NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Electrical & Electronic Engineering

IE3017 Computer Communications

Academic Year 2025-2026

L3017

Internetworking of Switched LANs

Communication Research Laboratory (S2-B4c-17)

Dress Code in the Laboratory

- **Work shirt that covers the upper torso and arms.**
- **Lower body clothing that covers the entire leg.**
- **Closed-toe shoes that cover the top of the foot.**

Please access this link:
http://tiny.cc/f6f5001 **or scan the QR code below to access EEE CA Guidelines.**
Request for MAKE-UP LAB SESSION must be submitted only after the online leave application form has been submitted.

Laboratory Manual

NANYANG TECHNOLOGICAL UNIVERSITY
SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING

ACADEMIC YEAR 2023/24

L3017 LABORATORY MANUAL

Internetworking of Switched LANs

Communication Lab
(S2 – B4c – 17)

Students are expected to read through the theoretical parts (Appendices D & E) of this manual before attending this laboratory session

NAME : _____

GROUP : _____

DATE : _____

INSTRUCTION

1. This 3-hour experiment consists of 2 parts:

   Part I: Spanning-Tree Protocol in switched LAN
   Part II: Multiple VLANs and trunk line between LAN switches

2. Enter your experimental results only in the space provided in this manual
3. Students may ask the lecturer-in-charge questions concerning the theory, laboratory equipment and experiment procedures but not questions set out in this manual.
4. Keep your answers short so that they can be written within the space provided in this manual.
5. Make sure you understand what you are doing and know how to operate the instruments. If you don't, please ask.

Part 1. Spanning-Tree Protocol in Switched LAN

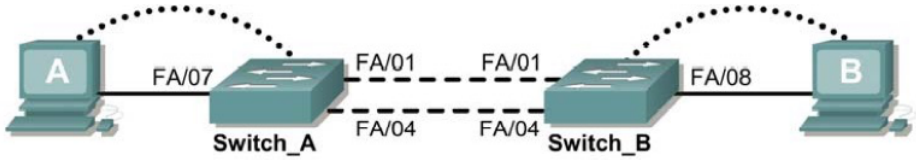
1. Objectives

a. To study the principle of spanning-tree protocol
b. To study the characteristics of LAN switches in presence of spanning-tree protocol.

2. Equipment

a. Two 24-port Catalyst switch 2950
b. Two PCs

3. Description of laboratory experiment set-up



Switch Designation	Switch Name	Enable Secret Password	Enable,VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0
Switch 2	Switch_B	class	cisco	192.168.1.3	192.168.1.1	255.255.255.0

Table 1

4. Procedure and Results

a. Verify the cable connections as shown in the experiment diagram.

b. Set up a Tera Terminal, each on Host A and B, to console to the Switch_A and Switch_B, respectively. (Refer to Appendix A on how to set up the Tera Terminal)

c. Verify the configurations of the switches to ensure all values are the same as shown in the Table 1 by using the following switch commands.

```
Switch_A (or B)>
Switch_A (or B)>enable
Switch_A (or B)#
Switch_A (or B)#show startup
```

Refer to Table 1 for the password required at the two different levels.
Refer to Appendix B for the different switch command modes that you will be using in both Part I and Part II of this lab.

d. Configure the IP network address, subnet mask, and default gateway on Host A and Host B, respectively, as shown in Table 2. (Refer to Appendix C on how to configure a host)

Host	IP Address	Default Gateway	Subnet Mask
PC_A	192.168.1.10	192.168.1.1	255.255.255.0
PC_B	192.168.1.20	192.168.1.1	255.255.255.0

Table 2

e. Verify to ensure successful connections between the host and the switch by using the "ping" function from the Command Prompt Window.

```
C:\>ping Switch_A IP address (or Switch_B IP address)
```

f. Discover LAN interface information.

i. In both switches, type the **show** command at the privileged EXEC mode prompt as follows:

```
Switch_A (or B)#show interface VLAN 1
```

ii. What are the MAC (hardware) addresses of the switches?
Switch_A _____
Switch_B _____

g. Discover the spanning-tree table on each switch.

i. At the privilege EXEC mode prompt on Switch_A and Switch_B, inspect the spanning-tree table on each switch using the following command.

```
Switch_A (or B)#show spanning-tree
```

ii. Answer the following questions based on your observations

1. Which switch is the root switch? _____
2. What is the root switch ID?

   Priority:_____and MAC address: _____

3. Which ports are forwarding on the root switch? _____
4. Which ports are blocking on the root switch? _____
5. What is the non-root switch ID?

   Priority:_____and MAC address: _____

6. Which ports are forwarding on the non-root switch? _____
7. Which ports are blocking on the non-root switch? _____

h. Reassign the root switch

i. Reset the priority value **ONLY on the non-root switch** using the following commands:

```
Switch_B (or A)#configure terminal
Switch_B (or A)(config)#spanning-tree vlan 1 priority 4096
Switch_B (or A)(config)#exit
```

ii. At the privilege EXEC mode prompt on Switch_A and Switch_B, inspect the spanning-tree table on each switch using the following command:

```
Switch_A (or B)#show spanning-tree
```

iii. Answer the following questions based on your observations

1. Which switch is the root switch? _____
2. What is the root switch ID?

   Priority:_____and MAC address: _____

3. Which ports are forwarding on the root switch? _____
4. Which ports are blocking on the root switch? _____

5. What is the non-root switch ID?

   Priority:_____and MAC address: _____

6. Which ports are forwarding on the non-root switch? _____
7. Which ports are blocking on the non-root switch? _____
8. Explain why the root switch has been changed?

_____
_____
_____
_____
_____
_____
_____
_____
_____

i. Spanning-tree Recalculation

i. Remove the cable from the forwarding port on the non-root switch, which is previously connected to the root switch.
ii. Wait for at least two minutes
iii. Inspect the spanning-tree status on each switch using the following command:

```
Switch_A(or B)#show spanning-tree
```

iv. Comparing the observations with the results obtained in Step h, what changes have taken place on

Switch_A? _____
_____
_____

Switch_B?_____
_____
_____

v. Reconnect the cable to the port that it was removed from.
vi. Inspect the spanning-tree status on each switch using the following command:

```
Switch_A(or B)#show spanning-tree
```

vii. Comparing the observations with the results obtained in Step h, what changes have taken place on

Switch_A? _____
_____
_____

Switch_B?_____
_____
_____

viii. Explain your observations.

_____
_____
_____
_____
_____
_____

Part 2. Virtual LAN (VLAN)

1. Objectives

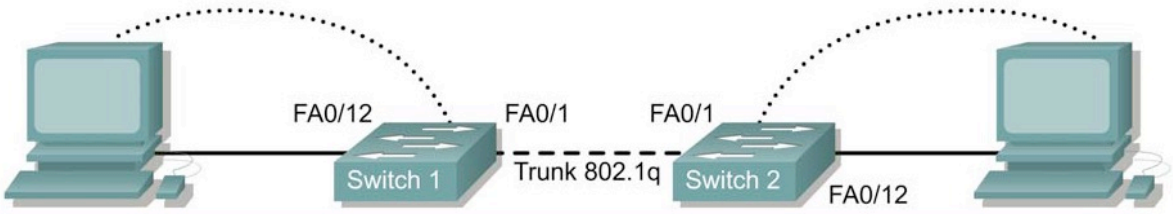
a. To study the principles of Virtual LAN (VLAN)
b. Create multiple VLANs and assign multiple member ports to each VLAN
c. Create a trunk line between the two switches for inter-communications between paired VLANs
d. Test the VLANs functionality

2. Preparation

a. Remove the cable from port 4 of both switches
b. Make sure PC_A is connected to Switch_A port 0/12
c. Make sure PC_B is connected to Switch_B port 0/12

6

3. Description of laboratory experiment set-up



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Subnet Mask	VLAN Names and Numbers	Switch Port Assignments
Switch 1	Switch_A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12
Switch 2	Switch_B	class	cisco	192.168.1.3	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12

---

4. Procedure and experiment results

a. Discover LAN interface information

i. In both switches, type the following command at the privileged EXEC mode prompt:

```
Switch_A (or B)#show vlan
```

ii. How many active VLANs have been found in Switch_A _____and Switch_B _____

b. Go to the 'Interface Configuration' mode (refer to Appendix B for more details). Convert access mode in Switch_A port 0/1 and Switch_B port 0/1 using the following commands:

```
Switch_A(config)#interface fastethernet 0/1
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#end

Switch_B(config)#interface fastethernet 0/1
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#end
```

c. Create VLAN 10, VLAN 20, and VLAN 30 using the following commands on <u>both</u> switches:

```
Switch_A#configure terminal
Switch_A(config)#vlan 10
Switch_A(config-vlan)#name Accounting
Switch_A(config-vlan)#exit
Switch_A(config)#vlan 20
Switch_A(config-vlan)#name Marketing
Switch_A(config-vlan)#exit
Switch_A(config)#vlan 30
Switch_A(config-vlan)#name Engineering
Switch_A(config-vlan)#end
```

d. Assign multiple ports to VLAN 10, VLAN 20, and VLAN 30 using the following commands:
'

i. Assigning ports 0/4 - 0/6 to VLAN 10

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#exit

Switch_A(config)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#exit

Switch_A(config)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```

ii. Repeat Step i, assigning ports 0/7 - 0/9 to VLAN 20 and ports 0/10 - 0/12 to VLAN 30, respectively.
iii. Repeat Steps i and ii on Switch B

e. Test the VLANs.

i. In both switches, view the VLAN interface information using the following command:

```
Switch_A(or B)#show vlan
```

ii. How many active VLANs are there in Switch_A _____and Switch_B _____

iii. Are ports 0/4 through 0/6 assigned to VLAN 10?_____

iv. Are ports 0/7 through 0/9 assigned to VLAN 20?_____

v. Are ports 0/10 through 0/12 assigned to VLAN 30?_____

vi. **Ping** from the **host** in Switch_A port 0/12 to the **host** in Switch_B port 0/12. (**Note:** Host A and Host B should be connected to the correct switch port respectively before the **ping** command is issued.)

1. Was the ping successful?_____

2. Why?_____
_____
_____

vii. **Ping** from the **host** on Switch_A port 0/12 to the **Switch_A** IP 192.168.1.2

1. Was the **ping** successful?_____

2. Why?_____
_____
_____

viii. **Ping** from the **host** on Switch_B port 0/12 to the **Switch_B** IP 192.168.1.3

1. Was the **ping** successful?_____

2. Why?_____
_____
_____

f. Create the trunk line between Switch_A port 0/1 and Switch_B port 0/1 using the following commands:

```
Switch_A(config)#interface fastethernet 0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end

Switch_B(config)#interface fastethernet 0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#end
```

g. Wait for at least one minute for the status to change before proceeding to next page experiment.

h. Test the VLANs and the trunk

i. Ping from the host on Switch_A port 0/12 to the host on Switch_B port 0/12.
   1. Was the ping successful?_____
   2. Why?_____

ii. Ping from the host on Switch_A port 0/12 to the Switch_B IP 192.168.1.3
   1. Was the ping successful?_____
   2. Why?_____

iii. Move the host in Switch_A from port 0/12 to port 0/8 and wait until the port LED goes green. Ping from the host on Switch_A port 0/8 to the host on Switch_B port 0/12.
   1. Was the ping successful?_____
   2. Why?_____

iv. Ping from the host on Switch_B port 0/12 to the Switch_B IP 192.168.1.3
   1. Was the ping successful?_____
   2. Why?_____

v. Move the host in Switch_B from port 0/12 to port 0/7 and wait until the port LED goes green. Ping from the host on Switch_A port 0/8 to the host on Switch_B port 0/7.
   1. Was the ping successful?_____
   2. Why_____

vi. Move the host in Switch_A from port 0/8 to port 0/3 and wait until the port LED goes green. Ping from the host on Switch_B port 0/7 to the host on Switch_A port 0/3.
   1. Was the ping successful?_____
   2. Why?_____

vii. Ping from the host on Switch_A port 0/2 to the Switch_B IP 192.168.1.3
   1. Was the ping successful?_____
   2. Why?_____

viii. Move the host in Switch_B from port 0/7 to port 0/16 and wait until the port LED goes green. Ping from the host on Switch_A port 0/2 to the host on Switch_B port 0/16.
   1. Was the ping successful?_____
   2. Why?_____

ix. Ping from the host on Switch_B port 0/16 to the Switch IP 192.168.1.2
   1. Was the ping successful?_____
   2. Why?_____

x. Ping from the host on Switch_B port 0/16 to the Switch IP 192.168.1.3
   1. Was the ping successful?_____
   2. Why?_____

i. What conclusions can be drawn from the above tests in regards to VLAN memberships and VLANs across a trunk?

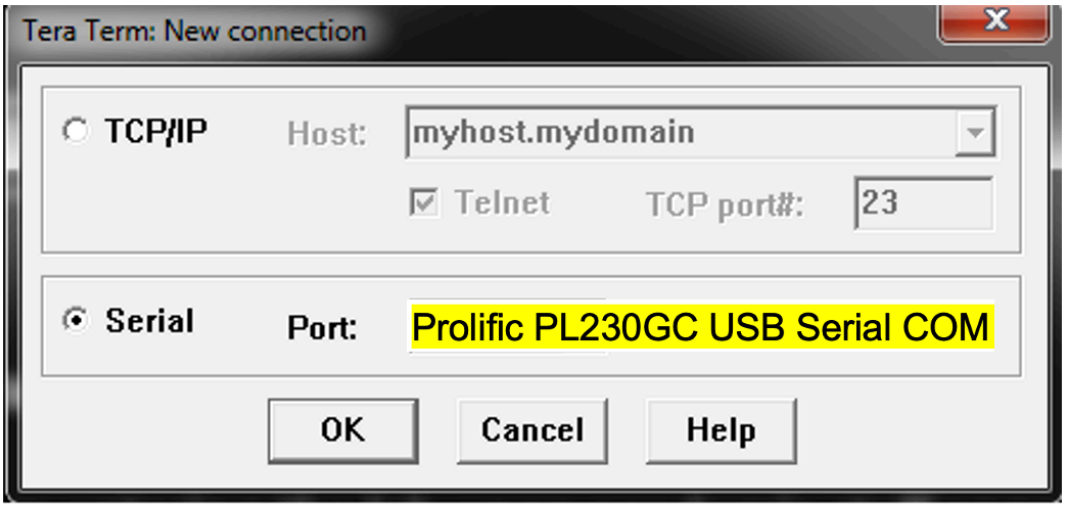
j. Once all experiment steps are complete, reset the IPv4 address to “automatically”. (Please refer to Appendix C).

k. Remove the VLANs in Switch_A by typing the following commands. Remove the VLANs in Switch_B in the same way.

```
Switch_A#configure terminal
Switch_A(config)#no vlan 10-100
```

Appendix A: Tera Term set up

A. Go to **Desktop** and double-click tera term. Ensure serial button and Prolific PL230GC USB Serial COM Port is selected



B. Select Setup -> Font -> Fixsys and enter if the wording in Tera Term is too small.

Appendix B: Verify the switch configuration

Switch Command Modes			
Command Mode	**Access Method**	**Switch Prompt Displayed**	**Exit Method**
User EXEC	Log in	Switch>	Use the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable**command.	Switch#	To exit to user EXEC mode, use the **disable**, **exit**, or **logout** command.
Global configuration	From the privileged EXEC mode, enter the **configure terminal**command.	Switch(config)#	To exit to privileged EXEC mode, use the **exit**or **end**command, or press **Ctrl-z**.
Interface configuration	From the global configuration mode, enter the **interface *type number*** command, such as **interface serial 0**.	Switch(config-if)#	To exit to global configuration mode, use the **exit**command.

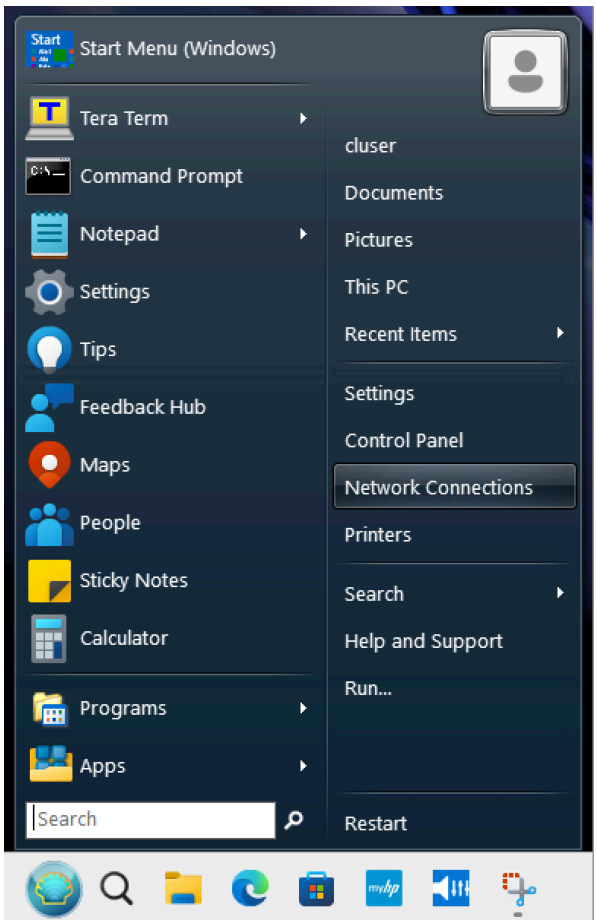
Useful commands

Switch#**show interface VLAN 1**	Display of MAC address
Switch#**show ip interface VLAN 1**	Display of IP address
Switch#**show interface fastethernet 0/12**	Display the port information
Switch#**show startup-config**	Display the switch configuration

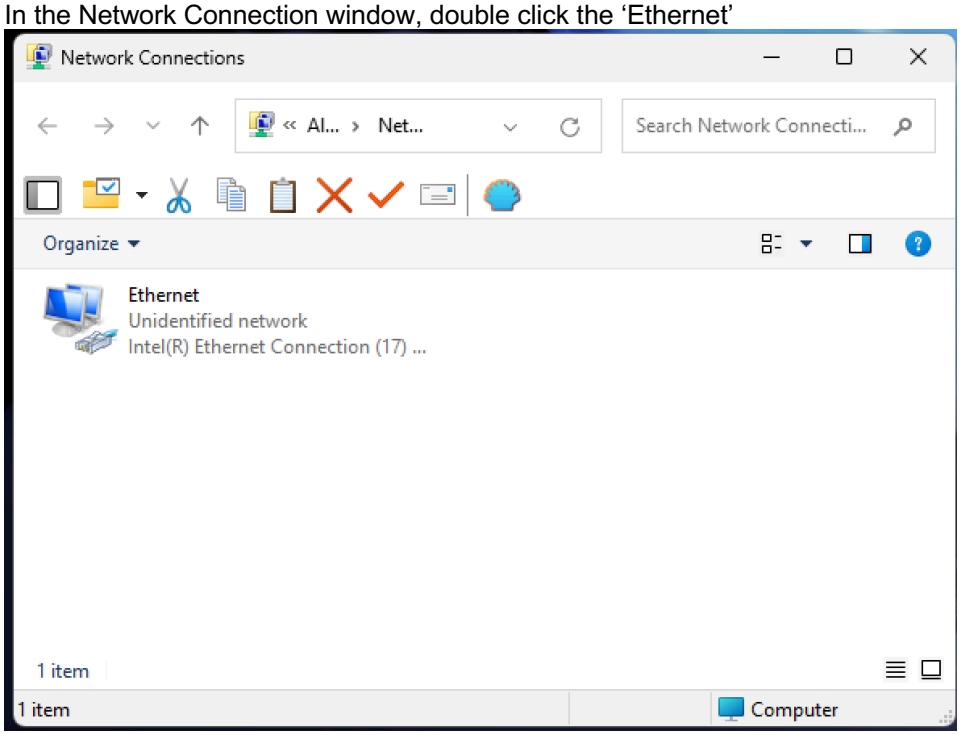
“Tab key”: key words auto-completion
“?”: context help

Appendix C: Host IP Address Configuration

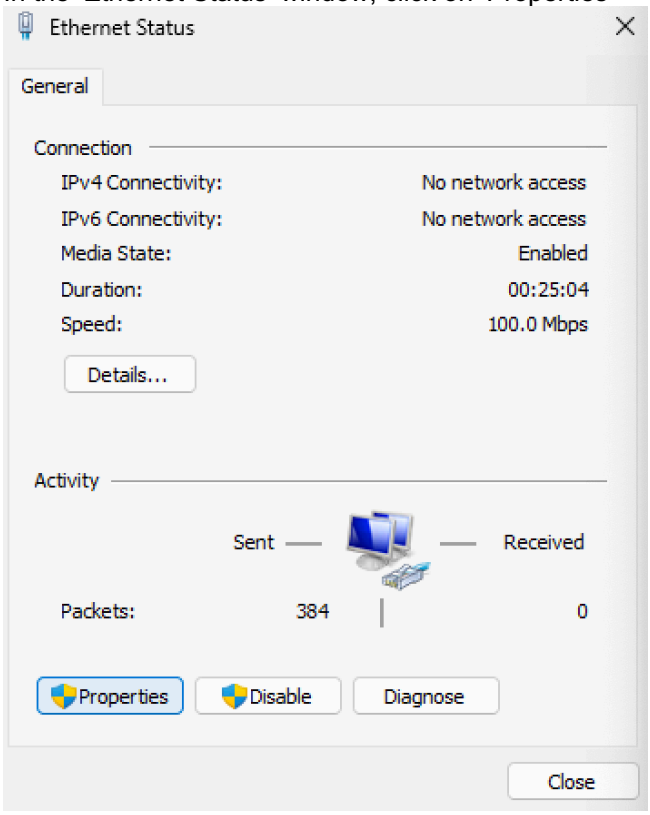
A. Click Start Menu icon on the desktop, and click '*Network Connections*' under '*Settings*'



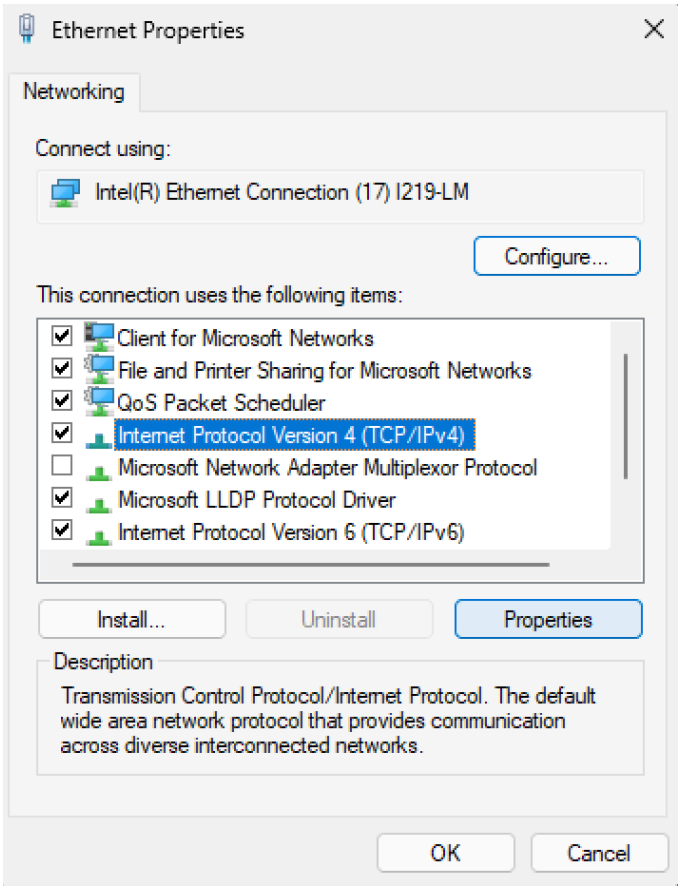
B. In the Network Connection window, double click the 'Ethernet'



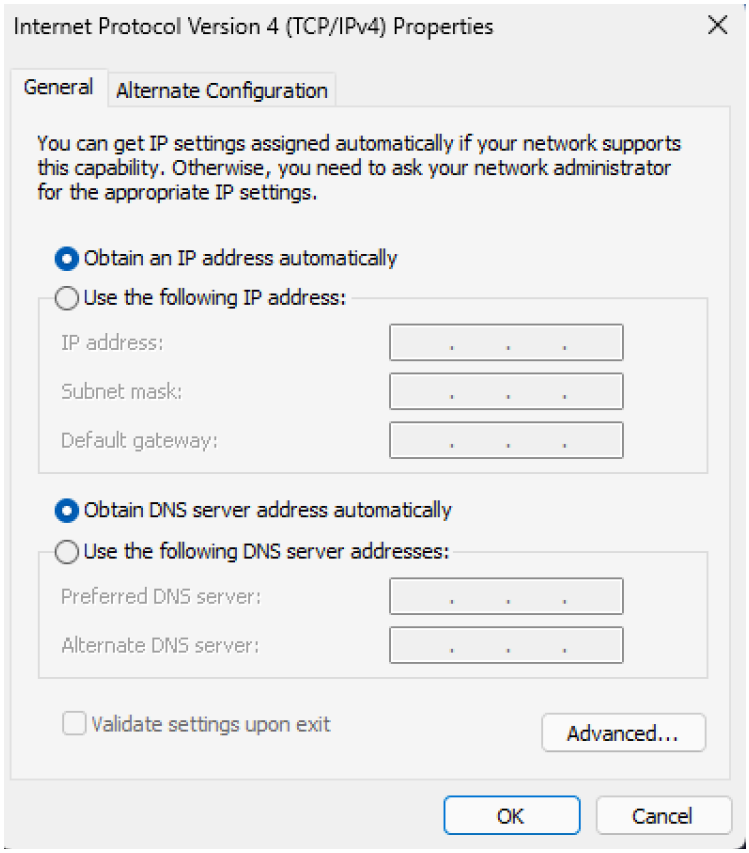
C. In the ‘Ethernet Status’ window, click on ‘Properties’



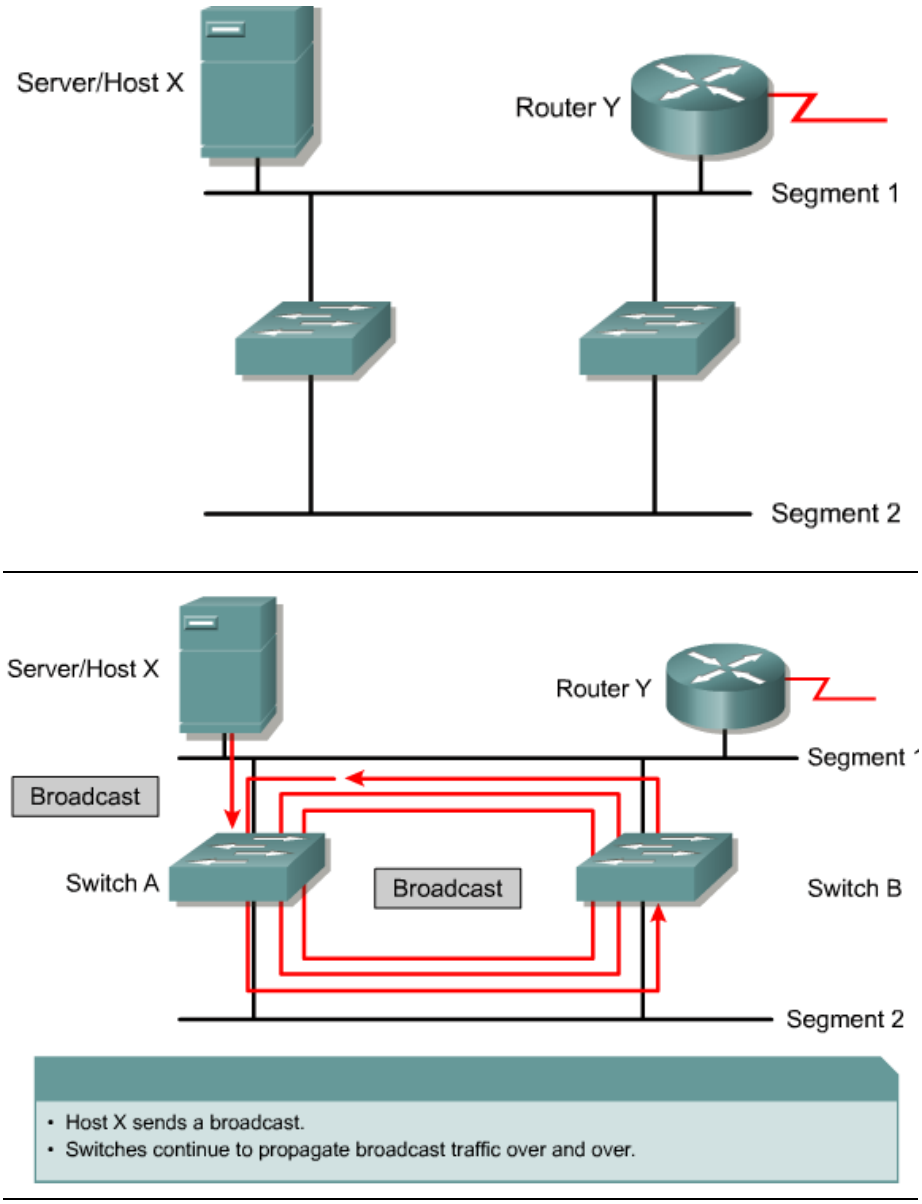
D. In the Ethernet Properties window, double click *Internet Protocol Version 4 (TCP/IPv4)*



E. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select *Use the following IP address*. Key in the IP address, subnet mask and default gateway for the PC (refer to Table 2) on page 3, then click OK to end the session.



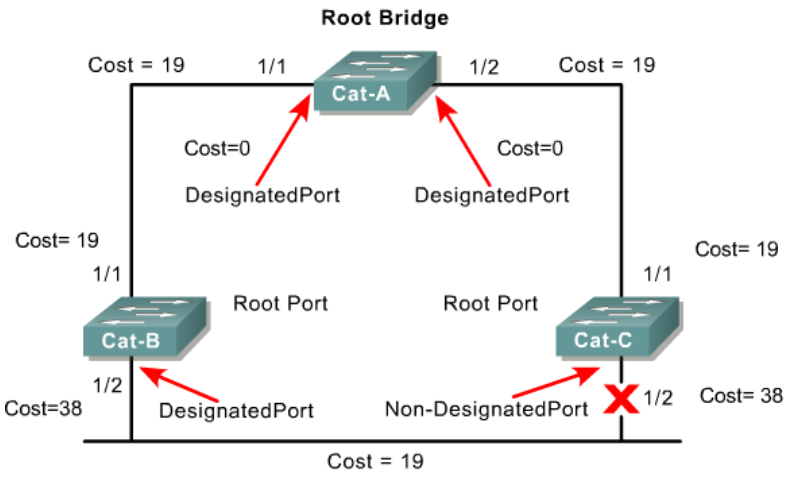
Appendix D: Spanning-Tree Protocol



Redundant network topologies are designed to ensure that networks continue to function in the presence of single points of failure. Work is interrupted less often for users because the network continues to function. Any interruptions that are caused by a failure should be as short as possible.

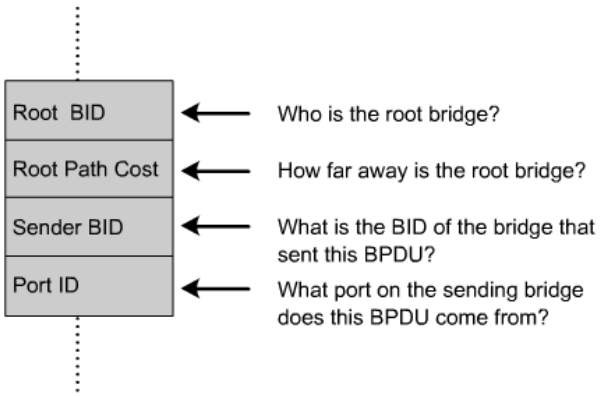
Reliability is increased by redundancy. A network that is based on switches or bridges will introduce redundant links between those switches or bridges to overcome the failure of a single link. These connections introduce physical loops into the network. These bridging loops are created so if one link fails another can take over the function of forwarding traffic.

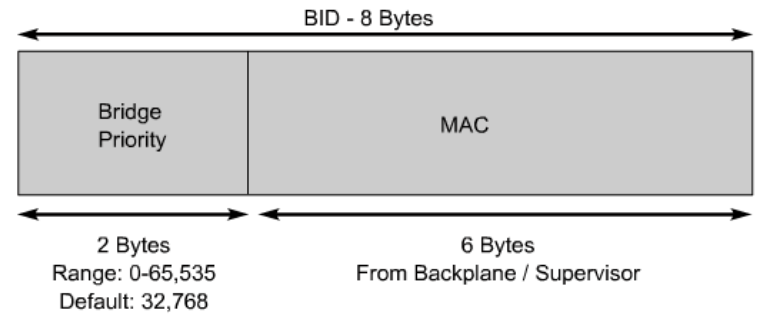
When the destination of the traffic is unknown to a switch, it floods traffic out all ports except the port that received the traffic. Broadcasts and multicasts are also forwarded out every port except the port that received the traffic. This traffic can be caught in a loop. In the Layer 2 header, there is no Time To Live (TTL) value. If a frame is sent into a Layer 2 looped topology of switches, it can loop forever. This wastes bandwidth and makes the network unusable. A physical topology that contains switching or bridging loops is necessary for reliability, yet a switched network cannot have loops.



The solution is to allow physical loops, but create a loop free logical topology. The loop free logical topology created is called a tree. This topology is a star or extended star logical topology. This topology is the spanning-tree of the network. It is a spanning-tree because all devices in the network are reachable or spanned.

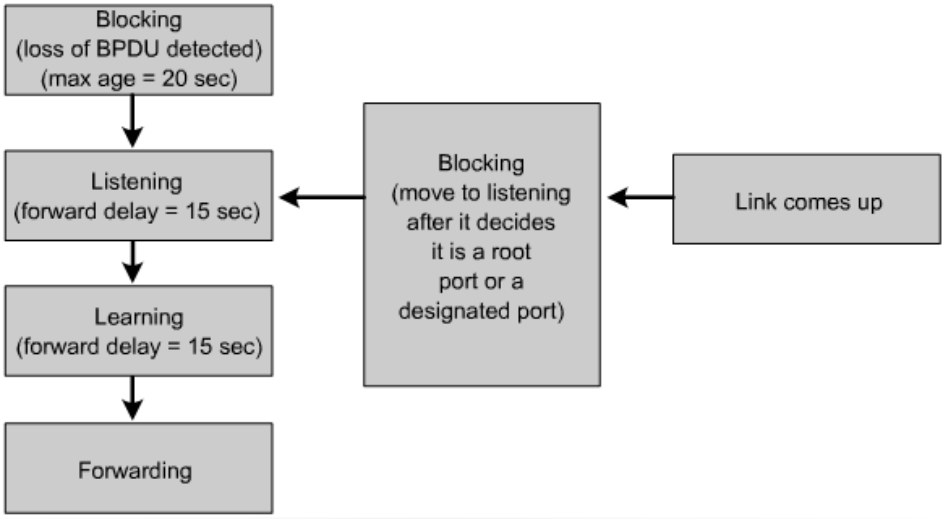
The algorithm used to create this loop free logical topology is the spanning-tree algorithm. This algorithm can take a relatively long time to converge. A new algorithm called the rapid spanning-tree algorithm was developed to reduce the time for a network to compute a loop free logical topology.



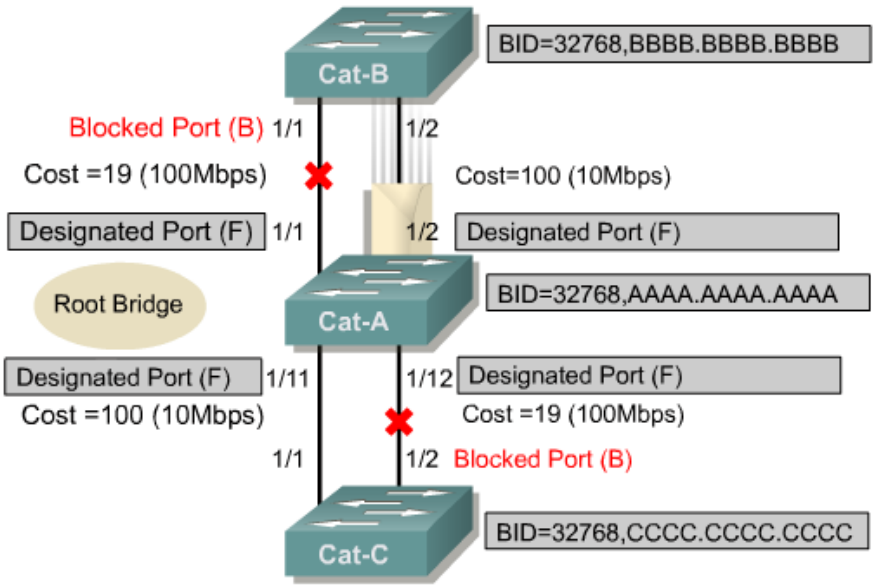


- Bridge ID (BID) is used to identify each bridge/switch.
- The BID is used in determining the center of the network, in respect to STP, known as the root bridge.

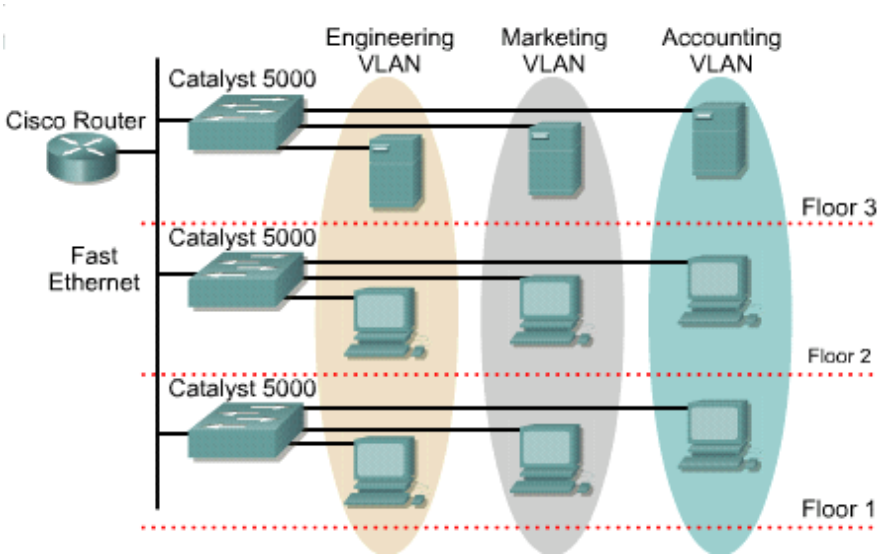
The Spanning-Tree Protocol establishes a root node called the root bridge. The Spanning-Tree Protocol constructs a topology that has one path for every node on the network. This tree originates from the root bridge. Redundant links that are not part of the shortest path tree are blocked. It is because certain paths are blocked that a loop free topology is possible. Data frames received on blocked links are dropped. The Spanning-Tree Protocol requires network devices to exchange messages to detect bridging loops. Links that will cause a loop are put into a blocking state. Switches send messages called the bridge protocol data units (BPDUs) to allow the formation of a loop free logical topology. BPDUs continue to be received on blocked ports. This ensures that if an active path or device fails, a new spanning-tree can be calculated.

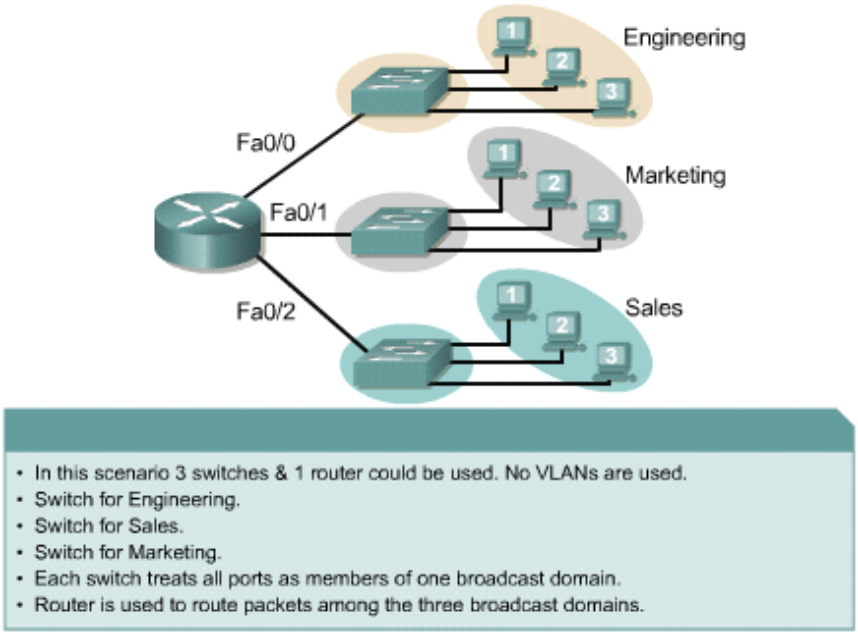


Spanning tree transits each port through several different states.



Appendix E: Virtual LAN





- In this scenario 3 switches & 1 router could be used. No VLANs are used.
- Switch for Engineering.
- Switch for Sales.
- Switch for Marketing.
- Each switch treats all ports as members of one broadcast domain.
- Router is used to route packets among the three broadcast domains.

A VLAN is a logical group of network stations, services, and devices that is not restricted to a physical LAN segment.

VLANs facilitate easy administration of logical groups of stations and servers that can communicate as if they were on the same physical LAN segment. They also facilitate easier administration of moves, adds, and changes in members of these groups.

VLANs logically segment switched networks based on job functions, departments, or project teams, regardless of the physical location of users or physical connections to the network. All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location. Configuration or reconfiguration of VLANs is done through software. Therefore, VLAN configuration does not require network equipment to be physically moved or connected.

A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group. VLANs logically segment the network into different broadcast domains so that packets are only switched between ports that are assigned to the same VLAN. VLANs consist of hosts or network equipment connected by a single bridging domain. The bridging domain is supported on different network equipment. LAN switches operate bridging protocols with a separate bridge group for each VLAN.

VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management. Switches do not bridge traffic between VLANs, as this violates the integrity of the VLAN broadcast domain. Traffic should only be routed between VLANs.

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified
802.IQ	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN id.