Lesson 3
TCP Protocol Suite & IP Addressing

Introduction to TCP/IP

Specific objectives

By the end of the lesson the learner should be able to:

- ✓ **Describe the function of the TCP/IP layers**
- ✓ **Distinguish between MAC address and IP addresses**

The Internet was developed to provide a communication network that could function in wartime. Although the Internet has evolved from the original plan, it is still based on the TCP/IP protocol suite. The design of TCP/IP is ideal for the decentralized and robust Internet. Many common protocols were designed based on the four-layer TCP/IP model.

Any device on the Internet that wants to communicate with other Internet devices must have a unique identifier. The identifier is known as the IP address because routers use a Layer 3 protocol called the IP protocol to find the best route to that device.

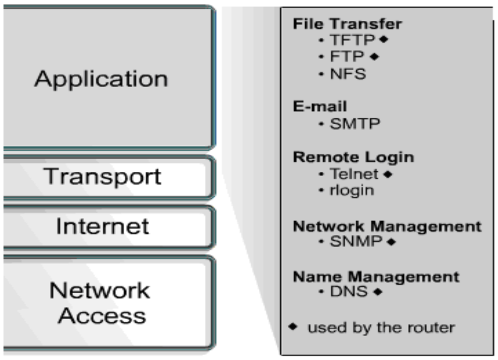
In addition to the physical ***MAC address***, each computer needs a ***unique IP address*** to be part of the Internet. This is also called the logical address. There are several ways to assign an IP address to a device. Some devices always have a static address. Others have a temporary address assigned to them each time they connect to the network. When a dynamically assigned IP address is needed, a device can obtain it several ways.

The TCP/IP model has become the standard on which the Internet is based.

The four layers of the TCP/IP model are:

- ➢ Application layer
- ➢ Transport layer
- ➢ Internet layer
- ➢ Network access layer

Functions of the TCP/IP Application Layer



The ***Application Layer*** handles high-level protocols, representation, encoding, and dialog control. The ***TCP/IP protocol*** suite combines all application related issues into one layer. It ensures that the data is properly packaged before it is passed on to the next layer.

The following protocols functions operate at the application layer:

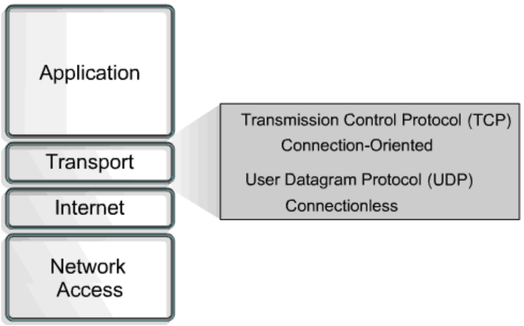
- **File Transfer Protocol (FTP)** - FTP is a reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP. It supports bi-directional binary file and ASCII file transfers.
- **Trivial File Transfer Protocol (TFTP)** - TFTP is a connectionless service that uses the User Datagram Protocol (UDP). TFTP is used on the router to transfer configuration files and Cisco IOS images, and to transfer files between systems that support TFTP. It is useful in some LANs because it operates faster than FTP in a stable environment.
- **Network File System (NFS)** - NFS is a distributed file system protocol suite developed by Sun Microsystems that allows file access to a remote storage device such as a hard disk across a network.
- **Simple Mail Transfer Protocol (SMTP)** - SMTP administers the transmission of e-mail over computer networks. It does not provide support for transmission of data other than plain text.
- **Telnet** - Telnet provides the capability to remotely access another computer. It enables a user to log into an Internet host and execute commands. A Telnet client is referred to as a local host. A Telnet server is referred to as a remote host.
- **Simple Network Management Protocol (SNMP)** - SNMP is a protocol that provides a way to monitor and control network devices. SNMP is also used to manage configurations, statistics, performance, and security.
- **Domain Name System (DNS)** - DNS is a system used on the Internet to translate domain names and publicly advertised network nodes into IP addresses.

Internet and transport layer specifications such as IP and TCP as well as specifications for common applications.

The Transport Layer

The transport layer:

- Provides a logical connection between a source host and a destination host
- Protocols segment and reassemble data sent by upper-layer applications into the same data stream, or logical connection, between end points
- Sends data packets from a source to a destination through the cloud.
- The primary duty of the transport layer is to provide end-to-end control and reliability as data travels through the network
- Also defines end-to-end connectivity between host applications.
- Transport layer protocols include TCP and UDP.



Transport Layer Protocol

The reliability is accomplished through the use of:

- **Sliding windows**
- **Sequence numbers**
- **Acknowledgments**

The functions of TCP and UDP are as follows:

- Segment upper-layer application data
- Send segments from one end device to another

The functions of TCP are as follows:

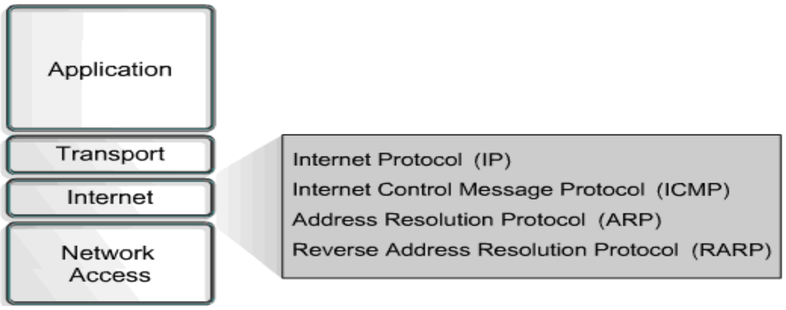
- Establish end-to-end operations
- Provide flow control through the use of sliding windows
- Ensure reliability through the use of sequence numbers and acknowledgments

The TCP/IP Internet Layer

The purpose of the Internet layer is to select the best path through the network for packets to travel. Best path determination and packet switching occur at this layer.

The main protocol that functions at this layer is IP.

Internet Layer Protocols


Application
Transport
Internet
Network Access
Internet Protocol (IP)
Internet Control Message Protocol (ICMP)
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)

The purpose of the Internet layer is to select the best path through the network for packets to travel

The following protocols operate at the Internet layer:

- **IP** provides connectionless, best-effort delivery routing of packets. IP is not concerned with the content of the packets but looks for a path to the destination.
- **Internet Control Message Protocol** (ICMP) provides control and messaging capabilities.
- **Address Resolution Protocol** (ARP) determines the data link layer address, or MAC address, for known IP addresses.
- **Reverse Address Resolution Protocol** (RARP) determines the IP address for a known MAC address.

IP performs the following operations:

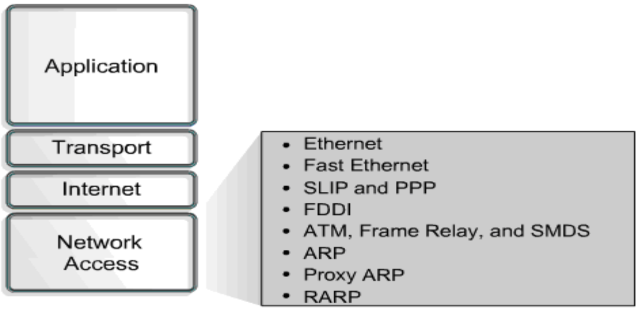
- Defines a packet and an addressing scheme
- Transfers data between the Internet layer and network access layer
- Routes packets to remote hosts

IP is sometimes referred to as an ***unreliable protocol***. This does not mean that IP will not accurately deliver data across a network. IP is unreliable because it does not perform error checking and correction. That function is handled by upper layer protocols from the transport or application layers.

TCP/IP Network Access Layer

The **network access layer** allows an IP packet to make a physical link to the network media. It includes the LAN and WAN technology details and all the details contained in the OSI physical and data link layers. Network access layer protocols also **map IP addresses to physical hardware addresses** and encapsulate IP packets into frames. The network access layer defines the physical media connection based on the hardware type and network interface.

Network Access Protocols

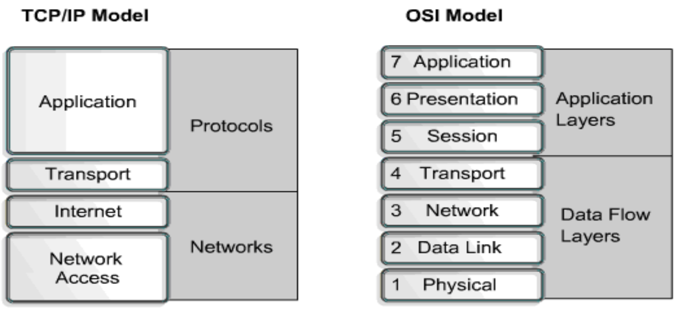


ARP and RARP work at both Internet and Network access layers

Drivers for software applications, modem cards, and other devices operate at the network access layer.

The network access layer defines the procedures used to interface with the network hardware and access the transmission medium. Modem protocol standards such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) provide network access through a modem connection. Many protocols are required to determine the hardware, software, and transmission-medium specifications at this layer.

Comparison of the OSI model and the TCP/IP model



The OSI and TCP/IP models have many similarities:

- Both have layers.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.

Here are some differences of the OSI and TCP/IP models:

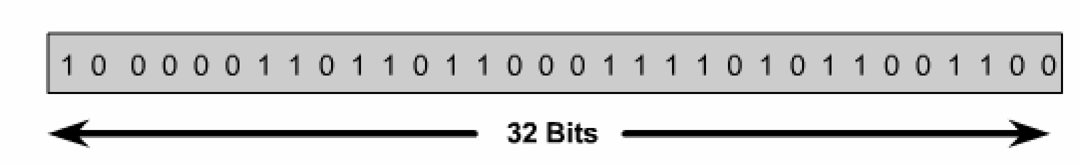
- TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- TCP/IP combines the OSI data link and physical layers into its network access layer.
- TCP/IP appears simpler because it has fewer layers.
- When the TCP/IP transport layer uses UDP it does not provide reliable delivery of packets. The transport layer in the OSI model always does.

> The Internet was developed based on the standards of the TCP/IP protocols. The TCP/IP model gains credibility because of its protocols. The OSI model is not generally used to build networks. The OSI model is used as a guide to understand the communication process

IP addressing

For any two systems to communicate, they must be able to identify and locate each other.

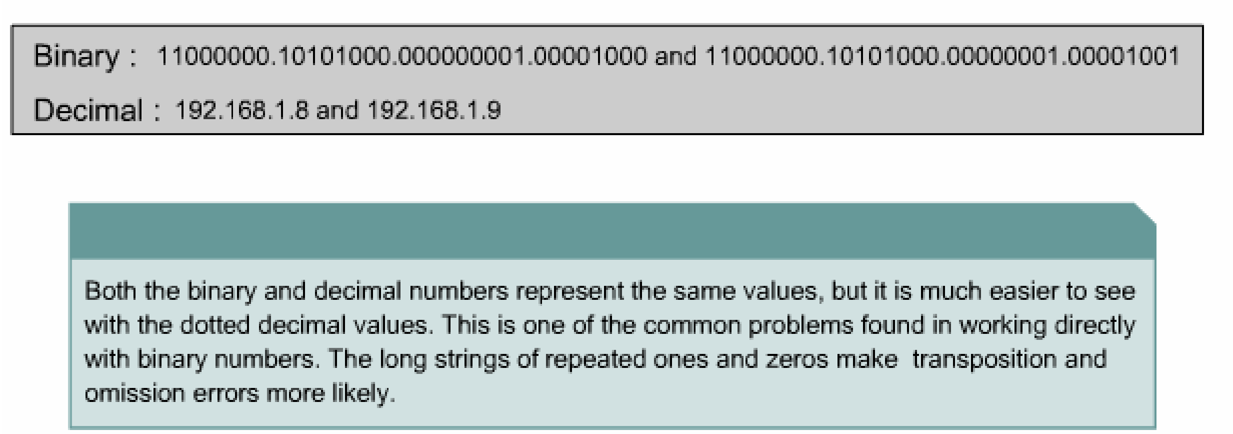
Each computer in a TCP/IP network must be given a unique identifier, or IP address. This address, which operates at Layer 3, allows one computer to locate another computer on a network. All computers also have a unique physical address, which is known as a MAC address. These are assigned by the manufacturer of the NIC. MAC addresses operate at Layer 2 of the OSI model.



An IP address is a 32-bit sequence of ones and zeros. Figure above shows a sample 32-bit number. To make the IP address easier to work with, it is usually written as four decimal numbers separated by periods. For example, an IP address of one computer is 192.168.1.2. Another computer might have the address 128.10.2.1. This is called the dotted decimal format. Each part of the address is called an octet because it is made up of eight binary digits. For example, the IP address 192.168.1.8 would be:

11000000.10101000.00000001.00001000 in binary notation.

The dotted decimal notation is an easier method to understand than the binary ones and zeros method. This dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used. Each octet ranges from 0 to 255.



Binary : 11000000.10101000.000000001.00001000 and 11000000.10101000.00000001.00001001

Decimal : 192.168.1.8 and 192.168.1.9

Both the binary and decimal numbers represent the same values, but it is much easier to see with the dotted decimal values. This is one of the common problems found in working directly with binary numbers. The long strings of repeated ones and zeros make transposition and omission errors more likely.

Both the binary and decimal numbers in Figure above represent the same values. However, the address is easier to understand in dotted decimal notation. This is one of the common problems associated with binary numbers. The long strings of repeated ones and zeros make errors more likely.

IPv4 addressing

A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network.

Every IP address also has two parts. The first part identifies the network where the system is connected and the second part identifies the system.

This kind of address is called a hierarchical address, because it contains different levels. An IP address combines these two identifiers into one number. This number must be a unique number, because duplicate addresses would make routing impossible. The first part identifies the system's network address. The second part, called the host part, identifies which particular machine it is on the network.

Identifying Address Classes

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127*	8
Class B	10	128- 191	16
Class C	110	192 - 123	24
Class D	1110	224 - 239	28

*** 127.x.x.x address range is reserved as loop back address**

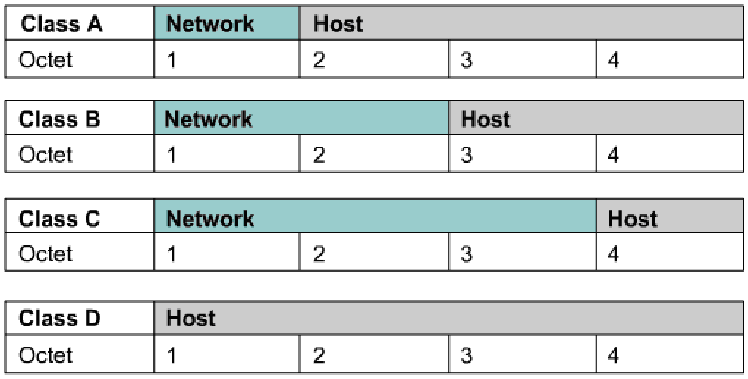
Address Class	Number of Networks	Number of Hosts per Network
A	126	16,777,216
B	16,384	65,535
C	2,097,152	254
D	N/A	N/A

IP addresses are divided into classes to define the large, medium, and small networks. Class A addresses are assigned to larger networks. Class B addresses are used for medium-sized networks, and Class C for small networks. The first step in determining which part of the address identifies the network and which part identifies the host is identifying the class of an IP address.

The Five IP Address Classes

Classful Addressing

To accommodate different size networks and aid in classifying these networks, IP addresses are divided into groups called classes. This is known as **classful addressing**. Each complete 32-bit IP address is broken down into a network part and a host part. A bit or bit sequence at the start of each address determines the class of the address. There are five IP address classes as shown in Figure below.



Class A	Network	Host		
Octet	1	2	3	4

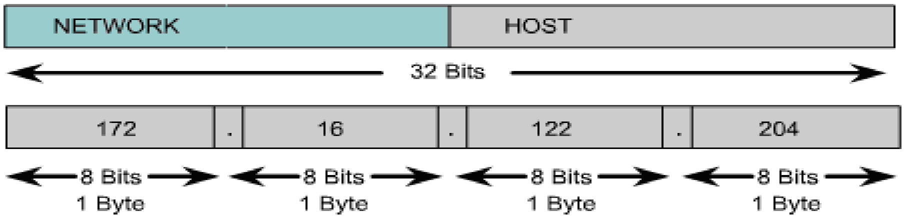
Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

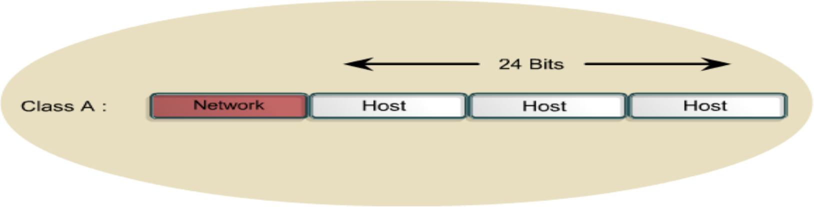
Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.

The Class A address was designed to support extremely large networks, with more than 16 million host addresses available. Class A IP addresses use only the first octet to indicate the network address. The remaining three octets provide for host addresses.



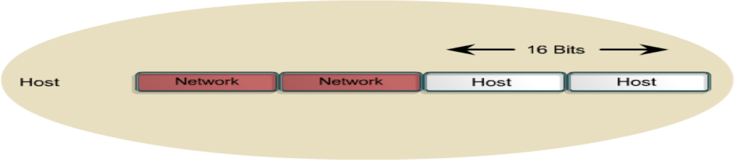
An IP address will always be divided into a network and host portion. In a classful addressing scheme, these divisions take place at the octet boundaries.

The first bit of a Class A address is always 0. With that first bit a 0, the lowest number that can be represented is 00000000, decimal 0. The highest number that can be represented is 01111111, decimal 127. The numbers 0 and 127 are reserved and cannot be used as network addresses. Any address that starts with a value between 1 and 126 in the first octet is a Class A address.



The 127.0.0.0 network is reserved for loopback testing. Routers or local machines can use this address to send packets back to themselves. Therefore, this number cannot be assigned to a network.

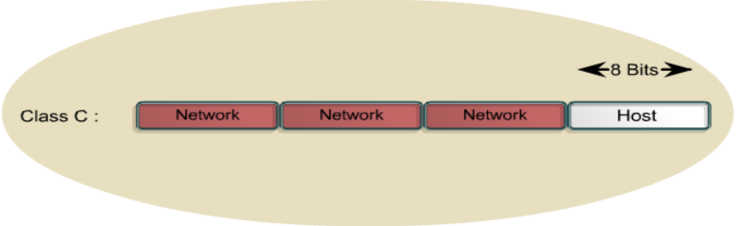
The Class B address was designed to support the needs of moderate to large-sized networks. A Class B IP address uses the first two of the four octets to indicate the network address. The other two octets specify host addresses.



Class B address

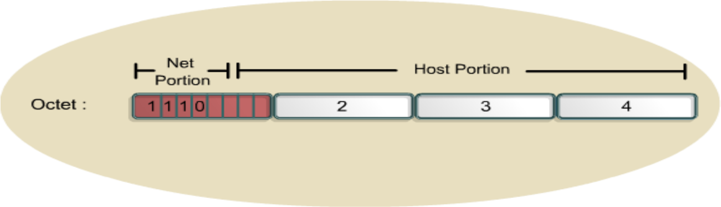
The ***first two bits of the first octet of a Class B address are always 10***. The remaining six bits may be populated with either 1s or 0s. Therefore, the lowest number that can be represented with a Class B address is 10000000, decimal 128. The highest number that can be represented is 10111111, decimal 191. Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

The Class C address space is the most commonly used of the original address classes. This address space was intended to support small networks with a maximum of 254 hosts.



A ***Class C address begins with binary 110.*** Therefore, the lowest number that can be represented is 11000000, decimal 192. The highest number that can be represented is 11011111, decimal 223. If an address contains a number in the range of 192 to 223 in the first octet, it is a Class C address.

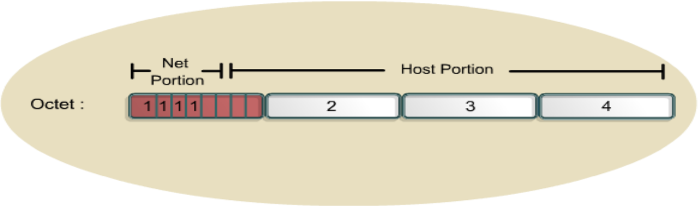
The **Class D address class was created to enable multicasting in an IP address**. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.



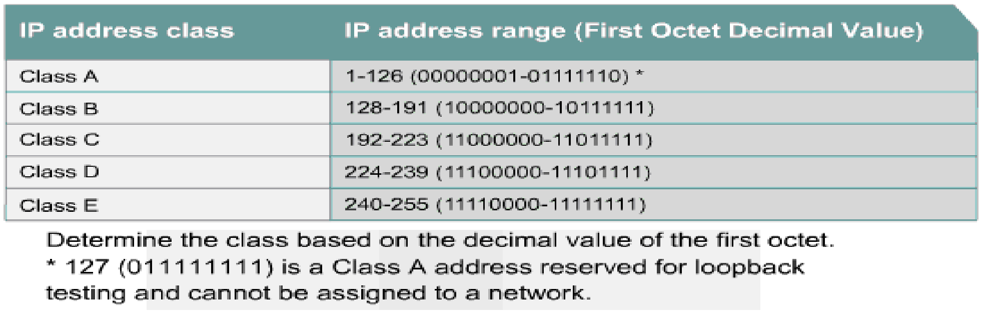
Class D address

The Class D address space, much like the other address spaces, is mathematically constrained. The first four bits of a Class D address must be 1110. Therefore, the first octet range for Class D addresses is 11100000 to 11101111, or 224 to 239. An IP address that starts with a value in the range of 224 to 239 in the first octet is a Class D address.

A Class E address has been defined. However, the Internet Engineering Task Force (IETF) reserves these addresses for its own research. Therefore, no Class E addresses have been released for use in the Internet. The first four bits of a Class E address are always set to 1s. Therefore, the first octet range for Class E addresses is 11110000 to 11111111, or 240 to 255.



Class E address



IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Determine the class based on the decimal value of the first octet.
* 127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

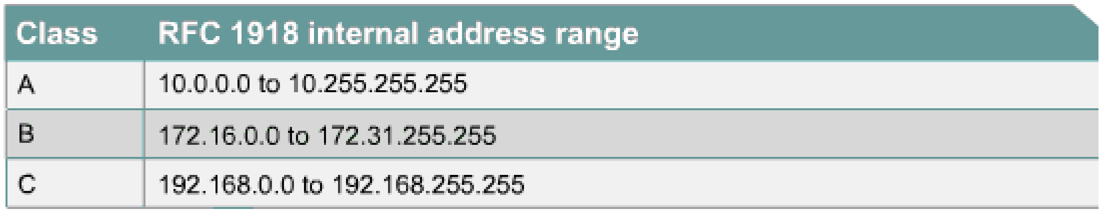
Public and private IP addresses

The stability of the Internet depends directly on the uniqueness of publicly used network addresses.

No two machines that connect to a public network can have the same IP address because public IP addresses are global and standardized. All machines connected to the Internet agree to conform to the system. Public IP addresses must be obtained from an Internet service provider (ISP) or a registry at some expense.

With the rapid growth of the Internet, public IP addresses were beginning to run out. New addressing schemes, such as classless interdomain routing (CIDR) and IPv6 were developed to help solve the problem. CIDR and IPv6 are discussed later in the course.

Private IP addresses are another solution to the problem of the impending exhaustion of public IP addresses. As mentioned, public networks require hosts to have unique IP addresses. However, private networks that are not connected to the Internet may use any host addresses, as long as each host within the private network is unique. Many private networks exist alongside public networks. However, a private network using just any address is strongly discouraged because that network might eventually be connected to the Internet. RFC 1918 sets aside three blocks of IP addresses for private, internal use.



Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Private IP Addresses

These three blocks consist of one Class A, a range of Class B addresses, and a range of Class C addresses. Addresses that fall within these ranges are not routed on the Internet backbone. Internet routers immediately discard private addresses. If addressing a nonpublic intranet, a test lab, or a home network, these private addresses can be used instead of globally unique addresses.

IPv4 and IPv6

When TCP/IP was adopted in the 1980s, it relied on a two-level addressing scheme. At the time this offered adequate scalability. Unfortunately, the designers of TCP/IP could not have predicted that their protocol would eventually sustain a global network of information, commerce, and entertainment. Over twenty years ago, IP Version 4 (IPv4) offered an addressing strategy that, although scalable for a time, resulted in an inefficient allocation of addresses.

The Class A and B addresses make up 75 percent of the IPv4 address space, however fewer than 17,000 organizations can be assigned a Class A or B network number.

Class C network addresses are far more numerous than Class A and Class B addresses, although they account for only 12.5 percent of the possible four billion IP addresses.

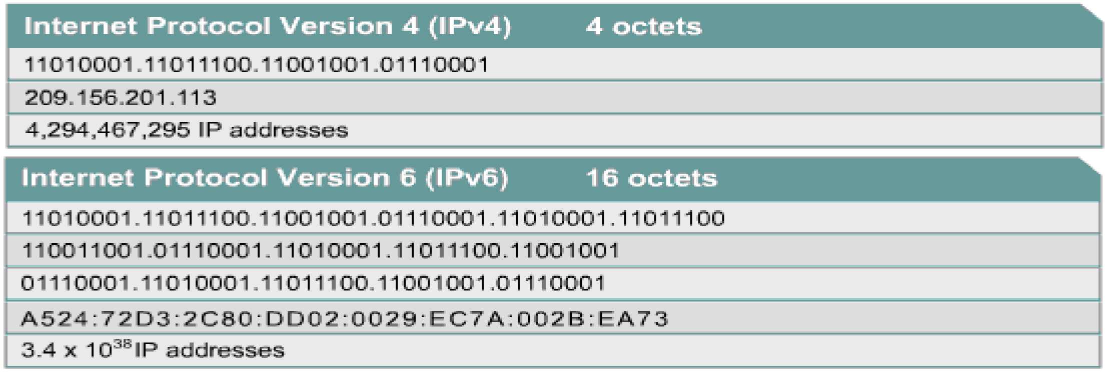
Unfortunately, Class C addresses are limited to 254 usable hosts. This does not meet the needs of larger organizations that cannot acquire a Class A or B address. Even if there were more Class A, B, and C addresses, too many network addresses would cause Internet routers to come to a stop under the burden of the enormous size of routing tables required to store the routes to reach each of the networks.

As early as 1992, the Internet Engineering Task Force (IETF) identified the following two specific concerns:

- Exhaustion of the remaining, unassigned IPv4 network addresses. At the time, the Class B space was on the verge of depletion.
- The rapid and large increase in the size of Internet routing tables occurred as more Class C networks came online. The resulting flood of new network information threatened the ability of Internet routers to cope effectively.

Over the past two decades, numerous extensions to IPv4 have been developed. These extensions are specifically designed to improve the efficiency with which the 32-bit address space can be used. Two of the more important of these are subnet masks and classless interdomain routing (CIDR), which are discussed in more detail in later lessons.

Meanwhile, an even more extendible and scalable version of IP, IP Version 6 (IPv6), has been defined and developed.



Internet Protocol Version 4 (IPv4)	4 octets
11010001.11011100.11001001.01110001	
209.156.201.113	
4,294,467,295 IP addresses	

Internet Protocol Version 6 (IPv6)	16 octets
11010001.11011100.11001001.01110001.11010001.11011100	
110011001.01110001.11010001.11011100.11001001	
01110001.11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3.4 x 10^{38} IP addresses	

IPv6 uses 128 bits rather than the 32 bits currently used in IPv4. IPv6 uses hexadecimal numbers to represent the 128 bits. IPv6 provides 640 sextrillion addresses. This version of IP should provide enough addresses for future communication needs.

IPv4 addresses:

- are 32 bits long
- written in decimal form
- separated by periods.

IPv6 addresses:

- are 128-bits long and
- are identifiers for individual interfaces and sets of interfaces.
- addresses are written in hexadecimal
- and separated by colons
- fields are 16 bits long

To make the addresses easier to read, leading zeros can be omitted from each field. The field :0003: is written :3:. IPv6 shorthand representation of the 128 bits uses eight 16-bit numbers, shown as four hexadecimal digits.

IPv6 addresses are assigned to interfaces, not nodes. Since each interface belongs to a single node, any of the unicast addresses assigned to the interfaces of the node may be used as an identifier for the node.

After years of planning and development, IPv6 is slowly being implemented in select networks. Eventually, IPv6 may replace IPv4 as the dominant Internet protocol.