ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)

Tracking The Effects of Loops in A Switched Network Using Rapid Spanning Tree Network

[I]Ufoaroh S.U, [II]Obi Chukwumaobi .O, [III]Oranugo C.O
[I,II,III]Dept. of Electronics and Computer Engineering. Nnamdi Azikiwe University, Awka

Abstract
Networking is an all important aspect and an indispensable tool in communication. Ethernet is a family of technologies that provides data link and physical specifications for controlling access to a shared network medium. It has emerged as the dominant technology used in local area networking. It provides a simple and low cost solution at high bandwidth for access to the different kind of Networks. The Institute of Electrical Electronics Engineers (IEEE) develops the protocols and standards used for Ethernets. This work presents a system that is capable of providing a mechanism for disabling redundant links in a switched network. This project aims at the implementation of a low cost but efficient and flexible open standard protocol, used in a switched environment to create a loop-free logical topology. It is designed in such a way to achieve faster convergence time through the use of acknowledged communications between devices rather than the passive method used by Spanning Tree Protocol (STP). Thus this system proposes a continuous, real time, speedy recalculation and reconfiguration of the Spanning tree which ensures complete elimination of loops in an Ethernet Switched Network as well as boosts the quality of the network; minimize excessive downtimes and decreases recovery time.

Keywords
Ethernet, IEEE, Spanning tree protocol (STP), Loops, Convergence, Recovery time, Network

I. Introduction

Modern enterprises rely on their networks for their existence. The network is the lifeline of many organizations. Network downtime translates to potential disastrous loss of business, income, customer confidence and productivity. Due to the increase in the number of people on the network (Internet), and the immense amount of simultaneously requested services, it is pertinent that protocol has to be fished out which not only decreases the cost function as described above but also minimizes congestions and conflicts in Switching Network, this then brings us to traffic loops which are the fundamental problem in Ethernet switched Networks. This causes problems such as unicast duplication and multicast frame multiplication. In Computer networking, Unicast transmission is the sending of messages to a single network destination identified by a unique address. When two or more Bridges are connected in a loop they multiply multicast frames, sending them round and round until the network becomes clogged. A loop occurs in a computer network when there is more than one layer 2 (OSI model) path between two endpoints (e.g. multiple connections between two network switches or two ports on the same switch connected to each other). The loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast message thereby flooding the network. The effects of loop to an Ethernet switched network are the reduction in bandwidth, clogs up memory and causes loss of packet data. Thus this work is effectively designed to present Rapid Spanning Tree Protocol (RSTP) as a tool for solving the problem of loops in Ethernet Switched Network by establishing redundant path/link to a particular destination in switched network and also presents a simulation Model using Packet Tracer Software to establish redundant path from source to destination and also to explore RSTP algorithm and present the benefits over STP algorithm in Switched Network.

II. Background Study

When IEEE developed the original 802.1d Spanning tree protocol, recovery time of 1 to 2 minutes was acceptable. Today layer 3 switching and advanced routing protocols provide a faster alternative path to destination. The need to carry delay-sensitive traffic, such as voice and video requires that switch network converge quickly to keep up with the new technology [1]. From [2], in 2001, the IEEE introduced RSTP as 802.1W. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backward compatible with standard STP. RSTP defined in IEEE 802.1W significantly speeds up the recalculation of the spanning tree. Unlike port fast, uplink fast, backbone and backbone fast. RSTP is not proprietary; RSTP requires full duplex, point to point connection between switches to achieve the highest reconfiguration speed. Reconfiguration of the spanning tree by RSTP occurs in less than 1 second, as compared to 50 seconds in STP [3]. RSTP eliminates the requirement for features such as port fast and uplink fast, RSTP can revert STP to provide services for legacy equipment. The standard IEEE 802.1D incorporates RSTP and obsoletes the original STP standard [4]. To speed up the recalculation process RSTP reduces the number of port states to three states- Discarding, Learning, and Forwarding

Discarding: It is the state of a port in an RSTP network where the server does not send a reply. A solid amber LED signifies in the switch that discarding is in process.

Learning: One of the states that a port cycles through when a switch powers on an RSTP network. The switch uses information learned to forward a packet.

Forwarding: It is the process of sending a frame out of a port towards the destination by way of an inter-networking device. Examples of devices that forward frames are Hosts, Repeaters and Routers.

In other to speed up the recalculation process, these three port states outlined above replace the five port states (blocking, learning, forwarding, listening, and disabled) that where been used before in STP [5]. RSTP also introduces the concept of active topology. All ports that are not discarding are part of the active topology and will immediately transit to the forwarding state. According to [6], in the case of STP, when a switch powers on, each port cycles through a series of four states: blocking, listening, learning and forwarding, a fifth state, disabled indicates that the administrator has shut down the switch port. As the port cycles through these states,

the LED on the switch changes from flashing orange to steady green. It takes as long as 50 seconds for a port to cycle through all of these states and be ready to forward the frames [7]. When a switch powers on, it first goes into blocking state to immediately prevent the formation of a loop. It then changes to listening mode, so that it receives Bridge Packet Data Units (BPDU) from the neighbor switches. After processing this instruction, the switch determines which port can forward frames without creating a loop. If the port can forward frames, it changes to learning mode and then forwarding mode. Access ports do not create loops in a switched network and always transit to forwarding if they have a host attached. Trunking ports potentially create a loop network and transition to either forwarding or blocking state. From [8] view that for STP to function, the switches in the network determines a switch that is the focal point in that network. STP uses the focal point called a Root Bridge or Root switch to determine which ports to block and which ports to put into forwarding state. A Root Bridge is a designated packet forwarding device in a spanning tree implementation that receive topology information and notifies all other bridges or switch in the network when topology changes are required. A root bridge prevents loops and provides a measure of defense against link failure. The Root Bridge sends BPDU (Bridge packet data units) containing network topology information to all other switches. This information allows the network to reconfigure itself in the event of a failure. There is only one Root Bridge on each network and it is elected based on the Bridge ID (BID). The Bridge priority value plus MAC address creates the BID. Bridge priority has a default value of 32768. If a switch has a MAC address of AA.11.BB.24.CC.33, The BID for that switch would be 32768: AA: 11: BB.24.CC.33.

The selection of the Root Bridge is based on the lowest BID value. Since switches typically use the same default priority value, the switch with lowest MAC address becomes the Root Bridge. As a switch powers on, it assumes that it is the Root bridge and sends out BPDUs containing its BID, for example if switch A advertises a root ID that is a lower number than switch B, the switch B stops the advertisement of its root ID and accepts the root ID of switch A. Switch A is now the Root bridge, as shown in fig 2.2 below.

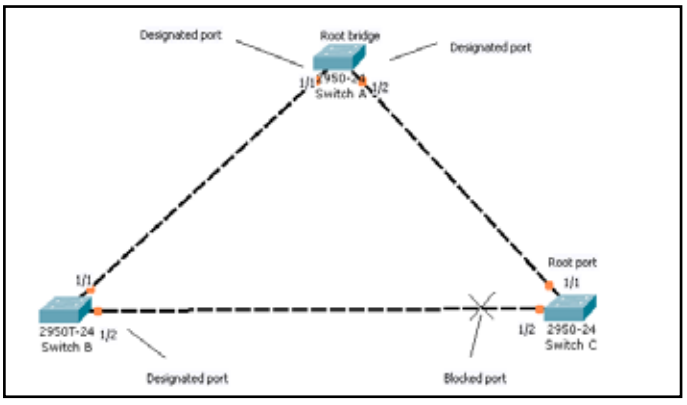

Fig 2.0: Shows the root bridges and the designated ports

RSTP designates three types of ports: root port, designated port and blocked port. The port that provides the least cost path back to the root bridge becomes the Root port. Switches calculate the least cost path using the bandwidth cost of each link required to reach the root bridge [9]. A designated port is a port that forwards traffic towards the Root Bridge but does not connect to the least cost path. A blocked port is a port that does not forward traffic. According to [10], it derives a Rapid Spanning Tree Protocol as a mechanism for disabling redundant links in a switched network and it is an open standard protocol used in a switched network or environment to create a loop-free logical topology.

In STP terminology, the term bridge is frequently used to refer to a switch, for example, the Root Bridge is a primary switch or focal point in the STP topology. The Root Bridge communicates with other switches using Bridge Protocol Data Units, BPDU are frames that multicast every 2 seconds to all other switches. BPDU contains information such as Identity of the source switch, Identity of the source port, Cumulative cost of path to Root Bridge, Value of aging timers and of the 'hello' time.

III. Review of Related Works

A. Multilayer Switching

From the work in [11], traditionally networks have been comprised of separate layer 2 and layer 3 devices. Each device uses a different technique for processing and forwarding traffic. Layer 2 switches are hardware-based. They forward traffic at wire speeds, using the internal circuits that physically connect each incoming port to every other port. The forwarding process uses the MAC address and the existence of the destination MAC address in the MAC table. A layer 2 switch limits the forwarding of traffic to within a single network segment or subnet. Routers are software–based and use microprocessor to execute routing based on IP addresses. Layer 3 routing allows traffic to be forwarded between different networks and subnets. As a Packet enters a Router interface, the Router uses software to find the destination IP address and select the best path forward the destination network.

B. Redundancy in A Switched Network

From the authors of [12], modern Enterprises rely on their networks for their very existence. The network is the lifeline of many organizations. Network downtime translates into potential disastrous loss of business, income and customer confidence. The failure of a single network link, a single device or a crucial port or Switch causes a network downtime. Redundancy is required in the network design in order to maintain a high degree of reliability and eliminate any single point of failure. Redundancy is accomplished by installing duplicate equipment and network links for critical areas. Sometimes, providing complete redundancy of all links and devices in a network becomes very expensive, network engineers are often required to balance the cost of redundancy with the need for network availability.

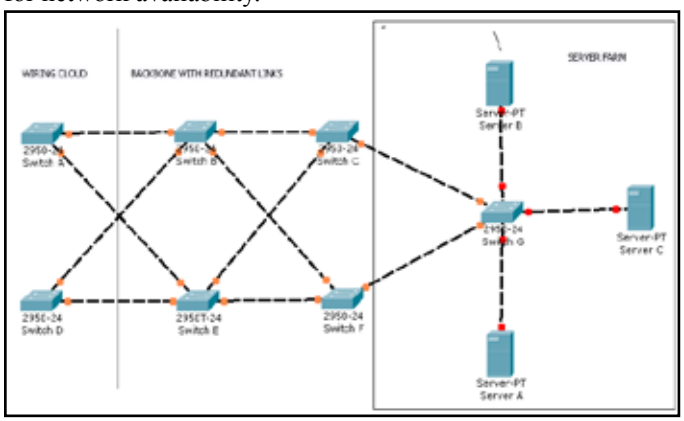

Fig 3.1: Shows redundantly paths to different Switches and File Servers.

Redundancy refers to as having two different pathways to a

ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)

particular destination. Examples of redundancy in non-networking environment include two roads into a town, two bridges to cross a river or two doors to exit a building. If one way is blocked another is still available. According to [13], redundancy can be achieved in switches by connecting them with multiple links, which in turn reduces congestion and supports load balancing. Connecting switches together however causes problems, for example, the broadcast nature of Ethernet traffic creates switching loops. The broadcast frame go around and around in all directions (round robin) causing a broadcast storm. Broadcast storms use up all of the available bandwidth and can prevent network connection from being established as well as causing existing network connections to be dropped. Broadcast storm are not the only problem created by redundant links in a switched network. Unicast frames sometimes cause problems such as; multiple frame transmission and MAC data base stability.

C. Multiple Frame Transmission

From [14], if a host sends a unicast frame to a destination host and a destination MAC address is not included in any of the connected switch MAC tables, then every switch floods the frame out to all ports. In a loop network, the frame could be sent back to the initial switch. The process repeats, creating multiple copies of the frame on the network, eventually the destination host receives multiple copies, this causes three problems namely; wasted bandwidth, wasted CPU time and potential duplication of signal traffic [18].

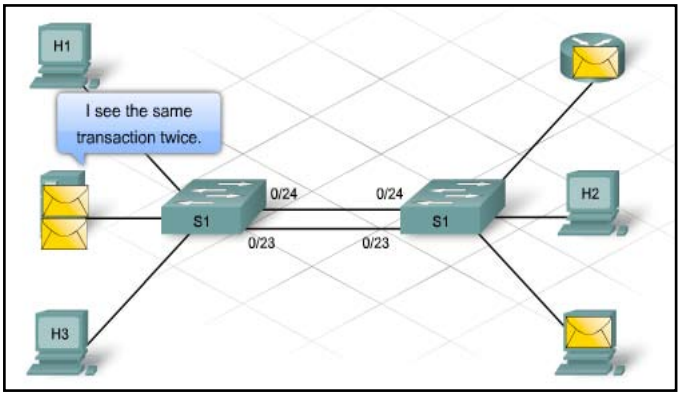

Fig 3.2: Shows multiple frame transmission in a switched network

D. MAC Database Instability

From the work in [15], it is possible for switches in a redundant network to learn the wrong information about the location of a host. If a loop exists, one switch may associate the destination MAC address, with two separate ports. This causes confusion and sub-optimal frame forwarding.

IV. Functional Units of The System

A. CISCO Packet Tracer V5.0

This tool helps in the design and configuration of the test network. The flexibility of this tool in demonstrating link resiliency through the use of RSTP to maintain traffic without interruption of service in the event of link failure is trilling. This tool is a software based on Cisco networking devices and other networking devices that enables device in a test network to be designed by interconnecting devices exactly the same way it is in the real environment. The results are therefore simply analyzed without ambiguity.

B. Network Switch

A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will only send a message to a device that needs it or requests it, rather than broadcasting the same message out of each of its ports. It is a multi-port network bridge that processes and forwards data at the data link layer (layer 2) of the OSI model. Some switches have additional features, including the ability to route packets. Switches exist for various types of networks including Fibre channel, Asynchronous transfer mode, Infiniband, Ethernet and others. But due to the nature of our work, Ethernet switches are going to be used in achieving this project.

C. RJ-45

The RJ-45 is a standardized physical network interface, both jack construction and wiring patterns, for connecting telecommunication or data equipment to a service provided by a local or long distance carrier. It is standardized as the IEC 60603-7 8P8C modular connector.

D. LAN Tester

It is an electronic device used to verify the electronic the electrical connections in a network cable. It is also used to verify that all the intended connections exist and that there are no unintended connections in the cable being tested. The testing is done in two phases, the first phase, called the open test makes sure that each of the intended connections is good. The second phase called the shorts test makes sure there are no unintended connections.

E. CAT 5E Network Cable

It is a twisted pair cable for carrying signals. This kind of cable is used in structured cabling for computer networks such as Ethernet. The cable standard provides performance of up to 100MHz. Cat5 is also used to carry other signals such as telephony and video. The cable is commonly connected using punch down blocks and modular connectors (RJ45). Most category 5 cables are unshielded, relying on the twisted pair design and differential signaling for noise rejection.

Fig 4.1: Site Specification

V. System Implementation And Result

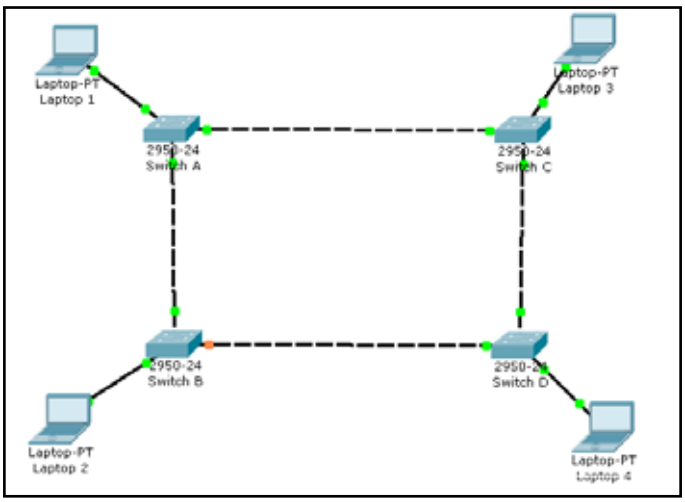

Fig 5.1 : Network design of the LAN

A. Configuring The Switches

The switches are configured with STP and RSTP. The end users which could be Laptops, Desktop Computers, Printers, IP phones are also configured based on their different IP addresses assigned to them to avoid conflict.

B. Simulation

We can use the ping utility (command line Interface) to reach the other systems on the Network from a machine using Microsoft window.

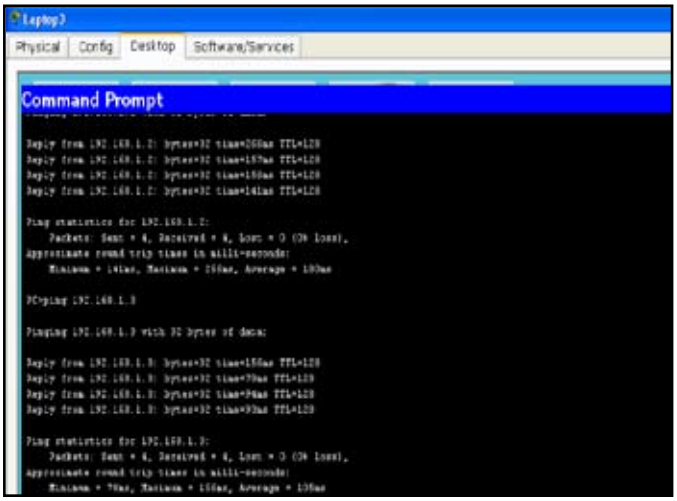

Fig 5.2: The Command Line Interface showing the replies from other End-users.

C. Effects of Loops In A An Ethernet Network

As soon as the first piece of data is sent on the network, a single Ethernet frame will cycle through the loop repeatedly. A single network and actually consume 100% of the possible network bandwidth. If you have a switch based network, then it may actually take a broadcast packet to cause a problem with a network device, it forwards it out through all ports. The neighboring switch will get that broadcast through all other ports and due to the loops, this broadcast will make its way into the original switch that received the broadcast from the network device. When the broadcast arrives, it will not know that it has seen it before, so it will forward it to all other ports. This process will be repeated thousands of times per second, causing a huge volume of traffic from a single broadcasted Ethernet frame. When this happens on your network, everyone will lose the ability to communicate on the network, and the activity lights on the switches will be solid (ON) rather than blinking (ON and OFF).

D. Results

The main difference in the operation of STP and RSTP no longer relies on conservative timers to re-converge after topology change. In order to accomplish this, the algorithm does the following:

- It monitors MAC operational states and retires ports that are no longer functional.
- It processes inferior BPDU's to detect topology changes.
- It keeps track of ports that provide alternative paths to the root bridge. If a root port fails, RSTP can quickly retire the port and make an alternative port its new root port. This new root port can be placed in the forwarding state without delay.
- When bridges are connected via point to point links (directly connected), they use handshake (sync), rather than timers to transit a designated port to forwarding.

To illustrate this, see figure 3.2 below. It depicts a network made up of four switches: Switch A, Switch B, Switch C and Switch D connected via a ring topology.

- Switch A is elected a Root bridge
- Ports that connect switch B and Switch C to the root bridge becomes root ports.

Switch D has two paths to the Root bridge via bridge B and bridge C. It elects port 01 as its root port (because it has the best port priority vector) and blocks port 02.

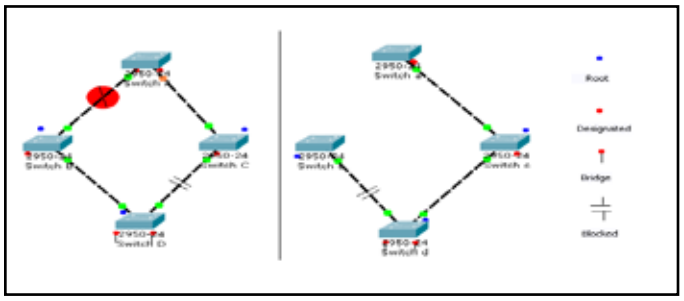

Fig 5.3: Shows The Election Of The Root Bridge

What happens when the connection between bridge A and bridge breaks? First, the STP case:

1. The STP Case

After the link failure, switch B and switch D continue to wait for the duration of the max age timer (default 20 seconds) before deciding their path to the root bridge is no longer operational. During that time, switch D discards BPDUs received on port 02 as inferior. Finally, after the max age timer expires, switch D ages out protocol information on port 01 recognizing it has path to the root bridge through port 02. It elects this port to be its new root port and advertises it to switch B through port 01 (designated port). In order to ensure all the switches on the LAN agree with this new topology, switch D will not forward user data on port 01 and 02 for an additional 30 seconds (two times forward delay). Instead, it transits both ports through listening and learning (15 seconds each) before placing them in a forwarding state. Switch B notices its new path to the root bridge is now through switch D and makes its port 03 a new root port, which also needs to transit through listening and learning. The total network outage perceived by stations connected to switch B and switch D will be

ISSN : 2348 - 9065 (Online)
ISSN : 2349 - 3143 (Print)

20 seconds (Max Age Time), 15 seconds (listening), +15 seconds (learning),Total: 50 seconds

What happens when the link between switch A and Switch B gets restored?

- As soon as switch B receives BPDUs from bridge A on port 01 it retires its port 03 and makes port 01 its new root port. This port however, needs to transit through listening and learning before it can send user data.
- Switch B also makes port 03 it's designated port.
- Similar things happen on switch D. As soon as it receives BPDUs from switch B on port 01, it retires port 02 and makes port 01 its new root port. This port also needs to transit through listening and learning. Port 02 will stay in blocking mode since it provides redundant connection to the root bridge.

The network outage for stations connected to switch B and switch D will be 15 seconds (listening), 15 seconds (learning), for a total time of 30 seconds.

2. The RSTP Case

When switch B loses its connection to the root bridge, it immediately decides that it is the new root bridge and starts advertising that to switch D. Switch D recognizes the BPDUs received from switch B as inferior, and concludes its connection to the root bridge, through switch B, is no longer operational. It immediately activates its secondary path through port 02, makes the port its new root port and immediately places it in a forwarding state. It also makes port 01 it's designated port and advertises its new path to the root bridge to be bridge B. Bridge B accepts the information and makes port 03 its new root port. Finally, switch D performs a handshake called 'sync operation' with switch B to transit port 01 into a forwarding state. The sync requires a BPDU exchange, but does not use timers and therefore happens very fast. The time before all bridges agree a new topology may take less than a second.

What happens when link between bridge A and bridge B gets restored?

When Root Bridge (switch A) detects a link on port 03, it starts a sync process with the switch B to transit this port to a forwarding state. This requires switch A to send a BPDU to switch B with a proposal flag set.

- Switch B recognizes this BPDU as superior (received on the shortest path to the root) and asserts sync. The sync is a signal to all non-edge designated ports to go into blocking mode. Port 01 then sends a BPDU back to the root bridge with the agreement flag set indicating that switch B is in agreement with the topology. This is the indication to switch A that port 01 can transit to a forwarding state without additional delay.
- The break in the loop is now switch B and switch D.
- Next, switch B repeats the sync process to transition is designated port 03 into a forwarding state. It sends a BPDU with a proposal flag set to switch D which retires port 02 from its role of a root port and makes port 01 its new port. It also asserts sync to place all non-edge designated ports in blocking mode and returns a BPDU to switch B with the agreement flag set. This informs switch B that it may transition its port 03 to a forwarding state.

Notice the final break has been moved to a link connecting switch D and switch C. Also note that the whole process required no timers and could take less than a second before all bridges agree on the new topology.

VI. Performance Evaluation

Once the ping stream begins, we physically disconnect the cable from one of the spanning tree interfaces. The ping request will fail to reach the destination host for some interval. After spanning tree routes traffic onto the redundant link, the ping request will again reach the destination host, which in turn will resume sending replies in milliseconds. The initial RSTP converge time, after all switches are connected and powered up, is similar to that of STP. However, once the network becomes stable and all switches agree on the current topology, any subsequent changes (e.g., link failure) are propagated rapidly without the need for Spanning Tree Timers. Depending on the complexity of the network, the time it takes to establish the new topology may vary from tens of milliseconds to seconds.

VII. Conclusion

This project has introduced Rapid Spanning Tree Protocol (RSTP) as a solution for designing high availability systems based on d-link switch specification. RSTP has many advantages over its predecessor, Spanning Tree Protocol (STP). In an event of a link or component failure, carefully designed systems may use RSTP to switch over to their redundant connections in less than a second. In order to design a high availability systems with RSTP, this project serves as a manual to such a user, this will help the user in configuring and enabling RSTP on switches on an Ethernet network to track the fundamental problem of traffic loop. We recommend that this protocol RSTP will be used where network downtime of one minute can cause a loss of customer and employee satisfaction. Hence this project serves as a manual to achieving this. Thus technological advancements and evolution of communication protocols has led to the introduction of this system which has the capability for a continuous, real time, speedy recalculation and reconfiguration of the Spanning tree which ensures complete elimination of loops in an Ethernet Switched Network as well as boosts the quality of the network; minimize excessive downtimes and decreases recovery time.

References

[1]. Stalling .W. "Data and computer communication" upper saddle River NJ, prentice hall, 2014.
[2]. http://www.wikipedia.org/wiki/RSTP ,12/11/2013
[3]. Forouzan .B. "Data communication and networking" NY, McGraw-Hill, 2007
[4]. Keiser .G "Local area network" New York NY, McGraw-Hill 2002.
[5]. www. Cisco.netacad.net, 11/11/2013
[6]. Cisco 2960 catalyst switch configuration guide 2009
[7]. Switching and VLAN implementation student guide 2008
[8]. www.cisco.com, 11/11/2013
[9]. Perlman .R. "Interconnection: Bridges, Routers, Switches and internetworking protocols", Reading address. Wesley 2000
[10] Theodore Rappaport "wireless communication principle and practice"
[11]. Forouzan .B. "TCP/IP protocol suite" NY, McGraw-Hill 2006.
[12] Surgeon .C. "Ethernet" sebastapol C.A. Reilly 2000
[13]. Kumar .A. Manjunath .D. and Kuri. J. "Communication networking" San Francisco CA. Morgan 2004.
[14]. http://www.juniper.net/techpubs, 12/11/2013
[15]. Kurose J.F, Ross K.W. (2005). Computer networking: a

top-down approach featuringthe internet (3rd ed.). Boston: Pearson/Addison Wesley.

Authors Profile

Engr. Ufoaroh Stephen U.is a Lecturer at the Department of Electronic & computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria. He holds M.Eng. in Communications Engineering from Nnamdi Azikiwe University Awka, Nigeria and currently a doctoral candidate in Computer and Control Engineering in the same department. Nigeria. His research interest is on communication and Control Engineering. He is a registered Engineer with Council for regulation of engineering in Nigeria(COREN) and a professional member of Institute of Electrical and Electronics Engineers (IEEE). He can be contacted via e-mail sufoaroh@yahoo.com or Call +2348035018583.

Oranugo Charles. O is a B.Eng. holder in Electronic and computer engineering from Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. His areas of interest include Modeling and simulation of communication networks, expert systems, Intelligent control, Wireless Sensor Networks and many other areas. He is a Student Member of Nigeria Society of Engineers, NSE, and IAENG.