LABORATORY WORK NO. 10
LAYER 2 NETWORKS, SPANNING TREE PROTOCOL, LINK AGGREGATION AND ETHERCHANNEL

1. Objectives

At the end of the lab, students will be able to explain the functions of the switches, the Spanning-tree and EtherChannel operation, and to configure Layer 2 networks.

2. Theoretical considerations

The current practical work focuses on the Data Link layer of the ISO/OSI stack (Figure 11.1).

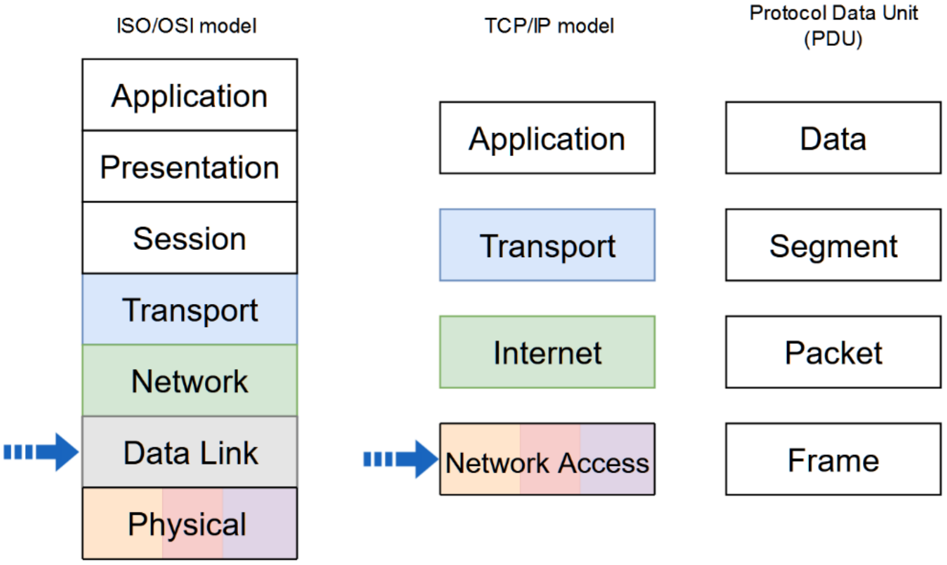
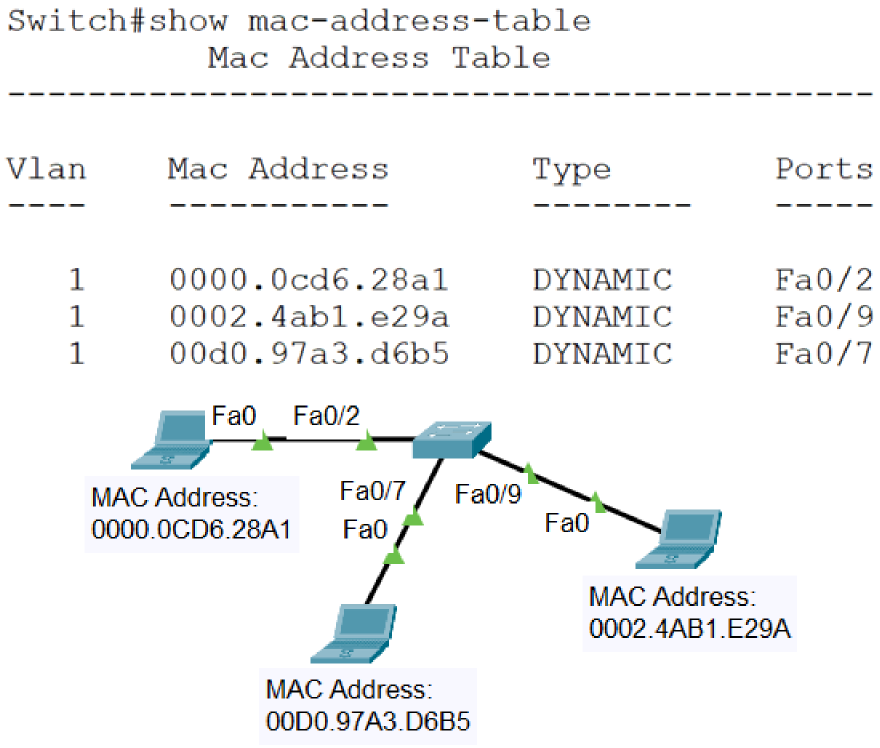


Figure 11.1 *Network stack models and PDU naming in each level. The arrows indicate the addressed layers in the current activity*

2.1 Switches and bridges

Switches and bridges are layer 2 devices that are used to increase available bandwidth and reduce network congestion. Switches and bridges perform two basic operations: switching data frames and maintaining switching operations. Switches and bridges segment the LAN creating multiple smaller collision domains. Each port creates one segment which is a collision domain because the switch or the bridge learns the MAC addresses of devices connected to each port, enters this information into a switching or bridging table and forwards or blocks traffic based on that table (Figure 11.2). Segmentation allows network congestion to be significantly reduced within each segment. The devices within that segment share the total available bandwidth. If the switch or the bridge does not know where to send the frame, it broadcasts the frame out to all ports. When a reply is returned, the switch or the bridge records the new address in the switching or bridging table. Another advantage of the switched connection is that it permits full-duplex Ethernet which allows the transmission of a packet and the reception of a different packet at the same time. The disadvantage of layer 2 devices is that they forward broadcast frames to all connected devices on the network, so all hosts connected to the switch or bridge are still part of the same broadcast domain.



```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0cd6.28a1    DYNAMIC     Fa0/2
   1    0002.4ab1.e29a    DYNAMIC     Fa0/9
   1    00d0.97a3.d6b5    DYNAMIC     Fa0/7
```

Figure 11.2 *Switching table*

Switching is classified as symmetric or asymmetric. Symmetric switching provides switched connections between ports with the same bandwidth. Asymmetric switching provides switched connections between ports of unlike bandwidth. Asymmetric switching enables more bandwidth to be dedicated to the server switch port in order to prevent a bottleneck.

Switching modes are classified as store-and-forward or cut-through, each mode representing a compromise between latency and error detection. In store-and-forward switching mode the entire frame is received before any forwarding takes place. This switching mode increases the transmission latency and allows more error detection. In cut-through switching mode the frame is forwarded through the switch before the entire frame is received. At least the frame destination address must be read before the frame can be forwarded. This switching mode decreases the transmission latency and allows less error detection. Cut-through switching mode has two forms: fast-forward and fragment-free. Fast-forward switching forwards the packet after reading the destination address. This switching mode has the lowest level of latency and error detection. Fragment-free switching forwards the packet after reading the first 64 bytes of the frame. Because collision fragments are smaller than 64 bytes, fragment-free switching mode filters out this type of error which also represents the majority of packet errors. This switching mode has a higher level of latency and error detection than the fast-forward mode.

2.2 Spanning-Tree Protocol

Redundant networking topologies increase the reliability of the network by introducing redundant links. These connections introduce physical loops into the network. Because layer 2 has no mechanism to eliminate lost frames, the frames can loop forever in a layer 2 looped topology causing two types of problems to appear: broadcast storm and switching or bridging table instability. The broadcast storm is created by endlessly flooded broadcast frames too all ports of the switches or bridges, wasting the bandwidth or making the network unusable. Switching or bridging table instability appears when multiple copy of a frame arrive at different ports of a switch or a bridge causing MAC entry instability in the switching or bridging table. The IEEE 802.1d Spanning-Tree Protocol uses the spanning-tree algorithm to create loop free shortest path logical topology in a layer 2 looped topology. The IEEE 802.1w Rapid Spanning-Tree Protocol uses a rapid spanning-tree algorithm to perform the same function as spanning-tree algorithm with a shorter convergence time.

Spanning-Tree Protocol uses Bridge Protocol Data Unit (BPDU) multicast layer 2 messages which are sent by the network devices every two seconds by default. The structure of these messages is presented in Figure 11.3.

Root BID	Root Path Cost	Sender BID	Port ID

Figure 11.3 *BPDU message structure*

The BID is an 8-byte field. The two high order bytes are the bridge or switch priority that defaults to 32768 and the six low order bytes are the MAC address of the bridge or switch. The BID structure is presented in Figure 11.4.

7	6	5	4	3	2	1	0
Bridge Priority		MAC address					

Figure 11.4 *BID structure*

Spanning-Tree Protocol calculates the shortest path network based on cumulative link costs. Link costs are based on the speed of the link. Some of the link costs defined by the IEEE 802.1D standard are presented in Table 11.1.

Table 11.1 *Link costs defined by the IEEE 802.1D standard*

Link Speed	**Cost**
4Mbps	250
10Mbps	100
16Mbps	62
100Mbps	19
1Gbps	4
10Gbps	2

Some of the link costs defined by the IEEE 802.1w standard are presented in Table 11.2.

Table 11.2 *Link costs defined by the IEEE 802.1w standard*

Link Speed	**Cost**
10Mbps	2000000
100Mbps	200000
1Gbps	20000
10Gbps	2000
1Tbps	20
10Tbps	2

The Port ID is a 2-byte field. The high order byte is the port priority that defaults to 128 and the low order byte is the port number. The Port ID structure is presented in Figure 11.5.

1	0
Port Priority	Port Number

Figure 11.5 *Port ID structure*

The Spanning-Tree Protocol establishes a single root node, called root bridge and constructs a topology that has one path for reaching every network node. The resulting tree originates from the root bridge. The bridges and switches calculate the shortest path from itself to the root bridge. The first decision that all bridges or switches in the network make is the root bridge identification, which is done through BPDU messages that are received by all bridges and switches. All other decisions in the network are made regarding this root bridge. When a bridge or switch first starts up, it assumes it is the root and sends BPDU-s containing the bridge or switch MAC address in both the root and sender BID. If a bridge or switch receives a BPDU with a lower root BID it sets this root BID in the BPDU-s that are sent out. The bridge or switch with the smallest BID value will be the root bridge. Setting the bridge or switch priority to a smaller value than the default will make the BID smaller and will influence the root bridge identification. For each LAN segment, Spanning-Tree Protocol establishes a designated switch as the closest one to the root bridge which handles all communication from that LAN towards the root bridge. For each non-root bridge a root port is elected, which gives the best path to the root bridge. So, the port with the lowest path cost to the root bridge is elected as the root port. If multiple ports have the same path cost to the root bridge, the port with lowest Port ID is selected as the root port. The Spanning-Tree Protocol also selects the designated ports which are part of the shortest path tree. So, the port with the lowest path cost to the root bridge is selected as the designated port. If more than one port in the segment has the same path cost, the port on which the bridge or the switch has the lowest bridge or switch ID is selected as designated port. On the root bridge, all its ports are designated ports. Redundant links that are not part of the shortest path tree are blocked and data frames received on blocked links are dropped.

Each port on a bridge or switch that is using the Spanning-Tree Protocol has one of the following five states: blocking, listening, learning, forwarding and disabled. In the blocking state ports can only receive BPDU-s, data frames are discarded and no addresses can be learned. It may take up to 20 seconds to change from this state. Ports go from the blocking state to the listening state. In this state, the switches or bridges determine if there are any other paths to the root bridge. The path that is not the least cost path to the root bridge goes back to the blocked state. In the listening state BPDU-s are processed, user data is not being forwarded and MAC addresses are not being learned. The listening period is called the forward delay and lasts for 15 seconds. Ports go from the listening to the learning state. In this state BPDU-s are processed, user data is not being forwarded, but MAC addresses are learned from any traffic that is seen. The learning state is also called the forward delay and lasts for 15 seconds. A port goes from the learning state to the forwarding state. In this state BPDU-s are processed, user data is forwarded and MAC addresses continue to be learned. The port can be in disabled state when it is administratively down or fails. The time values given for each state are the default values. These values have been calculated on an assumption that there will be a maximum of seven switches in any branch of the spanning tree from the root bridge. When the network topology changes, switches and bridges recompute the Spanning Tree. Convergence on a new spanning-tree topology using the IEEE 802.1D standard can take up to 50 seconds.

2.3 EtherChannel

Link aggregation is the ability to create one logical link using multiple physical links between two devices. EtherChannel is a form of link aggregation used in switched networks (Figure 11.6). This allows for redundancy and higher bandwidth through load sharing among the physical links. EtherChannel creates a one-to-one relationship; that is, one EtherChannel link connects only two devices. An EtherChannel link can be created between two switches or an EtherChannel link can be created between an EtherChannel-enabled server and a switch.

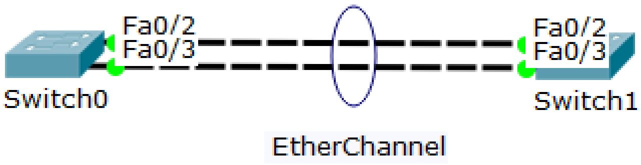


Figure 11.6 *EtherChannel*

EtherChannel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several physical ports into one logical channel. When an EtherChannel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface (Figure 11.7). Most configuration tasks can be done on the EtherChannel interface instead of on each individual port, ensuring configuration consistency throughout the links.

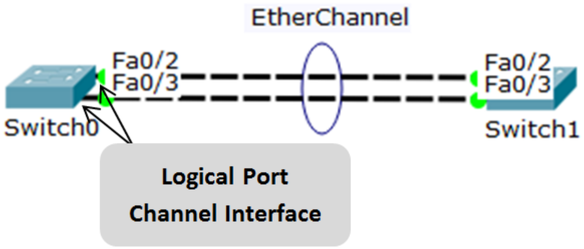


Figure 11.7 *Port channel interface*

EtherChannel relies on existing switch ports. There is no need to upgrade the link to a faster and more expensive connection to have more bandwidth.

Load balancing takes place between links that are part of the same EtherChannel. Depending on the hardware platform, one or more load-balancing methods can be implemented. These methods include source MAC to destination MAC load balancing, or source IP to destination IP load balancing, across the physical links.

EtherChannel creates an aggregation that is seen as one logical link. Where there is only one EtherChannel link, all physical links in the EtherChannel are active because STP sees only one logical link.

EtherChannel provides redundancy because the overall link is seen as one logical connection. Additionally, the loss of one physical link within the channel does not create a change in the topology; therefore a spanning-tree recalculation is not required. Assuming at least one physical link is present, the EtherChannel remains functional, even if its overall throughput decreases because of a lost link within the EtherChannel. The spanning-tree cost is calculated based on the number of ports assigned to the port-channel and it does not dynamically change when links go down or are brought back up within the port-channel. Spanning-Tree Protocol calculates the shortest path network based on cumulative link costs. Link costs are based on the speed of the link. Some of the link costs for links defined by the IEEE 802.1D standard are presented in Table 11.3.

Table 11.3 *Link costs defined by the IEEE 802.1D standard*

Link Speed	Cost (Short mode – 16bit)
10Mbps	100
100Mbps	19
Two-port * 100Mbps EtherChannel	9
Three-port * 100Mbps EtherChannel	8
Four-port * 100Mbps EtherChannel	7
Five-port * 100Mbps EtherChannel	6
Six-port * 100Mbps EtherChannel	5
Seven-port * 100Mbps EtherChannel	5
Eight-port * 100Mbps EtherChannel	5
1Gbps	4
Two-port * 1Gbps EtherChannel	3
Three-port * 1Gbps EtherChannel	2
Four-port * 1Gbps EtherChannel	2
Five-port * 1Gbps EtherChannel	2
Six-port * 1Gbps EtherChannel	2
Seven-port * 1Gbps EtherChannel	2
Eight-port * 1Gbps EtherChannel	1
10Gbps	2
Two-port * 10Gbps EtherChannel	1

Interface types cannot be mixed; they must be compatible-configured Ethernet ports. The individual EtherChannel group member port configuration must be consistent on both devices. If the physical ports of one side are configured as trunks, the physical ports of the other side must also be configured as trunks within the same native VLAN. Additionally, all ports in each EtherChannel link must be configured as Layer 2 ports. Each EtherChannel has a logical port channel interface. A configuration applied to the port channel interface affects all physical interfaces that are assigned to that interface. Layer 3 EtherChannels can be configured on Cisco Catalyst multilayer switches. A Layer 3 EtherChannel has a single IP address associated with the logical aggregation of switch ports in the EtherChannel.

The maximum number of physical ports in an EtherChannel link depends on the switch hardware platform and IOS version. Usually each EtherChannel can consist of up to 8 compatible-configured Ethernet ports.

The maximum number of EtherChannels supported by a switch depends on the hardware platform and IOS version. The Cisco IOS switch can usually support 6 EtherChannels.

EtherChannel can be configured static, unconditional or it can be formed through negotiation using one of two protocols: Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). These protocols allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches.

PAgP is a Cisco-proprietary protocol that aids in the automatic creation and management of EtherChannel links. There are three modes for PAgP: on, desirable and auto. The on mode forces the interface to channel without PAgP. The desirable mode places an interface in an active negotiating state in which the interface initiates negotiations with other interfaces by sending PAgP packets. The auto mode places an interface in a passive negotiating state in which the interface responds to the PAgP packets that it receives, but does not initiate PAgP negotiation. Figure 11.8 presents the channel establishment when ports of switches S1 and S2 are in the different modes for PAgP.

S1	S2	Channel Establishment
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not Configured	No
On	Desirable	No
Auto/On	Auto	No

Figure 11.8 *Channel establishment with PAgP*

LACP is part of an IEEE specification (802.3ad) that allows several physical ports to be bundled to form a single logical channel. LACP is also defined in IEEE 802.1AX standard for local and metropolitan area networks. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. It performs a function similar to PAgP. Because LACP is an IEEE standard, it can be used to facilitate EtherChannels in multi vendor environments. There are three modes for LACP: on, active and passive. The on mode forces the interface to channel without LACP. The active mode places a port in an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets. The passive mode places a port in a passive negotiating state in which the port responds to the LACP packets that it receives, but does not initiate LACP packet negotiation.

Figure 11.9 presents the channel establishment when ports of switches S1 and S2 are in the different modes for LACP.

S1	S2	Channel Establishment
On	On	Yes
Active/Pasive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

Figure 11.9 *Channel establishment with LACP*

3. Lab activity

3.1 Discuss the theoretical aspects presented in this chapter.

3.2 Switch configuration

Cisco switches and routers use a very similar command-line interface (CLI) which is used for configuration and verification purposes.

The help command is question mark (**?**) which displays the list of commands available for the current command mode, the list of commands that begin with a particular character sequence or the list of keywords or arguments that are associated with a particular command.

Switches have several command modes. The User EXEC mode has a limited command set that can change terminal settings, perform basic tests, or display system information. The *enable* command is used to change from User EXEC mode to Privileged EXEC mode. The Privileged EXEC mode has a larger command set that includes the User EXEC mode command set and the *configure* command used to change from Privileged EXEC mode to global configuration mode. Global configuration mode allows other command modes to be accessed, which are used to configure the switch. The command *exit* is used to exit back from a command mode.

Issue *show running-config* command to view the current configuration file of the switch.

Enter the Privileged EXEC mode with the *enable* command.

Issue *copy running-config startup-config* command to copy the current configuration file to back up configuration file.

In order to completely erase the switch configuration, the following steps have to be followed:

Delete the VLAN database file vlan.dat from the flash directory with the *delete flash:vlan.dat* command.

Erase the backup configuration file startup-config with the *erase startup-config* command.

Reload the switch with the *reload* command.

Switch# enable

```
Switch# copy running-config startup-config
Switch# delete flash:vlan.dat
Switch# erase startup-config
Switch# reload
```

Change from Privileged EXEC mode to global configuration mode with the *configure terminal* command.

Set the switch name with the *hostname host_name* command.

```
Switch# enable
Switch# configure terminal
Switch(config)# hostname SWITCH_EXAMPLE
```

Configure the primary terminal line with the following commands:

```
Switch(config)# line console 0
Switch(config-line)# password password
Switch(config-line)# login
Switch(config-line)# exit
```

Configure virtual terminal with the following commands:

```
Switch(config)# line vty 0 4
Switch(config-line)# password secret_password
Switch(config-line)# login
Switch(config-line)# exit
```

●

In order to allow the switch to be accessible by TCP/IP applications, IP addresses and a default gateway should be set. This allows switch configuration using a telnet or ssh connection. Unlike routers, in the case of switches, IP addresses are configured on VLAN interfaces. Configure IP address and default gateway with the following commands:

```
Switch(config)# interface VLAN1
Switch(config-if)# ip address ip_address netmask
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway default_gateway_address
```

3.3 Spanning Tree

Step 1: Configure the network presented in Figure 11.10. If the amber port LED in your topology is not in the same position as in the picture, move the switches so that the amber port LED to be as it is in the figure.

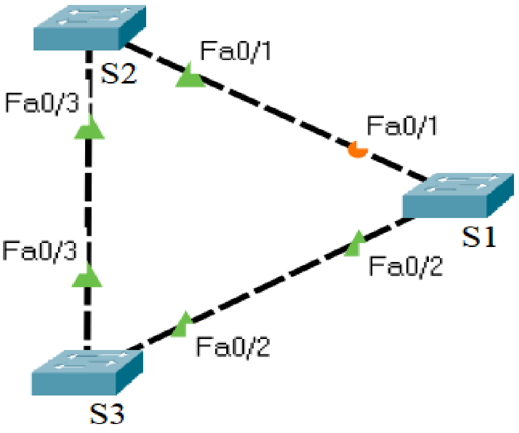


Figure 11.10 *Test network topology*

1. Specify the host names for the switches

2. Examine the Spanning Tree configuration

- The port LED color is green if the port is in forwarding state, while the port LED color is amber if the port is in blocking state.
- View the Spanning Tree information on each switch, with the corresponding show command. Examine and explain the output of the command.

General syntax:

Switch# show spanning-tree

Description: Displays Spanning Tree information

3. Answer the following questions:

- Why is this topology useful and implemented in computer networks?
- Which switch is the root bridge and why?

Step 2: To the previous topology connect the users to S2 and S3 switches and add the router that connects the network to other networks like in the Figure 11.11. In this way, an extended star topology with a backup path is obtained.

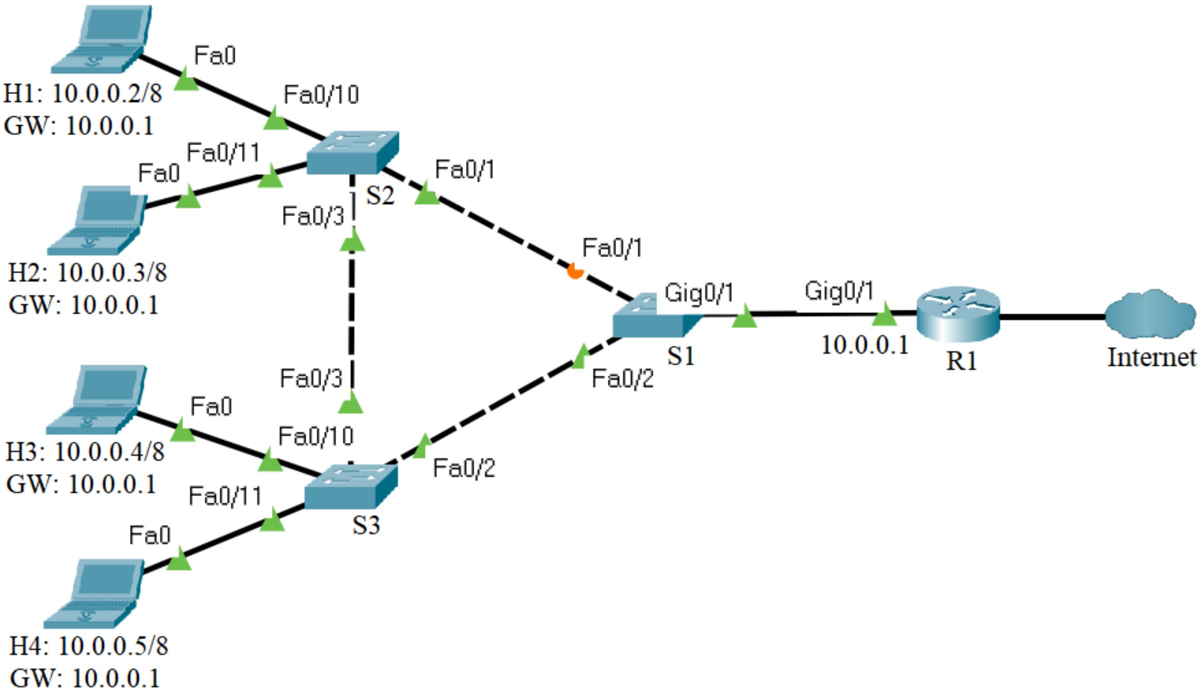


Figure 11.11 *Test network topology*

Before configuring the network devices, discuss the IPv4 address assignment in the Table 11.4:

Table 11.4 *IPv4 addresses for the test network*

Device	Interface	IP Address	Netmask	Gateway
Laptop H1	Fa0	10.0.0.2	255.0.0.0	10.0.0.1
Laptop H2	Fa0	10.0.0.3	255.0.0.0	10.0.0.1
Laptop H3	Fa0	10.0.0.4	255.0.0.0	10.0.0.1
Laptop H4	Fa0	10.0.0.5	255.0.0.0	10.0.0.1
R1	Gig0/1	10.0.0.1	255.0.0.0	-

1. Specify the host name for the router
2. Assign the IP information to the hosts and the router
3. Test the connectivity between the hosts and the router using the *ping* command
4. Analyze the network and answer the following questions:

- Which path should be the backup path (redundant link) and why?
- Which switch should be the root bridge to obtain the optimal paths in the Layer 2 network?

- What configuration should be done so that a particular switch becomes the root bridge regardless of the MAC addresses of the switches on the network?

5. Change the root switch by changing its priority to a lower value than the default value

General syntax:

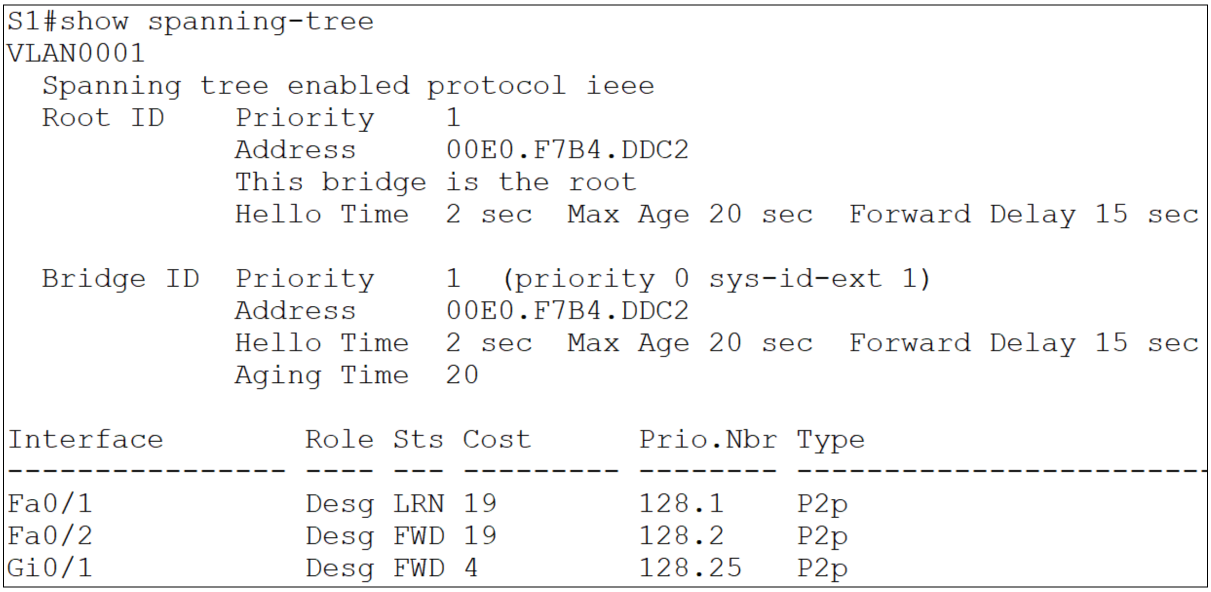
Switch(config)# spanning-tree vlan vlan_number priority priority_number

Description: Changes the Spanning-tree priority of the switch

Consider: switch *S1*, vlan *1* and priority *0*

6. Issue *show spanning-tree* command (Figure 11.12) several times to view the Spanning Tree information on switch S1

- Pay attention to the following:
  - Switch S1 becomes the root bridge
  - The port in the blocking state goes to the forwarding state passing through listening and learning states



```
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     00E0.F7B4.DDC2
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1  (priority 0 sys-id-ext 1)
             Address     00E0.F7B4.DDC2
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa0/1            Desg LRN 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p
```

Figure 11.12 *Show spanning-tree command output for S1*

- In the network topology, the amber port LED becomes green while a port LED between S2 and S3 switches becomes amber (Figure 11.13). The link between S1 and S2 forwards the traffic while the link between S2 and S3 becomes the backup path, the redundant link. Issue *show spanning-tree* command (Figure 11.14) to view the Spanning Tree information on the switch having the amber port LED.

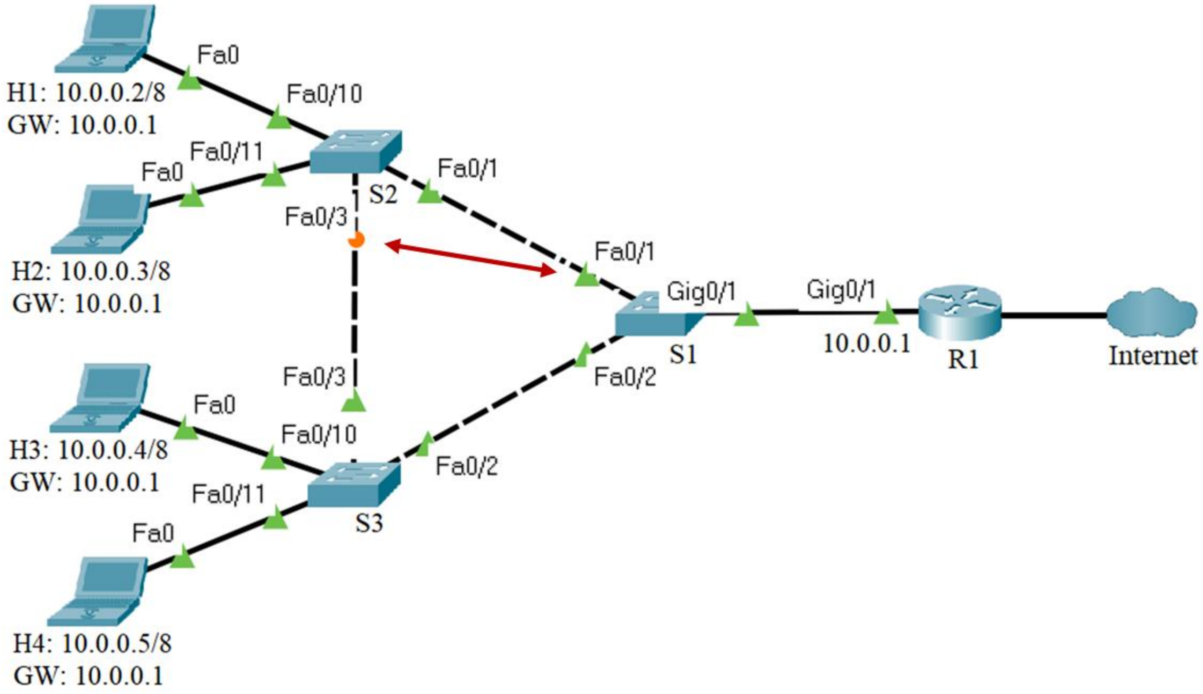


Figure 11.13 *STP changes the state of the ports*

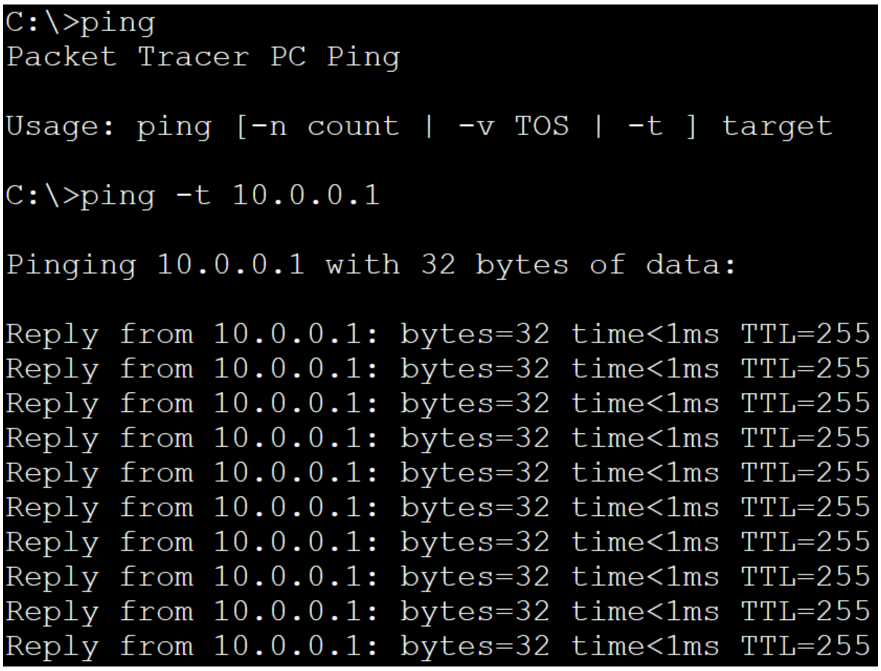
```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority     1
              Address      00E0.F7B4.DDC2
              Cost         19
              Port         1(FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority     32769  (priority 32768 sys-id-ext 1)
              Address      00D0.D349.4CEC
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   20

Interface         Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa0/1             Root FWD 19        128.1    P2p
Fa0/3             Altn BLK 19        128.3    P2p
Fa0/10            Desg FWD 19        128.10   P2p
Fa0/11            Desg FWD 19        128.11   P2p
```

Figure 11.14 *Show spanning-tree command output for the switch having the amber port LED*

7. Continuously test the connectivity between the host H1 and the router using the *ping* command with *-t* option (Figure 11.15)



```
C:\>ping
Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping -t 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```

Figure 11.15 *Connectivity test between the host H1 and the router*

8. While the *ping* command is testing the connectivity between the host H1 and the router, remove the link between the S1 and the S2 switches (Figure 11.16).

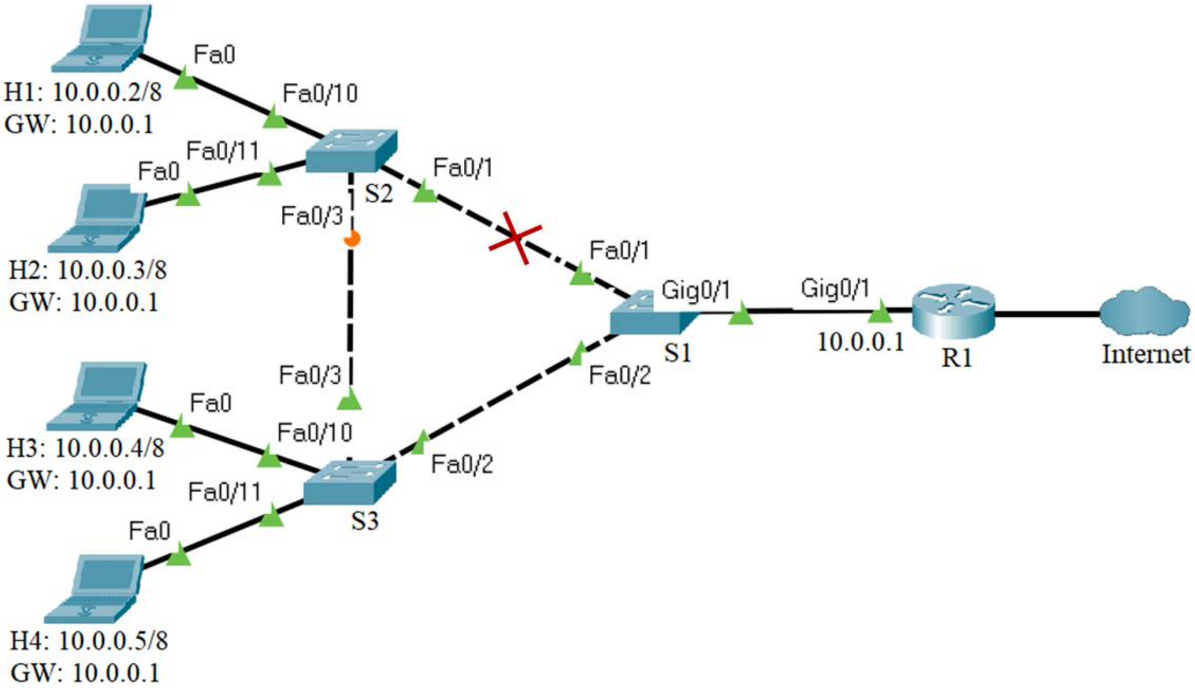
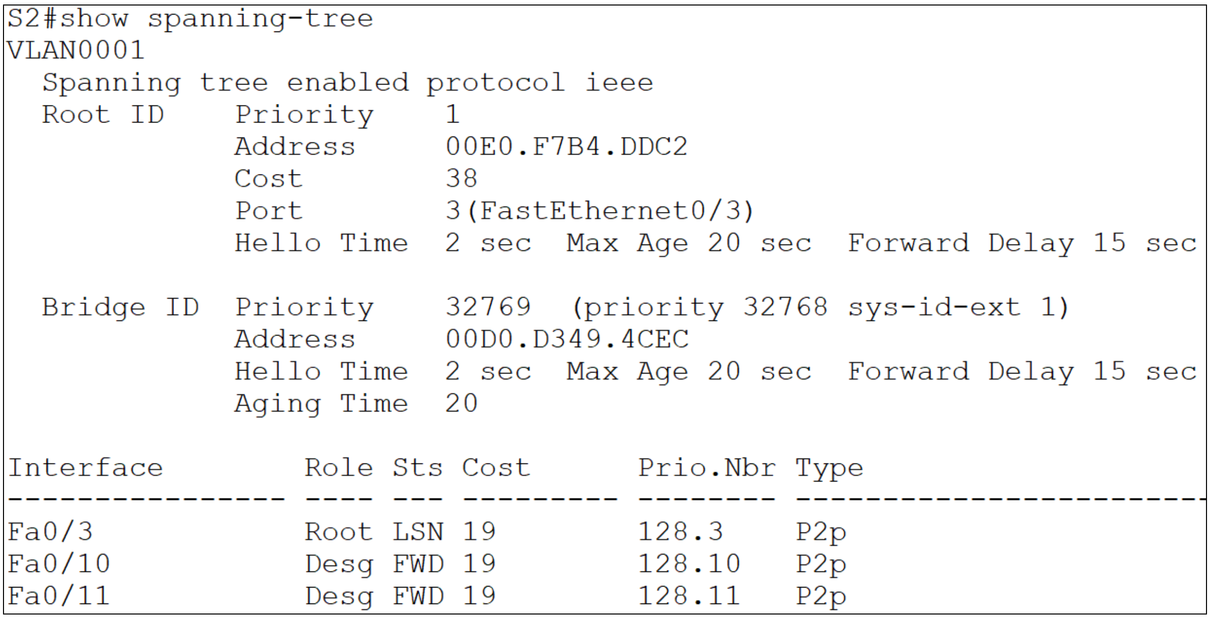


Figure 11.16 *Removing the link between S1 and S2 switches*

- Issue *show spanning-tree* command (Figure 11.17) several times to view the Spanning Tree information on switch S2; pay attention to the port in the blocking state, it goes to the forwarding state passing through listening and learning states



```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority     1
              Address      00E0.F7B4.DDC2
              Cost         38
              Port         3(FastEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority     32769  (priority 32768 sys-id-ext 1)
              Address      00D0.D349.4CEC
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/3            Root LSN 19        128.3    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

Figure 11.17 *Show spanning-tree command output for S2*

- In the network topology, the amber port LED becomes green (Figure 11.18), the link between S2 and S3 forwards the traffic.

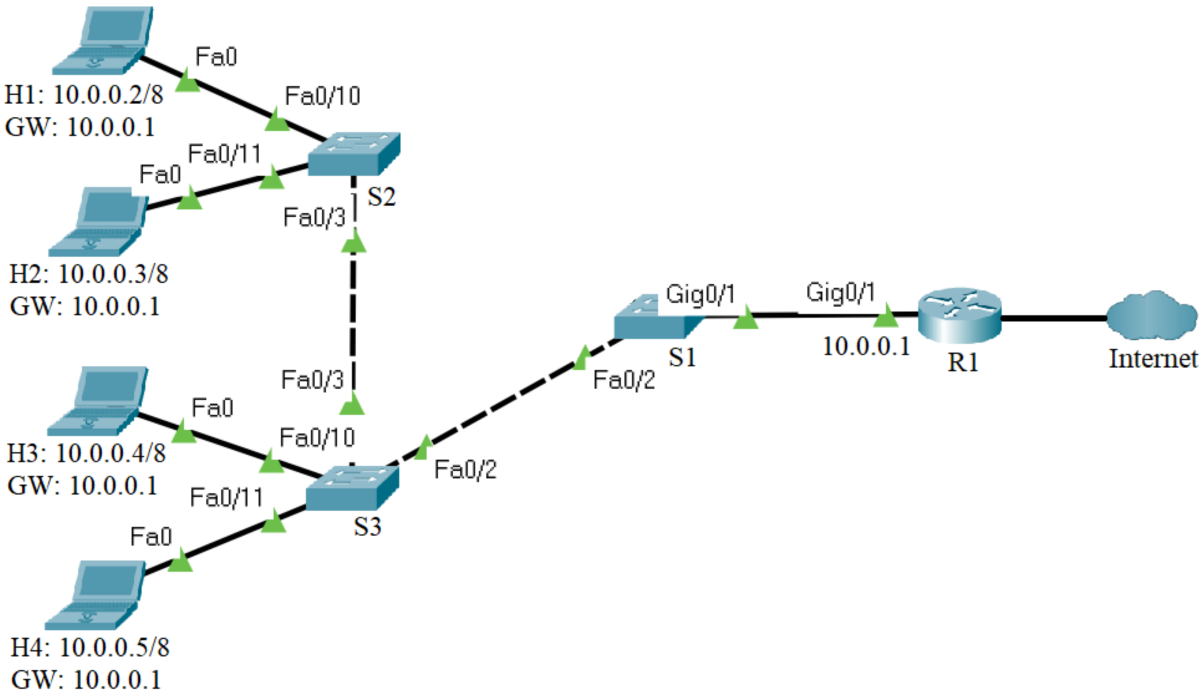
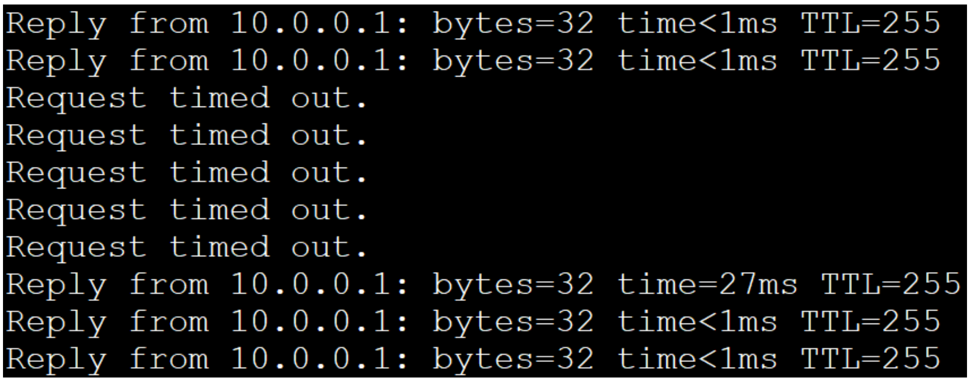


Figure 11.18 *STP changes the state of the ports*

- The Spanning-tree protocol restores connectivity between the H1 host and the router through the redundant link (Figure 11.19)



```
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.0.0.1: bytes=32 time=27ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```

Figure 11.19 *Connectivity test between the host H1 and the router*

9. Restore the link between the S1 and the S2 switches and observe how Spanning-tree protocol chooses the shortest paths to the root bridge and blocks the redundant links (Figure 11.20).

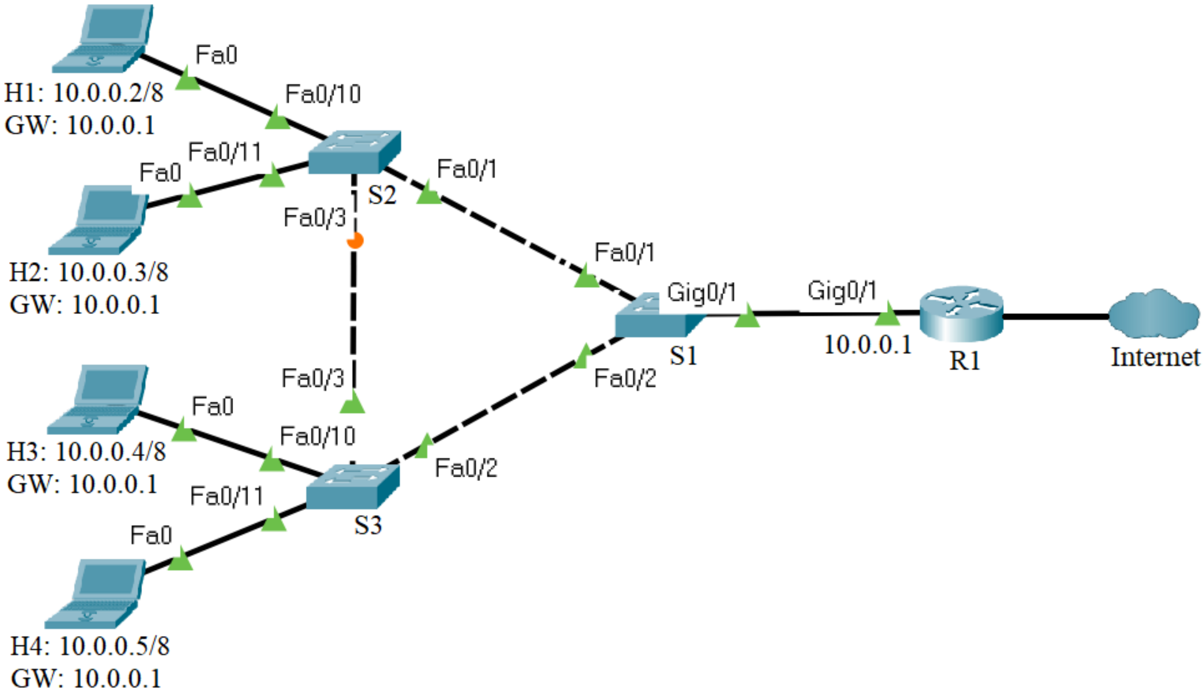


Figure 11.20 *Restoring the link between S1 and S2 switches*

3.4 EtherChannel

Cable the network presented in the Figure 11.21.

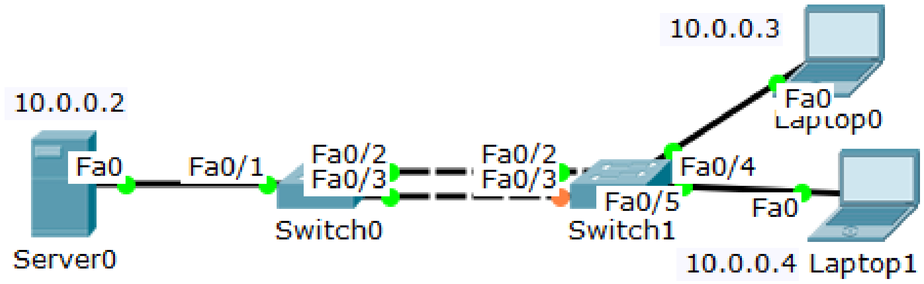


Figure 11.21 *Test network topology*

Before configuring the network devices, discuss the IPv4 address assignment in the Table 11.5:

Table 11.5 *IPv4 addresses for the test network*

Device	Interface	IP Address	Netmask
Server0	Fa0	10.0.0.2	255.0.0.0
Laptop 0	Fa0	10.0.0.3	255.0.0.0
Laptop 1	Fa0	10.0.0.4	255.0.0.0

1. Configure the IP addresses on the hosts.

2. Verify the connectivity between the laptops and Server0 with the `ping` command.

3. Connect to the Switch0 and enter the Privileged EXEC mode. View the Spanning Tree information with the *show spanning-tree* command. Examine and explain the output of this command.

Switch0#show spanning-tree

4. Repeat the previous step for Switch1.

5. Connect to Switch0 and specify the interfaces that compose the EtherChannel group using the *interface range* interface global configuration mode command. Create the port channel interface with the *channel-group identifier mode on* command in interface range configuration mode. The identifier specifies a channel group number.

Switch0(config)#interface range fastEthernet 0/2-3
Switch0(config-if-range)#channel-group 1 mode on

6. Repeat the previous step for Switch1.

7. Connect to the Switch0 and enter the Privileged EXEC mode. View the running-config file with the *show running-config* command. Examine and explain the output of this

command. View the Etherchannel information with the *show etherchannel summary* command. Examine and explain the output of this command. View the Spanning Tree information with the *show spanning-tree* command. Examine and explain the output of this command.

```
Switch0#show running-config
Switch0#show etherchannel summary
Switch0#show spanning-tree
```

8. Repeat the previous step for Switch1.

9. Connect to Switch0 and enter port channel interface configuration mode using the *interface port-channel* command, followed by the interface identifier. Configure the EtherChannel as a trunk interface using the *switchport mode trunk* command.

```
Switch0(config)#interface port-channel 1
Switch0(config-if)#switchport mode trunk
```

10. Repeat the previous step for Switch1.

11. Connect to the Switch0 and enter the Privileged EXEC mode. View the running-config file with the *show running-config* command. Examine and explain the output of this command. View the trunking information with the *show interfaces trunk* command. Examine and explain the output of this command.

```
Switch0#show running-config
Switch0#show interfaces trunk
```

12. Repeat the previous step for Switch1.

13. Connect to Switch0 and configure EtherChannel load balancing method using the *port-channel load-balance* global configuration mode command. Select the load-distribution method based on the destination-host MAC address of the incoming packet (dst-mac). Enter the Privileged EXEC mode and view the EtherChannel load balancing method information with the *show etherchannel load-balance* command. Examine and explain the output of this command.

```
Switch0(config)#port-channel load-balance dst-mac
Switch0(config)#end
Switch0#show etherchannel load-balance
```