RSTP – SOLUTION TO COUNT-TO-INFINITY PROBLEM AND FORWARDING ISSUES

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By

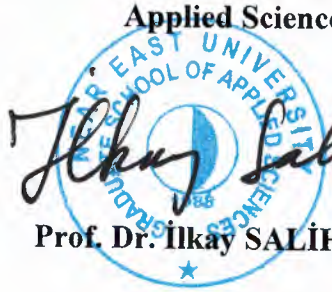
REBAZ MUHAMMED KHALIL

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA 2014

Rebaz Muhammed KHALIL: **RSTP–SOLUTION TO COUNT-TO-INFINITY PROBLEM AND FORWARDING ISSUES**

Approval of Director of Graduate School of Applied Sciences



Prof. Dr. İlkay SALİHOĞLU

We certify this thesis is satisfactory for the award of the degree of Masters of Science in Computer Information Systems

Examining Committee in Charge:

Prof.Dr. Doğan İbrahim — Committee Chairman, Department of Computer Information Systems, NEU

Prof.Dr. Rahib Abiyev — Department of Computer Engineering, NEU

Assoc.Prof.Dr. Nadire Çavuş — Supervisor, Department of Computer Information Systems, NEU

Assist.Prof.Dr. Besime Erin — Department of Computer Engineering, NEU

Assist.Prof.Dr. Elbrus Bashir Imanov — Department of Computer Engineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: REBAZ MUHAMMED KHALIL

Signature:

Date: 15/07/2014

ACKNOWLEDGMENTS

I am grateful to all members of the people who have preserved with me in putting this thesis. With immense pleasure, I express my profound sense of gratitude to my respected guide and supervisor Assoc. Prof. Dr. Nadire Cavus for her guidance.

Also, I would like to thank my Prof. Dr. Dogan Ibrahim for his constant encouragement and patience during the course of this work. I am thankful for the other staff members in my Computer Information System course.

I greatly appreciate my family and friends who have supported me at every stage of work in the doing Master in Computer Information System.

ABSTRACT

Rapid Spanning Tree Protocol is one of the most poorly understood protocols. Many people believe that Rapid Spanning Tree Protocol can converge in less than a second. Because of its complexity and complicated structure, it is difficult to be configured and modified. The main objective of this thesis is to discuss the overview of Spanning Tree Protocol, Rapid Spanning Tree Protocol and its relevant problem count-to-infinity and forwarding loop issues. Rapid Spanning Tree Protocol has been designed specifically in such a way that will reduce the convergence of switch-based Ethernet networks. The main aim of this study is to conduct and analyse the count-to-infinity problems in the RSTP. To investigate the effectiveness of the proposed solution, some experiments were done and evaluated. This thesis provided a clear picture on count-to-infinity problem in real time networks in the field of contrasting the throughput exchanged with the ends, and RSTP which is a change to the first STP acquainted with abatement the measure of time needed to respond to a connection or scaffold disappointment. The Spanning Tree Protocol is vital for circle evasion to make circle free ways. The count to infinity problem has been investigated in the laboratory environment. By changing the Hello time and forward delay parameters, it is found that better respond was obtained.

Keywords: RSTP, STP, forwarding loops, count to infinity, switch

ÖZET

Rapid Spanning Tree Protokolü en az anlaşılan protokollerden biridir. Birçok insanlar Rapid Spanning Tree protokolünün bir saniyeden daha az gibi bir zamanda toparlandığına inanırlar. Bu protokolün kompleks bir yapıya sahip oluşundan dolayı protokolü konfigür yapmak veya değiştirmek oldukça zordur. Bu tezin esas amacı Rapid Spanning Tree protokünün çalışmasını anlatmak ve buna bağlı olarak sonsuza kadar sayım (count to infinity) problemini anlatmaktır. Rapid Spanning Tree protokolü özel olarak sviç tabanlı Ethernet ağlarındaki toparlanma sorunlarını çözmek veya azaltmak için düzenlenmiştir. Bu tezde RSTP protokolünün sonsuza kadar sayım problemi ele alınarak incelenmiştir. Bu incelemeyi yapmak için bir deneysel ortam yaratılmış ve alınan neticeler analiz edilmiştir. Bu tezde sonsuza kadar sayım problemi laboıratuvar ortamında ele alınarak gerçek zamanda incelenmiştir. Hello zamanlamasını ve ileri gecikme parametresini (forward delay parameter) değiştirerek toparlanma sorunu nu çözmek için daha iyi neticeler alınmıştır.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

RSTP: Rapid Spaning Tree Protocol

STP: Spaning Tree Protocol

TTL: Time-To-Live

DIV: Distributed Path Computation with Intermediate Variables

VLANs: Virtual Local Area Networks

LAN : Local Area Network

PC: Personal Computer

BPDU: Bridge Protocol Data Units

IEEE: Institute of Electrical and Electronics Engineers

CPU: Central Processing Unit

DRSTP: Delay Rapid Spanning Tree Protocol

RRSTP: Reliable Rapid Spanning Tree Protocol

GNS3: Graphical Network Simulator

LIST OF TABLE

CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter talks about the target of the postulation and the applicable issues. It additionally furnishes the client with a short clarification about the foundation of this postulation. A workstation Network assumes an essential part in a large portion of the associations. With or without our perception in our normal business, the machine system assumes an extraordinary part. Case in point, Corporate industry, Educational organization and the Banking area, all rely on upon workstation systems to help. Also along these lines, every association has their own particular structure of system topology.

1.2 Introduction

There is a huge growth in computer networks compared to the early 90s. One of the major business challenges is the availability of network infrastructure, which is considered a major concern until now. The network administrator has to make redundancy in the network, or else a single path failure may influence the network entirely. For example, if one path in the network failed, then an alternative path should replace the connection that was lost. A hierarchical design architecture may lead to the redundancy at the distribution and core layer architecture. On the other hand, having alternative networks may result in traffic loops. To solve this problem a concept called the Spanning Tree Protocol (STP) has been employed for Ethernet based networks. It offers high bandwidth, low cost, simple maintenance and less complexity (Ray et al., 2009).

Egli (2014) demonstrated that for the central necessity of exchanged systems is to give repetitive associations without making circles. Spanning tree protocol (STP) was customarily utilized for this reason, yet its abate merging. This RSTP will take after the essential ideas of STP and coordinate its into own properties also. After exploration it has been discovered the real weakness of RSTP is check to-unendingness issue.

Jadroň et al. (2013) expressed that no compelling reason to number to-interminability is exceedingly undesirable in Ethernet organizes as it eases off the joining time of the system and in the long run diminishes the system accessibility.
Ganesh et al. (2010) exhibited a basic and compelling answer for decrease check to-interminability issues called RSTP with epochs.

Bhushan et al. (2012) displayed another calculation, Distributed Path Computation with Intermediate Variables (DIV), which might be consolidated with any appropriated steering calculation to surety that the administered diagram actuated by the directing choices stays non-cyclic at all times. Where, the key commitment of DIV, other than its capacity to work with any directing calculation, is a redesign system utilizing straightforward message trades between neighboring hubs that insurances circle flexibility at all times.

1.3 The Problem

There is a huge growth in computer networks compared to the early 90s. One of the major business challenges is the availability of network infrastructure, which is considered a major concern until now. The network administrator has to make redundancy in the network, or else a single path failure may influence the network entirely. For example, if one path in the network failed, then an alternative path should replace the connection that was lost. A hierarchical design architecture may lead to the redundancy at the distribution and core layer architecture. On the other hand, having alternative networks may result in traffic loops.
To solve this problem a concept called the Spanning Tree Protocol (STP) has been employed for Ethernet based networks. It offers high bandwidth, low cost, simple maintenance and less complexity.

The lettes RSTP denote Rapid Spanning Tree Protocol. According to Wodjak (2003) "a fundamental requirement for switched networks is to provide redundant connections without creating loops. Spanning tree protocol (STP) was traditionally used for this purpose, but its slow convergence has made it nearly obsolete". This RSTP will follow the basic concepts of STP and integrate its into own properties as well. After research it has been found out the major drawback of RSTP is count-to-infinity problem.

1.4 The Aim of the Study

The main aim of this study is to conduct and analyse the count-to-infinity problems in the RSTP. To investigate the effectiveness of the proposed solution, some experiments were done and evaluated.

1.5 Limitation of the Study

This study has the following limitations:

1. This study is limited by the date that starts from October 2013 until May 2014.
2. The lab experiment was carried out in a small network.
3. Less experience in handling the experiments, even though it is a small network because lots of configurations has been involved.
4. Known issues with the count to infinity problem and looping.

1.6 Overview of the Thesis

This thesis consists of five chapters:

Chapter One: This represents and overview of the spanning tree protocol (STP) and literature review of the study.

Chapter Two: It presents an overview of different research on STP and the advantages of using this protocol as a solution for the count-to-infinity.

Chapter Three: It explains the methodology of the STP, RSTP in details. Moreover, it explains briefly the Wireshark.

Chapter Four: It describes in details the setup procedure of the topologies and the obtained results of the experiments that made in the laboratory.

Chapter Five: It draws conclusion in the results achieved in the last chapter. What's more, it presents ideas that might profit the reader to undertake future research work in the region.

1.7 Summary

One of the challenge problems in the modern life is how propose an effective solution for the count-to-infinity in the RSTP. Where, this thesis presents an effective approach called epochs and etherfuse solution. Finally, these studies are compared and analysed.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The 802.1D phrasing remains principally the same. Most parameters have been left unaltered so clients acquainted with 802.1D can quickly design the new convention agreeably. As a rule, RSTP performs superior to restrictive augmentations of Cisco without any extra design. 802.1w can likewise return over to 802.1D keeping in mind the end goal to interoperate with legacy connects on a for every port premise. This drops the profits it presents.

2.2 Computer Networks

2.2.1 Basic Network Structure

A system comprises of 2 or more machines associated together, and they can impart and offer assets as data, where this data is as information correspondence. Systems are various types: Depending on one's point of view, they can characterize is organized in distinctive ways:

- In view of administration strategy: Peer-to-companion and Client/Server.
- In view of topology (integration): Bus, Star, Ring.

Topology is the physical design of machines, links, and different parts of a system. Numerous systems are a blending of the different topologies:

- Bus,
- Star,
- Mesh,
- Ring,

A bus topology utilizes one link to interface, numerous workstations. The link is likewise called a trunk, a spine, and a section. More often than not, as seen in Figure 2.1 beneath, T-connectors are utilized to unite with the cabled section. Ordinarily, coaxial link utilized within transport topologies (Meador, 2008).

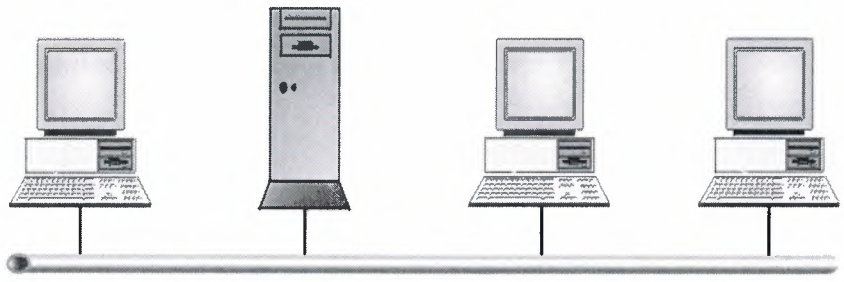


Figure 2.1: Bus Topology (Kaur, 2009)

An alternate key part of a transport topology is the requirement for the end. To keep parcels from bobbing here and there the link, gadgets called eliminators must be connected to both closures of the link. An eliminator retains an electronic significant and clears the link so that different machines can send parcels on the system. On the off chance that there is no end, the whole system fizzles. Stand out machine at once can transmit a bundle on a transport topology. Machines in a transport topology listen to all movement on the system, yet acknowledge just the parcels that tend to them. Telecast bundles are an exemption on the grounds that all machines on the system acknowledge them. At the point when a workstation conveys a bundle, it goes in both headings from the machine. This implies that the system is involved by the end of the line machine acknowledges the bundle. The amount of workstations on a transport topology system has a significant impact on the execution of the system. A transport is an aloof topology. The workstations on a transport topology just listen or send information. They do not take information and send it on or recover it. So if one workstation on the system fizzles, the system is still up (Kharagpur, 2006).

- **Favorable Circumstances**

One playing point of a transport topology is expense. The transport topology utilizes less link than the star topology or the cross section topology. An alternate point of interest is the simplicity of establishment. With the transport topology, the client basically interfaces the workstation to the link fragment, or spine. The client requires just the measure of link to unite the workstation client has. The simplicity of working with a transport topology and the base

measure of link settle on this the most practical decision for a system topology. In the event that a machine fizzles, the system stays up.

- **Drawbacks**

The principle inconvenience of the transport topology is the trouble of troubleshooting. With a substantial system this could be hard to detach. Versatility is a vital attention to the element universe of systems administration. Having the capacity to roll out improvements effectively in the size and design of the client's system could be vital in future gains or downtime. The transport topology is not extremely adaptable.

A star topology really originates from the times of the centralized computer framework. The centralized computer framework had a concentrated point where the terminals joined as shown in Figure 2.2 (Meador, 2008).

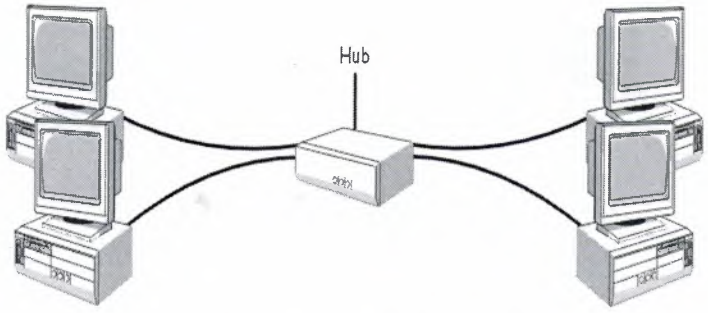


Figure 2.2: Star Topology (Konkoth, 2000)

- **Focal points**

Incorporating system segments can make a head's life much simpler in the long run. Unified administration and observing of system movement might be key to system achievement. With this kind of setup, it is likewise simple to include or change designs with all the associations going to an essential issue.

- **Detriments**

On the other side to this is the way that if the center point comes up short, the whole system, or a great bit of the system, descends. This is, obviously, a less demanding fix than attempting to discover a break in a link in a transport topology. An alternate weakness of a star topology is expense: to join every workstation to a brought together center point, the user needs to utilize substantially more link than he does in a transport topology.

A Mesh topology is not extremely normal in machine organizing. With the cross section topology, each workstation has an association with each other segment of the system, as outlined in Figure 2.3 (Cherkasova et al., 1995).

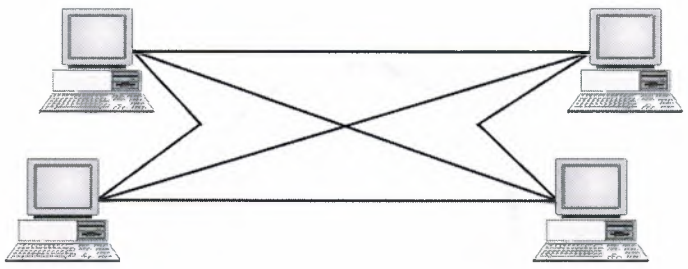


Figure 2.3: Mesh Topology (Konkoth, 2000)

- **Preferences**

The greatest preference of a lattice topology is shortcoming tolerance. In the event that there is a break in a link portion, movement could be rerouted. This deficiency tolerance implies that the system setting off down because of a link issue is very nearly unthinkable. Stretch practically in light of the fact that with a system, regardless of what number of associations user has, it can crash.

- **Burdens**

A cross section topology is tricky to oversee and oversee as a result of the various associations. An alternate impediment is expense. With an expansive system, the measure of link required to unite and the interfaces on the workstations would be exceptionally unmanageable.

In a ring topology, all workstations are joined with a link that circles around. Signs go in one bearing on a ring while they pass starting with one machine then onto the next. In the event that one of the workstations comes up short, the whole ring system goes down (Tangmunarunkit et al., 2002).

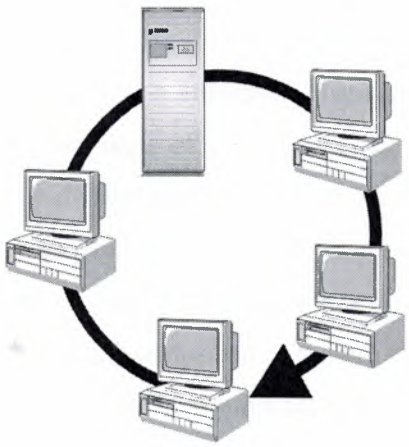


Figure 2.4: Ring Topology (Konkoth, 2000)

- **Points of interest**

The decent thing around a ring topology is that every machine has equivalent access to convey on the system. With transport and star topologies, one and only workstation can convey on the system at once. The ring topology gives great execution to every workstation. This implies that busier workstations who convey a ton of data don't hinder different machines from imparting.

Disservices

With more up to date engineering this is not generally the case. Secluding an issue could be troublesome in a few designs likewise. An alternate weakness is that on the off chance that the user roll out a cabling improvement to the system or a workstation change, for example, a move, the short separation can intrude on or cut down the whole system.

2.2.2 Switches

A Network switch is a gadget that channels, advances, or surges edges focused around the end of the line location of each one edge. A switch is an extremely versatile Layer 2 gadget; it replaces a center as the main issue of association for numerous hosts. In a most unpredictable part, a switch may be joined with one or more different switches to make, oversee, and keep up repetitive connections and VLAN network. A switch forms different varieties of movement in the same path, paying little mind to how it is utilized. Little office, Home office (SOHO) applications typically, utilize a solitary or a universally handy switch. As said prior, switches works at the information connection layer of the OSI model, switch capacity is to make an alternate impact space for every switch port. Not at all like a centaur, which permits the offering of data transmission by all ports, run fifty-fifty duplex and is inclined to the impacts of edges and retransmissions. With a few ISPs and other systems administration situations where there is a requirement for much examination of system execution and security, switches may be associated between WAN switches as spots for expository modules. A few switches give in fabricating firewall, system interruption recognition and execution investigation modules that can connect to, switch ports (Meyer et al., 2014; Contemporary Controls, 2011).

2.2.3 Models

An Ethernet is a gathering of machine systems administration apparatuses united with a particular set of norms. A system switch is an alternate term for a gadget that unites diverse parts of a machine arrange together. Created in 1980, Ethernet systems are focused around the IEEE 802.3 standard. An Ethernet switch must have the capacity to transmit information at a particular level with a specific end goal to guarantee the joined workstations and gadgets all capacities legitimately. It is essential to recall that while both switches and centers must have

the capacity to meet the fundamental standard, switches can have numerous ports working at diverse places. An Ethernet switch is the activity control community in the neighborhood (LAN). A LAN is a system for associating numerous machines, printers, Internet switches and other related gadgets. The system switches are obliged to deal with the transmission of information bundles between different gadgets (Meyer et al., 2014; Ismaeel, 2012).

2.3 Rapid Spanning Tree Protocol (RSTP)

The execution of an Ethernet system might be adversely affected by the shaping of an information circle in the system topology. An information circle exists when two or more hubs on a system can transmit information to one another over more than one information way. The issue that information circles stance is that information bundles can get to be discovered in rehashing cycles, alluded to as show storms, that unnecessarily expend system data transmission and can essentially decrease system execution. RSTP keeps information circles from framing by guaranteeing that one and only way exists between the end hubs in the system. Where numerous ways exist, this convention puts the additional ways in a standby or blocking mode, leaving stand out primary dynamic way. RSTP can additionally enact a repetitive way if the fundamental way goes down. So not just do these conventions prepare for different connections in the middle of sections and the danger of telecast storms, however they can additionally keep up system integration by initiating a reinforcement excess way in the event that a principle connection fizzles (Phil et al., 2010; Shafaat et al., 2007, and Shaffi et al., 2012).

At the point when a change is made to the system topology, for example, the expansion of another scaffold, a spreading over tree convention must figure out if there are excess ways that must be hindered to anticipate information circles, or enacted to keep up interchanges between the different system sections. This is the methodology of merging. RSTP can finish a joining in seconds, along these lines significantly lessens the conceivable effect the procedure can have on the system. One major drawback of STP is the low joining which is exceptionally critical in exchanged system. RSTP works by including an option port and a reinforcement port contrasted with STP. These ports are permitted to promptly enter the sending state as

opposed to inactively hold up for the system to meet. RSTP scaffold port parts. Where, this way is not the same as utilizing the root port, and backup port – A reinforcement/excess way to a section where an alternate scaffold port as of now interfaces. The reinforcement port applies just when a solitary switch has two connections to the same fragment crash area. To have two connections to the same crash space, the switch must be joined to a center as shown in Figure 2.5 (Balchunas, 2009).

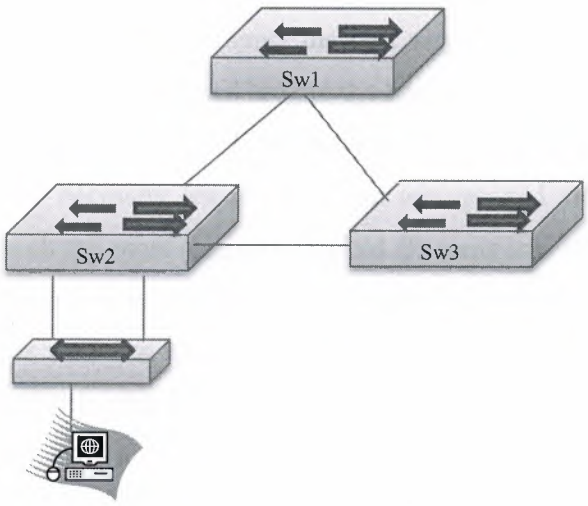


Figure 2.5: Three switches system (Balchunas, 2009)

2.4 Functionality of RSTP

Conventional Layer 2 exchanging situations comprise of Layer 2 gadgets, for example, switches that parcel information into show spaces. The telecast spaces could be made through physical topologies or through virtual local area networks (VLANs). On Juniper Networks switches can intelligently arrange telecast areas inside virtual switch directing occurrences, VPLS steering cases, or extension spaces. The individual directing cases or scaffold areas are separated through VLANs IDs, and these occurrences or spaces work much like customary VLANs. As is the situation with conventional Vlans, keeping in mind the end goal to evade circles inside scaffold areas, you must arrange a circle aversion instrument. These conventions

counteract circles inside a neighborhood local area network (LAN) or VLAN by making a tree topology in which there is stand out way from each one source to every objective. Before going into setup points of interest, let us gaze all the more nearly toward how the diverse circle avoidance conventions work (Yu et al., 2011).

STP is the least difficult circle counteractive action convention and is the premise for RSTP. As is the situation with other crossing tree conventions, STP utilization bridge protocol data units (BPDUs) to recognize a system's tree topology. A STP tree topology might be contrasted with a genuine tree. All leaf gadgets compute the best way to the root gadget and spot their ports in blocking or sending states focused around the best way to the root. This averts circles. The root gadget is dictated by thinking about extension Ids of the gadgets. The scaffold Ids comprise of the extension necessity which client can arrange and the MAC location of the extension. The gadget with the most minimal scaffold ID turns into the root gadget of a STP topology. In the event that a way is defective, the root port does not accept arrangement Bpdus and inevitably the Bpdus time out. On the off chance that the design BPDUs time out, the gadget sends BPDUs publishing the following best gadget as the root, and the procedure starts once more (Bhushan et al., 2012).

Despite the fact that STP gives essential circle aversion usefulness, it doesn't give quick system joining when there are topology changes. This reasons system delay, on the grounds that no information activity can cross this gadget until the topology is straightened out. RSTP extraordinarily diminishes the state move time. RSTP gives a quicker meeting time and preferred system steadiness over STP in light of the fact that it permits recently chose attach or sending ports to enter sending states all the more quickly. With STP, a nonroot gadget produces design BPDUs just when it accepts arrangement Bpdus on its root port (Shaffi et al., 2012).

A RSTP gadget creates design messages once every welcome time interim, regardless of the fact that it doesn't accept a setup BPDU on its root port. A nonroot gadget running RSTP has a root port, which is the best way to the root gadget; an assigned port, which is the briefest way association with the root gadget for a LAN section between two nonroot gadgets, a substitute

port, which gives an interchange root port, and a reinforcement port, which gives an exchange assigned port. At the point when a root port or an assigned port falls flat on a gadget, the gadget produces a setup message with the proposal bit set. Once its neighbor gadget accepts this message, it confirms that this design message is superior to the one put something aside for that port and afterward it begins a synchronizing operation to guarantee that every last bit of its ports are in sync with the new data. Comparative waves of proposal understanding handshake messages engender at the leaves of the system, restoring the network rapidly after a topology change in a decently planned system that uses RSTP, system union can take as meager as 0.5 seconds. On the off chance that a gadget does not get a consent to a proposal message it has sent, it comes back to the first IEEE 802.D meeting (Pal et al., 2013).

The switch consequently faculties port personality and sort, and naturally characterizes spreading over tree parameters for each one sort, and parameters that apply over the switch. While permitting one and only dynamic way through a system whenever, spreading over tree holds any excess physical way to serve as a reinforcement blocked way on the off chance that the current dynamic way fizzles (Phil et al., 2010).

Accordingly, if a dynamic way comes up short, traversing tree consequently initiates unblocks an accessible reinforcement to serve as the new dynamic way as long as the first dynamic way is down. In the manufacturing plant default arrangement, spreading over tree operation is off. On the off chance that an excess connection circle exists between hubs in customer system, customer ought to empower the traversing tree operation of as per the decision of the customer as indicated in Figure 2.6 (Shaffi et al., 2012).

- Active path from node A to node B: 1—> 3
- Backup (redundant) path from node A to node B: 4 —> 2 —> 3

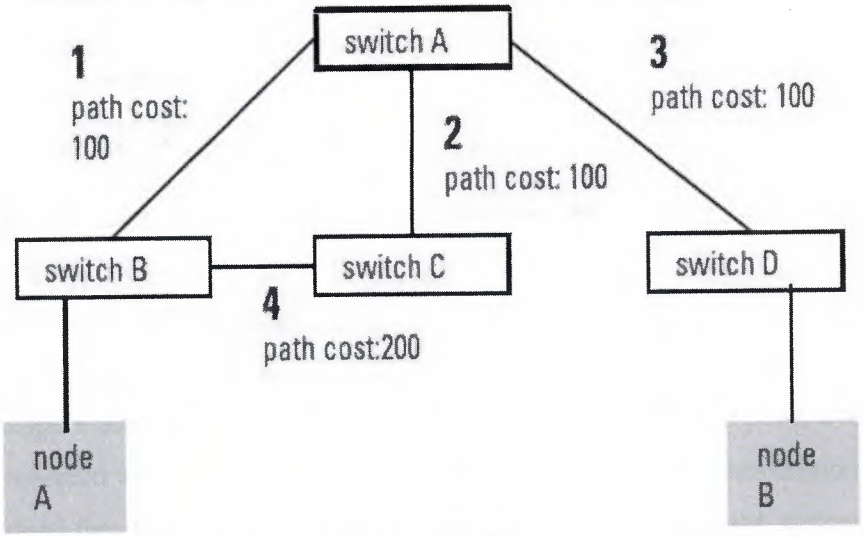


Figure 2.6: Redundant Paths Between Two Nodes (Spirent, 2010)

In RSTP, the discarding port state replaces the listening, blocking and disables the states of STP. Faur (2009) stated that the forwarding table can be defined as a table that keeps the records of MAC addresses and their associated ports learnt through address learning mechanism. It is important because a PC may change its location with respect to switching after a topology change.

By using Spanning Tree Algorithm RSTP it can be easy to calculate a unique spanning tree over the network of connected links, switches and others things.

The following are the rules/ways to construct a tree:

1. Initially, the root node must be selected.
2. The bridge will be the switch and it will be the smallest switch ID.
3. This switch ID consists of the MAC address of the bridge and its priority is managed by the administrator.
4. The other switch selects the nearest port to the root with the smallest distance to/from the port as the root port.
5. If a bridge has equal distance to the root, then the bridge will offers the lower ID which will be selected.

6. Finally, all the bridges have their designated ports and this will provide a faster means of communication.

The remaining parts will be blocked to avoid interfering with the existing ports.

2.5 Bridge Protocol Data Unit

A bridge protocol data unit (BPDU) is an information message transmitted over a neighborhood to catch circles in system topologies. A BPDU holds data in regards to ports, switches, port necessity and locations. BPDUs hold the data important to arrange and keep up traversing tree topology. They are not sent by switches; however the data is utilized by switches to compute their own particular BPDUs for data passing. At the point when gadgets are at first connected to switch ports, they don't begin information transmission instantly. Rather, they travel through diverse states while BPDU handling decides the system topology. This banner is proliferated to all different switches to teach them to quickly age out their sending table section switches (Koymans, 2008).

2.6 Spanning Tree Algorithm

By using BPDU's information, the Spanning Tree Algorithm selects the root switch and assign the port roles on each switch. The best information will be recorded in each port record it is received. The port that receives the best information, for a path to the root among all information received by all switch ports will become the root port. The port other than the root port is called the alternative port and it receives better information than the one it transmits as shown in Figure 2.7 (Pfenning, 2010).

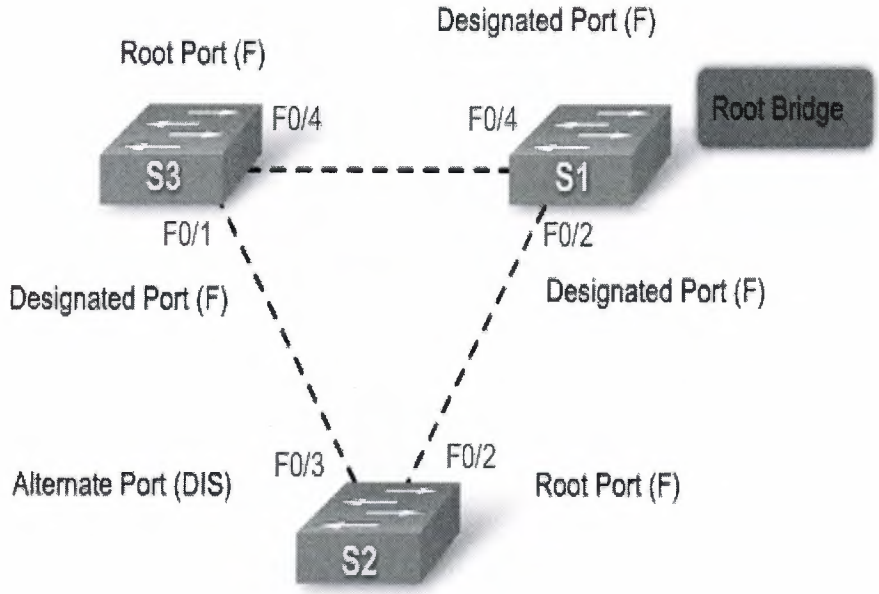


Figure 2.7: RSTP Port States 1 (Lapukhov, 2010)

Figure 2.3 is an example of RSTP and it shows three port states which are discarding, learning and forwarding. S1 is the root switch with two designated ports (F), F stands for forwarding state. S2 and S3 are the other two switches. The port F/03 on switch S2 is an alternative port in discarding state (Lapukhov, 2010).

RSTP (802.1w) uses type 2. It has version 2 BPDUs. Therefore, RSTP switch can communicate 802.1D with any switch running 802.1D or on any shared link. RSTP bridge communicates with BPDU and sends, with its current information, every hello time period (which is usually two seconds), even RSTP switch will not ping BPDU from the root bridge. The best part in RSTP is that it provides a faster convergence in the case of failure or while reconnecting to a switch, switch port or a path. The change of RSTP topology causes a transition in the appropriate switch ports to the forwarding state through either explicit handshakes or a proposal and agreement process and synchronization. It is important because a node may change its location with respect to switch after a topology change as shown in Figure 2.8.

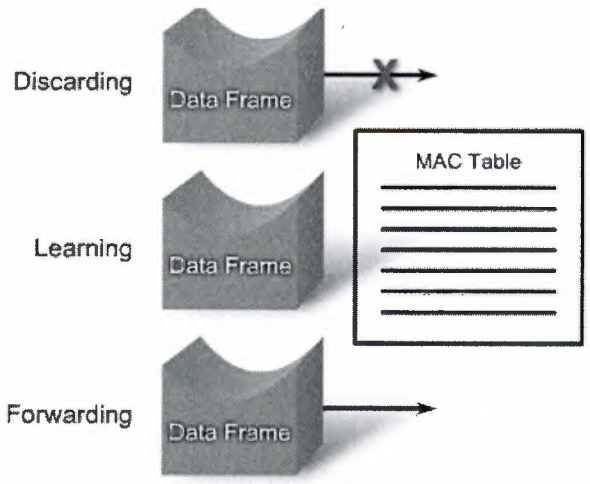


Figure 2.8: RSTP Port States 2 (Rambhadjan, 2010)

In the case of RSTP, the state of a port is separated from the role of a port. For instance, though the final state of the designated port is forwarding, it could be present in the discarding state temporarily. In all the port states, a port accepts and process the BPDU frames. There won't be any forwarding of frames, when the ports in the STP blocks, listens or disable port states. If a port was chosen by spanning tree to become the designated port, then it should wait for two times the forward delay time before transitioning the port to the forwarding state, whereas RSTP magnificently boosts up the recalculation process after a topology change occurs since it converges on a link by link basis and does not depend on timers. Rapid transition to the forwarding state can be accomplished on the edge ports and point to point ports (Pfenning, 2010).

2.7 Existing Problems with RSTP

This topic discusses the problems arising with RSTP such as Count to infinity and Forwarding Loops.

2.7.1 Count To Infinity

In count to infinity, the concept of sync, which is a handshake operation between adjacent switches helps to prevent a forwarding loop. A race condition between two RSTP state machines and a non-deterministic transition within a state machine that together allow a sync operation to be mistakenly bypassed. Once this sync operation is bypassed, a forwarding loop is formed which lasts until the end of count to infinity (Phil et al., 2010).

Cisco (2014) presented a case to illustrate the count to infinity problem. When a network is partitioned and the partition without root switch has a cycle, then a race condition can result in a count to infinity behavior. In this case, at least one switch in the partition will declare itself as the new root switch and will start spreading BPDUs. These BPDUs will race with the stale BPDUs announcing the previous root around the cycle. This race may lead to count to infinity as shown in Figure 2.9 (Golestanian et al., 2013).

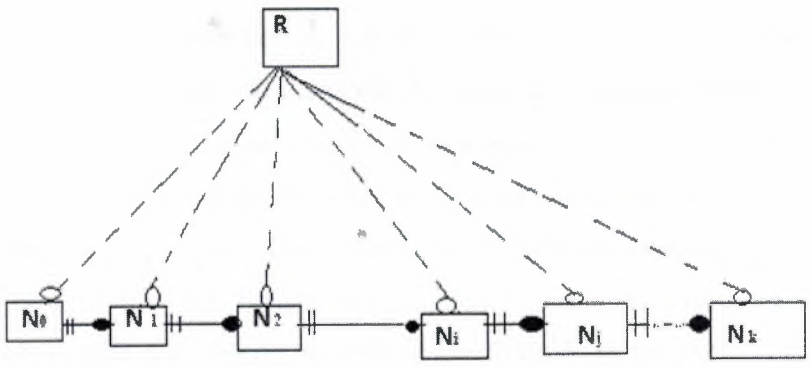


Figure 2.9: Network Partition (Phil et al., 2010)

1) When a network is partitioned, the partition without the previous root switch must have a switch that has no alternative port.

In the above Figure 2.9, the partition R is the root switch in the network. The solid line shows the switch - to - switch connection and the dotted lines represented the network path that may include intermediate hops. The switch R_x has the shortest path to R (root switch) with a cost of C_x. After the partitions the switches from N_o to N_k lose connectivity with the root node R. Let us consider that the switch from N_o to N_k have more than one alternative paths to R. Also, Let's start from the switch N_o. Since No has more than one alternative port, let say it is connected to N_1 which also has an alternative path to R, which doesn't include N_o. Without the loss of generalzation, suppose that BPDU sent by N1 is better than BPDU sent by N_o. Now N_o has an alternative path to R through N1. The same is with N_1 as it should have alternative to R through N2. And this scenario is applied to reach N_k. Because there is a finite number of switches, N_k should obtain an alternative port to R through one of the switches N_o to N_{k-2}. The issue is quite complicated as $N_{k's}$ BPDU is better than all other switches of BPDUs. This is considered a conflict and now there is a switch in the partition that does not include the previous root that has no alternative port. Therefore, it must announce itself as the new root switch and starts sending BPDUs by means of declaring itself as the new root switch. These types of BPDUs will be more in the partition (Faur, 2009).

2) Consider if a network is partitioned, and the partition without the previous root bridge contains a cycle, the a race condition exists which may lead to count to infinity.

In the above scenario, in which a partition contains a cycle, one or more switches without the alternative port must declare themselves as the root switches and send their own BPDUs to the rest of the switches in the partition. There should be one or more switches in the network with an alternative port to the root before the partition in order to avoid forwarding loops. Therefore, an alternative port should be there at the link where the cycle is cut (Phil et al., 2010).

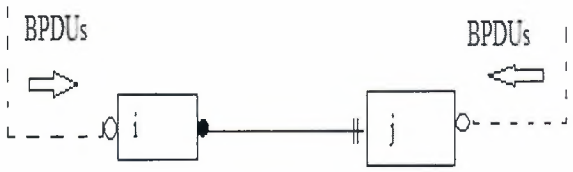


Figure 2.10: i and j representing switches (Fiduccia et al., 1982)

Figure 2.10 manifest an example of such a case, where i and j represents switches. There is an alternative port in the cycle and the switches i and j are connected to the rest of the loop. So, i has been connected with a root port on its left and has a designated port that does the linking. The switch j is connected to the loop with its root port on the right and it is connected to the switch i by an alternative port. BPDUs in one or more than one switch announcing themselves to be root will race around the cycle (Golestanian et al., 2013).

If the BPDUs receive the switch j on its root before the alternative port, then it finds its alternative port which has better cached topology information. This information suggests a path to a superior root port that is no longer reachable. Now, using the stale information, switch j will use its alternative port as its new root port. Then with the containing stale information, the switch j will start transmitting the BPDUs to the switch on its right. The reason behind that is because the switch j considers the topology information it has cached is better than the information it received from the neighboring switch at its right. After that, switch j will get BPDUs on its new root port, then switch i from switches declares them to be the root. Switch j will then recognize that the topology information at its root port is stale and will accept the new topology information and also forwards such new information to its right. Now the fresh BPDUs will chase the stale information around the loop resulting in a count to infinity (Shafaat et al., 2007).

If the switch j receives the fresh BPDUs from other switches which declare themselves as the root on its alternative port first before receiving them on its root port, the stale topology information will be wiped out and no count to infinity will occur. Even without the network partition, the count to infinity problem may occur. The highest path cost will be chosen if the

loop in the physical topology loses its cheapest link to the root. This new new information which is will race around the loop until it reaches an alternative port caching stale. Now this stale topology information will chase the new information around the network, which results in a count to infinity. This stale information will be removed after the cost reported by the stale information increases and exceeds that of fresh information or it reaches its Max Age. The reason behind that is because the cost of stale information increases during its circle to loop in a count to infinity. Count-to-infinity problems in switch based Ethernet network. A count-to-infinity can occur in RSTP when there is a cycle in the physical topology and this cycle loses connectivity with the root bridge because of a network failure as shown in Figure 2.11 (Lapukhov, 2009).

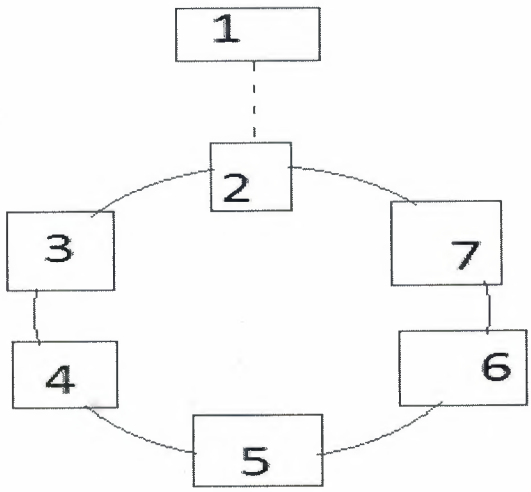


Figure 2.11: Count to infinity – Physical Topology (Elmeleegy et al., 2007)

The path between S1 and S2 may or may not be a direct link. In the case of failure, this path will lead to the rise of count-to-infinity problems. A switch has cache topology information on its alternative ports initiated in the past. If the connection is lost between the root port and root bridge, then the stored information can be retrieved. But the received information may be new or old one. In case, if it is to use the cache information without any differentiation, then the stale information can be used. Then that particular switch will spread those stale information to other switches through BPDUs and this will result in the rise of count-to-infinity problems.

Now, let take a quick look on count-to-infinity problems.

1. If a switch loses a connectivity from the root switch and also if it does not have any alternative ports, then it will declare itself as the root switch.
2. After the topology information has been changed, then the switch transmits BPDUs instantly. i.e. when the root or cost of root is changed.
3. A designated port changes into a root port if it receives a better BPDU than the switch has received earlier.
4. If a switch loses a connectivity from the root switch and if it has an alternative root, then the alternative root with low cost will be chosen as the new root port.

perceived by the current switch. The lower right number represents the cost to the root switch. In the example, the cost to each link is set to 20 (TSAI, 2011; Tang et al., 2011).

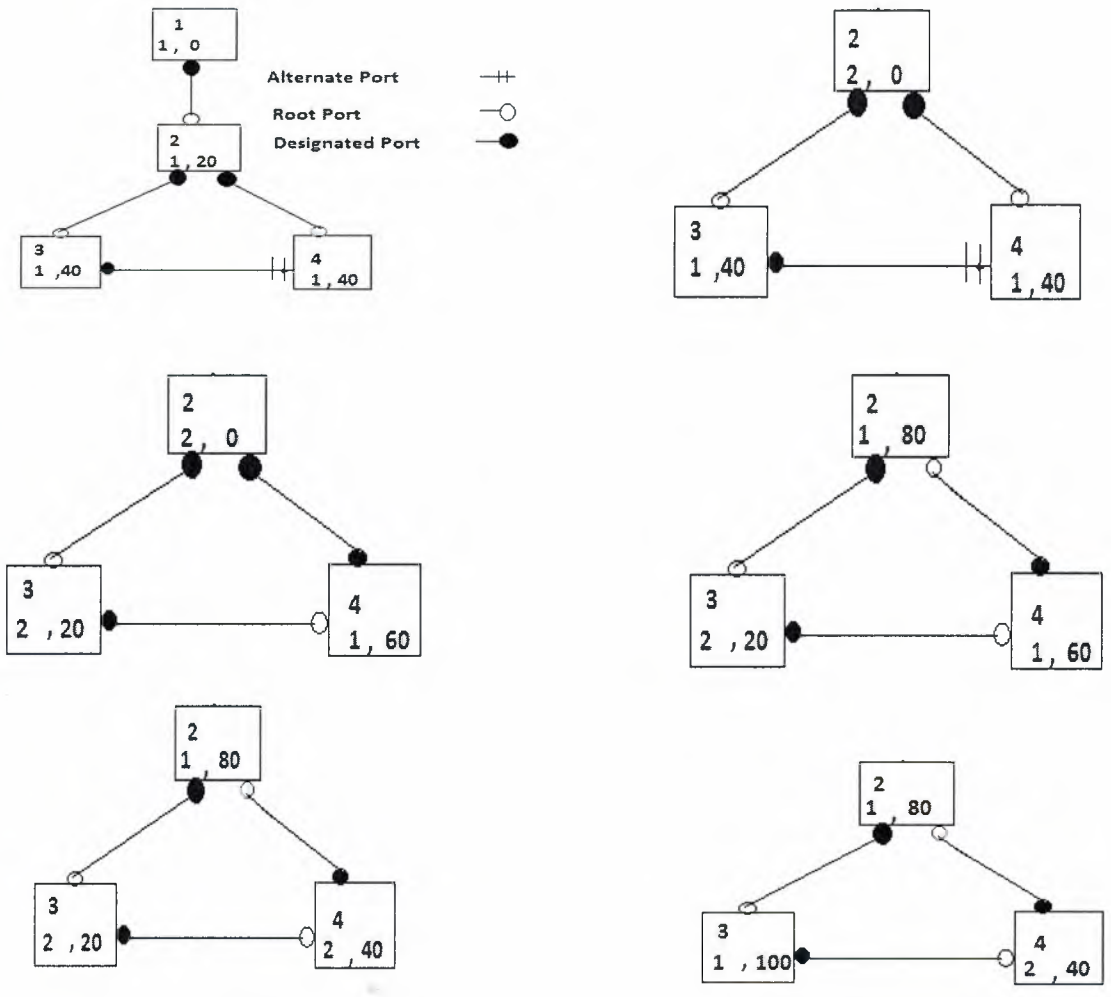


Figure 2.12: Simple Network Topology Count to Inifinity Problem (Junipe, 2012)

The Figure 2.12, shows a simple network topology. The switches are represented by boxes. The uppermost number shows switch ID. The lower left number shows the root switch ID as Figure 2.12a, demonstrates the stable topology at given time t1. Figure 2.12b, At time t2, it shows the path failure between switch 1 and 2. Since there is no alternative port, switch 2 has declared itself as the root switch. Then it announces itself as the root switch to the switches 3 and 4. therefore, at time t3, switch 3 doesn't have any alternative port, and so it makes 2 as its root node. But in case 4, it has an alternative port to switch 1. Hence, switch 4 makes an incorrect decision by taking 1 as its root node. This reason behind that is because switch 4 has

no way of identifying that the cached topology information at the alternative port is stale. At time t4, the switch 4 notifies switch 2 that it has a path to switch 1 by spreading the stale information resulting in count-to-infinity problem. Thereby switch 2 makes switch 4 as its parent and updates the cost to switch 1 to 80. At time t5, switch 3 sends a BPDU to switch 4, inforing that switch 2 is the root switch. As switch 3 is the parent of switch 4, and switch 4 accepts this information and sets its cost to switch 2 to to be 40. At time t6 switch 2 sends a BPDU to switch 3 stating that it has a path to switch 1. Then Switch 3 makes switch 2 its parent by updating its cost to switch 1 to be 100. This stale topology information about switch 1 will continue to move around until it reaches its MaxAge or caught up and replaced by fresh topology information (Golestanian et al., 2013).

2.7.2 Forwarding Loops

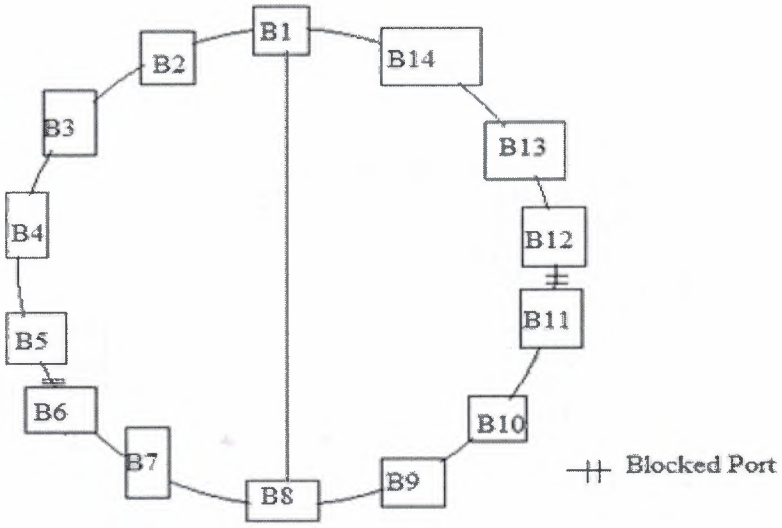
Elmeleegy et al. (2007) stated that a forwarding loop is formed in a network when a switch's port erroneously switches from a blocked state to a forwarding state and starts forwarding packets. If the loops are going to be short lived then it will converge after the loop is broken in case it is long lived or permanent, then it will make the network unusable.

2.7.2.1 BPDU Loss infuenced Forwarding Loops

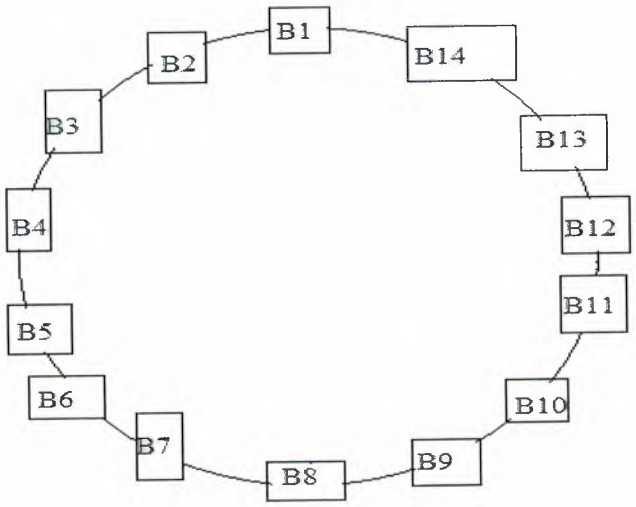
As per the spanning tree rules, if a port is blocked and not the root port and it receives BPDUs from the parent switch that advertises a low-cost path to the root switch than its own BPDUs. In case if the port doesn't receive BDPUs for a certain period of time, then it will begin data forwarding. The reason for BPDU loss can be due to the overload of CPU control or the bandwidth of the link. This BPDU's forwarding loop loss could be due to the uni-directional link. The uni-directional link takes place due to the failure of an optical fibre link or because of the transceiver. Ethernet links are bi-directional. Therefore, the BPDU that travels in the wrong direction will be lost. This kind of BPDUs loss can make the blocked port, suddenly, start forwarding data in the direction. However, It is functional and can create a forwarding loop (Jauregui, et al., 2011).

2.8 MaxAge Rouse Forwarding Loops

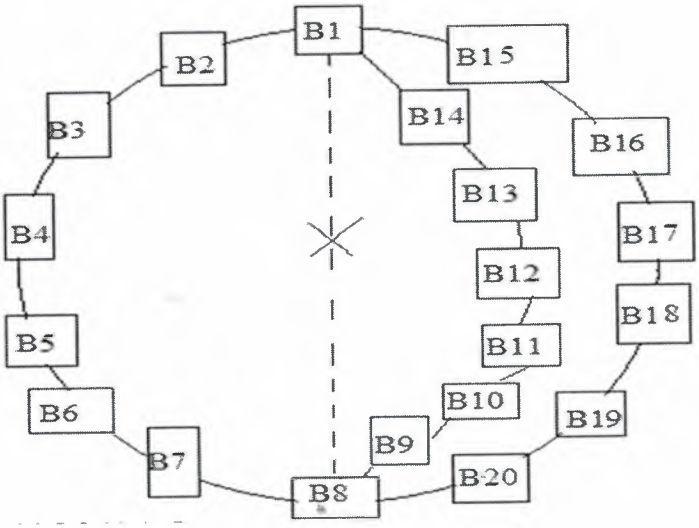
In RSTP, MaxAge shows the maximum height of a spanning tree. In case of very large network, the BPDU from the root switch will not reach the other switches in the network. For example, switch 1 sends BPDU to switch 2, then the BPDU arrives with a message that equals a MaxAge. Now the Switch 2 will block its port to switch 1, by separating the network. Finally switch 2 is not connected to switch 1, and the port connecting switch 2 to switch 1 will become forwarding by default. These spanning trees result in a forwarding loop because it conjoined at the leaves. In some cases, a single localized failure can lead to a forwarding loop (Kohli, 2005).



(a) Before Link Failure



(b) After failure



(c) Multiple loops

Figure 2.13: Forwarding Loops – Before and After Failure, Multiple Loops (Becchetti, 2009)

Figure 2.13 shown above, B1 is the root switch and the value of MaxAge is set to 6. Blocked port will be represented as it is shown in the Figure. Figure 2.13 b shows the failure of the link between switch 1 and switch 8. All the links were within 4 hops of the root bridge before

failure takes place. A spanning tree has been created by the blocked ports at B5 and B11 by cutting the physical cycle. B8 becomes 7 hops away from B1. Hence, B1 reaches its MaxAge before reaching B8. Therefore, they are dropped by B8. Now, as there are no valid BPDUs received from its neighbors, B8 declares itself as the new root. Then it will make its ports which are connecting it to B7 and B9 as its designated ones. On the other side B7 and B9 still hoping that B1 is the root of the spanning tree as BPDUs received have message which age is below MaxAge. B7 and B9 still trust that B8 is their child and make their ports with connection with B8 as their designated port. Hence, a permanent forwarding loop is formed because all the ports in the network are, meanwhile, transmitting data packets. Figure 2.13 c, shows that multiple forwarding loops can take place in the case of large and complex topology. Therefore the broadcast packets will be replicated and it may lead to rendering the whole network.

2.9 Approaches to Encounter the Count to Infinity Problem in RSTP

This section discusses the different approaches to encounter the count to infinity problem in RSTP.

1. RSTP with Epochs
2. Etherfuse
3. RRSTP
4. DRSTP

2.9.1 RSTP with Epochs

There are many researchers who carried out their research and made a significant contribution in solving the count to infinity problem. Elmeleegy et al. (2009) proposed that RSTP with epochs which is an extension of RSTP as a solution for count to infinity problem. The RSTP with epochs, is a serial number that is added to each and every BPDU which are originated by root switch. Based on this root switch and changed topology information, other switches receive this BPDU and generate their own version BPDU. From this it can distinguish the stale

BPDU and stale cache information of a dead root switch. The count to infinity problem does not resolve by only adding the sequence number.

Lyons (2010) gave the example of an old root switch A and new root switch B which joined the network with a lower Switch ID than switch A. When B is chosen as the new root switch, then it will receive the BPDU with sequence number from A. Now switch B will spread its BPDU by setting the sequence number higher than the switch A's BPDU. Here A's BPDUs are overridden. When switch B's BPDU reaches switch A, it may have the transmitted one or more BPDUs with a higher sequence number. Switch A will not back off and the whole network will not converge.

This is the way the Epochs are used to solve the problem. Epoch can be defined as the time interval which begins when a true root switch achieves root status and ends when another switch competes for root status. The reasons for competition for root switch might be due to:

1. A Switch might not be knowing that a previous root switch has been retired,
2. The root switch may be still reachable, since contended switch has lost its path to the root without having any other alternative ports.
3. A switch has newly joined the network, but the switch ID will be lower than the current root switch.

Elmeleegy et al. (2009) used the scenario, discussed above, that when the old root switch retires, and the contending switch is eligible to be the root switch. Hence the new root will use a sequence number which is higher than the sequence number it received from the old root switch by announcing a new epoch with a new root switch. But if the old root switch canhed and is eligible to be the root switch, then it pumps up its sequence number to override the contending switch's sequence number to re-take the network. This indicates a new epoch, but it is with the same root switch as in the case of the previous epoch.-There will be two sequence numbers present in an interval, Firstsequence number and Currentsequence number. The First sequence number is of the current root, whereas the Current sequence number is the current sequence number, from the root switch. In the above example, epochs allow the new root B to catch up with the A's sequence numbers so that it can take control of the entire network. Thus when the new root switch B's reaches switch A, the switch A may have transmitted BPDUs

with a higher sequence number, but the B's BPDU sequence number remains within the interval which represents the current epoch. Here switch A realizes that switch B coexists with it in the same epoch. The downside of RSTP with epochs is that its small overhead can result from its relative negativity (Pfenning, 2010).

2.9.2 Etherfuse

It is a device and that needs to be inserted into an existing Ethernet so that it speeds up the reconfiguration of the spanning tree and it will prevent count to infinity problem. To eliminate count to infinity from Ethernet networks. The working principle of Ether fuse is that it detects the count to infinity by obstructing all BPDUs that flow through it. For example, it will check if there are 3 BPDUs announcing an increasing cost to the same root. A counter has been maintained by Etherfuse which will be incremented every time when it receives a BPDU with increasing cost to the same root. If there are similar consecutive BPDUs received by the Etherfuse then the counter will be reset to 1. If the counter value is 3 then it means that count to infinity problem occurred. The stale information is circulating in the form of the loop and will keep running until it expires. The reason behind checking three consecutive BPDUs that announce an increasing cost is that BPDUs are transmitted to announce new topology information or after every hellotime (typically of 2 seconds). Etherfuse checks for duplicate packets to monitor forwarding loops in a network. Anyhow, the effect of Etherfuse on count to infinity is very limited because of the design of the spanning tree protocols. RSTP with the extension Epoch is a new protocol that is specially developed in order to resolve the count-to-infinity problem but it is unprotected to temporary count-to-infinity (Cox et al., 2011).

2.9.3 RRSTP

RRSTP stands for Reliable Rapid Spanning Tree Protocol is to safeguard switched Ethernet networks against count to infinity. This protocol involves two mechanisms; namely Root switch Reelection Mechanism and Rapid BPDU distribution mechanism for timely convergence of network to a new topology after a topology has changed (Baldi et al., 2002).

2.9.3.1 Rapid BPDU Distribution Mechanism

RRSTP won't permit switches to use their alternative ports. But instead, it uses Rapid BPDU Distribution Mechanism in order to keep convergence time minimum (Zargar et al., 2012).

Below mentioned are the functionality of the Rapid BPDU Distribution Mechanism:

1. If a non-edge designated port of a switch fails then,
   a) Send a configuration BPDU on all its non-edge designated ports
   b) Send a Request BPDU from its root port.
2. If a switch receives a Request BPDU on its non-edge designated port then it must do the step 'a' and 'b' of 1.

2.9.3.2 Root Switch Reelection Mechanism

In Reliable Rapid Spanning Tree Protocol, for converging to a new topology the switches in isolated child tree are dependent upon switches in the rooted child tree. The configuration BPDUs which are generated through Rapid Distribution Mechanism cannot enter into an isolated child tree if the network is absolutely segregated i.e., the network has no single rooted alternative port. In order to solve this problem, RRSTP has to have a Root Switch Reelection Mechanism. This can be used only as an alternative or a secondary mechanism for converging the network (Hughes et al., 2012).

Bellow are the function of the switch Reelection Mechanism

1. If the root port of a switch fails then:
   i. Set the mode of the switch to inconsistent
2. Start inconsistent mode timer
3. If a switch receives a fresh (valid) BPDU and the consistent flag is clear on its root port then do the step ii) of 1.
4. If a switch in the inconsistent mode receives a fresh BPDU and the consistent flag is set, then it is reversed back to the consistent mode again.

5. If the Inconsistent Mode, the timer of the switch expires and the switch will be in the Inconsistent Mode then the switch must announce itself the Root Switch and it moves into a consistent mode again.

RRSTP Protocol uses Rapid BPDU Distribution Mechanism to enable the switches for very quick and rapid convergence. In other words, RRSTP is expected to outclass all its modern spanning tree protocols in all three key characteristics, especially scalability, reliability and availability. Ethernet can now safely used along with RRSTP even in highly sensitive networks (Hughes et al., 2013).

2.10 DRSTP

DRSTP stands for Delay Rapid Spanning Tree Protocol, which is an extension to RSTP. To make sure that an Ethernet network converge as quick as possible, after a link, port or switch failure, occurs without inducing count-to-infinity into the network. The most important advantage is that we can back track to legacy RSTP/STP switches. The working principle of DRSTP is that it prevents the count-to-infinity problem in mixed environments by forcing the DRSTP switches to postpone transmission of BPDUs. It will be purely done on recently retiring root. This is to make sure that stale information has better BPDUs transmitted by legacy switches will not diminish the whole network. It is noteworthy that period of effective inconsistence for a bridge usually last for only a few hundreds of microseconds in most cases (Stănică et al., 2011).

2.11 Wireshark

Wireshark is a system bundle analyzer. A system bundle analyzer will attempt to catch system parcels and tries to show that parcel information as defined as could be allowed. A user could think about a system bundle analyzer as a measuring gadget used to inspect what's happening inside a system link, much the same as a voltmeter is utilized by a circuit repairman to analyze what's happening inside an electrical link yet at a larger amount, obviously. Previously, such apparatuses were either exceptionally unreasonable, restrictive, or both. Wireshark is maybe one of the best open source bundle analyzers accessible today (Mis et al., 2011; Febrero 2011).

Here are a few illustrations individuals use Wireshark for:

- Network directors use it to troubleshoot system issues
- Network security architects use it to analyze security issues

Alongside these samples, Wireshark might be useful in numerous different circumstances. The accompanying are a portion of the numerous gimmicks Wireshark gives:

- Capture lives bundle information from a system interface.
- Open documents holding bundle information caught with tcpdump/Windump, Wireshark, and various other parcel catch programs.
- Import bundles of content documents holding hex dumps of parcel information.
- Display bundles with exceptionally definite convention data.
- Save bundle information sought.
- Export some or all bundles of various catch record designs.
- Filter bundles on numerous criteria.
- Search for bundles on numerous criteria.
- Colorize bundle showcase focused around channels.
- Create different detail.

2.12 Summary

This chapter explained the networking protocols in general, and briefly the RSTP such as Count to infinity and Forwarding Loops. Where, the next chapter is going to explain the methodology in details.

CHAPTER 3

METHODOLOGY

3.1. Overview

This topic Research methodology discusses the research methodology and the implementation carried out in this thesis. The methodology used in this report is highly qualitative because of its explanatory nature. It will give the researchers an immense knowledge on how, why and under what conditions a count to infinity occurs in RSTP. So, many research work has been carried out by numerous researchers on count to infinity problem in RSTP (through simulation), but this work tackled the same problem in a different way (in real networks). That was conducted to improve the understanding and to give a very clear vision of count to infinity problem, by means of comparing different solutions which has been carried out in the next few topics.

3.2 Research Model

So many researchers have been carrying out research on the recovery time of RSTP in count-to-infinity using simulation. Many of those failed to prove the results in real time experiment. That might be due to the hardware delays and other reasons which will be discussed later. These research works could have been done on emulators like GNS3, but these emulation results will yield exact results only in ideal circumstances because of the operation of the protocol used. It is not only with the protocol used but also there are other factors which influence it. There are lots of challenges to find out the failover performance of RSTP in count-to-infinity in real world life. This research approach has been carried out on different switch manufacturers and network administrators so that it can check the reliability of Ethernet by measuring its precise recovery time. These researches have been carried out in real switches in a laboratory in order to get the most precise results. It has discussed about two test cases naming Test case 1 and Test case 2, which I have carried out 20 times. The first scenario will involve four switches and the second one includes tree topologies which have five switches. The duration of count to infinity has been measured because the network was

designed in such a way that root switch failure occurs, topology change or loss connectivity between switches will result in count to infinity.

3.3 Data Collection Tools

Wireshark, in the past known as Ethereal, is the world's premier system convention analyzer and the standard crosswise over various commercial enterprises and inside numerous instructive establishments. Wireshark advancement flourishes because of the commitments of systems administration specialists over the globe. Wireshark can intuitively search bundle information from a live system or from a beforehand spared catch document. Wireshark's parcel catching is performed utilizing the pcap library; its local catch document configuration is the libpcap design, which is likewise the organization utilized by tcpdump and different instruments. Wireshark's principle window demonstrates three perspectives of a parcel: a synopsis line quickly depicts the bundle sort, the convention field of investment could be demonstrated and dissected in the bit of the window straightforwardly underneath the rundown line, and a hexadecimal dump indicates precisely what the parcel looks like when it goes over the wire. What's more, Wireshark has a few peculiarities that make it novel; for instance, it can amass all the bundles in a TCP discussion and highlight the ASCII information in that discussion. The showcase channels in Wireshark are influential; a larger number of fields are filterable in Wireshark than in other convention analyzers. System heads frequently experience issues picking up a complete learning of the way of the control-plane activity coursing through their system, yet perceivability into control-plane movement is basic to full control over the system. The building design makes it simple to insert gainful devices utilized by system directors who are working in Linux-based situations. The most noteworthy sample of this mix is backing for an incorporated bundle analyzer for the system movement bound to or produced by the Cisco Nexus 7000 Series boss (NotiBala, 2008).

3.4 Setup

The test specification setup consists of Cisco 2960 series Ethernet switches which are upgraded with the IOS 12.2 Firmware. All these switches were initially configured the same with the default RSTP parameters and as follows:

- MaxAge 20s
- HelloTime 2s
- Switch forward delay 15 sec
- Switch priority 32768
- Root switch 4096

The PCs using windows 7 operating system have been connected to switch in the network. A tool called Ethernet packet analyser Wireshark has been running on each PC., the Wireshark software catches only RSTP BPDUs packets and were also analysed. On their arrival they were provided with a timestamp. No user data packet traffic is analysed. After the topology change, the BPDUs on each switch were observed. Hence, new topology information was measured by every switch. It is mandatory to note the highest time consumed by any switch to agree on new topology information that was taken into experiment measurement, as this was the convergence time of the whole network.

- **MaxAge**

The parameter displays the maximum amount of time that BPDU's are stored before being deleted on the root bridge. The length of time after which stored bridge protocol data units (BPDU's) are deleted by the bridge.The max age clock controls the greatest time allotment that passes before an extension port spares its design BPDU data. Every arrangement BPDU holds these three parameters. What's more, every BPDU arrangement holds an alternate time-related parameter that is known as the message age. The message age holds the timeframe that has passed since the root, connect at first began the BPDU. Viably, this quality holds the data on how far a user is from the root span when a user accepts a BPDU.

- **Hello Time**

This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge. The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the hello time. The interval is measured in seconds. Consequently, if the switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds. The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought online, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

- **Switch forward delay**

The parameter displays the time interval between generating and sending configuration messages by the root bridge. If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately. It may take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. A temporary data loop could occur if a topology change is made before all bridges have been notified and that could adversely impact network performance. To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states - listening and learning - before it begins to forward frames. The amount of time a port spends in these states is set by the forwarding delay value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The appropriate value for this parameter depends on a number of variables; the size of your network is a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should specify a smaller value so that the time for a topology change is optimized for minimum data loss

- **Switch priority**

There was a solitary basic crossing tree over all switches. At the point when Vlans began becoming regular for system framework division, STP was improved to incorporate backing for Vlans. Subsequently, the developed framework ID field holds the ID of the VLAN with which the BPDU is related. At the point when the broadened framework ID is utilized, it changes the amount of bits accessible for the scaffold necessity esteem, so the augmentation for the extension necessity worth progressions from 1 to 4096. Accordingly, connect necessity qualities must be products of 4096. It implies 4096*2=8192 (different from 4096..). The developed framework ID quality adds to the extension necessity esteem in the BID to distinguish the necessity and VLAN of the BPDU outline. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost.

- **Root switch**

A root bridge is selected by the bridge priority number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number *in the network is selected as the root bridge. If two or more bridges have the same lowest* bridge priority number, the one with the lowest MAC address is designated as the root bridge. The early execution of STP was intended for systems that did not utilize Vlans. Arranging crossing tree effectively is extremely imperative on any neighborhood. The most essential component to traversing tree is the root span arrangement. Naturally, crossing tree which is running on all switches in the system, will choose a root connect consequently. In most all cases, programmed root span decision is not a decent thought. On the off chance that no other

component of spreading over tree is physically designed on userr system, the root extension ought to certainly be set. Before client design STP, select a switch to be the base of the spreading over tree. This switch does not have to be the most capable switch, however pick the most unified switch on the system. All information stream over the system is from the point of view of this switch. Switches in the appropriation layer frequently serve as the traversing tree root on the grounds that these switches regularly don't join with end stations. Additionally, moves and changes inside the system are more averse to influence these switches.

3.5 Implementation

Test cases for laboratory experiments and their pictorial representation were tested and explained in details below.

3.5.1 Test Case 1:

As it is already discussed the testcase 1 was carried out on a network of 4 switches with the Pcs connected to them to capture RSTP BPDUs. Figure 3.1a just to show a general scenario of the network.

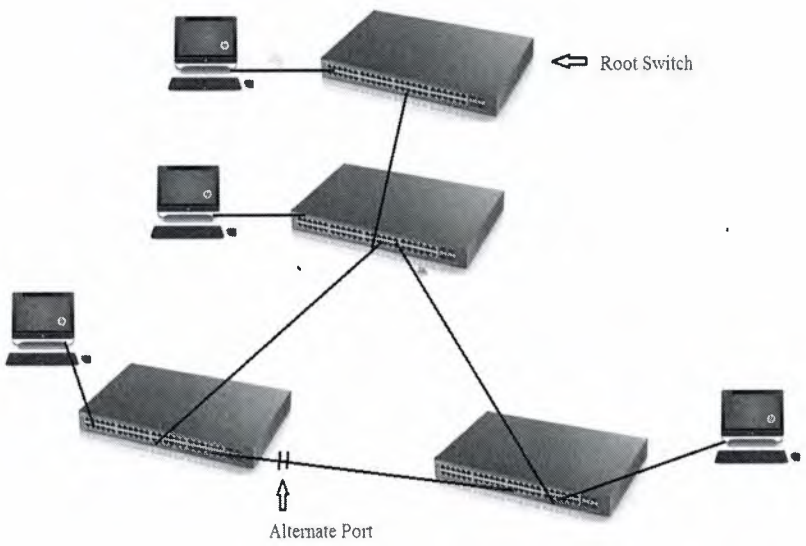


Figure 3.1a: Test Case 1(Before root failure)

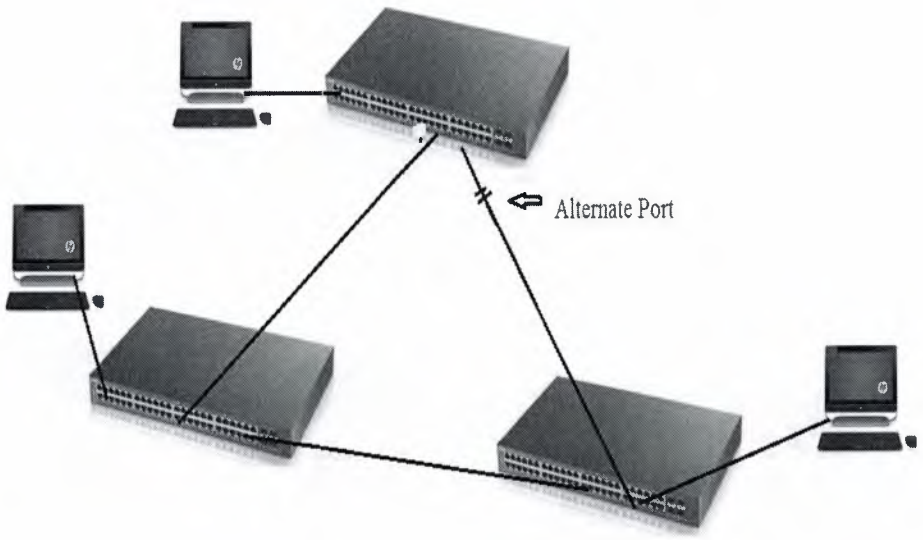


Figure 3.1b: Test Case 1 (After Root Failure)

Figure 3.1b demonstrates the scenario after the root switch failure occured. The aim of this was to show the behavior of the network, that is to say, how a network portion without root switch behaves or when a root switch fails and a cycle exists in the network. This test case 1 has been carried out 20 times in order to measure the correct network convergence time of the. The Wireshark is a wonderful tool to monitor what is going on in each switch. When the topology changes it helps to display every BPDU and information inside the frame. The convergence time is the time consumed by all switches in the network to approve the same correct topology after the end of count to infinity. As shown in Figure 3.1 above, a cycle was created in the network.

3.5.2 Test Case 2:

As discussed earlier, there is a tree topology with five switches in test case 2. Here the root switch failure leads to count to infinity. As the case of the test case 1, this testcase 2 was carried out 20 times after the network is converged as shown in Figure 3.2a, and Figure 3.2b.

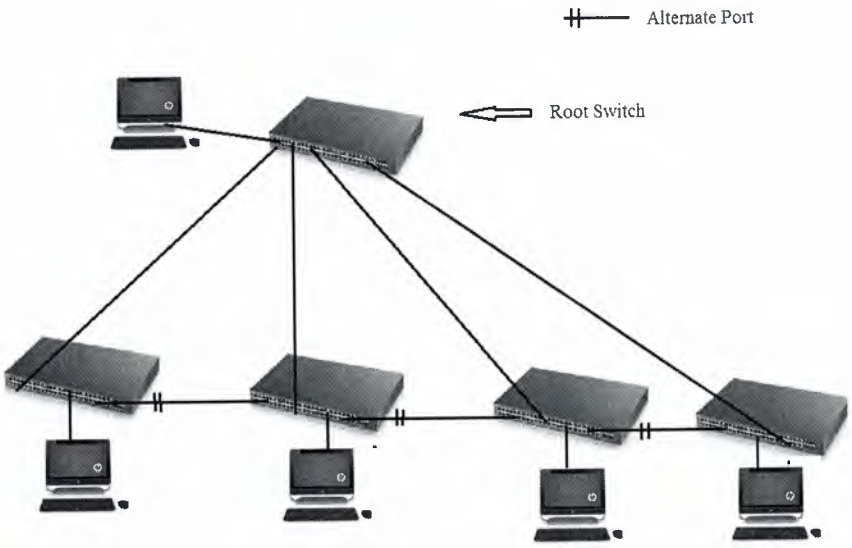


Figure 3.2a: Test Case 2 (before root failure)

Figure 3.2b: Test Case 2 (after root failure)

3.6 Summary

This chapter explained the methodology setup in details. Moreover, the details of the Wireshark which is considered as the control unit for each switch in the network.

CHAPTER 4

RESULTS

4.1 Results for Test Case 1

One of the enormous favorable circumstances in RSTP is the quick union. This is in addition to everything else basically accomplished by utilizing BPDUs mainly between two switches to arrange port states. So in the event that there is another root extension brought into a SPT space, it will first arrange with the straightforwardly joined switch that it is root and has an assigned port. are tossing and arranging with their particular neighbor switches. The entire methodology is much speedier than established crossing tree, however relying upon the topology concise blackouts for some movement may happen. The new attach auxiliary to get to advances straight away so loosing the essential doesnt have an effect. Optional root is designed and primed to expect root span. The issue just arrises when the first essential appropriation returns on line after a rebbot- it is arranged as the root essential so the excess switch switches control once more to the essential. It creates the impression that it is working once more to ordinary STP clocks (tuning in, learning, forwarding) i.e. not exceptionally quick.

Test Case 1 has been carried out 20 times and the results has been displayed in Figure 4.1. As it is known only the highest time taken by any switch to agree on new topology information was taken into experiment measurement. The Y-axis represents the convergence time and the x-axis represents the number of experiments.

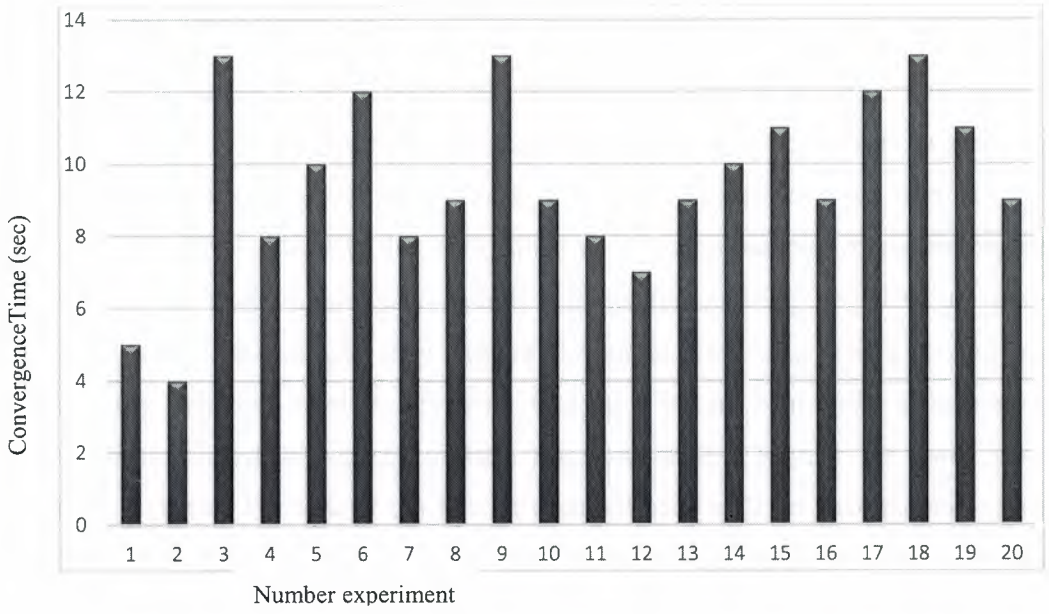


Figure 4.1: Test of Case 1 (After Root Failure)

As noticed in Figure 4.1, STP is moderately abate at recuperating from a disappointment in the system. RSTP was made to lessening this recuperation time. This lessening experiencing significant change time makes it workable for RSTP to recuperate all the more rapidly from disappointments in the system.

STP has four distinctive port states: tuning in, learning, blocking, sending, and incapacitated. This 20-second move time brings about a 20-second misfortune of movement, which is not adequate in a hefty portion of today's systems. Switches running RSTP and switches running STP might be on the same system and cooperate to discover and break circles in the system. Interoperability is attained by the capability of RSTP to distinguish the vicinity of scaffolds running STP and to work in as something to be shared traversing tree mode. At the point when a RSTP extension is joined with a STP connect and accepts STP span convention information units BPDUs, the RSTP Bridge sends just STP Bpdus out the port that is associated with the STP Bridge.

4.2 Results for Test Case 2

In Chapter 3, Figure 3.2b is the pictorial representation after root switch failure. Figure 4.2 displayed the results of 20 times when the convergence time of the network occurred after the root failure for the test case 2. As shown that the convergence time has been reached more than or equal to 20 sec twice in this case. Since such a large number of associations basically acknowledge the switch's producer default settings for crossing tree they are not ideally controlling STP. Associations may not be designing traversing tree to avoid against a coincidentally included rebel switch from making a circle. Numerous associations utilize Cisco's Portfast interface settings to help raise switchports rapidly for ports joined with workstations that we know don't run STP. It does not bode well for have the port uniting with a workstation holding up through the listening and learning states before initiating the interface. Where, in the meantime, Switch 2 accept the part of a root span following its root port fizzled and it has no operational Alternate port. At the point when Port3/Switch 2 accepts the RST BPDU, 802.1w calculation confirms that it is better than the RST BPDU that it can transmit; subsequently, Port3/Switch 2 gets another part; that of a Root port.

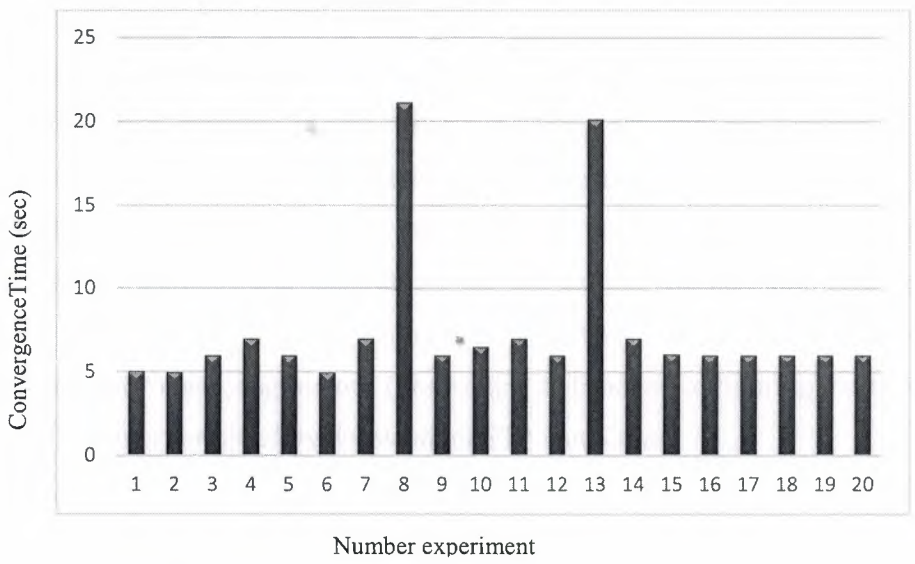


Figure 4.2: Test Case 2 (After Root Switch Failure)

Where, Figure 4.2 describes the port states, RSTP allots and keeps up port parts for all ports in a Spanning Tree space. One of five conceivable parts could be appointed to a port: Root, assigned, substitute, reinforcement, and handicapped. Root and assigned ports are the main ports that energetically take part in the STP by sending edges. Exchange and reinforcement ports are blocked, yet in the event that a disappointment happens in the system, they will quickly change to root or assigned if essential. Exchange and reinforcement ports are fundamental to RSTP's quick recuperation from port disappointments. An interchange or reinforcement port can send activity instantly. Root ports give the least cost way to the root span. Assigned ports give the most minimal expense way from a system portion to the root span. Interchange ports give a substitute way toward the root span. In the event that the root port on the extension falls flat, one of the interchange ports rapidly changes to sending state. Reinforcement ports give a reinforcement way toward the leaves of the traversing tree. In the event that an assigned port on a LAN fragment fizzles, then one of the reinforcement ports on that LAN section rapidly accept the part of assigned port for the portion. Since RSTP keeps up this data, it can all the more rapidly enact an excess way.

4.3 Results Changing the Default After RSTP Parameters

The STP forward deferral parameter indicates the time of time an extension holds up before sending information bundles. In this manner, utilizing the standard forward deferral, union obliges 30 seconds (15 seconds for listening and an extra 15 seconds for realizing) when the default quality is utilized. Particularly, Fast Port Span permits quicker union on ports that are connected to end stations and accordingly do not exhibit the possibility to cause Layer 2 sending circles. Since the end stations can not result in sending circles, they can securely experience the STP state progressions (obstructing to listening to figuring out how to sending) more rapidly than is permitted by the standard STP union time.

Furthermore, Fast Port Span upgrades general system execution in the accompanying ways:

- Fast Port Span diminishes the amount of STP topology change warnings on the system.
- Quick Port Span disposes of unnecessary MAC store maturing that could be brought about by topology change warnings. Spanning gadgets age out the scholarly MAC addresses in their MAC reserves if the locations are unrefreshed for a given time of

time, at times called the MAC maturing interim. At the point when STP sends a topology change notice, gadgets that get the warning utilize the estimation of the STP forward deferral to rapidly age out their MAC stores. For instance, if a gadget's typical MAC maturing interim is 5 minutes, the maturing interim changes incidentally to the estimation of the forward deferral (for instance, 15 seconds) in light of a STP topology change.

On the off chance that an alternate port on that extension expects the Root port part, then the old Root port moves into a disposing of state as it accept an alternate port part. At the point when that port gets chose to the Root port part, RSTP rapidly puts it into a sending state. On the off chance that a port on one extension has a designated part and that port is joined with a port on an alternate scaffold that has an alternate or backup part, the port with a designated part can not be given a root port part until two examples of the forward deferral clock lapses on that port.

In typical STP, the quickened store maturing happens actually when a solitary host goes up or down. Quick Port Span is a framework wide parameter and is empowered naturally. For ports that are not qualified for Fast Port Span, for example, ports joined with other systems administration gadgets, the gadget naturally utilizes the ordinary STP settings. An STP configuration BPDU has been gained on the port, in this manner demonstrating the vicinity of an alternate scaffold on the initially, there is the setup of some default RSTP parameters and the convergence time was measured in both topologies in count to infinity as shown in Figure 4.3.

4.3.1 MaxAge

Figure 4.3 shows the MaxAge parameter was changed from 6s to 40s, with respect to the convergence time

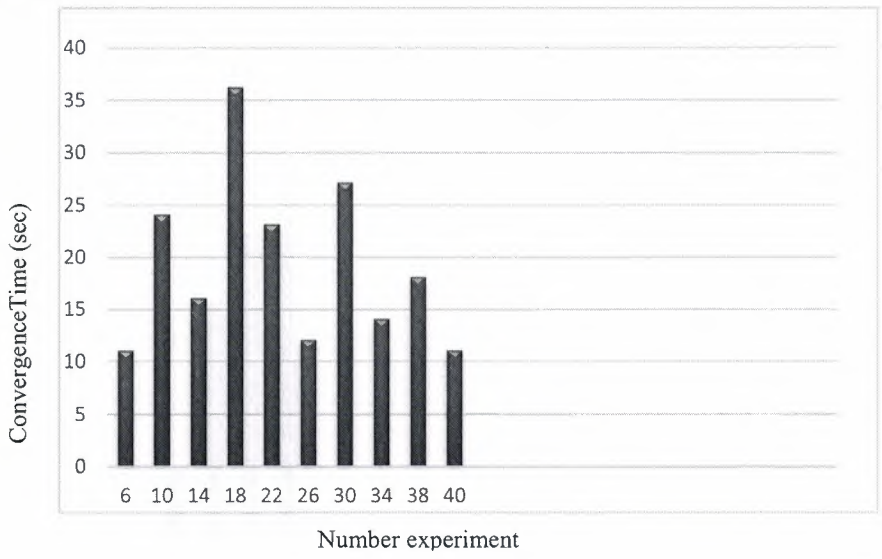


Figure 4.3: After Changing Default Parameters-MaxAge

In Figure 4.3, on the off chance that a switch quits getting Hellos, it implies that there is a disappointment in the system. The methodology obliges the utilization of 3 STP clocks. Max age – greatest period of time a BPDU might be put away without getting an upgrade. This is critical on the grounds that regularly just following five minutes a passage is matured out from the MAC location table of the switch and the system gadgets could be inaccessible for up to 5 minutes. This is known as a dark gap on the grounds that edges could be sent to a gadget, which is no more accessible.

4.3.2 hellotime

Figure 4.4 shows the variation when hellotime which is the parameter was changed between 2s to 10s seconds, a sharp increase in the convergence time is clearly noticed.

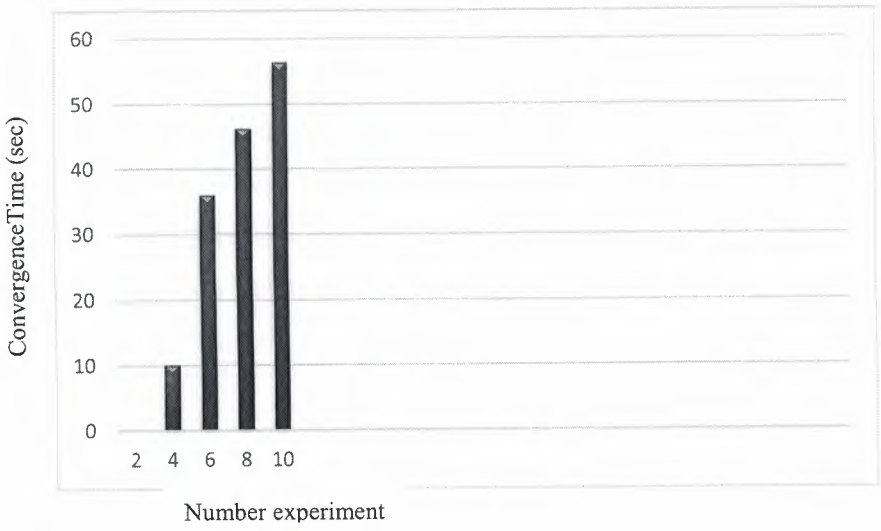


Figure 4.4: After Changing Default Parameters- Hellotime

4.3.3 Forward Delay

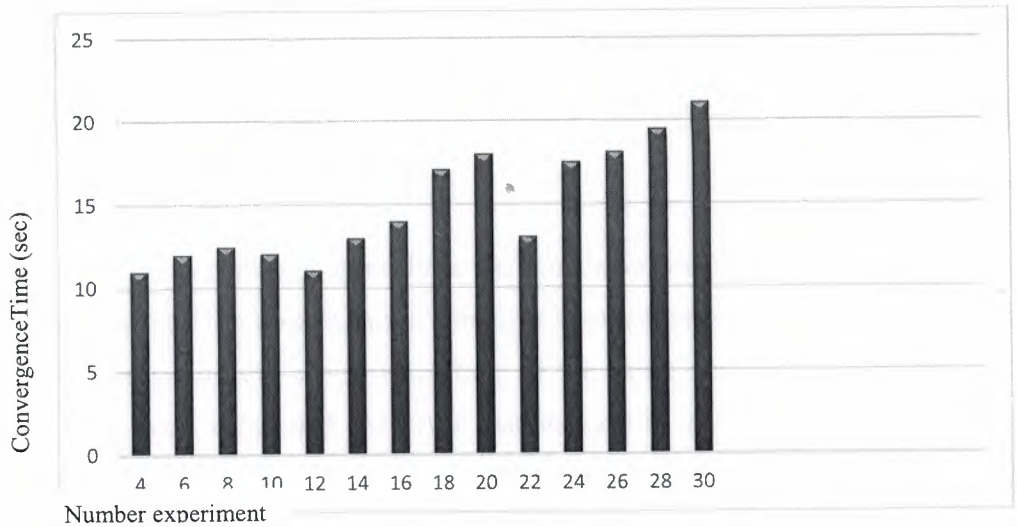


Figure 4.5: After Changing Default Parameters-Forward Delay

Figure 4.5 has been plotted for the test case 2, after changing the default parameter of forward delay.

RSTP calculation chooses Port7 as the assigned port while Port8 turns into the Backup port. All different ports are given an assigned port part with disposing of states. The port stays in tossing state. Port3 turns into the Root port for the scaffold; all different ports are given an assigned port part with disposing of states. The port is likewise given an Alternate port part, and stays in disposing of state. Ports on all the scaffolds in the topology with assigned port parts that accepted RST BPDUs with concurred banners go into sending states right away. Be that as it may, assigned ports that did not get RST Bpdus with concurred banners must hold up until the forward deferral clock lapses twice on those ports. The whole RSTP topology unites in under 300 msec and the key network is built between the assigned ports and their joined root ports.

As discussed all the three parameters have been changed and the results were taken and tabulated in Table 4.1.

Table 4.1: Comparison of Parameter Values

Parameter	Default parameter value	Change in parameter value
MaxAge	20s	6s to 40s
HelloTime	2s	2s to 10s
Forward delay	*15s*	4s to 30s

Note : All values in seconds

To have a better understanding, analysis were made on when a count to infinity problem has been encountered with respect to the parameters passed during the experiment. As discussed above, by measuring the convergence time of the entire network the duration of count-to-infinity has been calculated. MaxAge parameter has not made any difference in the convergence time in our experiment. When changing the value of hellotime, it affects or increases the convergence time. Also, when the value of the forward delay changes, an increase in convergence time is noticed.

4.4 General Results

From the test case 1 and test case 2, the researcher conducted experiments and plotted the results in Figuer 4.1 to 4.5. In the test case 1, it was noticed that the average time taken by a network to converge is 9.5 seconds. This is not the same in all the cases, as it differs in every experiment. In a time it was measured as 4 seconds and in another it was measured as 13 seconds. In the case of a large and complex network running sensitive applications, it may take a few minutes to recover. In the test case 2, it was 7.5 seconds that is the average convergence time for the network. Also in one of the experiments the convergence time was 4.97 seconds.

The above results can be an ideal situation in a network, when fresh BPDUs reached on each switch without even allowing any stale information to spread in the network. From the experiment convergence time can also be noticed that the was 20 seconds and 21 seconds on two occasions.

This situation has occurred when the count to infinity was at its highest level, and spreading stale BPDUs. This is one of the worst case scenario for any type of network. Then the parameters have been changed from the default values and noted the results in a graph. When the RSTP parameters was changed, the convergence time has been noted that also increased with respect to the increase of the forward delay. For instance, from the figuer we see that I had set the forward delay at 30, then the convergence was 21 seconds and when the forward delay was set to 22 then the convergence time was 13 seconds. But the MaxAge parameter hasn't made any difference in the convergence time in our experiment. But there is a mix in the output.

In the experiment, as shown in the Figuer, it was more influenced by stale topology information because of MaxAge changes. From the research done, it is found out that it can decrease the count to infinity in large networks thereby decreasing the MaxAge, but it will also reduce the spanning tree diameter. From the above figures, it can also notice that, when MaxAge was 18, the convergence time recorded was 36 seconds. There is a dramatic increase in convergence time when there is increase in hellotime.

4.5 Results After Changing Topology in Test Case 2

The experiments shown in this thesis have proven that the reliability of the network has been affected because of count-to-infinity problems, the reason of Wireshark can read and compose catch documents in its characteristic record design, the libpcap form, which is utilized by numerous other system catching devices, e.g. tcpdump. Notwithstanding this, as one of its qualities, Wireshark can read/compose records in numerous diverse record organizations of other system catching instruments. The wiretap library, created together with Wireshark, gives a broadly useful interface to peruse/compose all the record forms. All these experiments were carried out in a simple network. By measuring the convergence time of the entire network the duration of count-to-infinity has been calculated. When compared to STP, RSTP has shown improvement in the convergence time of the network. In some cases of my experiment, I have noticed that the convergence time has been just 4 to 5 seconds, even though the count-to-infinity problem occurs.

But in some of the cases it was more than 35 to 55 seconds to converge. The convergence time may be very high, in case of very large networks. This is because in the large network there will be more redundant path and time taken by the stale to expire will be more.

4.5.1 Switch 1

In test case 2, after root switch fails, every switch will act as the root switch. By assuming that they have an alternative path to non-existing old root switch, they will use the cache information on its alternative port. As discussed brefore, the root switch priority in all the experiments was set to 4096. Noticing that the root switch value of switch 2 has been changed from 4096 to 32768. Then by wrongly assuming that its alternative port has a path to old root switch (which no longer exists) and with the value of 4096 it will cache information from its alternative port. At last and after 12 seconds, the root switch with the value of 32768 has been approved by the whole network as shown in Figure 4.6.

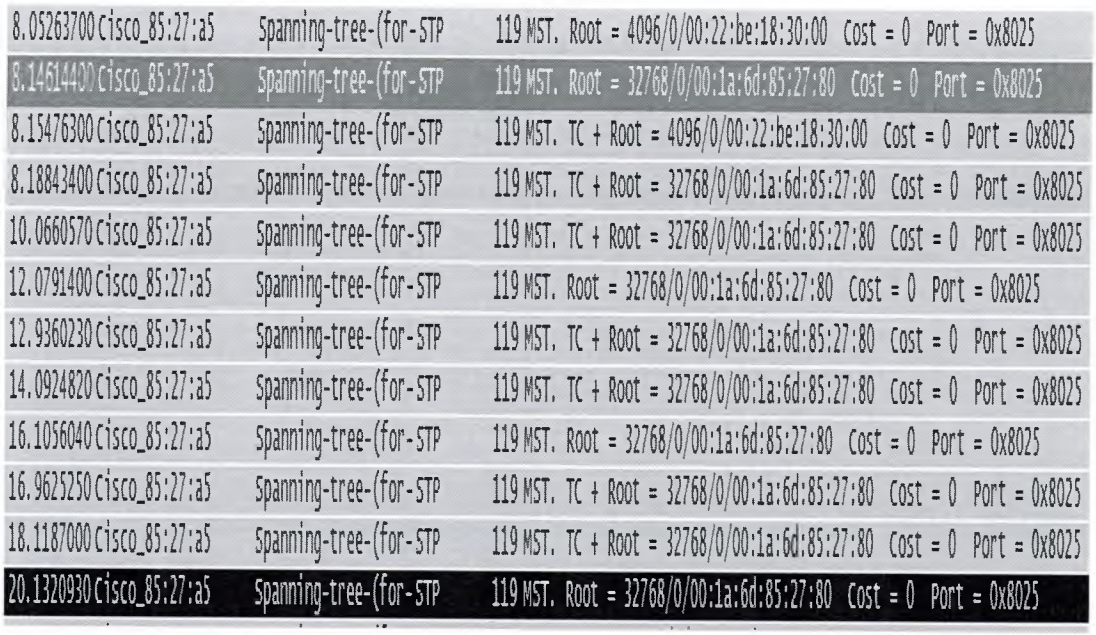


Figure 4.6: Test Case 2 - Packets Captured by WireShark 1

Figure 4.6, shows the experiment number 14 in test case 2 by switch 1, showing the packets which are captured by Wireshark. This shows the count to infinity problem across the whole network.

4.5.2 Switch 2

The root switch has changed many times before the entire network converged in 20 seconds as shown in Figure 4.7.

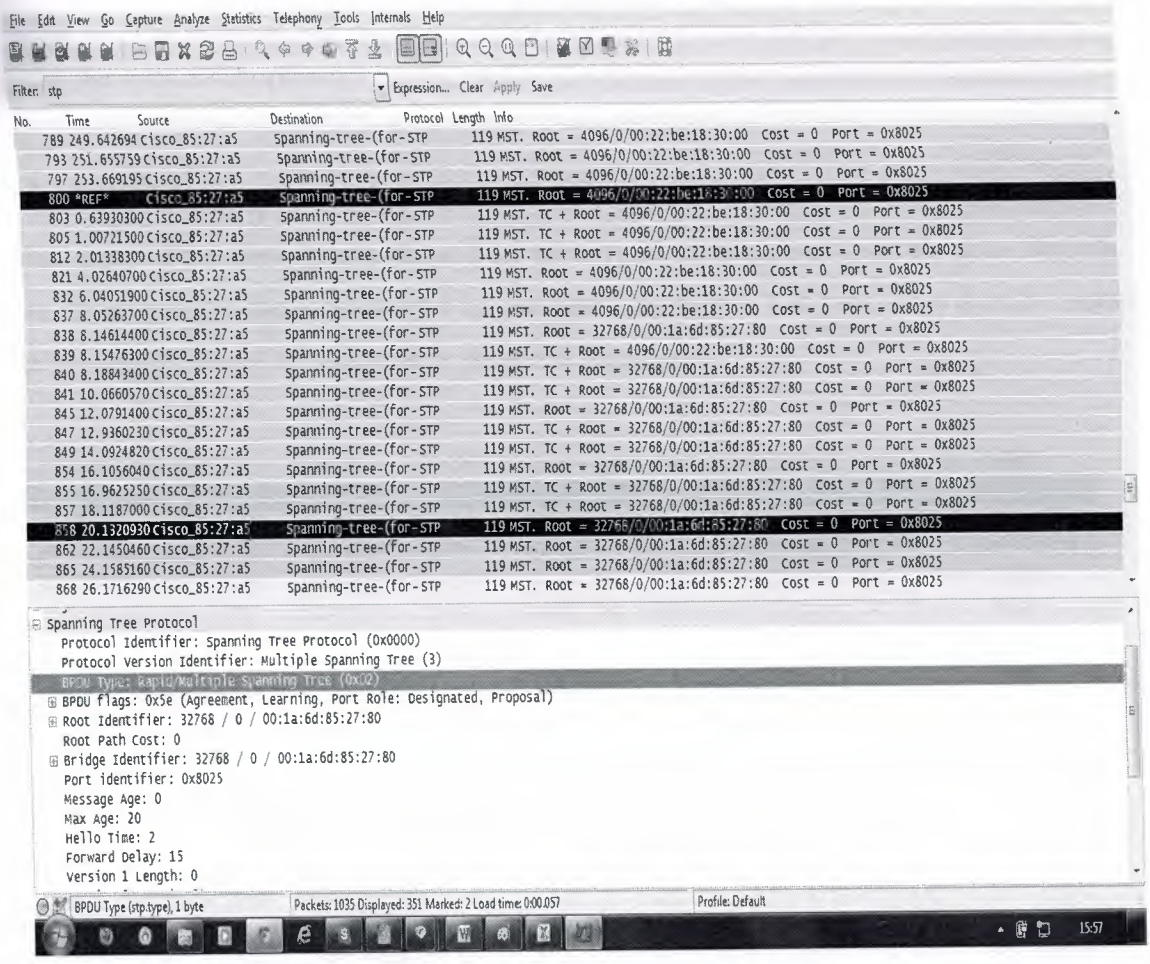


Figure 4.7: Test Case 2 - Packets Captured by WireShark 2

Figure 4.7 explaines the forceful that worth for the max-age parameter and the forward deferral can prompt an exceptionally temperamental STP topology. In such cases, the misfortune of a few BPDUs can result in a circle to show up. An alternate issue that is not well known identifies with the measurement of the scaffold system. The moderate default values for the STP clocks force a greatest system measurement of seven. This greatest system width limits how far from one another extensions in the system might be. For this situation, two unique extensions can't be more than seven bounces far from one another. Where, on the off chance that a switch with a lower span necessity than that of the current dynamic root span connects to a Portfast-arranged port or interface, it might be chosen as the root span. This

change of root scaffold can antagonistically influence the dynamic STP topology and can render the system suboptimal.

4.5.3 Switch 3

Also, some of the experiments showed the severity of the situation. From the done analysis, it can undertand that the experiment 9 of test case 2 by switch 3, it took more than 21 seconds for the entire network to converge as shown in Figure 4.8.

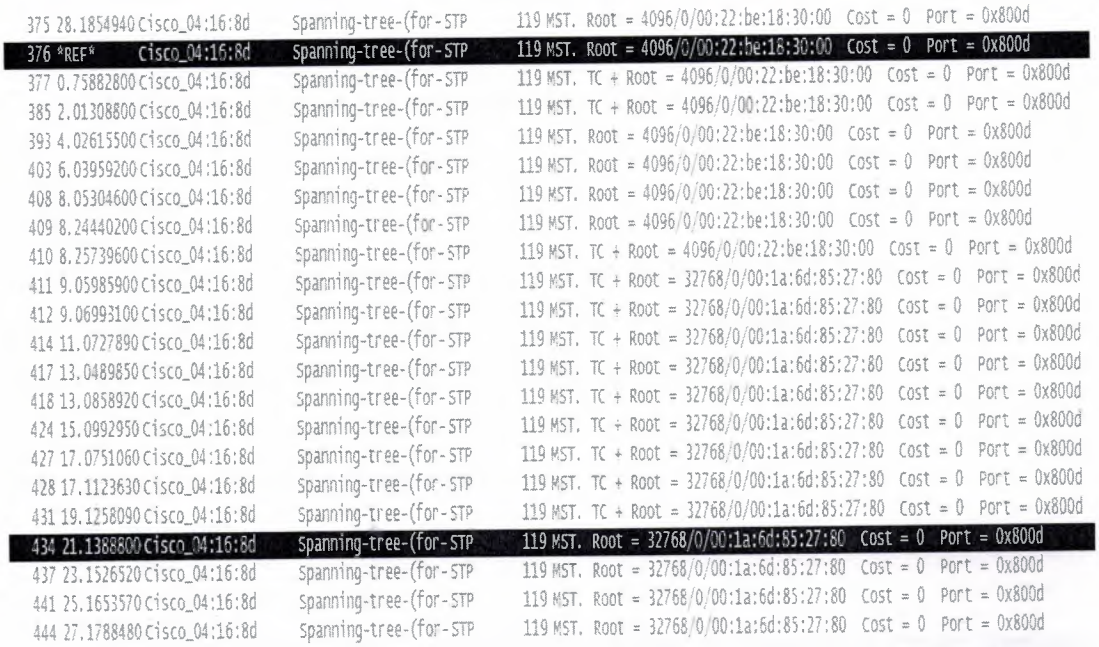


Figure 4.8: Test Case 2 - Packets Captured by WireShark 3

Figure 4.8 describes the parcel catch will show the points of interest of every bundle as they were transmitted over the remote LAN. The top board of the window distinguishes every bundles source and end hubs, convention actualized, and data about every parcel. Customer can select a particular bundle to show more points of interest. The center board shows data about this parcel, and user can pick a particular field of the bundle, and the substance of that field is shown in hex and ASCII design in the bottom board. Thus, it can break down the

stream and view each one field including information field payloads of all bundles. In Figure 4.8, at the point when designing a Wireshark catch point, client can copartner a filename. At the point when the catch point is enacted, Wireshark makes a document with the indicated name and composes bundles to it. On the off chance that the document exists when the record is cohorted or the catch point is enacted, Wireshark inquiries concerning whether the record might be overwritten. On the off chance that the end of the Wireshark composing methodology is full, Wireshark comes up short with fractional information in the document. Where, customer must guarantee that there is sufficient space in the document framework before beginning the catch session. Customer can decrease the obliged storage room by holding just a portion, rather than the whole parcel. Regularly, client does not oblige points of interest past the initial 64 or 128 bytes. The default conduct is to store the whole parcel.

4.5.4 Switch 4

In most of the cases, new information was quick enough to beat the stale information, then count to infinity will not occur. Here the occurencing probability is one out of hundred cases. It was noticed that, the RSTP took less than seven seconds to converge, when the root switch is connected again to the network. Below is shown in Figure 4.9 where the desired convergence time from RSTP after a topology change.

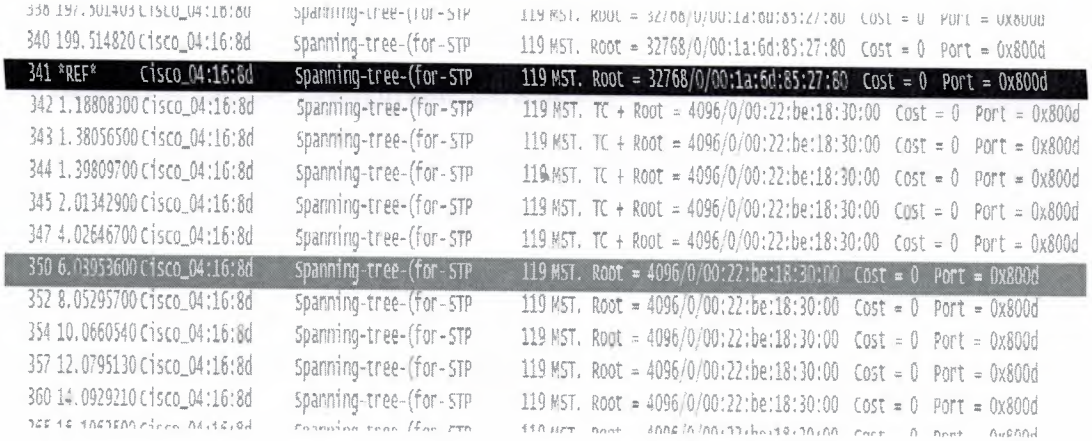


Figure 4.9: Test Case 2 - Packets Captured by WireShark 4

From Figures 4.1 and 4.2, it is noticed that RSTP was designed in such a way that it should not more than 6 seconds to converge. But in case of count to infinity scenario, its performance is not reliable. It is noted that the average convergence time in test case1 is 9.5 seconds and in test case 2 it is 7.5 seconds. Which yields that at the point when troubleshooting a remote LAN, use Wireshark to catch the parcels, and investigate the stream of bundles to check whether customer can recognize the issue. A remote 802.1x customer gadget on the remote system, for instance, may seem associated with the remote system, however the client is not ready to get to system assets. In the wake of inspecting the bundle follow, it is demonstrated that by watching the VLAN labeling in the proper bundles, that the customer gadget is associated with the visitor organize rather than the corporate system. This would indicate an issue with the customer's 802.1x supplicant. Where, remote bundle examination obliges a strong understanding of the 802.11 standard and different conventions. Likewise, a few sellers include exclusive capacities that may cause disarray when investigating the stream of bundles. Despite the fact that this may make life troublesome when troubleshooting, focus on considering the bundle follow caught by Wireshark to take in the subtle elements of how remote systems function. Obviously this implies that customer will likely need to delve into the guts of the 802.11 benchmarks and IETF determinations, which characterize a significant number of the non-802.11 bundles. In the wake of catching parcels, click the Analyze menu and pick Options. A window will create the impression that may demonstrate slips, which customer can research as the conceivable issue.

4.6 Benefits of the five configurable parameters

RSTP gives quick merging of the spreading over the tree. MSTP, which utilizes RSTP to give fast joining, empowers Villains to be gathered into a traversing tree case, accommodates various sending ways for information movement, and empowers burden adjusting. It enhances the issue tolerance of the system on the grounds that a disappointment in one occasion sending way does not influence different occasions sending ways. The most well-known introductory sending of MSTP and RSTP is in the spine and conveyance layers of a Layer 2 exchanged system; this arrangement gives the profoundly accessible system needed an administrative nature.

- Root port-gives the best way (least cost) when the switch advances parcels to the root switch.
- Designated port-interfaces with the assigned switch, which causes the most reduced way cost when sending bundles from that LAN to the root switch. The port through which the assigned switch is connected to the LAN is known as the assigned port.
- Backup port—goes about as a reinforcement for the way gave by an assigned port at the leaves of the spreading over the tree.

A port with the root or an assigned port part is incorporated in the dynamic topology. A port with the interchange or reinforcement port part is avoided from the dynamic

Rapid Convergence

The RSTP accommodates fast recuperation of integration after the disappointment of a switch, a switch port, or a LAN. It gives fast meeting to edge ports, new root ports, and ports associated through point-to-point interfaces as takes after:

- Root ports-If the RSTP chooses another root port, it obstructs the old root port and promptly moves the new attach port to the sending state.
- Point-to-point joins If you join a port to an alternate port through a point-to-point join and the nearby port turns into an assigned port, it arranges a fast move with the other port by utilizing the proposal-Ascension handshake to guarantee a circle free topology.

In the wake of accepting switch Bs assertion messages, Switch an additionally quickly moves its assigned port to the sending state.

Switch C chooses the port associated with Switch B as its root port, and both closures promptly move to the sending state. As the system merges, this proposal-Ascension handshaking advances from the root around the leaves of the crossing tree.

User can override the default setting that is dictated by the duplex setting by utilizing the spreading over tree connection sort interface setup .

Synchronization of Port Roles

At the point when the switches associated with a point-to-point connection are in ascension about their port parts, the RSTP quickly moves the port states to sending.

Processing BPDU Information

On the off chance Superior that a port gets predominant root data lower span ID, lower way cost, et cetera than presently put away from the port, the RSTP triggers a reconfiguration. The new root port obliges double the forward-postponement time to move to the sending state. On the off chance that the predominant data gained on the port causes the port to turn into a reinforcement or exchange port, RSTP sets the port to the blocking state however does not send the understanding message. The assigned port keeps sending Bpdus with the proposal banner set until the forward-deferral clock terminates, at which time the port moves to the sending state.

Processing Inferior BPDU Information

In the event that an assigned port gets a substandard BPDU higher extension ID, higher way cost, et cetera than right now, put away from the port with an assigned port part, it quickly answers with its data.

4.7 Summary

Though it is not significantly high, when compared with the expected one, in some experiments it was 2 to 3 times higher than the average time. By using BPDUs captured by Wireshark, the count to infinity was noticed in each experiment. By adding more redundant links, the count to infinity also increases with respect to the convergence time. Likewise, when the network diameter gets bigger, count to infinity also increases.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This thesis provided a clear picture on count-to-infinity problem in real time networks in the field of contrasting the throughput exchanged with the ends, and RSTP which is a change to the first STP acquainted with abatement the measure of time needed to respond to a connection or scaffold disappointment. The Spanning Tree Protocol is vital for circle evasion to make circle free ways. The count to infinity problem has been investigated in the laboratory environment. By changing the Hello time and forward delay parameters, it is found that better respond was obtained.

5.2 Recommendations

In this thesis, the existence of count to infinity problem has been proved in real time environment to expand the topologies with more switches and links as much as going to simulate these topologies using OPNET software. In the future work, more researches are going to be on different approaches on how to overcome the problems with RSTP. After connecting complete system with the android so to obtain a Dialogic system. Where, Dialogic system going to include multimedia work for smartphones.

REFERENCES

Balchunas A., (2009). Spanning Tree Protocol. *Spanning Tree Protocol, 1*(21). Retrived April, 11, 2012 from http://www.routeralley.com

Baldi M., Nicoletti P., (2002). Switched LAN, McGraw-Hill, ISBN 88-386-3426-2.

Becchetti, L. (2009). Computer Networks II: RIP - Routing Information Protocol. la sapienza university. Dipartimento di Informatica e Sistemistica.

CAIDA. (2013). A historical view of the evolving internet topology. Retrive April, 1, 2014 from http://www.caida.org/research/topology/as_core_network/historical.xml

Cherkasova, L., Kotov, V. E., & Rikicki, T. (1995). *Evaluation of Network Topologies*. Hewlett-Packard Laboratories, Technical Publications Department.

Contemporary Controls. (2011). Understanding Ethernet Switches and Routers. Essentials. Retrive April, 1, 2011 from http://www.ccontrols.com/pdf/Essentials0411.pdf

Cox L., A. (2011). An Ethernet watchdog. Rice University. Retrive April, 1, 2014 from report.rice.edu/sir/faculty.detail?p=B90CF624C8196C17

Dimitropoulos, X., Krioukov, D., Vahdat, A., & Riley, G. (2009). Graph annotations in modeling complex network topologies. *ACM Transactions on Modeling and Computer Simulation*, *19*(4), 17.

Elmeleegy K., Cox, L. A., & Ng, T. S. E. (2007). EtherFuse: An Ethernet Watchdog. *SIGCOMM'07,* August 27–31, 2007, Kyoto, Japan. Copyright 2007 ACM 978-1-59593-713-1/07/0008.

Faur A., Milesco G., (2009). STP/RSTP implementation in Lisa. University of Bucharest. Automatic Control and Computers Faculty. Computer Science Department.

Febrero B., M., (2011). Traffic Analysis with Wireshark. INTECO-CERT. Instituto Nacional de Tecnologías de la Comunicación – INTECO. Retrive April, 1, 2014 from http://www.inteco.es

Galea, M., (2010). Rapid Spanning Tree in Industrial Networks. RuggedCom Inc. - Industrial Strength Networks Woodbridge, Ontario, Canada.

.

Ganesh, D, Venkata R., & Prasad, V. (2010). An Effective Solution to Reduce Count-to-Infinity Problem in Ethernet. *IJCSI International Journal of Computer Science Issues*, *7*(4), 1694-0784.

Golestanian, M., & Ghazizadeh, R., (2013). A New Approach to Overcome the Count to Infinity Problem in DVR Protocol Based on HMM Modelling. *Journal of Information Systems and Telecommunication*, *1*(4).

Hughes, M., Pels, M., & Michl, H., (2012). Internet Exchange Point "Wishlist". EIX wishlist. Version 4.0.0.

Hughes, M., Pels, M., & Michl, H., (2013). Internet Exchange Point "Wishlist". EIX wishlist. Version 4.0.4.

Ismaeel, A., Y. (2012). New Technique For Proposing Network's Topology Using GPS and GIS. *International Journal of Distributed and Parallel Systems, 3*(2), 53-65.

Jadron, E., Hunorová, L. (2013). Empowering the Internet Generation. *LCNA - Local Cisco Network Academy. Network Cisco Academy,* 1 – 1669.

Jauregui, D., Wang, B., & Chen, R. (2011). Power Loss Calculation With Common Source Inductance Consideration for Synchronous Buck Converters. *Texas Instruments. Application Report. Power Loss Calculation With Common Source Inductance Consideration for Synchronous Buck Converters.*

Kaur, M. (2009). Computer Network Topologies. Retrive April, 1, 2014 from http://www.eazynotes.com/notes/computer-networks/slides/network-topologies-handouts.pdf. professormaninder@gmail.com.

Kharagpur, (2006). Broadcast Communication Networks. Version 2 CSE IIT. Retrive April, 1, 2014 from http://nptel.iitk.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Computer%20networks.

Kohli, G., (2005). An Investigation into the Use of B-Nodes and State Models for Computer Network Technology and Education. *A thesis submitted in fulfilment of the requirement for the award of Doctor of Philosophy*. Faculty of Computing, Health and Science Edith Cowan University.

Konkoth, B., (2000). Understanding Basic Network Structure. Retrive April, 1, 2014 from www.mecps.org/konkoth/Lesson_1_Understanding%20Basic%20Network.

Koymans, C. P. J., (2008). (Rapid) Spanning Tree Protocol A simple bridge loop. *Informatics Institute University of Amsterdam.*

Lapukhov, P. (2010). Understanding STP and RSTP Convergence. *Understanding STP and RSTP Convergence Petr Lapukhov, CCIE#16379.*

Meador, B. (2008). A Survey of Computer Network Topology and Analysis Examples.

Meyer, P., Cokelaer, T., Chandran, D., Kim, K. H., Loh, P. R., Tucker, G., ... & Saez-Rodriguez, J. (2014). Network topology and parameter estimation: from experimental design methods to gene regulatory network kinetics using a community based approach. *BMC Systems Biology*, *8*(1), 13.

MIS, H., A., McKelvey. (2011). Wireshark-Looking into the Packet. Blacks in Technology. Retrive April, 1, 2014 from http://www.wiresharktraining.com.

Peter R. E. (2014). STP – Spanning Tree Protocol. *Indigoo.com.*

Pfenning, F., (2010). Lecture Notes on Spanning Trees. Lecture 24. 15-122: *Principles of Imperative Computation.*

Phil, M., Kiruthika, R. (2010). An Exploration of Count-To-Infinity Problem In Networks. *International Journal of Engineering Science and Technology. 2* (12), 7155-7159.

Prakash Pal, G., Pal, S., (2013). Vertual Local Area Network (VLAN). *International Journal of Scientific Research Engineering & Technology*, *1*(10), 006-010.

Tangmunarunkit, H., Govindan, R., Jamin, S., Shenker, S., & Willinger, W. (2002). Network topology generators: Degree-based vs. structural. *ACM SIGCOMM Computer Communication Review*, *32*(4), 147-159.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *Communications Surveys & Tutorials, IEEE*, *15*(4), 2046-2069.