# Hasan Hashim

11/02/2020

# Week 9 Readings

**Networking Overview:**

Two or more machines that have the capacity to connect with each other and exchange information are a network as it applies to computers. A network helps computer users to exchange files, connect by email, browse the web, share a printer, modem, or scanner, and access files and applications. Based on the scale and form of networks, networks can be broken into major groups. The different types of networks are:

1. Personal area network (PAN): Personal gadgets that can connect in close proximity via a wired or wireless network, such as a keyboard, mouse, Computer, cell phone, laptop, desktop, handheld screen, or pocket video games. The use of a PC with a Bluetooth keyboard is an example of a PAN.
2. Local area network (LAN): A collection of devices that can share resources, such as a room, home, or house, in a single location. Ethernet is the most common LAN form. Wired or wireless may be a LAN. One example of a LAN is the computers in a networked classroom.
3. Metropolitan area network (MAN): Connectivity inside the same city between locations. Multiple LANs are linked by a MAN. MANs can use fiber-optic cables or can be cellular. An example of a MAN is several college campuses linked to a city.
4. Wide area Network (WAN): On a broad geographic scale, communication between LANs. A WAN is two remote areas that have links as part of the business network between them.
5. Wireless LAN (WLAN): A wireless network that consists of an entry point, like notebooks, tablets, and smartphones, and other wireless cameras. A wireless network can be short-range, such as where Bluetooth is used, or provide broader reach, such as with a home or business wireless network. To link devices between two buildings, wireless bridges could be used.
6. Wireless WAN (WWAN): Wireless networking, using a combination of systems such as cellular or WiMAX, for a wider geographic region.
7. Wireless mesh networks (WMN): In emergency scenarios, wireless communication is extremely useful because WMNs do not require standard access points, transfer data between peer radio devices, and can be used over wide distances.

**Network Topologies:**

How a network is wired is the electrical network topology. Bear in mind that there might be variations of these topologies for a big organization. The most common LAN form is Ethernet. Each network unit, usually a hub or a switch, connects to a central device. Two or three RJ-45 network jacks comprise both the hub and the switch. Not as clever as a turn, the center is. When it comes through the switch, the switch takes a look at each data frame. This can not be achieved by the hub. Often, since they are identical in design, you would look at the model number to know the difference between a hub and a switch.

Collisions can occur while a hub is used, since two devices may concurrently position data on the network. For a period of time, each system needs to postpone transmitting data, and transmissions will then occur again. It is inadequate to use of bandwidth. A switch prevents collisions and is a safer system to use on the network. It is possible to either control or unmanaged switches. An IP address has been allocated to a controlled switch and can be installed, updated, and tracked via a corporate network. An unmanaged switch simply links devices such that a network is created. It would be like a switch that you may have in a wired network for a home or small business. Star topologies can be troubleshot quickly. The issue is with the system, cable, or port on the hub/switch if one network device goes down. The fault is most likely with the system that joins them together (the hub or switch) if a group of network devices goes down.

**The OSI Model:**

The International Organization for Standardization ( ISO) has developed a protocol called the OSI (Open Networks Interconnect) model for network communications. The OSI model is a standard for the network-wide transfer of information. The model sets many rules, including (1) how the multiple communication media are organized and interconnected, (2) how network devices interact with each other using different languages, (3) how another network system is contacted by a network device, (4) how and where data is transmitted over the network, (5) how data is transmitted to the correct computer, and (6) how it is understood if the network data has been correctly obtained. A collection of rules must perform all of these functions, and the OSI model provides a framework into which these rules match.

Can you imagine a generic model for building a car? This model would state that you need some means of steering, a type of fuel to power the car, a place for the driver to sit, safety standards, and so forth. The model would not say what type of steering wheel to put in the car or what type of fuel the car must use but would just be a blueprint for making the car. The OSI model is a similar model in networking.

Networking is broken into various layers by the OSI model so that it is easier to understand (and teach). Manufacturers are often aided by splitting the network into different layers. If a certain vendor decides to render a network interface running on Layer 3, the manufacturer just needs to do with Layer 3. This division makes it even easier for networking technology to emerge. It is also possible to teach network principles at each level using a layered model as a separate network feature.

There are 7 OSI model layers starting front the top and going down: application, presentation, session, transport, network, data link, and physical.

The layer below it (except for the physical layer that is at the bottom) is used by each layer of the OSI model. Each layer gives the layer above it some feature. For eg, after first passing through the physical layer, it is not possible to reach the data link layer. The physical and data link layers must be used first if coordination is to be done at Layer 3 (the network layer).

Each of the seven layers of the OSI model performs a specific role and communicates with the layers that surround it. The actual transmission of data across the network is done by the bottom three layers. The top four levels, particularly in a multitasking operating system environment, handle the ins and outs of delivering effective data transmission between computers and their individual processes.

**The TCP/IP Model:**

A network protocol is a language for transmitting data. A suite of protocols is a set of protocols intended to work together. The protocol set used on networks today is the Transmission Control Protocol / Internet Protocol (TCP / IP). It is the most common protocol for a network that is needed when accessing the Internet. TCP / IP is used by most businesses and homes as a standard protocol. Many protocols, including Transmission Control Protocol ( TCP), Internet Protocol ( IP), Dynamic Host Configuration Protocol ( DHCP), File Transfer Protocol ( FTP), and Hypertext Transfer Protocol ( HTTP) are included in the TCP / IP protocol suite, to name a handful. When TCP / IP-based protocols are used, the TCP / IP model explains how communication flows through the device. In comparison to the seven layers in the proposed OSI model, the TCP / IP model has only four layers. It is easier to research and understand networking from a TCP / IP model viewpoint because there are fewer layers and because the TCP / IP model consists of protocols that are in production.

**Network Addressing:**

Usually, network adapters have two types of addresses allocated to them: a MAC and an IP address. A MAC address is a special 48-bit integer that is burned and represented in hexadecimal on a chip placed on a NIC. For any device on the network, the MAC address is special. However, given that the first 24 bits reflect the maker, the MAC address has no scheme for it. As a Layer 2 address or a physical address, the MAC address is known. The IP address is a much more organized means of addressing a computer and is often known as a Layer 3 address in comparison to the OSI network layer. There are two IP address types: IPv4 (IP version 4) and IPv6 (IP version 6). IPv4 is the most common IP address used on LANs. An IPv4 address is a 32-bit integer entered into the initialization parameters of a NIC. This address is used to connect separate networks to each other and to access the Internet.

IPv6 addresses have a length of 128 bits and are shown in hexadecimal format. Corporate computers and certain Internet service providers use IPv6 addresses, and further IPv4 to IPv6 conversions are coming soon. Today, machines have both an IPv4 and an IPv6 address allocated to them. fe80::13e:4586:5807:95f7 is an example of an IPv6 address. 16 bits are expressed in each sequence of four digits. There are just three digits anywhere, such as 13e, a "silent" zero is left omitted in the front (013e). A string of zeros has been omitted anywhere there are double colons: (:). An IPv6 address only makes one set of double colons. IPv6 addresses are allocated to a lot of network cards, even though IPv6 is not used.

**More IPv4 Addressing:**

An IP address is divided into two main parts: the number of the network and the number of the host. The network number is the component of an IP address representing the network on which the device is situated. There is the same network number on all machines on the same network. The host address (or host component of the address) reflects a single device on the network. Both machines on the same network have identical host numbers; they would not be able to connect if they did not. The number of bits that reflect the network number and the host number depends on which class of IP address is used. With Class A IP addresses, the network component is represented by the first 8 bits (the first number), and the host number by the remaining 24 bits (the last three numbers). The first 16 bits (the first two numbers) represent the network part, with Class B IP addresses, and the remaining 16 bits (the last two numbers) represent the host number. With Class C IP addresses, the network part represents the first 24 bits (the first three numbers), and the host number represents the remaining 8 bits (the last number).

VLANs:

The use of VLANs is another way of building networks. The tool used to build several networks within a switch is a virtual local area network (VLAN). IP phones, PCs, and printers, for example, usually connect to a switch, and organizations that have switches that support VLANs prefer to build independent networks in a single area for certain kinds of devices or devices. An example that mentions in the book was if you had two IP phones, three PCs, and a printer connected to the same switch, the switch ports connecting to the IP phones as VLAN 17, the switch ports connecting to the PCs as VLAN 18, and the port connecting to the printer as VLAN 19 could be configured. As part of the IP addressing, the IP addressing mechanisms used within an organization usually provide the VLAN number. Note in Figure 13.34 that the IP addresses of phones are 192.168.17.x (where x is a unique number) and that the IP addresses of PCs are 192.168.18.x. The printer has 192.168.19.3 IP addresses.

Subnet Masks:

You must also assign a subnet mask in addition to assigning the device an IP address. The (sometimes simplified to mask) subnet mask is a number used by a machine to decide which part of the IP address is represented by the network and which part is represented by the host. The default subnet mask is 255.0.0.0 for a Class A IP address, the default subnet mask is 255.255.0.0 for a Class B IP address, and the default subnet mask is 255.255.255.0.0 for a Class C IP address. Subnet masks are often shown with a slash (/) followed by a number. How many consecutive 1s are in the subnet mask is expressed by the sum? For eg, /8 indicates that in the subnet mask, there are eight consecutive 1s, or 11111111.00000000.00000000.000000000. Note that after the eight 1s are seen, the subnet mask is all 0s. This is regarded as displaying in a prefix notation format the subnet mask. Network documents may have to be listened to by a technician, and the subnet mask to be used would be displayed in the prefix notation format. For a Class A address, the prefix notation format is /8, Class B is /16 and Class C is /24. It is not always appropriate to obey classic boundaries for a subnet mask. Often, a subnet mask that looks like the following samples may be used by a technician: 255.255.254.0 or /23, 255.255.255.192 or /26, and 255.255.255.240 or /28. These are known as subnet masks of classless inter-domain routing (CIDR). CIDR (pronounced 'cider') is an IP address allocation system focused on the number of host addresses needed by a given network. CIDR subnet masks are numbers that are distinct from the usual 255.0.0.0, 255.255.0.0, and 255.255.255.0 subnet masks since the subnet mask specifies where the network portion stops and where the host portion starts.

**Network Troubleshooting**

Determining how many computers are affected is one step in troubleshooting a network. For starters, if only one computer is unable to communicate through a network, it would be treated differently than if it is unable to communicate between many (or all) computers on a network. You should try another cable if a network port is suspicious or use a loopback connector to verify the port. By using a basic survey, the best way to assess how many computers are having problems is. Since most machines use TCP / IP, the ping command is one method that can be used for checking.

The Ping Command:

The ping command can be used to verify (if you assume no connection or sporadic connectivity) connectivity across the network.

The IPconfig Command:

Use the ipconfig command from the Windows prompt, or the ifconfig command from Linux or macOS, to display the latest IP setup on a Windows device. If all are mounted, the ipconfig /all command can be used to access all wired and wireless NICs. Use the ipconfig /release command if a network computer does not receive an IP address properly from the DHCP server. Then give the order ipconfig /renew. Since a DHCP server is unavailable, a computer receiving an APIPA (IPv4) or link-local (IPv6) address is a symptom of this. Make sure the appliance is actually configured for DHCP as well. On Windows-based computers, a warning occurs when the same IP address has been manually assigned to two devices. Notice that this isn't achieved for all operating systems and/or computers. For any duplicate IP addresses that cause an IP address dispute, search any computer that has a manually installed IP address.

* How would you classify Champlain's network (for example, is it a PAN, LAN, or WAN)? Justify your answer.

I would say it is WAN because I feel it is a wide area network and also it connected between the LANs.

* Between the OSI and TCP/IP Model, which one seems more useful for describing networks? Justify your answer.

It helps to direct manufacturers and engineers so that they can communicate with the digital connectivity devices and software applications they build and provide a simple structure that defines the roles of a network or telecommunications system.

* Suppose Champlain College was given a Class A network ID for its network (i.e., it had 224 addresses to assign to computers). Give one reason why this would be a good thing, and one reason why this might be a bad thing.

Champlain will have up to 16 million hosts to use which a good thing. It has 8 bits for the network id and 24 for the host id. It has only 8 bits for a network id.