INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 1, Issue 2, NOVEMBER 2015.

Performance Evaluation Survey on Loop Prevention Mechanisms in Redundant Switch Topology

Harjot Singh[#1], Mandeep Singh Saini[#2]
Department of Information Technology, Chandigarh Engineering College
Mohali, Punjab

***Abstract*— Redundant links between switches are necessary as they help prevent network failures in the event one link goes down, but it also gives rise to problems such as broadcast storms, inconsistent switch tables and multiple frame transmission. Spanning tree was designed to solve this problem created by the interconnection of Local Area Networks with redundant transparent bridges. STP is a layer 2 protocol that detects all links in the network and shut down the redundant ones. STP uses spanning-tree algorithm to search out and disable the redundant links. With STP running, frames will be forwarded only on the superior links picked by the STP. This paper addresses issues between IEEE Spanning Tree-based protocols and other loop prevention algorithms. Evaluation of such protocols, convergence issues between them and suggestion on how to resolve these issues are presented.**

***Keywords*— Redundancy, load balancing, spanning tree protocol, convergence time, Ethernet Bridges.**

I. INTRODUCTION

Bridge loops can occur any time there is a redundant Layer 2 path between two endpoints. By default, switches forward broadcast or multicast out all ports, except the port from which the broadcast/multicast was sent. When a switching loop is introduced into the network, broadcast messages will be rebroadcasted repeatedly resulting in broadcast storms. Broadcast storms occur when broadcasts endlessly switch through the loop disrupting normal network operations. Ethernet frames have no TTL field which is a mechanism to limit the lifespan of packets. So a frame sent to a looped network can loop forever. Switches needed a mechanism to prevent loop formation. This led to the development of Spanning Tree Protocol (STP). STP uses an algorithm called Spanning Tree Algorithm (STA). First STA selects a reference point and is called Root Bridge. It then evaluates the available paths to reach the Root Bridge. If there are redundant paths to reach that reference point, then STA selects the best and puts the rest in a blocking state. The blocked ports on the switch can be reactivated if the best link goes down.

II. SPANNING TREE PROTOCOL

Spanning Tree Protocol (STP) prevents network loops on layer 2 switches by continuously monitoring the network to track all links and block the redundant ones. STP [8] makes use of the spanning-tree algorithm (STA) to form a database of the network topology and then search out and disable the redundant connections. Spanning-tree algorithm enforces a distributed variant of the Bellman-Ford iterative algorithm which constantly looks for the optimal solution and selects an optimal candidate every time. Every switch except the root accepts and retains only the best current root bridge information and elect one root port upstream toward the root switch. Switches then block alternate paths to reach the root switch, leaving only the single optimal upstream path and continue passing optimal information downstream. If the switch learns of a superior root switch, the previous information is wiped out and the new one is immediately accepted and relayed. With STP enabled, frames will be forwarded on only superior links chosen by the STP protocol.
Network convergence becomes an issue because of the large number of steps that STP undergoes for removing layer2 loops. The convergence time of STP is 50-60 seconds per switch. The spanning tree algorithm (STA) would require to be executed every time a link comes up or goes down in the network. This leads to performance issues on a layer 2 network. Such disadvantages have led to the evolution of certain protocols such as uplink fast, backbone fast and port fast. But these protocols still suffer from high convergence times.

A. STP PORT STATES

The switch ports with STP enabled are in one of the following five states

- Blocking State: The Switch Ports change to blocking state at the time of the election process, when a switch gets a BPDU on a port that suggests a better path to the Root Switch and if a port is neither a Root Port nor a Designated Port. A port that is in the blocking state does not take part in frame forwarding and also reject frames received from the connected network segment. During blocking state, the port only listens to and processes BPDUs on its interfaces. After 20 seconds, the switch port shifts from the blocking state to the listening state.

- Listening State: After the blocking state, a Root or a Designated Port will change to a listening state. All the other ports will remain in a blocked state. During the listening state the port rejects frames received from the connected network segment and it also reject frames that are switched from some other port for forwarding. In this state, the port receives Bridge Protocol Data Units (BPDUs) from the network segment and sends them to the system module of the switch for processing. After 15 seconds, the switch port changes from the listening state to the learning state.

- Learning State: A port switches to learning state after listening state. During the learning state, the port listens and processes BPDUs. In the listening state, the port start processing user frames and updating the MAC address table. But the user frames are still not forwarded to the destination. After 15 seconds, the switch port changes from learning to the forwarding state.

- Forwarding State: A port that is in the forwarding state forwards frames across the connected network segment. In a forwarding state, the port will process Bridge Protocol Data Units (BPDUs), update its Media Access Control (MAC) Address table with frames that it takes in, and send user traffic through the port. Forwarding. Information and configuration messages are communicated through the port, when it is in the forwarding state.

- Disabled State: A port that is in the disabled state neither participates in frame forwarding nor in the operation of STP because such ports are considered non-operational.

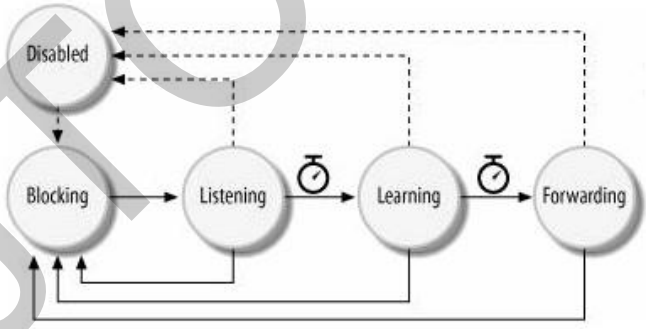

Fig. 1 STP Port States

III. RAPID SPANNING TREE PROTOCOL

The main disadvantage of the standard Spanning Tree Protocol is the low convergence. To overcome this problem, Rapid Spanning Tree Protocol (RSTP) was developed, which significantly reduces the convergence time after a network topology change. The main difference between RSTP (IEEE 802.1W) and STP (IEEE 802.1D) is that RSTP [5] assumes the three STP port states Blocking, Listening and Disabled are same as these states neither forward Ethernet frames nor learn physical addresses. Hence RSTP places all of them into a new state known as the Discarding state. Learning and forwarding ports function more or less the same. STP has two additional types of ports called backup ports and alternate ports along with the Root Port and Designated Port. A backup port is a port

that could be used to get to the root switch, but there already exists an active Designated Port for the segment. It can also be considered as an extra unused Designated Port. An alternate port is one that has a substitute path or paths to the Root Bridge but is presently in a discarding state. It can also be considered as an extra unused Root Port. RSTP uses proposal and agreement process for synchronization. Hello, Forward delay and Max Age timers are used for backward compatibility with original STP. It provides quicker transition on edge ports. RSTP does not wait to be notified by others about any link failure, instead, actively looks for possible failure by using a feedback mechanism called Request Link Query (RLQ).

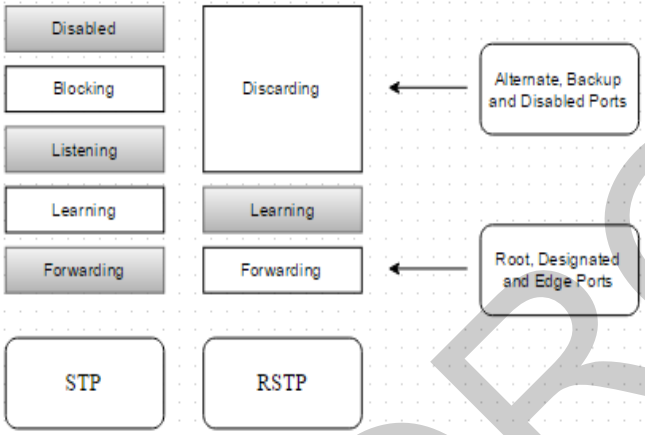

Fig. 2 STP and RSTP Port States

IV. Multiple Spanning Tree Protocol

Multiple Spanning Tree (MST) permits groups of VLANs to be assigned their own STP process. Each Spanning Tree Protocol process is called an instance. MST divides the STP topology into regions that must have similar parameters including:

- Configuration Name - It is a 32-bit value similar to a VLAN Trunking Protocol (VTP) domain.
- Revision Number – It is a 16-bit value that tells the current MST configuration's revision.
- Virtual LAN to instance Mappings.

Each region executes its own Internal Spanning Tree (IST) to get rid of loops within that region. Internal Spanning Tree is basically an enhanced form of Rapid Spanning Tree Protocol that supports various Multiple Spanning Tree specific parameters. Rapid STP can keep track of one spanning tree, whereas Multiple STP can keep track of many spanning trees, called instances. Multiple STP allows to have different forwarding paths for different Multiple Spanning Tree instances. This provides load balancing network traffic across the redundant links, so that all links present in a network can be put to use and no link is left entirely idle. Multiple STP is VLAN aware, whereas Rapid STP is not. Multiple STP BPDUs and Rapid STP BPDUs are compatible, so a network can have a fusion of Multiple STP and Rapid STP areas. Multiple Spanning Tree is fully compatible with all other implementations of STP.

V. Drawbacks in Existing System

With the importance that large organizations are placing on information and network connectivity, many of these are implementing redundant technology to offer failure tolerance on the network level. When a link goes down, it is significant that the protocol recognizes that failure, and converges upon a new topology to permit the network segment to still be online. STP that has a convergence time between 30 and 50 seconds is insufficient for the needs of modern Ethernet networks [6]. In a large network, a modification in the existing root switch initiates an event, meaning all other switches in the network have to stop and reconfigure themselves according to the new root switch. When such an event is initiated, all the switches in the group stops forwarding data while they are busy reconfiguring their Spanning Tree databases. Data flow will continue once all the switches in the group synchronize their databases with each other, a process called convergence. This could potentially interrupt the network performance. Networks these days need a convergence time of tens of milliseconds to compensate time critical

traffic such as voice and video [10]. STP is stateless, trustful and does not have a solid authentication mechanism. If a malicious hacker has access to ports that have the ability to become trunk ports, he can put in a rogue switch into the network. Rogue switch with less priority declares its superior BPDUs and can cause the STP topology to reconverge. The rouge switch will become the root bridge and all the traffic will pass through it. This gives the attacker the ability to sniff all the network traffic crossing the switch. The attacker can forward traffic from high bandwidth links between real switch to maybe a 100 Mbps link on the rouge switch. This can significantly reduce network speed and can lead to Denial of Service (DoS) attack. STP also suffers from BPDU flooding attack that can also lead to DoS. STP does not complain about handling large number of incoming BPDUs. It just tries to process as many as it can until its processing power is used up fully. The original STA was designed with utmost stability in mind. All switches adjust to the information sent by the root, slowly unblocking their ports to guarantee loop free active topology. This procedure resulted in slow convergence, delimited by Max_Age+2x Forward_Time seconds that were needed to adapt to a generic topology change. Also, it does not provide any load balancing using the redundant links. The ineffective timer mechanisms are mainly responsible for the limitations of STP (802.1D). Rapid Spanning Tree Protocol (RSTP) is the Ethernet standard that has replaced STP (802.1D). RSTP unlike STP does not depend on timers rather it uses feedback mechanisms which permit a much faster transition to the forwarding state that result in a much better convergence performance, RSTP serves the same function as STP in providing a loop free network topology with improved convergence, however; it also has limitations in that it fails to provide any load sharing mechanisms. By using regions, MSTP permits for isolating different physical topologies from each other while preserving Layer 2 connectivity between the regions. However, even with improved fault isolation, MSTP still suffers from the issues built-in to Ethernet topology – broadcast and unicast flooding and sluggish spanning tree convergence. This confines MSTP deployments to small Layer 2 domains.

VI. CONCLUSION AND FUTURE WORK

This paper compares the loop prevention mechanisms in redundant switch topology. STP that has a convergence time between 30 and 50 seconds is insufficient for the needs of modern Ethernet networks [6]. STP is a stateless protocol that lacks a solid authentication mechanism and is vulnerable to various attacks including sniffing and DoS attacks. Rapid Spanning Tree Protocol (RSTP), the Ethernet standard that replaced STP, does not provide any load balancing mechanisms. MSTP suffers from the issues built-in to Ethernet topology - broadcast and unicast flooding and sluggish spanning tree convergence. This confines MSTP deployments to small Layer 2 domains.

In the future, the comparative analysis can be performed with higher level of performance analysis using the higher number of parameters. Also, the techniques under the survey can be improved or mixed in order to improve the overall performance of the scheme.

REFERENCES

[1] Pallos, R. , Ericsson Res., Farkas, 1. , Moldovan, 1. , Lukovszki, C, *Performance of rapid spanning tree protocol in access and metro networks,* Access Networks & Workshops, Pages 1-8, 2007.

[2] Charles E. Spurgeon "Ethernet the Definitive Guide", O'REILLY, 2000.

[3] M. Huynh, P. Mohapatra, S. Goose "Cross-Over Spanning Tree: Enhancing Metro Ethernet Resilience and Load Balancing", Technical Report CSE-2006-34, Department of Computer Science, UC Davis, 2006

[4] *Link Aggregation Control Protocol for Gigabit interfaces* IEEE 802.3ad,2000

[5] Wald Wojdak. Rapid spanning tree protocol: A new solution from an old technology, 2008.

[6] Nada Al-Balushi,, Rahma Al-Klabani, Faizal Hajmohideen," Performance Evaluation using STP Across Layer-2 VLANs ",*International Journal of Communication and Networking System* Volume: 01 Issue: 01 January- June 2012 ISSN: 2278-2427

[7] Michael Galea, Marzio Pozzuoli, "Redundancy in Substation LANs with the Rapid Spanning Tree Protocol

(IEEE 802.1w)", RuggedCom Inc. - Industrial Strength Networks, 2004.

[8] *Spanning tree protocol for WAN*, IEEE 802.ld, 1980

[9] David Barnes, Basir Sakandar."Cisco LAN Switching Fundamentals", Cisco Press, 2004.

[10] N. Slabakov, "Spanning tree: Death is not an option," Technology Withepapaer, Riverstone Networks, 2002.

[11] Bonada, E.; Sala, D. "RSTP-SP: Shortest path extensions to RSTP", *High Performance Switching and Routing (HPSR), 2012 IEEE 13th International Conference on*, On page(s): 223 - 228.
[12] Gopalan, A.; Ramasubramanian, S. "Fast recovery from link failures in Ethernet networks", *Design of Reliable Communication Networks (DRCN), 2013 9th International Conference on the*. On page(s): 1 - 10, Volume: Issue:, 4-7