Spanning Tree Protocol

A Masterôs Project

Presented to

Department of Telecommunications

In Partial Fulfillment

of the Requirements for the

Master of Science Degree

State University of New York

Polytechnic Institute

By

Sivalasya Kasu

May 2015

Spanning Tree Protocol

Declaration

I declare that this project is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Sivalasya K

Sivalasya Kasu

05/21/2015

SUNYIT

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES

Approved and recommended for acceptance as a project in partial fulfillment of the requirements for the degree of Master of Science in Telecommunications

5-21-15

DATE

Dr. Larry J. Hash

Thesis Advisor

Dr. John Marsh

Mr. Ronny Bull

EXECUTIVE SUMMARY

This technology case study focuses on Spanning Tree Protocol (STP). The Spanning Tree Protocol is a layer2 protocol that ensures a loop free topology for any LAN network. The basic function of STP is to prevent loops in the network. Spanning Tree Protocol is standardized as IEEE 802.1D. Spanning tree is created within a Layer 2 network of connected switches, leaves only one active path between two network devices. Spanning tree has evolutions and extensions such as; Per VLAN Spanning Tree Protocol (PVST), Rapid Spanning Tree Protocol(RSTP) and Multi Spanning Tree Protocol (MSTP).

Table of Contents

List of Figures

List of Tables

CHAPTER 1: INTRODUCTION

A switch is a networking component which forwards frames depending upon layer 2 MAC address and connects the multiple devices like servers, computers and so on in a building with RJ45 and/or SFP (Small form-factor pluggable) transceiver modules. Switches enable efficient communication between devices, decreasing the amount of broadcast traffic. They are widely used in the corporate world as they increase productivity of employees and save money.

A hub is also a networking component, which can also be used for data transfers, but the hub and switch differ in the way they send data to the connected devices. The hub transmits data to every device, which increases network traffic and reduces the throughput of the data forwarding. Every device connected to the hub needs to filter the incoming packets and allow packets which are intended for networking devices only. The switch learns the MAC (Media Access Control) address of the devices connected to each port and stores them in MAC tables. When a switch receives a packet it registers the MAC address against that particular port and checks for the destination MAC address. Thus, switches increase the efficiency of the network by reducing broadcast traffic.

When a packet is supposed to be sent out from a source to a destination, it checks for the destination MAC address port in the MAC table. If the destination MAC address is available in the MAC table of the switch, then the switch forwards the packets to the port mapped with the destination MAC

address. If the destination MAC address is not recorded in the switchôs MAC table, then the packet is transmits (broadcasted) to all the port of the switch except to the port from which that packet is received.

For example, consider the figure below. Switch A wants to send a packet to switch B. Switch A sends its packet to Switch 1. Because switch1 does not have that MAC address of destination, it broadcasts the packet to all its ports, except to the sender (switch A) from which the packet is received. Switch 2 and switch 3 also broadcast the packet, as they do not have that destination MAC address in their MAC tables. Switch 4 receives packets from switch 3 and switches 2 and transmits them to switch B. In this case, Switch 3 sends that packet to switch 2 and vice versa. After receiving the packet from switch 3, switch 2 transmits it to all its ports including switch 1, excluding switch 3. Switch 3 also sends the packet to all its ports except switch 2. This process continues and results in transmitting the same packet multiple times to the destination and endless loop formation between switch 1, switch 2 and switch 3.

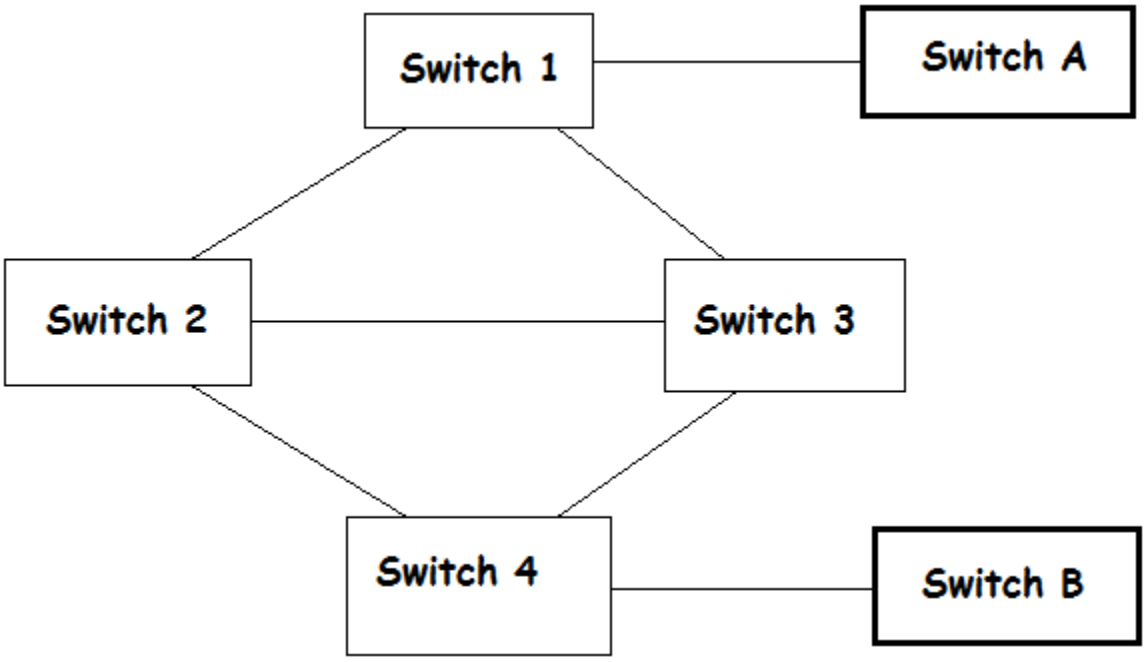


Figure 1: Network Topology

To prevent loop formation, STP (Spanning Tree Protocol) came into the picture. When multiple switches are connected to each other then STP (Spanning tree protocol) helps to prevent loop formation with BPDU (Bridge protocol data unit) messages. BPDU messages are exchanged between switches, and have complete information of switch such as the MAC address, cost of link, priority and so on. BPDU's help switches to identify potential loop formation.

This paper explains Spanning Tree Protocol with IEEE standard as 802.1d and how it works in detail. In addition, PVST (Per VLAN Spanning Tree) is enabled in the CISCO switches by default. Rapid Spanning Tree (RSTP) IEEE standard of 802.1w is used to reduce the forwarding delay for an access port on the switch and Multiple Spanning Tree Protocol (MSTP) IEEE standard 802.1q is used for running group of VLANs as one instance. For every VLAN, Spanning tree elections are conducted (in PVST). If there are many VLANs with similar functionalities, MSTP group those VLANs and run one STP instance instead of running STP per VLAN. When a switch that has low priority is connected to topology, then that switch which is connected will be the root bridge and change everything in the topology, which is a big problem. In this case if the port to which the new switch is connecting is provided with port security, solves this problem by providing security to that port (Cisco technology, 2010).

The router has routing protocols and TTL (Time to live) for a packet, which avoids loops. But switch broadcast frames have no TTL value, thus loops can occur. This paper explains how switching loops occur and how loop free switching networks are designed with STP. This paper will also cover how STP works, how loops are eliminated through STP, drawbacks in STP, and how those drawbacks are resolved with RSTP and MSTP.

As far as the role and overview of Spanning Tree Protocol is concerned, the Spanning Tree Protocol is a network protocol that ensures a loop-free topology for any LAN network. The basic function of STP is to prevent bridge loops and. Spanning Tree Protocol is standardized as IEEE 802.1D. Spanning tree is a Layer 2 network connecting switches, leaves only one active path between two network devices

The operation is simple as a collection of switches in a local area network can be represented as a graph whose nodes are switches and LAN segments, and whose edges are connections interfaces of

switch segments. To break the bonds of LAN while maintaining access to all LAN segments, switches collectively compute a spanning tree. A network administrator can reduce the cost of a spanning tree, if necessary, by altering some of the configuration parameters so as to affect the election of the root of the spanning tree. In 2001, the IEEE introduced 802.1w Rapid Spanning Tree Protocol. RSTP provides significantly faster convergence spanning tree after a topology change, the introduction of new convergence behavior and bridge port roles for this. RSTP was designed to be backward compatible with the standard STP. While STP may take 30-50 seconds to respond to a topology change, RSTP usually is able to respond within a few milliseconds of a physical link failure. The call Hello time is an important and configurable interval time of used by RSTP for various purposes; the default value is 2 seconds. IEEE 802.1D-2004 incorporates RSTP and STP obsolete original standards.

1.1 Audience Definition:

This paper is intended for people interested in networking and who have basic knowledge in hubs, switches and routers, such as like under graduate students of networking related streams like electronics and communications, etc.

CHAPTER 2: BACKGROUND

2.1 Switch

With a switch port is connected to another device like a switch, computer, printer, scanner and so on, for communicate between the switch and the device connected to that switch they need to learn MAC addresses; the switch need to learn the MAC address of the device and that device need to learn MAC address of the switch. If the device connected to the switch is a printer or scanner, these devices are not intelligent enough to learn the MAC address of switch. Through Address Resolution Protocol (ARP) switches learn MAC addresses and establishing communication between them.

If there is more than one link between any two switches, then there is a possible chance for a loop to be generated. When more than one link is connected between switches, both links will be forwarding packets on both the switches which causes a loop between them. Spanning Tree Protocol (STP) helps to prevent the loops by allowing only one of the port to be in forwarding state and blocks all the others. What is STP? How does STP work? How does the network converge with STP? All these questions are explained in depth further on in this document (Cisco technology, 2010).

2.2 How switch learns MAC addresses

Switch has a MAC address table (LAT ï Local address table), in which it stores MAC addresses of the interfaces. For any frame received by the switch, if the MAC address specified has no entry in its MAC table then switch learns MAC address through different ways. Whenever the switch receives new frames on a specific interface, then it will look at the source MAC address from the frame and store this information in its lookup table corresponding to the port on which it received the frame. When the switch receives a frame and if it doesnôt know the destination MAC-address (if the entry is not present in its lookup table), then the switch tries to broadcast this frame on all the interfaces other than the interface on which it received it. So now if the destination device responds back with a reply, then the switch will look at this reply frame and adds the source MAC-address to its lookup table corresponding to the port on which it received the reply frame. A switch can also learn MAC address by observing ARP packets received from layer 3.

A switch may have multiple VLAN's; in this case it need inter VLAN routing to communicate between them. What are VLAN's? How do they work?

2.3 VLAN and Inter VLAN Routing

A VLAN create multiple broadcast domains in the switch. A VLAN isolates its ports from another VALN. A VLAN is a group of user devices or network devices in a single virtual LAN irrespective of their geographical location. VLAN's create multiple broadcast domains in a switch, and the ports of a VLAN are isolated from other VLAN's. Every switch has a native VLAN identified as VLAN 1; by default all ports of the switch are in the native VLAN (Cisco technology, 2010).

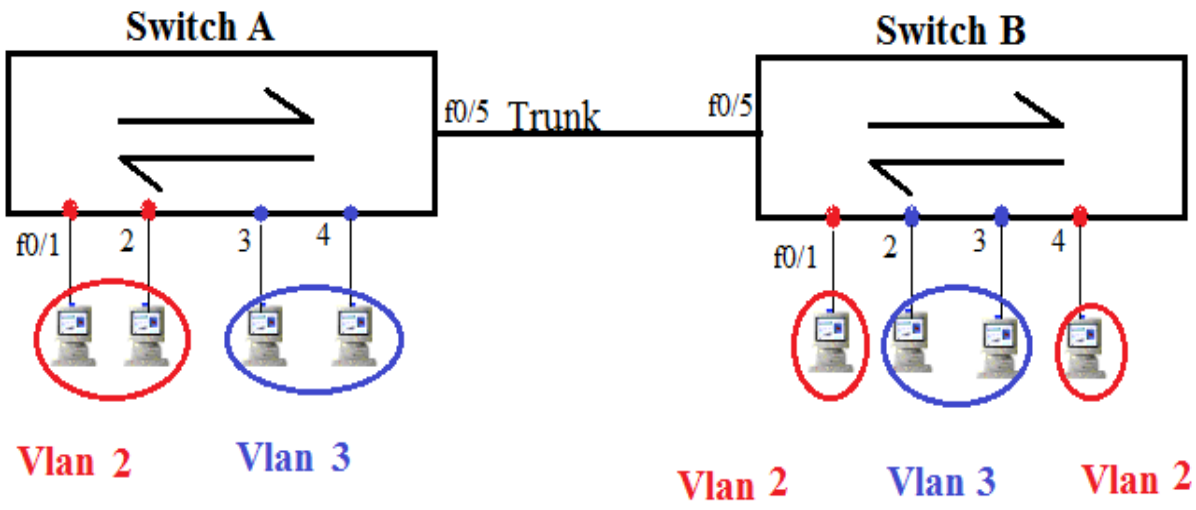


Figure 2: Multiple VLAN's and inter VLAN routing

In figure 2, switch A has VLAN 2 (named RED) and VLAN 3(named BLUE), ports in the same VLAN can only communicate without inter VLAN routing, i.e. ports in VLAN 2 can only talk to VLAN 2 ports either in Switch A or Switch B. Frames are only broadcasted within VLAN 2. The trunk carries the VLAN ID (number) along with the frame, and based on the VLAN ID, the trunk broadcasts the frame in the desired VLAN. Different VLAN's are in different Subnets. For ports in VLAN 2 to communicate with VLAN 3 ports, inter VLAN routing is needed. Inter VLAN routing enables communication between VLAN's (Cisco technology, 2010).

VLANs are quite useful to make use of a switch, dividing it into many broadcast domains as ports more efficiently use the switch. They also allow us to guarantee the quality of service and they group users into specific groups; the above and other benefits may be achieved using a single switch using VLANs.

Initially only one switch is configured to explain the syntax of the commands required to configure VLANs on a switch, but later in other tutorials multiple switches are configured with the respective VLANs and VTP (VLAN Trunking Protocol). (See Appendix A for configuration of VLAN switches).

2.4 Switch loops and Introduction to STP (Spanning Tree Protocol)

A switch can either be connected either to a router or an user devices or other switch. If a switch is connected to another switch then the operational port is trunk (VLAN information is carried) and this port sends and replies for DTP (Dynamic Trucking Protocol) messages and if a user device is connected to that port then the port is an access port which can't reply to DTP messages.

If two switches are connected with a link then the ports that connect the switches are called trunk ports. If two switches are connected with multiple paths, then there is every possibility of loop formation, because as the trunk sends the request to every port, every port will receive the request multiple times and bandwidth and processor may not sufficient for the detection of circular paths which will results in loops (Cisco technology, 2010).

Spanning Tree Protocol (STP) solves the problem of loops in topologies. STP selects one link and blocks the other links. If there are two are more than one link between two switches, and then with the STP only one of the multiple ports can be in the forwarding state leaving all the other ports in the blocking state. Hence only one of the multiple ports will be active. STP blocks all other ports with STP port selections such as root port, destination port, and blocked port. These are selected based on elections.

The Root Bridge is the switch, which has lowest priority; if the priority is the same, then the switch with lowest MAC address will be the root bridge. Every switch has its default priority as 32,768 according to IEEE 802.1D (STP) standards, so the bridge with the lowest MAC is elected as the root bridge. This priority value chances with every VLAN is added; the priority number is incremented with VLAN number for every VLAN added. If we want any particular bridge to become Root Bridge, then change its priority to lower value than default; priority can be changed with multiples of 4096. We can manually change priority of a bridge (Cisco technology, 2010).

Syntax: To change priority value

SwitchA(config)#spanning-tree vlan 2 priority <priority value - multiples of 4096>

SwitchA(config)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#spanning-tree vlan 2 priority 4096
SwitchA(config)#end
SwitchA#
```

To force a switch to be root switch,

Syntax: To make a switch as primary root switch

SwitchA(config)#spanning-tree vlan <vlan no> root primary

Example (Seifert, 2000):

```
SwitchA(config)#spanning-tree vlan 2 root primary
SwitchA(config)#
```

Syntax: To make a switch as root secondary

SwitchA(config)#spanning-tree vlan <vlan no> root primary

Example (Seifert, 2000):

```
SwitchA(config)#spanning-tree vlan 2 root secondary
SwitchA(config)#
```

STP conducts elections for the Root Bridge, the root port, the designated port and the blocked ports. There are different criteria for electing the Root Bridge and different ports.

The Root Bridge is selected based on bridge ID (BID) that has lowest priority of bridge and MAC address. The Root port is the port that can reach the root bridge with lowest path cost. The Root Bridge does not have a root port. Except for Root Bridge, every other switch will find its root port. STP conducts elections between the ports and elects the designated port and blocked ports based on election priorities. The link which is pointing towards the Root Bridge is called upstream, which has root port, and the link which is facing in the other direction to the root bridge is downstream, which has either the blocking port or the blocked port. The cost of the link depends on the bandwidth; the cost of a link is inversely proportional to the bandwidth of the link. We will discuss all the processes in detail later. There are two kinds of ports in a switch: trunk and access ports. Trunk ports are used to connect to other switches, and access ports are used to connect user devices. Consider two switches are connected with two links as shown in figure 3.

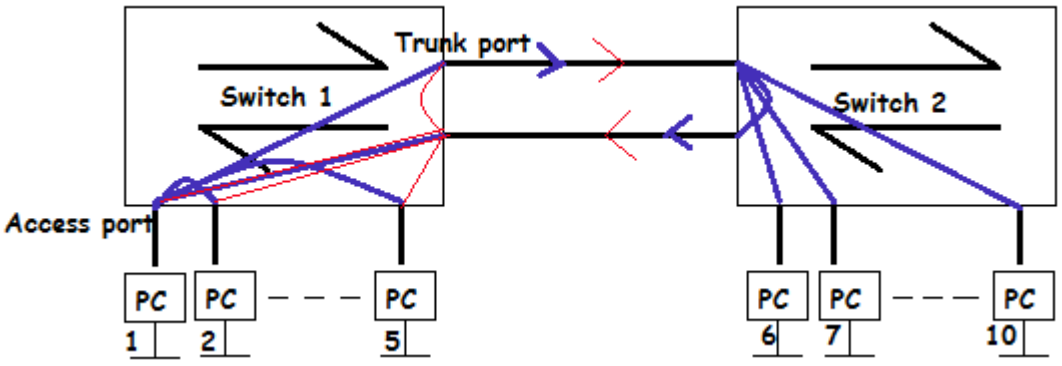


Figure 3: How loop formation occurs

Two switches are connected with two links and each switch is connected with a user device such as a PC (personal computer). All these pc's are in the same VLAN; if they are in different VLANs we need to enable inter VLAN routing to provide communication between them. An example of this would be, if PC1 wants to ping with any other PC, as like for example PC7.

Loop formation results in no data transmission in the network topology, and switches need to force restart the switch. To avoid this problem of loop formation STP (Spanning Tree Protocol) is introduced. STP IEEE standard is 802.1d. STP detects and breaks those loops. This protocol disables the redundant links by detecting them till they are needed. When the primary link goes down immediately a secondary link is activated. STP finds the loop free path for every destination.

2.4.1 BPDU (Bridge Port Data Unit)

When STP is enabled in the switch first it broadcasts BPDU (Bridge Port Data Unit) to every switch and with this BPDU every switch will know each other. BPDU has two types of BPDUs as configuration BPDU and TCN (Topology change Notification) BPDU. BPDUs are sending through downstream. Configuration BPDUs are sending during election, for every 2 seconds and also used to send information of timers. TCN BPDU are used when link failure, receives a TCN BPDU from its neighbor and thus that port state changes to learning. Switch ports are discussed in detail below.

A BPDU contains:

- Root BID: Bridge ID (BID) of Root Bridge.
- BID of Sender: Priority and MAC address of sender.
- Path cost of sender: Root cost.
- Port ID of Sender: Port number.
- Hello time: Default two seconds.
- Forward time: Default fifteen seconds.
- MAX Age: Default twenty seconds.

Root Bridge ID	Root Path Cost	Sender Bridge ID	Version	Port ID	Message Age	Maximum Age	Hello Age	Forward Delay Age

Figure 4: BPDU

2.4.2 Switch Port States

- Disable State: This is the state where any device is not connected.
- Listening State: Receives BPDU from other switches but don't learn about MAC address. Listening state timer is fifteen seconds.
- Learning State: Learns MAC address and build MAC table. Sends and receive BPDUs. Learning state timer is fifteen seconds.
- Forward State: This is the only state accepts frames. In this state switches start transmitting and receiving the frames (Cisco technology, 2010).
- Blocking State: Data cannot be received or transmitted in this state. Receives BPDU but don't learn MAC address. If the BPDU is not received within maximum age of 20 sec.

Spanning Tree link Costs:

Link cost is one of the important criteria in determining the best path to reach Root Bridge. Speed of the link is inversly proportional to cost of the link. These link costs are predetermined in STP. The IEEE standard 802.1D used two methods: short and long methods to calculate the path cost. Short path is the default method for path cost.

Short Method: The original IEEE 802.1D published in 1998, used 16 bit default values (as shown in table 1) of port cost that limited the range to fall in between 1- 65535.

Link Speed	Default cost of link
10Mb/sec (Ethernet)	100
100Mb/sec (Fast Ethernet)	19
1Gb/sec (Giga Ethernet)	4
10Gb/sec	2

Table 1: Spanning tree link costs

Long Method: The latest IEEE 802.1D published in 2004 uses a 32bit(long method) integer metric to calculate the STP path cost with a range to be in 1-200000000. Formula to calulate path cost is

Path Cost = (20,000,000,000) / (Link Speed in Kbps)

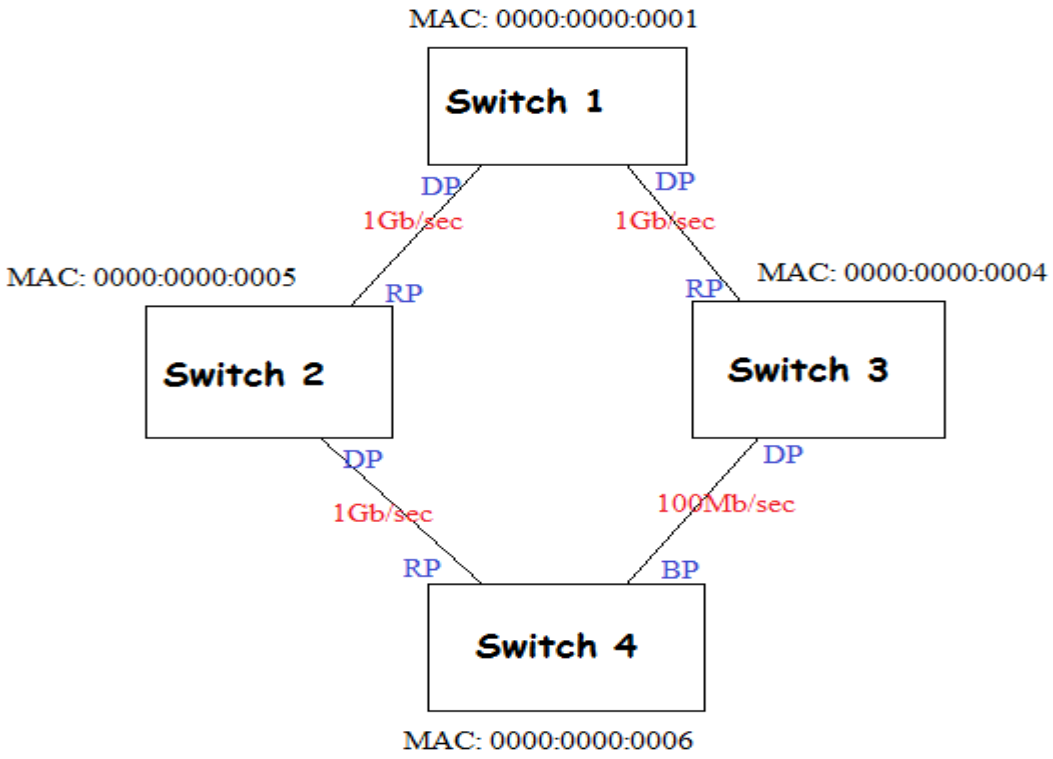


Figure 5: Explains Root Bridge and path cost

In the figure 7, switch 1 is elected as the Root Bridge based on the lowest MAC address, as every switch has a default priority. In this case, switch 4 has two paths to reach Root Bridge (switch 1) through switch2 and switch3. Thus, switch4 will elect one path as the root path and blocks the other path by calculating the path cost to reach the root bridge. For switch4 to reach switch1 through switch2, the path cost can be calculated as the addition of path costs of links between switch4 to switch2 and switch2 to switch1, i.e, 4+4= 8 (from the above table). The path cost from switch4 to reach switch1 through switch3 is an addition of the link cost between switch4 to switch3 and switch3 and switch1, i.e, 4+19=23 (from the above table). The path cost is less through switch2 to reach switch1 (root bridge); thus the port to reach switch2 from switch4 is elected as root port and the port connecting switch4 and switch3 is blocked.

The designated port is the port that is on the other side of the root port. In a link connecting two switch ports, if one port is root port, then STP makes other port the designated port. BPDUôs increases

path cost. When a BPDU is received by the switch, path cost value is increased by adding the port cost of sender (Cisco technology, 2010).

The switch will select its root bridge based on its neighbor IDs if the link path cost is same. The port priority of a switch by default is 128. If in any case, for a switch having two paths and the path costs and neighbor IDs are same, then port priority will help selecting root port; the port with lowest port priority is elected as root port.

Port priority can be changed,

Syntax:

SwitchA#config t

SwitchA(config)#interface fastethernet0/1

SwitchA(config-if)#spanning-tree vlan <vlan no> port-priority <port priority value - multiples of 16>

SwitchA(config-if)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#spanning-tree vlan 2 port-priority 16
SwitchA(config-if)#end
SwitchA#
%SYS-5-CONFIG_I: Configured from console by console
```

2.4.3 Timers

Timers are used to determine the interval for transmission of BPDU's, STP re-convergence and the interval for each port state.

Hello Timer: Time interval in which BPDU's are send to other ports connecting other switches. Default value of this timer is 2 sec, but can be changed from 1sec to 10sec.

Forward Delay Timer: This is the timer for both listening and learning states. Default value is 15 sec but can be changed from 4 sec to 30sec.

Max Age Timer: Maximum time taken for a switch to save the BPDU configuration information. Default value is 20sec, but can be changed from 6 sec to 40sec.

These timers can be changes:

Syntax: To change hello time

SwitchA#config t

SwitchA(config)# spanning-tree vlan <vlan no> hello-time <time in seconds>

SwitchA(config)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#spanning-tree vlan 2 hello-time 3
```

Syntax: To change forward delay timer

SwitchA#config t

SwitchA(config)# spanning-tree vlan <vlan no> forward-time <time in seconds>

SwitchA(config)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#spanning-tree vlan 2 forward-time 10
```

Syntax: To change Max Age time

SwitchA#config t

SwitchA(config)# spanning-tree vlan <vlan no>

SwitchA(config)#end

Example (Seifert, 2000):

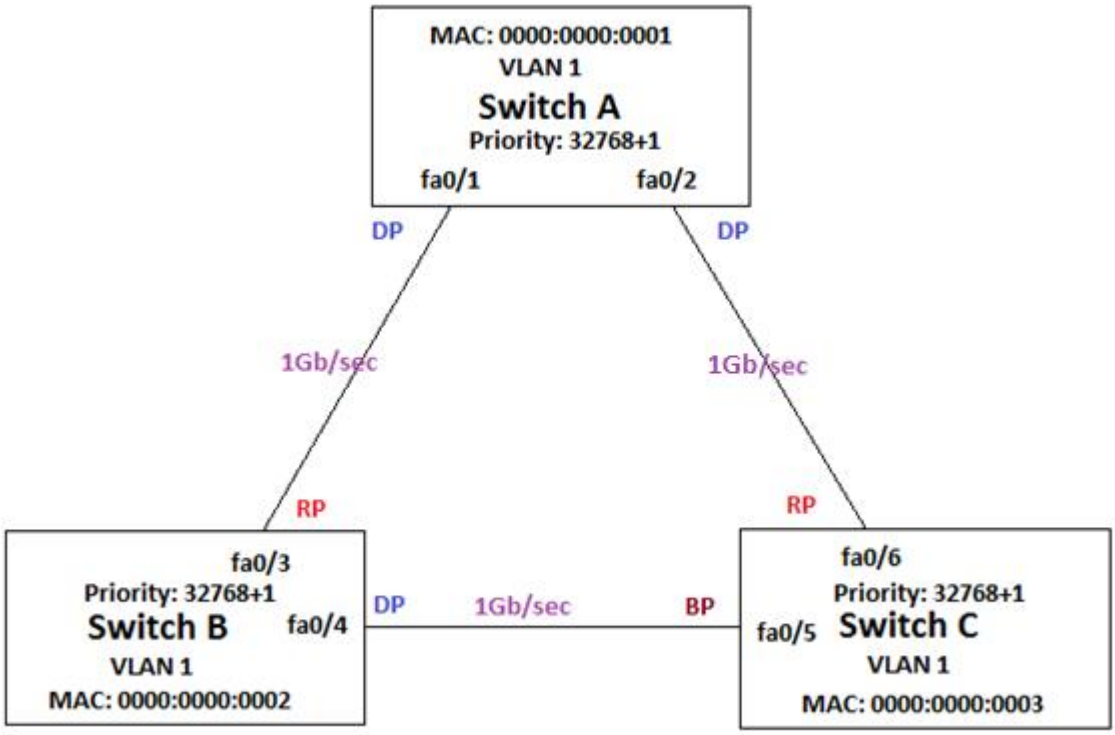
```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#spanning-tree vlan 2 max-age 10
```

CHAPTER 3: SPANNING TREE PROTOCOL (STP)

In any network topology, STP initially selects its root bridge based on the priority value; the switch having lowest priority will be the root bridge and if switches have same priority values then they go with the switch having the lowest MAC address. Then root ports are selected with the link path cost; the port with the link having the lowest path cost will be selected as the root port and other end of the link is selected as the designated port. If the links have same path cost, then port having the lowest priority is selected as the root port and the other port is blocked. In a switch only one port is the root port, but any number of ports can be designated ports.

With this process of electing root bridge and ports (root port, designated port and blocked port) STP creates a loop free network topology. BPDU plays a major role in selecting Root Bridge as it contains all the information about the particular switch, which mainly helps in conducting elections and selecting Root Bridge and ports. For every VLAN, STP can select a root bridge (Cisco technology, 2010).

In the figure 8, three switches are connected with each other. Switch A is the root switch because it has the lowest MAC address. Fast Ethernet ports fa0/3 and fa0/6 will be the root ports for switch B and switch C respectively, as they have lowest path cost to reach switch A, but they do have alternate paths to reach switch A. As both the ports have the same path cost, the switch compares port priority which is also same, so the switch selects the port with the lowest port number. Thus fa0/4 becomes the designated port and fa0/5 becomes the blocked port.



RP: Root port; DP: Designated port; BP: Blocked port.

Figure 6: Spanning Tree Protocol

Topology changes will be notified through TCN (Topology Change Notification) BPDUs. When a topology change is identified the switch sends notification to the root bridge and the root bridge sends it to every other switch in the network and then starts the STP process again.

Spanning Tree convergence time is more, as it includes blocking time of 20 seconds, listening time of 15 seconds and learning time of 15 seconds, a total of 50 seconds during which no traffic is transmitted or received. 50 seconds in today's modern world is too high; personal computers boots very faster and are not getting an IP address because of DHCP time outs. To decrease convergence time, portfast, BPDU guard, uplink fast, and backbone fast were introduced.

Portfast: When the portfast feature is enabled, listening and learning states in spanning tree are bypassed and port will be directly in forward state. But ports connected to user devices can only be in the portfast state (Cisco technology, 2010).

Syntax: Portfast

SwitchA(config)#interface fastethernet 0/1

SwitchA(config)#spanning-tree portfast

BPDU guard: BPDUs should never be received in portfast enabled ports, loops will occur if a switch is connected to portfast enabled port and receiving BPDUs. BPDU guard feature disables (Errdisable state) the port if BPDUs are received in portfast enabled ports.

Syntax:

SwitchA(config)#spanning-tree bpduguard enable/disable

Uplink fast: When designated port fails, the uplink fast feature enables the blocked port to go directly to forward state without the listening and the learning states. If this feature is enabled, the network will be recovered in five seconds instead of the 45 seconds with listening, learning and forwarding states. This feature should be enabled only in the access layer, not in the distribution layer switches because it prevents the switch from being a Root Bridge.

Syntax: For uplink fast

SwitchA(config)#spanning-tree uplinkfast

Backbone fast: When there is a link failure for the root bridge, until max age timeout (20 seconds) all the other the switches indirectly connected to the root bridge will believe that the link for root bridge is active and will ignore BPDUs from the other switch which is acting as the root bridge. After 20 seconds the indirectly connected switch will start accepting BPDU's and the spanning process of electing Root Bridge starts and elects a new root bridge. This process will take 50 seconds for the devices to transmit or receive data. If backbone fast detects the indirect link failure and sets the max age timeout to 0 seconds (zero seconds) waiting time is reduced and the port can go through normal spanning tree port states (Cisco technology, 2010).

If this feature is enabled, each and every device in the switch should be enabled with this feature.

Syntax: Backbone fast

SwitchA(config)#spanning-tree backbonefast

Spanning tree is enabled by default on switches, if you want to enable STP;

Syntax: Enable STP

SwitchA(config)#spanning-tree vlan <vlan no>

SwitchA(config)# end

Example:

```
SwitchA(config)#spanning-tree vlan 2
SwitchA(config)#end
SwitchA#
```

Syntax: Disable STP

SwitchA(config)#no spanning-tree vlan <vlan no>

SwitchA(config)# end

Example:

```
SwitchA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#no spanning-tree vlan 2
SwitchA(config)#end
SwitchA#
```

If a loop does occur after using STP, then we need to follow a sequence of steps to stop the loop

1) Looking at our topology diagram, we need to look at the link utilization rate of all the ports of the switches that are connected in our topology. This gives us the idea of which ports have very high link utilization rate from which we can have an idea on which all ports might be suspects for causing the loop.

2) From the list of ports with high link utilization rate, we need to shutdown one by one the ports and then observe if the loop has been stopped. Looking at the switch backplane utilization rate and identifying if it has been back to normal when compared to the rate before shutting down the port, can identify this port has caused the loop. If not we need to keep repeating this process, by shutting down one by one all the ports.

3) When the switch backplane utilization rate has been back to normal after shutting down a particular port, we need to mark that port and need to identify why that specific port has caused the issue.

4) Looking at our topology, around the culprit port we need to see if there are any redundant paths. If there are, then we need to look at the switches along that path. Identify if the switch has correct details regarding the discovery of STP root, if the port of the root has been learned correctly. Also check if the BPDUs are being received at regular intervals. These details will help us most of the times on the reason for the loop.

5) Finally once we identify the link or device with the issue, we need to detach this device from the network or in some cases, resolve the issue by taking actions like replacing the fiber, etc.; and then restoring the link back.

Metro Networks: Metro Ethernet networks basically connect branch offices (LAN) to Internet (service providers). In this large networks STP can be used to avoid loops in the network topology. But since the Metro networks are huge (connecting customer networks to service providers), whenever a link failure occurs STP re-convergence time is huge which delays the actual data transmissions in the network. To address this problem RSTP can be used. RSTP has alternate ports instead of blocked ports, which skips learning and listening states and directly takes the port to forwarding state. This reduces the re-convergence time taken on a link failure in the network. We will discuss RSTP in detail in future. Thus Metro Ethernet networks can reinitiate the traffic flow.

Another challenge in a Metro network for a service provider is to isolate one customer network from another based on each customerôs requirements. This resulted in service provider coming up with VLAN based service provision. Service providers use PVST to isolate its one customer network from another. PVST runs one instance per VLAN.

3.1 Security Vulnerabilities:

BPDU Unauthenticated: BPDUôs are not authenticated, which is the major disadvantage. BPDUôs contains who is the root bridge, what is the priority and MAC address of that Root Bridge. If a malicious switch enters the network and received an unauthenticated BPDU can see who is the Root Bridge and what is the Bridge ID (priority and MAC address) of Root Bridge. Thus the malicious switch can become the root bridge by reducing its priority lower that Root Bridge, which is security vulnerability. We can shut down all unused ports in the network manually, thus malicious user cannot enter the network without the knowledge of network administrator.

Denial of service: In this type of attack, the attacker switch sends BPDUôs with lowest possible Root bridge ID which results in attacker switch wining the election and becoming the Root bridge. After becoming the Root Bridge, he disappears from the network, which results in STP reelection after max age timer expires. Now attacker again reconnects and tries to participate into the election by resending BPDU with lowest possible bridge ID. This results in the attacker becoming the root bridge again. In this way, the attacker keeps repeating the process of becoming the root bridge and disappearing from the network, which results in the network STP elections (network flooded with BPDU messages all the time). This delays the ports being in forwarding state, resulting in the actual traffic never being sent across the network.

Man in the Middle attack: This is similar to DOS attack. In this attack, after receiving BPDU from Root Bridge, attacker reduces his priority and advertises himself as the Root Bridge with lowest Bridge ID, thus results in STP elections. As the attacker has lost bridge ID, he will win the election and become the Root Bridge. As every communication has to go through Root Bridge, attacker can see the data and modify. This needs to be addressed in STP.

CHAPTER 4: SPANNING TREE PROTOCOL (STP) - EVOLUTIONS AND EXTENSIONS

4.1 Per-VLAN Spanning Tree (PVST)

This is Cisco proprietary protocol. CST - Common spanning tree protocol has a single instance STP for a complete switch. This causes delay in sending BPDUs. To solve this, PVST (Per-VLAN STP) was introduced. The type of a single instance Spanning Tree Protocol (STP) is known as Common Spanning Tree (CST) (Cisco technology, 2010). A delay in receiving BPDUs is common in large switched Common Spanning Tree (CST) networks. The delay in receiving BPDUs can cause problems such as convergence time problems. Per-VLAN Spanning Tree (PVST) is a solution for these problems. Per-VLAN Spanning Tree (PVST) is a Cisco proprietary Spanning Tree Protocol (STP), which operates a separate instance of Spanning Tree Protocol (STP) for each individual VLAN. A separate instance of Spanning Tree Protocol (STP) for each VLAN helps VLAN to be configured independently and also to perform better. Per-VLAN Spanning Tree (PVST) requires Inter-Switch Link (ISL).

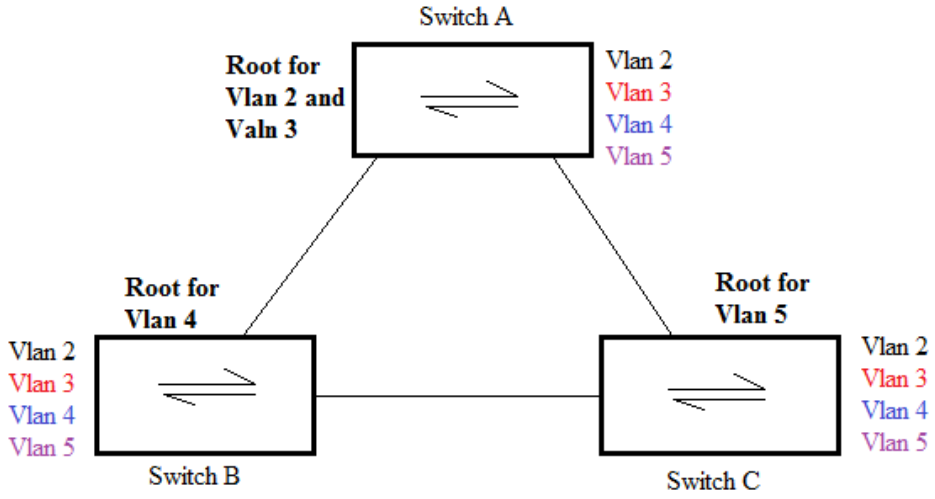


Figure 7: PVST - Per VLAN STP

4.2 Rapid Spanning Tree (RSTP)

This is IEEE 802.1w standard. If a switch port is connected with a user device like a computer, the user device cannot form loops and so we can skip listening and learning time (30sec). In the spanning tree port, user devices like personal computers will boot fast than the time taken for the ports to pass all spanning tree states, which may lead to DHCP timeout. DHCP gives an IP address for the devices dynamically; time outs result in no IP address for the user device. Thirty (30) seconds is the time taken for both listening and learning states; we can skip these two states with RSTP. No data is transmitted or received till the port reaches forwarding state. This is the problem with STP. RSTP helps to skip states and changes the port to forward state if the port is connected to a user device. RSTP changes the port blocking state into forward state in minimum time, thus the convergence time is reduced and communication time will never change with STP/RSTP.

RSTP takes a few seconds to change blocking state to forwarding state of a port. RSTP changes its port's states to discarding, learning and forwarding states. Discarding state is the state, which has disabled, blocking and listening states in STP.

RSTP has alternate ports and backup ports. Alternate port is the port which is blocked in STP; and the alternative port will be up in few second and the port will be in forwarding state in RSTP rather than the ports going through listening, learning and forward state in STP. A port will be in blocking state if there are two links to reach a switch. Then one link will be designated and the other will be backup port. Backbone fast and uplink fast are enabled by default in RSTP; portfast need to be enabled if needed (Cisco technology, 2010).

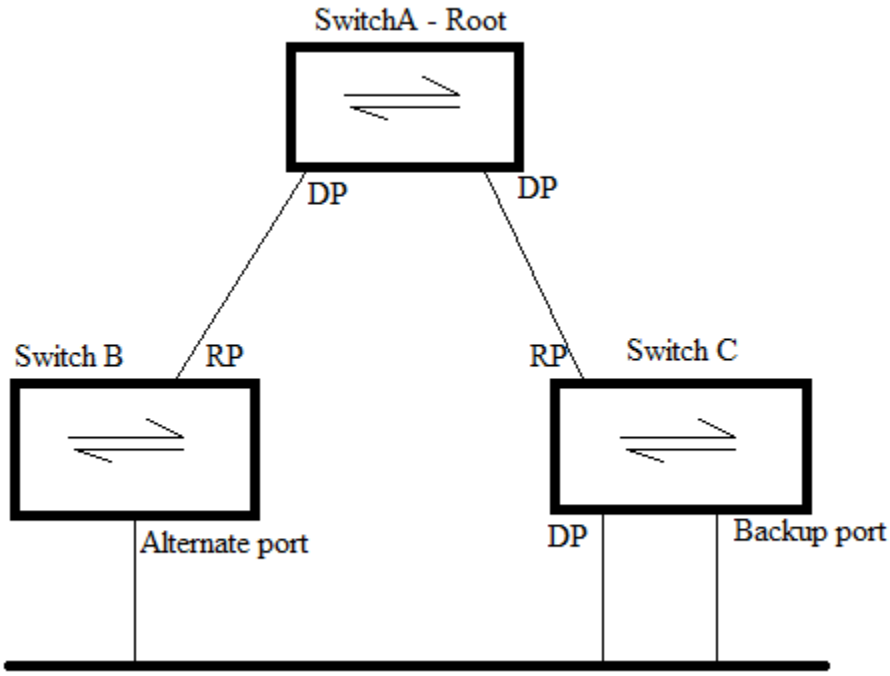


Figure 8: Alternate port and Backup port

4.3 Multi Spanning Tree Protocol (MSTP)

This is IEEE 802.1s standard. To decrease the number of instances in PVST, MSTP is introduced. VLANs with the same type of configurations are grouped as a single instance. Those VLANs are grouped for load balancing. MSTP has MST region, which has the switches with same configuration attributes. To be in a MST region switches need an alphanumeric configuration name with a maximum of 32 characters. This configuration name must be unique. MSTP has a configuration revision number of length 2 bytes

and these values start from 0 to 65535. To be in the part of MSTP, VLAN's need individual VLAN ID and range of VLAN ID's. If any switch has different configuration settings, then that will not be in the MST region.

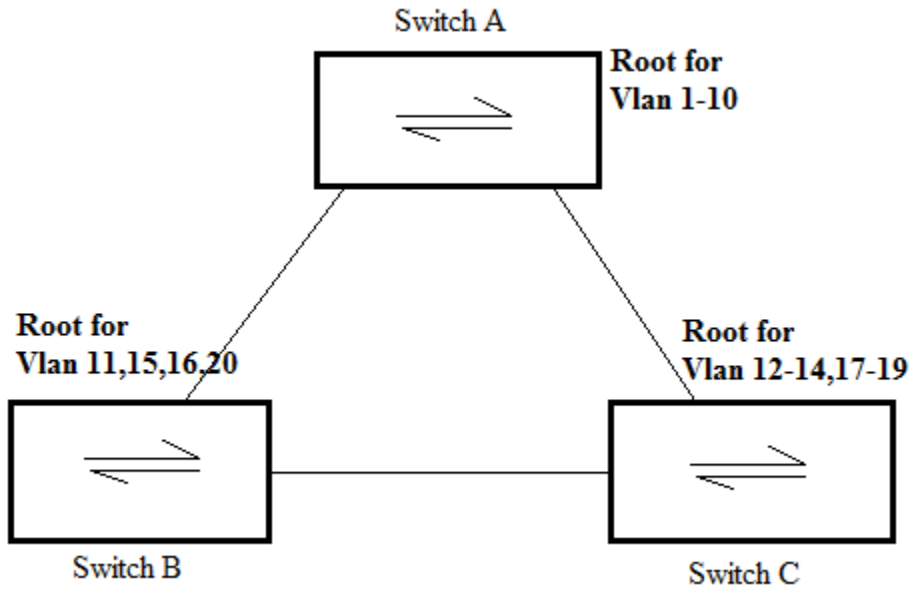


Figure 9: MSTP - Multi Spanning Tree Protocol

MSTP is fully compatible with RSTP bridges, in that an MSTP BPDU can be interpreted by an RSTP bridge as an RSTP BPDU. This not only allows compatibility with RSTP bridges without configuration changes, but also makes the RSTP bridges outside of an MSTP region to see the region as a single RSTP bridge, regardless of the number of MSTP bridges inside the region itself. To further facilitate this view of an MST region as a single RSTP bridge, the MSTP protocol uses a variable known as hops as a time-to-live instead of the message age timer used by RSTP. The message age time is increased only once a split tree information enters an MST region, and therefore the RSTP bridges will see a region just a "jump" in the spanning tree. Ports on the edge of an MST region connected to either one STP or an RSTP bridge or an end point are known as boundary ports. As in RSTP, these ports can be configured as edge ports to facilitate the rapid changes in the delivery status when connected to endpoints.

CHAPTER 5: LITERATURE REVIEWS

5.1 Literature Review 1

Improving Network Infrastructure Security by Partitioning Networks Running Spanning Tree Protocol:

This paper ñImproving Network Infrastructure Security by Partitioning Networks Running Spanning Tree Protocolò is written by K. H. Yeung, F. Yan and T.C. Leung. This paper was published in Los Alamitos, CA; by IEEE Computer Society in August, 2006. The authors explained the security issues in STP and a solution to protect the STP network from security attacks.

This paper explains a solution for security problems in STP (Spanning Tree Protocol). The drawbacks of STP running switches are, they transmit BPDU (Bridge Protocol Data Units) messages, which are not authenticated, STP convergence is slow, the role of root is not properly defined and the mechanism is complex. Thus, with all these drawbacks, STP running switches can be easily attacked (Cisco technology, 2010).

The solution is to partition the network into tiers, such as higher tier (STP network infrastructure) and lower tier (connected to user devices) switching networks to hide STP operations from the lower tier network. To implement this partition, a special type of boundary switches are needed such as Ethernet boundary switches, which have additional functions in addition to the normal switch has. The boundary

switch creates a partition between the higher tier switching network and lower tier switching network to prevent attacks on STP network.

Cisco invented ROOT guard (for Root role attack); LOOP guard (for infrastructural attacks) and BPDU guard (stops BPDU messages); all are techniques to protect the STP network from security attacks. But these BPDU guards do not add other new switches to the network port, which is BPDU guard enabled and is not acceptable for design of STP. Thus a new technique of partitioning STP network is obtained, which stops security attackers from affecting the higher tier with lower tier STP networks.

Network is divided into NI (Network Infrastructure) and NNI (Non-Network Infrastructure) networks. Both run STP and enable adding new devices in both networks. Boundary switches cooperate between NI and NNI devices and prevent loops and they make STP details of NI not available to NNI networks. Boundary switches use Loop guard technique.

With this partitioning of STP network we can protect the network from security attacks such as flooding TCN (Topology change notification) BPDUs, role claiming internal node, etc. This partition technique launches boundary switches and tiers to protect the STP network from security attacks. Boundary switches protect the network infrastructure (higher tier) from lower tier network attacks (Cisco technology, 2010).

This paper mainly discusses the security problems in STP and solutions to those security issues with no limitations, as new switches cannot be added in solutions like BPDU guard, Root guard and Loop guard.

This project completely explains how about STP working, and problems and solutions. General solutions to security in STP have some limitations, but this paper explains about how to overcome those limitations with the proposed solutions to security attacks.

5.2 Literature Review 2

An Approach to select the Best Spanning Tree in Metro Ethernet Networks:

This paper ñAn Approach to select the Best Spanning Tree in Metro Ethernet Networksò, is written by Ghasem Mirjality, Mohammad Hadi Karimi, Fazlollah Adibnia and Shahram Rajai. This paper was published in Los Alamitos, California; IEEE Computer Soc in July, 2008.

The authors explained a different way to select STP (Spanning Tree Protocol) in a Metro network, which is more effective as metro Ethernet has different requirements compared to LANs. This does not replace STP but is as STP complement.

The authors explained that Metro Ethernet LAN need functionalities of traffic engineering, admission control and better QOS (Quality of service). Load balancing is the task performed by traffic engineering. IEEE STP ensures a loop free network with reducing the network topology and provides a unique path from one node to any other node in the network. This results in no load balancing and very slow recovery if network fails.

RSTP came into existence to overcome the problem of slow recovery but RSTP lacks in load balancing. In metro Ethernet networks, this leads to inefficient use of expensive links. MSTP addressed this problem by creating a spanning tree instance for every virtual group of LANS. This resulted in high overhead and incompatibility. To overcome these problems, STP is selected based on load balancing along with switch ID and link cost. The author's approach is to force STP to assign values properly to link cost and switch IDs while STP is running. In this case if there is failure in the network, an alternate STP is selected based on ranks to changed link costs.

Through this paper, the authors introduced a theoretical approach to find the best STP with ranking among all the possible STPs based on link and switch load balancing and the shortest path in a Metro network. There are three criterions: as shortest path, link load balancing and switch load balancing. Based on the goal of the Metro Ethernet network, the weight of each criterion is calculated. This approach is to force STP based on link cost assigned values (Cisco technology, 2010).

As the project is on STP, performance of STP is also an important constraint. This paper explained performance issues of STP in Metro Ethernet networks even with improvisation of STP such as RSTP and MSTP, and explained an efficient way to select the best STP in Metro networks, which will give a better performance of STP.

5.3 Literature Review 3

Performance of Rapid Spanning Tree Protocol in Access and Metro Networks

This paper, ñPerformance of Rapid Spanning Tree Protocol in Access and Metro Networksò, is written by Richard Pallos, Janos Farkas, Istvan Moldovan, Csaba Lukavszki. This paper was published in August 2007. The authors explained performance in fast recovery, hardware delay and processing time of RSTP in real environment for small and large (Metropolitan) network topologies.

Ethernet is a widely used technology in metro and aggregation networks as they are simple, have high capacity and are not costly. LANs (Local Area Networks) uses Ethernet switches for easy maintenance and operation and also fast data transfer, but in metro and access networks traffic protection is also a very important criterion. Access networks are used mainly for connecting networks of customers with the Internet. Today access networks have increased greatly because of user demand, thus reliability of the network has become a problem, which cannot be solved with Ethernet technology (Cisco technology, 2010).

STP (Spanning Tree Protocol) is an extension to the Ethernet technology, which provides loop free topologies and redundancy in network topologies. But STP cannot handle the problem of failures in the network efficiently. To improve this RSTP (Rapid Spanning Tree Protocol) was developed with low convergence time. The tasks of RSTP are loop free topology, fast re-convergence time, MAC address learning control and FDB (Filtering Database) control. FDB has the information about MAC address port mapping in accordance with RSTP topology. Through this paper, the authors answered the question as to whether RSTP can provide a fast recovery of a network for sensitive traffic.

RSTP has fast re-convergence time, ten milliseconds compared to seconds for traditional STP. Re-convergence time is fast but RSPT has hardware delays, FDS and port manipulation delays and the time taken for learning the MAC address, which makes its operations slow. These delays increase the convergence of the network. The authors used a time model, which can be used for measurement of RSTP performance in bridges. The authors mentioned that this proposed model can overcome the problem of inaccuracy in general RSTP simulators, the applicability of which are limited by obtaining accurate simulators. They stated a conclusion that recovery is directly proportional to the processing time of BPDU and ring size (Cisco technology, 2010).

This project include RSTP, thus the performance of RSTP can be compared and calculated, as this paper explains the performance of RSTP compared to Ethernet which limits the applicability. This paper also proposed an accurate RSTP simulator to calculate the re-convergence and performance with which the applicability can be improved in Metro networks.

5.4 Literature Review 4

Traffic Engineering for Multiple Spanning Tree Protocol in Large data centers:

This paper, ñTraffic Engineering for Multiple Spanning Tree Protocol in Large data centersò is written by HO Trong Viet, Yves Deville, Olivier Bonaventure and Pierre Francois. 23rd International Teletraffic Congress (ITC) published this paper in 2011. The authors explained an optimization scheme, which works more efficiently on data centers than using STP (Spanning Tree Protocol) for transmission of data.

The capacity of data center increases widely as they play a key role for the Internet. Their size and the number of servers increase quickly. Data centers are mainly used for computation or for the Internet services; along with this they support many applications simultaneously. These data centers are constructed with Ethernet switch networks that use STP. But STP is not efficient in case of switch/network failure, thus RSTP is used for fast convergence of an alternate tree.

STP blocks the links that are not selected in a spanning tree. Data centers are divided into many VLANs; the idea behind VLANs is isolation between users. Servers can communicate only if they are in the same VLAN. MSTP (Multiple Spanning Tree Protocol) is an extension of STP that supports many spanning trees in a single topology. With MSTP, VLANs can spread over different switches and links in different spanning trees. MSTP uses are links than STP and can compute only between 16 STPs and VLANs in those STPs; thus, MSTP is not efficient in managing traffic in data centers, which have many switches and spanning trees. This is a drawback for managing the traffic in a network topology (Cisco technology, 2010).

The authors solved combinatorial problems using Constraint-Based Local Search (CSLS) and Constraint Programming (CP). They used a language, COMET, which is an innovative object oriented language that controls CP and CBLS abstraction. The authors used Local Search algorithm to select spanning tree sets based on the traffic demand in MSTP. They explained the algorithm and how it showed good results in solving the problem of traffic engineering in large network topologies.

In this paper, authors explained an algorithm that can be used in MSTP for selecting the spanning trees based on the traffic requirements. This algorithm works more efficiently in metropolitan networks or data centers for traffic engineering and load balancing in the bandwidth available, compared with using only MSTP for the network topology.

This paper explained the problems in MSTP in a data center or Metropolitan network with an algorithm, which solves traffic-engineering problems in large network topologies. The project is to explain STP and the extensions of STP.

CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

Spanning Tree Protocol (STP) is a network protocol that operates on the data link layer of the OSI model. There are two versions of the protocol that are not compatible with each other, the original version standard by the IEEE, and the second which is the one commonly used (RSTP) today. This protocol is transparent to the host user, and provides an optimal communication channel between hosts on a network.

STP uses the spanning tree algorithm to configure the switch ports to form hierarchical network topology that prevents the formation of loops, which arise due to the existence of redundant links. STP links automatically activate certain interfaces and block redundant physical paths to ensure a single logical path in any configuration of bridges; this ensures a loop-free topology. A port is considered blocked when network traffic cannot get in or out.

In a hierarchical design, redundancy is achieved by distributing applications and network devices through additional and redundant hardware. Multiple alternative routes between network devices are generated, so when the interruption or failure occurs, there is no loss of connectivity as there is another link to support the traffic reservation and data transmission.

The spanning tree algorithm designates one switch as the root bridge, and uses it as a reference point in all calculations to determine redundant paths to be blocked, either in a switched LAN or in a

broadcast domain. The maximum spanning tree is five minutes this remains valid until there is a topology change, which is detected automatically by the protocol when it occurs.

When such a change occurs, the current root bridge redefines the spanning tree topology or chooses a new root bridge. The bridges are interconnected via configuration messages called BPDUs (Bridge Protocol Data Unit).

The protocol sets identifiers (ID) of the Bridge, and select the person with the highest priority (smallest number) as root. The root bridge sets the shortest path (the path of least cost) for the entire network; each port has a configurable parameter called Span Path Cost.

In STP, designated bridges are the bridges that are in the path of lowest cost and are chosen from all the bridges that connect one network segment to transmit frames to the root, if there are two bridges with the same cost, the selection criterion is defined according to the lower MAC address. The port on the designated bridge that connects a segment is called the designated port and offers the lowest cost path to the root port. All other ports and routes are blocked in a steady state. If the STP configuration changes or redundant network segment becomes unreachable, the algorithm reconfigures the links and restores connectivity, activating a reserved link. If the protocol fails, it is possible that two connections are active simultaneously, which could make a loop of traffic on the LAN.

Any provision of bridges can be configured with a tree topology through any of the four versions STP: the classic described by IEEE 802.1d reviewed previously, fast RSTP (IEEE 802.1w RSTP), Multiple STP (MSTP 802.1s) and VLAN STP (VSTP).

In MSTP, a network is divided into segments connected by several bridges; the protocol blocks some bridges to prevent a message from being left hanging in the network.

RSTP maintains much of the terminology and most STP parameters are unchanged. It uses the same BPDU format except that the version field is set to 2 to indicate that RSTP. This protocol manages redundant links, significantly reducing the time of convergence of the network topology when there are any changes or after a failure or during recovery from a switch port or link. In other words, it detects and uses network topologies that provide faster convergence of the spanning tree without creating forwarding

loops. Active RSTP can confirm that a port can undergo a safe transition to sending state without relying on any timer settings.

Therefore, it is important create an awareness of how important it is to apply security to local area networks. Allowing the implementation of STP and RSTP creates security policies in which all network users involved.

Future study can be done in detail about evolutions(PVST, RSTP and MSTP) of STP and proposals can be made to overcome the disadvantages of STP. Can also study in details about security vulnerabilities.

REFERENCES

1. RFC 4318 http://tools.ietf.org/pdf/rfc4318.pdf
2. Antonova, G.S., "Spanning Tree Protocol Interoperability with Other Loop Prevention Algorithms," Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on , vol., no., pp.1098,1101, 22-26 April 2007 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4232939&isnumber=4232659
3. Business Editors/High-Tech Writers NetWorld+Interop 2003,Las Vegas. (2003, May 19). FutureSoft demonstrates spanning tree protocol enhancements -- RSTP & MSTP -- in its intelligent switch solution at Networld+Interop, Las Vegas 2003.*Business Wire*.
4. Cisco technology assigned patent for multiple instance spanning tree protocol. (2012, Apr 29). *Targeted News Service*.
5. Cisco technology, inc. files patent application for a spanning-tree protocol for wireless networks. (2010, Aug 05). *Indian Patents News*.
6. Cisco technology, inc.; patent issued for system and method for running a multiple spanning tree protocol with a very large number of domains. (2013). *Journal of Engineering,* , 9994.

7. He Peng; Pan Heng; Li Xiangdong; Zheng Qiusheng, "Physical topology discovery based on spanning tree protocol," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.14, no., pp.V14-308,V14-311, 22-24 Oct. 2010 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5622296&isnumber=5622109
8. Hirschmann automation and control GmbH; patent issued for parallel operation of RSTP (rapid spanning tree protocol) and MRP (media redundancy protocol) and Segmentation/Coupling. (2014). *Journal of Engineering,* , 9745.
9. Marchese, M.; Mongelli, M.; Portomauro, G., "Simple Protocol Enhancements of Rapid Spanning Tree Protocol over Ring Topologies," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , vol., no., pp.1,5, 6-10 Dec. 2010 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5683943&isnumber=5683069
10. Pallos, R.; Farkas, J.; Moldovan, I.; Lukovszki, C., "Performance of rapid spanning tree protocol in access and metro networks," Access Networks & Workshops, 2007. AccessNets '07. Second International Conference on , vol., no., pp.1,8, 22-24 Aug. 2007 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4447112&isnumber=4447087
11. Syed Muhammad Atif; RRSTP: A Spanning Tree Protocol for Obviating Count-to-Infinity from Switched Ethernet Networks 2011 URL: http://www.cscjournals.org/manuscript/Journals/IJCN/volume3/Issue1/IJCN-133.pdf
12. K, H, Yeung; F, Yan ; T,C, Leung.,; "Improving Network Infrastructure Security by Partitioning Networks Running Spanning Tree Protocol," IEEE Computer Society in August, 2006 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1690403
13. Ghasem, Mirjality; Mohammad, Hadi, Karimi; Fazlollah, Adibnia; Shahram, Rajai,; " An Approach to the select the Best Spanning Tree in Metro Ethernet Networks," IEEE Computer Soc in July, 2008 URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4594749&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4586225%2F4594630%2F04594749.pdf%3Farnumber%3D4594749

14. H, O, Trong, Viet; Yves, Deville; Olivier, Bonaventure, Pierre, Francois,; ñTraffic Engineering for Multiple Spanning Tree Protocol in Large data centersò 23rd International Teletraffic Congress (ITC) in 2011URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6038460&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6038460
15. NA,; IEEE standard for Local and metropolitan area networks Media Access Control (MAC) Bridgesò IEEE 3 Park Avenue, New York in June 2004 URL: http://standards.ieee.org/getieee802/download/802.1D-2004.pdf
16. NA,; Troubleshooting STP on Catalyst Switch Running Cisco IOS System Softwareò Cisco in 2005 URL: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/28943-170.html#troubleshoot
17. NA,; ñConfiguring Spanning Treeò URL: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/spantree.html
18. Eric, Vyncke,; Christopher, Paggen,; ñ Attacking the Spanning Tree Protocolò Cisco Press in 2008 URL: http://www.ciscopress.com/articles/article.asp?p=1016582&seqNum=2

APPENDICES

Appendix A

Syntax: To create a VLAN

switch>enable

switch#config t

switch(config)#vlan <*vlan number*>

switch(config)#name <*vlan name*>

switch(config)#end (Seifert, 2000)

Example (Seifert, 2000):

```
SwitchA#enable
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 2
SwitchA(config-vlan)#name RED
SwitchA(config-vlan)#end
SwitchA#
```

Syntax: Assigning ports to VLAN

switch#config t

switch(config)#Interface fastethernet0/1

switch(config-if)#switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface fastethernet0/1
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 2
SwitchA(config-if)#end
SwitchA#
```

Even if we did not create VLAN 2 in the above example switch will creates VLAN 2 without name when we gave the command "switchport access vlan 2".

VLAN's should have IP addresses to enable inter VLAN routing.

Syntax: Assigning IP address VLAN

switch#config t

switch(config)#Interface vlan 2

switch(config-if)#ip address <ipaddress> <subnet mask>

switch(config-if)#end

Example (Seifert, 2000):

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#int vlan 2
SwitchA(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

SwitchA(config-if)#ip address 192.168.10.3 255.255.255.0
SwitchA(config-if)#end
SwitchA#
```

Syntax: Enabling inter VLAN routing

switch#config t

switch(config)#ip routing

switch(config)#interface fastethernet 0/5

switch(config-if)#no switchport

switch(config-if)#ip add <IP address> <subnet mask>

switch(config-if)#no shutdown

switch(config-if)#exit

switch(config)#ip route 0.0.0.0 0.0.0.0 <next hop IP address>

switch(config)#end

Example:

```
SwitchA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip routing
SwitchA(config)#interface fastethernet 0/5
SwitchA(config-if)#ip address 172.16.1.1 255.255.255.0
SwitchA(config-if)#no shutdown

SwitchA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

SwitchA(config-if)#exit
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
SwitchA(config)#end
SwitchA#
```

VLAN configuration procedure

To configure a VLAN, you must enter the VLAN configuration method (S1 (config-vlan) #)from the global configuration mode (S 1 (config) #) using the "vlan" command, followed by the number the vilan we want to configure and assign the name to the vlan we are setting use the "name" command followed by the name you want to assign to that VLAN. To assign the VLAN to one or more ports must enter configuration mode interface (S1 (config-if) #) using the "interface" command followed by the corresponding interface e.g. "FastEthernet 0/1". Then using the "switchport mode access" command declare the port to access mode and using the "switchport access vlan" command followed by the number of the VLAN you want to assign for example: "10".

Note: To configure more than one interface at the same time, we just enter the setup mode several interfaces with the "interface range" command followed by the type of interface you want to

configure "Fast Ethernet" for example, then the range or numbers of ports separated by a comma "," if they are not in sequence e.g. "fastethernet 0/1, fastethernet 0/3"or separated by a hyphen "-" if you are a range in sequence, e.g. "0/1 - 5 ".