CCNA Networking Fundamentals Course

Course tutor: David Bombal, Udemy

What is a Network?

- **Computer Network**: digital telecommunications network for sharing resources between nodes, which are computing devices, which share a common telecommunications technology, e.g. printer, file sharing
- **Sneakernet**: Walking from one computing device to another with the data to be shared on a portable data storage device. (humorous)
- **Basic Network**: Copper wires, ethernet cables, coaxial cable, optical (fibre optic) cable, radio waves; wireless, wifi, bluetooth

What is a Server?

- A **Server** is a computer program or computing device that provides functionallity to other programs or devices, called 'clients'.

What is a Client?

- A **Client** is a piece of computer hardware or computer software that accesses a service made available by a server.

What is an NIC?

- A **Network Interface Controller** (also know as a network interface card, network adapter, LAN adapter, or physical network interface), is a computer hardware component that connects a computer to a computer network.

What is a MAC address?

- A **Media Access Control** address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment, common in most IEEE 802 networking technologies (Ethernet, Wifi, Bluetooth).
- MAC addresses are primarily assigned by the device manufacturers. Often refered to as, *the burned-in address*, the ethernet hardware address, hardware address, and physical address.
- MAC addresses can be recognised as six pairs of hexadecimal numbers, typically separated by hyphens, colons, or without a separator. (sometimes three sets of four hex digits with a separator, often a period).
- Each MAC address can be stored in hardware, such as the divices' read-only memory, or my a firmware mechanism. Many interface devices, however, support changing their MAC address.
- Typically, the MAC address includes the manufacturers' organisationally unique identifier (OUI). AC addresses are formed according to the principles of two numbering spaces based on Extended Unique Identifiers (EUI) managed by the Institute of Electrical and Electroncs Engineers (IEEE): EUI-48.

What is modulation?

- In electronics and telecommunications, modulation is the process of varying one or more properties of a periodic waveform, known as a carrier signal, with a modulating signal that typically contains infomation to be transmitted. Most radio systems of the 20th century used frequency modulation (FM) or amplitude modulation (AM) for radio broadcast.
- A modulator is a device that performs modulation. A demodulator (sometimes refered to a detector or demod) is a device that performs demodulation, the inverse of modulation. A modem (from MOdulator-DEModulator) can perform both operations.

What is a bus network?

- A *bus* network is a network topology in which nodes are directly connected to a common half-duplex link called a bus. (typically a coaxial cable). (10BaseT networks typically connect each device to a central *hub*, in one of several arrangent topologies, star, loop, ring, etc).
- A host on a bus network is called a station. In a bus network, every station will receive all network traffic, and the traffic generated by each station has equal transmisson priority.
- A bus network forms a single network segment and collision domain. In order for nodes to share a bus, they use a medium access control technology such as carrier-sense multiple access (CSMA) or a bus master.
- If any link or segment of the bus is severed, all network transmisson may fail due to signal reflection caused by the lack of electrical termination.
- Some types of electrical bus cables: 10Base5, 10Base2. Some types of non-electrical transmisson: fibre optics, free-space optical.

What is DHCP?

- The *Dynamic Host Configuration Protocol* (DHCP) is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network do they can communicate with other IP networks.
- An IP address must be manually assigned to a computer or other device on a network if a DHCP server is absent.

What is a Repeater?

- In telecommunications, a repeater is an electronic device that receives a signal and retransmits it.
- There are different types of repeaters. Some broadcast the identical signal, but alter its transmission method, e.g. a different frequency or baud rate.
- Different types of repeaters:
  - Telephone repeater - an amplifier in a telephone line.
  - Optical repeater - optoelectrical circuit for amplifying the light beam in an optical fibre cable.

    - Radio repeater - receives and retransmits a radio signal.
- Repeaters are use to extend transmissions over a larger area, and to transmit around or over obstacles, e.g. mountains, buildings.

What is a Hub?

- A hub, also refered to as, an ehternet hub, network hub, repeater hub, multiport repeater, is a network hardware device for connecting multiple Etherner devices together, so that they act a single network segment.
- A hub has multiple input/output (I/O) ports. A signal introduced at the input of any port appears at the output of every port other than the original incoming port.
- A hub operates at the physical layer (layer 1) of the OSI or TCP/IP model. A repeater hub also participates in collision detection, forwarding a jam signal to all ports if it detects a collision.

What is a Switch?

- A network *switch* is a networking hardware device that connects devices on on a computer network. It makes these connections by using frame switching to receive and forword data to the destination device.
- A network switch is a multiport network bridge the uses MAC addresses to forword data at layer 2, the data-link layer of the OSI or TCP/IP model. Some switches are also able to forward data at the network layer, layer 3 of the OSI or TCP/IP, by additionally incorporating routing functionality. These types of switches are commonly known as layer-3 switches or multilayer switches.

What is a Router?

- A **Router** is a networking device that forwards data packets between computer networks.
- Routers perform the traffic directing functions on the internet. Data sent through the internet, such as email or a web page, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork, e.g. the internet, until it reaches its destination node.
- Routers are typically connected to two or more data lines from different IP networks. When a data packet is received at one of the lines, the router uses the network address infomation in the packet header to determine the ultimate destination. Then, using infomation in its routing table or routing policy, it directs the packet to the next network on its journey.

What is a LAN?

- A **Local Area Network** (LAN) is a computer network that interconnects computers and computing devices within a limited area such as a residence, an educational institution, or office building, etc.
- Ethernet and Wi-Fi are the two most common technologies in use for local area networks.

What is a WAN?

- A **Wide Area Network** (WAN) is a telecommunications network that extends over a large geographical area for the primary purposr of computer networking.

- The textbook difinition of a WAN is a computer network spanning regions, countries, or even the world.

What is a Firewall?

- A **Firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted internal network and untrusted external networks, such as the Intrnet.
- Firewalls can be categorised as either network firewalls or host-based firewalls.
- Network firewalls filter traffic between two or more networks and run on network hardware.
- Host-based firewalls run on host computers and control network traffic in and out of those machines.

What is an IDS?

- An **Intrusion detection system** (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.
- Any intrusion activity or violation is typically reproted either to an administrator or collected centrally using a security infomation and event management (SIEM) system.

What is an IPS?

- **Intrusion prevention systems** (IPS), also known as Intrusion detection and prevention systems (IDPS), are network security appliances that monitor network or system activies for malicious activity.
- The main functions of intrusion prevention systems are to identify malicious activity, log infomation about this activity, report it, and attempt to block or stop it.