Wylian de Souza Ferreira
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

MULTIPLE SPANNING-TREE (MST) TO IMPROVE ENTERPRISE NETWORK SECURITY

Abstract: *This paper presents the scheme for MSTP that considers all possible and separate Edge spanning trees and all possible VLAN pooling, and finds the best load-balancing solution on links and switches. In fact, we define three main criteria: link load balancing, switch load balancing, and the shortest path selection. We can regard the importance of each criterion based on our goal.*

Keywords: *MST, PVST+, RPVST+, port priority, path cost, STP timers, CISCO*

Де Соуза Феррейра Вилиан
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

MULTIPLE SPANNING-TREE (MST), ЧТОБЫ УЛУЧШИТЬ БЕЗОПАСНОСТЬ СЕТИ ПРЕДПРИЯТИЙ

Аннотация: *В статье представлена схема для MSTP, в которой рассматриваются все возможные основные пограничные деревья и все возможные группы VLAN, а также найдено наилучшее решение на основе балансировки нагрузки на линии и коммутаторы. В настоящее время мы определяем три основных критерия: распределение нагрузки по ссылкам,* *распределение нагрузки на коммутаторах и выбор кратчайшего пути. Мы можем оценить важность каждого критерия в зависимости от нашей цели.*

Ключевые слова: *MST, PVST+, RPVST+, приоритет порта, стоимость пути, таймеры STP, CISCO.*

Introduction

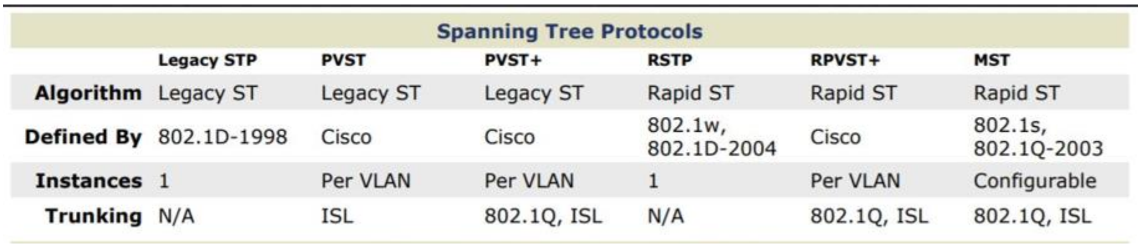
In the beginning, there was the IEEE STP protocol, preceded by the DEC and IBM STP variants. They all were used in the same logic originally proposed by Radia Perlman in the 1980s while it worked at DEC. The IEEE version has been adapted for the use with multiple VLANs using 802.1q frame tagging. The issue related to the building of STP where more traffic is routed through the links closest to the root bridge, which demands more root bridge resources both in terms of CPU utilization and link capacity [1].

STP Flavos

Types of Spanning Tree Protocol (STP) are represented in Figure 1 [2] and are the following [1]:

1. 802.1D – is also known as the Common Spanning Tree (CST). It is an IEEE-developed spanning tree standard that elects only one root bridge across the topology.
2. Per VLAN Spanning Tree + (PVST+) – is a standard Cisco version of STP. It finds a separate instance of the 802.1d spanning tree for each VLAN.
3. 802.1w – Rapid Spanning Tree Protocol (RSTP) – is a spanning standard developed by IEEE that provides faster convergence than CST but maintains the same idea of finding a single root bridge in the topology.
4. Rapid Per VLAN Spanning Tree + (RPVST+) – is Cisco Spanning Tree standard, which provides faster convergence than PVST + and finds a separate instance of 802.1w per VLAN. It requires much more memory and CPU than other STP standards.

5. 802.1s (Multiple Spanning Tree) – is developed by IEEE, where the VLAN team is performed and for each unique group RSTP is performed. This is basically a spanning tree protocol running over another spanning tree protocol.



Spanning Tree Protocols

	Legacy STP	PVST	PVST+	RSTP	RPVST+	MST
Algorithm	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	Rapid ST
Defined By	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	802.1s, 802.1Q-2003
Instances	1	Per VLAN	Per VLAN	1	Per VLAN	Configurable
Trunking	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	802.1Q, ISL

Figure 7- Spanning Tree Protocols.

Many STP instances use CPU resources to generate, receive, and process BPDUs on all VLANs on the switch. This was possible when there were only a few VLANs on the network (as it was in the beginning). Today, hundreds of VLANs are possible and the quality of CPU / hardware and software is stressed. Many switches have inexpensive, low-performance CPUs. Campus switches often have poor quality software, because lower prices mean less testing or cheap developers [4]. For example, smaller Cisco switches (2960X for example) support 128 (R) PVST instances, but the switch operationally supports 256 VLANs. Moreover, the 128 VLAN mark disables PVST on all enabled VLANs beyond 128.

Another problem is that STP is a much slower convergence because it has a slightly different state machine – it waits 10x Hello (20 seconds) for the BPDU timeout and listens for another 15 seconds, followed by learning state for another 15 seconds, giving only about 50 seconds to converge [2]. This delay in network convergence is fatal in the critical network, where any network outage is financially detrimental, for example, if a failure or DDOS attack occurs on the Layer 2 switches of the critical network. stock exchange, etc and the STP takes 50 seconds to converge, this delay could damage these companies for millions of dollars. A hacker or competing company can use this to attack another company by doing DDOS on switches and generating the looping convergence. MSTP with some security mechanisms in place, is able to avoid this problem.

Advantages of Multiple Spanning Tree (MST)

Multiple Spanning Tree (MST) is designed to allow multiple spanning tree topologies preserving scalability. MST allows an administrator to map an arbitrary number of VLANs to a single instance of MST, resulting in the minimum number of instances required to satisfy a design. If, for example, you have six VLANs, but only two single-layer topologies, you only need two MST instances [5].

In the RSTP or MSTP environment, if an interface goes down (for example, it is unplugged or unplugged), the topology change is triggered immediately - between just two switches, a new tree should be established in less than one second and forwarding will be restarted [6]. If there is a break not caused by link down (e. g: configuration change, intermediate device failure, etc), then RSTP and MSTP waits for 3x Hello Interval (3x2 (default) = 6 seconds by default) before re-converging. IEEE 802.1s combines the best aspects of PVST + and 802.1q.

The idea is that multiple VLANs can be mapped to a small number of Spanning Tree instances, because most networks do not need more than a few logical topologies. In other words, MSTP is a configurable and more scalable version of PVST +. In MSTP, you can define an STP instance for a configurable set of VLANs. By default, there is Instance 0 (fallback instance) and all VLANs are bound to this instance (Figure 2) [1].

From the technical point of view, MST is the best solution. From an end-user perspective, the main disadvantages associated with migrating to MST are:

- The protocol is more complex than the common tree and requires additional staff training.

- Interacting with legacy bridges can be challenging.

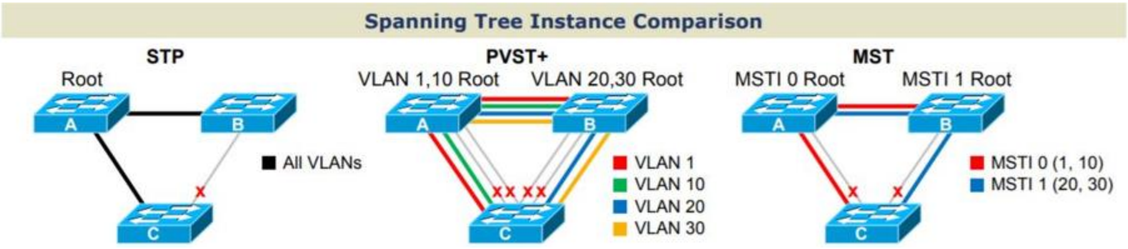


Figure 8- Spanning Tree Instance Comparison

The MST topology and port rules are demonstrated in Figure 3.

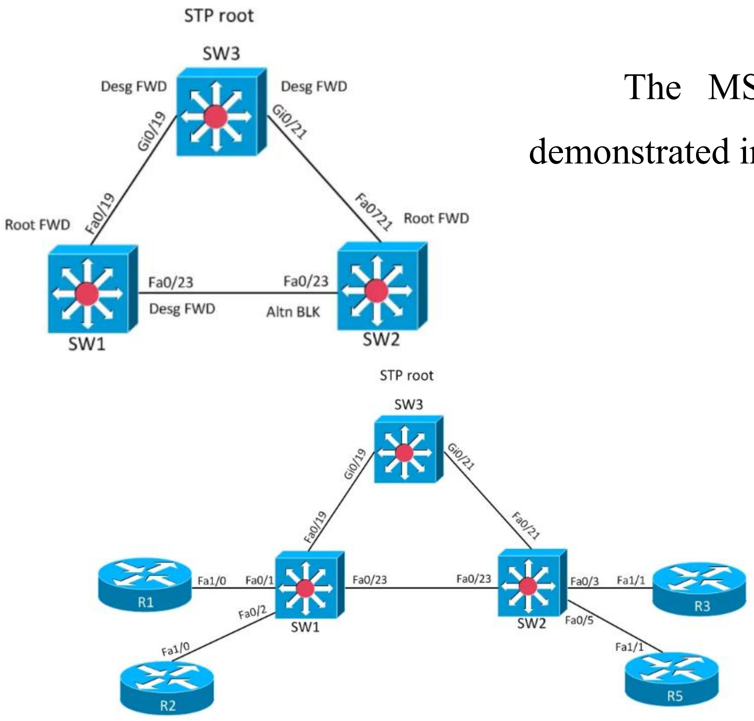


Figure 3 - Topology and port rules.

Some basic MST and NTP settings on the switches are in Figure 4.

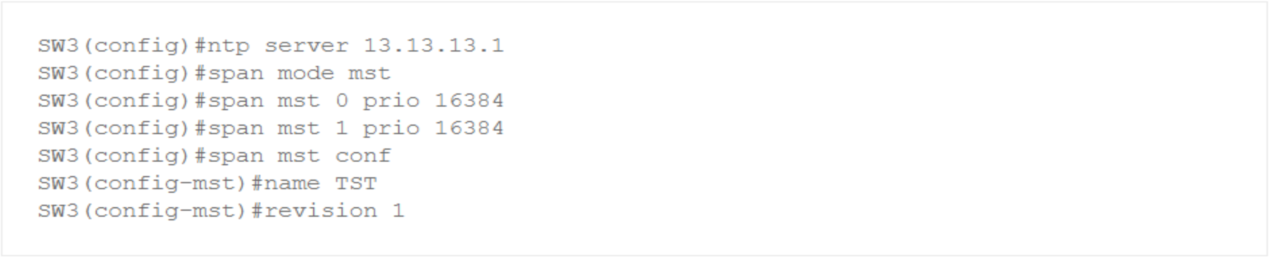

```
SW3(config)#ntp server 13.13.13.1
SW3(config)#span mode mst
SW3(config)#span mst 0 prio 16384
SW3(config)#span mst 1 prio 16384
SW3(config)#span mst conf
SW3(config-mst)#name TST
SW3(config-mst)#revision 1
```

Figure 4 - MST configuration

The Gi0/21 shutdown on SW3 leads to SW2 root port. Debug spanning-tree events show the sequence of events (Figure 5).

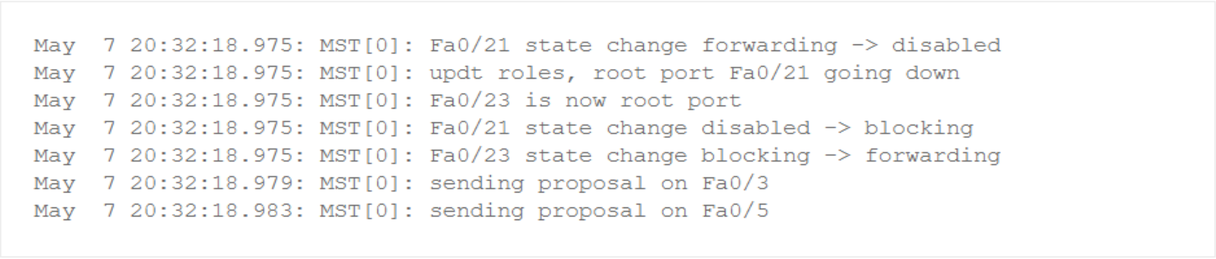
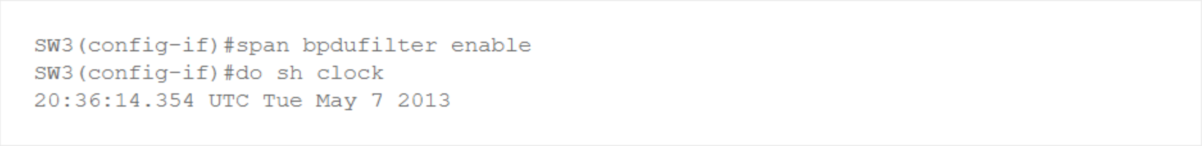

```
May  7 20:32:18.975: MST[0]: Fa0/21 state change forwarding -> disabled
May  7 20:32:18.975: MST[0]: updt roles, root port Fa0/21 going down
May  7 20:32:18.975: MST[0]: Fa0/23 is now root port
May  7 20:32:18.975: MST[0]: Fa0/21 state change disabled -> blocking
May  7 20:32:18.975: MST[0]: Fa0/23 state change blocking -> forwarding
May  7 20:32:18.979: MST[0]: sending proposal on Fa0/3
May  7 20:32:18.983: MST[0]: sending proposal on Fa0/5
```

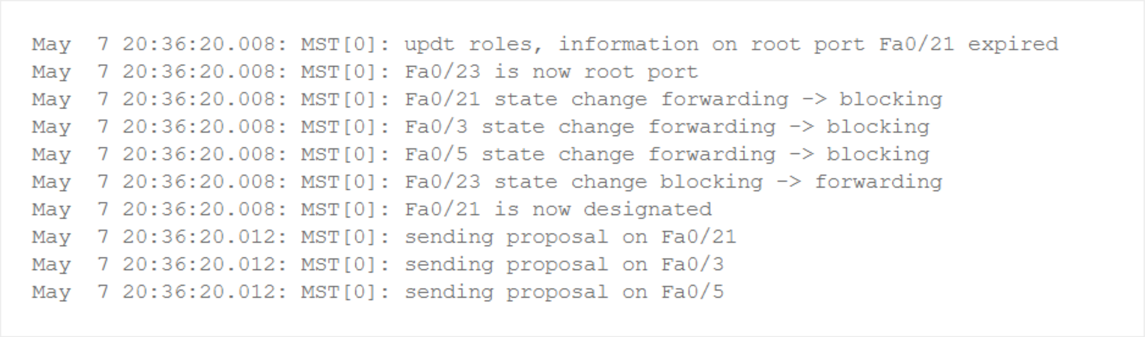
Figure 5 - Debug spanning-tree events

If the passive error is simulated by implementing BPDU filter, we receive the result in Figure 6. The result changes in 6 seconds (Figure 7).



```
SW3(config-if)#span bpdufilter enable
SW3(config-if)#do sh clock
20:36:14.354 UTC Tue May 7 2013
```

Figure 6 - Implementing BPDU filter



```
May  7 20:36:20.008: MST[0]: updt roles, information on root port Fa0/21 expired
May  7 20:36:20.008: MST[0]: Fa0/23 is now root port
May  7 20:36:20.008: MST[0]: Fa0/21 state change forwarding -> blocking
May  7 20:36:20.008: MST[0]: Fa0/3 state change forwarding -> blocking
May  7 20:36:20.008: MST[0]: Fa0/5 state change forwarding -> blocking
May  7 20:36:20.008: MST[0]: Fa0/23 state change blocking -> forwarding
May  7 20:36:20.008: MST[0]: Fa0/21 is now designated
May  7 20:36:20.012: MST[0]: sending proposal on Fa0/21
May  7 20:36:20.012: MST[0]: sending proposal on Fa0/3
May  7 20:36:20.012: MST[0]: sending proposal on Fa0/5
```

Figure 7 - From SW2

Conclusion

Switched networks should meet stringent requirements for robustness, resiliency and high availability. With growing technologies such as Voice over IP (VoIP) and Video over IP, the rapid convergence around link or component failures is no longer a desirable feature: fast convergence is important. However, until recently, redundant switched networks had to rely on the relatively slow 802.1d STP to achieve these goals. MSTP is designed to overcome the major problem with the classic STP protocol. While this feature does not allow accurate and optimal traffic engineering, it does improve the use of redundant links. By using regions, MSTP allows you to isolate different physical topologies while maintaining the Layer 2 connectivity between regions.

REFERENCES

1. Narbik Kocharians, Peter Paluch, Terry Vinson. CCIE Routing and Switching v5.0 Official Cert Guide Library (5th Edition)/ Narbik Kocharians, Peter Paluch, Terry Vinson - Cisco Press; 5 edition, December 20, 2014. - C. 103-160.

2. David Hucaby. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide/ Narbik Kocharians - Cisco Press; 1 edition, December 26, 2014. - C. 147-241.

3. Raymond Lacoste, Kevin Wallace. CCNP Routing and Switching TSHOOT 300-135 Official Cert Guide / Raymond Lacoste, Kevin Wallace - Cisco Press; 1 edition, December 20, 2014. - C. 129-169.

4. Narbik Kocharians. CCIE Routing and Switching v5.1 Foundations: Bridging the Gap Between CCNP and CCIE / Narbik Kocharians - Cisco Press; 1 edition, June 1, 2017. C. 35-164.

5. Adaptive Root Election for Multiple Spanning Trees of Ethernet VLANs. [Электронный ресурс]. — URL: https://www.researchgate.net/publication/322511170_Adaptive_Root_Election_for_Multiple_Spanning_Trees_of_Ethernet_VLANs (дата обращения: December 2017).

6. Traffic Engineering for Multiple Spanning Tree Protocol in Large Data Centers. [Электронный ресурс]. — URL: https://www.researchgate.net/publication/224261376_Traffic_engineering_for_multiple_spanning_tree_protocol_in_large_data_centers (дата обращения: October 2011).