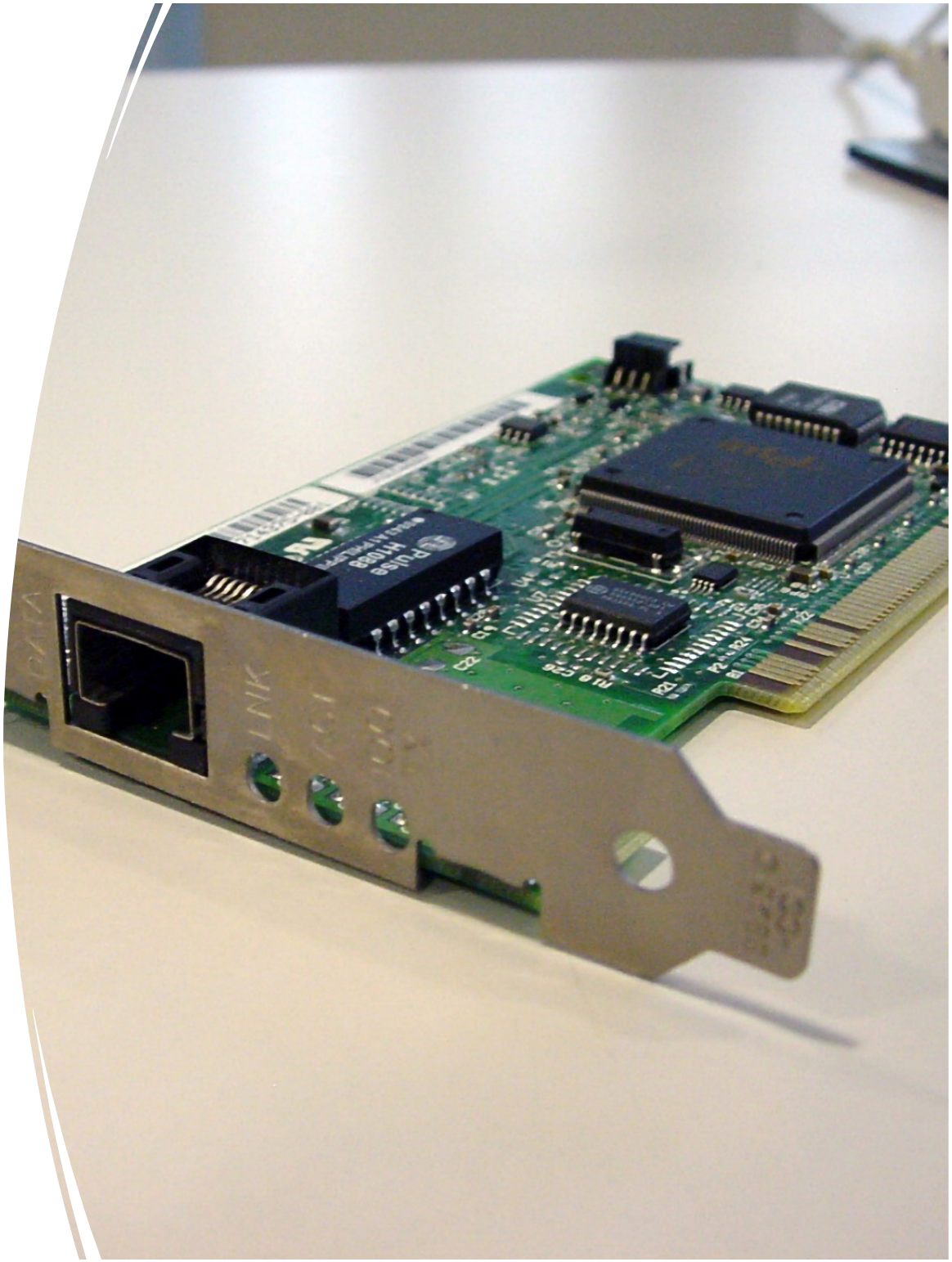


Summary Point

- The Wi-Fi Protected Access (WPA) standard adds improved data encryption, using Temporary Key Integrity Protocol (TKIP) and IEEE 802.1X Extensible Authentication Protocol (EAP) user authentication protocol to provide increased security. This combination requires users to employ usernames and passwords to access the network.

Summary Point

- All the intelligent devices attached to the network must have a network interface adapter capable of physically connecting the device to the network transmission media.



Summary Point

- Switches collect MAC address information to keep track of the devices attached to them. As they interact with those devices, they record their MAC information in an onboard memory structure called a *MAC address table*.

Summary Point

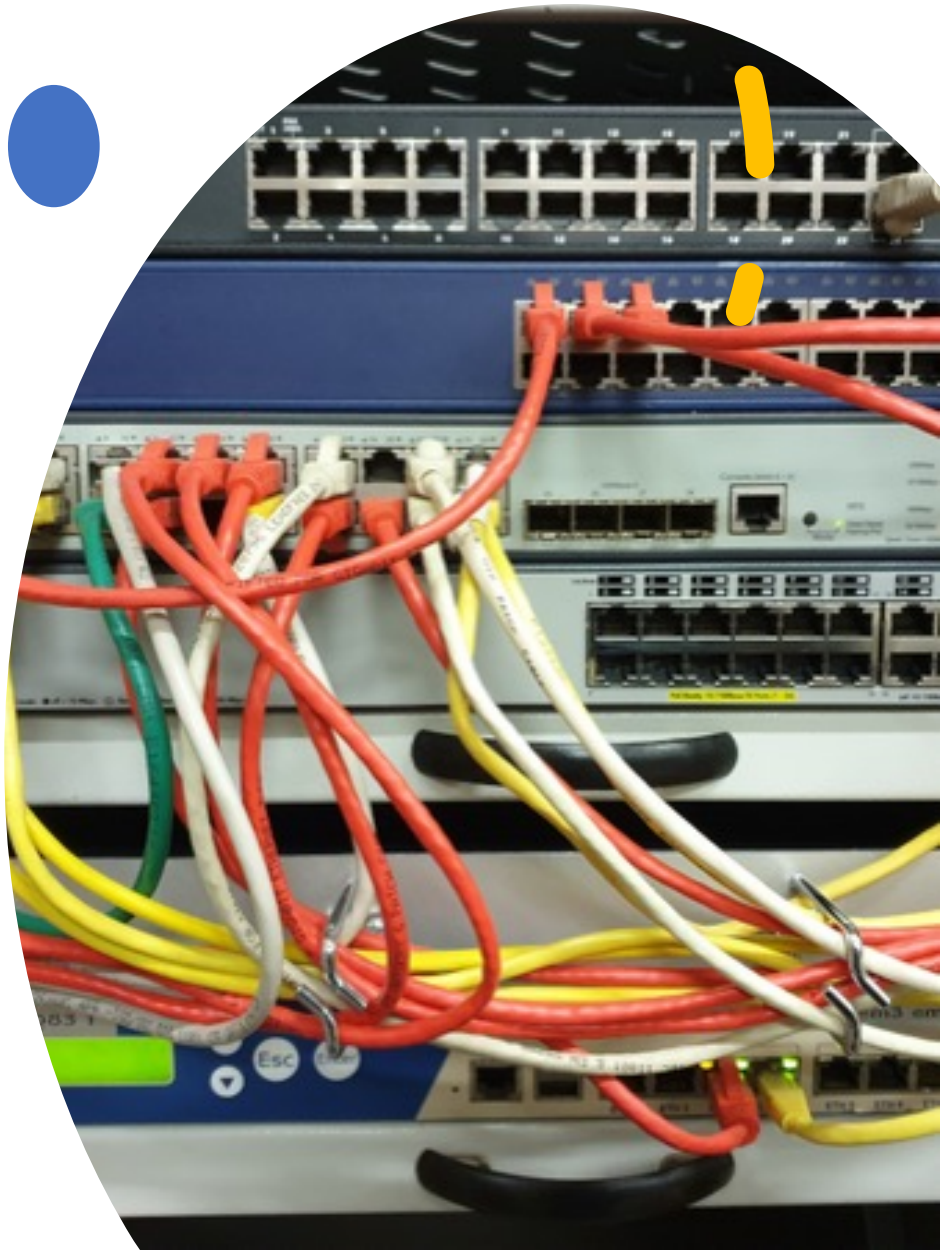
- Switches can also be used to create logically secured Virtual Local Area Networks (VLANs) – a security topology that restricts visibility of network traffic by limiting the movement of network packets so that they only pass between designated ports.

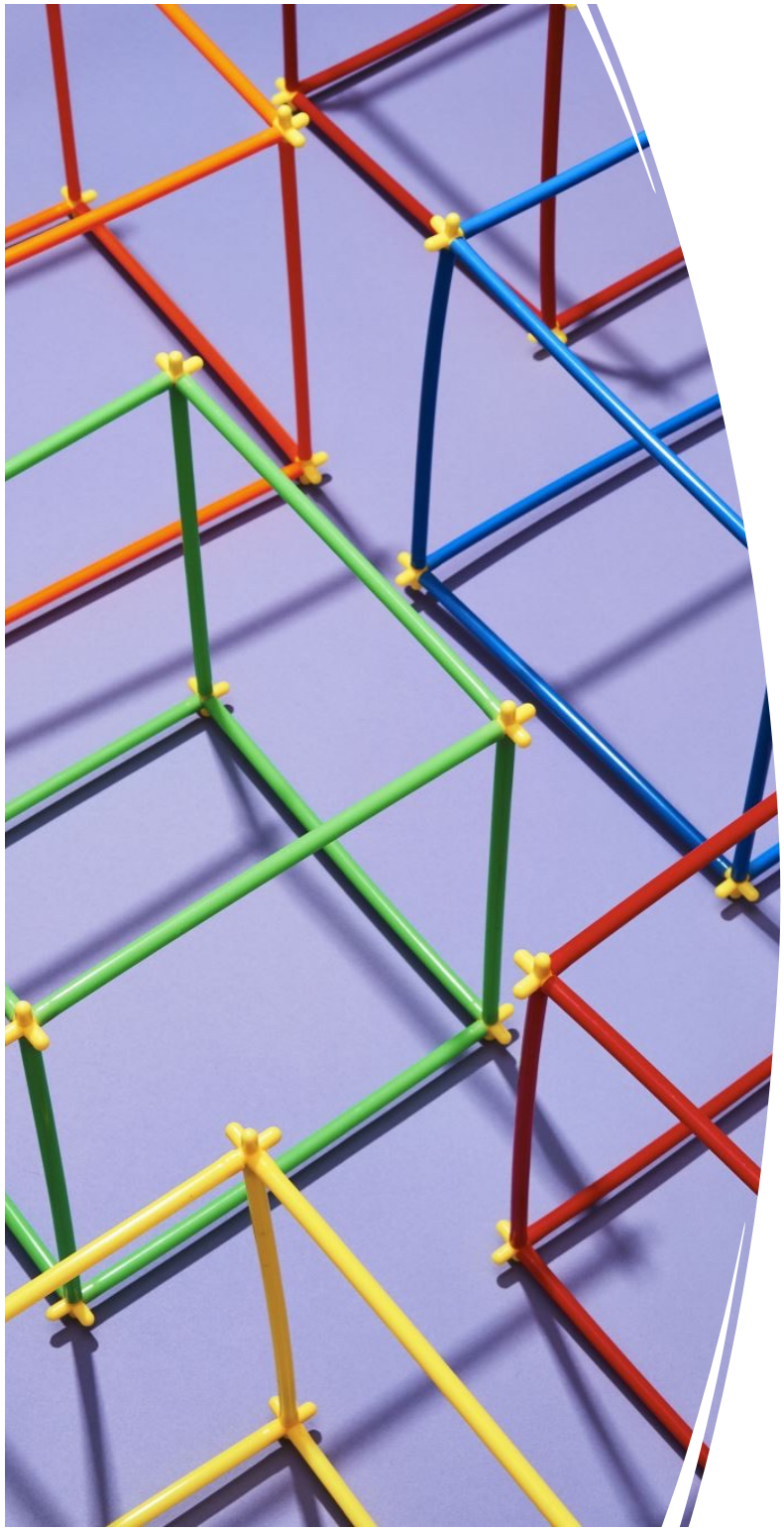
Summary Point

- *Unmanaged switches* are Plug and Play (PnP) devices that do not include any options for user configuration.

Summary Point

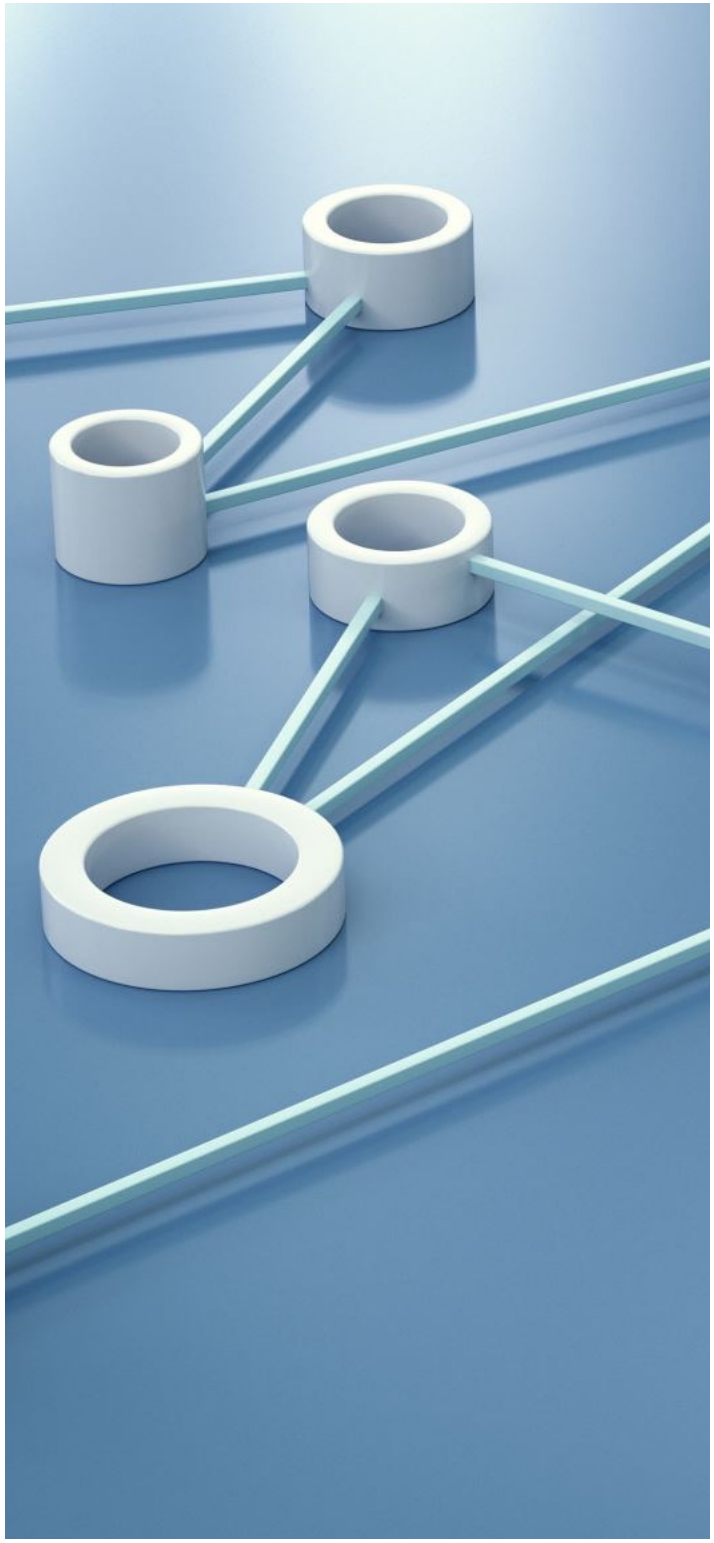
- *Managed switches* are connectivity devices that have programmable management functions built into them that enable administrators to configure them for the specific network environment in which they will be used in. As such, they provide some type of management console that the administrator can use to set parameters.





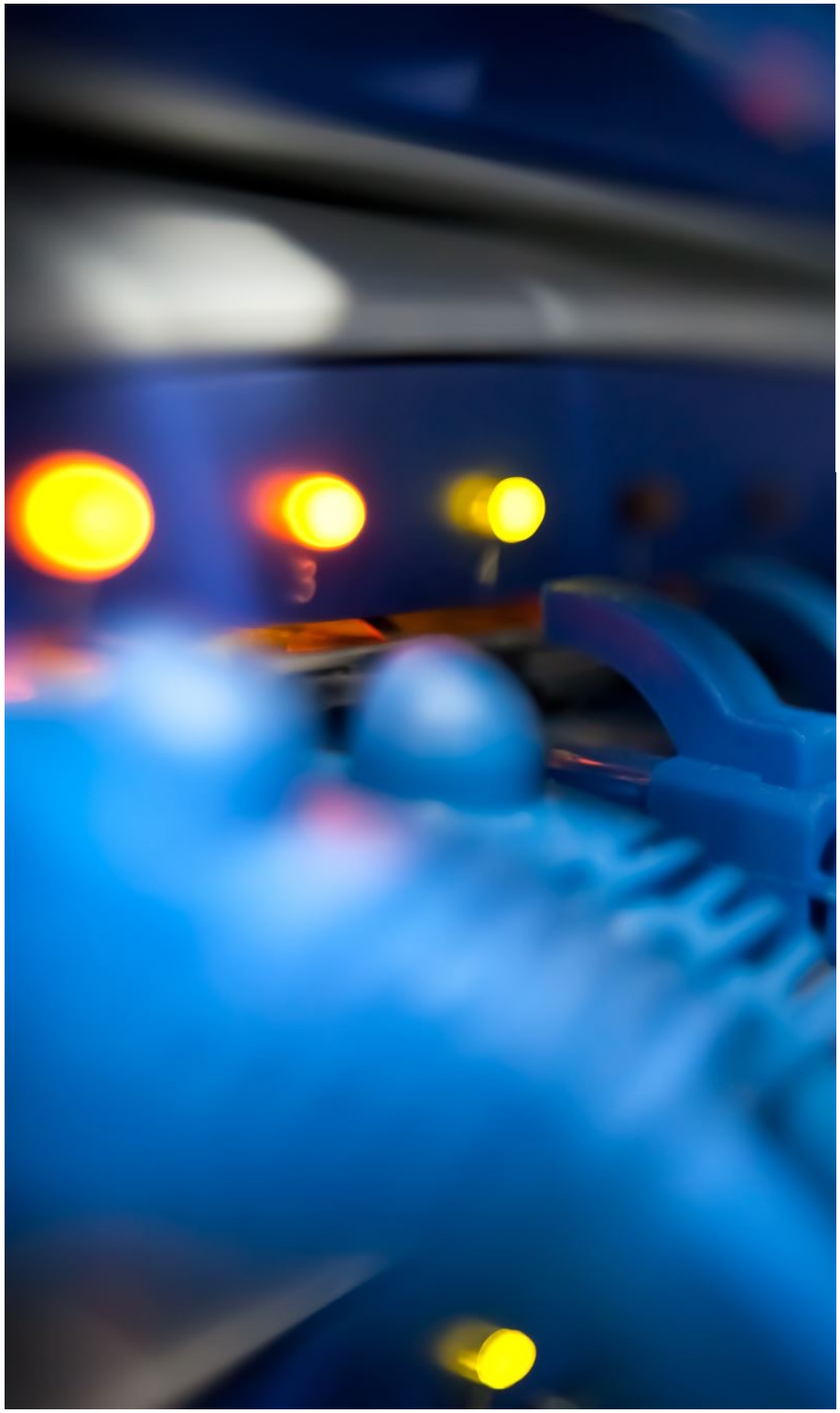
Summary Point

- *Routers* are network connectivity devices that forward network information in a manner similar to switches. However, unlike switches, routers can forward information across different network segments. This gives routers the ability to join different networks together through a process known as *routing*.



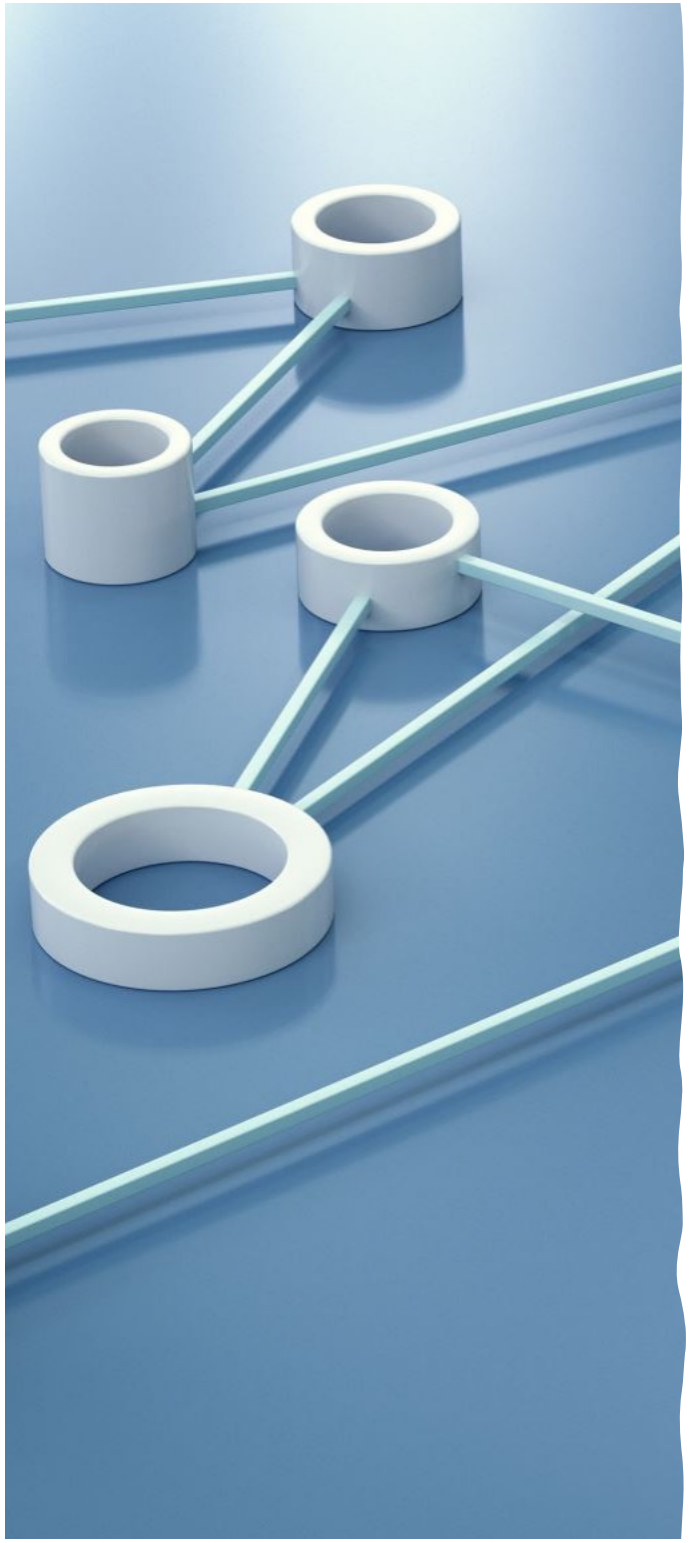
Summary Point

- Routers contain different sections of DRAM memory to hold message routing information and to buffer data flow between its ports. The routing information is stored and updated in a logical memory table referred to as *routing table*.



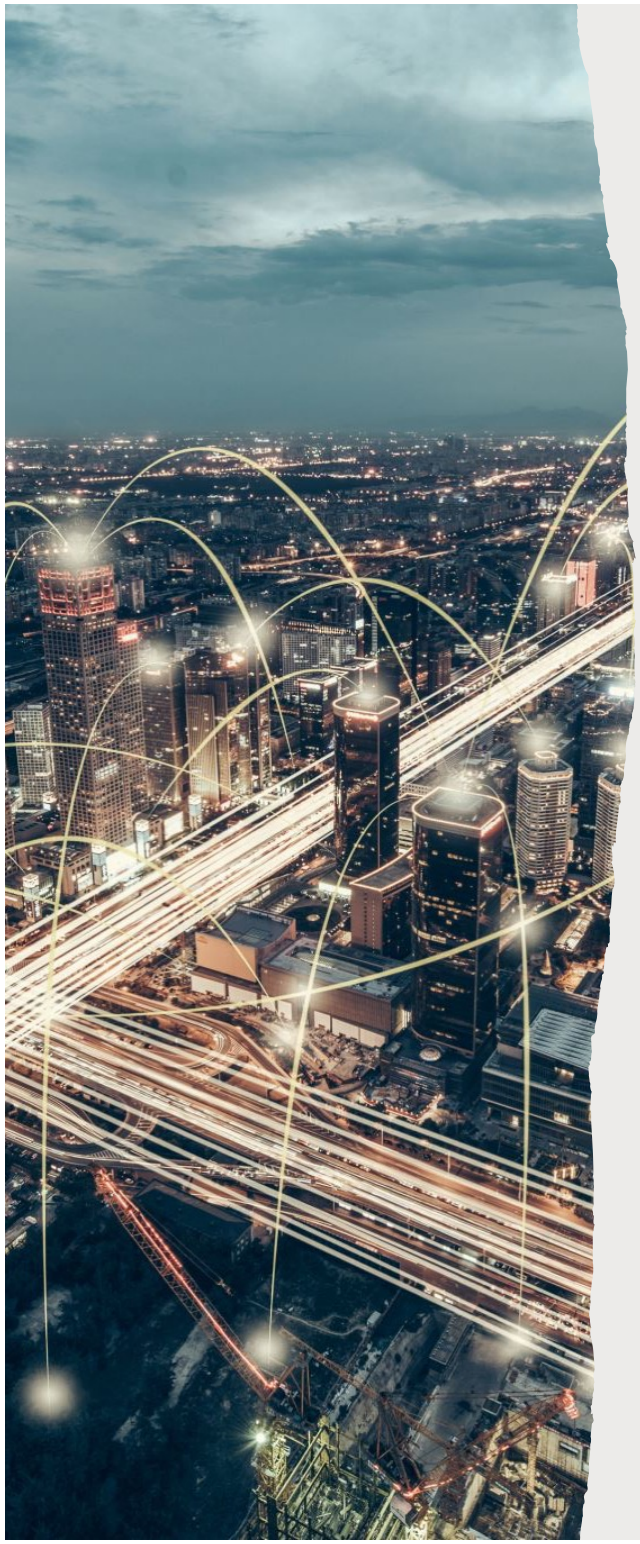
Summary Point

- Routers communicate with other routers using a routing protocol to build and maintain their routing tables. These tables are used to record the best route between different network locations.



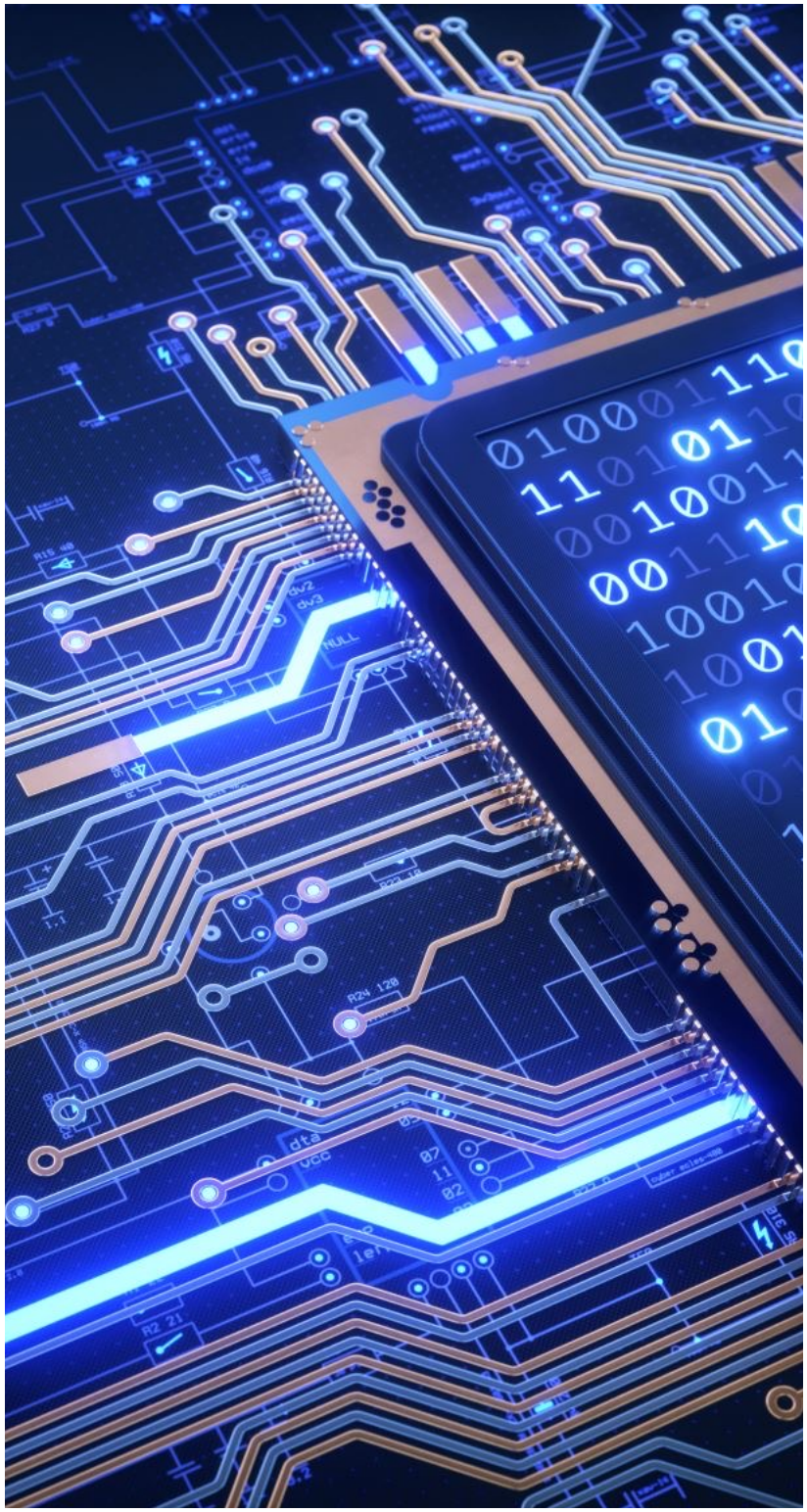
Summary Point

- A *gateway* is defined as a device that interfaces a network with another network that employs a different protocol. Recall that a *protocol* is a defined set of rules for carrying out communication between different devices or systems.



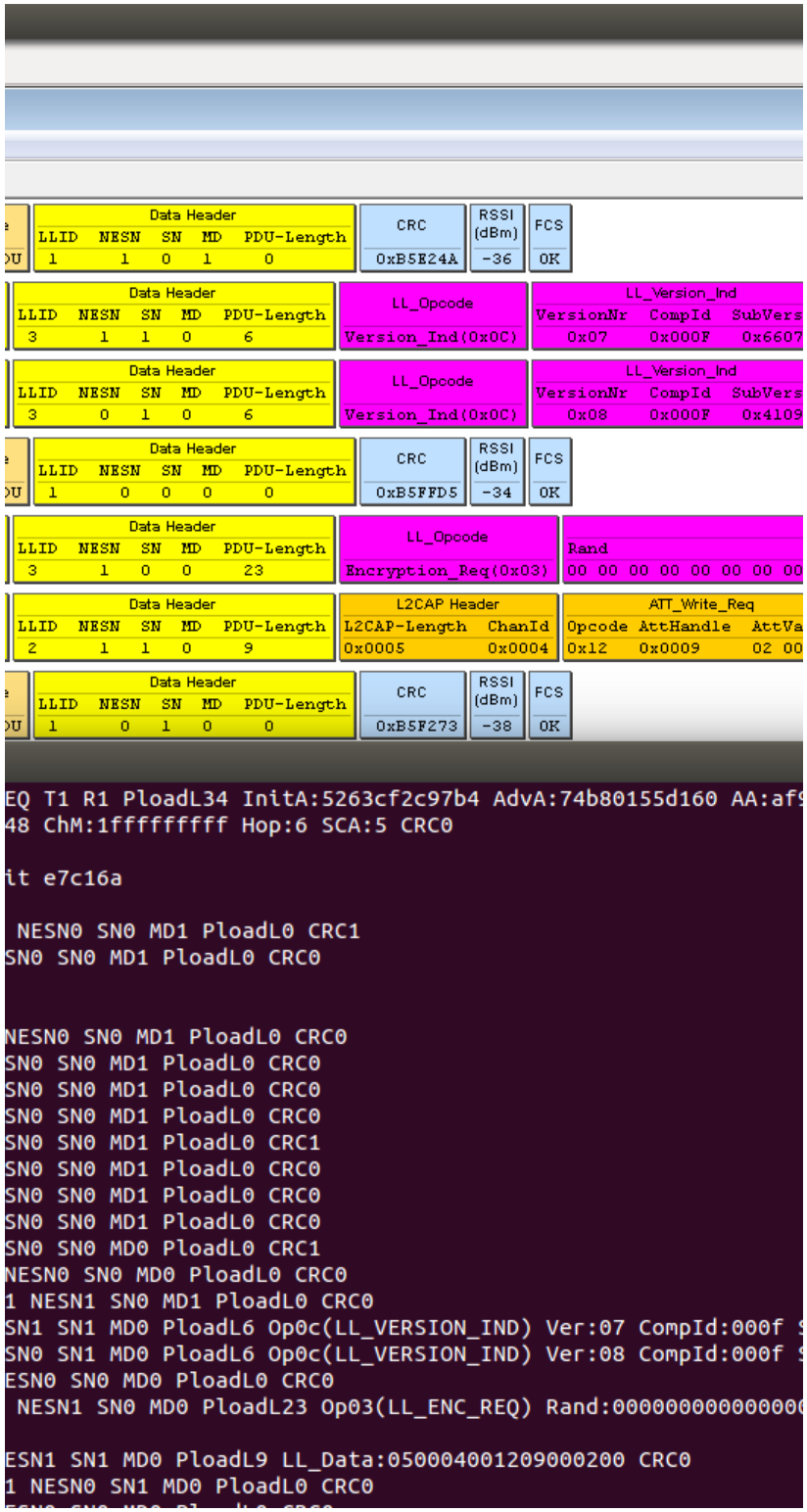
Summary Point

- A *network bridge* (or a network switch) bridges network segments together and forwards traffic from one network to another. Like the switch, a bridge uses MAC addresses to guide information to the correct ports.



Summary Point

- Most network connectivity devices possess some level of configuration possibilities. As such, their operation can be manipulated if their configuration parameters can be accessed. As with other types of network and computing devices, passwords should be employed to control access to the connectivity device's configuration data whenever possible.



Summary Point

- *Packet sniffing* is the act of listening to packets as they move through a network. This activity is normally conducted using a network analyzer tool referred to as a *packet sniffer*. Attackers use these tools to listen to network traffic looking for items such as passwords and usernames sent across the network in a plaintext mode; they also listen for sensitive information such as credit card or other financial information they can hijack.

Summary Point

- *Address Resolution Protocol (ARP) spoofing* attacks send fake ARP messages to associate their MAC address with the IP address of another user. Once the association has been established, messages directed to that address will be diverted to the attacker. The attacker can then use information obtained from the intercepted messages to mount other types of attacks, such as DoS or man-in-the-middle attacks.

Summary Point

- A *MAC broadcast flood attack* can be launched against a Layer 2 device, such as a network switch, from a device connected to one of its ports. The attack software on the controlled device is designed to flood a high volume of different MAC addresses into the switch's CAM table causing it to fill up. When this state is reached, the switch will run out of room to map the new MAC addresses to its ports. Because all of the MAC addresses in the CAM are now new addresses that have not been mapped, the switch will be forced to broadcast all of the frames it receives to all of its ports.

Summary Point

- Router *flood attacks* are designed to consume all, or a significant part, of the router's resources, thereby rendering them non-functional. Router resources commonly targeted include onboard memory, processor operation and internal bus bandwidth.

Summary Point

- In *MAC duplicating attacks* also known as MAC cloning attacks, the attacker updates their own MAC address with the target's MAC address. This will cause the switch to forward traffic to both locations.

Summary Point

- *Switch-port-stealing attacks* are designed to flood the switch with altered response packets. This will cause the switch to forward all traffic through the switch to the attacker’s location.

Summary Point

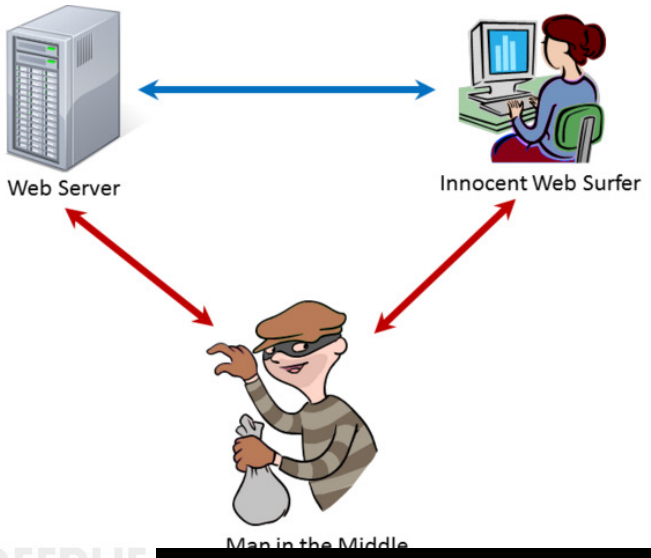
- *Denial of Service (DoS) attacks* are designed to overuse a host, server or network resource to the point where it functionally ceases to provide its services. Depending on the exact nature of the attack, the failure may be temporary or indefinite. *Distributed Denial of Service (DDoS) attacks* involve multiple remote systems being used to simultaneously amass the attack on the targeted resource.

Summary Point

- *Spoofing attacks* are based on changing a device's MAC or IP address to change its apparent identity. Because a TCP/IP packet contains many different headers, attackers can create a TCP/IP packet and send its contents using a false source IP address. When the addressed recipient receives the message, the response generated would be sent to the spoofed address.

Summary Point

- *Man-in-the-middle attacks* involve an attacker creating links to two or more victims so they can intercept messages moving between them and insert new information into them before forwarding them. This is accomplished without either victim realizing the attacker is controlling the communications.



Summary Point

- *Session replay attacks* involve the attacker recording a sequence of IP packets or router commands, manipulating the data in them and then reintroducing them to the router to gain access or cause undesirable actions to be performed.

Summary Point

- *Rerouting attacks* are enabled by an attacker gaining access to the routing tables in a network router and reconfiguring it to redirect IP packets to alternate locations. These types of attacks are prevented by using transmission protocols that require route authentication. They can also be thwarted by employing static routers.

Summary Point

- *Masquerade attacks* involve an attacker manipulating IP packets to create a false IP address so they can gain access to the network or inject false data into it.

Summary Point

- The main defense against IP spoofing attacks is a packet filtering device. *Packet filtering* is the process of passing or blocking network packets based on their source/destination addresses, logical ports, or protocols. Managed switches typically provide filtering configuration options for all of these elements.

Questions?