Improving network convergence with Multiple Spanning Tree Protocol

Roxana Stănică

SC Civitas Systems S.R.L., Craiova, Romania
(e-mail: roxana_batm@yahoo.com)

Abstract: In this paper are presented detailed explanations of Spanning Tree features and new developed commands to improve network convergence (hello-timer, forward-delay, MaxAge, max-hops, and priority for Bridge Protocol Data Units (BPDUs)).

The Multiple Spanning Tree Protocol (MSTP) allows multiple spanning tree instances (MSTI) while mapping each Virtual Local Area Network (VLAN) or VLAN group to the most appropriate instance.

Using MSTP, a recovery time (for link or device failure) of less than 50 milliseconds can be obtained and can be decreased to 15 milliseconds.

Keywords: network, protocol, bridge, convergence, topology change, command.

1. INTRODUCTION

The main focus of this paper is to obtain a faster convergence time and load balancing. To demonstrate the utility of spanning tree protocols, in addition to developing new commands for solving convergence problems, this paper provides examples on how to apply the proposed commands.

With the new Multiple Spanning Tree Protocol (MSTP) commands, users can configure and attach a priority to the transmitted packets and are able to configure the hello-timer, MaxAge, forward-delay, and max-hops parameters. Detailed explanations on how the Spanning Tree Protocols behave are also offered in this paper.

Spanning Tree Protocol (STP), also known as IEEE 802.1d, is a Layer-2 network protocol that ensures a loop-free topology for any bridged Ethernet Local Area Network (LAN). STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation and its main purpose is to make sure that users do not create loops when redundant paths appear in a network.

Rapid Spanning Tree Protocol (RSTP) shares most of STP basic characteristics. This protocol is an evolution of STP. It provides faster convergence (less than one second) when a network topology change occurs. RSTP automatically selects the bridge that has the best bridge Identifier (ID) as the Root bridge. Each bridge has a unique bridge ID that is derived from the bridge address and from a manageable priority.

Multiple Spanning Tree Protocol (MSTP) is similar to Cisco Systems' Multiple Instances Spanning Tree Protocol (MISTP) (Cisco Systems RSTP 2006), and is an evolution of STP and RSTP protocols. It was defined in (IEEE Computer Society 802.1s 2002) as an amendment to 802.1Q 1998 edition and now is included in Standard IEEE 802.1Q from (IEEE Computer Society 802.1Q 2003).

1.1 Differences between RSTP and STP (Stanica and Petre 2011; Cisco Systems STP 2006)

- STP has five port states (see Table 1) and RSTP has three port states (see Table 3).
- The detection of Root switch failure is done in 3 x hello-timer (see Table 2).
- Ports can be configured as Edge ports (see Table 4) if they are attached to a LAN that has no other bridges attached. When the bridge detects a Bridge Protocol Data Unit (BPDU) coming to an Edge port, the port becomes a non-Edge port.
- Unlike STP, RSTP responds to BPDUs sent from the Root bridge. A bridge will "propose" its spanning tree information to its Designated ports (see Table 5). If another RSTP bridge receives this information and determines this is the superior Root information, it sets all its other ports to Discarding. The bridge sends an "agreement" to the first bridge confirming its superior spanning tree information. This allows RSTP to achieve faster convergence times than STP (Wojdak 2003).
- RSTP maintains backup details regarding the Discarding status of ports. This avoids timeouts if the current Forwarding ports failed or BPDUs were not received on the Root port in a defined interval.

1.2 Differences between MSTP and STP

- MSTP calculates the same spanning tree topology with the same configuration.
- MSTP achieves faster conversion times;
- MSTP has three port states (Forwarding, Learning, and Disabled) and new port roles (see Table 5);
- MSTP has different definition for topology change;

• BPDUs used for Hello mechanism are different.

2. SPANNING TREE PROTOCOL

2.1 STP algorithm

The STP algorithm (Perlman 1985) calculates each path cost for all switches in the network's spanning tree. The paths with the lower cost are active paths and the other paths are blocked.

• Root Bridge: First step of the algorithm is to elect the active paths in a network; STP first determines a Root bridge. (The Root is the switch towards which all other switches calculate the path cost.) STP then selects the path with the lowest cost from each switch to the Root as the active path, while blocking all other redundant paths.

• Designated bridge: The second step is to elect the Designated bridge, per network segment, after establishing the Root bridge. This is the closest bridge to the Root, and forwards packets from that segment towards the Root bridge. Each segment has only one Designated bridge. The Designated bridge has one Designated port that forwards packets from the Root bridge to this segment.

• Root and Alternate ports: The last step is to elect a Root port (per bridge) that sends data towards the Root bridge. To avoid loops, all other ports that provide redundant paths to the Root bridge are set as Alternate ports.

2.2 STP Bridge Protocol Data Units (BPDUs)

BPDUs are data messages sent to detect loops in a network topology (Lammle 2007). BPDUs include:

- Root bridge ID;
- Designated bridge ID;
- path cost - the distance from the Root to the switch;
- Designated port ID.

There are two BPDU types:

• Configuration BPDU - used to define loop-free technology;

• Topology Change Notification (TCN) BPDU - used to announce network topology change (Cisco Systems STP 2006).

2.3 Calculating the STP Timers

To calculate the STP timers, the following formulas can be used [Stanica and Petre (2011)]:

$$MaxAge = 4 \times hello + 2 \times dia - 2 \quad (1)$$

$$Forward\text{-}delay = (4 \times hello + 3 \times dia) / 2 \quad (2)$$

• Where *hello* is the hello-timer and *dia* is the STP diameter.

Based on the above formulas, a low hello-timer value decreases the other STP parameters. However, it doubles the amount of BPDUs sent/received by each bridge.

Table 1. STP States.

STP State	Description
Blocking	The port does not forward frames. It moves to this state after the initialization phase, when a different switch/port was selected as Root.
Listening	The listening state is the first transitional state a port enters after the Blocking state. STP determines if the port will forward frames.
Learning	The port is preparing to forward frames. This is the second transitional state through which a port moves in anticipation of frame forwarding.
Forwarding	The port forwards frames. The bridge/switch processes BPDUs and waits for possible new information that might cause it to return to Blocking state to prevent a loop.
Disabled	The port does not participate in forwarding frames and spanning tree.

Table 2. STP Timers.

Timer	Description
Hello timer	The interval (between two consecutive BPDUs) a switch sends to other switches.
Forward-delay timer	The time a port is in Listening and Learning states before the port begins forwarding frames.
Maximum-age timer (MaxAge)	The time the switch stores protocol information received on a port.
Message Age	Shows how far a switch is from the Root when it receives a BDPU.

Table 3. RSTP Port States.

RSTP State	Description
Learning	As in STP, the port prepares to forward frames. It learns source addresses from the frames received and adds them to the filtering database.
Forwarding	As in STP, the port enters this state from the Learning state. The switch processes BPDUs and waits for possible new information that may cause it to move to the Discarding state to prevent a loop.
Discarding	This state contains STP Disabled, Blocking, and Listening states. In this state, a port that does not forward traffic in either direction. The port discards received frames and no learning occurs.

3. RAPID SPANNING TREE PROTOCOL

3.1. RSTP algorithm

The RSTP algorithm dynamically creates a tree through the network, used to efficiently direct packets to their destinations. It reduces the bridged network to a single spanning tree topology in order to eliminate packet loops.

To create a loop-free environment and to provide rapid convergence, RSTP selects the switch with the highest priority as the Root bridge, assigns the port roles, and determines the active topology. RSTP assigns a role to each bridge port throughout the bridged LAN.

3.2 RSTP Bridge Protocol Data Units (BPDUs)

The RSTP BPDU (Cisco Systems RSTP 2006) has the same format as the STP BPDU except for the protocol version that is set to 2. The switch proposes itself to be the designated device by setting (see Fig. 1):

- Proposal flag (bit 1);
- Port Role flag (bits 2-3) to Designated port.

The receiving device accepts the proposal by setting:

- Agreement flag (bit 6);
- Port role flag to Root port.

RSTP uses the Topology Change (TC) flag (Cisco Systems RSTP 2006) to indicate topology changes. The Learning and Forwarding flags (bits 4 and 5) are determined according to the sending port state.

Table 4. RSTP Rapid Convergence.

Port	Description
Edge ports	Edge ports are configured by users. Once they are configured, these ports transit to Forwarding state.
Root ports	When RSTP selects a new Root port, it blocks the old Root port and puts the new Root port in Forwarding state.
Point-to-point links	Point-to-point links are links that directly connect two switches.

Table 5. RSTP and MSTP Port Roles.

Role	Description
Root port	Port connected to the Root bridge. A Root port is in Forwarding state.
Designated port	Port connected to the Designated bridge - the bridge closest to the Root bridge. Frames are forwarded to the Root through the Designated bridge. A Designated port is in Forwarding state.
Alternate port	Port that offers a path to the Root bridge as an alternative to the path provided by the Root port. The Alternate Port can replace the current Root port if a link failure or a configuration change (such as port priority change) occurs. Alternate port is in Discarding state. This role is equivalent to the STP Blocking state.
Backup port	Backup for the path provided by a Designated port in the direction of the Spanning Tree leaves. Backup port is in Discarding state. This role is equivalent to the STP Blocking state.
Disabled port	Disabled ports do not forward frames and are not operational.

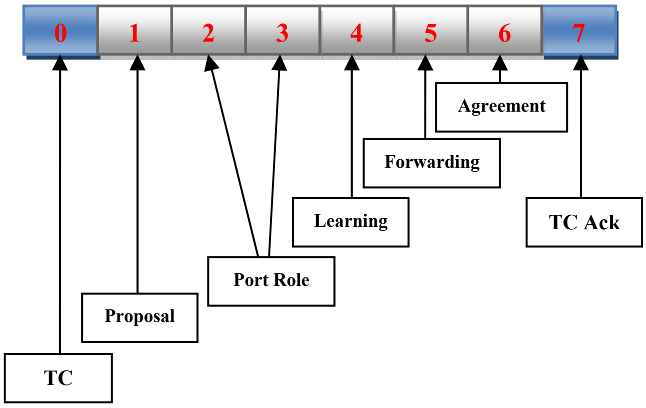

Fig. 1. RSTP BPDU format.

4. MULTIPLE SPANNING TREE PROTOCOL

MSTP allows multiple spanning tree instances (MSTI) while mapping each VLAN or VLAN group to the most appropriate instance. The protocol is applied separately for a set of VLANs instead of the whole network.

MSTP is compatible with STP and uses RSTP for convergence algorithms. MSTP and RSTP share many common characteristics such as rapid convergence and parameters (path cost, timers, port roles and states). MSTP has the advantage of having different forwarding paths for different MST instances. This enables load balancing of network traffic across redundant links (Allied Telesis 2004).

MSTP uses the same port roles as RSTP (see Table 5) and supports large networks by grouping bridges into regions. The switches in the same MST region share the following attributes:

- region name and revision number;
- MST instance to VLAN assignment map. (Each VLAN can be mapped only to one instance.)

Bridges running MST provide interoperability with Single Spanning Tree (SST) bridges:

- MST bridges run Internal Spanning Tree (IST). IST adds internal information about the MST region to the Common Spanning Tree (CST) information.
- IST connects all the MST bridges in the region and appears as a sub-tree in the CST that includes the whole bridged domain.
- Adjacent Single Spanning Tree (SST) and MST regions regard the MST region as a single virtual bridge.
- Common and Internal Spanning Tree (CIST) is a collection of the following (as IEEE Standard 802.1Q):
  - ISTs in each MST region;
  - CST that interconnects the MST regions;
  - SST bridges.
- Within an MST region, CIST is identical to an IST.
- Outside an MST region, CIST is identical to a CST.

STP, RSTP, and MSTP elect a single bridge as the Root of the CIST.

4.1 MSTP Bridge Protocol Data Units (BPDUs)

MSTP includes all its spanning tree information in a single BPDU format. This reduces the number of BPDUs required on a LAN to communicate the spanning tree information for each Virtual Local Area Network (VLAN) and ensures backward compatibility with RSTP and STP.

MSTP allows the creation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using a single CST.

4.2 MST Instances (MSTI)

Each bridge in the MSTP region contains up to 16 MSTIs (IEEE Computer Society 802.1Q (2003) sub-clause 3.19) that act like separate RSTP bridges for a specific set of configured VLANs. All MSTIs within the same region share the same protocol timers, but each instance has its own topology parameters, such as Root Bridge ID, Root path cost, and active topology.

By manipulating these parameters, system administrator can modify the spanning tree topology (defining Forwarding ports and Blocked ports) for the MSTI VLANs, thus traffic load-balancing within the region is achieved (IEEE Computer Society 802.1Q 2003).

The MSTIs are identified by their instance ID (IEEE Computer Society 802.1s 2002; IEEE Standard 802.1Q 2003):

- Instance 0: this is the Common Internal Spanning Tree (CIST) to which all VLANs are mapped by default. This instance cannot be removed.
- Instances 1 to 15: can be configured by users and are optional instances to which the system administrator maps VLANs.

4.3 MSTI Parameters

MST Region

An MSTP region (IEEE Computer Society 802.1s 2002; IEEE Standard 802.1Q 2003; Cisco Systems MSTP 2009) is a collection of interconnected bridges that share the same MSTP configuration. There is no limit on the number of MST regions in the network. To form an MST region, bridges can be either:

- An MST bridge that is the only member of the MST region.
- An MST bridge interconnected by a LAN. A LAN’s designated bridge has the same MST configuration as an MST bridge. All the bridges on the LAN can process MST BPDUs.

Boundary Ports

A boundary port (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003; Cisco Systems MSTP 2009) is a port that connects the designated bridge to a LAN.

A designated port knows that it is a boundary port if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration. The role of MST ports is not important because their state is forced to be the same as the IST port state. The IST port at the boundary can take any port role except a backup port role.

IST Master

The IST master (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003) of an MST region is the bridge with the lowest bridge identifier and the lowest path cost to the CST Root. If an MST bridge is the Root bridge for an MST instance, then it is the IST master of that MST region. If the CST Root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master.

Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the Root.

If two or more bridges at the boundary of a region have an identical path to the Root, a slightly lower bridge priority can be set.

The Root path cost and message age inside a region remain constant, but the IST path cost is incremented and the IST remaining hops are decremented at each hop.

Regional Root

The Root bridge of each MSTI in a region is the MSTI’s regional Root (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003; Cisco Systems MSTP 2009). For IST (MSTI0), it is the CIST Regional Root. Therefore, the terms “IST Master” and “CIST Regional Root” are interchangeable.

Edge Ports

A port that is connected to a non-bridging device (for example, a host or a switch) is an Edge port (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003). A port that connects to a hub is also an edge port if the hub or any LAN that is connected to it does not have a bridge. An Edge port can start forwarding as soon as the link is up.

Link Type

Rapid connectivity is established only on point-to-point links. When connecting a port to another port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003); Cisco Systems MSTP 2009).

Message Age and Hop Count

IST and MST use a separate hop count mechanism very similar with IP time-to live (TTL) mechanism (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003; Cisco Systems MSTP 2009). Each MST Bridge can be configured with a maximum hop count.

The MSTI Root bridge sends a BPDU with the remaining hop count that is equal to the maximum hop count.

When a bridge receives a BPDU, it decrements the received remaining hop count by one. The bridge discards the BPDU and ages out the information held for the port if the count reaches zero after decrementing. Non-Root bridges propagate the decremented count as the remaining hop count in the BPDUs (M-records) they generate.

Port Priority

The port priority (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003; Cisco Systems MSTP 2009) is used to put a port into the Forwarding state if a loop occurs. To the ports selected first, higher priority (lower priority value) can be assigned. If all ports have the same priority, MSTP puts the port with the lowest number in the Forwarding state and blocks all the other ports.

Path Cost

MSTP uses the path cost (IEEE Computer Society 802.1s 2002; IEEE Computer Society 802.1Q 2003; Cisco Systems MSTP 2009) to put a port into the Forwarding state if a loop occurs. To the ports selected first, higher priority (lower priority value) can be assigned. If all ports have the same cost, MSTP puts the port with the lowest number in the Forwarding state and blocks all the other ports.

5. NEW MSTP COMMANDS

To apply and configure the new MSTP commands, the steps displayed in Fig. 2 must be followed.

• **mstp enable** command enables the MSTP.

• **mstp disable** command disables the MSTP protocol.

• **mstp priority** <*instance-id*> <*priority value*> command sets the MSTP bridge priority an MSTP instance. The default bridge priority is 32768.

o <*instance-id*> is the MSTP instance ID, in the range of <1–15>.

o <*priority value*> is bridge priority in the range of <0–65535>. The bridge with the highest bridge priority (the lowest numerical priority value) is selected as Root switch.

• **name** *NAME* command sets the region name, a case-sensitive string of up to 31 characters.

• **mstp hello-timer** <*hello value*> command sets the hello-time for all MST instances. This is the interval between consecutive configuration messages generated by the Root switch, indicating that the switch is alive.

o <*hello value*> is the hello-timer interval in the range of <1–10> seconds. The default value is 2 seconds.

• **mstp max-age** <*maxage value*> command sets the interval the switch waits for receiving a BPDU before attempting a reconfiguration.

o <*maxage value*> is the maximum aging time in the range of <6–40> seconds. The default value is 20 seconds.

• **mstp forward-delay** <*delay value*> command sets the time the port waits in the Listening state and the Learning state before moving to the Forwarding state.

o <*delay value*> is the forward-delay interval in the range of <4–30> seconds. The default value is 15 seconds.

• **mstp max-hops** <*hops value*> command sets the maximum number of hops allowed in a region before discarding a BPDU.

o <*hops value*> is the number of hops in a region, in the range of <1–40>. The default value is 40 hops.

• **mstp edge-port** *UU/SS/PP* command sets the specified port (*UU/SS/PP*) as an Edge Port.

o Admin Edge Port: configuring a port as an Edge port is known as Administrative Edge Port; the port has the permission to transition directly to Forwarding state when it becomes Designated.

o Edge Port: indicates whether the port operates as an Edge Port or not. When a port that was configured as Administrative Edge Port receives a BPDU, it automatically changes its operational state to operate as a non-Edge Port, in order to prevent loops in the network.

• **mstp path-cost** <*cost value*> command sets the cost for an MST instance.

o <*cost value*> is the MSTP path cost value, in the range of <1–200000000>.

The path cost value can be used to give priority to preferred links (for example physical speed and bandwidth). When building the active spanning tree, the port path-cost determines which port is included in the active topology. Ports with lower cost values are preferred to ports with higher cost values. If all ports that provide redundant paths to the Root bridge have the same path-cost value, MSTP puts the port with the lowest number in Forwarding state and blocks the other ports.

• **mstp display** command shows the current MSTP configuration.

6. CONFIGURATION EXAMPLE

Fig. 3 illustrates an example of configuring three bridges: Bridge A, Bridge B, and Bridge C.

Each bridge has a unique ID attached and an active connection to the other bridge.

Initially, each bridge believes that it is the Root Bridge. For example, Bridge C sends a BPDU to Bridges A and B notifying them that it is the Root Bridge and has the ID 32678.00-00-00-00-02. The ID of Bridge B will change from 03 to 02 (because its ID is bigger), and the ID of Bridge A will not change (because its ID is smaller).

Each Bridge compares the Root Bridge ID with its own ID. If it is smaller than the Root ID, the bridge becomes Root Bridge and sends a BPDU to announce the new Root Bridge (see Fig. 4).

Having the lowest ID, Bridge A sends a BPDU to Bridges B and C, notifying them that the new Root Bridge is Bridge A. The IDs of Bridges B and C will change in 01 and the ID of Bridge A will not modify.

All Bridges agree that Bridge A is now the Root Bridge because it has the smallest ID.

After electing the Root Bridge, Bridges B and C (non-Root) must select a Root Port - chosen according to the Root Path Cost.

Ports that have the lowest cost are the Designated Ports - Port 1/1 of Bridge B and port 1/1 of Bridge C.

In this network, three segments can be distinguished.

The Bridge that contains the Designated port for a particular segment is actually the Designated Bridge for that segment.

Since the ID of Bridge C is smaller than the ID of Bridge B, the Designated port for segment 3 is port 1/2 of the Bridge C. Root and Designated ports will be in Forwarding state. The ports that are not Root Ports or Designated Ports transition into the Blocking state (see Fig. 5).

If Bridge B does not receive a BPDU from Bridge C in an interval equal to MaxAge, it will transition to Forwarding state.

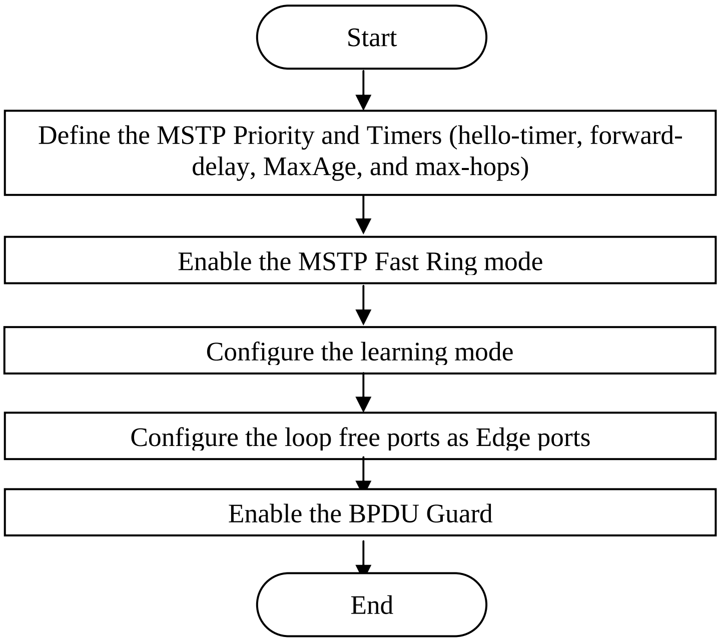

Fig. 2. MSTP Structure.

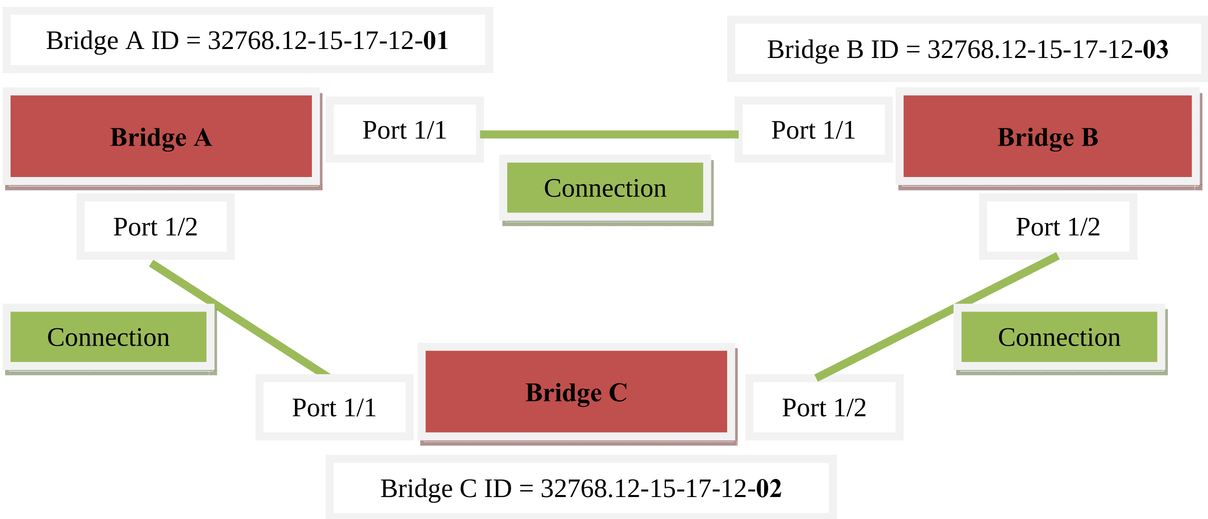

Fig. 3. Example of configuring three bridges using Spanning Tree Protocol.

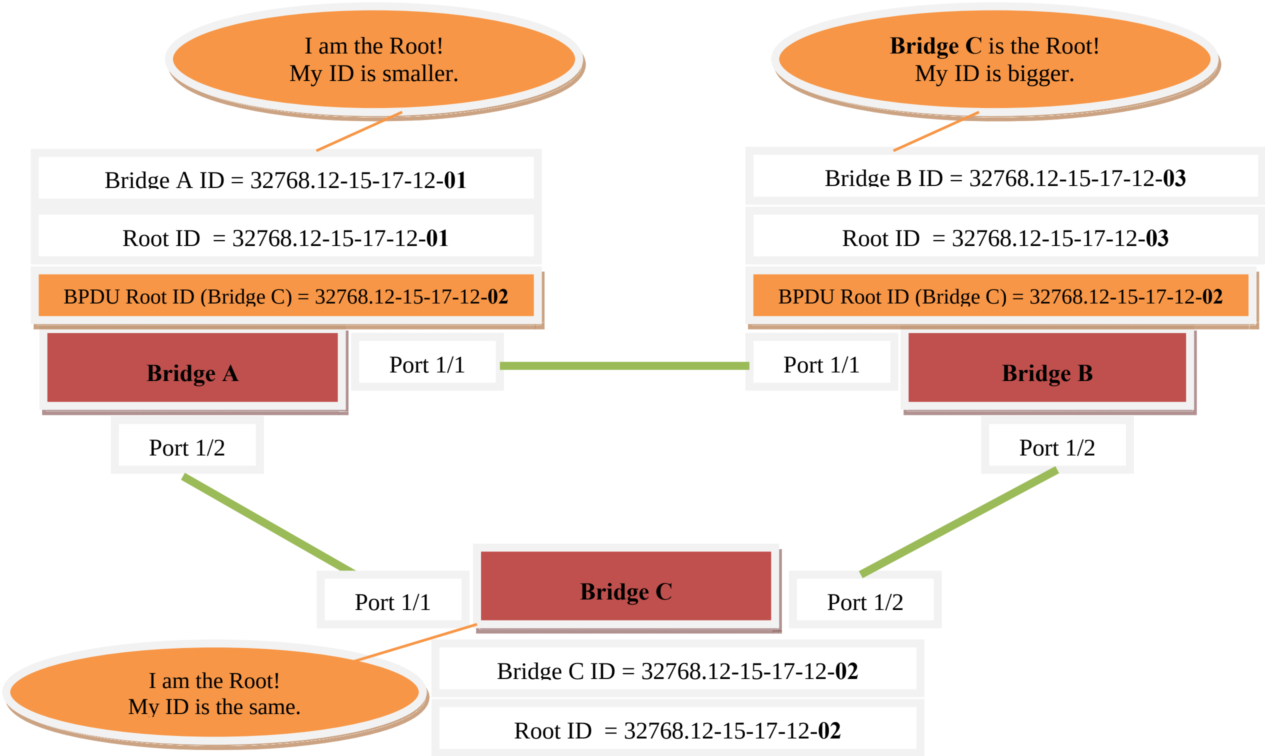

Fig. 4. Electing the Root bridge.

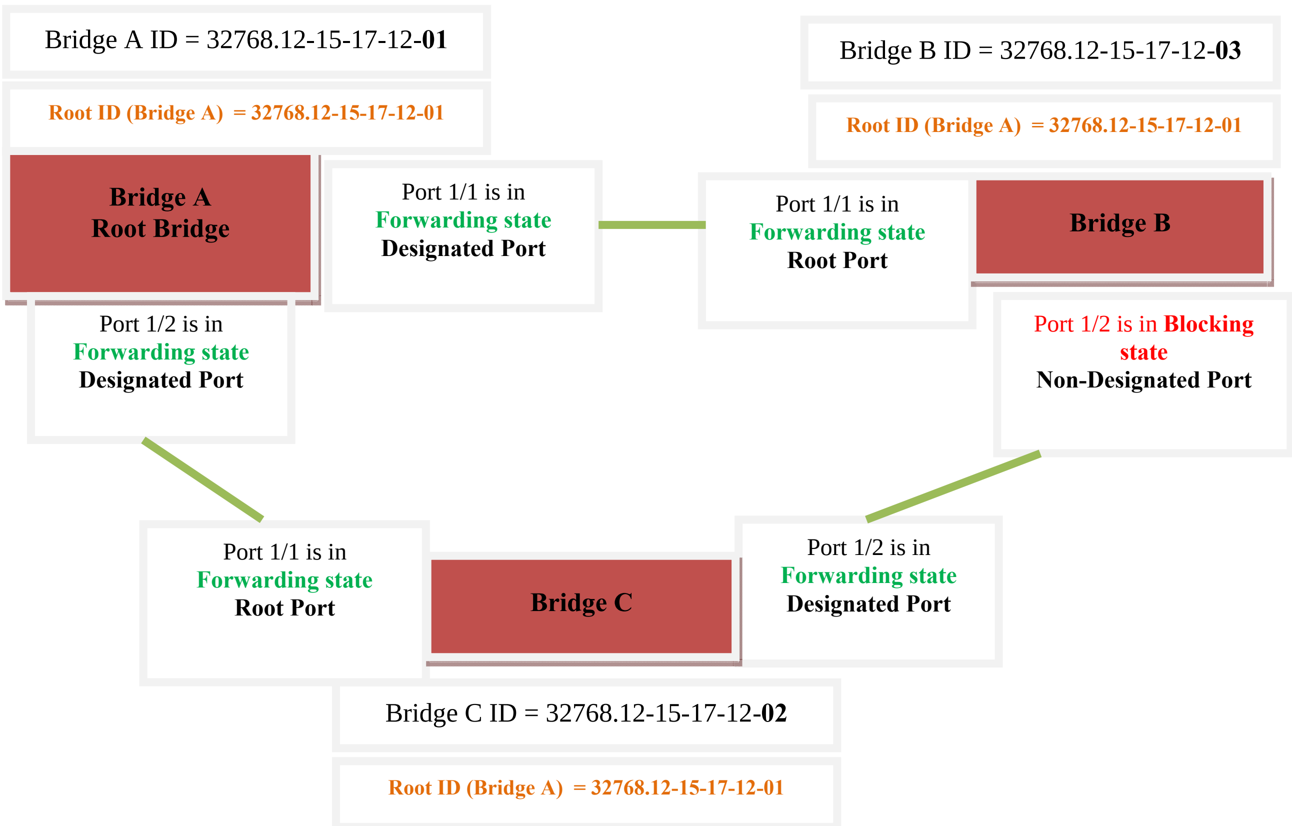

Fig. 5. Establishing the port roles and states.

7. TESTING RESULTS

The following example is an MSTP configuration:

1) Enable MSTP:

   # mstp enable

2) Set MSTP priority to 10 for instance 1:

   # mstp priority *1 10*

3) Set MSTP MaxAge timer:

   # mstp max-age *34*

4) Set MSTP forward-delay:

   # mstp forward-delay *5*

5) Set MSTP hello-timer:

   # mstp hello-timer *4*

6) Set MSTP max-hops:

   # mstp max-hops *23*

7) Display MSTP configuration

   # mstp display

Multiple spanning trees	= enabled
ProtocolSpecification	= ieee8021s
Priority	= 10, instance 1
TopChanges	= 8
Root	= 00001.00:A0:12:0F:2F:27
Edge Port	= 1/1/1
Path Cost	= 20000
BridgeMaxAge	= 34 (Sec)
BridgeHelloTimer	= 4 (Sec)
BridgeForwardDelay	= 5 (Sec)
MaxHopCount	= 23
TxHoldCount	= 3
FastRing	= disabled
SpanIgmpFastRecovery	= disabled
FastRing	= disabled
LearnMode	= Standard

8. CONCLUSIONS

The main purpose of Spanning Tree protocols is to make sure that users do not create loops when redundant paths appear in a network. Redundant links are as important as backups if a failure occurs in a network. A failure of primary link activates the backup links so that users can continue to use the network. Without STP enabled on bridges and switches, such a failure can result in a loop (Cisco Systems RSTP 2006).

The use of STP protocol (Juniper Networks 2012) can cause a failure of a connection of up to 50 seconds (MaxAge + 2 x forward-delay). For a host port, it can take up to 30 seconds (2 x forward-delay) to start transmission. Such convergence times are not accepted in today's high performance networks.

RSTP provides a faster convergence when an STP topology change occurs. While STP needs between 30 and 50 seconds to respond to a topology change, RSTP responds to changes within 3 x hello-timer or within milliseconds from the failure of a physical link (Juniper Networks 2012).

MSTP allows multiple instances to run concurrently over a bridged network (Juniper Networks 2012). MSTP enables load balancing over a large number of VLANs (IEEE Computer Society 802.1Q 2003).

To demonstrate the utility of Spanning Tree protocols, new commands were developed to solve the convergence problems.

For RSTP protocol, a convergence less than one second can be obtained. To create a loop-free environment and to provide a rapid convergence, RSTP selects the bridge with the highest priority as the Root Bridge, assigns port roles, and determines the active topology.

For MSTP, the recovery time of a link failure is less than 50 milliseconds and may be reduced to 15 milliseconds.

RSTP improves the STP convergence time by introducing new port roles (Edge, Alternate and Backup).

MSTP protocols can be configured to automatically detect Edge ports. STP protocol cannot set a port as Edge port.

REFERENCES

Allied Telesis. (2004). *How to configure Multiple Spanning Tree Protocol (MSTP)* - available at www.alliedtelesis.com/media/fount/how_to_note_alliedware/c613-16036-00-A.pdf. [Accessed on 26/07/2012].

Angelescu, S. (2010). *CCNA® Certification All-In-One for Dummies®*. Wiley Publishing Inc. pp. 385-415.

Cisco Systems. (2006). *Understanding Spanning-Tree Protocol Topology Changes* - available at www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094797.shtml. [Accessed on 22/07/2012].

Cisco Systems. (2006). *Understanding Rapid Spanning Tree Protocol (802.1w)* - available at www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml. [Accessed on 22/07/2012].

Cisco Systems. (2009). *Configuring Multiple Spanning Tree* - available at www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/MST.html. [Accessed on 20/07/2012].

IEEE Standard 802.1s™. (2002). *Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees*. IEEE Computer Society, Published by The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue. New York. USA.

IEEE Standard 802.1Q™. (2003). *Virtual Bridged Local Area Networks*. IEEE Computer Society, Published by The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue New York. USA.

Juniper Networks. (2012). *Spanning Tree Protocol in Layer2/Layer 3 Environments* - available at http://www.juniper.net/us/en/local/pdf/implementation-guides/8010002-en.pdf. [Accessed on 25/07/2012].

Lammle, T. (2007). *CCNA®: Cisco® Certified Network Associate: Study Guide, Sixth Edition*. Wiley Publishing Inc. pp. 493-550.

Perlman, R. (1985). An algorithm for distributed computation of a Spanning Tree in an Extended LAN. ACM SIGCOMM Computer Communication Review, *Proceedings of the ninth symposium on Data communications*. vol. 15 (4). pp. 44-53.

Perlman, R. (2000). Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols. *Addison-Wesley Professional Computing Series*. pp. 58-94.

Stanica, R. and Petre, E. (2011). Achieve faster spanning tree convergence. *Journal of the Polytechnic Institute of Iasi*. vol. LVII (LXI). Fasc. 3. pp. 95-111.

Wojdak, W. (2003). Rapid Spanning Tree Protocol: A new solution from an old technology. *Reprinted from CompactPCI Systems*.

Xu, Z. (2010). *Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services: An Advanced Guide for VPLS and VLL*. Wiley Publishing Inc. pp. 840-895.