**EO 001.04.03 – Networking Equipment Reading Assignment**

**What is a router?**

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches.

**How does a router work?**

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks). Just as each plane has a unique destination and follows a unique route, each packet needs to be guided to its destination as efficiently as possible. In the same way that an air traffic controller ensures that planes reach their destinations without getting lost or suffering a major disruption along the way, a router helps direct data packets to their destination IP address.

In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

**What are the different types of routers?**

In order to connect a LAN to the Internet, a router first needs to communicate with a modem. There are two primary ways to do this:

* Wireless router: A wireless router uses an Ethernet cable to connect to a modem. It distributes data by converting packets from binary code into radio signals, then wirelessly broadcasts them using antennae. Wireless routers do not establish LANs; instead, they create WLANs (wireless local area networks), which connect multiple devices using wireless communication.
* Wired router: Like a wireless router, a wired router also uses an Ethernet cable to connect to a modem. It then uses separate cables to connect to one or more devices within the network, create a LAN, and link the devices within that network to the Internet.

In addition to wireless and wired routers for small LANs, there are many specialized types of routers that serve specific functions:

* Core router: Unlike the routers used within a home or small business LAN, a core router is used by large corporations and businesses that transmit a high volume of data packets within their network. Core routers operate at the "core" of a network and do not communicate with external networks.
* Edge router: While a core router exclusively manages data traffic within a large-scale network, an edge router communicates with both core routers and external networks. Edge routers live at the "edge" of a network and use the BGP (Border Gateway Protocol) to send and receive data from other LANs and WANs.
* Virtual router: A virtual router is a software application that performs the same function as a standard hardware router. It may use the Virtual Router Redundancy Protocol (VRRP) to establish primary and backup virtual routers, should one fail.

**What is a network switch?**

A network switch connects devices within a network (often a local area network, or LAN\*) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

**What is the difference between a switch and a router?**

Routers select paths for data packets to cross networks and reach their destinations. Routers do this by connecting with different networks and forwarding data from network to network — including LANs, wide area networks (WANs), or autonomous systems, which are the large networks that make up the Internet.

In practice, what this means is that routers are necessary for an Internet connection, while switches are only used for interconnecting devices. Homes and small offices need routers for Internet access, but most do not need a network switch, unless they require a large amount of Ethernet\* ports. However, large offices, networks, and data centers with dozens or hundreds of computers usually do require switches.

**What is a layer 2 switch? What is a layer 3 switch?**

Network switches can operate at either OSI layer 2 (the data link layer) or layer 3 (the network layer). Layer 2 switches forward data based on the destination MAC address (see below for definition), while layer 3 switches forward data based on the destination IP address. Some switches can do both.

Most switches, however, are layer 2 switches. Layer 2 switches most often connect to the devices in their networks using Ethernet cables. Ethernet cables are physical cables that plug into devices via Ethernet ports.

**What is an unmanaged switch? What is a managed switch?**

An unmanaged switch simply creates more Ethernet ports on a LAN, so that more local devices can access the Internet. Unmanaged switches pass data back and forth based on device MAC addresses.

A managed switch fulfills the same function for much larger networks, and offers network administrators much more control over how traffic is prioritized. They also enable administrators to set up Virtual LANs (VLANs) to further subdivide a local network into smaller chunks.

**What is the difference between a MAC address and an IP address?**

Network switches refer to MAC addresses in order to send Internet traffic to the right devices, not IP addresses.

Every device that connects to the Internet has an IP address. An IP address is a series of alphanumeric characters, like 192.0.2.255 or 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IP addresses act like a mailing address, enabling Internet communications directed at that address to reach that device. IP addresses often change: because there is a limited number of IPv4 addresses, user devices are typically assigned new ones when they form a new connection with a network.

IP addresses are used at layer 3, which means computers and devices all over the Internet use IP addresses for sending and receiving data, no matter which network they are connected to. All IP packets include their source and destination IP addresses in their headers, just as a piece of mail has a destination address and a return address.

In contrast, a MAC address is a permanent identifier for each piece of hardware, somewhat like a serial number. Unlike IP addresses, MAC addresses do not change. MAC addresses are used at layer 2, not layer 3 — which means they are not included in IP packet headers. In other words, MAC addresses are not part of Internet traffic. They are only used inside a given network.

**Network Interface Card (NIC)**

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

**Purpose**

* NIC allows both wired and wireless communications.
* NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
* NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

**Types of NIC Cards**

NIC cards are of two types:

* Internal Network Cards
  + In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).
* External Network Cards
  + In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

**What is a firewall?**

A firewall is a security system that monitors and controls network traffic based on a set of security rules. Firewalls usually sit between a trusted network and an untrusted network; oftentimes the untrusted network is the Internet. For example, office networks often use a firewall to protect their network from online threats.

Firewalls decide whether to allow incoming and outgoing traffic to pass through. They can be built into hardware, software, or a combination of both. The term ‘firewall’ is actually borrowed from a construction practice of building walls in between or through the middle of buildings designed to contain a fire. Similarly, network firewalls work to contain online threats.

**Why use a firewall?**

The primary use case for a firewall is security. Firewalls can intercept incoming malicious traffic before it reaches the network, as well as prevent sensitive information from leaving the network.

Firewalls can also be used for content filtering. For example, a school can configure a firewall to prevent users on their network from accessing adult material. Similarly, in some nations the government runs a firewall that can prevent people inside that nation-state from accessing certain parts of the Internet.

**Ethernet Cables**

An Ethernet cable resembles a traditional phone cable but is larger and has more wires. Both cables share a similar shape and plug, but an Ethernet cable has eight wires, while phone cables have four. Ethernet cable connectors are also larger.

Ethernet cables come in many different colors, but phone cables are usually grey.

Ethernet cables plug into Ethernet ports, which are larger than phone cable ports. An Ethernet port on a computer is accessible through the Ethernet card on the motherboard. This port is usually on the back of a desktop computer, or on the side of a laptop.

**Types of Ethernet Cables**

Ethernet cables support one or more industry standards including Category 5 and Category 6. Most technicians refer to these standards as CAT5 and CAT6, respectively. Because of this, many online stores that sell network cables use this abbreviated language as well.

Ethernet cables are manufactured in two basic forms:

* Solid Ethernet cables offer slightly better performance and improved protection against electrical interference. They're also commonly used on business networks, wiring inside office walls, or under lab floors to fixed locations.
* Stranded Ethernet cables are less prone to physical cracks and breaks, making them more suitable for travelers or in-home network setups.

A crossover cable is a type of Ethernet cable that connects two computers to each other. By contrast, most Ethernet cables connect one computer to a router or switch.

**Limitations of Ethernet Cables**

A single Ethernet cable has a maximum distance capacity, meaning the cable has an upper limit as to how long it can be before there is a signal loss (called attenuation). This problem results because the electrical resistance of a long cable affects performance.

Both ends of the cable should be close enough to each other to receive signals quickly, and far enough away from outside electrical interference to avoid interruptions. However, this precaution doesn't limit the size of a network, because hardware like routers or hubs can join multiple Ethernet cables together on the same network. This distance between the two devices is called the network diameter.

The maximum length of a CAT5 cable, before attenuation occurs, is 100m (328ft). CAT6 can go up to 700 feet. Ethernet cables can be longer but may suffer from signal loss, especially if they pass near large electrical appliances.

A short cable may suffer from reflection. However, some people have reported no problems with cable lengths as low as 4 inches.

Different types of RJ-45 connectors serve different purposes. One type, designed for use with stranded cables, is incompatible with solid cables. Other types of RJ-45 connectors may work with both stranded and solid cables.