Mitigating Broadcast Storm on Metro Ethernet Network Using PVST+

Beny Nugraha*, Bayu Fitrianto, Fahraini Bacharuddin
Mercu Buana University, Jalan Meruya Selatan No. 1, +62 21 5840816
*Corresponding author, e-mail: benynugraha@mercubuana.ac.id

Abstract

Broadcast storm attack continuously transmits duplicate packets in order to disrupt the service of the network. In this research, a Spanning Tree Protocol method, namely PVST+ (Per VLAN Spanning Tree Plus), is used to overcome the problem that is caused by the broadcast storm attack on the Metro Ethernet Network. The PVST+ serves as a redundant network management and it prevents looping on the network. The results obtained from this research are the following, PVST+ is able to mitigate broadcast storm that is shown by the decrease of number of packets and the decrease of the average packet per-second. The average packets per-second on VLAN 1 decrease to 274,041 and the average packets on VLAN 10 decrease to 267,794 packets per-second.

Keywords*: Broadcast Storm, Metro Ethernet, PVST+, Security Network, Spanning Tree Protocol*

1. Introduction

Ethernet can be seen as standard for LAN (Local Area Network)/MAN (Metro Area Network)/WAN (Wide Area Network) connection as 98% of data traffic in worldwide network is based on the Ethernet. Metro Ethernet networks are designed to be able to provide up to 200.000 high-speed lines to end-users and organizations that need more capacity in their communications, thus, the Metro Ethernet networks are best to be connected with fiber optics. Emamjomeh, et al., [1] has proposed an optical system for the Metro Ethernet and MPLS (multi protocol label switching) technique is used for faster communication that meets the user's needs; however, there is no security analysis on their research.

STP (Spanning Tree Protocol) manages and provides path redundancy while avoiding undesirable loops in the Ethernet networks, a new STP, namely Load Balanced Spanning Tree (LBST) has been proposed to to reduce the computational complexity of the previous BST algorithm [2]. Moreover, Huu-Hung Phan et al. [3] has proposed a new model of Metro Ethernet Network as an undirected connectivity graph by using the Bridge Protocol Data Units (BPDUs) frame exchange to determine the shortest paths between network switches, however, both [2] and [3] did not analyze the security of their method.

The broadcast storm is an attack that utilizes sequence of broadcast operations from one or more devices that occur at rapid packets per-second rate, its goal is to bring down the network. The number of packets that is considered abnormal is more than 500 packets per-second [4]. A method to control the network storm, as well as broadcast storm, has been proposed in [5], multiple static agents are used to control the network storm in order to improve the performance of Ethernet LAN network, however, it is not mentioned that their method is able to be implemented on Metro Ethernet. Various solutions to prevent broadcast storm also have been proposed in [6-10], however, all of those methods are implemented on VANETs (Vehicular Ad Hoc Networks), not on Metro Ethernet network.

Broadcast storm is one variant of DoS/DDoS attack, as mentioned above; its goal is to break down the target system by flooding the network with junk packets. Monitoring and detection system can be used to mitigate broadcast storm as early as possible, Ni et al. [11] proposed a monitoring detection to detect anomaly packets flow at the DNS server, it is shown that their solution can detect DDoS attack accurately. Another solution to prevent the broadcast storm is a firewall, Alfan Presekal and Riri Fitri Sari [12] proposed a firewall to prevent DoS attack that is implemented on a Host Identity Protocol (HIP), and its shown that HIP with their

Received April 25, 2016; Revised November 24, 2016; Accepted November 30, 2016

firewall still manage to work eventhough there was a DoS attack. Despite all of the above proposed systems, their solution does not handle the broadcast storm in particular, thus, a mitigation system for broadcast storm is still not available.

Based on the above previous researches, it can be concluded that there is no solution to mitigate the broadcast storm on a Metro Ethernet Network, thus, to overcome the problem, we propose an SPT method, namely PVST+ (*Per VLAN Spanning Tree Plus*) to be implemented on the Metro Ethernet network. The Graphical Network Simulator (GNS 3) is used for implementation and simulation process, and two VLAN, namely VLAN 1 and VLAN 10 are used in this research. The average packets per-second on both VLAN are measured before and after the implementation of PVST+ to show that the broadcast storm is mitigated.

The rest of the paper is organized as follows: Section 2 describes the implementation of PVST+ method on the Metro Ethernet network, Section 3 discusses the results, and Section 4 concludes the whole research.

2. Implementation of PVST+ on Metro Ethernet Network

This section described the processes of mitigating the broadcast storm attack by implementing the PVST+. The first processes are scanning and capturing the packets on the network to detect broadcast storm (described in sub-section 2,1), the second process is implementing the PVST+ to mitigate the broadcast storm (presented in sub-section 2.2), and the last process is optimizing the network to prevent the future attack of the broadcast storm (discussed in sub-section 2.3).

2.1. Scan and Capture Packets on the Metro Ethernet Network

For the initial process, the GNS 3 simulator equipped with Wireshark is used to scan the data packet on each interface to detect a broadcast storm, which is already set to occur. The topology that is used for the scanning process is shown in Figure 1.

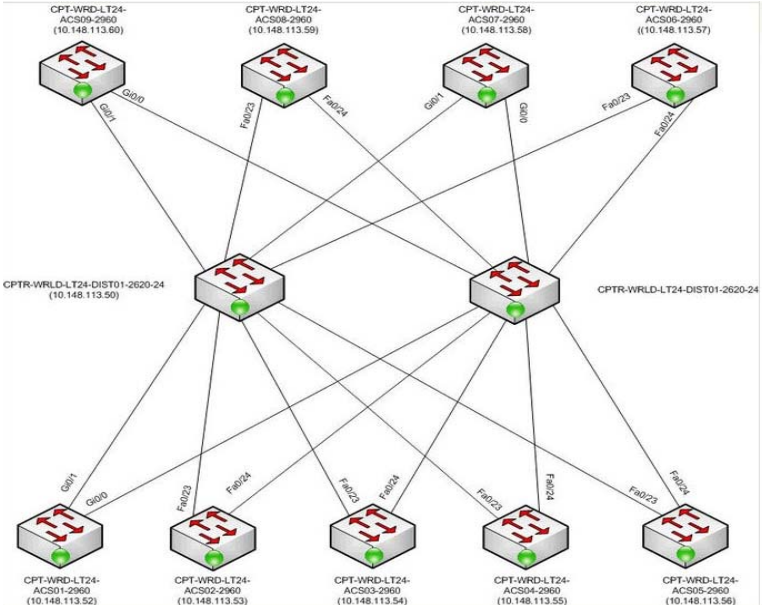


Figure 1. Metro Ethernet Network Topology

Figure 1 represents the topology that is used in this research; such topology is used to simulate the broadcast storm attack that usually happens when there are a lot of switches. These switches generate a lot of duplicate packets to cause the broadcast storm attack.

To determine a network that is a victim of broadcast storm, the data packets, in the form of ping packets, are sent from the host to the gateway with minimum time limit of 60 seconds.

Wireshark will monitor the traffic that occurs during the simulation time, the parameters that were monitored are number of packets and average packet per-second during. Based on [4], the broadcast storm attack occurs when the average packets per-second is above 500 packets-second.

2.2. Implementation of the PVST+

The PVST+ is implemented in order to mitigate the broadcast storm. The implementation of PVST+ performed on Core A, Core B, and on all four access switches, the illustration of the implementation on the network elements can be seen in Figure 2.

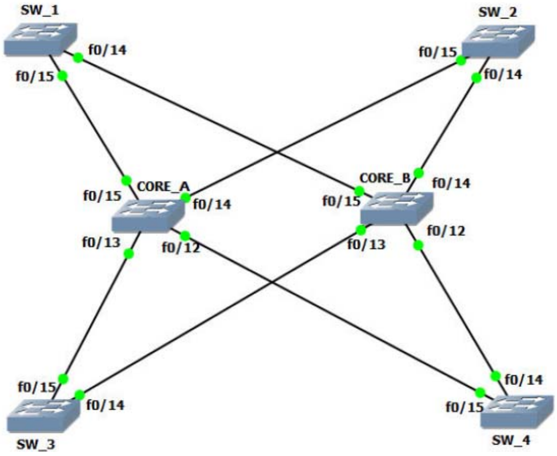
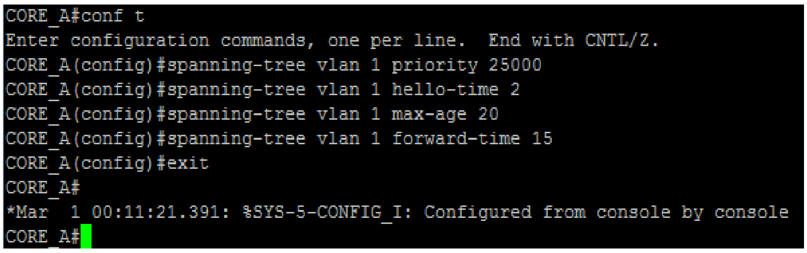


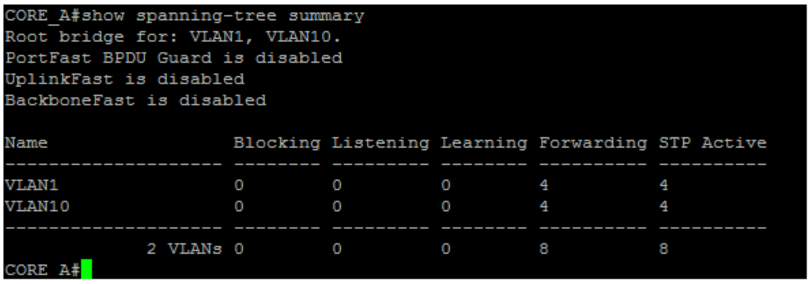
Figure 2. PVST+ Implementation on Every Network Element

Figure 2 illustrates the implementation of PVS+ on Core A, Core B, and all switches. Figure 2 represents the simulation of our research in GNS 3 simulator. PVST+ implementation process for each network element consists of two processes, namely the configuration process and the verification process. The command that is used to configure the PVST+ on Core A is shown in Figure 3, while the command that is used to verify the process is shown in Figure 4.



```
CORE_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_A(config)#spanning-tree vlan 1 priority 25000
CORE_A(config)#spanning-tree vlan 1 hello-time 2
CORE_A(config)#spanning-tree vlan 1 max-age 20
CORE_A(config)#spanning-tree vlan 1 forward-time 15
CORE_A(config)#exit
CORE_A#
*Mar  1 00:11:21.391: %SYS-5-CONFIG_I: Configured from console by console
CORE_A#
```

Figure 3. Command to Configure PVST+ on Core A



```
CORE_A#show spanning-tree summary
Root bridge for: VLAN1, VLAN10.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                0        0         0        4          4
VLAN10               0        0         0        4          4
-------------------- -------- --------- -------- ---------- ----------
             2 VLANs 0        0         0        8          8
CORE_A#
```

Figure 4. Command to Verify PVST+ on Core A

It is shown in Figure 3 and Figure 4 that there are two VLANs used for simulation, namely VLAN 1 and VLAN 10, these VLANs as well as the configuration and verification process are the same for all network elements.

2.3. Network Optimization

Network optimization is necessary if the broadcast storm still occurs after the implementation of PVST+, several options for network optimization are the following:

1. Port Fast

   Port Fast is a feature that is provided by the Cisco switch device for faster spanning tree formation. This feature is only performed on ports that are connected to the end user and is not recommended for port with “trunking” status because the duplicate packets forwarding will still occur.

2. Uplink Fast

   This feature has similar function with Port Fast, it is to form the spanning tree faster, and moreover, this feature can be used on port with “trunking” status.

3. Bridge Protocol Data Unit (BPDU) Guard

   The function of the command BPDU Guard is to maintain the spanning tree protocol algorithm that has been adapted to an integrated network. If a port that is connected to the end user, which already configured with Port Fast connection, is then replaced with the switch X, then the port will be shut down due to switch X will send BPDU message to the other switch to reset the algorithm.

4. Backbone Fast

   Backbone Fast is a feature to accelerate the delivery of BPDU with the principles of using the Root Link Query (RLQ), RLQ has a function to detect inactive/inderict link. With Backbone Fast, the process of determining the root bridge can be accelerated.

3. Results and Analysis

In this section, the result and analysis of the obtained data are presented. Simulation and evaluation of the implementation of PVST+ are consists of the following steps:

1. Traffic monitoring before the implementation of PVST+
2. Traffic monitoring after the implementation of PVST+

3.1. Traffic Monitoring before the Implementation of PVST+

Traffic monitoring is carried on VLAN 1 and VLAN 10 and it is performed at intervals of 90 seconds, 180 seconds, 270 seconds, 360 seconds and 450 seconds. The obtain results are the amounts of packets and the average packets per-second. The results of monitoring the traffic before the implementation of PVST+ on VLAN 1 and VLAN 10 can be seen in Table 1 and Table 2 respectively.

Table 1. Traffic Monitoring on VLAN 1 before the implementation of PVST+

Interval (Seconds)	Amounts of Packets	Average Packets per Second
90	6357287	69695.631
180	10578588	58271.710
270	14380776	53141.090
360	18029562	50007.938
450	21845159	48145.299

Table 2. Traffic Monitoring on VLAN 10 before the implementation of PVST+

Interval (Seconds)	Amounts of Packets	Average Packets per Second
90	371366	3925.396
180	990780	5461.581
270	1976285	7200.289
360	2896961	8021.201
450	4166094	9058.774

It can be seen from Table 1 and Table 2 that the average packets per-second on both VLAN 1 and VLAN 10 is above 500 packets per-second, with the average number of packets per-second for VLAN 1 is 55852.334 packets per-second and the average number of packets per-second for VLAN 10 is 6733.448 packets per-second. From these results, it can be concluded that the broadcast storm occurred on both VLAN 1 and VLAN 10. Sub-section 3.2 presents the result of the average number of packets per-second after the implementation of PVST+.

3.2. Traffic Monitoring after the Implementation of PVST+

The results of monitoring the traffic after the implementation of PVST+ on VLAN 1 and VLAN 10 can be seen in Table 3 and Table 4 respectively.

Table 3. Traffic Monitoring on VLAN 1 after the implementation of PVST+

Interval (Seconds)	Amounts of Packets	Average Packets per Second
90	25033	275.897
180	48912	271.579
270	75226	276.045
360	98633	273.597
450	123351	273.089

Table 4. Traffic Monitoring on VLAN 10 after the implementation of PVST+

Interval (Seconds)	Amounts of Packets	Average Packets per Second
90	24420	269.948
180	48303	267.512
270	72361	267.481
360	96093	266.858
450	120319	267.175

Table 3 and Table 4 show that after the implementation of PVST+, the number of packet and the average packes per-second have decreased, which the later being less than 500 packets per-second. The average number of packets per-second on VLAN 1 has decreased to 274.041 packets per-second, while the average packets per-second for VLAN 10 has decreased to 267.794 packets per second, therefore, it can be concluded that PVST+ is able to mitigate the broadcast storm. This result resolves the missing point that occur in research [5-12] where there is no mechanism to counter broadcast storm on the Metro Ethernet.

4. Conclusion

In the initial process of this research, a broadcast storm is simulated on Metro Ethernet Network, it is shown by the large number of average packets per-second, which are 55852,334 packets per-second on VLAN 1 and 6733,448 packets per-second on VLAN 10. In order to mitigate the broadcast storm, a variation of spanning tree protocol, namely the PVST+ is implemented on both VLAN 1 and VLAN 10. The results shown that the broadcast storm on both VLAN are able to be mitigated by PVST+, it is shown by the decrease of the average packets per-second on both VLAN, which are 274,041 packets per-second on VLAN 1 and 267,794 packets per-second on VLAN 10. PVST+ is able to mitigate broadcast storm due to its function to prevent loops occurring on the network and it is also able to handle a redundant path on the network.

References

[1] Alireza Emamjomeh, Hossein Emami, Ali Hashemi. Design and Simulation of Metro Ethernet using Optical System. *Majlesi Journal of Telecommunication Devices*. 2014; 3(3): 109-114.

[2] Ghasem Mirjalily, Samira Samadi. Load Balanced Spanning Tree in Metro Ethernet Networks. *Journal of Information Systems and Telecommunication*. 2014; 2(2): 119-126.

[3] Huu-Hung Phan, Tuyet-Thi Anh Mai, Tae-Wan Kim, Chul-Soo Kim. A Loop-Free Method on Ethernet Using Undirected Connectivity Graph. *International Journal of Emerging Technology and Advanced Engineering*. 2014; 4(2): 713-723.

[4] Daniel J. Nassar. Network Performance Baselining. 1st Edition. Indianapolis, USA: Sams Publishing. 2000.

[5] TR Gopalakrishnan Nair, BR Shubhamangala, Vaidehi M. *A Novel Agent Based Approach for Controlling Network Storms*. IEEE 3rd International Conference on Communications and Electronics (ICCE). Nha Trang, Vietnam. 2010.

[6] Xu Wu, Jun Zheng, Hui Tong, Nathalie Mitton. *DAYcast: A Dynamic Transmission Delay Based Broadcast Protocol for Vehicular Ad Hoc Networks*. IEEE International Conference on Communications (ICC). Sydney, Australia. 2014.

[7] Fogué Cortés M, Garrido Picazo MP, Martínez Domínguez FJ, Cano Escribá JC, Tavares De Araujo, Cesariny Calafate CM, Manzoni P. An adaptive system based on roadmap profiling to enhance warning message dissemination in VANETS*. IEEE/ACM Transactions on Networking*. 2013; 21(3): 883-895.

[8] Anna Maria Vegni, Enrico Natalizio. Forwarder Smart Selection Protocol for Limitation of Broadcast Storm Problem. *Journal of Network and Computer Applications*. 2015; 47: 61-71.

[9] Adil Mudasir Malla, Ravi Kant Sahu. Security Attacks with an Effective Solution for DOS Attacks in VANET. *International Journal of Computer Applications*. 2013; 66(22): 45-49.

[10] Rasheed Hussain, Junggab Son, Hasoo Eun, Sangjin Kim, Heekuck Oh. *Traffic information system: A lightweight geocast-based piggybacking strategy for cooperative awareness in VANET*. IEEE International Conference on Consumer Electronics (ICCE). Las Vegas, NV. 2013.

[11] Tongguang Ni, Xiaoqing Gu, Hongyuan Wang. Detecting DDoS Attacks Against DNS Servers Using Time Series Analysis. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014; 12(1): 753-761.

[12] Alfan Presekal, Riri Fitri Sari. Performance Comparison of Host Identity Protocol and TCP/IP with Firewall against Denial of Services. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014; 12(12): 8335-8343.