Hybrid MPLS - Internet VPN Networks

Vasile Dorinel NICOLAE, Ştefan NISTOR, and Petrică CIOTÎRNAE

Abstract—Nowadays, the data network area offers a very wide range of data switching techniques according to user needs. The current paper is concerned with a new broadband solution, namely the use of an MPLS-Internet VPN hybrid network. Even though MPLS is the basic solution in most private transport networks, with the explosive growth of the Internet, it has begun to be an alternative solution for data transmission. The purpose of this study is to balance the advantages and disadvantages of implementing this solution by bringing arguments on both sides and, finally, to draw an objective conclusion as to its applicability.

***Index Terms*—Hybrid MPLS, VPN, Internet.**

I. Introduction

If we are talking about broadband techniques in today's networks, surely one of the first instincts is to think about MPLS. The ability to use labels for traffic classes, Quality of Service (QoS), and traffic engineering are indisputable advantages in terms of the quality of this technique. However, with the explosive development of the Internet and new cloud technologies, the use of a simple Intranet network has become a limitation to the expansion of the networks. Another factor to consider is that the Internet allows the interconnection of networks in different location of the globe, eliminating the distance impediment.

Related to security issue, the possibility of implementing QoS and the traffic engineering allow us to catalog the data transmitted through the network, according to the level of classification and according to our perception of priorities. E-mails or files that do not contain critical data can be transmitted smoothly over the Internet; video conference between remote locations can be achieved with a good quality over the Internet without involving the costs of renting an international private circuit. From a security point of view, we can use VPN clients over the Internet, we can use a firewall filtering, or we can use dedicated software to monitor attacks and traffic.

The advantages of building a private network architecture is the total control over the network, removing any exposure to possible attacks, and making sure the data arrives at destination without latency or loss, but comes with a compromise, because it is necessary to obtain access to a layer 2 network provider, and the financial cost increases.

The bandwidth required for private networks is rising every day. To solve the cost issue, more clients migrate to hybrid networks composed of a private MPLS backbone interconnected with the Internet. Routing between the private network and the Internet requires special management of network applications and traffic sources and destinations. Data routing is done in the network border area where, depending on the application or destination of the stream, the routing equipment will route the stream to the Internet connection or to the private MPLS network. To better understand the operation principle, consider Figure 1 which clearly illustrates the schematic diagram of a hybrid network.

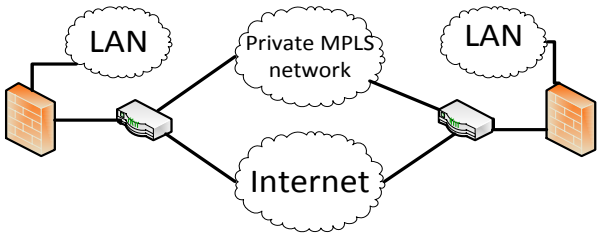

Figure 1. Hybrid network topology

II. The Challenges of New Technologies for MPLS

Regarding the QoS of the network, MPLS offers a different approach than the classic concept of Quality of Service. Video and voice packets can be considered among the most demanding type of traffic in terms of loss, delay and jitter. This is because the vast majority of time voice and video data is used for live services and applications (live streaming, voice and video calls, video conference, etc). Over the Internet, QoS consists of placing the packets in different priority queues that are physically located in different hardware network equipment buffers. Because of their sensitive status, voice and video packets are assigned in the highest priority queues (the voice datagrams are placed with a higher priority than video datagrams due to the fact that voice packets are considerably smaller in size and will be the first who exit the buffers). Type of service (TOS) field of the IP header provides the necessary information in order for routers and other network devices to be able to map the traffic. TOS is divided into two fields: a six bit field named DSCP (Differentiated Services Code Point) and a two bit field ECN (Explicit Congestion Notification). DSCP defines in fact the queues different types of traffic are mapped to. The most common queue for voice traffic is EF (Expedited Forwarding) where for video traffic is AF (Assured Forwarding).

This is an efficient method of providing end to end connectivity for certain services at the expense of other ones, not so sensitive (email, file transfer, etc). However, in some extreme scenarios when the network congestion is high, buffers reach their maximum capacity and packets are being dropped.

MPLS offers a different type of QoS using traffic engineering mechanisms. The principle consists of redirecting the traffic to an uncongested path, with available

V. D. Nicolae is with the Communications Department, Military Technical Academy, 39-49 George Coşbuc Ave., Sector 5, 050141, Bucharest, Romania.

Ş. Nistor is with the Communications Department, Military Technical Academy, 39-49 George Coşbuc Ave., Sector 5, 050141, Bucharest, Romania.

P. Ciotîrnae is with the Communications Department, Military Technical Academy, 39-49 George Coşbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: petrica.ciotirnae@mta.ro).

bandwidth instead of congesting the shortest path of one link, leaving available bandwidth unused on various links. QoS in this case is achieved through bandwidth reservation. In MPLS terminology a LSP is a unidirectional tunnel between two different points in the network. RSVP-TE (resource reservation protocol – traffic engineering) protocol associate every LSP with a certain bandwidth value. This value can be determined through an offline calculation (outside the router, can be a script or a tool) or auto-bandwidth (calculated on the router).

When the shortest path with enough bandwidth to carry a certain LSP is found, RSVP-TE signals the LSP between a set of links, practically reserving the path. The pool of available bandwidth is stripped of the LSP bandwidth. Unlike traditional QoS, where packets are dropped in case of congestion, this method simply redirects the packets to different paths with higher latency.

In Figure 2 is presented an LSP distribution where LSP 1 is the shortest path (an ATM network, for example), LSP 2 provides higher latency than LSP 1 (Frame Relay network, for example) and LSP 3 is a low quality one (best effort IP network). In this scenario the three LSP's can be reserved for different traffic, from the QoS offered by the MPLS technology. In a large MPLS domain can co-exist different type of protocols as shown in Figure 4 (ATM, Frame Relay and IP).

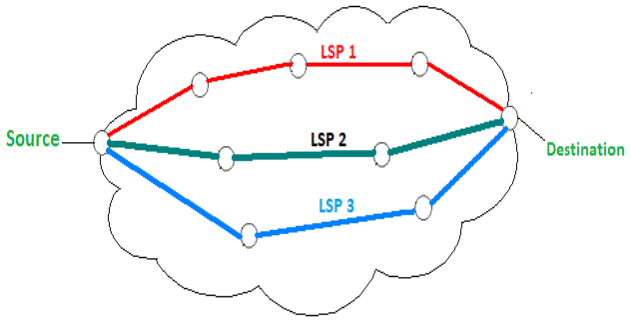

Figure 2. LSP distribution in an MPLS network

Certain customers or specific traffic can be mapped to a dedicated LSP in order to grant priority. The most important aspect of the unusual QoS that exists within MPLS is that the packets aren't dropped, just sent over other paths than the shortest one. It is unconditionally better that data to arrive with a delay than not to arrive at all.

III. Proposed Topology

In practice, implementation of a functional topology implies, besides the actual design of the network, a laborious configuration, for example Figure 3 presents an up to date topology for a network with MPLS backbone and an Internet Gateway. This network architecture is an example on how to integrate the private network with the public one (Internet).

In a classic transport network, the public and private parts are well separated and have little or no access to each other. In the case of the proposed topology, we want the two to be integrated in a safe and efficient way. Thus, new applications such as cloud work are not blocked when an accredited user from a remote location (using an Internet connection) wants to access resources from the private network (servers from the company's headquarters).

It is easy to observe that the IP packet reached Site 1 is labeled with a Forward Equivalence Class (FEC) and forwarded to the core router.

The LSR 1 router receives the labeled package, and processes it properly with the FEC initially, adding a label conforming to the backbone switching rules. Thus, when the packet reaches the last border node, the Site 3 router removes the tag and transmits it to the desired destination. This package route description, from its entry into the MPLS network to its destination, is valid for data that is considered sensitive, and which use a private and secure network throughout the route.

If it is necessary to communicate over the Internet with a remote location, the packets are sent to one ore more central nodes which will direct that data to a firewall.

The router that directs traffic to the firewall will have two connections to it, one to be used to transmit user traffic to the Internet, and the other to transmit traffic coming from the Internet to users.

In terms of gateways to the Internet, to avoid network congestion or overloading a single firewall, it is recommended to use multiple gateway devices to the Internet.

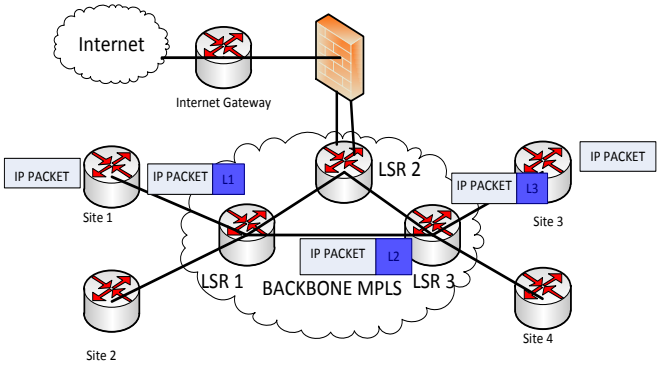

Figure 3. MPLS topology with Internet output

One important aspect when using a traditional VPN model is the convergence time between VPN sites. The virtual circuits managed by the Internet Service Provider can take timers adjustments, thus being capable of obtaining high-speed convergence. Although we can reach high-speed convergence times through the MPLS/VPN service, these are primarily a service provider duty.

The convergence delay can occur in one of these processes:

- The advertisement of routes to the backbone;
- The propagation of the routes across the backbone;
- The import and advertisement of the routes to other sites.

The choice of routing protocol has also an import role on convergence. For example, if BGP protocol is used in the propagation of routes across the backbone, these will not be affected by introduction of MPLS. In this case a factor that can affect convergence is the invocation of the BGP scanner process to scan the BGP table and routing tables. This is necessary to check for next-hop changes in order to obtain accurate information to be passed to the BGP neighbors. For any new routes that needs to be discovered, the network and redistribute commands are handled by the same process. The process of addition the new routes learned by the BGP

neighbors or modification of existing routes is done using advertisement interval. The maximum time interval for a route to not be advertised to a neighbor is tens of seconds.

Some of the advantages of choosing BGP as the routing protocol in order to transport VPN routes:

- the large number of VPN routes in the network;
- BGP is multiprotocol by design, it can carry routing information for a number of different address families;
- the information attached to a route can be carried as an optional BGP attribute; additional attributes can be defined and forwarded by any BGP router that doesn't understand them, making propagation of routes very simple.

In order to speed up the convergence times the BGP scanner process can be tuned. There are no actual optimal settings of this tuning process, these must be determined empirically by monitoring your implementation, because every topology will be different and will have specific particularities.

Another important factor when an ISP offers an IP-based VPN service based on MPLS/VPN technologies is represented by overlapping addresses issue. The ISP traditionally deals with the address space problem in three ways:

- customers renumbering their networks;
- implementing the VPN service with IP-over-IP tunnels;
- translate customer addresses into different set of addresses at the Internet Gateway router (provider edge router) and then translate those addresses back using a complex NAT (network address translation) scheme.

In the peer-to-peer VPN implementations' the major obstacle is the overlapping addresses situation. The MPLS/VPN technology has a solution to this problem, each VPN has its own routing and forwarding table in the router so any host that belongs to a VPN is granted access only to the set of routes contained within that table.

In each VPN can be used either global or private IP address space. The only rule is that the address space must be unique within that VPN.

Besides the virtual IP routing table, each virtual router associate structures like:

- a forwarding table that is derived from the routing table;
- a set of interfaces that use the forwarding table;
- a set of rules to managed the import and export routes from the VPN routing table;
- a set of routing protocols to add information into the VPN routing table;
- a set of router variables associated with the routing protocols that populates the VPN routing table.

The VPN routing and forwarding instance (VRF) represents the combination between the VPN IP routing table and VPN IP forwarding table. In an MPLS environment the difference between IP routing table and IP forwarding table is that the IP forwarding table contains MPLS encapsulation information.

IV. Simulation - Results and Analyzes

In the previous chapters we briefly presented what MPLS means, why it is useful in hybrid networks and what advantages this protocol has when is used in conjunction with traffic engineering techniques.

Figure 4 presents a network topology whose behavior will be analyzed in the following cases: IP with RSVP for traffic prioritization, MPLS without traffic engineering techniques and MPLS-TE (MPLS with traffic engineering techniques).

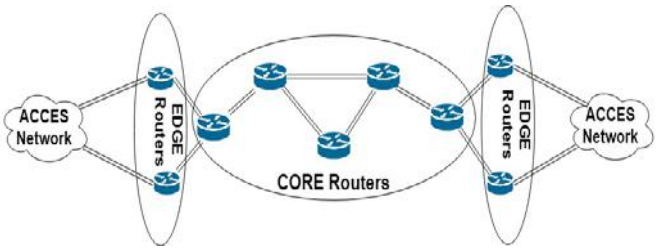

Figure 4. The network topology used in simulation

In case of congesting the core network (packet flooding or during a link failure), communication between hosts is affected by latency and packet loss until it becomes impossible. The same topology was used for the IP, MPLS and MPLS-TE networks and the analysis was carried under the same scenario: increasing number of packets were injected in the core network followed up by ping tests to measure packet loss and latency.

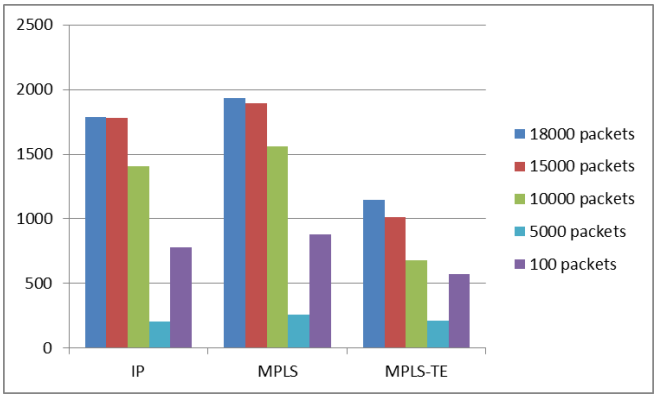

Figure 5. Latency (ms)

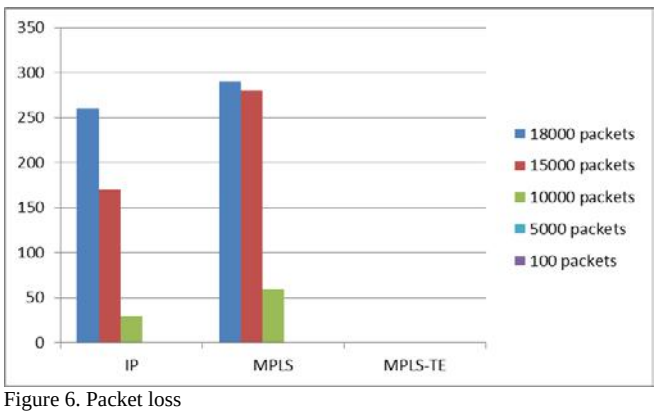

Figure 6. Packet loss

In Figure 5, latency is quantified by round trip delay time (RTT). For the IP and MPLS network there is an increase in RTT while for the MPLS-TE network the RTT is significantly reduced. In terms of packet loss MPLS-TE network is far more efficient because it noticed no losses when sending packets. In the IP and MPLS network on the other hand, the number of lost packets increases when

sending packets.

As the network becomes more and more congested the graphics showed that the MPLS-TE network had clearly better results in terms of latency and packet loss. In case an MPLS network is disabled, it will continue to operate as an IPv4 network. By using traffic engineering with label switching we can avoid congestion in a core network or service provider network.

V. Conclusion

In order to meet the new customer's requirements it is necessary to use various network technologies and scenarios. This translates in using the hybrid networks in order to manage various types of traffic. Services, security and QoS vary on each network segment, depending on different factors such as available bandwidth, latency, the protocols used in that segment, etc. Special treatment is necessary for sensitive voice and video traffic.

It is certain that today's requirements are quite different from those 10 years ago, technologies are different, applications have evolved, and the communications networks have to adapt to the new requirements. Therefore, in a hybrid network, using MPLS characteristic traffic engineering techniques, and VPN over the Internet, encrypted, allows users to access the network remotely, or to connect multiple locations in different areas of the world, without damaging any of the services used (data, voice or video).

Network administrators need to find a network optimization solution with lower costs, but without lowering the quality of services offered. Creating a hybrid network that allows users to access the sensitive services, but also to access the Internet; it is an efficient alternative and significantly reduces the cost of renting private circuits.

Currently, the MPLS networks can't be completely replaced by the Internet, these being a crucial segment of the proper functioning of the companies' production. But taking into account the increasing need to access the public cloud, remote work, mobility and the costs for renting high-capacity transfer circuits, it is obvious that the current Intranet networks will be transformed into hybrid networks.

This work was supported by a grant of the Ministry of Innovation and Research, UEFISCDI, project number 9SOL/ 12.04.2018 within PNCDI III.

References

[1] I. Pepelnjak, J. Guichard, *MPLS and VPN Architectures*, Cisco Press, 2000.

[2] R. Layland, "The Future of the Branch Office is a Hybrid WAN," in The 2015 WAN Challenge, pp. 1-4, Cisco, 2015.

[3] A. Park, "Ensuring Application Performance in the Hybrid WAN Environment," in The 2015 WAN Challenge, pp. 5-7, Cisco, 2015.

[4] A. Claaßen, "The networks of the future are hybrid," T-Systems International, Germany, 2016.

[5] J. Evans and C. Filsfils, *Deploying IP and MPLS QoS for Multiservice Networks*, © Morgan Kaufmann, 2007.

[6] L. De Ghein, *MPLS Fundamentals*, Cisco Press, 2006.

[7] L. Andersson, R. Asati, *Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field*, Cisco Systems, Feb. 2009.

[8] Y. Rekhter, E. Rosen, *Carrying Label Information in BGP-4*, Cisco Systems, May 2001.

[9] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, RFC, 2001. doi: 10.17487/RFC3209

[10] Y. Rekhter, R. Aggarwal, *Graceful Restart Mechanism for BGP with MPLS*, Juniper Networks, Jan. 2007.