In these note, you will read about the responsibilities of the Internet Protocol (IP) and both IPv4 and IPv6 addresses.

During the late 1960s, a branch of the U.S. government titled the advanced research projects agency, also known as ARPA, created one of the first country wide area packet switched network, known as ARPANET. Selected universities, military bases, and government labs were allowed to use the ARPANET for services such as electronic mail, file transfer, and remote login.

Backbone was capable of supporting 56 kbps transmission speeds and eventually became financed by the National Science Foundation (NSF). Today's present Internet is a vast collection of thousands of networks and their attached devices.

The Internet depends on many protocols to provide a variety of services and support. Many protocols are necessary. The most common protocols used are:

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)

Recall the layers of the TCP/IP protocol suite that you learned about earlier in this course. The layers are designed so that the Internet user who needs to use the application, such as email, requires the use of the application layer; which in turn requires the use of the transport layer; which requires the use of the network layer; which requires access to the network access layer. In other words, the layers build on one another in this hierarchy, and the user is not exposed to the details of those layers with which the user does not have direct contact.

The protocols that reside at the network layer in the TCP/IP protocol suite are called the Internet Protocol or IP. IP’s primary function is to perform the routing necessary to move data packets across the Internet.

The Internet protocol provides a connectionless data transfer service over heterogeneous networks by passing and routing IP datagrams. An IP datagram is essentially another name for a data packet. To be passed and routed on the Internet, all IP datagrams that are passed down from the transport layer to the network layer are encapsulated with an IP header that contains the necessary information to transmit the packet from one network to another.

There are currently two versions of IP: IP Version 4 and IP Version 6.

- IP Version 4, which has been in existence since the early 1980s, is currently the most commonly used version.
- IP Version 6 was introduced in 1998 and has been slow to take off, but that won’t always be the case. It is now starting to see a substantial move towards replacing Version 4.

The Internet Protocol Version 4 uses a 32 bit IP initial source and final destination address of the datagram. Routing decisions are made based on the 32-bit destination address. A 32 bit address uniquely defines a connection to the Internet – usually a workstation or device.

Internet Protocol Version 4 allows a router to break or fragment a large datagram into smaller fragments so it will fit into the next network. It may determine that the current datagram has been hopping around the network too long and delete it. The time to live field indicates how long a particular datagram is allowed to live, or bounce, from one router to another within the system.

Think of the IP address as a logical address, possibly temporary, while the 48-bit address on every NIC is the physical, or permanent, address. To make Internet protocol version 4 addresses a little easier for humans to understand, these 32 bit binary addresses are represented by a dotted decimal notation. This
dotted decimal notation is created by converting each 8 bit string of the 32 bit IP address into decimal equivalent.

When Internet protocol and the Internet protocol address were created in the 1960s, an IP address belonged to a particular class; and it was based on 5 different classes. This type of addressing was called classful addressing. There are basically five types of IP addresses: Classes A, B, C, D, and E.

There are 128 Class A address or networks. Each class A address can have over 16 million hosts or computers. Clearly, 128 is not very many networks; in fact, all 128 class A addresses were assigned many years ago.

Class B addresses allow 16384 net ids or networks each supporting over 65536 host ids. This means that each of the 16 thousand networks can have 65536 host computers attached to it.

Class C addresses allow for 2,097,152 net ids or networks and 256 host ids. For the class C address type, the number of host computers allowed is so small that it can only accommodate the smallest networks.

Class D addresses are available for networks that allow multicasting of messages. IP multicasting is the capability of a network server to transmit a data stream to more than one host at a time. Although IP multicasting has some very good advantages, it suffers from the lack of security.

The basic idea behind subnet masking is to take the host id portion of an IP address and divide it into subnet id and host id. This approach becomes useful when you have a large number of IP addresses to manage. By using this approach, a company can take a large number of host ids and break them into subnets. Each subnet can then support a smaller number of hosts.

Today, IP addresses are considered classless addresses. With classless addressing, companies or users do not apply for particular class of addresses. Instead, companies will get their IP addresses from an Internet service provider (ISP). Most ISPs have already applied for a large number of IP addresses and are willing to lease those addresses to companies.

When the Internet Protocol was created in the 1960s, there were far fewer users of the Internet and the telecommunication lines used to support the high speed network were not as fast or error free as they are today. Also, the application transmitted over the Internet involves smaller data packets and there was not a high demand to transmit in real time. As the demands of the Internet began to grow, the designers decided that it was time to create a more modern Internet protocol that takes advantages of the current technology. Therefore, Internet protocol version 6 was created.

IPv6 calls for addresses to be 128 bits long; This gives us virtually unlimited addresses. The IPv6 IP header is much simpler. It contains a priority field that could be useful to assign a priority to one or more packets, causing a data stream with higher priority to get serviced more quickly than a lower priority packet. The creators of IPv6 felt that most of the networks operating today could handle packets of a very large size, and it is no longer necessary to break or fragment a packet into smaller pieces.

IPv6 addresses are 128-bits in size. $2^{128}$ is a very large number! This provides a virtually unlimited source of IP address. The size alone makes it challenging simply to reference them. These IP addresses are usually written in hexadecimal form, where each four bit quantity is replaced by a hexadecimal digit from zero to one. They are also classless addresses, similar to IPv4 addresses.