USING MPLS TECHNOLOGY TO SOLVE BGP "BLACKHOLE" PROBLEM

Knaj Nouma Khalil,
Master student of the Tartous University, Tartous, Syrian Arab Republic
knajnouma@gmail.com

DOI: 10.36724/2664-066X-2022-8-3-7-11

ABSTRACT

Traditional IP networks use a hop-by-pop principle for transmitting traffic. This leads to aggregation of heterogeneous traffic on links in different parts of the network, which causes considerable possible growth of congestion and leaves the network with both unbalanced use of resources and link failure in congested parts. To support a growing number of users and multiple classes of applications with different performance requirements and characteristics, service providers have been forced to adapt to new technologies. Researchers have found that conventional IP packet forwarding is not suitable for applications such as VOIP and video conferencing, which are currently in huge demand. In addition to offer a general provision of MPLS technology, architecture, operation method and features, we will consider the Border Gateway Protocol (BGP) "Black hole" issue that results in the inability of the network to transfer traffic between some end points, and how MPLS help us avoid this problem and even optimize network operation and resources utilization.

KEYWORDS: *Label switching technology, MPLS, Multiprotocol label switching, MPLS TE, Routing problems, BGP "Blackhole".*

To improve traffic management and Internet service quality, the Internet Engineering Task Force (IETF) proposed MPLS technology to support several classes of latency-critical applications. MPLS is an extremely fast and efficient packet forwarding technology using labels look-up. MPLS components support the interconnection of many different multiple protocols on top of the current IP-based network to implement simple load balancing techniques as dynamic traffic management to maintain the required level of QoS and optimize network performance.

Traditional IP networks use a hop-by-pop principle for transmitting traffic. This leads to aggregation of heterogeneous traffic on links in different parts of the network, which causes considerable possible growth of congestion and leaves the network with both unbalanced use of resources and link failure in congested parts.

In conventional IP networks, routing is based on the destination address and one parameter, such as the number of hops or the value of the delay. The router looks for the next hop (the closest) to the destination without taking into account the results of congestion control, this results the route closest to the destination to become the most congested.

There is another problem related to the characteristics of different packets, for example, voice and video packets are different in length and size and should have a higher priority than regular data packets. In addition, searching the routing table takes time, so packets carrying voice and video may not be able to reach their destination in order and time, getting stuck behind regular data packets. For these reasons, researchers have found that conventional IP packet forwarding is not suitable for applications such as VOIP and video conferencing, which are currently in huge demand.

This raises the need for traffic engineering to ensure bandwidth guarantees and efficient use of network resources.

To overcome these problems, the IETF has proposed a new data transmission mechanism, which is MPLS (Multi protocol label switching), in accordance with the current requirements.

MPLS is an extremely fast and efficient packet forwarding technology using labels look-up.

An MPLS network consists of several routers called LSRs (Label Switching Routers). Other routers that connect to IP routers are called LERs (Label Edge Routers).

An ingress router is a router within an MPLS domain, connected to the outside world, through which a packet enters the MPLS domain. The Egress Router is the router through which packets leave the MPLS domain. Each incoming packet is assigned a label depending on the destination address, this label determines the most efficient and fastest label switching path (LSP) to direct traffic to the MPLS domain the entire way instead of finding the destination address at each point (see Figure 1).

The concept of label switching is not new; it was developed in the late 1990s from CISCO label switching. Multiprotocol label switching is called a 2.5-layer protocol because it sits somewhere between layer 2 (the data link layer) and layer 3 (the network layer).

MPLS was provided as a high-value WAN connection from the service provider and applied to all other types of WAN also has another application as MPLS VPN.

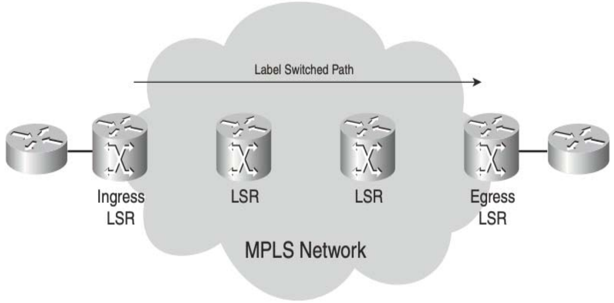

Figure 1. MPLS Architecture (MPLS domain consist of LSRs and LERs at the edges of the network field)

MPLS technology supports the interconnection of many different technologies including IP routers, ATM switches and Frame Relay, as LERs support the connection of multiple ports as edge carriers in an access network.

At the edge router (ingress) a label is assigned to each incoming packet. These labels are distributed by the signaling protocol to create an LSP and forward traffic into the MPLS network.

The label switched routers are the main routers in the MPLS domain and are commonly referred to as core network routers.

When a packet enters the MPLS network, a label or labels are attached to it, and when these packets leave the MPLS network, these labels are removed by the edge routers. The ingress router creates a small MPLS header 32 bits long to encapsulate each incoming packet. This small header is embedded between the Layer 2 and Layer 3 headers, so we call it shim (see Figure 2).

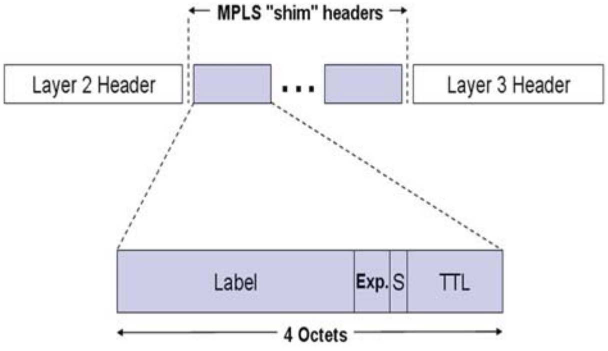

Figure 2. MPLS shim header

Label consists of 20 bits, which means it can have (2^20) values or labels.

However, the first 16 label values are from 0 to 15 are exempted from the normal use as they have a special meaning. Label value can be used by LSR to look up either next hop, operation to perform, or outgoing data-link encapsulation.

(EXP) or experimental consists of three bits and is used for QOS-related functions. It is now renamed TF traffic class. The next field is a single bit called bottom-of-stack. It is used as a flag when more than one label is assigned to a packet as in the case of the MPLS VPN or MPLS TE.

The next byte, the MPLS TTL (time to live) field, consisting of eight bits that can have a value from 0 to 255, serves the same purpose as the IP TTL byte in the IP header. Therefore, each time an LSR forwards a packet, it decrements the TTL field in the packet header, and if the value reaches zero the packet is discarded.

An edge router and a label-switched router create a short, fixed-length object to decide where and how to forward the frame, this object is called a label (see Figure 3). All label information is specified in the Label Forwarding Information Base (LFIB).

At each LSR the old label is removed and a new label is inserted into the packet, and then the packet is forwarded to the next hop.

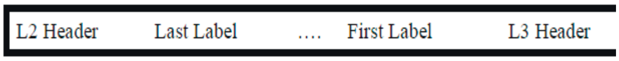

Figure 3. MPLS label structure between Layer 2 and Layer 3 headers

Forwarding Equivalence Class (FEC) is a group of packets that have the same characteristics and transport requirements. All packets that have the same FEC are forwarded along the same path with the same processing. The function of assigning FEC to a packet is a function of the edge router as it is part of the MPLS domain, then all information is embedded in the label and attached to the packet. This way there is no more header analysis within the MPLS domain in the forwarding process.

There are some applications that require a high level of QoS, such as audio/video conferencing and VPNs. These High revenue-generating applications have always been the main focus of service providers. The traditional conventional IP network cannot provide the necessary bandwidth for specific applications, and cannot provide an adequate level of QoS due to lack of support for traffic engineering, but is limited in scalability or flexibility, or sometimes both.

The Internet and service providers pose a new challenge due to some real-time or mission-critical applications because these applications have different latency, bandwidth, jitter and packet loss needs. On the Internet we have an unpredictable traffic flow, so there is a huge need for traffic engineering to run these applications efficiently.

IP (Internet Protocol) was not designed to support QoS, rather it was designed for education and research, but the network has to carry a large volume of traffic and still has limited resources, so it is important to allocate and optimize available resources. Allocating or scheduling network resources based on the required QoS to optimize the use of our network resources is known as traffic engineering. In traditional IP networks, some links are congested, but others remain underutilized because of the destination-based forwarding paradigm.

Making a forwarding decision without considering the available bandwidth and traffic flow between the destination and the source will create congestion on that link, while leaving other links in the network unused, resulting in reduced bandwidth, latency and packet loss.

MPLS provides a solution by providing a connection-oriented structure on top of the current IP-based network to maintain the required level of QoS for these applications. Traffic engineering in MPLS considers resource utilization, making it more efficient to design routes based on single flows or different flows between the same endpoints.

There are two main planes in the MPLS architecture, the control plane and the data plane.

Control Plane Performs information exchange between neighboring devices using various protocols such as OSPF (open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), IS-IS (Intermediate System-to-Intermediate System), RIP (Routing Information Protocol) and BGP (Border Gateway Protocol). Label exchange also takes place using TDP (Tag Distribution protocol), LDP (Label distribution Protocol), BGP, and RSVP (Resource Reservation Protocol).

Data plane based on labels and regardless of the routing protocol or label switching protocol, it simply forwards the packet. A label is assigned to each packet by searching the label forwarding information base (FIB) table, all information in the table is populated with TDP (label distribution protocol) or LDP (label distribution protocol).

From the name MPLS "Multi Protocol Label Switching" shows that MPLS has the wonderful feature of supporting multiple protocols. The main advantage of MPLS is that it can be used with other networking technologies, as well as in pure IP, ATM and Frame Relay networks or even all three technologies, because a router that supports MPLS can coexist with a pure IP network as well as with ATM and Frame Relay switches. Support for multiple protocols makes MPLS universal, which attracts other users with mixed or different network technologies.

LSP (label switched path) is a path through the intermediate LSRs from the entry and exit nodes in the MPLS domain (see Figure 4). All necessary information used to create the LSP is transmitted using two protocols between LSR.LSRs can transmit all packets depending on the label assigned to these packets.

One or more labels can be attached in the MPLS packet header, so here we do not have an IP table, but a label table, and packet switching uses label look-up instead of IP table look-up.

Adding a label to packets avoids route look-up to forward the packet over the LSP. To create an LSP, all labels must be distributed between MPLS nodes using the Label

Distribution Protocol (LDP) or RSVP (Resource Reservation Protocol).

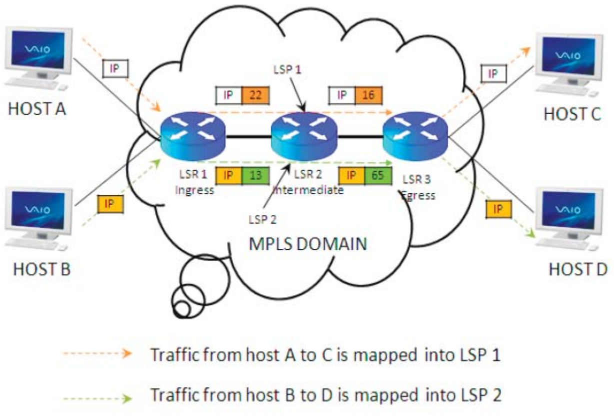

Figure 4. A label-switched path on an MPLS-enabled network

The flow of packets between the edge devices in the MPLS domain is defined by a label, which defines the forwarding equivalence class (FEC). Therefore, the packet forwarding process will take place along this label-switched route as virtual connections in a physical IP network without connection-oriented guaranteed processing.

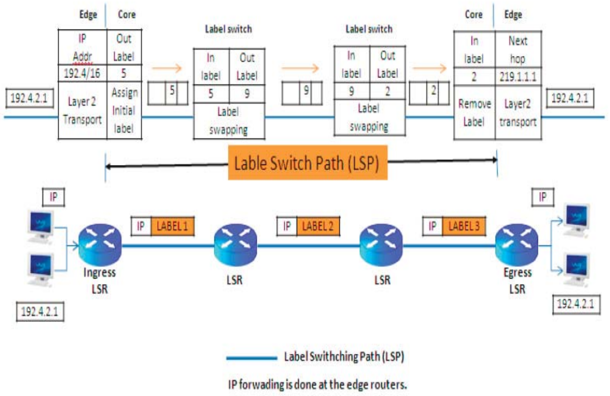

Figure 5. Label assignment in the MPLS domain and IP forwarding

MPLS edge routers only can determine whether a packet belongs to a label and forward it by examining its header and their special database to allocate the destination address.

Forward Equivalence Class (FEC) is a class for identifying a group of packets that have the same characteristics, transportation, processing and routing requirements for the destination. There are many parameters used to determine the FEC of a packet, such as source or destination IP address, source or destination port number, a DiffServ code point, and IP protocol identifier. Each LSR builds a table called the LIB label information base, which is based on the FEC, the FEC is determined for each packet, then the corresponding label from the LIB is attached to it.

And it is forwarded through the LSP, each LSR checks and replaces the packet label with another corresponding label before sending the packet to the next nearest LSR to the destination via the LSP.

In general, anything goes into the black hole never come back. In networking world, a Black hole is a routing mechanism in the ISP WAN used as a filter to drop unwanted traffic from different source IP's to unknown destination. Technique BGP Black hole can exclude and isolate some attacks by re-directing the unwanted traffic to a special interface (Null interface) so it never reaches to their intended destination.

BGP Black hole used to isolate DDoS attacks which aiming a certain IP addresses causing the congestion of physical link between services provide and a customer router. Installing a black hole on a provider router, can prevent unwanted traffic from entering customer's network or before that.

Sending traffic across an OSPF area with a lack of BGP routing information, will cause dropping packets (depending on Black hole mechanism) which have an unknown destination for these routers running OSPF.

So deploying MPLS technology within core network, BGP is still deployed at the network edges, provide transit traffic from any end point as MPLS routers carry just the information about the BGP's next step and don't scatter BGP across the network.

We will describe how MPLS can help us avoid the BGP black hole. In this topology we have: interface Loopback address is x.x.x.x/32, where x is the number of device.

X will be used as LDP transport address, LSR ID and OSPF router ID.

To advertise IP address of the interfaces (loop-back and directly connected), OSPF is running on all routers. IBGP neighbor’s relationship based on loop-back 0, is established between R1 and R4, but BGP is not running on R3 and R2.

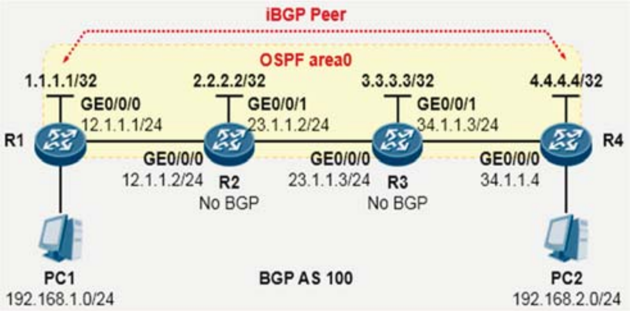

Figure 6. Network topology and configuration (Black hole is installed on routers with following IP addresses 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4)

R1 advertises the direct route 192.168.1.0/24 to BGP, and R4 advertises the direct route 192.168.2.0/24 to BGP, but on an OSPF network R1 cannot advertise the route to 192.168.1.0/24 and R4 cannot advertise the route to 192.168.2.0/24.

After completing the configuration this is what happens: R1 know form the BGP peer relationship the route to 192.168.2.0/24.

R1 start forwarding data packet (packets that are transmitted from PC1 to PC2) to R2, but R2 don't know about 192.168.2.0 because BGP is not running on it, so R2 will discard the packets and sending it to the black hole interface 2.2.2.2.

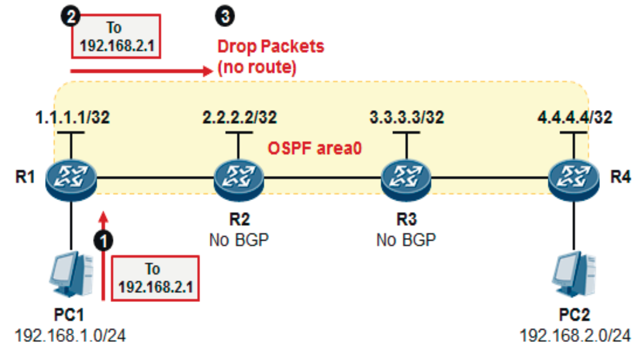

Figure 7. R2 discard the packets were sent it from R1 to his black hole interface 2.2.2.2

MPLS can be deployed on all routers to enable PC1 and PC2 to communicate with each other.

When PC1 wants to forward packets to PC2 it sent it to R1. From BGP, the next hop to 192.168.2.0/24 is 4.4.4.4. LFIB has an LSP destined for 4.4.4.4 so all packets to 4.4.4.4 be destined through this LSP, too.

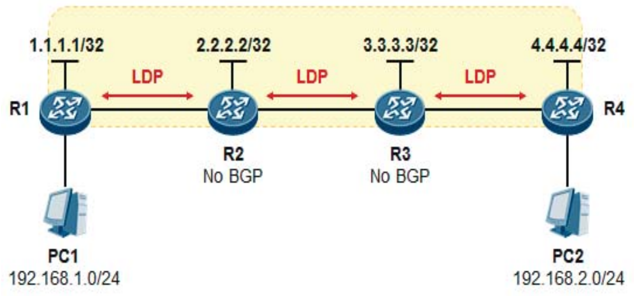

Figure 8. Deploying MPLS technology on all routers (Label Distribution Protocol or LDP distribute labels between MPLS nodes. All information in LFIB table is populated by LDP or TDP between MPLS nodes)

From PC1, the packets are first sent to R1.

Looking at the routing table, R1 finds that the destination can be reached depending on MPLS information. The next hop to the 192.168.2.0 is 4.4.4.4, R1 now adds a label in a push process (the 1026 label is corresponding to 4.4.4.4) into the packets and it sends them to R2.

R2 in its turn swaps label 1026 into label 1028 and sends the packets to R3. The next hop (4.4.4.4) R4 is directly connected so R3 pops out the label and sends the packet to R4. In this way, PC1 can successfully ping PC2 using MPLS.

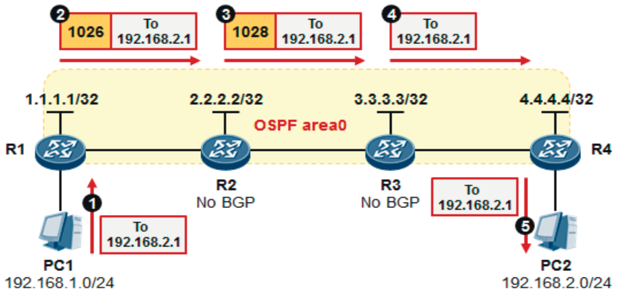

Figure 9. The packets successfully were sent from PC1 to PC2 depending on MPLS information, avoiding BGP “Black hole”

CONCLUSION

1. High revenue applications have always been the main focus of service providers. Internet and service providers have a new challenge because these applications have different latency, bandwidth, jitter and packet loss needs.
2. Internet Protocol was not designed to support QoS, rather it was designed for education and research. On the Internet, we have unpredictable traffic flow, so there is a huge need for traffic engineering to run these applications efficiently.
3. MPLS provides a solution by providing a connection-oriented structure on top of the current IP-based network to maintain the required level of QoS for these applications. The main advantage of MPLS is that it can be used with other networking technologies, as well as with pure IP.
4. Black hole is a routing mechanism, used as a filter to drop unwanted traffic from different source IP's to unknown destination. Sending traffic across OSPF area with a lack of BGP (Border Gateway Protocol) routing information, will cause dropping packets which have unknown destination for these routers running OSPF.
5. Deploying MPLS technology within core network, Border Gateway Protocol is still deployed at the network edges. Help avoiding Black hole and provide transit traffic from any end point as MPLS routers carry just the information about the BGP's next step and do not scatter BGP across the network.

REFERENCES

[1] S.N. Stepanov. Teletraffic Theory: Concepts, Models, Applications. Moscow: Hot Line – Telecom, 2015. 868 p. (Theory and Practice of Infocommunications Series).

[2] V. Olifer, N. Olifer. Computer networks. Principles, technologies, protocols: Study book for universities. 5th edition. St. Petersburg: Peter, 2018. 992 p.

[3] Srivas Vegeshna. Srinivas Vegeshna. Quality of service in IP networks. Fundamental principles of quality of service functions in Cisco networks. Moscow: Williams Publishing House, 2003. 368 p.

[4] I.V. Stepanova, M.O.A. Abdulvasea. Use of perspective technologies for development of the distributed corporate communication networks. *T-Comm*. 2017. Vol. 11, No. 6, pp.10-15.

[5] E.A. Kucheryaviy. Traffic management and quality of service in the Internet. SPb: Nauka i tekhnika. 2004. 336 p.