2020

CISC 4331 – Systems and Network Administration - Week 2

Jimmy Richford
CUNY Brooklyn College

NYC Tech-in-Residence Corps

CISC 4331 – Systems and Network Administration

WEEK 2

Protocol Review

- Protocol - a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed. You can think of a protocol as a spoken language. Each language has its own rules and vocabulary. If two people share the same language, they can communicate effectively.
- Link layer - PPP, DSL, Wi-Fi, etc.
- Internet layer - IPv4, IPv6, etc.
- Transport layer - TCP, UDP, etc.
- Application layer - HTTP, IMAP, FTP, etc.

OSI Protocols

The following are the OSI protocols used in the seven layers of the OSI Model:

- Layer 1, the Physical Layer: This layer deals with the hardware of networks such as cabling.
- Layer 2, the Data Link Layer: This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE.802.3, PPP, X-25, SLIP, ATM, SDLS and PLIP.
- Layer 3, the Network Layer: This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer. The network layer assists the following protocols: Internet Protocol (IPv4), Internet Protocol (IPv6), IPX, AppleTalk, ICMP, IPSec and IGMP.
- Layer 4, the Transport Layer: The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node. It uses the most important protocols of OSI protocol family, which are: Transmission Control Protocol (TCP), UDP, SPX, DCCP and SCTP.
- Layer 5, the Session Layer: The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process. The protocols used are: PPTP, SAP, L2TP and NetBIOS.
- Layer 6, the Presentation Layer: The functions of encryption and decryption are defined on this layer. It converts data formats into a format readable by the application layer. The following are the presentation layer protocols: XDR, TLS, SSL and MIME.
- Layer 7, the Application Layer: This layer works at the user end to interact with user applications. QoS (quality of service), file transfer and email are the major popular services of the application layer. This layer uses following protocols: HTTP, SMTP, DHCP, FTP, Telnet, SNMP and SMPP.

Protocols and the OSI Layer

Layer #	Layer Name	Protocols	Devices
7	Application	HTTP, IMAP, FTP, SMTP	
6	Presentation	SSL	
5	Session	PPTP, L2TP (VPN)	
4	Transport	TCP, UDP	
3	Network	IPv4, IPv6	Switches (L3), Routers
2	Data Link	ARP	Switches (L2)
1	Physical	Bluetooth, DSL, 802.11	Network Cards

TCP - Transport Control Protocol

- TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.
- TCP is connection-oriented, and a connection between client and server is established (passive open) before data can be sent. Three-way handshake (active open), retransmission, and error-detection adds to reliability but lengthens latency. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that prioritizes time over reliability. TCP employs network congestion avoidance. However, there are vulnerabilities to TCP including denial of service, connection hijacking, TCP veto, and reset attack. For network security, monitoring, and debugging, TCP traffic can be intercepted and logged with a packet sniffer.
- Source: https://en.wikipedia.org/wiki/Router_(computing)

IP Address Fundamentals

- IP addresses are a 32-bit binary number, made of ones and zeros.
- An IPv4 address is 32 binary digits (or bits) long.
- An IPv6 is 128 bits long, allowing many more IP addresses to be used.
- IP addresses are usually written in human-readable form, where 8 bits are grouped into one octet.
- An IP address is converted to physical or Media Access Control Address using the Address Resolution Protocol (ARP). If an IP address is your phone number, then your MAC address is your name. You may change your phone number, but your name will not change

IP Addressing

- Think of an IP address like your home address. For you to receive mail at home, the sender must have your correct mailing address (IP address) in your town (network) or you will not receive your mail. The same is true for all equipment on the Internet. Without this specific address, information cannot be received.
- IP addresses come in two forms, static and dynamic.
  - Dynamic IP address: this address changes often (depending on a configuration setting on your DHCP server).
  - Static IP address: this address never changes and is hard coded. Care must be used not to give the same address to two hosts/devices.
- Why choose one over the other?
  - Whenever possible, use dynamic addresses. Assigning static addresses is a lot of manual labor, and it's easy to make mistakes.

Public and private IP addresses

- Devices that are connected to the Internet have public IP addresses assigned to them.
- Remember, private IP addresses are not routable, so they cannot be used to access the Internet. If you try this, the router will drop the packets.
- In theory, anything between 0.0.0.0 – 255.255.255.255 is public, except the private address ranges, BUT, public IP addresses are governed by a body who issues them, mostly to ISP's.
- Your business or home ISP will issue a public IP address for your network to get Internet access.

Public and private IP addresses

- If we didn't use private IP addressing, the Internet would run out of IP addresses.
- We use a process called subnetting to define the portion of an IP block that will be used for the networks and hosts.
- If you are a large corporation, you will want more networks to break things up into location and function.
- You can have networks for a region, state, building floor, department, etc.
- You will need enough hosts in each one of these networks to cover all devices.

DHCP

- Dynamic Host Configuration Protocol – this protocol is the service that assigns IP addresses to devices on a network.
- Every device on your network needs an IP address, so DHCP will issue an IP by receiving a DHCP discover request.
- DHCP is a service that is installed on a server (Windows or Unix), or a router (like your home router).
- It keeps track of all IP's issued so that it does not distribute duplicate IP addresses. That would be bad (imagine if you had two apartments and they both had the same exact address for mail, some mail would go to one place, some to the other. Not very efficient.

DHCP

- Lease duration – how long the device keeps the IP address.
- Multiple DHCP servers – for load balancing and failover.
- Custom options – some devices require custom IP settings that DHCP servers can offer.
  - IE: TFTP, syslog.
- A DHCP scope must include an IP address range, subnet mask, gateway, and DNS server.
- You cannot overlap IP address ranges!

Default gateway

- Think of a default gateway as your last-ditch effort, or your “go to” if you have no other option.
- If you are trying to access a resource, and your local network does not know how to get to that resource, your device will use its default gateway, also called ”default route,” to attempt to get to that device. Usually this is a router.
- For example, if you are attempting to go to www.google.com, your local computer will use DNS to translate www.google.com into an IP address and then attempt to resolve that address. The DNS server will return the IP, and since your local network does not host google.com, it will forward the packets to its default gateway, which will in turn send it on its path to the Internet to bring the Google homepage back to your computer.