Performance Analysis of a Spanning Tree Protocol

Harsha Nataraian. Karthik Ram.. Abhishek Challa

Abstract

This paper mainly focuses on the design of STP, packet analysis of STP and the different scenarios of STP deployment and working. Spanning tree protocols is used basically to avoid loops in Local Area Networks; a loop in networks can get the entire network down. In order to prevent these loops we use the spanning tree protocol. The 802.1D spanning tree protocol was designed at a time when the quick recovery of connectivity after a network outage was considered as crucial.

I Introduction

The increased deployment of the Layer 2 switches in almost all network designs used today has made the Spanning Tree Protocol to be a very reliable protocol to the network managers. Spanning tree protocol is an 802.1d IEEE standard which creates redundant links between source and the destination so that loops are not created in a network, as loops in a network would create broadcast storms and cause a network outage.

II IEEE 802.1D

The 802.1D Spanning tree protocol is a layer 2 protocol which runs on bridges and switches which are 802.1D compliant. The main purpose of this protocol is to ensure that the loops are not created in a network in presence of redundant paths in a network. STP is mainly used to create redundant links in a network which acts as a backup in case of network failure, so that if there a break in the primary link then the redundant links comes into picture thereby preventing the network outage. In the absence of STP in switches and bridges, such a failure results in loops. There are different flavors of STP's that can be configured in switches.

- Common Spanning Tree (CST) – where in a single Spanning Tree Process is used for all VLAN's.
- Per-VLAN Spanning Tree (PVST) – In this case there is a separate STP process for each VLAN. This is a Cisco proprietary.
- Per-VLAN Spanning Tree Plus (PVST+) – This is the next version of PVST, which allows switches configured with different flavors of STP to interoperate.

Process –

STP performs the following steps to maintain a loop free topology.

- Root bridge election- this serves as the centralized point of the topology.
- Identification of the root ports – these are the ports on the switches that has the lowest path cost to the elected root bridge.
- Identification of the designated ports- if there is a loop a port is put to a blocked state, which is activated again once the loop is removed.

STP Port States-

There are different states in a Spanning Tree Protocol which is explained in the table 1

States	*working*
Blocking	Default state of STP port i.e whenever a switch is turned on or when a port is closed to avoid a loop.
Listening	When there is no loop the port will not be closed, this is when the port continues to move to the listening state from the blocking state.
Learning	A port will be selected as a root port or designated port which listens for BPDU's and fetches the MAC address.
Forwarding	Here Ports can send and receive all data frames and continue to build MAC address table
Disabled	A port in disabled state will not take part in the STP process and will not forward any frames.

Below are some of the STP configurations that can be performed.

To check the current state of the port

Switch1# show spanning-tree interface fa0/10

To disable the STP for a specific VLAN

Switch1(config)# no spanning-tree vlan 10

To get the switch to work as root bridge

Switch1(config)# spanning-tree vlan 10 root primary

To adjust the bridge priority of the switch from a default value to increase its chance to get elected as root bridge

Switch1(config)# spanning tree vlan10 priority 150

The main idea of the spanning tree is for the bridges to select the ports over which they will forward the frames . The algorithm selects the ports as follows, Each bridge has a unique identifier, lets say b1, b2, b3. The algorithm first elects the bridge with the smallest id as the root of the spanning tree, this root bridge always forwards frames out all over its ports. Next each bridge computes the shortest path to the root and notes which of its ports are on this ports. This port is also selected as the bridge's preferred path to the root. Finally, all the bridges connected to a given LAN elect a single designated bridge that will be responsible for forwarding frames towards the root bridge. Each LAN's designated bridge is the one that is closest to the root, and if two or more bridges are equally close to the root, then the bridge's identifiers are used to break ties; the smallest id wins. Of course, each bridge is connected to more than one LAN, so it participates in the election of a designated bridge for each LAN it is connected to. In effect, this means that each bridge decides if it is the designated bridge relative to each of its ports. The bridge forwards frames over those ports for which it is the designated bridge.

III. Simulation using Cisco Packet Tracer

Cisco packet tracer is a powerful network simulator developed by Cisco systems. The version that is used here is 5.3.2 which supports an array of application layer protocols and routing with some of the protocols such as RIP, STP, OSPF, EIGRP and many other.

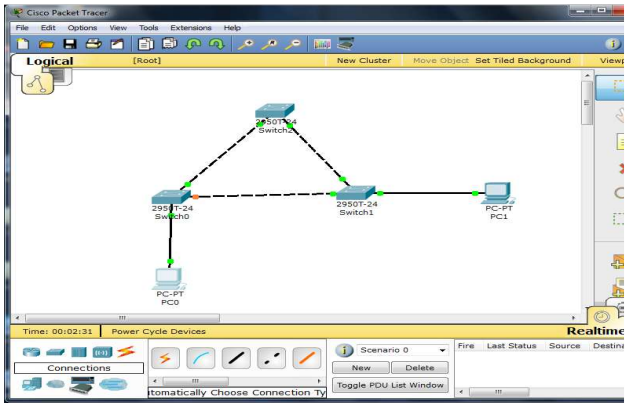

Figure: 1

Figure 1 shows the scenario we have used that is 3 switches and two PC's in simulating the basic functionality of the Spanning Tree Protocol. The network topology has been implemented using Packet Tracer to learn the different stages of the Spanning tree protocol and the time it takes to converge when there is any change in the network topology.

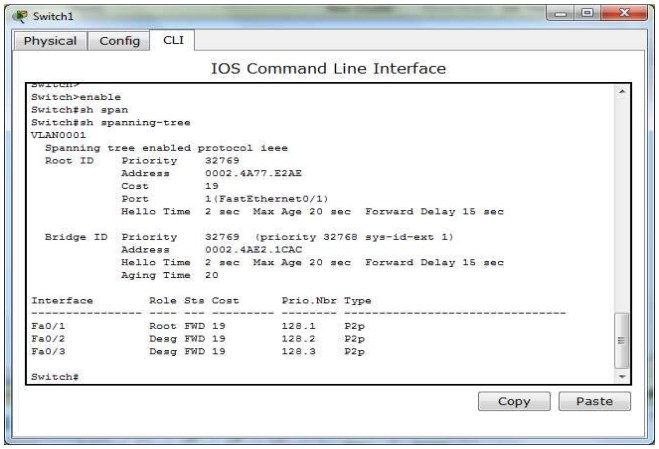

Figure: 2

As shown in the figure 2 we can see the configurations of the Switch 1, and the different modes of the ports of the switch which are Root and Designated, we can also see from the output that all the ports are in forwarding. Switch 1 is not elected as the root bridge as it is connected to the root bridge.

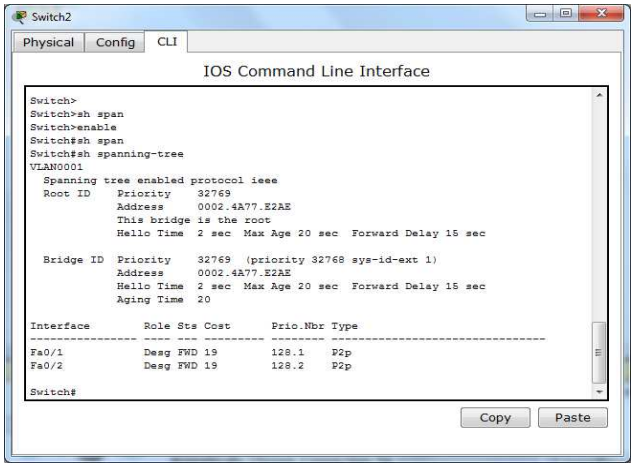

Figure: 3

These are the configurations that were simulated on packet tracer for Switch 2, from the figure 3 we can see that Switch 2 is elected as the Root Bridge. And its ports are the designated ports and the states of the ports are forwarding.

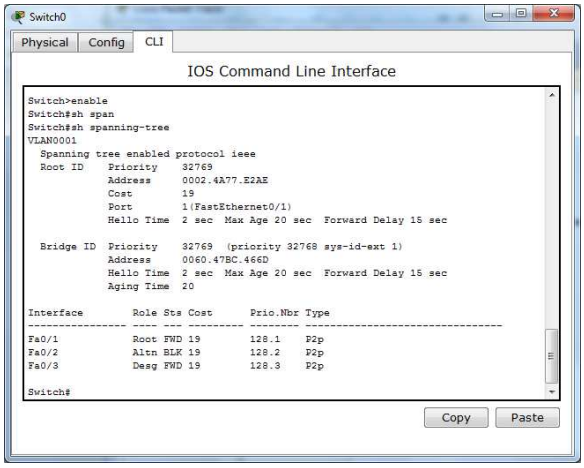

Figure: 4

The running configuration of Switch0 for the network topology is shown in fig 4, we can observe from the output of Switch0 that its interface Fa0/2 is in Blocking state, interface fa0/1 is directly connected to the root bridge that is Switch 2 and hence it is called as the root port and is in forwarding state and finally interface Fa0/3 is connected the host PC0 which has an ip address of 10.1.1.5.

Currently the path taken by the packets to reach PC1 at 10.1.1.10 is via the fa0/1 on Switch0.

Now to calculate the time taken for STP to converge if there are any topology changes, we have shut down the interface Fa0/2 on Switch 2 which is the root-bridge and simultaneously sent icmp packets from 10.1.1.5 to 10.1.1.10, during this observation we tried clocking the time for STP to recalculate and for the network to converge and find an alternate path for the icmp packets to traverse was found to be around 54.032 seconds.

IV. Conclusion

In this simulation we discussed about the basic functionality of the Spanning Tree Protocol. We studied the functionality of the different switches that has been used in the topology. By simulating different scenarios using the Cisco packet tracer we were able to study the different stages of the STP through which we were able to study the different ports and the way those ports went through the different states. Finally we were able to analyze the time taken by the Spanning Tree Protocol to converge whenever there was a change in the network topology. In order to see the converging time we tried pinging from one PC to another thereby sending ICMP packets. Finally our experiment results show how a spanning tree protocol could be used to avoid loops in a network using redundant paths.

V. References

1. http://www.routeralley.com/ra/docs/stp.pdf

2.http://www.orbit-computer-solutions.com/Spanning-Tree-Protocol-Standards---Types.php

3,http://www.petri.co.il/csc_preventing_network_loops_with_stp_8021d.htm

4.http://www.ccontrols.com/pdf/abc7.pdf

5.http://www.cisco.com/en/US/tech/tk389/tk621/technologies_configuration_example09186a008009467c.shtml

6.http://www.hojmark.net/spane_an.pdf

7.http://projectsinnetworking.com/?p=36