5/24/2020

Introduction to Networking Terminology, Interfaces, and Protocol

Prepared By: Robera Teshome

Reference Book: CCNA®: Cisco® Certified Network Associate Study Guide Sixth Edition

Introduction to Networking Terminology, Interfaces, and Protocol

Introduction

A basic understanding of networking is important for anyone managing a server. Not only is it essential for getting your services online and running smoothly, it also gives you the insight to diagnose problems.

OSI Model

OSI stands for Open Systems Interconnect. One of the greatest functions of the OSI specifications is to assist in data transfer between disparate hosts—meaning, for example, that they enable us to transfer data between a Unix host and a PC or a Mac.

The OSI has seven different layers, divided into two groups.

- The top three layers define how the applications within the end stations will communicate with each other and with users. Application layer (layer 7) , Presentation layer (layer 6) and Session layer (layer 5)
- The bottom four layers define how data is transmitted end to end. Transport layer (layer 4) , Network layer (layer 3) , Data Link layer (layer 2), Physical layer (layer 1)

OSI layer	**function layers in detail**	
Application layer (layer 7)	✓ Provides a user interface, file, print, message application service	The upper layers
Presentation layer (layer 6)	✓ Presents data Handles processing such as encryption, data encryption, compression and translation services	
Session layer (layer 5)	✓ Keeps different applications' data separate ✓ dialog control	
Transport layer (layer 4)	✓ Provides reliable or unreliable delivery Performs error correction before retransmit ✓ end-to –end connection	The lower layers
Network layer (layer 3)	✓ Provides logical addressing, which routers use for path determination ✓ Routing	
Data Link layer (layer 2)	✓ Combines packets into bytes and bytes into frames ✓ Provides access to media using MAC address ✓ Performs error detection not correction ✓ Framing	
Physical layer (layer 1	✓ Moves bits between devices ✓ Specifies voltage, wire speed pin-out of cables ✓ Physical topology	

The Application Layer

The Application layer of the OSI model marks the spot where users actually communicate to the computer. The application layer is the layer that the users and user-applications most often interact with. Network communication is discussed in terms of availability of resources, partners to communicate with, and data synchronization.

The Presentation Layer

It presents data to the Application layer and is responsible for data translation and code formatting. This layer is essentially a translator and provides coding and conversion functions. A successful data-transfer technique is to adapt the data into a standard format before transmission.

It is responsible in encryption, data encryption, and compression and translation services

The Session Layer

The Session layer is responsible for setting up, managing, and then tearing down sessions between Presentation layer entities. This layer also provides dialog control between devices, or nodes. It coordinates communication between systems and serves to organize their communication by offering three different modes: simplex, half duplex, and full duplex. To sum up, the Session layer basically keeps different applications' data separate from other applications' data.

The Transport Layer

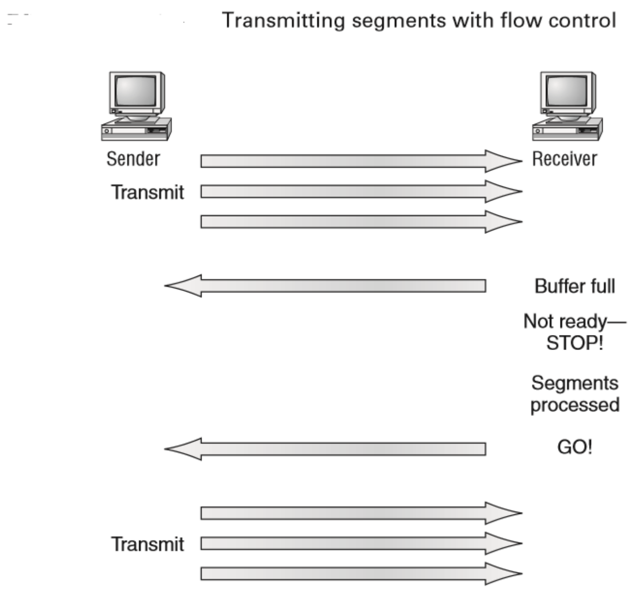
The Transport layer segments and reassembles data into a data stream. Services located in the Transport layer segment and reassemble data from upper-layer applications and unite it into the same data stream. They provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an internetwork.

The Transport layer is responsible for providing mechanisms for multiplexing upper-layer applications, establishing sessions, and tearing down virtual circuits.

Transport layer can be connectionless or connection-oriented

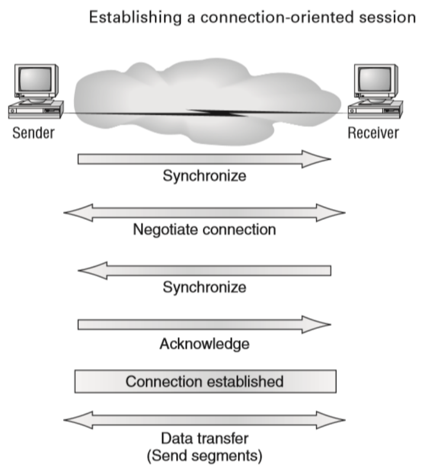
Flow Control

Flow control prevents a sending host on one side of the connection from overflowing the buffers in the receiving host—an event that can result in lost data.



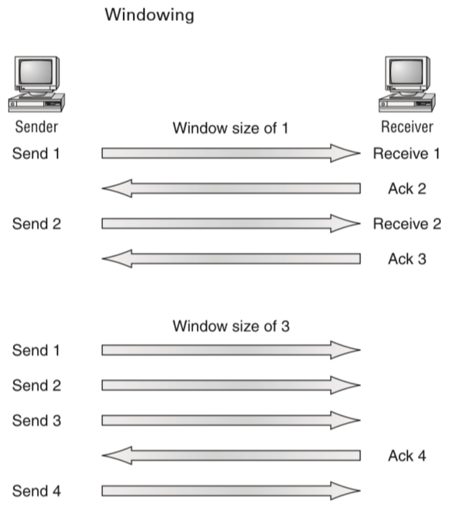
Connection-Oriented Communication

In reliable transport operation, a device that wants to transmit sets up a connection-oriented communication with a remote device by creating a session. The transmitting device first establishes a connection-oriented session with its peer system, which is called a call setup or a **three way handshake**. Data is then transferred; when the transfer is finished, a call termination takes place to tear down the virtual circuit.



Windowing

Ideally, data throughput happens quickly and efficiently. And as you can imagine, it would be slow if the transmitting machine had to wait for an acknowledgment after sending each segment. But because there's time available after the sender transmits the data segment and before it finishes processing acknowledgments from the receiving machine, the sender uses the break as an opportunity to transmit more data. The quantity of data segments (measured in bytes) that the transmitting machine is allowed to send without receiving an acknowledgment for them is called a window.



Acknowledgments

Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional data link. It guarantees that the data won't be duplicated or lost. This is achieved through something called positive acknowledgment with retransmission—a technique that requires a receiving machine to communicate with the transmitting source by sending an acknowledgment message back to the sender when it receives data. The sender documents each segment it sends and waits for this acknowledgment before sending the next segment. When it sends a segment, the transmitting machine starts a timer and retransmits if it expires before an acknowledgment is returned from the receiving end.

The Network Layer

The network layer is used to route data between different nodes on the network. It uses addresses to be able to tell which computer to send information to. This layer can also break apart larger messages into smaller **packet** chunks to be reassembled on the opposite end.
Routers (layer 3 devices) are specified at the Network layer and provide the routing services within an internetwork.

Two types of packets are used at the Network layer: data and route updates.

Data packets Used to transport user data through the internetwork. Protocols used to support data traffic are called routed protocols.

Route update packets Used to update neighboring routers about the networks connected to all routers within the internetwork.

- ✓ **Network addresses** Protocol-specific network addresses.
- ✓ **Interface** The exit interface a packet will take when destined for a specific network.
- ✓ **Metric** The distance to the remote network.

Router

- ✓ Routers, by default, will not forward any broadcast or multicast packets.
- ✓ Routers use the logical address in a Network layer header to determine the next hop router to forward the packet to.
- ✓ Routers can use access lists, created by an administrator, to control security on the types of packets that are allowed to enter or exit an interface.
- ✓ Routers can provide layer 2 bridging functions if needed and can simultaneously route through the same interface.
- ✓ Layer 3 devices (routers in this case) provide connections between virtual LANs (VLANs).
- ✓ Routers can provide quality of service (QoS) for specific types of network traffic.

The Data Link Layer

The Data Link layer provides the physical transmission of the data and handles error notification, network topology, and flow control. This means that the Data Link layer will ensure that messages are delivered to the proper device on a LAN using hardware addresses and will translate messages from the Network layer into bits for the Physical layer to transmit. The Data Link layer formats the message into pieces, each called a data **frame**, and adds a customized header containing the hardware destination and source address

Data Link layer has two sublayers:

Media Access Control (MAC)

Defines how packets are placed on the media. Contention media access is “first come/first served” access where everyone shares the same bandwidth—hence the name.

Logical Link Control (LLC)

Responsible for identifying Network layer protocols and then encapsulating them. An LLC header tells the Data Link layer what to do with a packet once a frame is received. It works like this: A host will receive a frame and look in the LLC header to find out where the packet is destined—say, the IP protocol at the Network layer. The LLC can also provide flow control and sequencing of control bits.

Switches

A layer 2 switch is a type of network switch or device that works on the data link layer (OSI Layer 2) and utilizes MAC Address to determine the path through where the frames are to be forwarded. It uses hardware based switching techniques to connect and transmit data in a local area network (LAN).

The Physical Layer

Finally arriving at the bottom, we find that the Physical layer does two things: It sends bits and receives bits. Bits come only in values of 1 or 0—a Morse code with numerical values. The Physical layer communicates directly with the various types of actual communication media.

The Physical layer specifies the electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating a physical link between end systems.

Hubs at the Physical Layer

An active hub does the same thing like repeater. Any digital signal received from a segment on a hub port is regenerated or reamplified and transmitted out all ports on the hub. This means all devices plugged into a hub are in the same collision domain as well as in the same broadcast domain.

Ethernet Networking

Ethernet is a contention media access method that allows all hosts on a network to share the same bandwidth of a link.

Ethernet networking uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD), a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium.

Half- Duplex Ethernet

port can send data only when it is not receiving data. In other words, it cannot send and receive data at the same time.

Full Duplex Ethernet

All nodes can send and receive on their port at the same time. There are no collisions in full-duplex mode, but the host NIC and the switch port must support the full-duplex mode.

Ethernet Cabling

Ethernet cabling is an important discussion, especially if you are planning on taking the Cisco exams. Three types of Ethernet cables are available:

- ✓ Straight-through cable
- ✓ Crossover cable
- ✓ Rolled cable

Straight-through cable

The straight-through cable is used to connect

- ✓ Host to switch or hub
- ✓ Router to switch or hub

Crossover cable

The crossover cable can be used to connect

- ✓ Switch to switch
- ✓ Hub to hub
- ✓ Host to host
- ✓ Hub to switch
- ✓ Router direct to host

Rolled cable

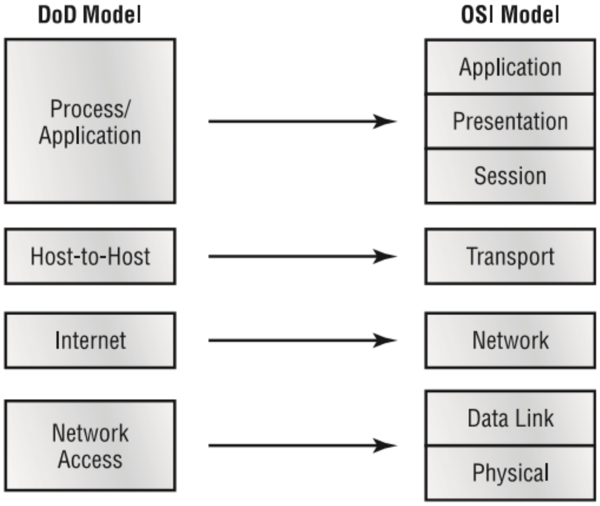
Although rolled cable isn’t used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port.

TCP/IP and the DoD Model

The DoD model is basically a condensed version of the OSI model—it's composed of four, instead of seven, layers:

- ✓ Process/Application layer
- ✓ Host-to-Host layer
- ✓ Internet layer
- ✓ Network Access layer

The DoD and OSI models



The Process/Application Layer Protocols

In this section, I'll describe the different applications and services typically used in IP networks. The following protocols and applications are covered in this section:

- ✓ Telnet
- ✓ FTP
- ✓ TFTP
- ✓ NFS
- ✓ SMTP
- ✓ LPD
- ✓ X Window
- ✓ SNMP
- ✓ DNS
- ✓ DHCP/BootP

Telnet

It is the chameleon of protocols—its specialty is terminal emulation. It allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is the protocol that actually lets us transfer files, and it can accomplish this between any two machines using it. But FTP isn't just a protocol; it's also a program.

Trivial File Transfer Protocol (TFTP)

It is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it, plus it's so easy to use and it's fast too!

Network File System (NFS)

It is a jewel of a protocol specializing in file sharing. It allows two different types of file systems to interoperate. It works like this:

Simple Mail Transfer Protocol (SMTP)

It answering our ubiquitous call to email, uses a spooled, or queued, method of mail delivery. SMTP is used to send mail; POP3 is used to receive mail.

Line Printer Daemon (LPD)

It protocol is designed for printer sharing. The LPD, along with the Line Printer (LPR) program, allows print jobs to be spooled and sent to the network's printers using TCP/IP.

X Window

Designed for client/server operations, X Window defines a protocol for writing client/server applications based on a graphical user interface (GUI). The idea is to allow a program, called a client, to run on one computer and have it display things through a window server on another computer.

Simple Network Management Protocol (SNMP)

It collects and manipulates valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information.

Domain Name Service (DNS)

It change IP address to domain name, and DNS allows you to use a domain name to specify an IP address.

Dynamic Host Configuration Protocol (DHCP)/Bootstrap Protocol (BootP)

It assigns IP addresses to hosts. It allows easier administration and works well in small to even very large network environments.

Here's a list of the information a DHCP server can provide:

- ✓ IP address
- ✓ Subnet mask
- ✓ Introduction to TCP/IP
- ✓ Domain name
- ✓ Default gateway (routers)
- ✓ DNS
- ✓ WINS information

Stands for secure shell (SSH)

SSH stands for secure shell. It is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity.

There are many other protocols that we haven't covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible.

The Host-to-Host Layer Protocols

The following sections describe the two protocols at this layer:

- ✓ Transmission Control Protocol (TCP)
- ✓ User Datagram Protocol (UDP)

Transmission Control Protocol (TCP)

TCP stands for transmission control protocol. It is implemented in the transport layer of the IP/TCP model and is used to establish reliable connections.

TCP is one of the protocols that encapsulates data into packets. It then transfers these to the remote end of the connection using the methods available on the lower layers. On the other end, it can check for errors, request certain pieces to be resent, and reassemble the information into one logical piece to send to the application layer.

The protocol builds up a connection prior to data transfer using a system called a three-way handshake. This is a way for the two ends of the communication to acknowledge the request and agree upon a method of ensuring data reliability.

After the data has been sent, the connection is torn down using a similar four-way handshake.

TCP is the protocol of choice for many of the most popular uses for the internet, including WWW, FTP, SSH, and email. It is safe to say that the internet we know today would not be here without TCP.

User Datagram Protocol (UDP)

UDP stands for user datagram protocol. It is a popular companion protocol to TCP and is also implemented in the transport layer.

The fundamental difference between UDP and TCP is that UDP offers unreliable data transfer. It does not verify that data has been received on the other end of the connection. This might sound like a bad thing, and for many purposes, it is. However, it is also extremely important for some functions.

Because it is not required to wait for confirmation that the data was received and forced to resend data, UDP is much faster than TCP. It does not establish a connection with the remote host, it simply fires off the data to that host and doesn't care if it is accepted or not.

Because it is a simple transaction, it is useful for simple communications like querying for network resources. It also doesn't maintain a state, which makes it great for transmitting data from one machine to many real-time clients. This makes it ideal for VOIP, games, and other applications that cannot afford delays.

The Internet Layer Protocols

The following sections describe the protocols at the Internet layer:

- ✓ Internet Protocol (IP)
- ✓ Internet Control Message Protocol (ICMP)
- ✓ Address Resolution Protocol (ARP)
- ✓ Reverse Address Resolution Protocol (RARP)
- ✓ Proxy ARP

Internet Protocol (IP)

The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

Networks can be linked together, but traffic must be routed when crossing network boundaries. This protocol assumes an unreliable network and multiple paths to the same destination that it can dynamically change between.

There are a number of different implementations of the protocol. The most common implementation today is IPv4, although IPv6 is growing in popularity as an alternative due to the scarcity of IPv4 addresses available and improvements in the protocols capabilities.

Internet Control Message Protocol (ICMP)

ICMP stands for internet control message protocol. It is used to send messages between devices to indicate the availability or error conditions. These packets are used in a variety of network diagnostic tools, such as ping and traceroute.

ICMP packets have the following characteristics:

- ✓ They can provide hosts with information about network problems.
- ✓ They are encapsulated within IP datagrams.

Destination Unreachable If a router can't send an IP datagram any further

Buffer Full If a router's memory buffer for receiving incoming datagrams is full, it will use ICMP to send out this message until the congestion abates.

Hops Each IP datagram is allotted a certain number of routers, called hops, to pass through. If it reaches its limit of hops before arriving at its destination, the last router to receive that datagram deletes it.

Address Resolution Protocol (ARP)

It finds the hardware address of a host from a known IP address. ARP translates the software (IP) address into a hardware address

Proxy ARP can actually help machines on a subnet reach remote subnets without configuring routing or even a default gateway.

Proxy Address Resolution Protocol (Proxy ARP)

Proxy ARP can actually help machines on a subnet reach remote subnets without configuring routing or even a default gateway.

IP Addressing

An IP address is a software address, not a hardware address—the latter is hard-coded on a network interface card (NIC) and used for finding hosts on a local network. IP addressing was designed to allow hosts on one network to communicate with a host on a different network regardless of the type of LANs the hosts are participating in.

IP Terminology

Throughout this chapter you'll learn several important terms vital to your understanding of the Internet Protocol. Here are a few to get you started:

Bit A bit is one digit, either a 1 or a 0. Byte A byte is 7 or 8 bits, depending on whether parity is used. For the rest of this chapter, always assume a byte is 8 bits.

Octet An octet, made up of 8 bits, is just an ordinary 8-bit binary number. In this chapter, the terms byte and octet are completely interchangeable.

Network address this is the designation used in routing to send packets to a remote network—for example, 10.0.0.0, 172.16.0.0, and 192.168.10.0.

Broadcast address the address used by applications and hosts to send information to all nodes on a network is called the broadcast address. Examples include 255.255.255.255, which is all networks, all nodes; 172.16.255.255, which is all subnets and hosts on network 172.16.0.0; and 10.255.255.255, which broadcasts to all subnets and hosts on network 10.0.0.0.

Network Addressing

The network address (which can also be called the network number) uniquely identifies each network.

Class A, a Class B, a Class C , a Class D and Class E addresses

Class A Addresses

This network is 8-bit network prefix. Its highest bit is set to 0, and contains a 7-bit network number and a 24-bit host number. A maximum of 126, which is (2 ^{7} -2,) networks can be defined

Class A Valid Host IDs

Here's an example of how to figure out the valid host IDs in a Class A network address:

- ✓ All host bits off is the network address: 10.0.0.0.
- ✓ All host bits on is the broadcast address: 10.255.255.255.

Class B Addresses

This network is a 16-bit network prefix; its highest bit order is set to **1-0**. It is a 14-bit network number with a 16-bit host number.

This class defines 16,384 (2 ^{14}) /16 networks, and supports a maximum of 65,534 (2 ^{16} -2) hosts per network. Class B /16 block address is (1,073,741,824) = 2 ^{30}; therefore it represent 25% of the total IPV4.

Class B Valid Host IDs

Here’s an example of how to find the valid hosts in a Class B network:

- ✓ All host bits turned off is the network address: 172.16.0.0.
- ✓ All host bits turned on is the broadcast address: 172.16.255.255.

Class C Addresses

This is a 24-bit network prefix; it has a 3 bit set to the highest order **1-1-0**. It is a 21-bit network number with 8-bit host number.

This class defines a maximum of 2,097,152 (2^{21}) /24 networks. And each network supports up to 254 (2^{8} -2) hosts. The entire class C network represents 2^{29} (536,870,912) addresses; therefore it is only 12.5 % of the total IPv4.

Class C Valid Host IDs

Here’s an example of how to find a valid host ID in a Class C network:

- ✓ All host bits turned off is the network ID: 192.168.100.0.
- ✓ All host bits turned on is the broadcast address: 192.168.100.255.

Class D has its highest bit order set to **1-1-1-0** it is used to support multicasting.
Class E has its highest bit order set to **1-1-1-1** which is reserved for experimental use.

Private IP Addresses

A private IP address is an IP address that's reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public. Private IP addresses are in contrast to public IP addresses, which are public and can't be used within a home or business network. Sometimes a private IP address is also referred to as a local IP address.

Reserved IP Address Space

Address Class	Reserved Address Space
Class A	10.0.0.0 through 10.255.255.255

Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

Broadcast address

It represents all devices of the network. If an IP packet is sent on a broadcast address, it is intended for all devices of that network. Broadcast addresses are usually used to locate hosts or services in network.

Multicast address

Multicast address represents a group of devices. If an IP packet is sent on a multicast address, it is intended for all members of that group. Multicast addresses are usually used by networking devices for running their own services.

Unicast address

It represents an individual end device. If an IP packet is sent on a unicast address, it is intended only for that particular recipient. Unicast addresses are usually used by end devices for end to end communication.

- **Firewall**: A firewall is a program that decides whether traffic coming into a server or going out should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server.
- **NAT**: NAT stands for network address translation. It is a way to translate requests that are incoming into a routing server to the relevant devices or servers that it knows about in the LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers.
- **VPN**: VPN stands for virtual private network. It is a means of connecting separate LANs through the internet, while maintaining privacy. This is used as a means of connecting remote systems as if they were on a local network, often for security reasons.

There are many other terms that you may come across, and this list cannot afford to be exhaustive. We will explain other terms as we need them. At this point, you should understand some basic, high-level concepts that will enable us to better discuss the topics to come.