Report of Day-12(Spanning Tree Protocol)

What are Switching Loops?

Switching loops occur when network switches are connected in such a way that network traffic loops around infinitely instead of traversing the hops needed to travel from source to destination.

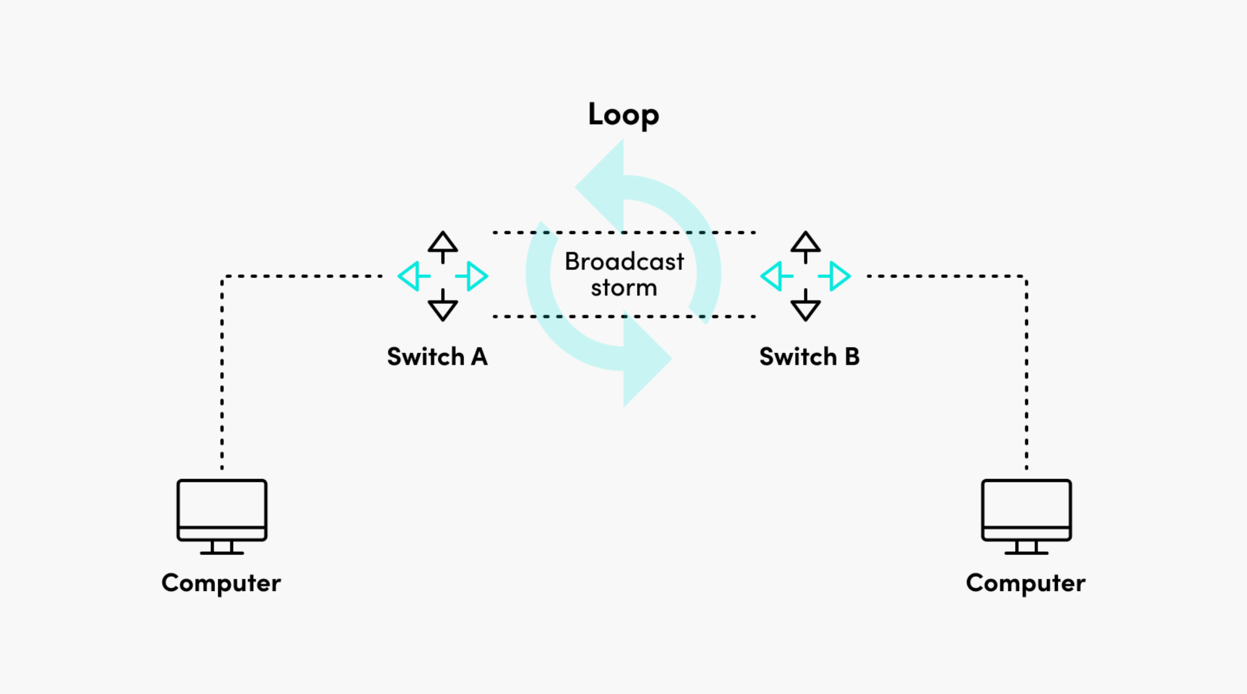
To understand what a switching loop is and how it happens, it's necessary to have a basic grasp of network switching.

Network switches are the backbone of the local area network (LAN). Switches work at Layer 2 of the OSI model, meaning they deal in forwarding traffic based on MAC addresses. MAC addresses are unique hardware addresses that are encoded within a network interface on a device. They are written in hexadecimal format and have values that range from 00:00:00:00:00:00 through FF:FF:FF:FF:FF:FF.

MAC addresses are basically like people's names. They rarely change, and you can use them to address an individual device. Switches and network devices also have special reserved MAC addresses used to address all devices on the network. The real-life equivalent would be saying "hey everyone" to address a group of people as opposed to using each of their individual names. With networking, "everyone" is the broadcast MAC address, which is FF:FF:FF:FF:FF:FF.

Switches work by learning the MAC addresses of all connected devices and forwarding traffic received from any transmitting device to only the device it is addressed to, based on the destination MAC address. This ensures that unnecessary traffic and broadcasts are minimized, which preserves network bandwidth and improves performance.

There are a couple of special cases. When a switch receives traffic targeted to a broadcast or multicast MAC address, it floods the traffic out all ports to the broadcast address except for the port the traffic was received on. Also, when a switch receives traffic destined for a MAC address that it does not know, it will flood traffic to the broadcast address on all ports except the one from which it was received.



What is RSTP?

Rapid Spanning Tree Protocol (RSTP: IEEE 802.1w) is a network protocol that is an advancement over Spanning Tree Protocol (STP: IEEE802.1D) that promotes high availability and “loop-free” topology within Ethernet networks.

A primary advantage to RSTP networks is that they offer high availability when compared to traditional daisy chain topology. When a network failure does occur, devices are able to continue communicating across the network as data can be rerouted around the failure. Critical systems depend on a high level of resiliency to faults and hardware failures and RSTP provides a key improvement over traditional network architectures by minimizing downtime.

RSTP prevents network loops when using multiple switches by blocking redundant paths on a network. In essence, the protocol is a set of rules by which switches on the network determine the most efficient way to send broadcasts across the network by establishing a “root bridge” and blocking specific ports with the purpose of preventing network loops.

There are three primary reasons why it is important to have a “loop free” Ethernet network, briefly explained here.

Erratic MAC Address Tables

A MAC address table is what allows a switch to understand the topography of the network. It is the way a switch knows where traffic on the network is from and where it needs to be sent. If there is a loop on the network, the switch can receive an identical broadcast message from two different switches on the network. Every time a new copy of the broadcast message is received, the switch must update its MAC address table.

Duplicate Data

When a switch receives a broadcast, but does not know the MAC address of the destination, it will send the broadcast out every port. This can create a situation where a device will receive duplicate copies of each broadcast being sent, wasting valuable bandwidth on redundant data. It can also lead to unrecoverable data errors.

Broadcast Storms

Perhaps the most important reason to avoid loops in network topography is to prevent “broadcast storms.” A broadcast storm is created when switches in the network each send out multiple, duplicate copies of data (or “broadcast packets”) across the network. When switches are connected in a loop, data can travel to a switch from multiple paths. Because the MAC address table is unstable in a loop arrangement, a switch has no way to understand where data needs to be sent so it broadcasts the information out of every port. This data is received by all switches on the network, and rebroadcast out again because the recipient is still unknown. This can overwhelm switches and severely degrade network performance. The broadcast storm will continue until one of the switches fails or is disconnected from the system.

What is STP?

Spanning Tree Protocol (STP) is a Layer 2 network protocol used to prevent looping within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network (LAN) that contains redundant paths. If the flow of traffic is not carefully monitored and controlled, the data can be caught in a loop that circles around network segments, affecting performance and bringing traffic to a near halt.

Networks are often configured with redundant paths when connecting network segments. Although redundancy can help protect against disaster, it can also lead to bridge or switch looping. Looping occurs when data travels from a source to a destination along redundant paths and the data begins to circle around the same paths, becoming amplified and resulting in a broadcast storm.

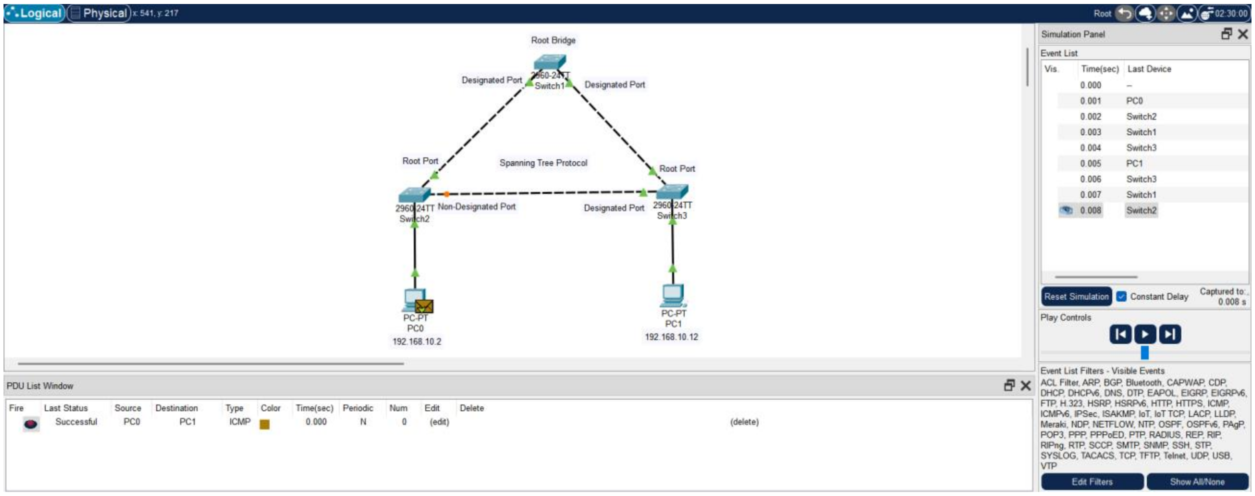
STP can help prevent bridge looping on LANs that include redundant links. Without STP, it would be difficult to implement that redundancy and still avoid network looping. STP monitors all network links, identifies redundant connections and disables the ports that can lead to looping.

What is PVST?

In a network, a spanning tree is a subset of the network's connections that connects all the nodes in the network without forming any loops. The idea is to create a tree-like structure that spans the entire network with the minimum number of connections possible while still ensuring that every node in the network is reachable.

PVST, or Per-VLAN Spanning Tree) is a network protocol that is used to prevent loops from forming in a network that is divided into multiple virtual local area networks (VLANs). In a typical network configuration, multiple devices are connected to a network through various switches and routers. Without a protocol like PVST, these devices can communicate with each other, but the network can become unstable if loops form, which can cause broadcast storms and other problems.

Network Topology for STP:



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	ICMP	🟨	0.000	N	0	(edit)	(delete)

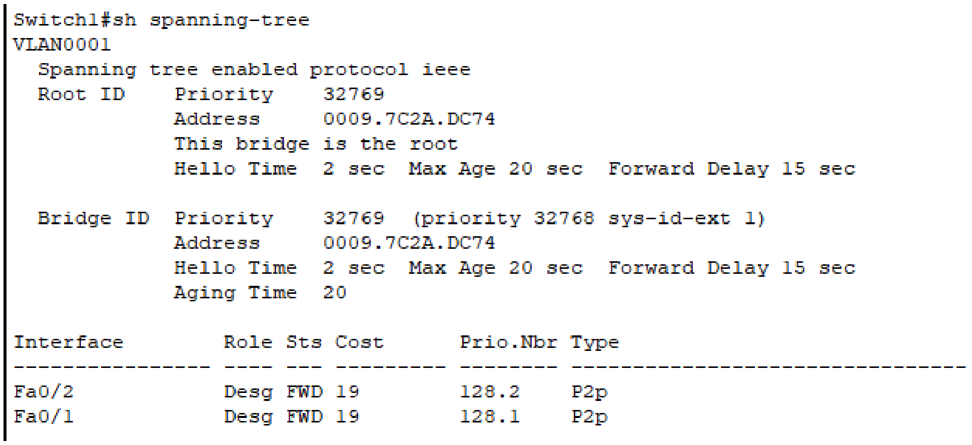
Event List

Vis.	Time(sec)	Last Device
	0.000	–
	0.001	PC0
	0.002	Switch2
	0.003	Switch1
	0.004	Switch3
	0.005	PC1
	0.006	Switch3
	0.007	Switch1
👁	0.008	Switch2

☑ Constant Delay Captured to: 0.008 s

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Switch1:

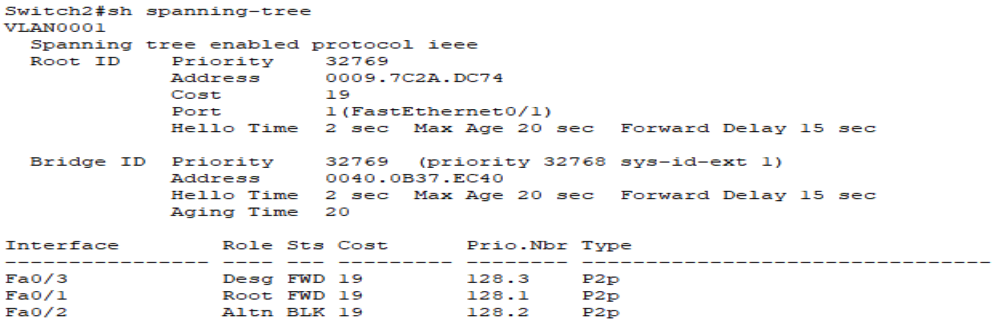


```
Switch1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7C2A.DC74
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0009.7C2A.DC74
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

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

Switch2:

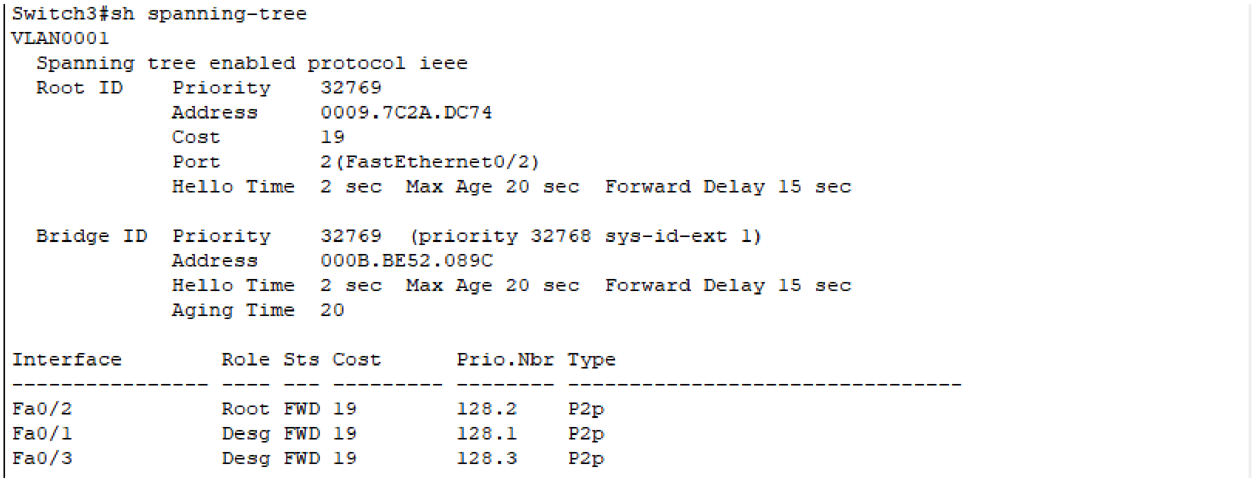


```
Switch2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7C2A.DC74
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0040.0B37.EC40
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

Switch 3:

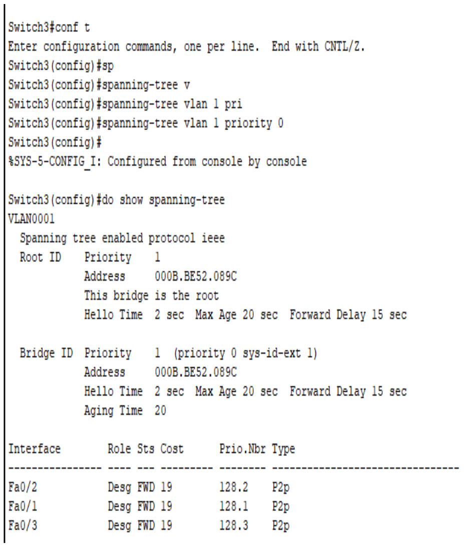


```
Switch3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7C2A.DC74
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000B.BE52.089C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Changing the Root bridge of the Network:



```
Switch3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)#sp
Switch3(config)#spanning-tree v
Switch3(config)#spanning-tree vlan 1 pri
Switch3(config)#spanning-tree vlan 1 priority 0
Switch3(config)#
%SYS-5-CONFIG_I: Configured from console by console

Switch3(config)#do show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     000B.BE52.089C
             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     000B.BE52.089C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```