LAB SESSION WEEK 4 – TUTORIAL NOTES

GENERAL INFORMATION

1. Labs will continue to run online during week 5
2. Next Week (week 5) we have our first group activity
    - You MUST be present in the lab session to participate
    - You MUST have finished the day's practice
    - **Groups will be formed among students <u>in the session</u>**
    - Activity handout will be made available on the day
3. Clean up the devices before the practice
    - Remove the startup-config file using **write erase**
    - Remove the vlan.dat file using **delete vlan.dat**
    - **Reload** and say **no** if asked to save the settings
    - Switch clean-up demo available in Echo360.

REVISION

The management VLAN

- Management IP on interface VLAN
- Best Practice not to use VLAN 1
- Only for management. Do not place host in the management VLAN
- In L2 Switches, we should only have 1 active interface VLAN → major error if more
- In Lab SU-3a You had to set up a trunk for switches to ping each other
- Then you could test telnet/ssh from one switch to the other.

Remote Access

- Telnet/SSH → plain text/encrypted communication
- What where the steps needed before enable SSH management?
    - Configure FQDN
    - Create encryption keys (certificate)
    - Create local user account (username/password)
    - Allow SSH as transport input in the line vty
    - Specify **login local** in the line vty
- Remote access connections are less trustworthy than console connections
    - If Telnet → must have an enable password to go to admin mode
    - If SSH → must have a user with the right privileged level

Switch Security Basics

- Line vty and console passwords (we don't do in future labs)
- Best practice is to use SSH for management (encrypted)
- Remove ports from default VLAN
- Shutdown unused ports

Port Security

- MUST be enabled first with the **switchport por-security**.
- Control how many MAC addresses are allowed to forward traffic on a switchport
- Control which MAC address can connect on a switchport
- What were the three types of violation actions? Shutdown, restrict, protect
- What were the three methods to allow MAC addresses in a port? Static, dynamic, sticky
- How do you come back from an **err-disable** state?
    - Shutdown the interface
    - Fix the issue that cause the violation
    - Unshut the interface
- How do you verify the err-disable state? → **sh int <int_ID>**

Some show commands

sh vlan → verify vlan database

sh ip int brief → verify IP on management VLAN and the status

A VLAN interface always **physically up**.

When is it **protocol down**?

You have NOT configured the VLAN

There are no active ports for the VLAN

sh port-security → port-security summary

sh port-security interface <if_id> → port-security settings and status for that interface

sh interface <if_id> → more in detail information for a given interface

VLAN database

1. You create VLANs from the CLI, but they are not saved to the running config file
2. Instead they are saved to the **vlan.dat** file in the Flash
3. To remove a single (or a few) VLANs you can use the *<no vlan>* command
4. To remove all VLANs is easier to delete the **vlan.dat** file

VLAN Membership

1. Once you "break" a switch into multiple L2 segments (i.e. VLANS), you can specify to which segment each switchport belongs to
2. Ports belonging to only one VLAN are called "access ports". End hosts connect to access ports.
3. By default, all ports belong to VLAN 1 → good practice to change them to a "parking" or "blackhole" VLAN

Lab SU-3a reflection

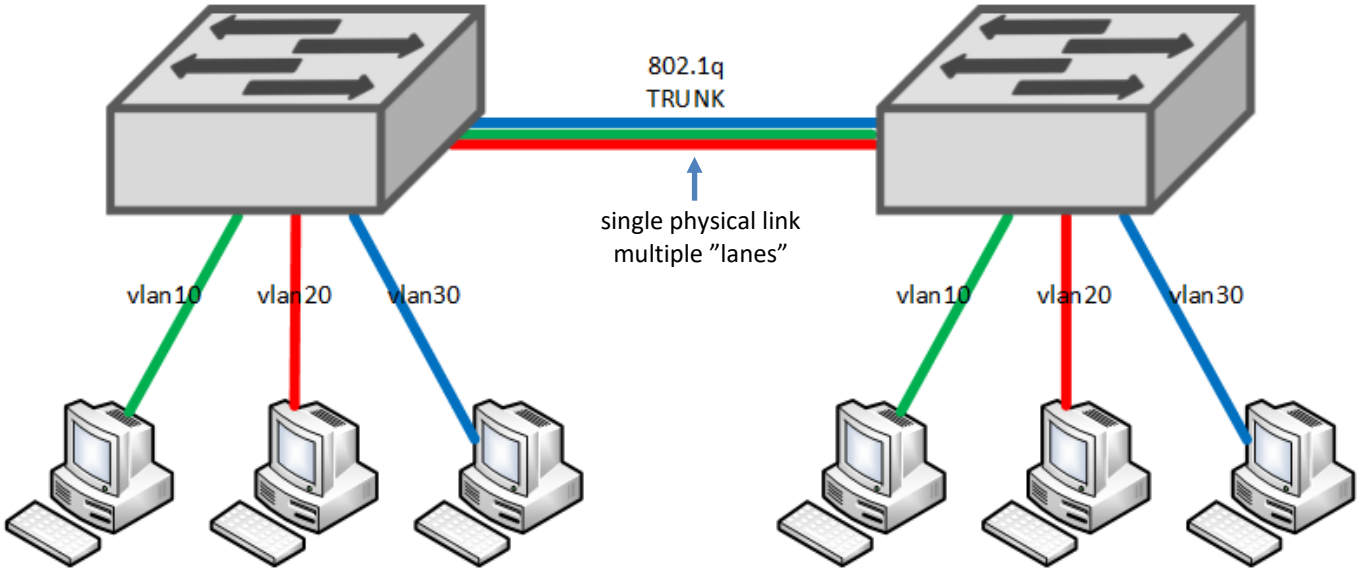
Let's answer the lab handout questions from last week.

TUTORIAL

802.1q

1. Frames are tagged with an 802.1q identifier showing to which VLAN they belong to
2. Usually, frames coming from end hosts enter the switch untagged.
3. When forward to another switch over a “trunk” they need to be tagged

   This is how the receiving device knows to which VLAN it belongs
4. Frames are tagged according to the VLAN membership of the incoming switchport
5. When interconnecting switches handling multiple VLANs the interconnection should be set as an 802.1q **trunk**



Dynamic Trunking Protocol

1. We can force the switchport mode → trunk or access
2. We can also let the switches negotiate the mode using DTP
3. Switchport Modes → refer to the table below
4. **Best practice is to set the switchport mode to trunk or access**

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

Subnetting

1. Legacy Classful Networks:
    - From the times when we thought the IPv4 address space was enough
    - Address would be broken into several networks of 3 different sizes only
    - Large Networks: Class A

      8 net bits

      24 host bits → 2^24
    - Medium Networks: Class B

      16 net bits

16 host bits → 2^16 = 65536

- Small Networks: Class C

  24 net bits

  8 host bits → 2^8 = 256

- The value of the 1st octet defines the legacy Class of a Network
- The legacy Class of a Network defines its ***classful mask***

	1st Octet value convention	1st Octet first combination		1st Octet last combination
Class A CIDR /8 2^24 addresses	Leftmost bit set to 0	00000001 1	-	01111111 127
Class B CIDR /16 2^16 addresses	2 Leftmost bits set to 10	10000000 128	- -	10111111 191
Class C CIDR /24 2^8 addresses	3 Leftmost bits set to 110	11000000 192	- -	11011111 223

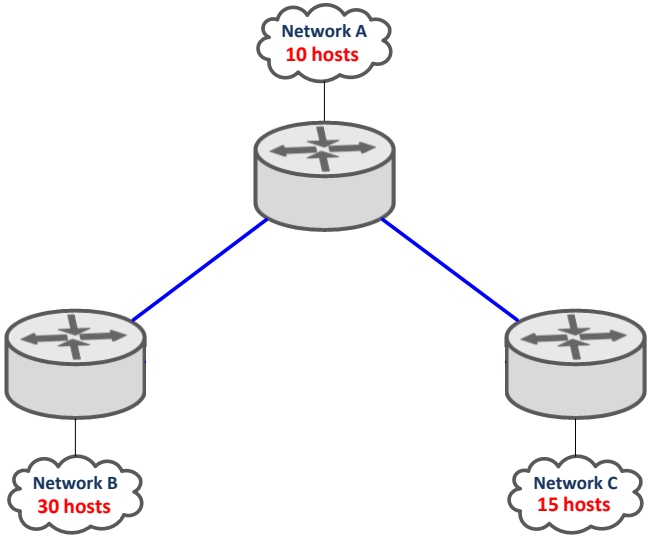
2. Classful subnetting:
   - Break major classful network into same-size subnets
   - Inefficient approach → tend to waste IP addresses

3. Variable Length Subnet Mask:
    - Break a network (or subnet) into smaller custom-size subnets
    - The size of the network is calculated as per host requirements
    - The number of host bits dictates the size of the network → 2^n – 2
    - Why -2? → Network Address and Broadcast address
    - For example, if we have 8 hosts → We need to provide for 14 usable IPs
4. When VLSM, we MUST arrange our networks from the largest to the smallest
    - If we don't arrange them, we might end up having gaps between subnets

Classful subletting exercise

Major Network: 192.168.10.0/24

Refer to diagram for Network and Host requirements



Solution:

- How many networks do we need? → 5
- How many usable IP addresses on each network? → 30
- How many host bits? → 32 = 2^5 → 5 host bits
- How many network bits? → 32 – 5 → 27 network bits
- Subnet mask? → /27 or 255.255.255.224 → same for all networks

11111111	.	**11111111**	.	**11111111**	.	**11100000**
255	.	255	.	255		128+64+32
255	.	255	.	255	.	224

- LAN A Network address → 192.168.10.0 /27

192	.	168	.	10	.	**00000000**
192	.	168	.	10	.	0

- LAN A Broadcast Address → 192.168.10.31

192	.	168	.	10	.	**00011111**
192	.	168	.	10	.	31

- LAN B Network address → 192.168.10.32 /27

192 . 168 . 10 . **00100000**
192 . 168 . 10 . 32

- LAN B Broadcast Address → 192.168.10.63

192 . 168 . 10 . **00111111**
192 . 168 . 10 . 63

- LAN C Network address → 192.168.10.64 /27

192 . 168 . 10 . **01000000**
192 . 168 . 10 . 64

- LAN C Broadcast Address → 192.168.10.95

192 . 168 . 10 . **01011111**
192 . 168 . 10 . 95

- Link 1 Network address → 192.168.10.96

192 . 168 . 10 . **01100000**
192 . 168 . 10 . 96

- Link 1 Broadcast Address → 192.168.10.127

192 . 168 . 10 . **01111111**
192 . 168 . 10 . 127

- Link 2 Network address → 192.168.10.128

192 . 168 . 10 . **10000000**
192 . 168 . 10 . 128

- Link 2 Broadcast Address → 192.168.10.159

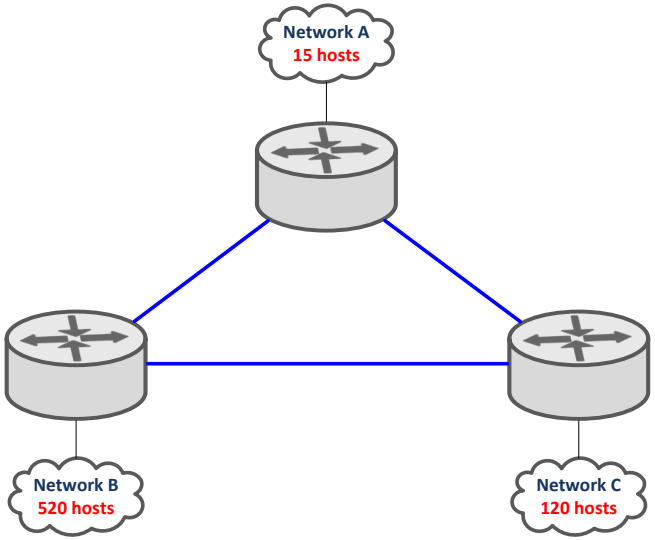
192 . 168 . 10 . **10011111**
192 . 168 . 10 . 159

VLSM exercise:

Note: this one is for students to attempt in their own time if they want. Will be demonstrated next week during tutorial time.

Major Network: 172.16.0.0/16

Refer to diagram for Network and Host requirements



Solution:

- How many networks do we need? 6
- Arrange the Networks by size:
  - Network B
  - Network C
  - Network A
  - Link 1
  - Link 2
  - Link 3

Network B:

- How many usable IP addresses? → 1024 – 2 = 1022
- How many host bits? → 1024 = 2^10 → 10 host bits
- How many network bits? → 32 bits – 10 host bits → 22 network bits
- Subnet mask? →
- Subnet mask in dotted decimal notation? → 255.255.252.0

11111111	.	**11111111**	.	**11111100**	.	**00000000**
255	.	255	.	128+64+32 +16+8+4		0
255	.	255	.	252	.	0

- Network address → 172.16.0.0/22

172	.	16		**0000000**	.	**0000000**
172	.	16		0	.	0

- Broadcast Address → 172.16.3.0

172	.	16	**0000011**	.	**11111111**
172	.	16	3	.	255

Network C:

- How many usable IP addresses? → 128 – 2 = 126
- How many host bits? → 128 = 2^7 → 7 host bits
- How many network bits? → 32 bits – 7 host bits → 25 network bits
- Subnet mask? → /25
- Subnet mask in dotted decimal notation? → 255.255.255.128

11111111 . **11111111** . **11111111** . **10000000**

255 . 255 . 255 . 128

- Network address → 172.16.4.0

172 . 16 . **0000100** . **00000000**

172 . 16 . 4 . 0

- Broadcast Address → 172.16.4.127

172 . 16 . **00000100** . **01111111**

172 . 16 . 4 . 64+32+16+8+4+2+1

172 . 16 . 4 . 127

Network A:

- How many usable IP addresses? → 32 – 2 = 30
- How many host bits? → 32 = 2^5 → 5 host bits
- How many network bits? → 32 bits – 5 host bits → 27 network bits
- Subnet mask? → /27
- Subnet mask in dotted decimal notation? → 255.255.255.224

11111111	.	**11111111**	.	**11111111**	.	**11100000**
255	.	255	.	255		128+64+32
255	.	255	.	255	.	224

- Network address → 172.16.4.128

172	.	16	.	**0000100**	.	**10000000**
172	.	16	.	4	.	128

- Broadcast Address → 172.16.4.159

172	.	16	.	**00000100**	.	**10011111**
172	.	16	.	4	.	128+16+8+4+2+1
172	.	16	.	4	.	159

Link 1:

- How many usable IP addresses? → 4 – 2 = 2
- How many host bits? → 4 = 2^2 → 2 host bits
- How many network bits? → 32 bits – 2 host bits → 30 network bits
- Subnet mask? → /30
- Subnet mask in dotted decimal notation? → 255.255.255.252

11111111	.	**11111111**	.	**11111111**	.	**11111100**	
255	.	255	.	255		128+64+32+16+8+4	
255	.	255	.	255	.	252	

- Network address → 172.16.4.160

172	.	16	.	**0000100**	.	**10100000**	
172	.	16	.	4	.	128+32	
172	.	16	.	4	.	160	

- Broadcast Address → 172.16.4.163

172	.	16	.	**0000100**	.	**10100011**	
172	.	16	.	4	.	128+32+ 2+1	
172	.	16	.	4	.	163	

Calculate Link 2 and Link 3's Networks.