LAB – 2

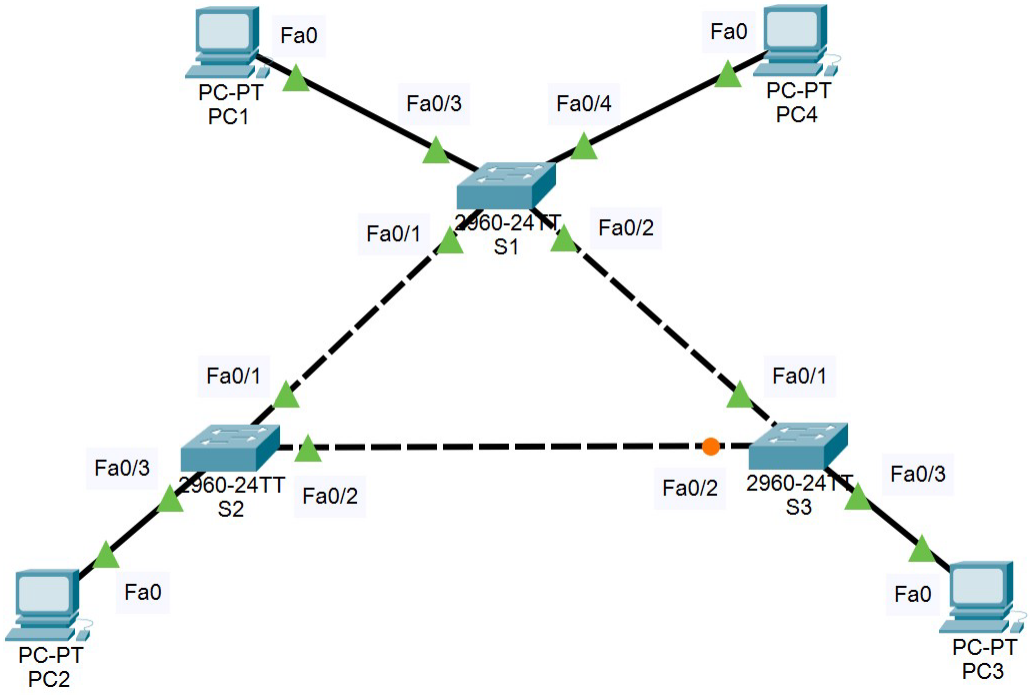
STP Network Examination

Learning Objectives

Upon completion of this lab, you will be able to:

- Configure a network according to the topology diagram.
- Configure switches with certain switch parameters to improve security.
- Configure switches with certain network interfaces to control connectivity.
- Configure PCs with default gateway, IP address, and subnet mask.
- Examine the default configuration of Spanning Tree Protocol (STP, 802.1D).
- Understand the mechanism of Spanning Tree Protocol and Bridge Protocol Data Units(BPDUs).
- Observe and analyze network message transmission with Spanning Tree Protocol.
- Observe and analyze network message transmission without Spanning Tree Protocol.
- Observe and analyze Spanning Tree Protocol response to network topology modification.

Topology Diagram



Address Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 1**	**192.168.10.1**	**255.255.255.0**	**N/A**
S2	**VLAN 1**	**192.168.10.2**	**255.255.255.0**	**N/A**
S3	**VLAN 1**	**192.168.10.3**	**255.255.255.0**	**N/A**
PC1	**NIC**	**192.168.10.11**	**255.255.255.0**	**192.168.10.254**
PC2	**NIC**	**192.168.10.12**	**255.255.255.0**	**192.168.10.254**
PC3	**NIC**	**192.168.10.13**	**255.255.255.0**	**192.168.10.254**
PC4	**NIC**	**192.168.10.14**	**255.255.255.0**	**192.168.10.254**

Task 1: Network Topology Configuration (Perform below steps and provide corresponding screenshot)

1. Connect 3 switches to form network based on the topology diagram.
    a. For switch type: Network devices -> Switches -> 2960
    b. For switch order:
        i. Switch0 at top middle, rename it into S1.
        ii. Switch1 at bottom left, rename it into S2.
        iii. Switch2 at bottom right, rename it into S3.
    c. For connections: Connections -> Connections -> Copper Cross-Over
    d. For connected ports:
        i. S1_Fa(FastEthernet)0/1 – S2_Fa0/1
        ii. S1_Fa0/2 – S3_Fa0/1
        iii. S2_Fa0/2 – S3_Fa0/2
2. Connect 3 PCs to form network based on the topology diagram.
    a. For PC type: End Devices -> End Devices -> PC
    b. For PC order:
        i. PC0 at top left, rename it into PC1.
        ii. PC1 at bottom left, rename it into PC2.
        iii. PC2 at bottom right, rename it into PC3.
        iv. PC3 at top right, rename it into PC4.
    c. For connections: Connections -> Connections -> Copper Straight-Through
    d. For connected ports:
        i. PC1_Fa0 – S1_Fa0/3
        ii. PC2_Fa0 – S2_Fa0/3
        iii. PC3_Fa0 – S2_Fa0/3
        iv. PC4_Fa0 – S1_Fa0/4
3. After a **STEP-BY-STEP guideline 1.1.a — 1.2.d,** you should have the **identical** network topology configuration to the topology diagram.
    a. Look for the **Fast Forward Time** functionality on the bottom left menu bar ->

b. Single click **Fast Forward Time** to accelerate the network auto configuration process.
c. Single click **any blank space on the screen** to stop the acceleration process.
d. Now all connections should not be block and show green triangles on both way **EXCEPT the port Fa0/2 of S3 is blocked and show orange circle**.
e. Make sure you have the identical network topology before moving on to the next task.

Task 2: Basic Switch Configurations (Perform below steps and provide corresponding screenshot)

1. Configure S1 with certain switch parameters following the guidelines:
    a. Ensure S1 have only default VLANs exist and that all ports are assigned to VLAN 1.
        i. Enter Switch1 CLI, type **enable** to enter EXEC mode, and type **show vlan** to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.
    b. Configure S1's hostname from 'Switch' to 'S1.'
        i. In EXEC mode, type **configure terminal** to enter global configuration mode, type **hostname S1** to rename it into S1.
    c. Configure a secret password 'cmpe206' for EXEC mode.
        i. In global configuration mode, type **enable secret cmpe206** to configure EXEC mode secret password.
    d. Disable DNS lookup.
        i. In global configuration mode, type **no ip domain-lookup** to disable DNS lookup.
    e. Configure a password 'cmpe206' for console connections.
        i. In global configuration mode, type **line console 0** to enter console line configuration mode, type **password cmpe206** to configure console connection password, and type **login** to enable password checking when logging into console line configuration mode.
    f. Configure a password 'cmpe206' for vty connections.
        i. In console line configuration mode, use **line vty 0 15** to enter vty line configuration mode, type **password cmpe206** to configure vty connection password, and type **login** to enable password checking when logging into vty connection configuration mode, type **end** to return to EXEC mode.
    g. Save the contents of the running configuration file to non-volatile RAM (NVRAM).
        i. In EXEC mode, type **copy running-config startup-config** to Save the contents of the running configuration file to non-volatile RAM.
        ii. Note: you can type **show startup-config** to check the content of current saved running configuration.
2. Configure S2 with the similar switch parameters following the **guidelines 2.1.a – 2.1.g** similarly.
    a. Note: Its hostname should be 'S2'
3. Configure S3 with the similar switch parameters following the **guidelines 2.1.a – 2.1.g** similarly.
    a. Note: Its hostname should be 'S3'

Task 3: Basic Network Interfaces Configurations (Perform below steps and provide corresponding screenshot)

1. Configure S1 with certain network interfaces following the guidelines:
    a. Disable all ports on S1.

i. Enter S1 CLI, press random key to request enter USER mode, type **cmpe206** as password to complete USER mode access verification, type **enable** to request enter EXEC mode, type **cmpe206** as password to complete EXEC mode access verification.
ii. In EXEC mode, type **configure terminal** to enter global configuration mode, type **interface range fa0/1-24** to enter fast ethernet configuration mode for ports fa0/1-24, type **shutdown** to shut down all its ports, type **interface range gi0/1-2** to enter gigabit ethernet configuration mode for ports 1-2, type **shutdown** to shut down all its ports.

b. Re-enable the user port (fa/03) on S1.
i. In S1 global configuration mode, type **interface range fa0/3, fa0/4** to enter fast ethernet configuration mode for port fa0/3, and type **switchport mode access** to set the trunking mode to 'access' to form user port, and type **no shutdown** to enable the specified port.

c. Re-enable the trunk ports (fa0/1, fa0/2) on S1.
i. In S1 global configuration mode, type **interface range fa0/1, fa0/2** to enter fast ethernet configuration mode for port fa0/1, fa0/2, and type **switchport mode trunk** to set the trunking mode to 'trunk' to form trunk port, and type **no shutdown** to enable the specified port.
ii. Note: Only a single VLAN 1 is being used in this lab, however trunking has been enabled on all links between switches to allow for additional VLANs to be added in the future.

d. Configure the management interface address on S1 based on the given **addressing table**.
i. In S1 global configuration mode, type **interface vlan1** to VLAN configuration mode, fa0/2, and type **ip address 192.168.10.1 255.255.255.0** to set its IP address and subnet mask, and type **no shutdown** to enable vlan1.

2. Configure S2 with the similar network interfaces following on the given **addressing table** following **guidelines 3.1.a – 3.1.d** similarly.
3. Configure S3 with the similar network interfaces following on the given **addressing table** following **guidelines 3.1.a – 3.1.d** similarly.
4. Verify that the S1, S2, S3 are correctly configured.
   a. In each switch's CLI, get into EXEC mode, and type **show interface status** to confirm the connected ports are correctly configured.

i.	Switch	connected trunk ports	connected user ports
ii.	S1	fa0/1, fa0/2	fa0/3, fa0/4
iii.	S2	fa0/1, fa0/2,	fa0/3
iv.	S3	fa0/1, fa0/2	fa0/3

   v. All other ports status should be **disabled**.
   b. In each switch's CLI, get into EXEC mode, and type **show interface Vlan 1** to confirm the IP address and subnet mask are correctly configured.
   c. Note: Confirm all switches correctly configured before moving on to the next task.

Task 4: Host PCs Configurations (Perform below steps and provide corresponding screenshot)

1. Configure the Ethernet interfaces of PC1 based on the given **addressing table**.
   a. Single click on PC1 -> Config -> Global -> Settings -> Gateway/DNS IPV4

b. On section **Default Gateway**, type **192.168.10.254**
c. Single click on PC1 -> Config -> Interface -> FastEthernet0 ->IP Configuration
d. On section **IPV4 Address**, type **192.168.10.11**
e. On section **Subnet Mask**, type **255.255.255.0**

2. Configure the Ethernet interfaces of PC2 based on the given **addressing table** following **guidelines 4.1.a -4.1.e** similarly.
3. Configure the Ethernet interfaces of PC3 based on the given **addressing table** following **guidelines 4.1.a -4.1.e** similarly.
4. Configure the Ethernet interfaces of PC4 based on the given **addressing table** following **guidelines 4.1.a -4.1.e** similarly.

Task 5: Understand the mechanism of Spanning Tree Protocol and Bridge Protocol Data Units (BPDUs). (No screenshot needed, read and study the following content)

Our Ethernet allows bridge loops exists to add network path redundancy which increase the reliability of the network(if one link is down, we still have choices of back up links). However, the bridge loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast messages flooding the network. Since the Layer 2 header does not support a time to live (TTL) value, if a frame is sent into a looped topology, it can loop forever, which eventually cause network resource (bandwidth) depletion where no network message can be transmitted.

The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to detect and prevent bridge loops and the broadcast radiation that results from them by performing the following:

a. All switches in the network communicates via BPDUs message to elect a root bridge switch for the network.
b. Each switch ranks its port and decide its most efficient path to the root bridge switch for transmitting data frame, and temporarily block certain ports to realize loop-free network topology.
c. When arbitrary path/port in the current network topology is down(cannot be reach), re-enable the previously blocked network interfaces to reconstruct a connected network topology while maintaining loop-free.

Bridge Protocol Data Units (BPDUs) are frames that contain information about the spanning tree protocol (STP). A switch sends BPDUs using a unique source MAC address from its origin port to a multicast address with destination MAC. Switches communicate with each other to elect a Root Bridge using BPDUs. Base on the received BPDUs from other switches, a typical non-root bridges switch will calculate the best path to the root bridge switch to form its STP information.

The best path is calculated by electing a root port based on the following routine:

1. First check the link speeds and choose the one with the lowest cost:
    a. 10 Gbps Link -> Cost 2
    b. 1 Gbps Link(Gigabit Ethernet Interface) -> Cost 4
    c. 100 Mbps (Fast Ethernet Interface) -> Cost 19
    d. 10 Mbps -> Cost 100

2. If link speed(cost) is equal, choose the one with lowest Bridge Identifier Priority(BIDP):
    a. **BIDP = bridge priority + system ID extension**
    b. In Cisco Packet Tracer:
        i. bridge priority = 32768
        ii. system ID extension = X where X in VLAN X
3. If BIDP is equal, choose the one with lowest Bridge Identifier (BID):
    a. **BID = bridge priority + system ID extension + switch MAC address**
4. If there are multiple links connected to the switch, choose the one with lowest Port identifier (PID) ->
    a. **PID = priority number + interface number**
    b. In Cisco Packet Tracer:
        i. Priority number = 128
        ii. interface number = Y where Y in Fa0/Y or Gi0/Y

The **show spanning-tree** command displays the stored STP information of a switch, it shows bridge switch info for both Root and itself and shows status for all available interfaces.

Task 6: Spanning Tree Protocol Examination(Perform below steps and provide corresponding screenshot)

1. Examine the default configuration of spanning tree protocol on S1.
    a. After access verification and enter in EXEC mode, type **show spanning-tree** to display the spanning-tree protocol info at the current switch.
2. Examine the default configuration of spanning tree protocol on S2 following **guidelines 6.1.a** similarly.
3. Examine the default configuration of spanning tree protocol on S3 following **guidelines 6.1.a** similarly.

Answer the following questions based on the output you examined at Task 6. (No screen shot needed for answering the question, enter your answer in text instead)

4. What do we use to form STP info for each switch in our network? how frequent does it send? How long does it last?
    a. Answer:

5. What is the BIDP for switches S1, S2, and S3 on VLAN 1?
    a. S1 :
    b. S2 :
    c. S3 :

6. What is the BID for switches S1, S2, and S3 on VLAN 1? (use form BID = BIDP + Mac Address)
    a. S1 :
    b. S2 :

c. S3 :

7. Which switch is the root bridge switch for the VLAN 1 spanning tree? Why?
   a. Answer:

8. Which spanning tree ports are in the blocking state on the root switch? Answer 'None' if no such port.
   a. Answer:

9. Which switch and port is in the blocking state? Why?
   a. Answer:

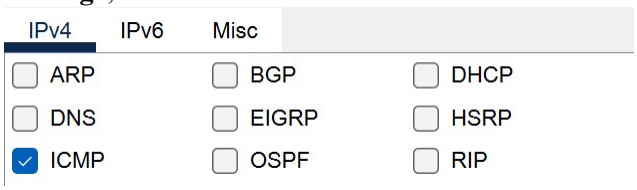
Task 7: Network Message Transmission With Spanning Tree Protocol (Perform below steps and provide corresponding screenshot)

1. Ping using Simple PDU(P) from PC1 to PC2, watch and record the Ping simulation.
   a. To keep our network message simulation clean and easier to focus on the Ping message**, turn off all network protocol messages except for messages in ICMP type**:
      i. Look for **Event List** functionality on the bottom right menu bar ->

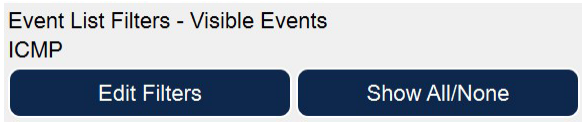
      ii. Single click **Event List** to call out simulation panel, and look for **Show All/None** ->

      iii. Single click **Show All/None** to show none of the network messages ->

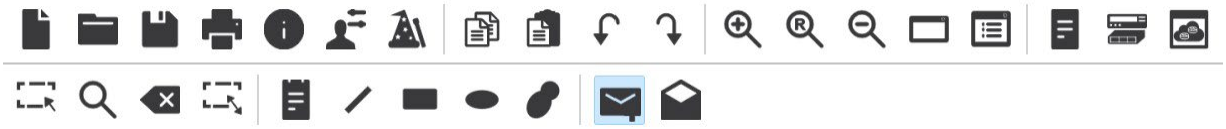
iv. Single click **Edit Filters**, a filter window will pop up. Look for **ICMP type message**, and **select** it ->



v. Close the filter window, now your **Event List** should show **ICMP message only** during the network simulation ->



b. Look for **Simple PDU(P)** functionality on the top menu bar ->

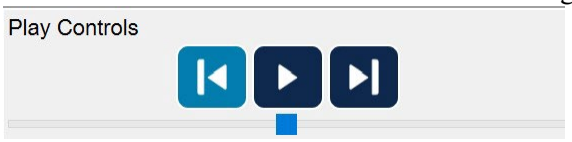


c. Single click it to enable **PDU(P) mode** for your cursor, click on PC1 first as source device, then click on PC2 as destination device.

d. Look for **Simulation** functionality on the bottom right menu bar ->

e. Single click **Simulation** to initialize the message transmission simulation.

f. Use the **forward control bar** to control the Ping message transmission flow ->



g. Keep forwarding the Ping message until the termination.

h. Take a screenshot of the simulation panel **Event List** section where the Ping message forwarding path is recorded.

i. Look for **Realtime** functionality on the bottom right menu bar ->

j. Single click **Realtime** to finish the network simulation mode and return to real time mode.

2. Ping using Simple PDU(P) from PC2 to PC3, watch and record the Ping simulation, following **guidelines 7.1.a – 7.1.j** similarly.

Answer the following questions based on the output you examined at Task 7. (No screen shot needed for answering the question, enter your answer in text instead)

3. When Pinging from PC1 to PC2, what is the complete path for the Ping message?
    a. Answer:

4. Assume each switch's backward learning table was initially empty, after Pinging from PC1 to PC2, what would the backward learning table looks like for each switch(S1, S2, S3)?
    a. Example: S1: PC1(Fa0/3), PC4(Fa0/4)
    b. Answer:
    c. S1:
    d. S2:
    e. S3:

5. When pinging from PC2 to PC3, what is the complete path for the Ping message?
    a. Answer:

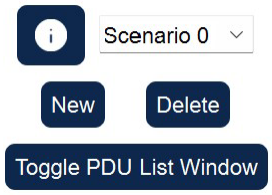
6. Assume we continue from the previous move(Pinged from PC1 to PC2), after Pinging from PC2 to PC3, what would the backward learning table looks like for each switch(S1, S2, S3)?
    a. Example: S1: PC1(Fa0/3), PC4(Fa0/4)
    b. Answer:
    c. S1:
    d. S2:
    e. S3:

7. When pinging from PC2 to PC3, we have a 'shorter path' from S2_fa0/2 to S3_fa0/2, why PDU(P) message did not take that path?
    a. Answer:

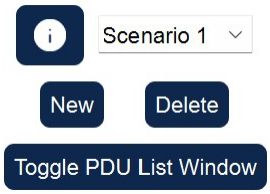
Task 8: Network Message Transmission Without Spanning Tree Protocol (Perform below steps and provide corresponding screenshot)

1. Disable spanning tree protocol for S1 in VLAN 1.
    a. After access verification and enter in EXEC mode, type **configure terminal** to enter global configuration mode, then type **no spanning-tree vlan 1** to disable STP protocol in VLAN 1.
2. Disable spanning tree protocol for S2 in VLAN 1 following **guidelines 8.1.a** similarly.
3. Disable spanning tree protocol for S3 in VLAN 1 following **guidelines 8.1.a** similarly.
4. How does the network topology look like after 7.1 – 7.3? What change have you noticed?
    a. Take a screenshot for the first question and answer the second question in text.
    b. Answer:

5. Create a new network scenario (**This step is CRITICAL, be sure to follow**).
    a. Look for the **Network Scenario Panel** functionality on the bottom middle menu bar ->



    b. Single click on **New** to create a new network scenario ->



6. Ping using Simple PDU(P) from PC3 to PC4, watch and record the Ping simulation, following **guidelines 7.1.a – 7.1.g** similarly.
    a. If you did the previous steps correctly, there is no end on this simulation, stop when your PDU(P) message starts looping few times.
7. Was the Ping successful? What happened to Ping message? Why?
    a. Answer:

8. How to Fix it?
    a. Answer:

9. Delete the current network scenario.
10. Re-enable spanning tree protocol for S1 in VLAN 1.
    a. After access verification and enter in EXEC mode, type **configure terminal** to enter global configuration mode, then type **spanning-tree vlan 1** to enable STP protocol in VLAN 1.
11. Re-enable spanning tree protocol for S2 in VLAN 1 following **guidelines 8.10.a** similarly.
12. Re-enable spanning tree protocol for S3 in VLAN 1 following **guidelines 8.10.a** similarly.

Task 9: Spanning Tree Protocol Response to Topology Modification (Perform below steps and provide corresponding screenshot)

1. Shutdown the port **fa0/1 on S1**.
    a. After access verification and enter in global configuration mode, type **interface fa0/1** to enter fast ethernet configuration mode for port fa0/1, type **shutdown** to shut down port fa0/1.
2. Record the current spanning tree protocol info in S1.
    a. In EXEC mode, type **show spanning-tree** to display the spanning-tree protocol info at the current switch.
3. Record the current spanning tree protocol info in S2 following **guidelines 9.2.a** similarly.
4. Record the current spanning tree protocol info in S3 following **guidelines 9.2.a** similarly.

Answer the following questions based on the output you examined at Task 5. (No screen shot needed for answering the question, enter your answer in text instead)

5. What has changed about the network topology? Why?(which port of which switch is not active anymore? which port of which switch has changed its port state? Why?)
    a. Answer:

6. What has changed about the way that S1 forwards traffic?
    a. Answer:

7. What has changed about the way that S2 forwards traffic?
    a. Answer:

8. What has changed about the way that S3 forwards traffic?
    a. Answer:

9. Does the root bridge switch for the VLAN 1 spanning tree changed? Why?
    a. Answer: