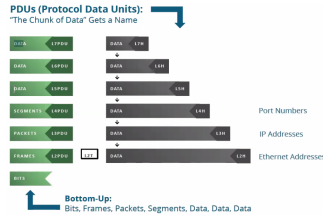


OSI Model	TCP/IP Protocol Suite						TCP/IP Model
Application							
Presentation	File Transfer FTP, TFTP	Web Browser HTTP	Email SMTP, IMAP, POP3	Remote Login Telnet, Rlogin	Name Resolution DNS	IP Address DHCP	Application
Session							
Transport	Transmission Control Protocol TCP			User Datagram Protocol UDP			Transport
Network	Internet Protocol IP			ARP, RARP ICMP			Network
Data Link	Ethernet II	Token Ring	FDDI	WAN Protocols			
Physical	Copper Twisted Pair						Network Access
	Fiber Optic			Wireless			



TCP - connection oriented, reliable, 3 way handshake

* FTP port 20 , 21

* SSH port 22

* Telnet Port 23

* SMTP port 25

* Http port 80

* HTTPS port 443

UDP - non reliable, connectionless

* DNS - 53

* DHCP - Ports 67 , 68

* TFTP - Port 69

* NTP - port 123

* SNMP - 161 , 162

		32768	16384	8192	4096	2048	1024	512	256		128	64	32	16	8	4	2	1
B	(Binary)	128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1
S	(Subnet mask)	128	192	224	240	248	252	254	255		128	192	224	240	248	252	254	255
C	(CDR)	17	18	19	20	21	22	23	24		25	26	27	28	29	30	31	32
H	(Hosts)	32768	16382	8190	4094	2046	1022	510	254		126	62	30	14	6	2	0	0

Layer-2 Fundamentals

OSI Model

- **Application (L7)** , Presentation (L6), Session Layer (L5) - where the data lives (ftp tftp, http, email, dns, dhcp)
- **Transport Layer (L4)** - Logical end to end communication between two objects. TCP and UDP operate here - **segments** - port numbers
 - TCP is reliable
 - UDP is unreliable
- **Network Layer (L3)** - where routers work using IP addressing and ICMP (ping & trace) - **packets** - IP addressing
- **Data Link Layer (L2)** - switches operate here using MAC (L2, burned-in, physical address) addresses - **frames** - MAC Addresses
- **Physical Layer (L1)** - Anything dealing with network cable or the standards in use - including pins - **bits**

Frame Forwarding Basics

- Switch receives frame
- Reviews source mac information
- Switch now reviews destination mac-address
 - If the mac is not in the mac address table, the frame is flooded out of all ports except of the receiving frame
 - If the mac is known, the switch forwards it out the designated port
- Once flooded frame is received by appropriate host, host responds to message
- Switch receives frame and forwards out appropriate port to original host
- Broadcast frames have an address of all ff's and is treated as a flooded frame
- Dynamically learned frames stay in the mac address table for 5 mins by default

TCP & UDP

- **TCP (6)**
 - Connection oriented
 - Sequencing and reliable delivery
 - Files sharing downloading
- **3 way handshake** - TCP - used to initiate communication
 - SYN Package - requests permission to send data
 - SYN/ACK - acknowledges initial syn request and requests permission to send data
 - ACK - initial sender acknowledges syn request
 - Data transfer begins (sends bytes of segments) negotiates window size
 - Window size - defines how much data can be sent before an ack has to be sent. Flow control
- **UDP (17)**
 - Connectionless, no sequencing, VOIP, Streaming video
- **Address Resolution Protocol** - maps IP addresses to mac-addresses within a LAN
- **Spanning Tree** - Spanning-Tree Protocol help reduce redundancy within switched networks, prevents switching loops and broadcast storms in the layer 2 network
- **Bridge ID** - combination of the bridge priority and MAC address. Used in the STP root bridge election as tie-breaker
- **Root Bridge** - Bridge that is base of the STP tree, elected based on BID
- **Bridge Priority** - default value is 32768, can be set in multiples of 4096, used in conjunction with, lowest value will become root bridge. Ties are broken the lowest MAC address MAC for BID
- **STP Port States**
 - **Election Process** - the switch reads the incoming BPDU and compares the BID against it's own.
 - The election process continues until all switches agree on the root bridge
 - **Disabled Mode** - a port that has been administratively shut down
 - **Blocking Mode** - no frame forwarding or receiving on the port. No dynamic learning of MAC addresses
 - **Listening Mode** - listening for BPDUs. Can send BPDUs, but can't forward or receive frames
 - **Learning Mode** - not forwarding frames but can learn MAC address. Learning ports continue to send and receive BPDUs
 - **Forwarding Mode** - Allows port to forward and receive frames, send and receive BPDUs, and learn MAC addresses. Only state in which a port if forwarding frames.

Layer-3 Fundamentals

- **Administrative Distance** - used to determine the best pathway when multiple routes are available to the same destination. The protocol with the lowest administrative distance will be selected as the best route
 - Connected - 0 : Static - 1 : External BGP - 20 : EIGRP Internal - 90 : OSPF - 110 : RIP - 120 : BGP Internal - 200
- **Longest Match Rule** - the most specific route is preferable to a less specific route in the routing table
- **Distance Vector Protocol** - calculates best route on hop count (number of routers (eigrp & rip))
- **Link-State Protocol** - calculates best route base on routing map of network (ospf)
- **Path-Vector** - allows you to see the entire path (BGP). BGP calculates best route by number of AS hops
- **IP Help Address** forwards UDP broadcasts to a specific address
- **Public IP Address** - routable IP address is that can be routed outside the private network
 - Public IPs are normally provided by Internet Service Provider
 - ISPs are assigned Public IP from Regional Internet Registrar

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 171.255.255.255 173.0.0.0 to 191.255.255.255
C	192.0.0.0 to 195.255.255.255 197.0.0.0 to 223.255.255.255
D	224.0.0.0 to 247.255.255.255 Multicast Addresses
E	248.0.0.0 to 255.255.255.254 Experimental Use

- **Private IP Address** - non-routable IP address on public networks (the internet) or between organizations

- will be blocked by edge router
 - can be routed on a private network
 - also called by reserved addresses
 - Network Address Translation (NAT) or proxy servers can resolve private addresses into public to become routable
 - anything starting with a 10 is a private class A, 172.16 - 172.31 is private class B, and 192.168 is private class C
- **Unicast** - message sent to one host
 - **Broadcast** - message sent to all hosts on a network except the sender
 - **Multicast** - message sent to multiple hosts

Class	Start of Range	End of Range
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

OSPF Notes

- **OSPFv2 Fundamentals** - open standard link-state protocol (every router has the network map) that dynamically determines best/most efficient path (Dijkstra shortest path) in a network (admin distance is 110 **port number 89**)
- **OSPF Key Terms**
 - **Neighborhood** - routers reside on the same network link and exchange hello messages
 - **Adjacencies** - neighbors that exchange information to build link state database. Only formed with the **Designated Routers and Backup Designated Routers**. Full adjacency requires hello and dead timers (default time is 10 - hello and 40 dead timers, area ID, and subnet all match
 - **Router ID (RID)** - 32-bit number that identifies a router in an OSPF network. RID can be manually assigned within OSPF or automatically assigned. Auto assign is the largest loopback or any IP interface.
 - Highest priority value become the DR and BDR. Tie breaker goes to the highest RID
 - Setting a router's priority to 0 prevents a router from participating in the DR/BDR election
 - All OSPF routers use multicast address of 224.0.0.5, and DRs use 224.0.0.6
 - **Dijkstra Algorithm** - the equation used to determine the best path in an OSPF network
 - **Area** - a logical grouping of networks, routers, and links within an Open Shortest Path First (OSPF) network that share the same area ID
 - **Area Border Router** - has interfaces participating in separate areas
 - **Link State Advertisement** - Information a router sends and receives about network reachability
 - Type 1 LSA created by a router and contains information about that routers directly attached networks
 - Type 2 LSA created for each transit network within an area on which a DR is elected
 - Type 3 LSA is a summary LSA and is sent from one area to another and is used to advertise a network in the source area
 - **Link State Database** - Map of the network
 - **Link State Update** - A packet that carries LSAs
 - **Link State Request** - request specific LSA information from a neighbor
 - **Link State Ack** - Used by a router to confirm it received LSU
- **OSPF Adjacency Process**
 - **Down State** - initially, the interface is considered down and does not send or receive hello packets
 - **Attempt State** - router starts sending hello packets to discover potential neighbors on the network
 - **Init State** - router receives packets from potential neighbors, sends its own hello packets, and awaits response
 - **2-way State** - bidirectional communication has been established
 - **Extstart State** - routers begin DR and BDR election process
 - **Loading State** - received LSAs are processed and added to routing table
 - **Full State** - all LSAs are processed and the routing table is updated

BGP Notes

- **BGP -Border Gateway Protocol (BGP)** - path vector protocol that is highly scalable inter domain routing protocol **port number 179**. The routing protocol of the internet
 - **BGP protocol** selects the path with the most desirable combination of attributes, more than likely selecting the path that traversers the least amount of Autonomous Systems (**AS_PATH**) if other local weights are not present
 - **IGBGP** - when neighbors share the same AS numbers - (AD 200)
 - **EBGP** - when neighbors have different AS numbers - (AD 20)

Additional Notes:

- **AAA** stands for authentication, authorization, and accounting. It's a security framework that controls access to computer resources, enforces policies, and audits usage
 - **Authentication** - provides the user access to the system
 - **Authorization** - users are granted access to certain areas of a network or system
 - **Accounting** - tracks and logs user activity while they are logged into a system
- **SSH** - networking protocol that allows two computers to communicate securely over an unsecured network
 - SSH requires a configured hostname, domain name, generated RSA key pair, username and password, and enabled access on VTY lines
- A **port number** is a unique identifier assigned to a specific application
 - TCP - FTP 20,21 : SSH port 22 : Telnet 23 : SMTP 25 : HTTP 80 : HTTPS 443
 - UDP - DNS 53 : DHCP 67, 68 : TFTP 69 : NTP 123 : SNMP : 161, 162
- **Network Address Translation & Port Address Translation** - translate private IP addresses to public routable IP addresses

Azure Cloud Notes:

- **Define the Cloud** -
 - **Public Cloud** - defined as computing services offered by third-party providers over the public internet, making them available to anyone who wants to use or purchase them
- **Share Responsibility Model** - defines how responsibility is divided between the customer and the vendor

Questions

- Can you describe the process once a RFS is received
- Describe the opportunities for growth
- Support attending training and industry conferences and workshops, is there a lab