Chapter 4

Effective Planning and Analysis of Huawei and Cisco Routers for MPLS Network Design Using Fast Reroute Protection

Martin Hlozak, Dominik Uhrin,
Jerry Chun-Wei Lin and Miroslav Voznak

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/66785

Abstract

This chapter deals with a description of the MPLS traffic engineering technology behavior on two heterogeneous, but nowadays the most commonly used network vendors are Cisco and Huawei. Compatibility and functionality between network devices Huawei and Cisco were verified by testing the appropriate network topology. In this topology, we mainly focused on the useful feature of MPLS TE called Fast Reroute (FRR) protection. It provides link protection, node protection and also bandwidth protection during the failure of the primary link, especially on backbone networks. After successful validation, compatibility and functionality of the network topology between the heterogeneous routers using the Fast Reroute protection will be possible to use this MPLS TE application in the real networks.

Keywords: Cisco, Fast Reroute, Huawei, MPLS

1. Introduction

In the 1990s, asynchronous transfer mode (ATM) was considered an ideal solution in transmission networks to operate with different demands [1]. In earlier times, this technology provided traffic engineering by a virtual channel as well as Frame-Relay. But subsequently IP began to replace the ATM technology, which became the most popular network protocol for transmission. On the other hand, the ATM was still widely used by telecommunication providers at that time. Since 1999, the draft of multiprotocol label switching (MPLS) has become the IETF [2] standard and internet service providers started to use this concept for IP/MPLS transmission over older ATM technology. In this chapter, we focus on the application

of MPLS called MPLS traffic engineering. MPLS TE can be understood as "effective planning utilization" [3]. Instead of the normal routing of IP packets, MPLS TE routes traffic according to the source IP addresses. This application can choose the most appropriate links according to the speed of individual lines, delay, delay variability and can also react automatically to the change of these parameters [3, 4]. In addition, the applications of MPLS are also used for an effective creation of separate virtual private networks among the company branches, or for addressing QoS issues in communication networks, such as satellite and mobile cellular networks. This chapter is focused on the most used function of MPLS TE called Fast Reroute. Fast Reroute can be used in the case of a link or node failure in the MPLS network. Both vendors Huawei and Cisco support MPLS TE, but each vendor can use a different function model. The main motivation of this chapter is to bring complex view on usage and cooperation between routers of two different vendors using Fast Reroute protection.

2. State of the art

Multiprotocol label switching (MPLS) is a backbone technology, which uses labels attached to the packets for their transmission. Packets are not transmitted based on the destination IP addresses but according to the MPLS labels. The protocol allows most packets to be forwarded at Layer 2 (switching) rather than at Layer 3 (routing). The term "multiprotocol" means that it can transport various protocols on Layer 3 such as IPv4, IPv6, IPX, and protocols of Layer 2, e.g., Ethernet, HDLC, Frame-Relay, or ATM [5].

As shown in **Figure 1**, source A sends a packet to the router CE1. CE1 handles the packet according to its routing table in a standard way. According to the destination IP address of each packet, the ingress router (PE1) inserts a label in front of the IP header at the edge of the backbone network. All the subsequent routers ignore the IP headers and perform the packet forwarding based on the labels in front of them. This MPLS label determines a path that is used for the routing of a particular packet. Paths through MPLS network are called LSPs [5, 7].

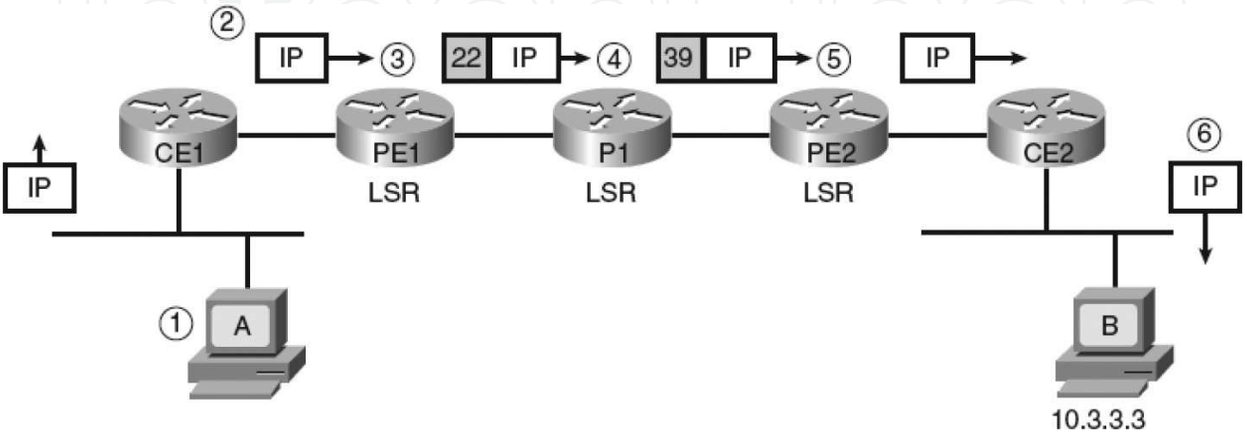

Figure 1. Packet forwarding via MPLS network [6].

http://dx.doi.org/10.5772/66785

Each label has its local importance and every MPLS backbone router processes the packet based on the MPLS label. Finally, the egress router (PE2) removes the label and forwards the original IP packet toward its final destination.

3. Methodology

Nowadays, practically, computer networks are not built only on a homogeneous infrastructure, but they use heterogeneous devices.

As depicted in **Figure 2**, the basic MPLS topology consists of two Huawei routers—the first one AR3200 and the second one AR2200 (marked in the red frame) and two Cisco 2800 series routers. The first goal was to verify MPLS functionality and interoperability among these above-mentioned routers.

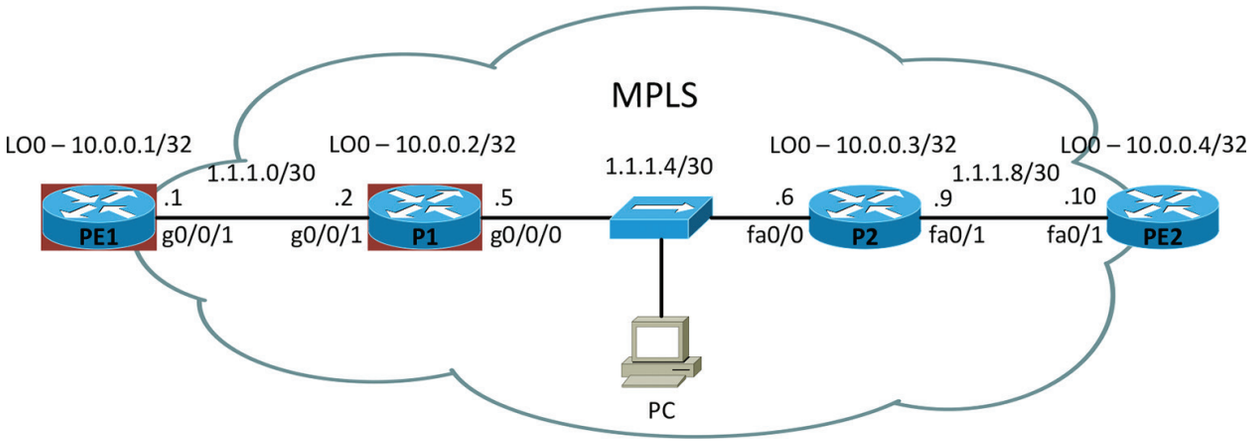

Figure 2. MPLS network.topology.

Huawei routers have only two CLI modes (basic view and the system view). The basic configuration of Huawei routers is as follows:

[Huawei]sysname PE1

[PE1]ospf 1

[PE1-ospf-1]area 0

[PE1-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.3

[PE1-ospf-1-area-0.0.0.0]network 10.0.0.1 0.0.0.0

[P1]mpls lsr-id 10.0.0.2

[PE1]mpls

[PE1-mpls]lsp-trigger all

[PE1]mpls ldp

[PE1]int lo0

[PE1-LoopBack0]ip address 10.0.0.1 255.255.255.255

[PE1]int g0/0/1

[PE1-GigabitEthernet0/0/1]ip address 1.1.1.1 255.255.255.252

[PE1-GigabitEthernet0/0/1]mpls

[PE1-GigabitEthernet0/0/1]mpls ldp

[PE1]int g0/0/0

[PE1-GigabitEthernet0/0/0]ip address 192.168.10.1 255.255.255.0

[PE1-GigabitEthernet0/0/1]mpls

[PE1-GigabitEthernet0/0/1]mpls ldp

All routers use OSPF as a routing protocol. Unlike Cisco routers, LSR identification must be configured on every Huawei router. For identification of Huawei routers, the loopback IP addresses were applied. The command *lsp-trigger all* allocates label for each IP prefix in the routing table. Then the LDP protocol for exchange of MPLS labels had to be activated for each MPLS physical interface.

3.1. Configuration of MPLS TE on Huawei routers

The network topology of the MPLS TE network is depicted in **Figure 3**.

First of all, it is necessary to configure MPLS TE technology and then turn on signalling protocol RSVP-TE. In the case of a link or node failure, we configure mpls rsvp-te hello as well. It is also necessary to enable modified SPF algorithm called CSPF which excludes. Using CSPF algorithm, the ingress MPLS router do not use these lines, which not satisfying the requirements of the data flow.

It is also necessary to explicitly turn on RSVP-TE for each MPLS physical interface. The part of the configuration is setting of the maximum bit rate of a line, which can be reserved. This bit rate cannot exceed the bit rate of a physical interface. The command *mpls te bandwidth bc0 10000* defines maximum total bandwidth for class type 0. In this case, the maximum bit rate of a physical interface is used.

In order to LSR routers could exchange information about set parameters such as maximum bit rate of the line, it is necessary to configure support for a special type of message OSPF LSA 10 for the OSPF area. Then this type of message is used for CSPF algorithm. By the command *opaque-capability enable*, we allow propagation of LSA 10 messages. Next command *enable traffic-adjustment advertise* includes static LSP tunnels into SPF calculation and to the routing table.

[PE1-mpls]mpls te

[PE1-mpls]mpls rsvp-te

http://dx.doi.org/10.5772/66785

[PE1-mpls]mpls rsvp-te hello

[PE1-mpls]mpls te cspf

[PE1-GigabitEthernet0/0/1]mpls rsvp-te

[PE1-GigabitEthernet0/0/1]mpls rsvp-te hello

[PE1-GigabitEthernet0/0/1]mpls te bandwidth max-reservable bandwidth 10000

[PE1-GigabitEthernet0/0/1]mpls te bandwidth bc0 10000

[PE1]ospf 1

[PE1-ospf-1]area 0

[PE1 ospf-1-area-0.0.0.0]mpls-te enable

[PE1-ospf-1]opaque-capability enable

[PE1-ospf-1]enable traffic-adjustment advertise

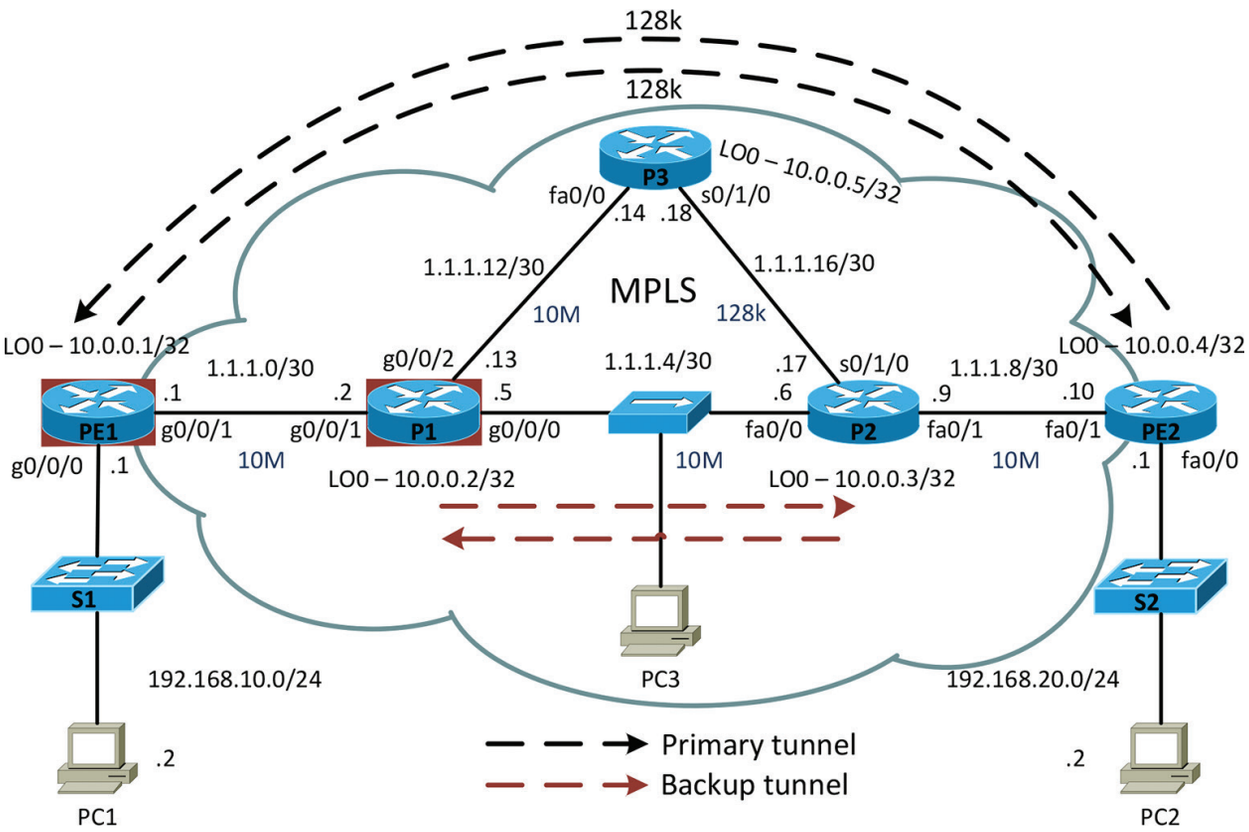

Figure 3. MPLS TE topology.

3.2. Configuration of MPLS TE on Cisco routers

To enable the MPLS TE technology on Cisco routers, it is necessary to configure *mpls traffic-eng tunnels and ip rsvp signaling hello* commands. To achieve establishment of the LDP signaling protocol from the loopback interface, *mpls ldp router-id Loopback0 force* is configured.

A part of the next configuration is to explicitly turn on RSVP-TE for each MPLS physical interface and set the maximum bit rate of a line which can be reserved. Using *mpls traffic-eng area 0* command is configured a special type of message OSPF LSA 10 for the OSPF area. Each Cisco router must be uniquely identified using OSPF router-ID. If the router did not have this identification, OSPF LSA 10 will not be transmitted.

PE2(config)#mpls ldp router-id Loopback0 force

PE2(config)#mpls traffic-eng tunnels

PE2(config)#ip rsvp signalling hello

PE2(config)#interface FastEthernet0/1

PE2(config-if)#mpls traffic-eng tunnels

PE2(config-if)#ip rsvp bandwidth 10000

PE2(config-if)#ip rsvp signalling hello

PE2(config)#router ospf 1

PE2(config-router)#mpls traffic-eng router-id Loopback0

PE2(config-router)#mpls traffic-eng area 0

3.3. Configuration of primary explicit path on Cisco router PE1

To define an explicit path for the primary line through the MPLS network via routers PE1-P1-P3-P2-PE2, each next hop is defined by the IP address of the LSR router.

MPLS TE technology includes configuration of MPLS tunnel connections. As a tunnel source, a loopback interface is defined by *IP address unnumbered interface LoopBack0* command. Last next hop IP address of an explicit path must match the destination of the tunnel. In our case, 10.0.0.4 is used. Identification of the MPLS tunnel is made by *mpls te tunnel-id 1* command. Priority is set by the command *mpls te priority 0*, where zero indicates the highest priority. A part of the configuration must be *mpls te record-route label* which records the links during the initiation of the tunnel.

[PE1]explicit-path PE1-P1-P3-P2-PE2

[PE1-explicit-path-PE1-P1-P3-P2-PE2]next hop 1.1.1.2

[PE1-explicit-path-PE1-P1-P3-P2-PE2]next hop 1.1.1.14

[PE1-explicit-path-PE1-P1-P3-P2-PE2]next hop 1.1.1.17

[PE1-explicit-path-PE1-P1-P3-P2-PE2]next hop 1.1.1.10

[PE1-explicit-path-PE1-P1-P3-P2-PE2]next hop 10.0.0.4

[PE1]interface Tunnel0/0/0

http://dx.doi.org/10.5772/66785

[PE1-Tunnel0/0/0]tunnel-protocol mpls te

[PE1-Tunnel0/0/0]ip address unnumbered interface LoopBack0

[PE1-Tunnel0/0/0]destination 10.0.0.4

[PE1-Tunnel0/0/0]mpls te tunnel-id 1

[PE1-Tunnel0/0/0]mpls te record-route label

[PE1-Tunnel0/0/0]mpls te priority 0

Bit rate 128 kbit/s is assigned to the MPLS tunnel. It is necessary to define an explicit path. During the failover of the primary line, command *mpls te fast-reroute bandwidth* guarantees switching to the backup line with a keeping bit rate of the primary line. By *mplsteigpshortcut* command, tunnel becomes a virtual tunnel line, which will be inserted into the IP routing table. To ensure the tunnel connection precedence over the traditional calculation by OSPF routing protocol, we define an absolute metric for this tunnel using *mpls te igp metric absolute 1*command.

[PE1-Tunnel0/0/0]mpls te bandwidth ct0 128

[PE1-Tunnel0/0/0]mpls te path explicit-path PE1-P1-P3-P2-PE2

[PE1-Tunnel0/0/0]mpls te fast-reroute bandwidth

[PE1-Tunnel0/0/0]mpls te igp shortcut

[PE1-Tunnel0/0/0]mpls te igp metric absolute 1

[PE1-Tunnel0/0/0]mpls te commit

3.4. Configuration of primary explicit path on Huawei router PE2

Because every explicit path is unidirectional, we need to configure MPLS tunnel in the opposite direction via routers PE2-P2-P3-P1-PE1.

Similarly, primary MPLS tunnel is configured on the Cisco router. As a tunnel source, a loopback interface is used. Because the last next hop of the explicit path is IP address 10.0.0.1, this address is defined as a destination address. By *tunnel mpls traffic-eng autoroute announce* command, Cisco router announces the presence of the MPLS tunnel to the IP routing table. The highest priority is set by *mpls te priority 0* command.

PE2(config)#ip explicit-path name PE2-P2-P3-P1-PE1

PE2(cfg-ip-expl-path)#next-address 1.1.1.9

PE2(cfg-ip-expl-path)#next-address 1.1.1.18

PE2(cfg-ip-expl-path)#next-address 1.1.1.13

PE2(cfg-ip-expl-path)#next-address 1.1.1.1

PE2(cfg-ip-expl-path)#next-address 10.0.0.1

PE2(config)#interface Tunnel0

PE2(config-if)#ip unnumbered Loopback0

PE2(config-if)#tunnel destination 10.0.0.1

PE2(config-if)#tunnel mode mpls traffic-eng

PE2(config-if)#tunnel mpls traffic-eng autoroute announce

PE2(config-if)#tunnel mpls traffic-eng priority 0 0

Same bit rate (128 kbit/s) is assigned to MPLS tunnel. The explicit path is then included in the MPLS tunnel interface. During failover of the primary line on the Cisco site, command tunnel *mpls traffic-eng fast-reroute bw-protect* guarantees switching to the backup line with a keeping bit rate of the primary line.

PE2(config-if)#tunnel mpls traffic-eng bandwidth 128

PE2(config-if)#tunnel mpls traffic-eng path-option 1 explicit PE2-P2-P3-P1-PE1

PE2(config-if)#tunnel mpls traffic-eng record-route

PE2(config-if)#tunnel mpls traffic-eng fast-reroute bw-protect

3.5. Configuration of backup path and Fast Reroute on Huawei router P1

In next step, the router P1 is configured. A backup explicit path is defined between routers P1 and P2. This backup tunnel will be used when the primary path PE1-P1-P3-P2-PE2 fails. The function of the backup exit node has a destination router P2 which uses 10.0.0.3 address. This tunnel interface becomes a backup link using *mpls te bypass-tunnel* command. Last command protects the interface GigabitEthernet0/0/2, in the case of failure of the router P3 or link between P1 and P3.

[P1]explicit-path P1-P2

[P1-explicit-path-P1-P2]next hop 1.1.1.6

[P1-explicit-path-P1-P2]next hop 10.0.0.3

[P1]interface Tunnel0/0/0

[P1-Tunnel0/0/0]ip address unnumbered interface LoopBack0

[P1-Tunnel0/0/0]tunnel-protocol mpls te

[P1-Tunnel0/0/0]destination 10.0.0.3

[P1-Tunnel0/0/0]mpls te tunnel-id 1

[P1-Tunnel0/0/0]mpls te record-route

[P1-Tunnel0/0/0]mpls te priority 0

[P1-Tunnel0/0/0]mpls te path explicit-path P1-P2

http://dx.doi.org/10.5772/66785

[P1-Tunnel0/0/0]mpls te bypass-tunnel

[P1-Tunnel0/0/0]mpls te igp shortcut

[P1-Tunnel0/0/0]mpls te igp metric absolute 1

[P1-Tunnel0/0/0]mpls te protected-interface GigabitEthernet0/0/2

[P1-Tunnel0/0/0]mpls te commit

4. Results

4.1. Verification of MPLS TE technology

After the configuration, it is time to verify the correct functionality of the MPLS TE technology. **Figure 4** shows the LFIB table with MPLS labels and also a created primary MPLS TE tunnel. The entry point of the tunnel is the PE1 router with IP address 10.0.0.1, which corresponds to the configured IP address on the loopback interface. The exit point is therouterPE2, which is identified by IPaddress10.0.0.4. Likewise, we can see establishment of the primary-tunnelPE2_t0 to theIPaddress10.0.0.4. Each one-way tunnel route has its own identification (LSPID) and assigned MPLS label.

[PE1]display mpls lsp

LSP Information: RSVP LSP

FEC	*In/Out Label*	*In/Out IF*	*Vrf Name*
10.0.0.1/32	*3/NULL*	*GE0/0/1/-*	
10.0.0.4/32	*NULL/1077*	*-/GE0/0/1*	

LSP Information: LDP LSP

FEC	*In/Out Label*	*In/Out IF*	*Vrf Name*
10.0.0.2/32	*NULL/3*	*-/GE0/0/1*	
10.0.0.2/32	*1024/3*	*-/GE0/0/1*	
10.0.0.5/32	*NULL/1074*	*-/GE0/0/1*	
10.0.0.5/32	*1076/1074*	*-/GE0/0/1*	
1.1.1.4/30	*NULL/3*	*-/GE0/0/1*	
1.1.1.4/30	*1041/3*	*-/GE0/0/1*	
10.0.0.1/32	*3/NULL*	*-/-*	
1.1.1.0/30	*3/NULL*	*-/-*	
192.168.10.0/24	*3/NULL*	*-/-*	
10.0.0.4/32	*1072/NULL*	*-/-*	
192.168.20.0/24	*1073/NULL*	*-/-*	
1.1.1.16/30	*NULL/1075*	*-/GE0/0/1*	
1.1.1.16/30	*1077/1075*	*-/GE0/0/1*	
1.1.1.12/30	*NULL/3*	*-/GE0/0/1*	
1.1.1.12/30	*1078/3*	*-/GE0/0/1*	

Figure 4. LFIB table of router PE1.

As it can be seen in **Figure 5**, the transmission rate of 128kbit/s is reserved throughout the LSP routersPE1-P1-P3-P2-PE2. The same transmission rate is reserved for the tunnellinePE2-P2-P3-P1-PE1 as well.

[PE1]display mpls te link-administration admission-control

LspID	In/Out IF	S/H	Prio	CT	BW(kbps)
10.0.0.1:1:13	--- / GE0/0/1	0 /0		0	128
10.0.0.4:-:164	GE0/0/1 / ---	0 /0		0	128

Figure 5. Reserved transmission rates of MPLS tunnels.

The records marked "T" in the LFIB table of the routerPE2indicated that packets are sent through MPLSTE tunnel. As we can see in **Figure 6**, Huawei router remembers only the IP address of the end of the MPLS tunnel. However, a Cisco router in the LFIB table also records the subnet 192.168.10.0/24.

Figure 7 shows the established primary tunnels, which pass through the router P1, but also established backup tunnels. The entry point of the backup tunnel is the IP address 10.0.0.2 and the exit point is the router P2, which is identified by the IPaddress10.0.0.3. Likewise, we see the backup tunnel(P2_t0), which was defined on the router P2.

PE2#sh mpls forwarding-table

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	Pop Label	10.0.0.3/32	0	Fa0/1	1.1.1.9
17	Pop Label	1.1.1.4/30	0	Fa0/1	1.1.1.9
18	18	10.0.0.2/32	0	Fa0/1	1.1.1.9
19	Pop Label [T]	10.0.0.1/32	0	Tu0	point2point
20	No Label [T]	192.168.10.0/24	0	Tu0	point2point
21	21	1.1.1.12/30	0	Fa0/1	1.1.1.9
22	22	1.1.1.0/30	0	Fa0/1	1.1.1.9
23	Pop Label	1.1.1.16/30	0	Fa0/1	1.1.1.9
24	23	10.0.0.5/32	0	Fa0/1	1.1.1.9

[T] Forwarding through a LSP tunnel.
View additional labelling info with the 'detail' option

Figure 6. LFIB table of router PE2.

[P1]display mpls te tunnel lsr-role all

Ingress LsrId	Destination	LSPID	In/Out Label	R	Tunnel-name
10.0.0.3	10.0.0.2	31	3/--	E	P2_t0
10.0.0.4	10.0.0.1	164	1076/3	T	PE2_t0
10.0.0.1	10.0.0.4	13	1077/28	T	Tunnel0/0/0
10.0.0.2	10.0.0.3	3	--/0	I	Tunnel0/0/0

Figure 7. Primary and backup MPLS TE tunnels established on the router P1.

http://dx.doi.org/10.5772/66785

4.1.1. Verification of MPLS TE Fast Reroute

Explicitly configured path through MPLS tunnel was verified using trace route command fromPC1toPC2 via PE1-P1-P3-P2-PE2 routers, as depicted in **Figure 8**.

An Ethernet link between routers P1 and P3 was disconnected. Every single second was sent an ICMP message from PC1 to PC2. Because 5ICMP messages were lost, the reconvergence time of Fast Reroute was just 5seconds, which can be seen in **Figure 9**.

As depicted in **Figure 10**, the primary tunnel line used inner MPLS label 28, there is still maintained as the inner label. Value "zero" is used as the outer MPLS label. This explicit NULL label signals to the receiving router P2 to remove the outer MPLS label.

```
root@pcn312h:~# traceroute 192.168.20.2
traceroute to 192.168.20.2 (192.168.20.2), 30 hops max, 60 byte packets
 1  192.168.10.1 (192.168.10.1)  1.446 ms  1.648 ms  1.880 ms
 2  1.1.1.2 (1.1.1.2)  7.365 ms  0.829 ms  7.608 ms
 3  1.1.1.14 (1.1.1.14)  69.859 ms  81.080 ms  92.280 ms
 4  1.1.1.17 (1.1.1.17)  17.246 ms  28.414 ms  39.631 ms
 5  1.1.1.10 (1.1.1.10)  43.780 ms  47.973 ms  52.167 ms
 6  192.168.20.2 (192.168.20.2)  58.398 ms  97.400 ms  11.852 ms
```

Figure 8. Verified explicit path through primary tunnel.

```
root@pcn312h:~# ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_req=1 ttl=62 time=13.0 ms
64 bytes from 192.168.20.2: icmp_req=2 ttl=62 time=12.9 ms
64 bytes from 192.168.20.2: icmp_req=3 ttl=62 time=12.9 ms
64 bytes from 192.168.20.2: icmp_req=9 ttl=60 time=0.913 ms
64 bytes from 192.168.20.2: icmp_req=10 ttl=60 time=0.747 ms
64 bytes from 192.168.20.2: icmp_req=11 ttl=60 time=0.738 ms
64 bytes from 192.168.20.2: icmp_req=12 ttl=60 time=0.720 ms
64 bytes from 192.168.20.2: icmp_req=13 ttl=60 time=0.721 ms
^C
--- 192.168.20.2 ping statistics ---
13 packets transmitted, 8 received, 38% packet loss, time 12041ms
rtt min/avg/max/mdev = 0.720/5.355/13.098/5.924 ms
```

Figure 9. Rerouting of ICMP traffic to the backup tunnel from PC1 to PC2.

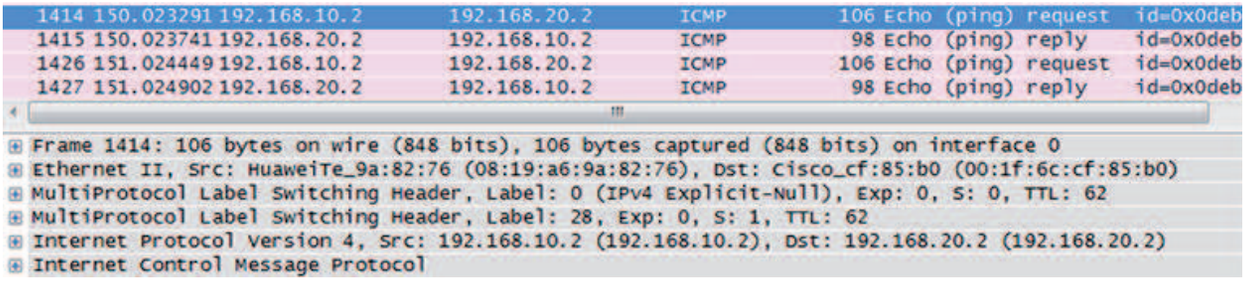

Figure 10. ICMP traffic between routers P1 and P2.

Fast Reroute was also tested on the Cisco site which was subsequently disconnected by means of a serial link between routers P2 and P3. Every single second was sent an ICMP message from PC2 to PC1. Because only two ICMP messages were lost, the convergence time of Fast Reroute was just 2 seconds, which can be seen in **Figure 11**.

```
root@pcn312g:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_req=1 ttl=59 time=13.0 ms
64 bytes from 192.168.10.2: icmp_req=2 ttl=59 time=12.9 ms
64 bytes from 192.168.10.2: icmp_req=3 ttl=59 time=15.0 ms
64 bytes from 192.168.10.2: icmp_req=6 ttl=60 time=0.899 ms
64 bytes from 192.168.10.2: icmp_req=7 ttl=60 time=0.906 ms
64 bytes from 192.168.10.2: icmp_req=8 ttl=60 time=0.739 ms
64 bytes from 192.168.10.2: icmp_req=9 ttl=60 time=0.718 ms
^C
--- 192.168.10.2 ping statistics ---
9 packets transmitted, 7 received, 22% packet loss, time 8018ms
rtt min/avg/max/mdev = 0.718/6.338/15.070/6.408 ms
```

Figure 11. Rerouting of ICMP traffic to the backup tunnel from PC2 to PC1.

As depicted in **Figure 12**, the reconvergence time of the OSPF protocol was also measured without the function of Fast Reroute. The measured time was 15 seconds.

```
root@pcn312h:~# ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_req=1 ttl=62 time=13.0 ms
64 bytes from 192.168.20.2: icmp_req=2 ttl=62 time=12.9 ms
64 bytes from 192.168.20.2: icmp_req=3 ttl=62 time=12.9 ms
64 bytes from 192.168.20.2: icmp_req=19 ttl=60 time=0.913 ms
64 bytes from 192.168.20.2: icmp_req=20 ttl=60 time=0.728 ms
64 bytes from 192.168.20.2: icmp_req=21 ttl=60 time=0.738 ms
64 bytes from 192.168.20.2: icmp_req=22 ttl=60 time=0.712 ms
^C
--- 192.168.20.2 ping statistics ---
13 packets transmitted, 7 received, 68% packet loss, time 21041ms
rtt min/avg/max/mdev = 0.722/5.924/13.013/5.128 ms
```

Figure 12. Rerouting of ICMP traffic without using Fast Reroute.

5. Conclusion

The goal of this chapter was to test a network scenario of interoperability between different vendor's network devices for MPLS TE technology using the Fast Reroute function. Our goal was to verify the compatibility and functionality between the Cisco and Huawei devices. Although MPLS technology is standardized by RFC, some of our practical experience showed us problems in interoperability between different vendors within various RFC standardized technologies. The basic MPLS configuration was without any problems. The appropriate IP prefixes were successfully exchanged. LIB and LFIB tables were filled up.

http://dx.doi.org/10.5772/66785

The major disadvantage of Huawei routers during the MPLS TE configuration is necessity to have the appropriate license. After the license activation, the MPLS TE technology worked properly and the primary and backup MPLS tunnels were established. Without using the technology MPLS TE, the OSPF reconvergence lasted about 15 seconds, after disconnecting Ethernet cable. Due to function Fast Reroute of MPLS TE, the reconvergence lasted only 5 seconds between routers P1 and P3, which is 1/3of convergence time within the OSPF protocol. When using Fast Reroute, the convergence lasted only 2 seconds after disconnecting serial link between routers P2 and P3. It is 1/8 of convergence time within the OSPF protocol. If more routers were added to the network topology, it would lead to a longer convergence time of OSPF but the reconvergence time within Fast Reroute would remain unchanged.

Because nowadays the fast convergence is very critical, this chapter showed that the ISPs can use these heterogeneous network routers together with Fast Reroute technology, which can greatly reduce the convergence time.

Acknowledgements

This publication was created within the project support of VŠB-TUO activities with China with financial support from the Moravian-Silesian Region and partially was supported by the grant SGS reg. no. SP2016/170 conducted at VSB-Technical University of Ostrava, Czech Republic.

Author details

Martin Hlozak[1*], Dominik Uhrin[1], Jerry Chun-Wei Lin[2] and Miroslav Voznak[1]

Address all correspondence to: martin.hlozak@vsb.cz

1 Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, Ostrava-Poruba, Czech Republic

2 School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen Graduate School, Shenzhen, China

References

[1] K. I. Park, "QoS in packet networks", *The Kluwer International Series in Engineering and Computer Science*, vol. 779, pp. 213–231, 2005.

[2] IETF, *RFC 3031: Multiprotocol Label Switching Architecture* [online], 2001. Available from: https://www.ietf.org/rfc/rfc3031.txt

[3] Ramadža, J. Ožegović, V. Pekić, "Network performance monitoring within MPLS traffic engineering enabled networks", in *Software, Telecommunications and Computer Networks (SoftCOM) 2015*, Croatia, IEEE pp. 315–319, 2015.

[4] B. Dekeris, L. Narbutaite, "Traffic control mechanism within MPLS networks", *IEEE Information Technology Interfaces*, pp. 603–608, 2004.

[5] M. Hlozak, J. Frnda, Z. Chmelikova, M. Voznak, "Analysis of Cisco and Huawei routers cooperation for MPLS network design", *Telecommunications Forum Telfor (TELFOR)*, pp. 115–118, 2014.

[6] Yoo-Hwa Kang, J. Lee, "The implementation of the premium services for MPLS IP VPNs", in *IEEE Advanced Communication Technology, ICACT 2005*, South Korea, IEEE pp. 1107–1110, 2005.

[7] T. Almandhari, F. Shiginah, "A performance study framework for Multi-Protocol Label Switching (MPLS) networks", in *GCC Conference and Exhibition (GCCCE)*, Oman, IEEE pp. 1–6, 2015.