**SPANNING TREE PROTOCOLS AND SHORTEST PATH BRIDGING**



**Final Report**

**By:   
 Palak Lodha CWID: 805589165**

**Chirag Padsala CWID: 805613197**

**CPSC : 558-02 13470 (Spring 2017)**

**Professor : Willie Peng**

**Department of Computer Science**

**California State University , Fullerton**

**May 19, 2017**

**Table of Contents**

1. Abstract
2. Introduction
3. Motivation
4. Project Description
   1. Spanning Tree Protocol
   2. Rapid Spanning Tree Protocol
   3. Multiple Spanning Tree Protocol
   4. Project Screenshots
   5. Per-VLAN Spanning Tree
   6. Shortest Path Bridging
5. Conclusion
6. References

**Table Of Figures**

1. Figure 1: BPDU Fields.
2. Figure 2: STP Port State.
3. Figure 3: State Transition Diagram of STP.
4. Figure 4: RSTP Port State.
5. Figure 5: STP vs RSTP Ports.
6. Figure 6: STP vs. RSTP BPDU.
7. Figure 7: MSTP Configuration.
8. Figure 8: Switches for implementing STP protocols.
9. Figure 9: After Co-axial cable connection (Election Process).
10. Figure 10: Implementation of STP protocol and port state changes.
11. Figure 11: After successful STP implementation.
12. Figure 12: Showing protocol type IEEE i.e.; STP.
13. Figure 13: Changing STP to RSTP via Command Line Interface (CLI), leading to port state change and re-election.
14. Figure 14: RSTP protocol established.
15. Figure 15: CLI showing protocol type implemented i.e.; RSTP
16. Figure 16: Working network with message forward from laptop 2 to laptop 1.
17. Figure 17 : PVST+ configuration
18. Figure 18: Configuration of switch S1
19. Figure 19: Output of the configuration
20. Figure 20 : Interface configuration
21. Figure 21 : Ping message using Command prompt

**Abstract**

Ethernet is a difficult and demanding taskmaster. The success and longevity of Ethernet can be put down to the fact that it has been able to evolve to accommodate new requirements, both in its original LAN application space and in the increasing proportion of Provider networking space. STP errors are very common and during the past 15 years we have witnessed the same errors being made over-and-over again. The most serious shortcoming is that STP has a brittle failure mode that can bring down entire data center or campus networks when something goes wrong. Essentially a replacement for the Spanning Tree Protocol (STP) and other point technologies (MSTP, RTSP, MMRP, etc.), SPB’s real value is its ability to enable unparalleled flexibility when building, deploying, and managing Ethernet networks. A natural, sympathetic evolution of Ethernet, SPB is all about efficiency, virtualization, and ease-of use. With SPB, you choose your migration path and pace. By doing for next-generation networks what the Virtual Machine did for server virtualization, SPB enables truly powerful and dynamic networks that are easier to plan, build, and run.

**Introduction**

STP was created to prevent bridge loops by allowing only one path between network switches or ports. STP was originally standardized as IEEE 802.1D.Shortest path bridging is an evolution of the various spanning tree protocol, and is meant to replace the spanning tree protocol (STP). On March 4th2006, 802.1aq draft was posted and on March 2012 IEEE approved 802.1aq standard.SPB is fully backward compatible with all the various spanning tree protocols. In the same way that the Virtual LAN (VLAN) enabled a new design approach for a single network, SPB’s creators see this new technology as a means to dramatically empowering distributed, interconnected, high-performance enterprise networking infrastructure. Based on a proven link state routing protocol, SPB combines decades of experience with IS-IS and Ethernet to deliver more power and scalability than its predecessors. Using the IEEE’s next generation VLAN, called an “I-SID”, SPB supports 16-million unique Services (compared with the VLAN limit of four thousand). And, because SPB’s I-SID is a true Service ID, once it is provisioned at the edge, the network core automatically interconnects like I-SID endpoints to create a contiguous “Service” that leverages all links and equal cost connections using an enhanced shortest path algorithm. Making Ethernet networks easier to use, SPB preserves the plug-and-play nature that established Ethernet as the de facto protocol at Layer 2, just as IP dominates at Layer 3. And, because it enhances IP management by improving Ethernet, SPB enables more dynamic deployments that are easier to maintain than attempts that use other technologies. Minimizing complexity while delivering vastly more functionality and flexibility, SPB eliminates the need to manage IP subnet overlays and/or to provision complex topologies of tagged trunks between Switches. With SPB, new network services are provisioned at the edge of the network. Decreasing the configuration burden and reducing errors, this model for simplified endpoint provisioning leverages a proven carriergrade link state protocol to automatically and instantaneously build the logical, optimized topology between access points.

**Motivation**

We got motivation to understand and dig deeper into this field by the following two instances:

* In May 2013, the first public multi-vendor interoperability was demonstrated as SPB served as the backbone for Interop 2013 in Las Vegas.
* The 2014 Winter Olympics were the first "fabric-enabled" Games using Shortest Path Bridging (SPB) "IEEE 802.1aq" technology. During the games this fabric network was capable of handling up to 54,000 Gbit/s (54 Tbit/s) of traffic. In 2013 and 2014 SPB was used to build the Interop Net backbone with only 1/10 the resources of prior years. During Interop 2014 SPB was used as the backbone protocol which can enable Software-defined networking (SDN) functionalities.

**Project Description**

1. **Spanning Tree Protocol (STP):**

Dr. Radia Perlman invented STP in 1985 at the Digital Equipment Corporation and was known as IEEE 802.1D. Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP was designed to provide “plug-and-play” operation for large Layer 2 networks based on shared Ethernet. STP forces redundant data path into a blocked state.

Operation of STP: The working of STP starts with the root switch selection process called as election process. During the election stage each switch transmits BPDU (Bridge protocol detection unit) to the all connected switch. The switch with the lowest mac “address + priority” becomes the root bridge. Also, administrator can select any switch as root bridge by giving switch the priority over other switches. After the root bridge is elected, all the port states and roles are identified. The port heading towards root switch are designated port. The port from the root switch as identifies as root port. If the port is neither root nor designated after avoiding the loops is identified as blocking port. The election process is shown in the project screenshot section below.

Bridges & Switches in STP: Bridges which are replaced by switches now-a-days can be either of the three types namely:

* Bridge: A bridge connects two or more LAN segments. As of today’s, switch based networks. For STP switch = bridge.
* Root Bridge: It’s the bridge (or switch) that provides connectivity for all segments. Every bridge in a LAN has a path leading towards root bridge. Root bridge is elected automatically based on elections and it can be elected/changed by the administrator.
* Non-Root Bridge: A bridge which is not the Root Bridge is considered Non-Root Bridge.

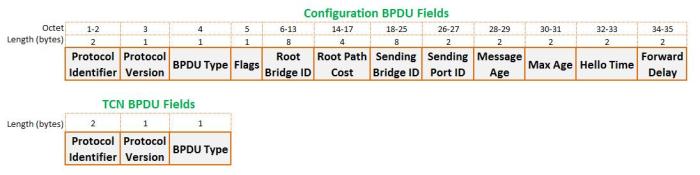
BPDU in STP:

Figure 1: BPDU Fields.

* Protocol ID: Contains the value 0000 for IEEE 802.1D.
* Version ID: Contains the value zero.
* Flags: The Topology Change (TC) bit signals a topology change. The Topology Change Acknowledgment (TCA) bit is set to acknowledge receipt of a configuration message.
* Root Bridge ID: Identifies the root bridge by listing its 2-byte priority number followed by its 6-byte MAC address.
* Root Path Cost: Contains the cost of the path from the bridge to the Root Bridge.
* Sender Bridge ID: Identifies the Sender bridge by listing its 2-byte priority number followed by its 6-byte MAC address.
* Port ID: Identifies the port from which the configuration message was sent.
* Message Age: The amount of time elapsed since the BPDU sent by Root Bridge (10 sec).
* Maximum Age: Indicates when the current configuration message should be deleted (20 sec).
* Hello time: Provides the time between Root Bridge configuration messages.
* Forward Delay: Provides the length of time that bridges should wait before transitioning to a new state after a topology change (15 sec).

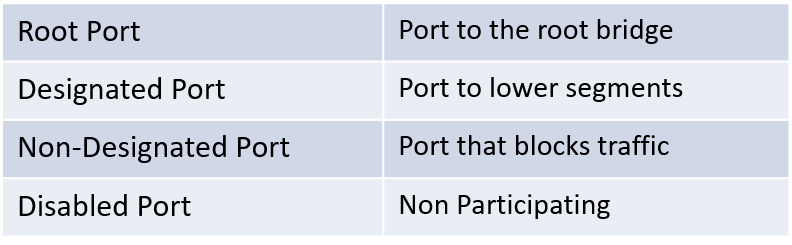
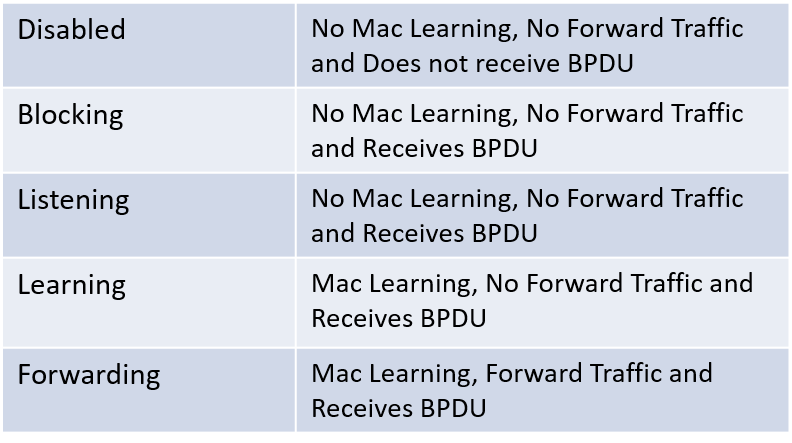
STP Port State & Roles:

Figure 2: STP Port State.

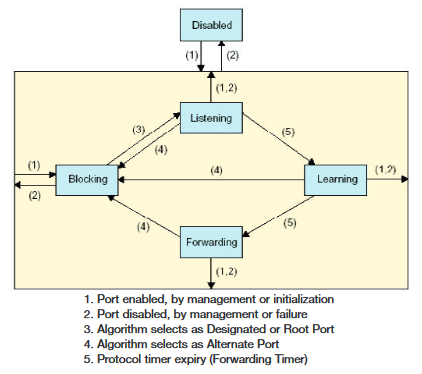
STP State Transition Diagram:

Figure 3: State Transition Diagram of STP.

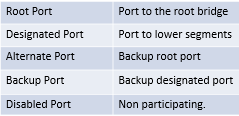
The above figure shows the state transition between port types in STP. The port which is disabled by administrator can reach to forwarding or blocking state once it is activated to work in the protocol. It depends on the root bridge and the path cost. The more the path cost to the root bridge higher the chances of port getting blocked and vice-versa for the forwarding port. The numbering in the above diagram indicates: 1) Port enabled, by administrator or initialization, 2) Port disabled by administrator or failure, 3) Algorithm selects as Designated or root port, 4) Algorithm selects as Alternate port, 5) Protocol timer expiry (Forwarding timer).

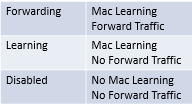
1. **Rapid Spanning Tree Protocol (RSTP):**

The original Spanning Tree Protocol is defined in the IEEE 802.1D 1998 specification. A newer version called Rapid Spanning Tree Protocol (RSTP) was originally defined in the IEEE 802.1w draft specification and later incorporated into the IEEE 802.1D-2004 specification. RSTP provides significantly faster spanning tree convergence during creation and even after a topology change, introducing new convergence behaviors and bridge port roles compared with STP to do this. IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w in 2011. RSTP is backward compatible; it is designed to be compatible and interoperable with the legacy STP.

Operation of RSTP: RSTP operation is like STP as mentioned in operation of STP, but it’s faster compared to STP because: RSTP only should wait 3\*Hello (default 6 seconds). It eliminates the forward delay (default 15 seconds) time in Listening States. It eliminates the forward delay (default 15 seconds) time in Learning States. Where STP takes 45-50 seconds to execute, RSTP only takes 6-8 seconds. In RSTP disabled, blocking and listening port of STP are replaced by Discard port.

BPDU in RSTP: RSTP work on a new BPDU format which has the 8-bit flag which differ from the STP BPDU. The 8 bit functions are as mentioned: 0: topology change (TC), 1: Proposal, 2-3: Port role, 4: Learning, 5: Forwarding, 6: Agreement and 7: Topology change acknowledgement.

RSTP Port States & Roles:

 Figure 4: RSTP Port State.

STP vs RSTP:

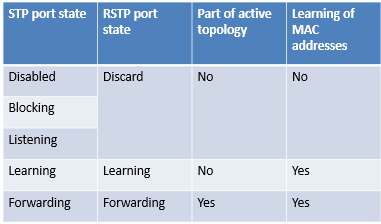
Difference between STP and RSTP’s port state and activities can be understood using the table below.

Figure 5: STP vs RSTP Ports.

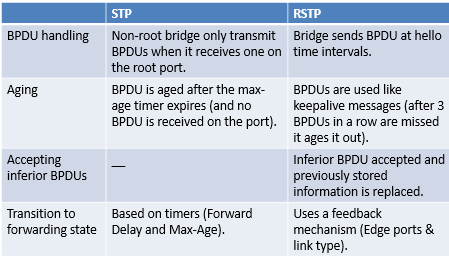
Difference between STP and RSTP’s BPDU factors and working can easily be understood using the table below.

Figure 6: STP vs. RSTP BPDU.

1. **Multiple Spanning Tree Protocol (MSTP):**

Multiple Spanning Tree Protocol (MSTP) was first specified in IEEE 802.1s and is standardized in IEEE 802.1Q. MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support many VLANs. MSTP provides multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance, or forwarding path, does not affect other instances. As, MSTP allows mapping multiple VLANs to a single spanning tree instance. It reduces the resource requirement while preserving the advantages of having multiple spanning trees for load balancing purposes. In the example below, the VLANs are mapped to 2 separate spanning tree instances as follows:

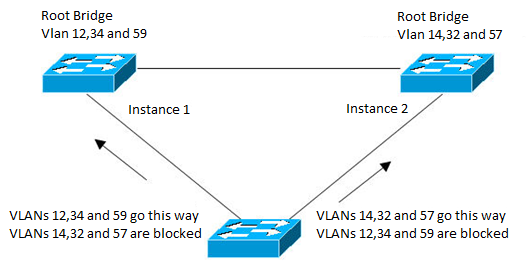
* VLANs 12,34 and 59: Spanning tree instance 1
* VLANs 14,32 and 57: Spanning tree instance 2

Figure 7: MSTP Configuration.

Configuration of MSTP: The above image MSTP can be configured using the command line interface as follows:

* Sw1(config-mst)# spanning tree mode mst
* Sw1(config)# spanning-tree instance configuration
* Sw1(config-mst)# instance 1 vlan 12,34,59
* Sw1(config-mst)# instance 1 vlan 12,34,59
* Sw1(config-mst)# instance 2 vlan 14,32,57
* Sw1(config-mst)# spanning-tree mst 1 root primary
* Sw1(config-mst)# spanning-tree mst 2 root secondary
* Sw1(config-mst)# spanning tree mode mst
* Similarly, we configure Sw2 (Switch 2) with mst 1 as secondary and mst 2 as primary.

MSTP Port Type and Transition: A port can transit from one state to another if the following mentioned conditions is met or occurred:

* Backup Port if a message is received from the bridge itself.
* Root Port if a message is received with a better root or a message is received with the same root.
* Designated Port if it’s in Initialization or a message with a better path cost to root or a message with the same path cost to root.
* Alternate Port if the port it not backup, not root port and not designated or the port is a Master Port – in the MSTIs or the port is connected to a LAN or a bridge in a different region.

STP & RSTP vs. MSTP: MSTP- operation 2006, The 802.1D (STP) and 802.1w (RSTP) spanning tree protocols operate without regard to a network’s VLAN configuration, and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology. The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

MSTP- operation 2006, While the per-VLAN spanning tree, approach adopted by some vendors overcomes the network utilization problems inherent in using STP or RSTP, using a per-VLAN technology with multiple VLANs can overload the switch’s CPU. MSTP on the switches covered in this guide complies with the IEEE 802.1s standard, and extends STP and RSTP functionality to map multiple independent spanning tree instances onto a physical topology. With MSTP, each spanning tree instance can include one or more VLANs and applies a separate, per-instance forwarding topology. Thus, where a port belongs to multiple VLANs, it may be dynamically blocked in one spanning tree instance, but forwarding in another instance. This achieves load-balancing across the network while keeping the switch’s CPU load at a moderate level. MSTP provides fault tolerance through rapid, automatic reconfiguration if there is a failure in a network’s physical topology. The MSTP configuration commands operate exactly like RSTP commands and MSTP is backward-compatible with the RSTP-enabled and STP-enabled switches in your network.

1. **Project Screenshots:**

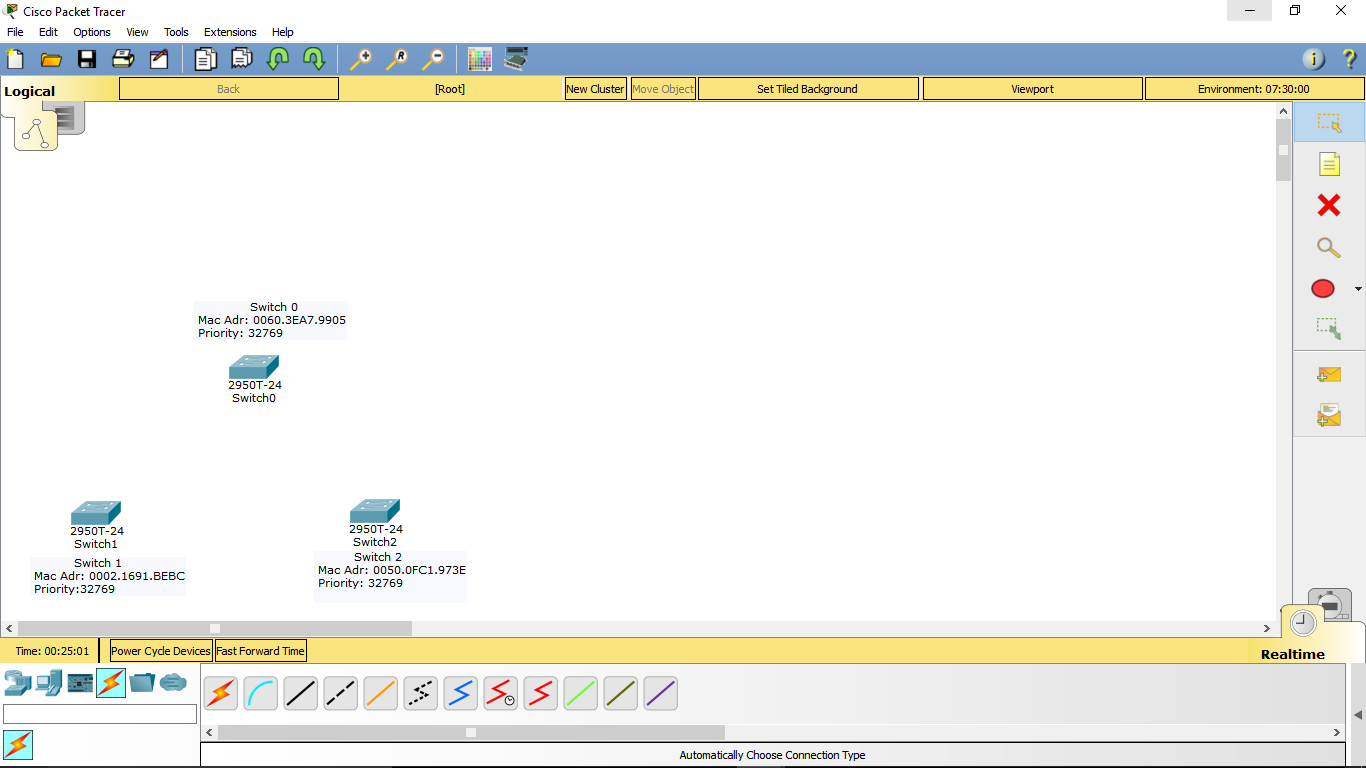


Figure 8: Switches for implementing STP protocols.

The above figure is snipped from cisco packet tracer. It shows the switches with their Mac Addresses and Priorities. These are the switches which will be used to implement STP & RSTP protocol.

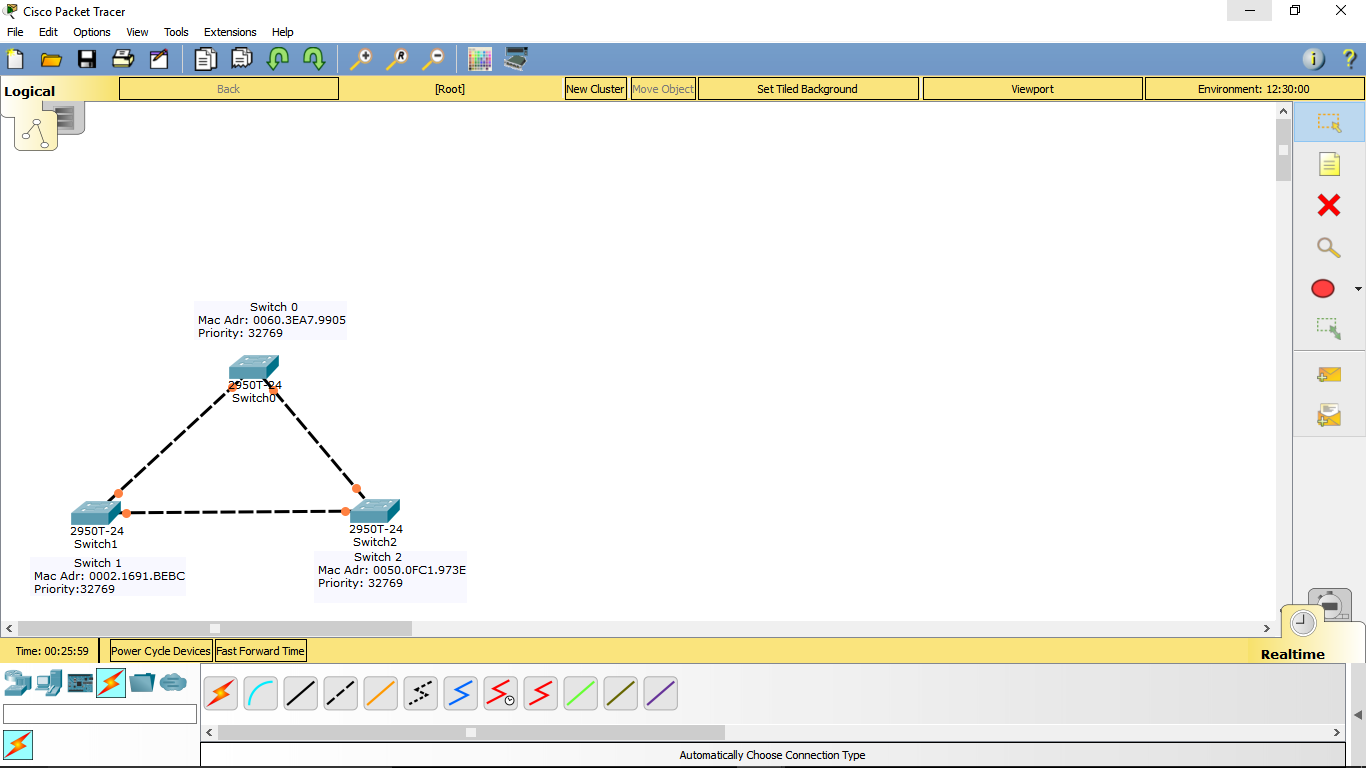


Figure 9: After Co-axial cable connection (Election Process).

The above figure shows the connection among the switches which is done via a co-axial cable. The figure shows the states of port right after the connection. Right after the connection election process takes place in background, which leads to port state changes multiple times.

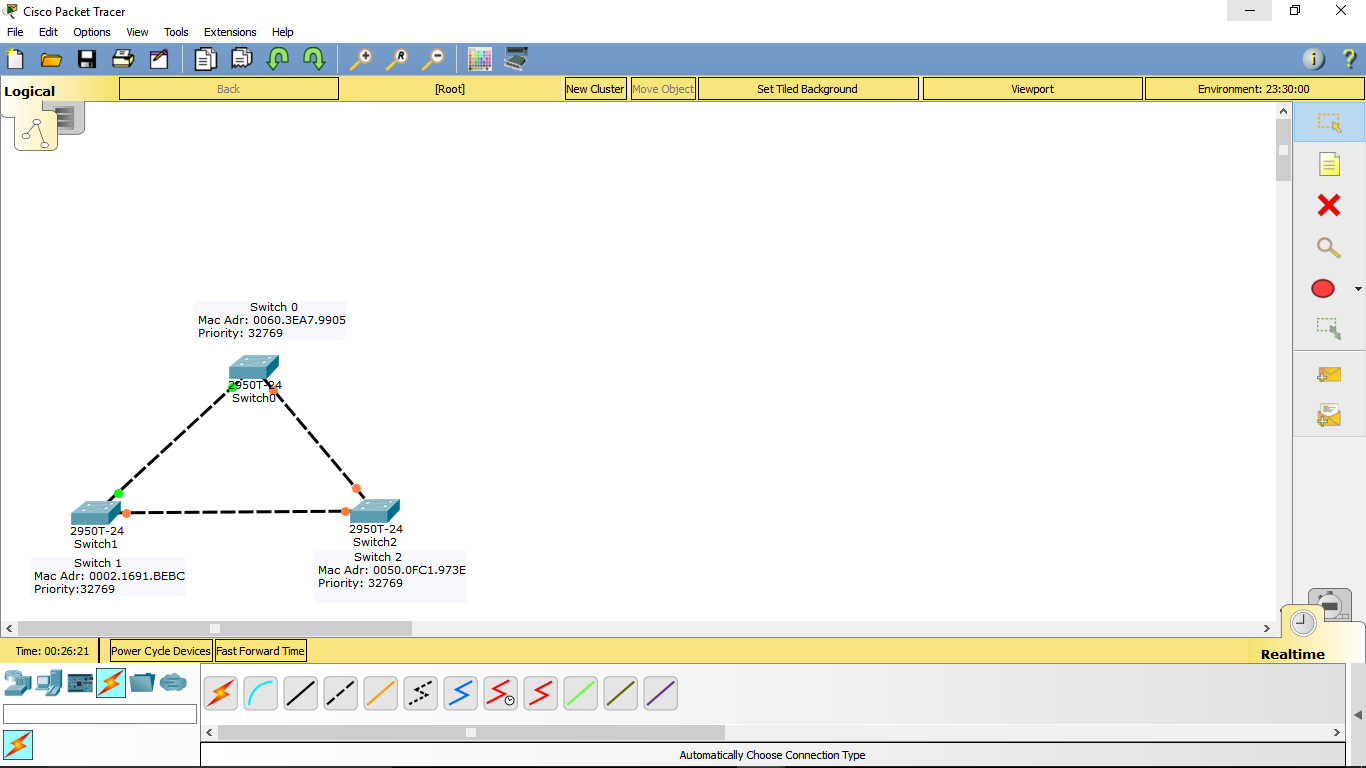


Figure 10: Implementation of STP protocol and port state changes.

The above figure displays the implementation of STP protocol which usually takes 40-50 sec, thus leading to port state change several times. The red connection dot denotes blocking state and green connection dot denotes forwarding state of the port.

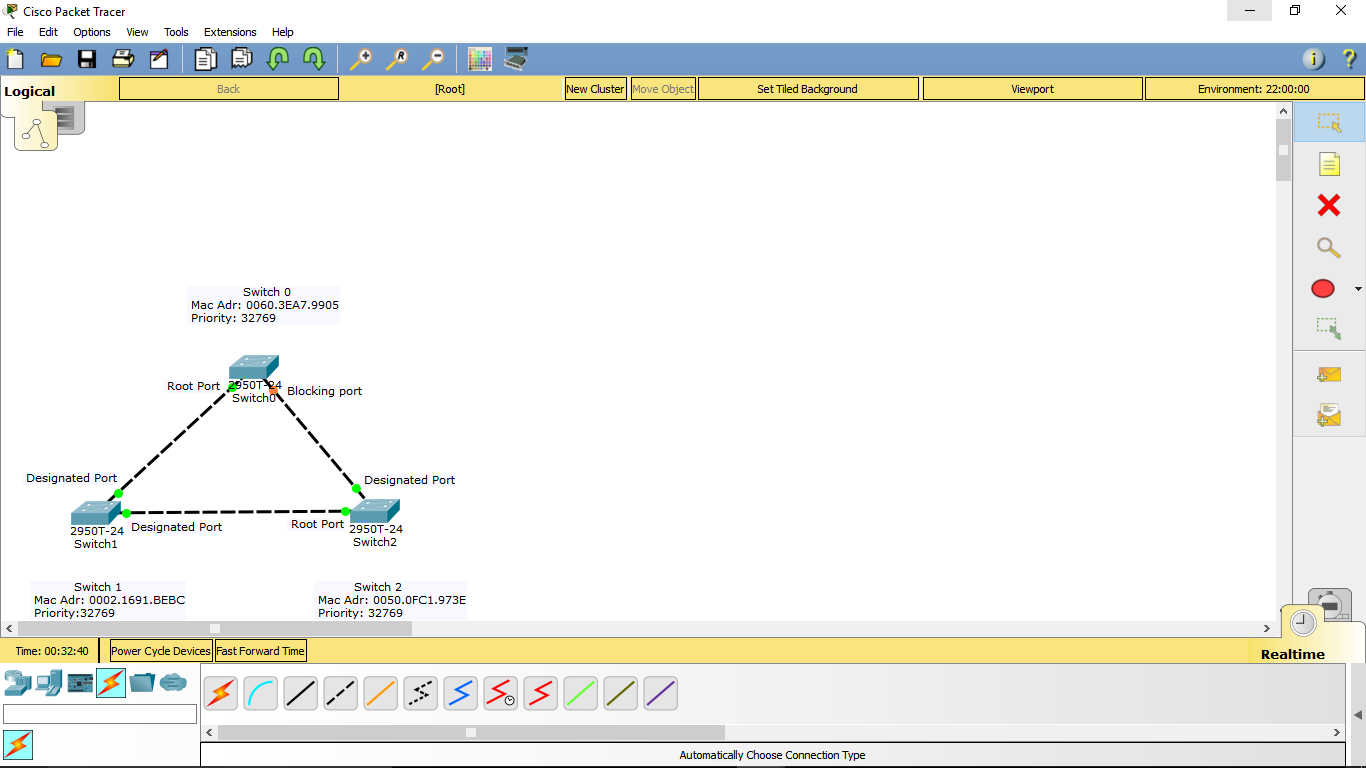


Figure 11: After successful STP implementation.

After successful implementation of STP protocol it look likes the above figure. As the figure displays the state of all the ports and that the Switch 1 is the root bridge because of the smaller mac address, thus making the ports as designated ports.

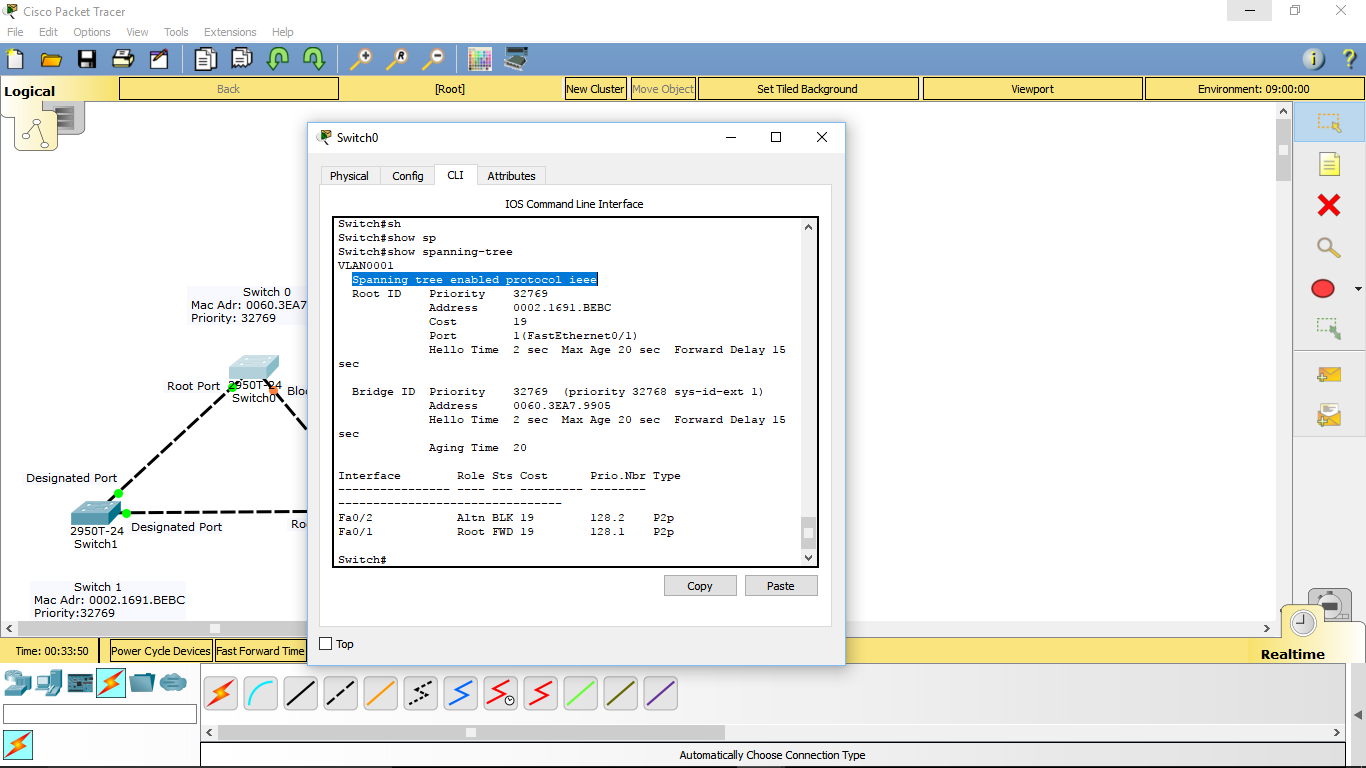


Figure 12: Showing protocol type IEEE i.e.; STP.

The above figure shows the configuration of spanning tree and displays the information of the root bridge and itself. It can be seen in CLI i.e.; Command Line Interface using “show spanning-tree” command. As the highlighted line in the above pic says that its running the STP protocol which is known as IEEE in packet tracer.

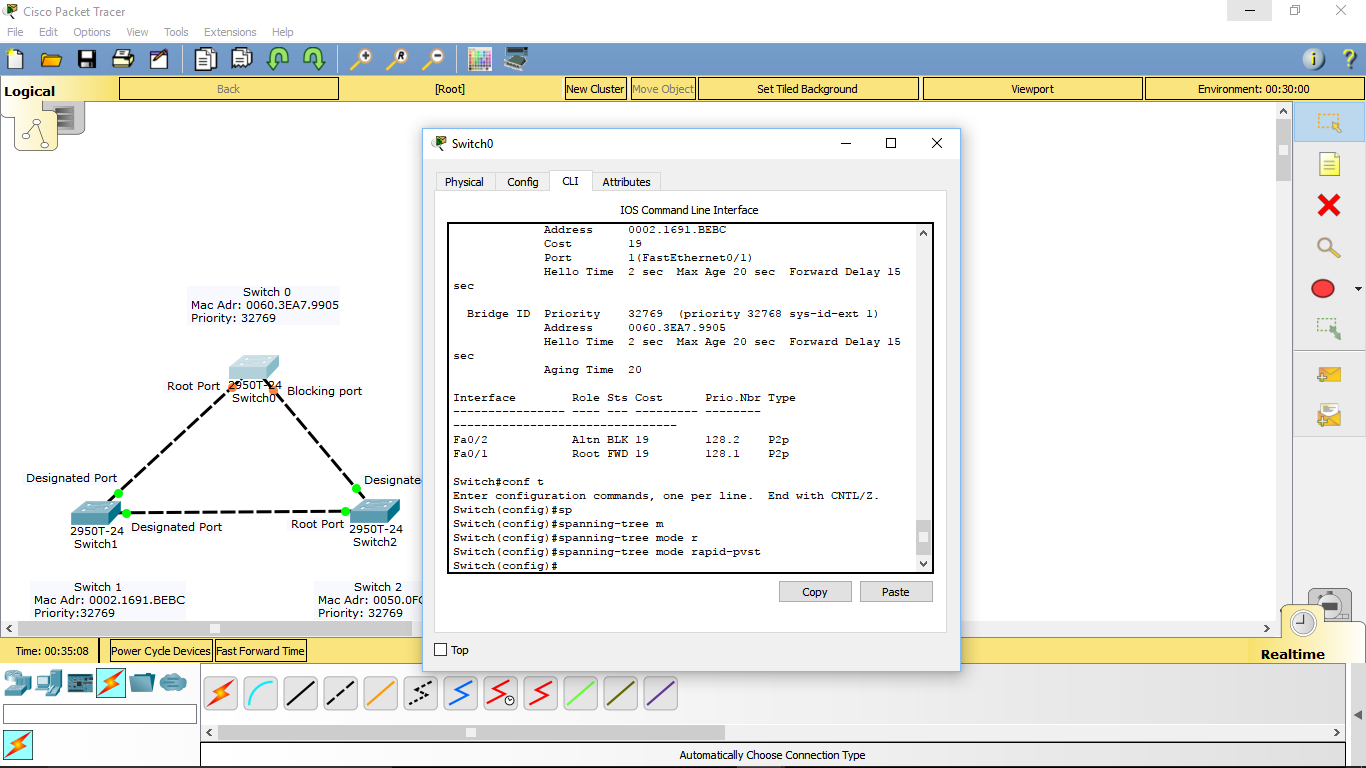


Figure 13: Changing STP to RSTP via Command Line Interface (CLI), leading to port state change and re-election.

The above figure shows the commands to change the spanning tree protocol to rapid spanning tree protocol. It can be accomplished after entering the configuration of the switch in the CLI and by running “spanning-tree mode rapid-pvst” command. And, displays the change of the port states because of the re-election and implementation of RSTP protocol.



Figure 14: RSTP protocol established.

The above figure displays the successful implementation of the RSTP protocol, and all the states of the ports and the switches with mac addresses and their priorities.

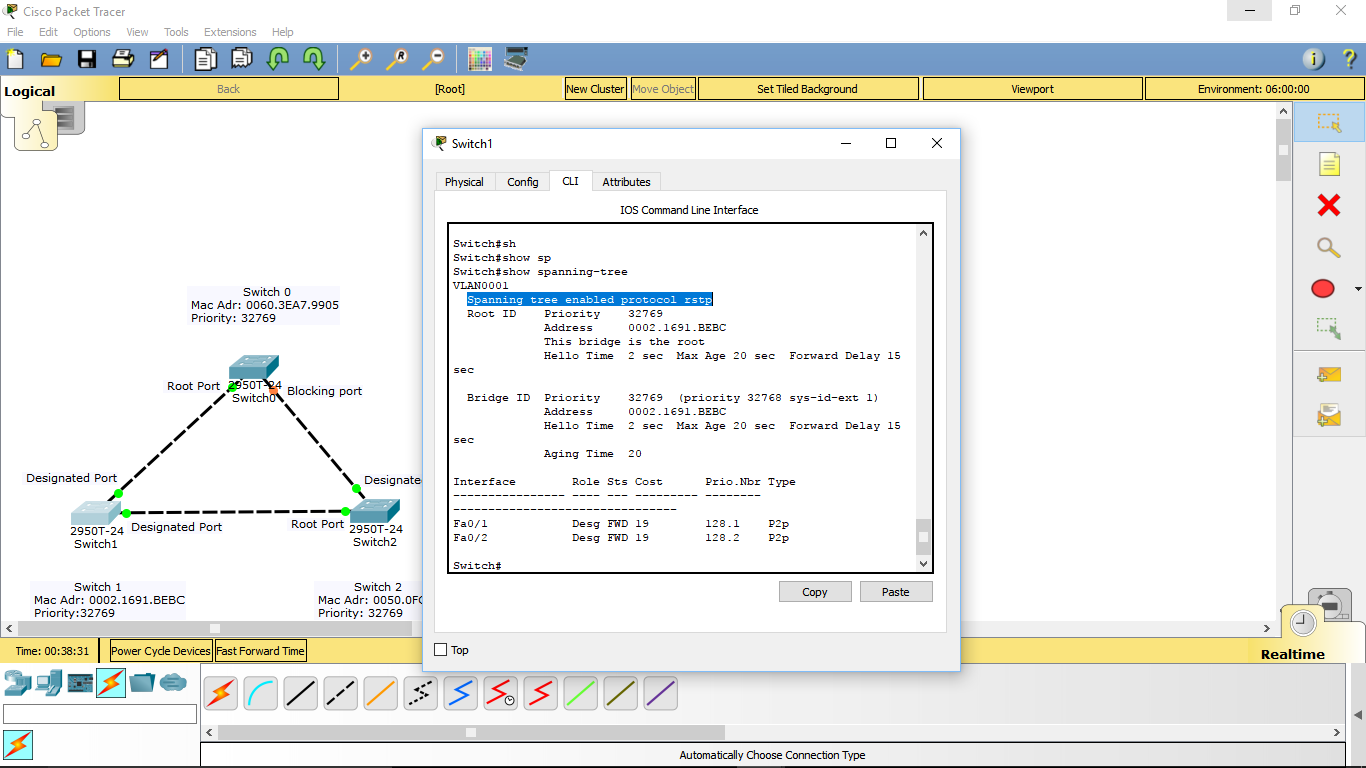


Figure 15: CLI showing protocol type implemented i.e.; RSTP.

The highlighted text in the above figure shows that the network is running the RSTP protocol successfully.

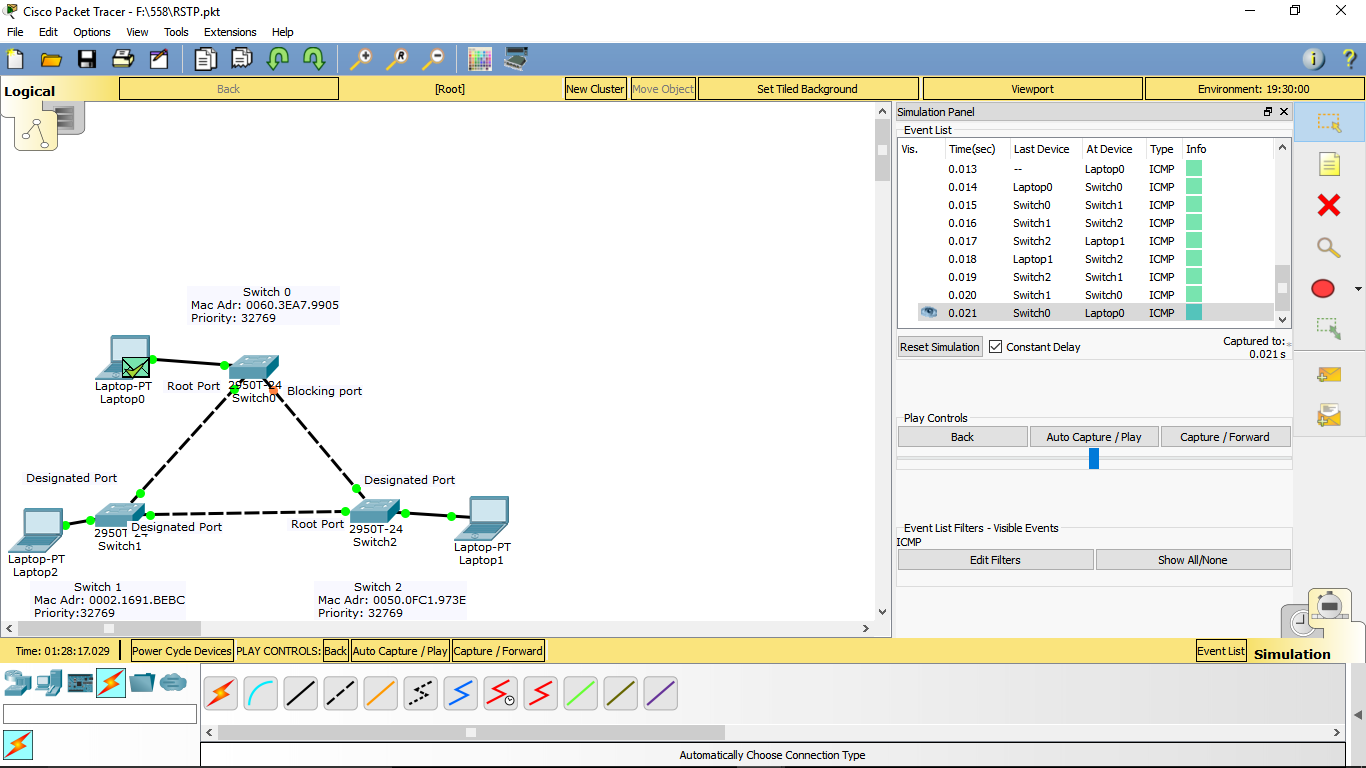
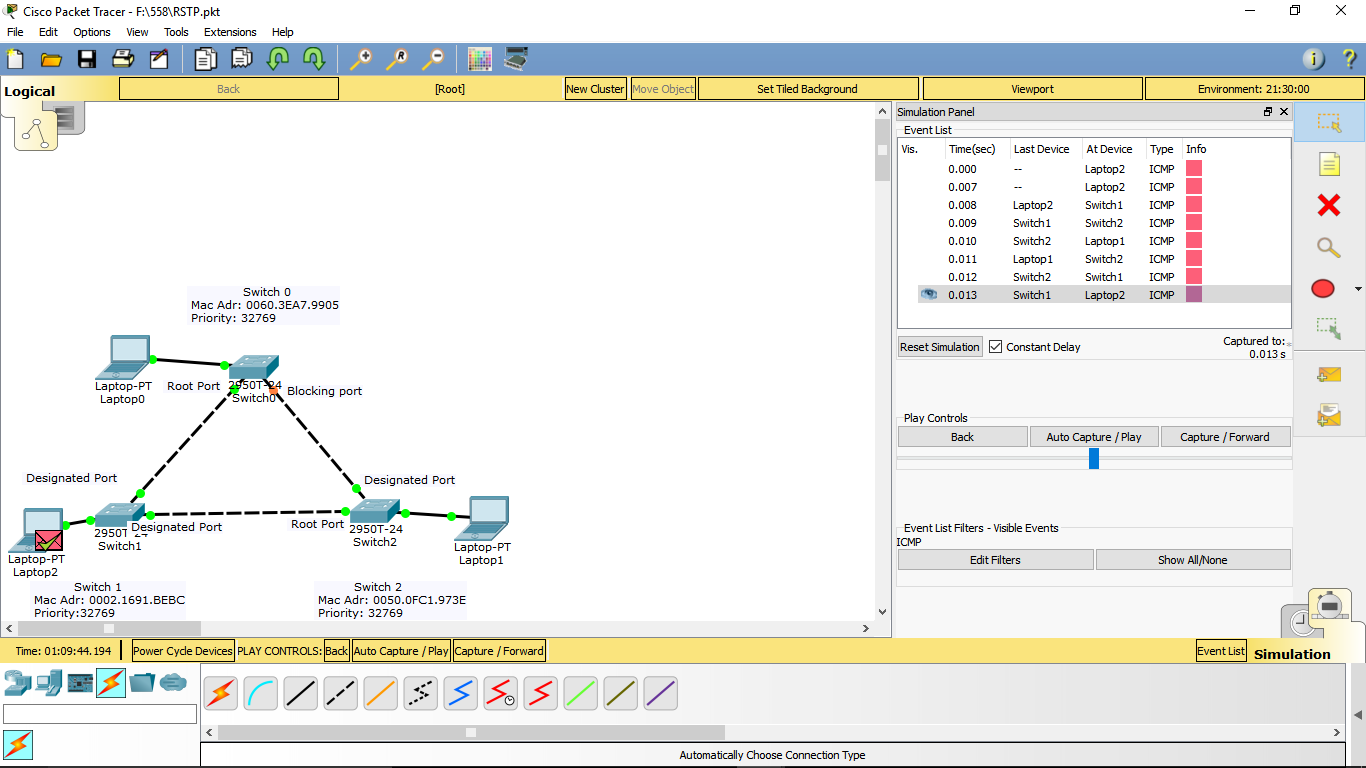


Figure 16: Working network with message forward from laptop 2 to laptop 1.

The above figure shows the working of the RSTP protocol with the help of packet forwarding from laptop 0 to laptop 1 and back to laptop 0. The green tick inside the green message symbol means the forwarding was successful. Also, the whole flow of the packet from one laptop to the respective switches and then returning to the origin can be seen in the simulation panel of the above figure.



1. **PVST and PVST+ :**

Per-VLAN spanning tree protocol plus (PVST+) is a Cisco proprietary protocol that expands on the Spanning Tree Protocol (STP) by allowing a separate spanning tree for each VLAN. Cisco first developed this protocol as PVST, which worked with the Cisco ISL trunking protocol, and then later developed PVST+ which utilizes the 802.1Q trunking protocol.

By creating a separate spanning tree for each VLAN, data traffic from the different VLANs can take different paths across the network, as opposed to all switched traffic taking the same path. This can effectively create a load balancing situation and improve network efficiency.

By default the Cisco switches in Packet Tracer appear to be using PVST+ as the default implementation of spanning tre protocol.

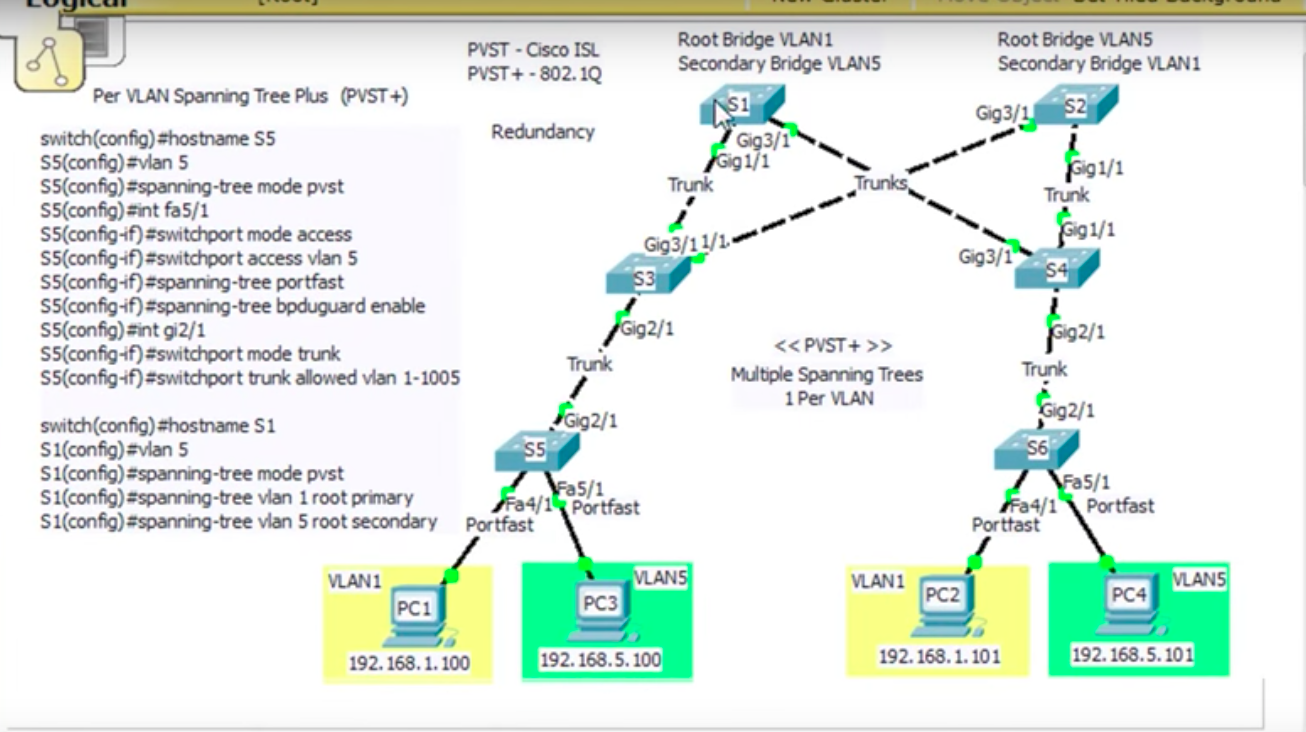


Figure 17 : PVST+ configuration

This figure shows the implementation of PVST+. The switches S1,S2,S3,S4,S5,S6 are all running STP by default but they are actually running PVST+ because they run multiple spanning trees for each VLAN. For each VlAN, there is a spanning tree root bridge that will handle all the spanning tree algorithms in the path cost associated with that VLAN. This protocol helps in redundancy as there is a backup root bridge for each root bridge. Hence, as shown in the figure VLAN5 is the secondary bridge for root bridge VLAN1 and vice versa. If one of the root bridges goes down, the other one would become the root bridge for both VLANs. This is a modern representation of STP. The PC1,PC2,PC3 and PC4 are clients. The clients in yellow are in VLAN1 and in green are in VLAN5. Trunk links are set up between the switches.

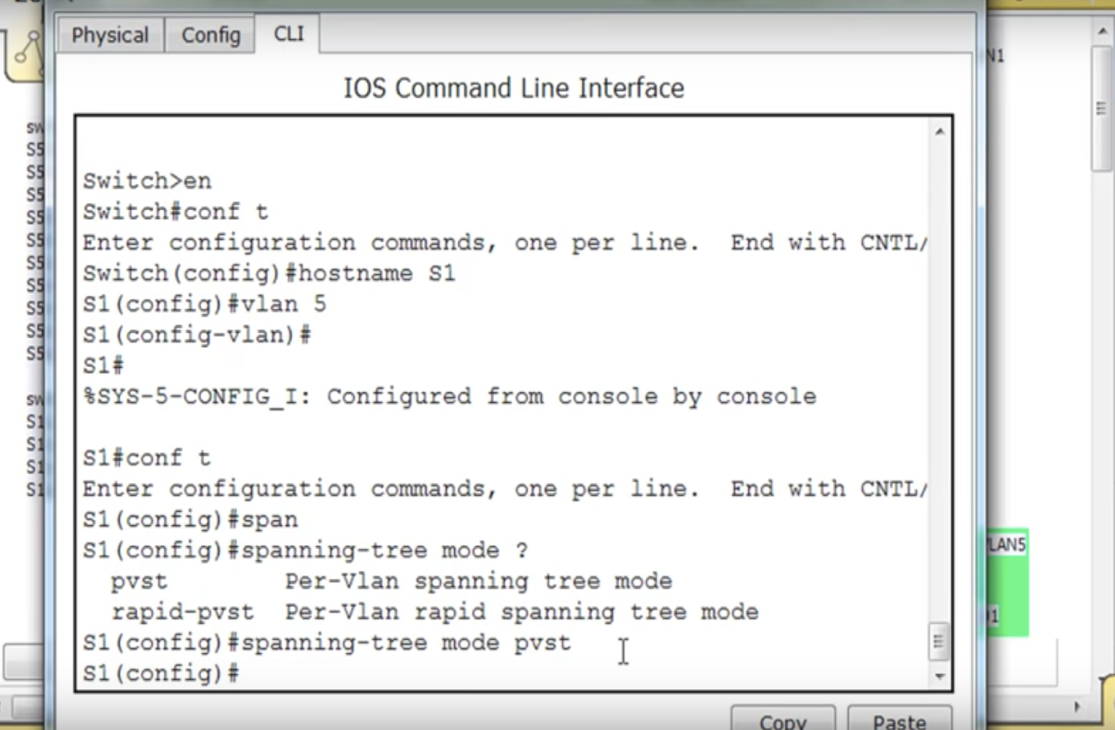


Figure 18: Configuration of switch S1

Switch S1 is the root bridge for VLAN1. To configure the switch the commands as shown in the figure are written. Gigabit port1/1 and gigabit port 3/1are manually configured so that they are trunk links. In the configuration mode, the Per-VLAN spanning tree is actually PVST+ mode.

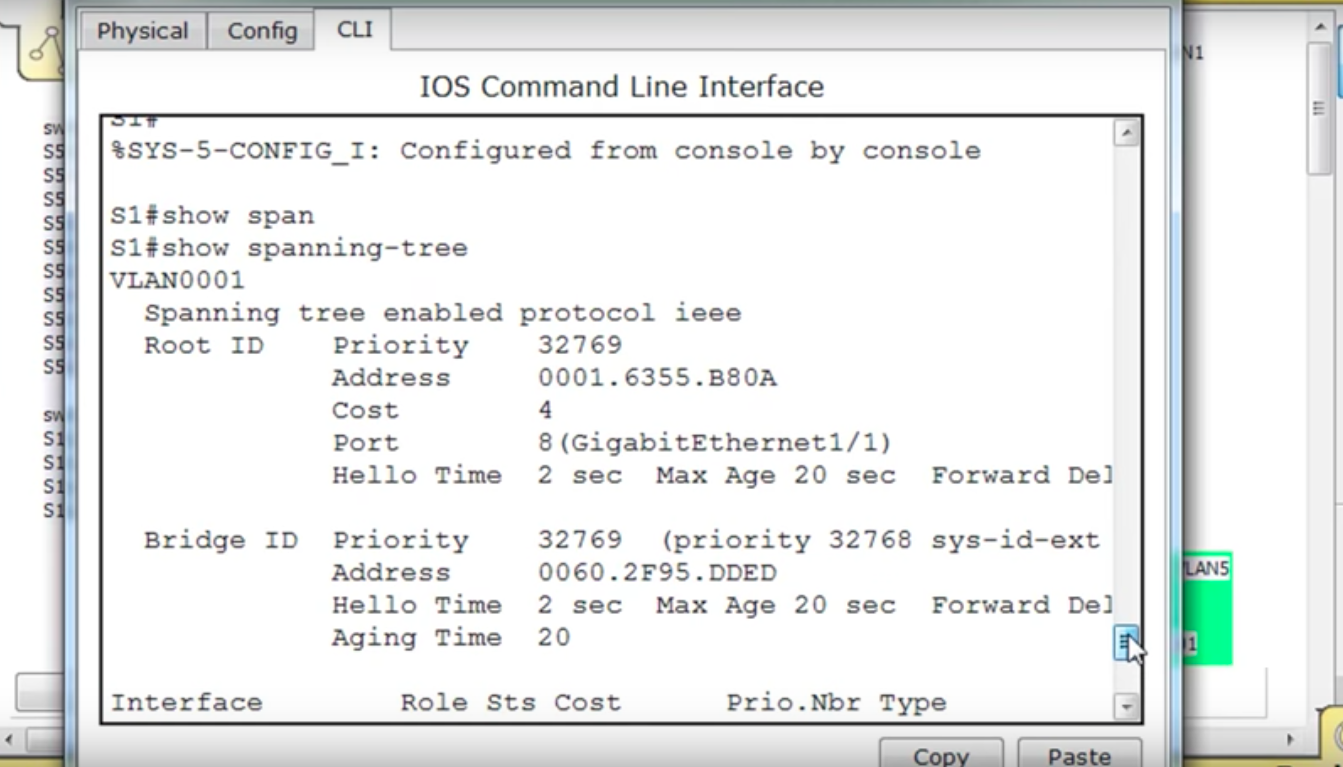


Figure 19: Output of the configuration

These are the results after configuring switch 1. The root ID and the bridge ID include priority, address, cost, port, hello time and aging time. The priority of both the ID’s should be the same.

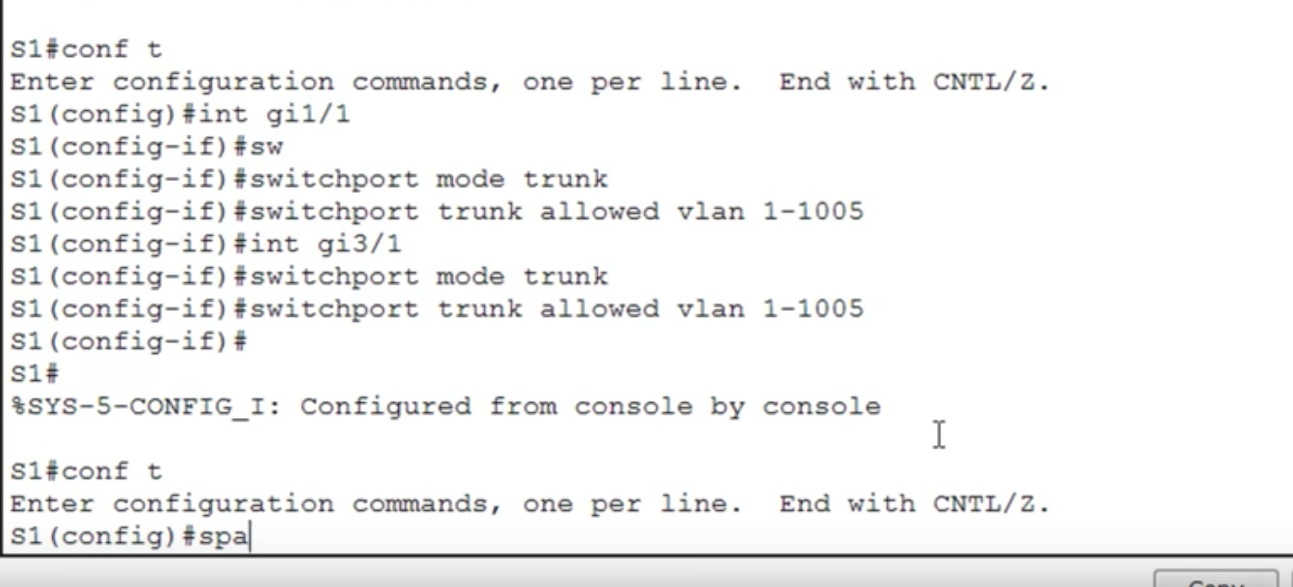


Figure 20 : Interface configuration

The configuration of interface gi 1/1 and gi 1/3 is done in the above figure with switchport mode trunk. After the SHOW RUN command, the gigabitEthernet 1/1 and 3/1 are in switch mode trunk and the other gigabit Ethernet and fast Ethernet are shutdown. Hence, it is configured. All the other ports are configured accordingly.

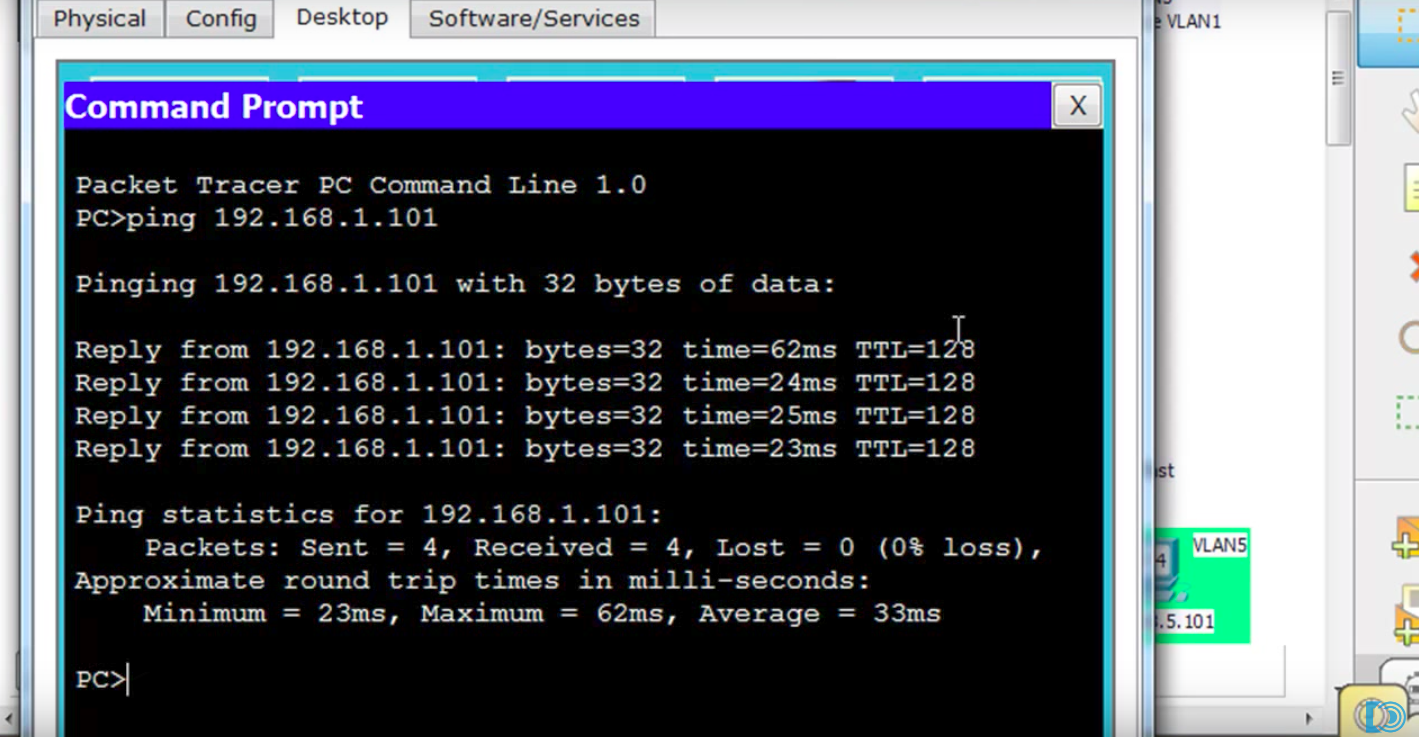


Figure 21 : Ping message using Command prompt

Figure 21 shows the connection between all the switches. It is done by sending a Ping message from one switch to another and how the connection is established between them. It shows the memory and the time for the transfer of the message.

1. **Shortest Path Bridging :**

Shortest Path Bridging (SPB) is being standardized by the IEEE as the next evolution step. It provides shortest path forwarding using layer 2 to provide shortest path forwarding. SPB uses the IS-IS protocol operating at layer 2 allowing for large networks with fast convergence, equal cost paths, and easy provisioning without having to add complex addition protocols in the core to support virtualization of VLAN’s or VRF’s. In summary, all that is needed is to enable SPB and IS-IS in the core and all the virtualization is done on the edge.

The 802.1aq standard supports two modes, SPB VID (SPBV) and SPB MAC (SPBM). Only SPBM supports true virtualization via the use of the 802.1ah MAC-in-MAC encapsulation. SPBV offers shortest path forwarding but with reduced functionality using 802.1ad Q-in-Q tagging for devices which cannot support the 802.1ah MAC-in-MAC encapsulation. All Avaya SPB capable switches support exclusively SPBM. SPBM virtualized services are delineated by ISIDs where the ISID is simply assigned at the BEB to either a VLAN for virtualized layer 2 services, a multicast group for virtualized multicast services, or to a VRF for virtualized layer 3 services. In a SPBM network, each bridge advertises its own unique MAC address using IS-IS which is known as the system-id. The system-id can also be manually provisioned to ease in trouble shooting when looking at the layer 2 forwarding table.

Provisioning an SPB core is as simple as enabling SPB and IS-IS globally on all the nodes and configuring SPB IS-IS interfaces on the core facing links (NNI links). The IS-IS protocol operates at layer 2, it does not need IP addresses configured on the links to form IS-IS adjacencies with neighboring switches (like OSPF does). Hence, there is no need to configure any IP addresses on any of the core links. IS-IS is a link-state protocol which will compute the shortest open path just like OSPF does. It can therefore be deployed on any regular (e.g. square or fully meshed core-to-distribution topologies) or irregular (e.g. ring topologies) fibre plants

**SPB Benefits :**

* Backbone provisioning simplicity

Provisioning an SPB core is as simple as enabling SPB and IS-IS globally on all the nodes and on the core facing links. The IS-IS protocol operates at layer 2, it does not need IP addresses configured on the links to form IS-IS adjacencies with neighboring switches (like OSPF does). Hence there is no need to configure any IP addresses on any of the core links.

* Natively provides virtualized Layer 2 services

Layer 2 virtualization is handled by the Backbone Edge Bridges (BEBs) where the end-user VLAN is mapped into a Backbone Service Instance Identifier (ISID) by local provisioning. Any BEB that has the same ISID configured can participate in the same L2 virtual services network (VSN). IS-IS within the SPB backbone is used as the Layer 2 routing protocol to forward traffic between the BEB and Provider Backbone Core Bridges (BCBs). Only the BEB has knowledge of the L2 VSN and corresponding MAC addresses. The BCB only has knowledge of each Backbone MAC address (B-MAC) used to send traffic across an SPB network.

* Natively provides virtualized routing services

Layer 3 virtualized routing is handled by the Backbone Edge Bridges (BEBs) where the end-user IPv4 enabled VLAN or VLANs are mapped to a Virtualized Routing and Forwarding (VRF) instance. The VRF in turn is mapped into a Backbone Service Instance Identifier (ISID) by local provisioning. Any BEB that has the same ISID configured can participate in the same L3 virtual service network (VSN). IS-IS within the SPB backbone is used as the Layer 2 routing protocol to forward traffic between the BEB and Backbone Core Bridges (BCB). Only the BEB has knowledge of the L3 VSN and corresponding IP/ARP/MAC addresses. The BCB only has knowledge of each Backbone MAC address (B-MAC) used send traffic across an SPB network.

* Adapts to any physical layer / fibre plant

IS-IS is a link-state protocol which will compute the shortest open path just like OSPF does. It can therefore be deployed on any regular (e.g. square or fully meshed core-to-distribution topologies) or irregular (e.g. ring topologies) fibre plants. Whereas OSPF computes the shortest path to destination subnets and then populates the IP routing table with the results, IS-IS (as used with SPB) computes the shortest path to backbone node MAC addresses (B-MACs) and then populates the backbone MAC tables.

* Robust/Scalable link-state routing applied to MAC tables

With SPB, the MAC table is now only populated by the IS-IS control plane. The conventional Ethernet bridging behavior which consisted of (a) “learning” the MAC tables with the source MAC address of packets seen arriving on local ports and (b) flooding unknown and broadcast traffic to all ports no longer apply in an SPB backbone. Furthermore, with SPB, IS-IS is leveraged to build source based forwarding trees for the delivery of multicast and broadcast traffic across the SPB backbone in such a way that the replication of broadcast/multicast traffic within the core is optimized to follow the shortest path from source to leaf nodes.

* Separation between Services and Backbone

Since SPB leverages the MACinMAC encapsulation of 802.1ah (BCB) only the nodes at the edge of the SPB backbone (the Backbone Edge Bridges - BEBs) need to learn the MAC addresses (C-MACs) used within the transported Customer VLANs (L2VSNs). These same nodes, when forwarding traffic into the SPB core will always re-encapsulate the service traffic in a Backbone MAC header with a destination B- MAC corresponding to the destination SPB node across the backbone where the service traffic will get de-capsulated. The encapsulation used is shown in Figure 1. As such, the nodes within the SPB backbone will have no knowledge of the addresses used within the service VSNs (C-MACs or IP addresses) transported across and only need to provide reachability to the B-MAC addresses within the backbone.

**Applications:**

•Anywhere that Spanning Tree is being used.

Take existing STP/MSTP based network and migrate to Shortest Path Routing.

•Ethernet Exchange Points

Big distributed switch to interconnect hundreds of different customers cheaply with L2VPNs.

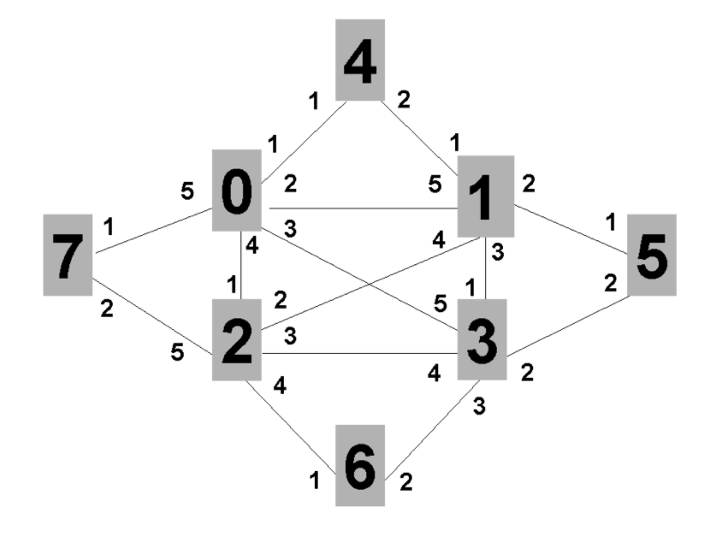
•Metro Ethernet

Light weight metro protocol, L2VPN solution simpler than VPLS with lower capex/opex.

•Wireless backhaul

Use of L2VPN for LTE backhaul

**Example :**



The example consists of 8 participating nodes numbered 0 through 7. These would be switches or routers running the IEEE 802.1aq protocol. Each of the 8 participating nodes has a number of adjacencies numbered 1..5. These would likely correspond to interface indexes, or possibly port numbers. Since 802.1aq does not support parallel interfaces each interface corresponds to an adjacency. The port / interface index numbers are of course local and are shown because the output of the computations produce an interface index (in the case of unicast) or a set of interface indexes (in the case of multicast) which are part of the forwarding information base (FIB) together with a destination MAC address and backbone VID.

The network has a fully meshed inner core of four nodes (0..3) and then four outer nodes (4,5,6 and 7), each [dual-homed](https://en.wikipedia.org/wiki/Dual-homed) onto a pair of inner core nodes.

Normally when nodes come from the factory they have a MAC address assigned which becomes a node identifier but for the purpose of this example we will assume that the nodes have MAC addresses of the form 00:00:00:00:N:00 where N is the node id (0..7) from Figure 1. Therefore, node 2 has a MAC address of 00:00:00:00:02:00. Node 2 is connected to node 7 (00:00:00:00:07:00) via node 2's interface/5.

Node 7 will therefore have a FIB that among other things indicates:

* MAC 00:00:00:05:00 / vid 101 the next hop is interface/1.
* MAC 00:00:00:05:00 / vid 102 the next hop is interface/2.

Node 5 will have exactly the inverse in its FIB:

* MAC 00:00:00:07:00 / vid 101 the next hop is interface/1.
* MAC 00:00:00:07:00 / vid 102 the next hop is interface/2.

The intermediate nodes will also produce consistent results so for example node 1 will have the following entries.

* MAC 00:00:00:07:00 / vid 101 the next hop is interface/5.
* MAC 00:00:00:07:00 / vid 102 the next hop is interface/4.
* MAC 00:00:00:05:00 / vid 101 the next hop is interface/2.
* MAC 00:00:00:05:00 / vid 102 the next hop is interface/2.

And Node 2 will have entries as follows:

* MAC 00:00:00:05:00 / vid 101 the next hop is interface/2.
* MAC 00:00:00:05:00 / vid 102 the next hop is interface/3.
* MAC 00:00:00:07:00 / vid 101 the next hop is interface/5.
* MAC 00:00:00:07:00 / vid 102 the next hop is interface/5.

**Conclusion**

SPB is the replacement for the older spanning tree protocols: IEEE 802.1D, IEEE 802.1w, IEEE 802.1s. These blocked any redundant paths that could result in a layer 2 loop, whereas SPB allows all paths to be active with multiple equal cost paths, provides much larger layer 2 topologies, supports faster convergence times, and improves the efficiency by allowing traffic to load share across all paths of a mesh network. Using this model, network administrators can deploy IP networking anywhere they need it, on the fly, and actually improve application performance. No longer bound by physical topology, associated subnet attachments are located where they are needed and are available when they are needed; time-to-service is dramatically enhanced. Imagine a network, in the next building or the next state, where adding new ports to an existing application or community of interest is as easy as configuring the access port of local Switches and having the network automatically interconnect all as part of a common service. This is the model that Avaya and the IEEE are delivering: any service, anywhere in your network, available exactly when it is needed. In addition, thanks to its IEEE heritage, SPB can co-exist with your existing Ethernet infrastructure without disrupting your operational model.

**References**

[1]Charlie Schluting, 2007. Understanding Spanning Tree.

<http://www.enterprisenetworkingplanet.com/netsp/article.php/3580966/Networking-101-Understanding-Spanning-Tree.htm>

[2]Cisco. Per VLAN Spanning Tree (PVST).

[http://www.cisco.com/en/US/tech/tk389/tk621/tk846/tsd\_technology\_support\_ sub-protocol\_home.html](http://www.cisco.com/en/US/tech/tk389/tk621/tk846/tsd_technology_support_sub-protocol_home.html)

[3]Juniper Networks(2014). Rapid Spanning Tree Protocol Port States and Port Roles.

[https://www.juniper.net/techpubs/en\_US/junos12.3/topics/concept/mx-series- rstp-port-states-roles.html](https://www.juniper.net/techpubs/en_US/junos12.3/topics/concept/mx-series-rstp-port-states-roles.html)

[4]Wikipedia(2017). Spanning Tree Protocol.

<https://en.wikipedia.org/wiki/Spanning_Tree_Protocol>

[5]Multiple Instance Spanning-Tree Operation (2006).

[ftp.hp.com/pub/networking/software/2900-AdvTrafficMgmt-Aug2006-59916197-Chap04.pdf](http://ftp.hp.com/pub/networking/software/2900-AdvTrafficMgmt-Aug2006-59916197-Chap04.pdf)

[6]<http://www.networkcomputing.com/networking/shortest-path-bridging-will-rock-your-world/1689548769>

[7]<http://www.networkcomputing.com/networking/shortest-path-bridging-will-rock-your-world/1689548769/page/0/1>

[8]<https://orhanergun.net/2015/05/bridgingprovider-bridgingprovider-backbone-and-shortest-path-bridging/>

[9]<https://www.avaya.com/en/documents/introduction_to_shortest_path_bridging_dn4799.pdf>

[10]<https://www.juniper.net/documentation/en_US/junos12.3/topics/concept/mx-series-multiple-stp.html>

[11]<http://www.force10networks.com/whitepapers/pdf/F10_wp19_v1%201.pdf>

[12]<https://www.slideshare.net/ArashForoughi/overview-of-spanning-tree-protocol>