Intro to Networking

Thursday, March 29, 2018 4:22 PM

- Networking - Moving information between two, or more, parties.
- Protocol - A set of rules used to move information between two people or devices.
    - Examples: IPv6, TCP, HTTP, TFTP, IMAP, Ethernet
- Communication Model - Method of organizing information transfer into components

Network Communication Models:

- SYN -> SYN-ACK -> ACK = Three way handshake
- The OSI Model - Open Systems Interconnect
    - Physical - Physical components
    - Data Link - Bridge between IP and Physical layer
    - Network - Global layer, uses IP addresses, where routing takes place
    - Transport - TCP exists here, UDP as well. Responsible between setting up conversation through TCP
    - Application - Where we transfer our data like websites, emails, etc
- OSI Model vs TCP/IP Model
    - TCP/IP Model:
        - Network Interface = Physical/Data link
        - Internet - Network
        - Transport - Transport
        - Application - Application

OSI Model

The OSI model consists of seven different layers that are labeled from 1 through 7; Figure 1 shows a representation of the OSI model:

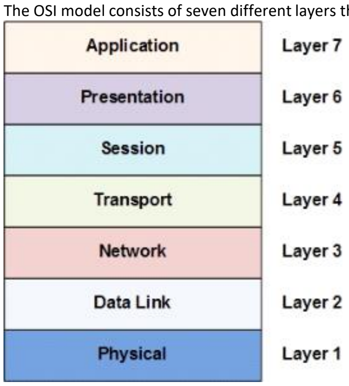

Figure 1 OSI Model

The Physical Layer (Layer 1)

Layer 1 of the OSI model is named the physical layer because it is responsible for the transmission and reception of wire level data. For example, the physical layer is where it is dictated how bits are represented across a specific networking medium. Regardless of whether the networking medium is electrical or optical in construction, the physical layer handles how data is physically encoded and decoded; examples of this would include whether a specific voltage on an electrical medium represents a 1 or 0 or another example would be how a light received at a specific wavelength would be interpreted. Standards examples include IEEE 802.3 (Ethernet), IEEE 802.11 (Wireless Ethernet) and Synchronous optical networking (SONET) among others.

The Data Link Layer (Layer 2)

Layer 2 of the OSI model is named the data link layer and is responsible for link establishment and termination, frame traffic control, sequencing, acknowledgement, error checking, and media access management. The most familiar standards used at the data link layer include IEEE 802.3 (Ethernet) Media Access Control (MAC) and Logical Link Control (LLC) sublayers. The LLC acts as an interface between the physical layer and the MAC sublayer, and the MAC sublayer provides the ability for multiple terminals (computers) to communicate over the same physical medium. Other standards examples include Asynchronous Transfer Mode (ATM), High-Level Data Link Control (HDLC), Frame Relay and the Point to Point Protocol (PPP).

The Network Layer (Layer 3)

Layer 3 of the OSI model is named the network layer and is where routing of network traffic begins. The network layer not only makes the traffic routing decisions but also provides traffic control, fragmentation, and logical addressing (Internet Protocol (IP) addresses). The most common network layer protocol is IP, but other commonly used protocols include the Internet Control Message Protocol (ICMP) and Internet Group Message Protocol (IGMP).

The Transport Layer (Layer 4)

Layer 4 of the OSI model is named the transport layer and is responsible for message segmentation, acknowledgement, traffic control, and session multiplexing. The transport layer also has the ability to perform error detection and correction (resends), message reordering to ensure message sequence, and reliable message channel depending on the specific transport layer protocol used. The most common of the used transport layer protocols include the Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Session Layer (Layer 5)

Layer 5 of the OSI model is named the session layer and is responsible for session establishment, maintenance and termination (the ability to have multiple devices use a single application from multiple locations). Common examples of session layer protocols are Named Pipes and NetBIOS.

The Presentation Layer (Layer 6)

Layer 6 of the OSI model is named the presentation layer and is responsible for character code translation (i.e. ASCII vs. EBCDIC vs. Unicode), data conversion, compression, and encryption. Some common examples include Multipurpose Internet Mail Extensions (MIME), Transport Layer Security (TLS) and Secure Sockets Layer (SSL).

The Application Layer (Layer 7)

Layer 7 of the OSI model is named the application layer and is responsible for a number of different things depending on the application; some of these things include resource sharing, remote file access, remote printer access, network management, and electronic messaging (email). There are a large number of application layer protocols that are familiar to the common Internet user, including the File Transfer Protocol (FTP), Domain Name Service (DNS), Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).

TCP/IP Model

Like the OSI model, the TCP/IP model is layered and is used in the same fashion as the OSI model but with fewer layers. As the modern Internet and most communications use the Internet Protocol (IP), the TCP/IP model is technically more in line with modern network implementations. As stated before, the layers within the TCP/IP model are considered less rigid then that of the OSI model, which basically means that many protocols implemented can be considered in grey areas between one area and another. The TCP/IP protocol suite (often referred to as the TCP/IP *protocol*) contains the same protocols referenced in the earlier OSI model sections. Figure 2 below shows a representation of the TCP/IP model:

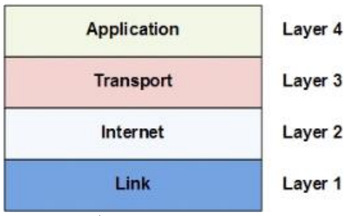

Figure 2 TCP/IP Model

The Link Layer
The link layer is the lowest layer of the TCP/IP model; it is also referred to in some texts as the *network interface* layer. The link layer combines the physical and data link layer functions into a single layer. This includes frame physical network functions like modulation, line coding and bit synchronization, frame synchronization and error detection, and LLC and MAC sublayer functions. Common protocols include the Address Resolution Protocol (ARP), Neighbor Discovery Protocol (NDP), IEEE 802.3 and IEEE 802.11.

The Internet Layer
The Internet layer is the next layer up from the link layer and is associated with the network layer of the OSI model. Functions include traffic routing, traffic control, fragmentation, and logical addressing. Common protocols include IP, ICMP and IGMP.

The Transport Layer
The Transport layer is the next layer and is typically related directly with the same named layer in the OSI model. Functions include message segmentation, acknowledgement, traffic control, session multiplexing, error detection and correction (resends), and message reordering. Common protocols include the Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The Application Layer
The Application layer is the highest layer in the TCP/IP model and is related to the session, presentation and application layers of the OSI model. The application layer of the TCP/IP model is used to handle all process-to-process communication functions; these functions were carried out by multiple different layers when referencing the OSI model. There are a number of different functions which are carried out by this layer, including session establishment, maintenance and termination, character code translations, data conversion, compression and encryption, remote access, network management and electronic messaging to name a few. Common protocols include Named Pipes, NetBIOS, MIME, TLS, SSL, FTP, DNS, HTTP, SMTP and many others.

Summary
The confusion that exists between these two different models is common for new network engineers, as many have at least some familiarity with TCP/IP but have never heard of OSI. It should be clear that these are strictly models and should be considered separate entities from each other when being taught. Hopefully this article is able to make clear the functions that are considered applicable to each layer within each model.

Page 1 of 1

Encapsulation:
- Packet - A chunk of data, with a network layer header
- TTL - Time to Live
- Network Layer:
  - Source IP Address
  - Destination IP Address
  - TTL
  - Other
- Data link layer
  - Destination MAC Address
  - Source MAC Address
  - Layer 3 Protocol
  - Network Layer
- Frame = A chunk of data, with a Data Link layer header
- Source MAC Address contains Ethernet header
- Segment Layer 4
- Packet as layer 3
- Frame as Layer 2
- Summary:
  - Segment
    - Transport layer header + data
  - Packet:
    - Network Layeer header + data
    - (Internet Layer - TCP/IP)
  - Frame:
    - Data Link layer header + data
    - (Network Interface Layer - TCP/IP)

Data Networks and Addressing
- Routers are also called gateways, or default gateways (default router if only one router is available)
- Local Address on Data Link layer
- MAC Address is 48 bit number in hexadecimal
- MAC Address is hardcoded into devices
  - First 24 bits is manufacturer id
  - And second 24 bits is Serial number
- Data Link Layer (Network Interface)
- Local Communication
  - Router separates two distinct networks
    - Assigns MAC address to inside of router, and assigns MAC address to internet
    - We need this because the frame is only allowed to communicate in one network
- Data Link Layer is responsible local communication, responsible for passing messages in network
- Global Addressing
  - Packet HAS to be put inside frame
  - Frame can only communicate locally
  - Frame is sent to default gateway
  - Gatway takes packet, builds new frame for outside network, puts packet into new frame and sends it to outside network
  - Frame is only used to pass messages inside local network
- IP Networks
  - Routers are a Layer 3 device
  - Subnet Mask seperates into two portions (Network and then Host)
    - 255.255.255 - Network | .0 - Host

        - 192.168.104 - Network | .1 - Host
- PING - packet internet grouper
- Physical address = MAC Address = Hard Address (layer 2 address)

Cisco Certifications:
- Entry Level - CCENT
- Associate - CCNA Route/Switch and then Security *********, Cyber Ops CCNA
- Professional - CCNP - Security
- Expert - CCIE - Security
- Architect - CCAr

Exams:
- CCEN Tech - Route/Switch Exam 100-105 ICND1
- CCNA Route/Switch - Exam 101-105 - ICND1 and then Exam 200-105 - ICND2
    - Exam 200-125 = CCNA

Studying for the CCNA:
- Pluralsight Videos
- Study guide or book
    - Todd Lammle
    - Cisco Networking Academy
- Lab
    - GNS3/VIRL
    - Use JCCC classroom

Network Layer Addressing and Operation

Friday, March 30, 2018 12:07 PM

Introduction to Binary:

- Binary 101
    - Base 10 - Use to count money, fingers on our hands, etc..
    - 1 = On
    - 0 = Off

- Converting Binary to Decimal
    - 1s place
    - 2s place
    - 4s place
    - 8s place
    - 16s place
    - 32s place
    - 64s place
    - 128s place
    - Example:
        - 11000000 = 1x128 + 1x64 + 0x32 + 0x16 + 0x8 + 0x4 + 0x2 + 0x1
        - 128+64+0
        - 192

- Converting Decimal to Binary:
    - Reversing process of binary to decimal
    - First try to subtract 128, then 64, then 32, then 16 ….

- Hexadecimal
    - IPv6 written in hexadecimal
    - 0000 = 0 = 0
    - 0001 = 1 = 1
    - 0010 = 2 = 2
    - 0011 = 3 = 3
    - 0100 = 4 = 4
    - 0101 = 5 = 5
    - 0110 = 6 = 6
    - 0111 = 7 = 7
    - 1000 = 8 = 8
    - 1001 = 9 = 9
    - 1010 = 10 = A
    - 1011 = 11 = B
    - 1100 = 12 = C
    - 1101 = 13 = D
    - 1110 = 14 = E
    - 1111 = 15 = F
    - 10000 = 16 = 10

Introduction to IP Addressing

- What is an IP Address?
    - 4 numbers separated by periods, that represents an identifier for a device on a network.
    - We assign the IP address to the network interface card
    - Has two portions - network portion & host portion
        - Network - group of networked devices
        - Host - individual device on a network
        - Zip code = network, host is street address
    - Each decimal number is a OCTET
        - Each contain 8 binary bits
    - Always 32 bits
    - How to identify the network and host portion?
        - 1995 and before = classful addressing
        - 1995 to present = classless addressing
- Classless Addressing
    - Subnet mask added on in 1995
    - Any place that we want network portion in our address, we will create a separate number in our mask. Will put all ones in network portion, and 0's in our host
    - Subnet mask tells which is network portion, and which is host, by putting 1 in subnet mask in network and 0 in host portion

- Classful Addressing
    - Before subnet mask
    - Class A - 8 bits in network portion. 0.0.0.0 to 127.255.255.255
    - Class B - 128.0.0.0 - 191.255.255.255

        - 16 bits network portion and 16 bits host portion
    - Class C: 192.0.0.0 - 233.255.255.255
    - Class D is all network portion, is used for broadcasting one single device to many
        - Still use class D for multicast in IPv4

- Address Types
    - Network Address
        - Identifier for a group of devices. Kind of like our zip code
        - Also called the Network Prefix

    - Broadcast Address
        - Identifier for all devices on a network
    - Host Address
        - Identifies unique device on a network like PC, printer, server, router
    - If we have a device that we want to apply ip address must have a host address and can NOT have a network or broadcast address assigned to it.
    - The only type of address that we assign to devices are host addresses.
    - The network and broadcast address are more concepts that we need in order to describe our networks

- Private and Public Addresses
- Summary:

Introduction to Subnetting

Subnetting Examples

Introduction to IPv6

IPv6 Subnetting

Router Operation

Variable Length Subnet Masking (VLSM)

Check your knowledge

Configuring a Cisco Router

Friday, March 30, 2018 12:07 PM

Network Interface layer and Ethernet Operation

Friday, March 30, 2018 12:07 PM

Troubleshooting Essentials

Friday, March 30, 2018 12:08 PM

Routing IPv4 and IPv6

Friday, March 30, 2018 12:08 PM

Intro to Dynamic Routing

Friday, March 30, 2018 12:08 PM

Intro to VLANs

Friday, March 30, 2018 12:08 PM

Securing the Switch

Friday, March 30, 2018 12:08 PM

TCP and UDP Operation

Friday, March 30, 2018 12:09 PM

Application Layer Protocols

Friday, March 30, 2018 12:09 PM

Access Control Lists

Friday, March 30, 2018 12:09 PM

Network Address Translation (NAT)

Friday, March 30, 2018 12:09 PM

Building and Troubleshooting a Network with ICND1 Skills

Friday, March 30, 2018 12:09 PM

Enterprise LAN Switching

Friday, March 30, 2018 12:10 PM

WAN Technologies

Friday, March 30, 2018 12:10 PM

Advanced Routing

Friday, March 30, 2018 12:10 PM

Network Services for Cisco

Friday, March 30, 2018 12:10 PM

Troubleshooting and Exam Prep

Friday, March 30, 2018 12:10 PM