Keith Barker

Sunday, June 8, 2025 10:19 AM

Discord: https://ogit.online/Join_OGIT_on_Discord

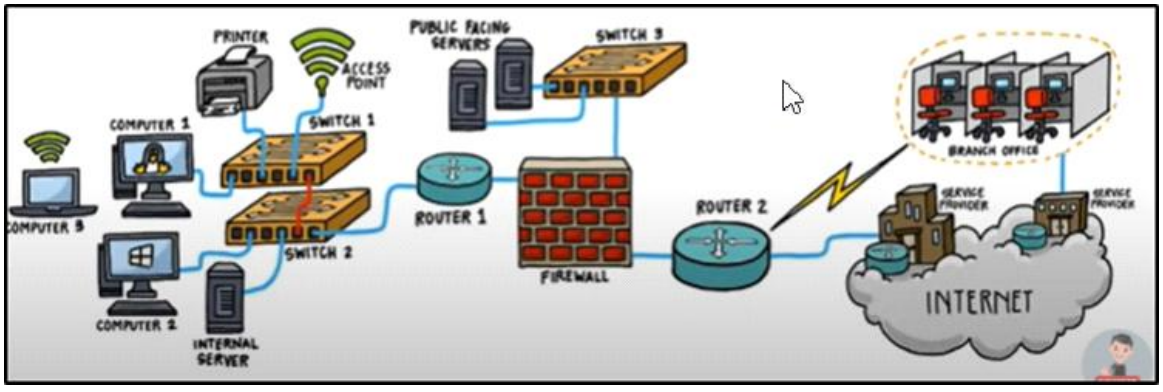
Playlist for Cisco CCNA 200-301:
https://ogit.online/sloth

Cisco CCCNA 200-301 IPv4 Subnetting:
https://ogit.online/subnet

Video 1.

Clients, Servers, and Protocols

CCNA - 3 months topics
Objectives: For us to be able to describe or explain:
- Roles of clients/ servers
- Benefit of layers
- What is a "protocol stack"

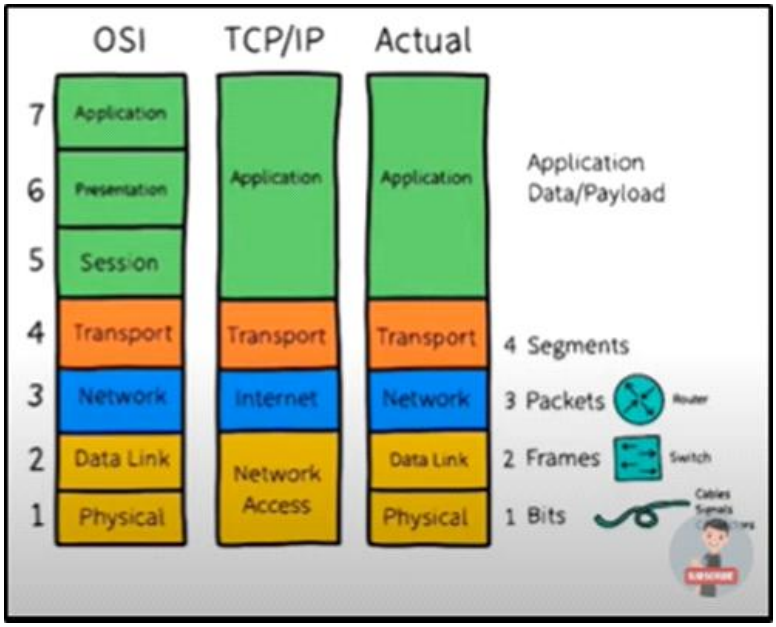


Server - provides services, providing a network services. Website, file, streaming service, authentication.

Client - requests services, requesting a network services. Requesting a website, file, or authentication.

Bob opens a browser quick example. Bob inputs in the search pane to surf to, requesting the website page, www.zoo.com, the zoo.com server will take that request and authorize the website to bob by allowing the website to be found on the internet and bob is able to see the website.

Layers - OSI Model, TCP/IP Model and Actual.



see every component and aspect that you understand them.

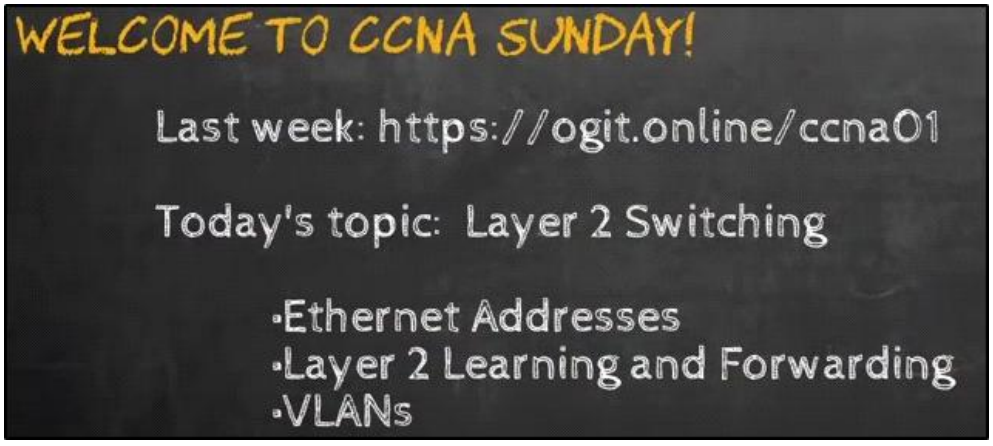
Protocol - Rules that communications are built upon so that the sender and recipient understands, in that communication. Allowing devices and users a way to communicate. Remember and memorize the TCP/IP and Actual models for use today.

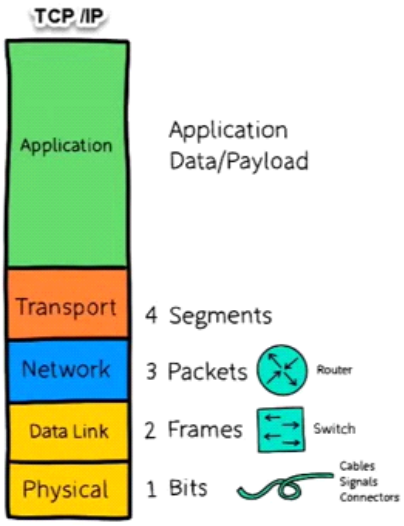
Application - Application: Data/Payload
Transportation - Segments
Network/Internet - Packets > router
Data Link - Frames > Switches
Physical - Bits > medium connectivity (cables, signals, connectors)

Transmission Control Protocol - Connection oriented: Three-way handshake. Somewhat encrypted confidential only between sender and recipient. Communication is confirmed and that messages that are sent are confirmed received and others.

UserDatagram Protocol - Connectionless oriented. No, encryption, doesn't care if messages is received and others.

Video 2:





Bob - On the laptop: In the browser inputs website address, IP address press enter and he gets a response. The browser is using: HTTP or HTTPS protocols in the Application layer. Those services will use the next layer services Transport layer. 3-way handshake. TCP protocol, messages in the form of segments. The next layer of services exchanges IP addresses and routing information in the form of packets at layer 3. Next layer exchanges MAC addresses in the form of frames. Network interface card information. Layer 2 MAC address is it's unique Identification number that is unique throughout the world. Sometimes called Physical Address, L2 address, MAC address, Ethernet address, all layer 2, and last BIA, (Burned in Address) It is the 12 digit number in the NIC to identify that specific device. Network Adapters, Network Cards, Same concept for layer 2 address. Address Resolution Protocol (ARP) is the protocol of how source and destination devices learn the MAC address of each other. Each device in a network will learn each other's MAC address through this same Protocol and put each address in a table within the network so that each device can take care of layer 2 protocols. The table known as a cache. Devices learn each devices and what port, frames come in and out, this is only in a local network. Layer two switch listens, learns, and forwards frames and learn dynamically and puts it into its MAC Address Table, and then it can forward frame.

Conf t > int switches > shutdown > no shutdown turns back on > show mac add > Mac address-table > MAC Address Table >
PC2 > ping bob computer > pc2 show ip >

Vlans - segregating a network into smaller networks. Chopping up a network: instead of one network (big room) with 300 devices. You can have 10 networks (rooms) with 30 devices each. Instead of having a large physical network, splitting the network into 10 virtual logical networks. We need network address. Subnetting will allow this to happen. To understand your current level of comprehension you need assessments. 200 questions on the quizzes playlist.

SW1 > Global config vlan 10 > exit > switch port access vlan 10 >

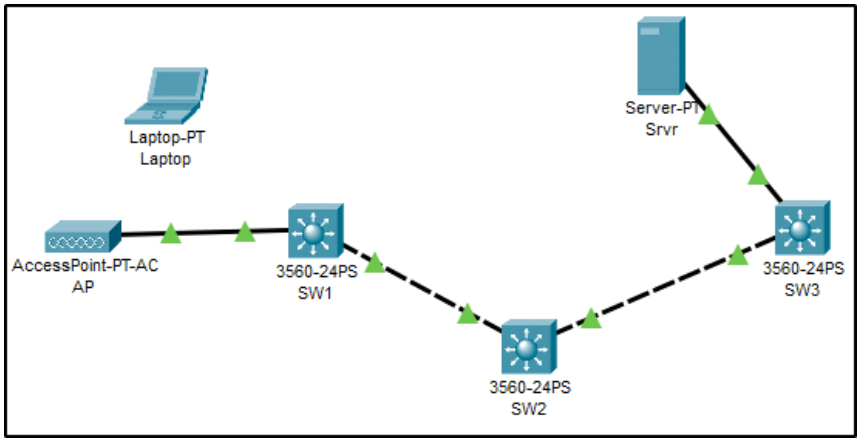
SW1 > show vlan brief
SW1 > vlan 10 > exit > global configuration command
Do show vlan brief command
Int gig 0/1
Switchport mode access > Sw switchport access vlan 10 > show vlan 10 brief >
Int gig 0/2 > do show mac add
Int gig 0/2 > sw > switchport mode access > SW

DEV NET > network fundamentals > Reinforce this information.

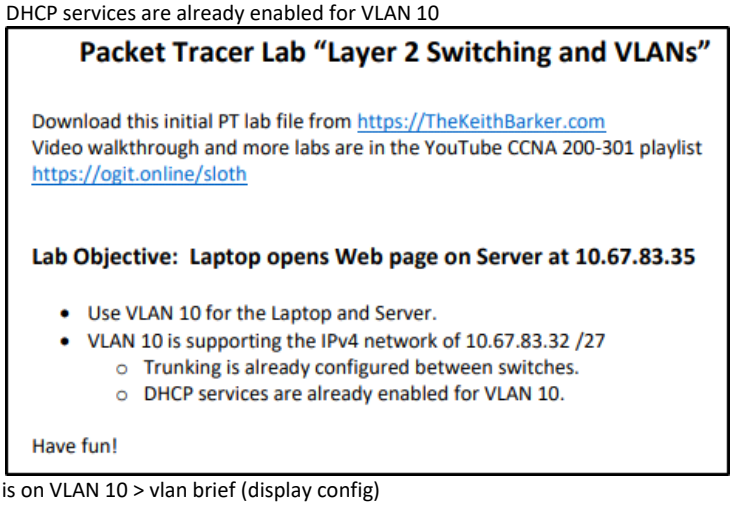
Packet Tracer Lab L2 Switching and VLANs | Cisco CCNA 200-301
Video 4

www.Thekeithbarker.com/

Topology We will be working with:



Objectives: Wireless model > AP > 3 switches > server with IP address already on it.
Lab Objectives: Laptop opens Web page on Server at 10.67.83.35

- Use Vlan 10 for the Laptop and Server
- VLAN 10 is supporting the IPv4 network of 10.67.83.35
  - Trunking is already configured between switches.
  - DHCP services are already enabled for VLAN 10
  - 

Packet Tracer Lab "Layer 2 Switching and VLANs"

Download this initial PT lab file from https://TheKeithBarker.com
Video walkthrough and more labs are in the YouTube CCNA 200-301 playlist
https://ogit.online/sloth

Lab Objective: Laptop opens Web page on Server at 10.67.83.35

- Use VLAN 10 for the Laptop and Server.
- VLAN 10 is supporting the IPv4 network of 10.67.83.32 /27
  - Trunking is already configured between switches.
  - DHCP services are already enabled for VLAN 10.

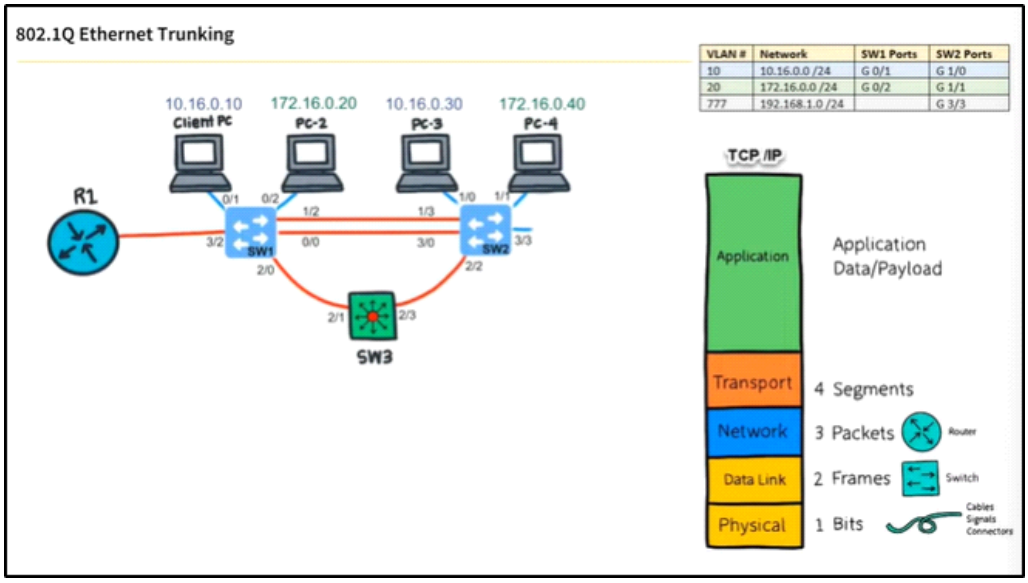
Have fun!

Verify SW3 is on VLAN 10 > vlan brief (display config)
Trunking is in place between SW1 > SW2 > SW3

Laptop had a 169.x.x.x IP address that is a private IP and it is not a good IP address and couldn't get to the DHCP port.
Check SW1 to see if it is in Vlan 10 >
Commands used for troubleshooting:

- Enable - connect to the switch using terminal emulator.
- Conf t - entering global configuration mode.
- Int <interface-ID>
- Vlan <vlan-ID>, name [vlan-name] - create vlans
- Int <interface-ID>, switchport access vlan [vlan-ID] - Assigns ports to vlans.
- Int <interface-ID> switchport mode trunk. - Configure trunk ports.
- Switchport trunk allowed vlan [vlan-range] - Specify allowed Vlans on the trunk ports.
- End - to exit global and enter Exec mode
- Show vlan
- Show interfaces trunk
- Show interfaces [interface-ID]
- Show vlan brief

802.1q Ethernet Trunking Video 5:

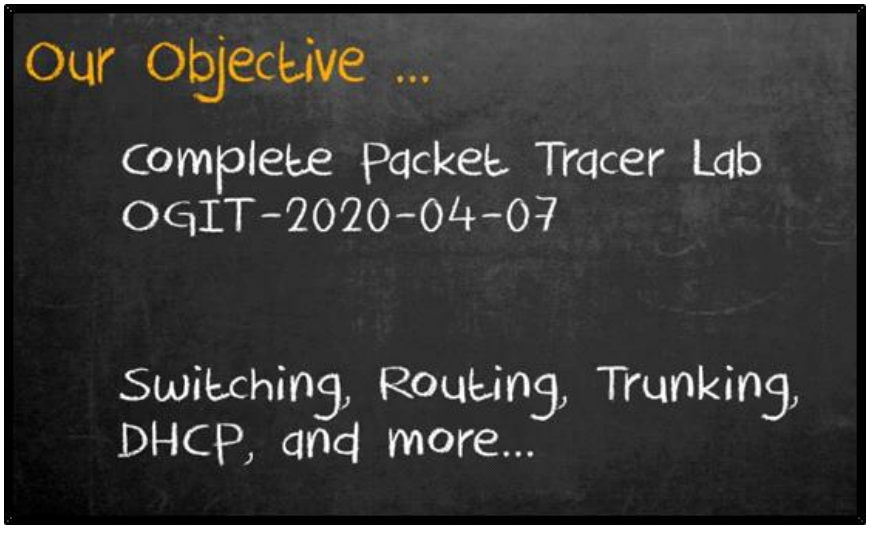


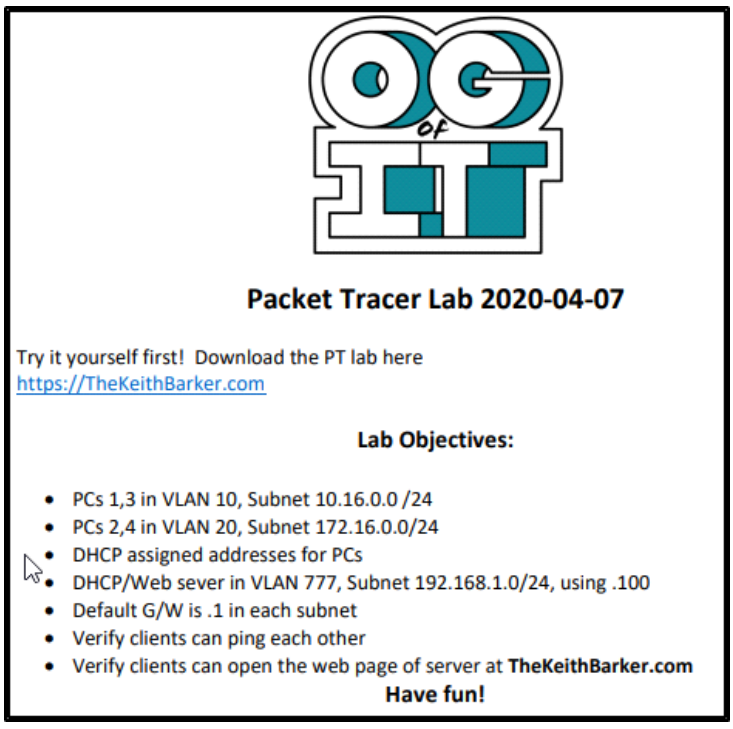
Client PC1 belonging to the Accounting depart is in Vlan 10 - PC3 also in the Acct. Dept. and in Vlan 10.

- Can PC1 ping PC3?
  - PC3 - 10.16.0.30
  - PC1 - 10,16,0,0/24
- If the ping doesn't work, ARP is done so that PC1 can get PC3 IP address.
- What mechanism can we use to make sure that the broadcast only sends to Vlan 10 host / devices. By using a tag (label) the switch adds the Vlan 10 tag (label) and this is Trunking so that the switches can add to the payload to reach the correct Vlan 10 recipients. This is done by Switches.
- Why do we need Trunking (802.1q)? So that the switches knows what Vlan it needs to go to. Tags are injected into the encapsulation so information for the switch to make routing decisions.
- Interface range <port range>
- Switchport trunk encapsulation dot1q
- Switchport mode trunk
- End
- Need to configure this on both inside Switch ports. SW1 and SW2
- EXEC > show interfaces

Devices on the same Vlan can only communicate with those in the Vlan, if they want to communicate outside of the Vlan, a router is needed which is layer 3, and layer 3 information is needed.

Video 6: Routing, Switching, Trunking





Packet Tracer Lab 2020-04-07

Try it yourself first! Download the PT lab here
https://TheKeithBarker.com

Lab Objectives:

- PCs 1,3 in VLAN 10, Subnet 10.16.0.0 /24
- PCs 2,4 in VLAN 20, Subnet 172.16.0.0/24
- DHCP assigned addresses for PCs
- DHCP/Web sever in VLAN 777, Subnet 192.168.1.0/24, using .100
- Default G/W is .1 in each subnet
- Verify clients can ping each other
- Verify clients can open the web page of server at **TheKeithBarker.com**

Have fun!

Commands to remember to use:
SW1
Conf t
No ip domain-lookup
Line con 0
Logging synch
No exec-timeout
Privi level 15
Exit or end
Spann mode rapid
Spann portf default
Hostname
SW1 and SW2
Conf t
Vtp domain ogit
Int range fa0/11
Switch mode trunk
End
SW1 and SW2
Conf t
Int gig0/1
Sw mode trunk
End.
SW3
Conf t
Int range gig0/1-2
Sw trunk encapsulation dot1q
Switchport mode trunk
Exit
Conf t
Vtp domain ogit
end
Vlan10
Vlan20
Vlan 777
Show vlan brief
Show int trunk

SW1 -fa0/1
Conf t
Int fa 0/1
Sw mode access

Switchport access vlan10
Int fa 0/2
Sw mode access
Switchport access vlan 20
Show vlan brief

SW2- Fa0/3 and fa0/4
Int fa0/3
Sw mode access
Switchport access vlan 10
Int fa0/4
Sw mode access
Switchport mode vlan 20

The Server needs to be in vlan 777
Conf t
Int fa0/5
Sw mode access
Switchport access vlan 777
Server1 Web Services
Configure > Interface > 192.168.1.100 > settings (its default gateway is 192.168.1.1 > It needs to be able to communicate with its local Vlan 777 network
In the server1 we need to configure DHCP DNS by adding Vlan 10 and vlan 20 with their appropriate default gateway. Then add a Start IP address, with the maximum number of users of 10 then click add to save this configuration and add it to the rule pane.

In SW3 >
Show vlan brief
Show Ip interface brief
Conf t
Interface vlan 10
add 10.16.0.1 255.255.255.0
Int vlan 20
Add 172.16.0.1 255.255.255.0
Interface vlan 777
Add 192.168.1.1 255.255.255.0
Show ip interface brief
Multiply vlan services > SW3
Conf t
Int vlan 10
Ip add <IP Address, Subnet>
Int vlan 20
Ip add <IP Address, Subnet>
Int vlan 777
Ip add <IP Address, Subnet>

In Router > Configuration
Int vlan 10
Ip helper-address <192.168.1.100> which is Server1
Do the same to vlan 20
Int vlan 20
Ip helper-address <192.168.1.100> Server1

SW3: Make sure the router is configured to route IP's
Command: ip routing in the routing switch.
Show ip route

Behind the scenes when any of these clients head to this web address it is using DNS of the website, it is a A record for the webserver.

- DHCP
- DHCP routing
- DHCP Trunking ports
- DHCP access ports
- DHCP relay
- Multi-layered
- SVI

VIDEO 7
Spanning Tree Protocol

Why do we have layer 2 loops in a network?
Why is it a problem?

Arp -a command :

- Will display the cache consisting of all the layer 2 addresses that that knows in the network.
- To reach and forward a frame to .30 it would use the layer two address of .30

If there is redundant paths, looping endlessly, a protocol analyzer >

- We want to ping from .10 to .30 > links in red represents configured trunks (make sure you configure that). Link that multiple vlans can travel through.
- Ping .30
    - If the layer 2 address is not in the cache an arp request needs to be sent to gather that detail.
        - Arp -d * erases arp cache
        - So when you ping from .10 to .30 the address resolution protocol needs to happen again.
            - There for it will capture the layer 2 address again an put it in it's .10 arp cache.
- Use Wireshark to see those arp request and see the details.
- Broadcast : ff:ff:ff:ff:ff:ff:ff:ff redundant packets would loop forever...
- TTL (time to live details)
    - When packet gets routed the ttl will get decremented every time that same packet gets routed back.
        - When that ttl reaches 0 then the router will not forward that packet.

Spanning Tree has to hit the right links, ports, to stop forwarding traffic.

There is no ttl function inside the header, unless we have identified paralleled paths:
Take a group of switches bpdu (Bridge Protocol data unit) can identify multiple routes, although they can choose one route, called a route bridge or route switch.

- Bridge ID
    - All switches will have a bridge ID
    - The lowest Bridge ID will be the newest routing bridge.
    - Core of the tree of the Spanning Tree
        - Which port is the least cost effective.
        - Root Port
            - Each are only going to have that port that is the fastest to the routing bridge.
                - Least cost of port will be the root port of each switch, forwarding to the core of route switch.
                - Giga bit links are a cost of 4
- Root port is also called a role
    - Status of forwarding direction of root bridge
    - Forwarding Away = ports is called a designated port
        - Always forwarding.

Loops that are not kept in check there will be many broadcast storms.

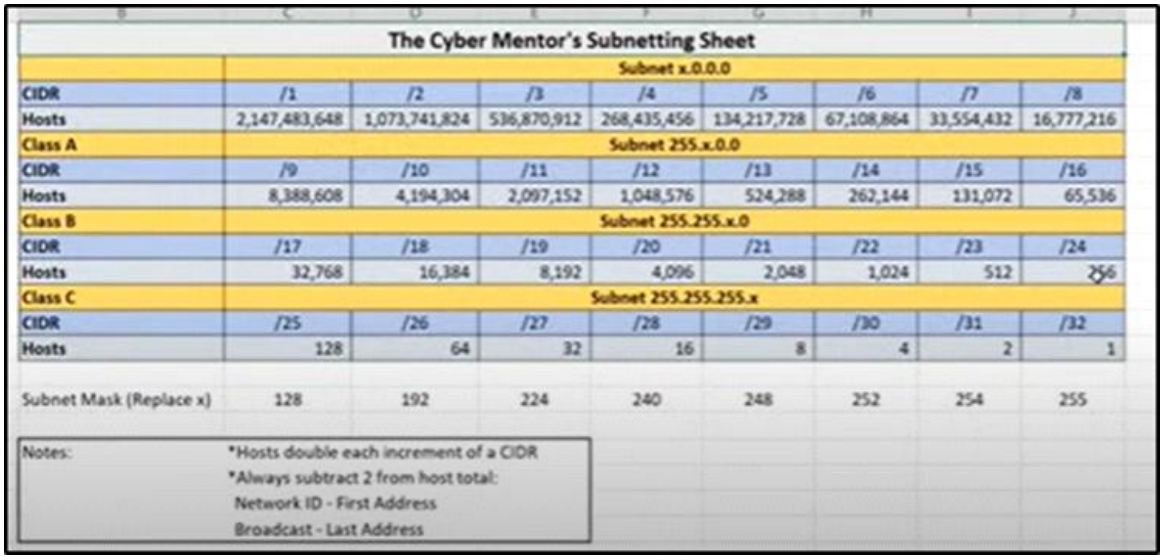
SW3 STP > Root Bridge > lowest cost > root Bridge > root ports (fwd towards root > Designated port (FWD away root bridge)

Every connection between two switches

- Designated port
- Blocking ports
    - If both cost is the same to get to root, the lowest cost will be root port
    - Designated port will then be determined by the lowest cost BID of the two ports.

If there are two switches with the same cost from the root, the switches look at the senders port ID cost, and whichever is the lowest wins and becomes the root.

Subnetting



The Cyber Mentor's Subnetting Sheet								
	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
Class A	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
Class B	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
Class C	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

Notes:
*Hosts double each increment of a CIDR
*Always subtract 2 from host total:
Network ID - First Address
Broadcast - Last Address

Notes:

- Hosts double each increment of a CIDR
- Always subtract 2 from host total
  - Top and bottom numbers
    - Network ID
      - First Address (Bottom Number)
    - Broadcast Address
      - Last Address (Top Number)

Whack <CIDR>

- /16, /24,

				Subnet x.0.0.0				
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Host	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
Class A				Subnet 255.x.0.0				
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Host	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
Class B				Subnet 255.255.x.0				
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Host	32,768	16,384	8,192	4,096	2,048	1,024	512	256
Class C				Subnet 255.255.255.x				
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Host	128	64	32	16	8	4	2	1
Subnet Mask Replace	128	192	224	240	248	252	254	255