Networking Fundamentals Summary

5.7.1

What Did I Learn in this Module?

Introduction to Network Fundamentals

A network consists of end devices such as computers, mobile devices, and printers that are connected by networking devices such as switches and routers. The network enables the devices to communicate with one another and share data. A protocol suite is a set of protocols that work together to provide comprehensive network communication services. Both the OSI and the TCP/IP reference models use layers to describe the functions and services that can occur at that layer. The form that a piece of data takes at any layer is called a protocol data unit (PDU). At each stage of the encapsulation process, a PDU has a different name to reflect its new functions: data, segment, packet, frame, and bits.

The OSI reference model layers are described here from bottom to top:

1. The physical layer is responsible with the transmission and reception of raw bit streams.
2. The data link layer provides NIC-to-NIC communications on the same network.
3. The network layer provides services to allow end devices to exchange data across networks.
4. The transport layer provides the possibility of reliability and flow control.
5. The session layer allows hosts to establish sessions between them.
6. The presentation layer specifies context between application-layer entities.
7. The application layer is the OSI layer that is closest to the end user and contains a variety of protocols usually needed by users.

End devices implement protocols for the entire "stack", all layers. The source of the message (data) encapsulates the data with the appropriate protocols, while the final destination de-encapsulates each protocol header/trailer to receive the message (data).

Network Interface Layer

Ethernet is a set of guidelines and rules that enable various network components to work together. These guidelines specify cabling and signaling at the physical and data link layers of the OSI model. In Ethernet terminology, the container into which data is placed for transmission is called a frame. The frame contains header information, trailer information, and the actual data that is being transmitted. Important fields of a MAC address frame include preamble, SFD, destination MAC Address, source MAC address, type, data, and FCS. Each NIC card has a unique Media Access Control (MAC) address that identifies the physical device, also known as a physical address. The MAC address identifies the

location of a specific end device or router on a LAN. The three major types of network communications are: unicast, broadcast, and multicast.

The switch builds and maintains a table (called the MAC address table) that matches the destination MAC address with the port that is used to connect to a node. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table. Depending on the result, the switch will decide whether to filter or flood the frame. If the destination MAC address is in the MAC address table, it will send it out the specified port. Otherwise, it will flood it out all ports except the incoming port.

A VLAN groups devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. VLANs define Layer 2 broadcast domains. VLANs are often associated with IP networks or subnets. A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. VLANs are organized into three ranges: reserved, normal, and extended.

Internetwork Layer

Interconnected networks have to have ways to communicate, and internetworking provides that "between" (inter) networks communication method. Every device on a network has a unique IP address. An IP address and a MAC address are used for access and communication across all network devices. Without IP addresses there would be no internet. An IPv4 address is 32 bits, with each octet (8 bits) represented as a decimal value separated by a dot. This representation is called dotted decimal notation. There are three types of IPv4 addresses: network address, host addresses, and broadcast address. The IPv4 subnet mask (or prefix length) is used to differentiate the network portion from the host portion of an IPv4 address.

IPv6 is designed to be the successor to IPv4. IPv6 has a larger 128-bit address space, providing 340 undecillion possible addresses. IPv6 prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities provide an IPv6 addressing hierarchy that allows for more efficient routing. IPv6 addresses are represented as a series of 16-bit hexadecimal fields (hextet) separated by colons (:) in the format: x:x:x:x:x:x:x:x. The preferred format includes all the hexadecimal values. There are two rules that can be used to reduce the representation of the IPv6 address: 1. Omit leading zeros in each hextet, and 2. Replace a single string of all-zero hextets with a double colon (::).

An IPv6 unicast address is an identifier for a single interface, on a single node. A global unicast address (GUA) (or aggregatable global unicast address) is an IPv6 similar to a public IPv4 address. The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider such as an ISP, to a customer or site. The Subnet ID field is the area between the Global Routing Prefix and the Interface ID. The IPv6 interface ID is equivalent to the host portion of an IPv4 address. An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). These are two common IPv6 assigned multicast groups: ff02::1 All-nodes multicast group, and ff02::2 All-routers multicast group.

A router is a networking device that functions at the internet layer of the TCP/IP model or Layer 3 network layer of the OSI model. Routing involves the forwarding packets between different networks. Routers use a routing table to route between networks. A router generally has two main functions: Path determination, and Packet routing or forwarding. A routing table may contain the following types of entries: directly connected networks, static routes, default routes, and dynamic routes.

Network Devices

A key concept in Ethernet switching is the broadcast domain. A broadcast domain is a logical division in which all devices in a network can reach each other by broadcast at the data link layer. S witches can now simultaneously transmit and receive data. Switches have the following functions:

- Operate at the network access layer of the TCP/IP model and the Layer 2 data link layer of the OSI model
- Filter or flood frames based on entries in the MAC address table
- Have a large number of high speed and full-duplex ports

The switch operates in either of the following switching modes: cut-through, and store-and-forward. LAN switches have high port density, large frame buffers, and fast internal switching.

Routers are needed to reach devices that are not on the same local LAN. Routers use routing tables to route traffic between different networks. Routers are attached to different networks (or subnets) through their interfaces and have the ability to route the data traffic between them.

Routers have the following functions:

- They operate at the internet layer of TCP/IP model and Layer 3 network layer of the OSI model.
- The route packets between networks based on entries in the routing table.
- They have support for a large variety of network ports, including various LAN and WAN media ports which may be copper or fiber. The number of interfaces on routers is usually much smaller than switches but the variety of interfaces supported is greater. IP addresses are configured on the interfaces.

There are three packet-forwarding mechanisms supported by routers: process switching, fast switching, and CEF.

A firewall is a hardware or software system that prevents unauthorized access into or out of a network. The most basic type of firewall is a stateless packet-filtering firewall. You create static rules that permit or deny packets, based on packet header information. The firewall examines packets as they traverse the firewall, compares them to static rules, and permits or denies traffic accordingly. The stateful packet-filtering firewall performs the same header inspection as the stateless packet-filtering firewall but also keeps track of the connection state. To keep track of the state, these firewalls maintain a state table. The most advanced type of firewall is the application layer firewall. With this type, deep inspection of the packet occurs all the way up to the OSI model's Layer 7.

Load balancing improves the distribution of workloads across multiple computing resources, such as servers, cluster of servers, network links, etc. Server load balancing helps ensure the availability, scalability, and security of applications and services by distributing the work of a single server across multiple servers. At the device level, the load balancer provides high network availability by supporting: device redundancy, scalability, and security. At the network service level, a load balancer provides advanced services by supporting: high services availability, scalability, and services-level security.

Network diagrams display a visual and intuitive representation of the network, how are all the devices connected, in which buildings, floors, closets are they located, what interface connects to that end device, etc. There are generally two types of network diagrams: Layer 2 physical connectivity diagrams, and Layer 3 logical connectivity diagrams. Layer 2, or physical connectivity diagrams are network diagrams representing the port connectivity between the devices in the network. It is basically a visual

representation of which network port on a network device connects to which network port on another network device. Layer 3, or logical connectivity diagrams are network diagrams that display the IP connectivity between devices on the network.

Networking Protocols

Telnet and SSH, or Secure SHell, are both used to connect to a remote computer and log in to that system using credentials. Telnet is less prevalent today because SSH uses encryption to protect data going over the network connection and data security is a top priority. HTTP stands for Hyper Text Transfer Protocol, and HTTPS adds the "Secure" keyword to the end of the acronym. This protocol is recognizable in web browsers as the one to use to connect to web sites. NETCONF does have a standardized port value, 830. RESTCONF does not have a reserved port value, so you may see various implementations of different values.

Dynamic Host Configuration Protocol (DHCP) is used to pass configuration information to hosts on a TCP/IP network. DHCP allocates IP addresses in three ways: automatic, dynamic, and manual. DHCP operations includes four messages between the client and the server: server discovery, IP lease offer, IP lease request, and IP lease acknowledgment.

The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data. The DNS protocol communications use a single format called a DNS message. The DNS server stores different types of resource records that are used to resolve names. These records contain the name, address, and type of record.

The SNMP system consists of three elements:

- SNMP manager: network management system (NMS)
- SNMP agents (managed node)
- Management Information Base (MIB)

There are two primary SNMP manager requests, get and set. A get request is used by the NMS to query the device for data. A set request is used by the NMS to change configuration variables in the agent device. Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network. SNMPv1 and SNMPv2c use community strings that control access to the MIB. SNMP community strings (including read-only and read-write) authenticate access to MIB objects. Think of the MIB as a "map" of all the components of a device that are being managed by SNMP.

NTP is used to distribute and synchronize time among distributed time servers and clients. An authoritative time source is usually a radio clock, or an atomic clock attached to a time server. NTP servers can associate in several modes, including: client/server, symmetric active/passive, and broadcast.

Network Address Translation (NAT) helps with the problem of IPv4 address depletion. NAT works by mapping thousands of private internal addresses to a range of public addresses. By mapping between external and internal IPv4 addresses, NAT allows an organization with non-globally-routable addresses connect to the internet by translating addresses into a globally-routable address space. NAT includes four types of addresses:

- Inside local address
- Inside global address
- Outside local address

- Outside global address

Types of NAT include: static NAT, dynamic NAT, and port address translation (PAT).

Troubleshooting Application Connectivity Issues

Network troubleshooting usually follows the OSI layers. You can start either top to bottom beginning at the application layer and making your way down to the physical layer, you can go from the bottom to the top. If you cannot find any network connectivity issues at any of the OSI model layers, it might be time to look at the application server.

Common uses for ifconfig are the following:

- Configure IP address and subnet mask for network interfaces.
- Query the status of network interfaces.
- Enable/disable network interfaces.
- Change the MAC address on an Ethernet network interface.

ping is a software utility used to test IP network reachability for hosts and devices connected to a specific network. It is also available on virtually all operating systems and is extremely useful for troubleshooting connectivity issues. The ping utility uses Internet Control Message Protocol (ICMP) to send packets to the target host and then waits for ICMP echo replies. Based on this exchange of ICMP packets, ping reports errors, packet loss, roundtrip time, time to live (TTL) for received packets, and so on.

traceroute uses ICMP packets to determine the path to the destination. The Time to Live (TTL) field in the IP packet header is used primarily to avoid infinite loops in the network. For each hop or router that an IP packet goes through, the TTL field is decremented by one. When the TTL field value reaches 0, the packet is discarded. Usually, the TTL field is set to its maximum value, 255, on the host that is the source of the traffic, as the host is trying to maximize the chances of that packet getting to its destination. traceroute reverses this logic, and gradually increments the TTL value of the packet it is sending, from 1 and keeps adding 1 to the TTL field on the next packet and so on. Setting a TTL value of 1 for the first packet, means the packet will be discarded on the first router. By default, most routers send back to the source of the traffic an ICMP Time Exceeded packet informing it that the packet has reached a TTL value of 0 and had to be discarded.

nslookup is another command-line utility used for querying DNS to obtain domain name to IP address mapping. This tool is useful to determine if the DNS server configured on a specific host is working as expected and actually resolving hostnames to IP addresses. It could be that maybe a DNS server is not configured at all on the host, so make sure you check /etc/resolv.conf on UNIX-like operating systems and that you have at least a nameserver defined.

5.7.2

Module 5: Network Fundamentals Quiz

1. Which statement describes the **ping** and **tracert** commands?

⚠ Topic 5.6.0 - The **ping** utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the **traceroute** utility (**tracert** in Windows) traces the route a message takes from its source to the destination. **Traceroute** displays each hop along the way and the time it takes for the message to get to that network and back.

- **Tracert** uses IP addresses; **ping** does not.
- Both **ping** and **tracert** can show results in a graphical display.
- **Tracert** shows each hop, while **ping** shows a destination reply only.
- **Ping** shows whether the transmission is successful; **tracert** does not.

2. Which IPv6 address is most compressed for the full FE80:0:0:0:2AA:FF:FE9A:4CA3 address?

⚠ Topic 5.3.0 - When an IPv6 address is being compressed, the :: can be used to replace a recurring set of 0s only once.

- FE80:::0:2AA:FF:FE9A:4CA3
- FE8::2AA:FF:FE9A:4CA3
- FE80::2AA:FF:FE9A:4CA3
- FE80::0:2AA:FF:FE9A:4CA3

3. Which command can be used on Linux and MAC hosts to get IP addressing information?

⚠ Topic 5.6.0 - Network administrators typically view the IP addressing information on Windows hosts by issuing the **ipconfig** command, and on Linux and Mac hosts by issuing the **ifconfig** command. The **networksetup -getinfo** command is used on Mac hosts to verify IP settings. The **ip address** command is used on Linux hosts to display IP addresses and properties.

- **ifconfig**
- **networksetup -getinfo**
- **ipconfig**
- **ip address**

4. What type of IPv6 address is FE80::1?

⚠ Topic 5.3.0 - Link-local IPv6 addresses start with FE80::/10, which is any address from FE80:: to FEBF::. Link-local addresses are used extensively in IPv6 and allow directly connected devices to communicate with each other on the link they share.

- multicast

- loopback
- global unicast
- link-local

5. Which two statements are true about NTP servers in an enterprise network? (Choose two.)

⚠ Topic 5.5.0 - Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

- [ ] There can only be one NTP server on an enterprise network.
- [ ] NTP servers control the mean time between failures (MTBF) for key network devices.
- [ ] NTP servers at stratum 1 are directly connected to an authoritative time source.
- [x] NTP servers ensure an accurate time stamp on logging and debugging information.
- [ ] All NTP servers synchronize directly to a stratum 1 time source.

6. A small-sized company has 30 workstations and 2 servers. The company has been assigned a group of IPv4 addresses 209.165.200.224/29 from its ISP. The two servers must be assigned public IP addresses so they are reachable from the outside world. What technology should the company implement in order to allow all workstations to access services over the Internet simultaneously?

⚠ Topic 5.5.0 - The company allocated only 6 usable host public addresses. Two public addresses should be assigned to the two servers. Since the four remaining public addresses are not enough for the 30 clients, NAT must be implemented for internal workstations to access the Internet. Therefore, the company should use PAT, also known as NAT with overload. DHCP can be used to dynamically assign internal private IP addresses to the workstations, but cannot provide the NAT service required.

- dynamic NAT
- port address translation
- DHCP
- static NAT

7. Which statement describes a stateful firewall?

⚠ Topic 5.4.0 - Basic packet filtering firewalls can only filter based on Layer 3 and sometimes basic Layer 4 information. An application gateway firewall, or proxy firewall, can filter based on information in the upper layers such as the application layer. A NAT firewall can expand the number of available IP addresses on the network.

- It can expand the number of IP addresses available and can hide network addressing design.
- It can only filter packets based on limited Layer 3 and 4 information.
- It can determine if the connection is in the initiation, data transfer, or termination phase.
- It can filter packets based on information at Layers 3, 4, 5 and 7 of the OSI reference model.

8. Which impact does adding a Layer 2 switch have on a network?

⚠ Topic 5.4.0 – Adding a Layer 2 switch to a network increases the number of collision domains and increases the size of the broadcast domain. Layer 2 switches do not decrease the amount of broadcast traffic, do not increase the amount of network collisions and do not increase the number of dropped frames.

- an increase in the size of the broadcast domain
- an increase in the number of dropped frames
- an increase in the size of the collision domain
- an increase in the number of network collisions

9. Data is being sent from a source PC to a destination server. Which three statements correctly describe the function of TCP or UDP in this situation? (Choose three.)

⚠ Topic 5.1.0 – Layer 4 port numbers identify the application or service which will handle the data. The source port number is added by the sending device and will be the destination port number when the requested information is returned. Layer 4 segments are encapsulated within IP packets. UDP, not TCP, is used when low overhead is needed. A source IP address, not a TCP source port number, identifies the sending host on the network. Destination port numbers are specific ports that a server application or service monitors for requests.

- [x] The UDP destination port number identifies the application or service on the server which will handle the data.
- [ ] The source port field identifies the running application or service that will handle data returning to the PC.
- [ ] UDP segments are encapsulated within IP packets for transport across the network.
- [ ] TCP is the preferred protocol when a function requires lower network overhead.
- [ ] The TCP source port number identifies the sending host on the network.
- [ ] The TCP process running on the PC randomly selects the destination port when establishing a session with the server.

10. What is the function of the MIB element as part of a network management system?

⚠ Topic 5.5.0 – The Management Information Base (MIB) resides on a networking device and stores operational data about the device. The SNMP manager can collect information from SNMP agents. The SNMP agent provides access to the information.

- to change configurations on SNMP agents
- to store data about a device
- to send and retrieve network management information
- to collect data from SNMP agents

11. Which two devices allow hosts on different VLANs to communicate with each other? (Choose two.)

⚠ Topic 5.2.0 – Members of different VLANs are on separate networks. For devices on separate networks to be able to communicate, a Layer 3 device, such as a router or Layer 3 switch, is necessary.

- [ ] Layer 3 switch
- [ ] repeater
- [ ] router
- [x] hub
- [ ] Layer 2 switch

12. What is obtained when ANDing the address 192.168.65.3/18 with its subnet mask?

⚠ Topic 5.3.0 – The value of the IP address 192.168.65.3 in binary is 11000000.10101000.01001110.00000011. The value of the subnet mask in binary is 11111111.11111111.11000000.00000000. When ANDing the two, the result is 11000000.10101000.01000000.00000000, which in turn converts into 192.168.64.0.

- 192.168.0.0
- 192.168.32.0
- 192.168.16.0
- 192.168.64.0

Check | Show Me

Reset

5.6
Troubleshooting Application Connectivity I...

6.0
Introduction to Application Deployment an...