Introduction to Enterprise Networks

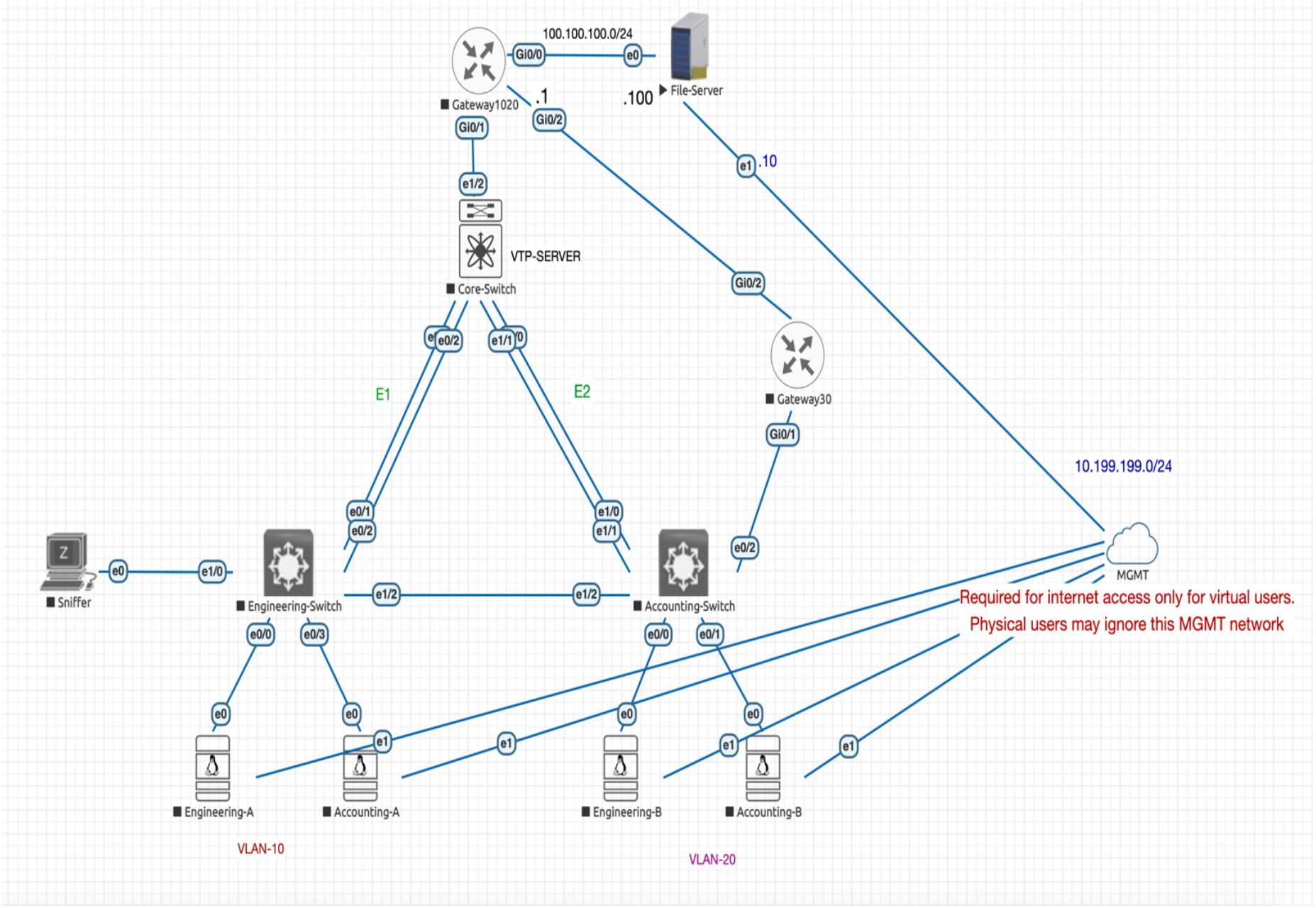
Lab 1

Learning about Switches

Spring 2025

OBJECTIVES

1. **Learn how to perform basic switch configuration & troubleshooting including.**
    a. **Review basics for the switch password assignment and IOS navigation**
    b. **How to activate/deactivate a Port**
    c. **How to change the Speed and Duplex Mode on a Switch port**
    d. **How to verify the MAC addresses of computers connected to a specific port**
2. **Learn how to secure a Switch port so that only a specific user/device can connect.**
3. **Learn how to Create VLANs within a single Switch**
4. **Learn how to create VLANs across multiple Switches**
5. **Learn how to achieve Inter-VLAN communication using Trunking Protocols such as 801q and ISL**
6. **Configure VLAN Trunking Protocol (VTP) to manage multiple switches from a single one**
7. **Review the usage of Spanning Tree Protocol and how the switching environment behaves in the event of a network failure**
8. **Learn how Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1W is essential for faster convergence**
9. **Learn to increase the efficiency of a redundant network (PVST)**
10. **Learn about optional STP features like “Portfast” and “Etherchannel”**
11. **Sniff packets from your network.**


100.100.100.0/24
Gi0/0
e0
Gateway1020
.1
.100
File-Server
Gi0/1
Gi0/2
e1
.10
e1/2
VTP-SERVER
Core-Switch
Gi0/2
e0/2
e1/1
E1
E2
Gateway30
Gi0/1
10.199.199.0/24
e0/1
e0/2
e1/0
e1/1
e0/2
MGMT
Sniffer
e0
e1/0
Engineering-Switch
e1/2
e1/2
Accounting-Switch
Required for internet access only for virtual users.
Physical users may ignore this MGMT network
e0/0
e0/3
e0/0
e0/1
e0
e0
e0
e0
e1
e1
e1
e1
e1
Engineering-A
Accounting-A
Engineering-B
Accounting-B
VLAN-10
VLAN-20

Scenario:

A company named **TechCorp** has two departments: **Engineering** and **Accounting**. Both departments need access to a centralized server, which hosts separate directories for each department. The server is located on a separate network (All required routes are configured for this lab), and the two departments are located on different VLANs. Inter-VLAN communication should be restricted except for accessing the server to ensure security and proper isolation.

Objectives:

1. **Basic Switch Configuration:**
   - Set up basic switch configurations, setup SSH on the Engineering-Switch and the Accounting-Switch including password protection and IOS navigation.

   Engineering:

   SSH command for Windows PC: ssh -oCiphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@192.168.1.10

   Accounting

   SSH command for Windows PC: ssh -oCiphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@192.168.1.20

   - OUTCOME: PCx should be able to SSH to all the switches in the network

     Report the commands with screenshots

```
!
interface Vlan1
 ip address 192.168.1.10 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

```
!
username admin privilege 15 password 0 admin
!
```

```
ip domain-name engineering.com
```

```
C:\Users\NetEngComputer6>ssh -oCiphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@192.168.1.20
The authenticity of host '192.168.1.20 (192.168.1.20)' can't be established.
RSA key fingerprint is SHA256:ajpcPM/9NU7u87OSQB58hg4wyWDgW8s10tyZHiOnhuI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.20' (RSA) to the list of known hosts.
Password:

Accounting#
Accounting#
Accounting#exit
Connection to 192.168.1.20 closed by remote host.
Connection to 192.168.1.20 closed.

C:\Users\NetEngComputer6>ssh -oCiphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@192.168.1.10
Password:

Engineering#
Engineering#
Engineering#
```

2. Default Switch Connectivity Test

- Activate and deactivate specific switch ports connected to each client as needed.
- Assign IP addresses of your choice (/24) and ping from one client to another using the default VLAN.

```
[(base) loganchayet@econ2-203-15-dhcp ~ % ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=128 time=1.184 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=0.935 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=0.891 ms
^C
--- 192.168.1.100 ping statistics ---
```

- Show the interfaces status on both switches. Use ‘show interface status’ or ‘show ip interface brief’

```
Engineering#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.10    YES manual up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
```

```
Accounting#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.20    YES manual up                    up
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
```

- Change port speed to 10Mbps and duplex mode to half for the port connected to Engineering-A.

```
!
interface GigabitEthernet1/0/3
 speed 10
 duplex half
!
```

Turn on debugging and report any changes you see when the port is in half or full duplex mode

- Verify connected devices using show mac address-table. On both switches.

```
[Accounting#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001b.0c7f.6681    DYNAMIC     Gi1/0/1
   1    001b.0c7f.66c0    DYNAMIC     Gi1/0/1
   1    5c26.0a24.8ec5    DYNAMIC     Gi1/0/1
   1    6c6e.0715.1211    DYNAMIC     Gi1/0/3
Total Mac Addresses for this criterion: 24
Accounting#
```

```
[Engineering#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001d.a1b3.7e01    DYNAMIC     Gi1/0/1
   1    001d.a1b3.7e40    DYNAMIC     Gi1/0/1
   1    5c26.0a24.8ec5    DYNAMIC     Gi1/0/3
   1    6c6e.0715.1211    DYNAMIC     Gi1/0/1
Total Mac Addresses for this criterion: 24
```

- OUTCOME: See how mac addresses are learned by all switches, for all systems connected.

  Attach the screenshots

3. **Port Security Configuration:**

- Configure port security on ethernet0/3 on the Accounting-Switch to ensure that only Accounting-B user can connect to this port.
  First, add the mac-address of Accounting-B manually and once again configure in such way that the mac-address is read automatically from the switch.

Manual:

```
Accounting(config-if)#do show port-security int gi 1/0/3
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Accounting(config-if)#do show port-security int gi 1/0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 5c26.0a24.8f5a:1
Security Violation Count   : 1
```

```
!
interface GigabitEthernet1/0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address 5c26.0a24.8f5a vlan access
!
```

Automatic:

```
!
interface GigabitEthernet1/0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface GigabitEthernet1/0/4
```

```
[Accounting(config-if)#do show port-security int gi 1/0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 5c26.0a24.8f5a:1
Security Violation Count   : 0
```

- Add a new client and test the security policy by swapping cables between devices and verify the console messages when unauthorized devices attempt to connect.

```
[Accounting#
[Accounting#
[Accounting#show port-security interface gigabitEthernet 1/0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 5c26.0a24.8f4e:1
Security Violation Count   : 1
```

***SAVE your config on the switch and clients then shut down the nodes before swapping cables.

Verify that your port security works, and its reversible once approved system is restored.

- OUTCOME: Prove that only a particular mac-address/system can connect to a unique physical port, and if you connect a different computer, port with stop its functionality

Report the commands you used and the screenshots of the debug messages.

- Debug interface gi 1/0/3
- Debug port-security

Restore network connectivity without reconnecting equipment. (**Adjust security policy only)**

- **Did a shut and no shut**

4. **Switch VLAN Configuration:**
   - Create VLANs for each department on each switch:

    - VLAN 10: **Engineering**
    - VLAN 20: **Accounting**
- Assign the ports connecting to each department's devices to the appropriate VLAN.
- Configure the single port between the two switches (e1/2) as a trunk to allow communication with both VLANs.

Here is the config to all of the points above:

```
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5c26.0a24.8f5a vlan access
!
interface GigabitEthernet1/0/4
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------
1    default                          active    Gi1/0/2, Gi
                                                Gi1/0/19, G
                                                Gi1/0/34, G
                                                Gi1/0/49, G
10   Engineering                      active    Gi1/0/3
20   Accounting                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Accounting#
```

Vlan 10
Name engineering
Vlan 20
Name accounting

- Which trunking encapsulation was supported by both Switches by default? What other options are available? Use all variants and test end-to-end connectivity.
    - Dot1q. The other options available are ISL and negotiate.
    - Verify it does have connectivity with ISL and negotiate
- Verify that devices within the same VLAN can communicate, but devices from different VLANs cannot.

- Ping from Engineering to Engineering

```
C:\Users\NetEngComputer6>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Ping from Engineering to Accounting. What is the result?

```
C:\Users\NetEngComputer6>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Request timed out.
Request timed out.
```

They could not ping each other, they are in different VLANs.

- OUTCOME: Verify VLAN isolation for each respective department. Users of each department should only be able to ping their members

Report the commands + screenshots

5. **Router-on-a-Stick for Inter-VLAN Communication:**
   - Use the router to enable inter-VLAN communication only for the purpose of accessing the server, and pinging across approved departments
   - Configure sub-interfaces on the Gateway1020 for VLAN 10 and VLAN 20, each with a different IP address in their respective subnets.
   - Use a /24 for Engineering and a /27 for Accounting.
   - Configure one port from the core switch to the Gateway1020 to enable inter-vlan connectivity. (Access or Trunk?)
     - Trunk
   - Ensure that the router provides access to both Engineering and Accounting to the Fileserver through their respective default gateway.
   - Do you need to worry about using the same IP addressing on Different VLANs? Why or why not?
     - I do need to work about using the same IP addressing. While it is possible, it can raise problems with routing conflicts and broadcast/arp issues
   - OUTCOME: Engineering and Accounting departments should be able to reach their respective default gateways and visit the Fileserver.

Accounting and Engineering being able to ping each other hence being able to reach DG:

```
^C
C:\Users\NetEngComputer6>ping 192.168.2.11 -S 192.168.1.10

Pinging 192.168.2.11 from 192.168.1.10 with 32 bytes of data:
Reply from 192.168.2.11: bytes=32 time<1ms TTL=127
Reply from 192.168.2.11: bytes=32 time<1ms TTL=127
Reply from 192.168.2.11: bytes=32 time=14ms TTL=127
Reply from 192.168.2.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Report the commands you used on the core switch and the DG for inter-vlan configuration

Commands used:

Core:

```
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Gateway 1020:

```
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
!
interface Serial0/2/0
```

6. **Multiple Simultaneous Switch VLAN Configuration using VTP ( ):**
   - The core switch provides access to the DG

     *You can add new vlans to the server and propagate them to other switches in the network without having them configured manually on other switches.

   - Configure the core switch as a VTP server, and the Accounting-Switch as a VTP client
   - Leave the Engineering-Switch as transparent.

```
Core(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : lab1
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aca0.16b6.7600
Configuration last modified by 192.168.1.150 at 3-10-93 06:17:43
Local updater ID is 192.168.1.150 on interface V110 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 3
MD5 digest                        : 0x0E 0xFC 0xE8 0x64 0xEF 0x12 0x38 0x18
                                    0x38 0x87 0x85 0xE6 0x49 0x44 0x0F 0x6A

Core(config)#x
Engineering(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : lab1
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 001b.0c7f.6680
Configuration last modified by 192.168.1.100 at 3-10-93 05:45:24

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 0
MD5 digest                        : 0xCA 0xCA 0xD8 0xAE 0xD4 0x01 0xA6 0x2F
                                    0xB2 0x71 0xF7 0x88 0xE3 0x25 0xB8 0x47

Engineering(config)#
Cannot modify version in VTP client mode unless the system is in VTP version 3
Accounting(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : lab1
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 001d.a1b3.7e00
Configuration last modified by 192.168.1.150 at 3-10-93 05:45:24

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xC3 0x6E 0x89 0x09 0x3A 0xD4 0xB9 0xDA
                                    0x5E 0xE0 0x07 0x22 0xE9 0x6F 0xC0 0xEE

Accounting(config)#vtp ver
```

- Add a new VLAN (30) on the core switch and make sure that the new VLAN is updated automatically on the other switches.
  VLAN 30 is updated on the VTP client and not transparent as it doesn't participate in the same domain as the server, just forwards info for other VTP clients.
- Configure different versions and password protection for the VTP.
  I configured password proctection on all switches and different versions as well (1,2,3).
- Configure trunk ports between the switches.
- Change the name of Accounting VLAN to HumanRes ONLY on the core switch. Verify that the Accounting-Switch adjusts to the new changes automatically as result of VTP.

Report from Switch IOS VLAN name propagation

```
Accounting#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/49
                                                Gi1/0/50, Gi1/0/51, Gi1/0/52
10   Engineering                      active    Gi1/0/3
20   Accounting                       active    Gi1/0/4
30   HumanRes                         active
1002 fddi-default                     act/unsup
```

- Connect a new Client name it as “Archive” to the Accounting-Switch in VLAN-30
- Ensure proper reachability to its default gateway Gateway30.

MAKE SURE TO SAVE YOUR CONFIGS BEFORE ADDING NEW NODES

Report the commands used for VTP versions, mode, domain, security and pruning + screenshots of the debug messages and the show results.

Commands used:

Core SW:

vtp mode server

vtp domain lab1

vtp password admin

vtp version 3

Engineering:

vtp mode transparent

vtp domain lab1 # Optional: Not required but good for consistency

vtp password admin

vtp version 3

Accounting:

vtp mode client

vtp domain lab1

vtp password admin

vtp version 3

* show vtp counters

```
Core(config)#end
Core#show vtp counters
*Mar 10 06:41:45.392: %SYS-5-CONFIG_I: Configured from console by console
VTP statistics:
Summary advertisements received    : 10
Subset advertisements received     : 8
Request advertisements received    : 3
Summary advertisements transmitted : 23
Subset advertisements transmitted  : 15
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0


VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- --------------------------
Gi1/0/1             0                0                0
Gi1/0/23            0                1                0
Gi1/0/24            0                1                0
Core#
```

* show vtp status

```
Core#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : lab1
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aca0.16b6.7600
Configuration last modified by 192.168.1.150 at 3-10-93 06:32:52
Local updater ID is 192.168.1.150 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 5
MD5 digest                      : 0x7C 0x1C 0xC6 0x41 0xBA 0x69 0x07 0x70
                                  0x2B 0x02 0xE8 0xA7 0x8B 0x39 0x59 0x44
Core#
```

OUTCOME: Understand the different roles of VTP, understand how changes are propagated automatically by this feature, and what must be manually configured.

6.1 MULTI-HOP Routing

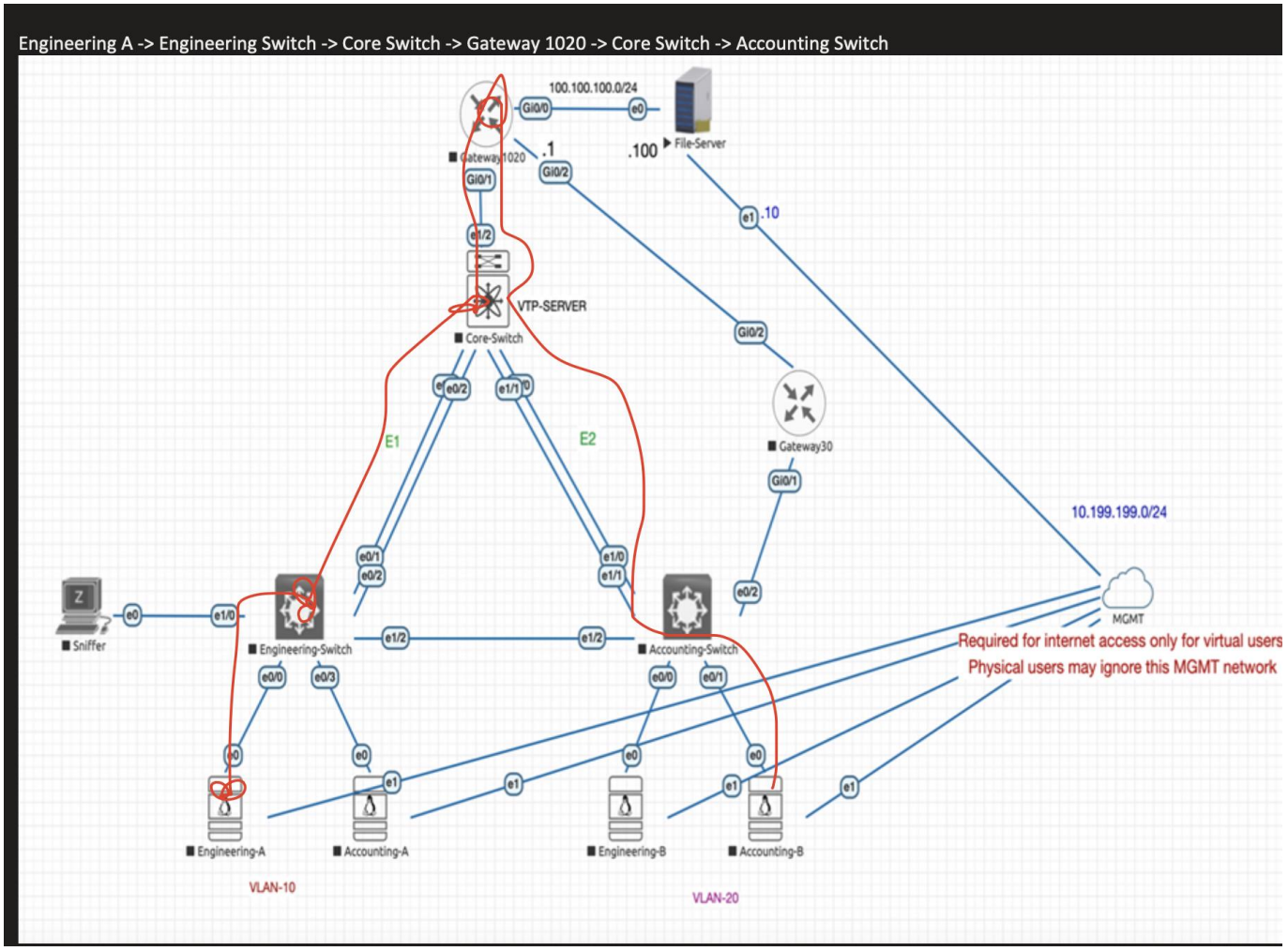
- Make configuration needed for Archive client to ping all other systems and the FileServer (via its respective default gateway) NOTE that Engineeirng and accounting make use of Gateway1020 for their traffic, while Archive uses Gateway30 for its connectivity. (HINT: use static routes)

Traceroute proving connectivity from Archive:

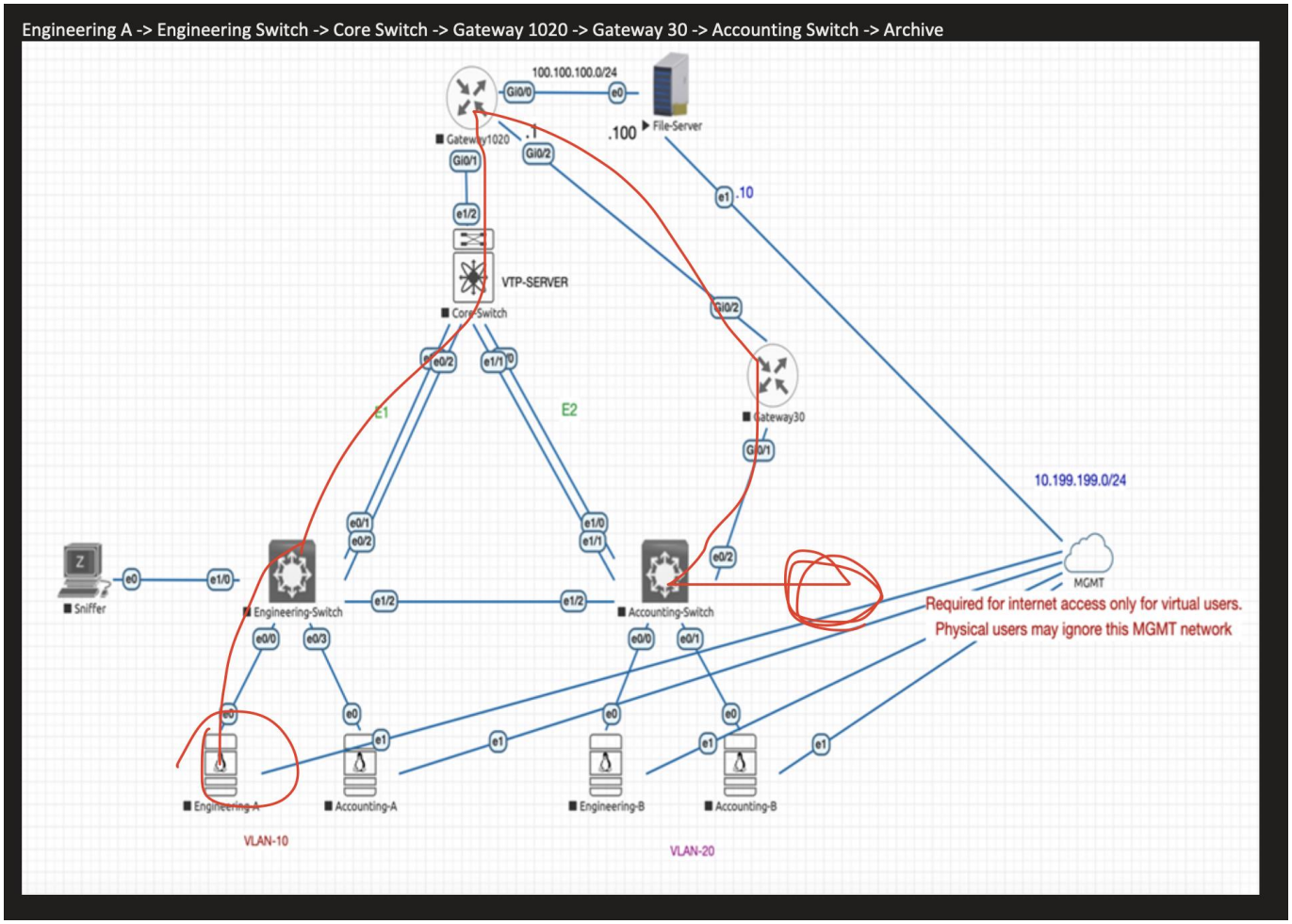
```
C:\Users\NetEngComputer6>tracert 192.168.3.10

Tracing route to DESKTOP-SGMPP6U [192.168.3.10]
over a maximum of 30 hops:

  1    <1 ms     1 ms     7 ms  192.168.1.1
  2    <1 ms     2 ms    <1 ms  10.0.0.2
  3     2 ms    <1 ms    <1 ms  DESKTOP-SGMPP6U [192.168.3.10]

Trace complete.
```

- Add in your report 2 diagrams explaining how packets travel from Engineering to Accounting, and from Archive to Either one of them.

Engineering to Accounting:



Archive to Engineering



- OUTCOME: Understand the need for a routing table to reach remote networks beyond default-gateway connectivity.

7. **Spanning Tree Protocol (STP) Configuration:**

   no debug spanning-tree bpdu

   no debug spanning-tree switch all

   Keep “debug spanning-tree bpdu” and “debug spanning-tree switch” ON on the core switch. Explain the messages generated from these commands when the topology changes.

```
*Mar 14 02:19:13.175:      T:0000 L:0002 D:000A
*Mar 14 02:19:13.175: STP: VLAN0010 rx BPDU: config protocol = ieee, packet from GigabitEthernet1/0/24  , linktype SSTP , enctype 3, encsize 22
*Mar 14 02:19:13.175: STP: enc 01 00 0C CC CC CD 00 1D A1 B3 7E 30 00 32 AA AA 03 00 00 0C 01 0B
*Mar 14 02:19:13.175: STP: Data     0000000000800A001B0C7F6680000000004800A001DA1B37E00803001001400002000F00
*Mar 14 02:19:13.175: STP: VLAN0010 Gi1/0/24:0000 00 00 00 800A001B0C7F6680 00000004 800A001DA1B37E00 8030 0100 1400 0200 0F00
*Mar 14 02:19:13.175: STP(10) port Gi1/0/24 supersedes 0
*Mar 14 02:19:13.175: STP SW: PROC RX: 0100.0ccc.cccd<-001d.a1b3.7e30 type/len 0032
*Mar 14 02:19:13.175:     encap SNAP linktype sstp vlan 1 len 64 on v1 Gi1/0/24
*Mar 14 02:19:13.175:     AATP
*Mar 14 02:19:13.175:     CFG P:0000 V:00 T:00 F:00 R:8001 001b.0c7f.6680 00000004
*Mar 14 02:19:13.175:     B:8001 001d.a1b3.7e00 80.30 A:0100 M:1400 H:0200 F:0F00 AA 03 00000C 010B SS
*Mar 14 02:19:13.175:      T:0000 L:0002 D:0001
*Mar 14 02:19:13.175: STP SW: PROC RX: 0180.c200.0000<-001d.a1b3.7e30 type/len 0026
*Mar 14 02:19:13.175:     encap SAP linktype ieee-st vlan 1 len 60 on v1 Gi1/0/24
*Mar 14 02:19:13.175:     42 42 03 SPAN
*Mar 14 02:19:13.175:     CFG P:0000 V:00 T:00 F:00 R:8001 001b.0c7f.6680 00000004
*Mar 14 02:19:13.175:     B:8001 001d.a1b3.7e00 80.30 A:0100 M:1400 H:0200 F:0F00
*Mar 14 02:19:13.175: STP: VLAN0001 rx BPDU: config protocol = ieee, packet from GigabitEthernet1/0/24  , linktype IEEE_SPANNING , enctype 2, encsize 17
*Mar 14 02:19:13.175: STP: enc 01 80 C2 00 00 00 00 1D A1 B3 7E 30 00 26 42 42 03
*Mar 14 02:19:13.175: STP: Data     0000000000800100180C7F6680000000048001001DA1B37E00803001001400002000F00
*Mar 14 02:19:13.175: STP: VLAN0001 Gi1/0/24:0000 00 00 00 8001001B0C7F6680 00000004 8001001DA1B37E00 8030 0100 1400 0200 0F00
*Mar 14 02:19:13.184: STP(1) port Gi1/0/24 supersedes 0
*Mar 14 02:19:13.184: STP SW: PROC RX: 0100.0ccc.cccd<-001d.a1b3.7e30 type/len 0032
*Mar 14 02:19:13.184:     encap SNAP linktype sstp vlan 20 len 64 on v20 Gi1/0/24
*Mar 14 02:19:13.18STP
*Mar 14 02:19:13.184:     CFG P:0000 V:00 T:00 F:00 R:8014 001b.0c7f.6680 00000004
*Mar 14 02:19:13.184:     B:8014 001d.a1b3.7e00 80.30 A:0100 M:1400 H:0200 F:0F004:     AA AA 03 00000C 010B S
*Mar 14 02:19:13.184:      T:0000 L:0002 D:0014
*Mar 14 02:19:13.184: STP: VLAN0020 rx BPDU: config protocol = ieee, packet from GigabitEthernet1/0/24  , linktype SSTP , enctype 3, encsize 22
*Mar 14 02:19:13.184: STP: enc 01 00 0C CC CC CD 00 1D A1 B3 7E 30 00 32 AA AA 03 00 00 0C 01 0B
*Mar 14 02:19:13.184: STP: Data     0000000000801400180C7F6680000000048014001DA1B37E00803001001400002000F00
*Mar 14 02:19:13.184: STP: VLAN0020 Gi1/0/24:0000 00 00 00 8014001B0C7F6680 00000004 8014001DA1B37E00 8030 0100 1400 0200 0F00
*Mar 14 02:19:13.184: STP(20) port Gi1/0/24 supersedes 0
*Mar 14 02:19:13.184: STP SW: PROC RX: 0100.0ccc.cccd<-001b.0c7f.66b0 type/len 0032
*Mar 14 02:19:13.184:     encap SNAP linktype sstp vlan 20 len 64 on v20 Gi1/0/23
*Mar 14 02:19:13.184:     AA AA 03 00000C 010B SSTP
*Mar 14 02:19:13.184:     CFG P:0000 V:00 T:00 F:00 R:8014 001b.0c7f.6680 00000000
*Mar 14 02:19:13.184:     B:8014 001b.0c7f.6680 80.30 A:0000 M:1400 H:0200 F:0F00
*Mar 14 02:19:13.184:      T:0000 L:0002 D:0014
*Mar 14 02:19:13.184: STP: VLAN0020 rx BPDU: config protocol = ieee, packet from GigabitEthernet1/0/23  , linktype SSTP , enctyp19:13.184: STP: enc 01 00 0C CC CC CD 00 1B 0C 7F 66 B0 00 32 AA AA 03 00 00
 0C 01 0B
*Mar 14 02:19:13.184: STP: Data     0000000000801400180C7F6680000000008014001B0C7F66808030000e 3, encsize 22
*Mar 14 02:00140002000F00
*Mar 14 02:19:13.184: STP: VLAN0020 Gi1/0/23:0000 00 00 00 8014001B0C7F6680 00000000 8014001B0C7F6680 8030 0000 1400 0200 0F00
*Mar 14 02:19:13.192: STP(20) port Gi1/0/23 supersedes 0
*Mar 14 02:19:13.192: STP SW: TX: opt sstp: 0100.0ccc.cccd<-aca0.16b6.7601 type/len 0032
*Mar 14 02:19:13.192:     encap SNAP linktype sstp vlan 20 len 64 on v20 Gi1/0/1
*Mar 14 02:19:13.192:     AA AA 03 00000C 010B SSTP
*Mar 14 02:19:13.192:     CFG P:0000 V:00 T:00 F:00 R:8014 001b.0c7f.6680 00000004
*Mar 14 02:19:13.192:     B:8014 aca0.16b6.7600 80.01 A:0100 M:1400 H:0200 F:0F00
```

I flipped a port on accounting switch connecting core to get messages that would change the topology. Here we see messages for STP. The messages being sent are BPDU frames for the different states in STP.

- Use “show spanning tree” command on each switch and locate any ports that are blocked by STP to prevent loops. Review the packet flow diagrams you created in the last objective and confirm exactly which ports/interfaces are being used by data flows.
- Identify and document the priority, root bridge, designated, root, forwarding and blocked ports on the three switches, for each respective VLAN.

  Include screenshots of the show commands used to document this

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     001b.0c7f.6680
              Cost        4
              Port        23 (GigabitEthernet1/0/23)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     aca0.16b6.7600
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/23            Root FWD 4         128.23   P2p
Gi1/0/24            Altn BLK 4         128.24   P2p
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     001b.0c7f.6680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.0c7f.6680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/48            Desg FWD 4         128.48   P2p
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     001b.0c7f.6680
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001d.a1b3.7e00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/48            Desg FWD 4         128.48   P2p
```

- Change the cost of the path in such way that traffic from Accounting-A follows the following path to reach the Fileserver. Change VLAN configs on the switches whenever needed.

  Accounting-A □ Accounting-Switch □ Engineering-Switch □ Core Switch □ Gateway1020 □ Fileserver

- Change the cost of the path in such way that traffic from Engineering-A follows the following path to reach the Fileserver. Change VLAN configs on the switches whenever needed.

  Engineering-A □ Engineering-Switch □ Accounting-Switch □ Core-Switch □Gateway1020 □ Fileserver

- Use appropriate commands to replace the root bridge for another of your preference, make sure each VLAN has a different root switch.
- Shut down one of the ports that connects your Root Bridge to another Switch on a particular VLAN (in forwarding state), document how the backup port transitions from Blocking to Forwarding.

  It went from a blocking state, to listening, to learning, then went to forwarding state.

- How long does it take STP to re-converge (Report)?

  It took about a minute.

- Stop the DEBUG once done. (NOTE if using a virtual lab tool, this might not show intermediate steps)

8. **RSTP**:

STP has disadvantage that it has low convergence which is important at layer 2 LAN. IEEE with document 802.1W introduced an evolution of spanning tree protocol: Rapid Spanning Tree Protocol (RSTP), which reduces the convergence time after a topology change occurs in the network. STP takes 30 to 50 seconds from transit from blocking state to forwarding state. RSTP usually responds less than 10 seconds of a physical link failure.

- Enable Rapid Spanning Tree Protocol (RSTP) for faster convergence.
  spanning-tree mode rapid-pvst

- Shut down one of the ports that connects your Root Bridge to another Switch, report how long does it take RSTP to re-converge (Report) Stop the debug commands

  It took about 10 seconds.

  Turn on debugging for spanning-tree and report the show command results and the differences.

```
*Mar  5 00:13:16.232:     encap SNAP linktype sstp vlan 30 len 64 on v30 Gi1/0/48
*Mar  5 00:13:16.232:     AA AA 03 00000C 010B SSTP
*Mar  5 00:13:16.232: STP SW: PROC RX: 0100.0ccc.cccd<-aca0.16b6.7617 type/len 0032
*Mar  5 00:13:16.232:     encap SNAP linktype sstp vlan 30 len 64 on v30 Gi1/0/48
*Mar  5 00:13:16.232:     AA AA 03 00000C 010B SSTP
*Mar  5 00:13:16.232:     CFG P:0000 V:02 T:02 F:3C R:801E aca0.16b6.7600 00000000
*Mar  5 00:13:16.232:     B:801E aca0.16b6.7600 80.17 A:0000 M:1400 H:0200 F:rface Gi1/0/48 vlan 30: vlan 30 does not exist
*Mar  5 00:13:17.164: STP SW: RX ISR: 0100.0ccc.cccd<-001d.a1b3.7e01 type/len 00320F00
*Mar
* Mar  5 00:513:17.172:      B:8010E 001d.a1b03.7e00 80.:01 A:0000 1M:1400 H:03200 F:0F00:
3Mar  5 100:13:17.1672:      T.:0000 L:00202 D:001E
 *Mar  5 020:13:17.17:2: STP SW:  DROP BPDU : received  sstp(118)  BPDU on i nterface G i1/0/1 vlaTn 30: vlan: 30 does n0ot exist
0*Mar  5 000:13:17.1890: STP SW:  TX: 0100.0Lccc.cccd<-:001b.0c7f.06681 type/0len 0032
0*Mar  5 002:13:17.189 :     encaDp SNAP lin:ktype sstp0 vlan 10 l0en 64 on v110 Gi1/0/1E
00:13:17.1
         89:     AA* AA 03 000M00C 010B SaSTP
*Mar r 5 00:13:1 7.189:      CFG P:00050 V:02 T:0 2 F:3C R:1000A aca0.106b6.7600 0:0000032
*1Mar  5 00:313:17.189::     B:8001A 001b.0c76f.6680 80..01 A:0100 2M:1400 H:03200 F:0F002
*Mar  5 :00:13:17.1 97:      TS:0000 L:00T02 D:000AP SW: DROP BPDU: received sstp(118) BPDU on inte
*Mar  5 00:13:18.279: STP SW: PROC RX: 0100.0ccc.cccd<-aca0.16b6.7617 type/len 0032
*Mar  5 00:13:18.279:     encap SNAP linktype sstp vlan 30 len 64 on v30 Gi1/0/48
*Mar  5 00:13:1ved sstp(118) BPDU on interface Gi1/0/48 vlan 30: vlan 30 does not exist
*Mar  5 00:13:18.556: STP SW: TX: sstp copy: 0100.0ccc.cccd<-001b.0c7f.6681 type/len 00328.279:     AA AA 03 00000C 010B SSTP
*Mar  5 00:13:18.279:     CFG P:0000 V:02 T:02 F:3C R:801E aca0.16b6.7600 00000000
*Mar  5 00:13:18.279:     B:801E aca0.16b6.7600 80.17 A:0000 M:1400 H:0200 F:0F00
*Mar  5 00:13:18.279:      T:0000 L:0002 D:001E
*Mar  5 00:13:18.279: STP SW: DROP BPDU: recei
*Mar  5 00:13:18.564:     CFG P:0000 V:02 T:02 F:3C R:801E 001d.a1b3.7e00 00000000
*Mar  5 00:13:18.564:     B:801E 001d.a1b3.7e00 80.01 A:0000 M:1400 H:0200 F:0F00
*Mar  5 00:13:18.564:      T:0000 L:0002 D:001E
*Mar  5 00:13:18.564: STP SW: DROP BPDU: received sstp(118) BPDU on interface Gi1/0/1 vlan 30: vlan 30 does not exist
*Mar  5 00:13:19.798: STP SW: TX: 0100.0ccc.cccd<-001b.0c7f.6681 type/len 0032
*Mar  5 00:13:19.798:     encap SNAP linktype sstp vlan 10 len 64 on v10 Gi1/0/1
*Mar  5 00:13:19.798:     AA AA 03 00000C 010B SSTP
*Mar  5 00:13:19.798:     CFG P:0000 V:02 T:02 F:3C R:100A aca0.16b6.7600 00000032
*Mar  5 00:13:20.536: STP SW: RX ISR: 0100.0ccc.cccd<-001d.a1b3.7e01 type/len 0032
*Mar  5 00:13:20.536:     encap SNAP linktype sstp vlan 30 len 64 on v30 Gi1/0/1
*Mar  5 00:13:20.536:     AA AA 03 00000C 010B SSTP
*Mar  5 00:13:20.536:     CFG P:0000 V:02 T:02 F:3C R:801E 001d.a1b3.7e00 00000000
*Mar  5 00:13:20.536:     B:801E 001d.a1b3.7e00 80.01 A:0000 M:1400 H:0200 F:0F00
*Mar  5 00:13:20.536:      T:0000 L:0002 D:001E
*Mar  5 00:13:20.544: STP SW: PROC/len 0032
*Mar  5 00:13:20.544:     encap SNAP linktype sstp vlan 30 len 64 on v30 Gi1/0/1
*Mar  5 00:13:20.544:     AA AA 03 00000C 010B SSTP RX: 0100.0ccc.cccd<-001d.a1b3.7e01 type
*Mar  5 00:13:20.544:     CFG P:0000 V:02 T:02 F:3C R:801E 001d.a1b3.7e00 00000000
*Mar  5 00:13:20.544:     B:801E 001d.a1b3.7e00 80.01 A:0000 M:1400 H:0200 F:0F00
*Mar  5 00:r  5 00:13:21.517:     AA AA 03 00000C 010B SSTP
```

```
*Mar  5 00:11:37.784: STP: VLAN0010 Gi1/0/1:0000 02 02 3C 100AACA016B67600 0000000A 800A001DA1B37E00 8001 0100 1400 0200 0F00
*Mar  5 00:11:37.784: RSTP(10): Gi1/0/1 repeated msg
*Mar  5 00:11:37.784: RSTP(10): Gi1/0/1 rcvd info remaining 6
*Mar  5 00:11:39.084: STP: VLAN0010 rx BPDU: config protocol = rstp, packet from GigabitEthernet1/0/48  , linktype SSTP , enctype 3, encsize 22
*Mar  5 00:11:39.084: STP: enc 01 00 0C CC CC CD AC A0 16 B6 76 17 00 32 AA AA 03 00 00 0C 01 0B
*Mar  5 00:11:39.084: STP: Data     000002023C100AACA016B67600000000000100AACA016B67600B017000014000200F00
*Mar  5 00:11:39.084: STP: VLAN0010 Gi1/0/48:0000 02 02 3C 100AACA016B67600 00000000 100AACA016B67600 8017 0000 1400 0200 0F00
*Mar  5 00:11:39.084: RSTP(10): Gi1/0/48 repeated msg
*Mar  5 00:11:39.084: RSTP(10): Gi1/0/48 rcvd info remaining 6
*Mar  5 00:11:39.571: RSTP(1): sending BPDU out Gi1/0/1
*Mar  5 00:11:39.571: RSTP(1): sending BPDU out Gi1/0/48
*Mar  5 00:11:39.571: RSTP(20): sending BPDU out Gi1/0/1
*Mar  5 00:11:39.571: RSTP(20): sending BPDU out Gi1/0/48
*Mar  5 00:11:39.814: STP: VLAN0010 rx BPDU: config protocol = rstp, packet from GigabitEthernet1/0/1  , linktype SSTP , enctype 3, encsize 22
*Mar  5 00:11:39.814: STP: enc 01 00 0C CC CC CD 00 1D A1 B3 7E 01 00 32 AA AA 03 00 00 0C 01 0B
*Mar  5 00:11:39.814: STP: Data     000002023C100AACA016B67600000000A800A001DA1B37E00B0010100140002000F00
*Mar  5 00:11:39.814: STP: VLAN0010 Gi1/0/1:0000 02 02 3C 100AACA016B67600 0000000A 800A001DA1B37E00 8001 0100 1400 0200 0F00
```

The messages are a bit different, here we are reporting what VLANs exist and also what BPDUs were sent and where.

References: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062146.html

Report the commands you used for configuring and manipulating spanning-tree.

OUTCOME: Learn how STP works by default, how to manipulate root role and path selection. Understand STP auto- convergence.

9. **Enhancing Network Efficiency with EtherChannel by overriding STP blockage between devices:**

- You are facing congestion problems on your uplinks to the core switch, configure EtherChannel on the uplinks between the two Switches and the core switch to increase network capacity and redundancy. Configure E1 with PAGP and E2 with LACP.
- Verify that STP treats the EtherChannel as a single logical link. Once you implement Etherchannel correctly you should not see a blocking port between Core switch and its neighbors

```
Core#show eth sum
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Gi1/0/21(P) Gi1/0/23(P)
2      Po2(SU)         LACP      Gi1/0/22(P) Gi1/0/24(P)

Core#
```

- Assure that data flow for engineering and accounting over the switches still follows the paths defined before. Adjust as necessary to restore it (if needed)

9.1 STP Stability with Etherchannel

- Test the network by disconnecting one of the EtherChannel member links and observing whether STP reconverges or not.
- Explain the difference between STP cost, port speed and bandwidth on an ethernet switch. Which of these features was useful to you for this objective? Where are the other ones used?
  STP cost is the actual cost for the SPF path algorithm in STP. Port speed is the actual speed it can transmit. Bandwidth is the total throughput of a certain link, which can consist of multiple links as well. The STP cost feature, and the bandwidth feature were the most useful. As the STP cost showed what the best cost was, and the bandwidth showed the total throughput of the etherchannels created.
- OUTCOME: Etherchannel (EC) configuration via 2 different protocols, and the effects of EC over STP.

  Report the results

10. **PortFast**

What are the advantages of portfast?

- Allows to skip listening and learning states of STP
- Reduce delay in DHCP
- Reduced convergence

Enable portfast on one of the ports on which one of the clients is connected

Verify the change in response time. Give a snapshot of the debug command used and explain what you see in it.

```
%Portfast has been configured on GigabitEthernet1/0/3 but will only
 have effect when the interface is in a non-trunking mode.
Engineering(config-if)#
*Mar  5 01:02:54.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down
*Mar  5 01:02:55.908: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down
*Mar  5 01:02:56.503: RSTP(10): initializing port Gi1/0/3
*Mar  5 01:02:56.503: RSTP(10): Gi1/0/3 is now designated
*Mar  5 01:02:58.500: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to up
*Mar  5 01:02:59.507: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up
```

debug spanning-tree events – I see the protocol is designated the computer instantly without listening, learning.

** This part might not be doable on the virtual lab. Just report the commands you used for configuring portfast**

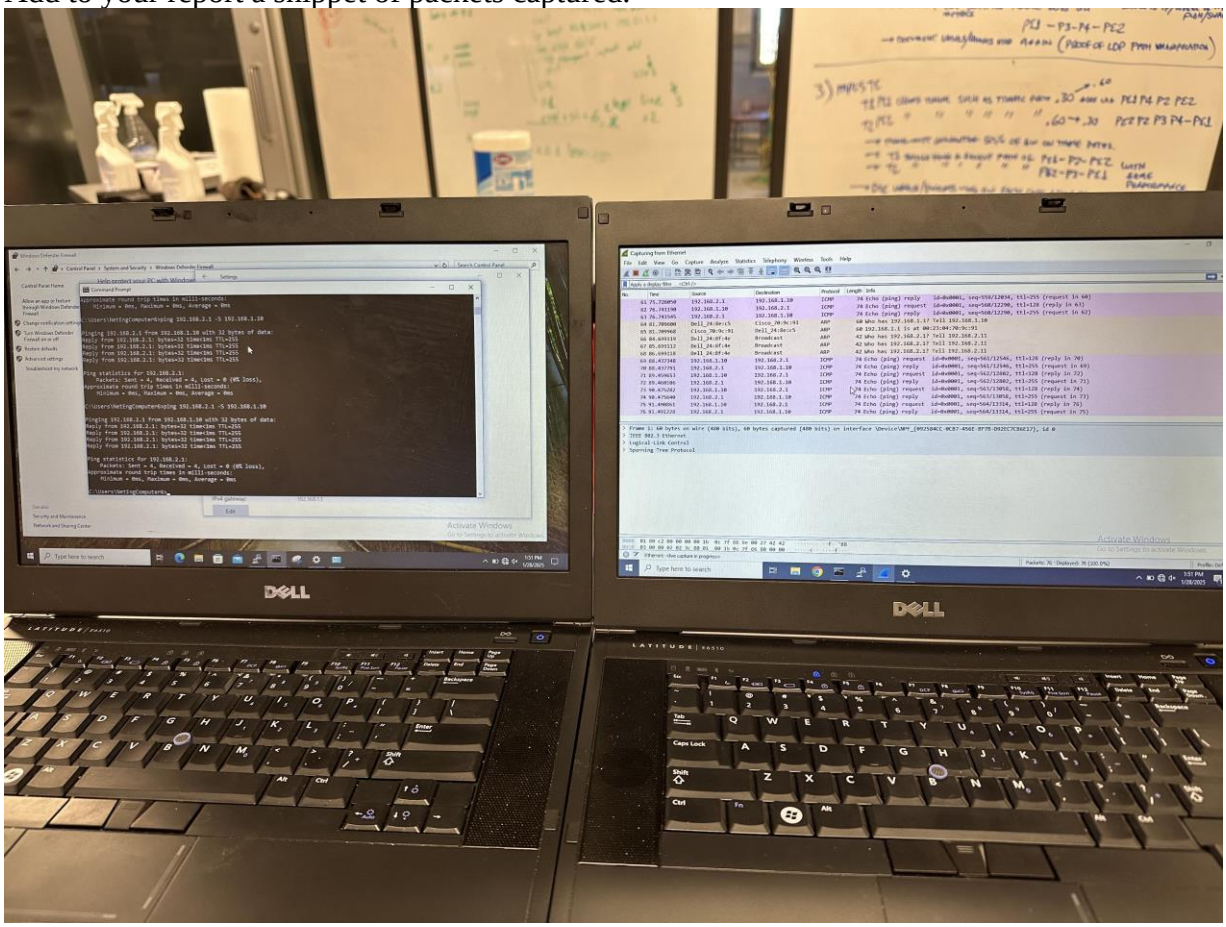
11. **Configuring SPAN for Packet Sniffing:**

- Configure SPAN on Engineering switch, so it can capture the traffic exchanged between all users and send it to the Sniffer System.

- What does SPAN do? Why is this capability provided?

  Switched Port Analyzer allows for packets to be sent to a sniffer port. It allows Network Admins to monitor network traffic for security and efficiency purposes.
- Set up a SPAN session on one of the switches to mirror traffic from a department's VLAN.
- Use Wireshark or TCPDump to capture and analyze packets. .

- Add to your report a snippet of packets captured.



Report Questions (answer after the questions):

1) How would you secure a switch to prevent others from accessing the network? (Hint: think layers)
I would install port security on ports to either be a sticky port to adapt to the MAC address or have a host of MACs that are allowed to connect to the

2) What is the length of the MAC address? How is it divided?

48 bits, its divided by the first 24 bits being the manufactureer and the second half being the unique device identifier

3) Are sticky ports secure? Why or why not? Is it recommended?

I would say they are secure because they are saved in the MAC-table even after a reboot. Or if you know someone's mac, you can just spoof it and then instantly have access to the switch. So there are tradeoffs.

4) Why are switches faster than routers?

Switches are faster than routers because switches do not have routing protocols that create much more overhead than just forwarding frames in a MAC table.

5) How many MAC addresses does your computer have? How do you find out?

You can do ip addr (Linux) or ipconfig (Windows) and it depends on how many NICs you have.

6) What problem is portfast meant to solve in a network?

Portfast solves the downtime that STP creates by bypassing the timers.

7) Can you change your MAC address? If so, how?

Deep in a Windows menu. And you can change your MAC.

9) Name/explain other applications of SPAN (Why do we need port replication/monitoring services for?)

We can analyze the traffic for security reasons, troubleshoot network problems, and potentially do capacity planning.

10) What are the advantages of using VLANs?

We can separate the network into segments.

11) Tell me any disadvantages of using VLANs\
Increased network complexity , risk of broadcast storms, cybsecurity risks.

12) Can you do trunking with a PC? Is this a popular practice?
You can if the NIC allows this, it is not a popular practice.

13) Can you telnet into a switch? Can any PC on any VLAN telnet into a switch (assume all PCs are connected to the same switch)?

If they are in the same network as the SVI, they can telnet into the device.

14) Why do we need a Native VLAN for?

To manage untagged traffic, being that all traffic must be tagged with a VLAN, so there is a default one.

15) Give any important details regarding native VLANs in 802.1Q trunking.

The native VLAN is configured exactly the same on both sides of the trunk to avoid network issues and security vulnerabilities.

16) Find and explain other trunking services used in industry.

LACP, EtherChannel, ISL

17) What is a multilayer switch?

A multilayer switch is a device that can route out its switchports.

18) Explain how is RSTP better than STP?

Faster forwarding state time/convergence. Fasters transitions for when calculating and getting STP to a forwarding state. It skips blocking and listening by putting them into one.

19) What is the advantage of having Per VLAN STP? Explain VTP VLAN pruning.

The advantage of having PVST is the ability to not have broadcast storms each time STP recalculates on all areas of traffic. VTP pruning is blocking certain VLANs on switches.