IMPACT OF TUNNELING ON NETWORK CAPACITY

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

DOI: 10.36724/2664-066X-2022-8-4-9-13

ABSTRACT

For many companies, setting up a VPN for secure, en-crypted communication is a cost-effective alternative to pur-chasing, operating, and managing a separate physical net-work. Many institutions, corporations, government agencies and non-profit organizations want to have their own private IP network for secure and reliable connectivity between of-fices across multiple geographies. A virtual private network (VPN) is a secure, encrypted connection over a public public network. Creating a separate network requires the purchase of equipment, its installation and maintenance. A VPN-based solution using the public Internet is becoming a cost-effective solution for many corporations. As a research task, the au-thors define an assessment of the impact of the tunneling technology used to solve problems arising from the lack of network support from existing data transfer protocols. The possibility of using the IPSec protocol and MPLS technology to implement tunneling is considered and compared. The results of the comparison and evaluation of the impact of the choice of protocol on the required bandwidth are presented.

KEYWORDS: *Packets, Bandwidth, Virtual Private Networks, Internet Protocol Security (IPsec), Multi Protocol Label Switching (MPLS), Label Switching Routers (LSR), Tunneling*

INTRODUCTION

Many institutions, corporations, government agencies and non-profit organizations want to have their own private IP network for secure and reliable connectivity between offices across multiple geographies. A virtual private network (VPN) is a secure, encrypted connection over a public public network. Creating a separate network requires the purchase of equipment, its installation and maintenance. A VPN-based solution using the public Internet is becoming a cost-effective solution for many corporations.

On the way to the destination address, data packets pass through many different networks. Packets use network protocols, but not all networks support the necessary protocols. To solve this problem, you can use the approach of placing the package inside another package using the protocols that are supported on the given network. This process of packet encapsulation is called tunneling. Tunneling allows VPN packets to reach their destination, which is usually a private network. The tunneling process provides a secure, encrypted connection between networks.

The aim of the work is to study the effect of tunneling on network throughput. Let's look at the MPLS protocol and the IPsec protocol, comparing the impact of each on network throughput for a Voice of IP (VoIP) application.

1. INTERNET PROTOCOL SECURITY (IP-SEC) CAPABILITIES

Tunneling is the technique of putting a packet of data into another packet (containing routing information) and sending it over the Internet. The packets travel along a path called a tunnel.

Internet Protocol Security, known as IPSec, is used to secure Internet communications over an IP network. Many VPNs use the IPsec protocol suite, which runs on top of an existing IP network. IPSec secures communications over the Internet by verifying the session. It encrypts every data packet during the connection. IPSec operates in 2 modes – transport and tunneling.

Transport mode encrypts the message in the data packet, while tunneling mode encrypts the entire data packet. IPSec can be used with other security protocols.

For example, suppose a company uses IPv6 to connect one of its offices (office A) to another (office B). The network between offices A and B only supports IPv4. It is necessary to pack (encapsulate) IPv6 packets into IPv4 packets in order to successfully transfer data between offices.

2. CAPABILITIES OF MULTI PROTOCOL LABEL SWITCHING TECHNOLOGY

A number of efforts have been made to increase the forwarding rate of packets in IP routers by introducing the concept of fixed-length labels. These efforts have been consolidated by the IETF (Internet Engineering Task Force) into the MPLS technology [RFC 3031, RFC 3032].

MPLS is a label lookup packet forwarding technology that does not affect the packet's IP header. An MPLS network consists of several routers called LSRs (Label Switching Routers). Routers that connect to IP routers are called LERs (Label Edge Routers).

The RFC defines the MPLS header format between MPLS capable devices (routers), between the second and third level headers. The MPLS Label header, as shown in Figure 1, consists of 20 bits (220 values or labels). The label value can be used by the LSR to find the next hop.

The EXP field consists of three bits of information and is used to implement functions related to QOS quality control. The next field is one 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 MPLS VPN or MPLS TE.

The next byte is an eight-bit MPLS TTL (time to live) field that serves the same purpose as the IP TTL byte in the IP header. Each time an LSR forwards a packet, it decrements the TTL field in the packet's header, and if the value reaches zero, the packet is dropped.

An MPLS router (LSR, LER) forwards MPLS packets by looking up the MPLS label in its forwarding table and then immediately forwards the datagram to the appropriate egress interface. There is no need to process the header of every packet on every hop to determine the destination IP address and then look up the longest prefix match in the forwarding table based on the destination IP address.

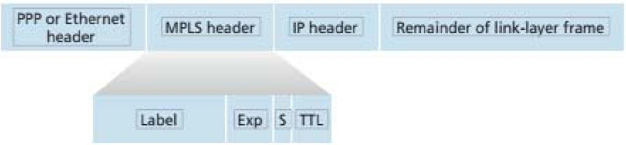
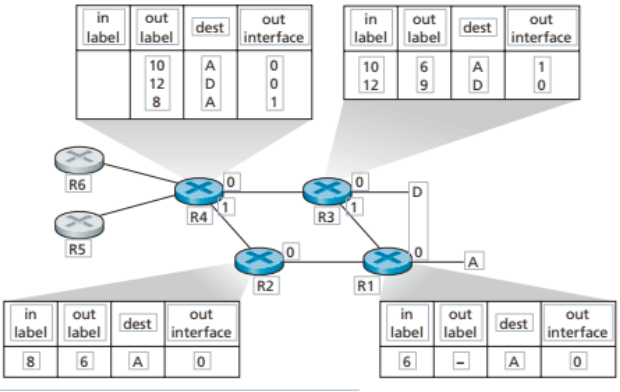


Figure 1. MPLS header

Figure 2 uses the following designations: R1-R4 – MPLS routers; R5 and R6 are standard IP routers.



in label	out label	dest	out interface
	10	A	0
	12	D	0
	8	A	1

in label	out label	dest	out interface
10	6	A	1
12	9	D	0

in label	out label	dest	out interface
8	6	A	0

in label	out label	dest	out interface
6	–	A	0

Figure 2. MPLS transfers

According to the MPLS concept, router R1 announces to R2 and R3 that destination A is reached by any MPLS frame with label 6.

Router R3 announces to R4 that received frames with MPLS tags 10, 12 will be forwarded to destinations A, D.

Router R2 announces to R4 that the received frame with MPLS label 8 will be switched in direction A.

Router R4 can reach A with outgoing MPLS label 10 on interface 0 and outgoing MPLS label 8 on interface 1.

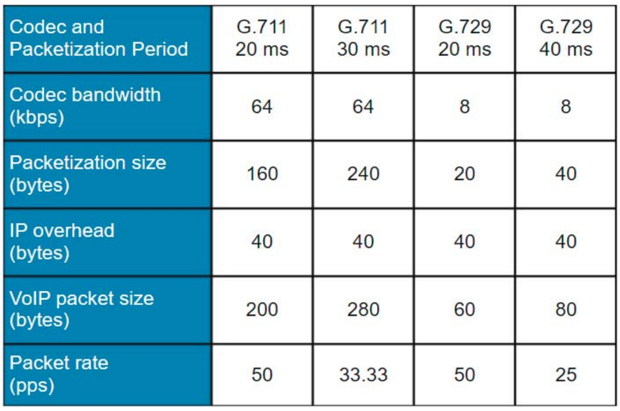
3. CODEC TYPE SELECTION

Various types of codecs based on different technologies are used to process audio and video data. To assess the quality of codecs, the Mean Opinion Score (MOS) indicator is used. MOS values are in the range from 1 to 5 (1 – "bad", 5 – "excellent"). The rating is given taking into account the P.800 and P.830 ITU-T standards.

G.711 is the default standard in any IP device and is the most widely used. The data transfer rate in one direction is 64 kbps, with a logarithmic compression ratio of 1:2 (16-bit sampling is reduced to 8-bit). On the MOS scale, it has a value of 4 (Fig. 3). G.711 can be used for LAN VoIP applications where there is a margin of available bandwidth.

G.729 is a codec that provides a drastic reduction in bit rate and payload size, but a slight reduction in voice quality.

G.729 and G.711 are most commonly used in VoIP applications. However, G.729 is more suitable for networks with limited bandwidth and low latency.



Codec and Packetization Period	G.711 20 ms	G.711 30 ms	G.729 20 ms	G.729 40 ms
Codec bandwidth (kbps)	64	64	8	8
Packetization size (bytes)	160	240	20	40
IP overhead (bytes)	40	40	40	40
VoIP packet size (bytes)	200	280	60	80
Packet rate (pps)	50	33.33	50	25

Figure 3. Codec characteristics

4. PACKET SIZE ESTIMATION FOR VOIP

We determine required network bandwidth for the implementation of VoIP according to formula:

$$B = (Pt \text{ x } 8 /1000) \text{ x } N,$$

where Pt = Payload – total packet size, bytes:

$$Pt = RP + O,$$

where RP is the packetization size defined as RP = (Tpack / 1000) × (codec bandwidth × 1000 / 8), bytes per packet; Tpack – packetization period; O – Overhead, bytes; N – the number of packets per second.

The packets per second (PPS) rate can be calculated by taking the reciprocal of the packetization period. Packet size is the amount of digitized and encapsulated voice in each IP packet, and it depends on the codec used. In G.711, a 20ms voice duration is digitized and encapsulated in one IP packet, so the packet rate is 1/20ms = 1/0.02 = 50pps. G.711 uses Pulse Code Modulation (PCM) 8000 samples with 8 bits for each sample with a total bandwidth of 8000*8=64Kbps. These 64 kbps contain 50 packets, which means the size of each packet

$$64 *1000 / 8*50 = 160 \text{ bytes.}$$

На выходе кодека голосовые кадры помещаются в real-time protocol (RTP) packets to give them the necessary information for real-time end-to-end transmission, such as sequence numbers, timestamps.

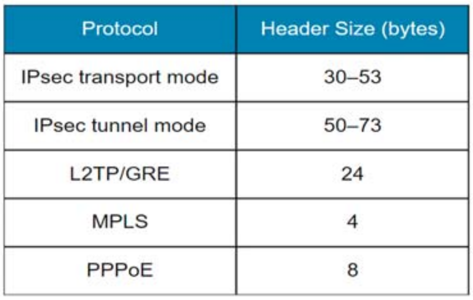
The overhead added by RTP to the payload is 12 bytes. In turn, the User Datagram Protocol (UDP) transport layer protocol adds an overhead of 8 bytes. The overhead added by IP is 20 bytes, and Ethernet adds 18 bytes. We will not add the size of the Ethernet header now, because this will be done in the last step after the tunneling process.

Considering the addition (excluding the overhead of tunneling and without adding the size of the Ethernet header), we get 160 + 12 + 8 + 20 = 200 bytes.

5. ESTIMATING OVERHEAD COSTS WHEN USING SECURITY AND TUNNELING PROTOCOLS

The implementation of tunneling leads to the appearance of so-called "overhead", that is, to an increase in share of service traffic in the transmitted information. There are many non-security protocols for tunneling IP packets and frames. Data for some common tunneling protocols with overhead for each packet is shown in Figure 4.

IPSec adds an Encapsulating Security Payload (ESP) header to the IP header to provide authentication and encryption. In transport mode, only the payload of the IP packet is encrypted. While in tunnel mode, the entire IP packet is encrypted, including the header. Encrypting the IP header eliminates the ability of routers to know the next hop of the packet and therefore route it, so an encrypted IP packet needs a different header to use in the routing process.



Protocol	Header Size (bytes)
IPsec transport mode	30–53
IPsec tunnel mode	50–73
L2TP/GRE	24
MPLS	4
PPPoE	8

Figure 4. Sizes of additional headers in security and tunneling protocols

ESP supports the use of a list of encryption and integrity protection algorithms such as HMAC. The operation of HMAC is based on the use of a given block size of 64 bytes. 8 bytes of message length are added to each packet (including 1 bit of the padding procedure identifier). After adding 8 bytes to a packet, if its size is not a multiple of 64, it must be padded so that it can be handled.

8 bytes of the padding HMAC procedure ID will be added to the 200 byte packet.

200 + 8 = 208 bytes.

ESP also adds some additional data and overhead: ESP header = 8 bytes; ESP initialization vector = 16 bytes; ESP trailer = 16 bytes; tunnel mode header = 20 bytes.

The package size is:

208 + 8 + 16 + 16 + 20 = 268 bytes.

Now you can add an 18 byte overhead for the link layer Ethernet header. It turns out:

Pt = 268+18= 286 bytes.

Let's calculate the bandwidth per voice connection when using the IPSec protocol using the formula:

$B_{1\ IPSec}$ = (Pt X 8 / 1000) X N,

where t= packetization size + O = 286 bytes; N – packet rate, N = 50 pps.

We get B1ip-sec = 114.4 kbps.

When using the MPLS protocol with a header size of 4 bytes, to create a tunnel, we calculate the overhead:

O= Eth + MPLS+ IPv4 + UDP +RTP =
= 18+ 4+ 20 +8 +12= 62 bytes.

Pt = packetization size + O = 160 + 62 = 222 bytes.

N is the packet rate, N = 50 packets per second.

Let's calculate the throughput per voice connection when using MPLS

B_1mpls = 88,8 kbit/s.

Thus, when using the security protocol and tunneling technology MPLS, the required network bandwidth per connection is reduced by 114.4 / 88.8 = 1.29 times compared to the IPSec protocol.

6. PLANNING AND CALCULATING BANDWIDTH FOR A CORPORATE NETWORK

The process of planning a telecommunications network requires carrying out the necessary measurements or traffic calculations. The results are used to determine the network topology, the bandwidth of the backbone group, the necessary lines to provide communication between network divisions. The most delay-sensitive, growing in demand, and revenue-generating applications are VoIP.

After calculating the throughput for a single voice call, we can calculate the total throughput based on the estimated traffic for all calls in Erlang multiplied by the throughput for a single call.

As an example, consider a corporate network that has a central office in Moscow (200 employees), two branches in St. Petersburg (100 employees) and Kazan (150 employees). They need to be able to communicate with each other through the central office.

Table 1

The results of the calculation of telephone load intensity in the CNN

Branch	Moscow	St. Petersburg	Kazan
Number of employees	200	150	100
Traffic volume (minutes/day)	9600	7200	4800
HNN (minutes)	1632	1224	816
A (Earl)	27.2	20.4	13.6

We need traffic delivery capabilities to implement VoIP (in terms of number of channels and required bandwidth), so we need to calculate the traffic during busy hour (HHH) in Erlang.

Traffic in HNN can be calculated by taking a percentage of the total number of daily minutes of calls in HNN (Table 1). The telecom industry defaults to a multiplier in HTN (17%) with a percentage of blocked calls or a Blocking Target (1%).

The results of calculating the required bandwidth in kilobytes for each branch of the company are presented in Table 2.

Table 2

The results of required throughput calculation

kbit/s	Moscow	St. Petersburg	Kazan
IPSec	3112	2333	1556
MPLS	2415	1811	1208

Comparing the required bandwidth when using MPLS and IPSec for a specific corporate network structure, we see that the use of MPLS technology can significantly save network bandwidth.

CONCLUSION

1. Many institutions, corporations, government agencies and non-profit organizations want to have their own private IP network for a secure and reliable connection between offices in several geographic regions. Instead of creating a separate physical network that is expensive to purchase, install, and maintain, a VPN solution over the existing public Internet is becoming a viable solution for many corporations.

2. Packets travel through many different networks on their way to their final destination. Communication protocols in networks differ. To overcome this problem, tunneling is performed, that is, packing packets inside other packets using protocols that are supported in a particular section of the network. The tunneling process allows a secure, encrypted connection to be established between users on different networks.

3. The performed analysis and calculation showed that when using the security protocol and tunneling technology MPLS, the required network bandwidth per connection is reduced by 1.29 times compared to the IPSec protocol.

4. Creating a tunnel with guaranteed QoS requirements for a highly sensitive application such as VoIP using MPLS saves significant bandwidth compared to IPSec, the secure tunneling protocol used in VoIP. This circumstance is especially important for the organization of corporate communications using the resources of the public Internet.

REFERENCES

[1] V. Olifer, N. Olifer. Computer networks. Principles, technologies, protocols: A textbook for universities. 5th edition. St. Petersburg: Piter, 2018. 992 p.

[2] A. B. Goldstein, B. S. Goldstein. MPLS technology and protocols. St. Petersburg: BHV-Peterburg, 2014. 304 p.

[3] V. P. Koryachko, D. A. Perepelkin. Analysis and design of data transmission routes in corporate networks. Moscow: Hotline – Telecom, 2020. 235 p.

[4] B.Ya. Lichtsinder. Traffic of multiservice access networks (interval analysis and design). Moscow: Hotline – Telecom, 2018. 290 p.

[5] S.N. Stepanov. Theory of teletraffic: concepts, models, applications. Moscow: Hotline – Telecom, 2015. 868 p.

[6] I. V. Stepanova, M. O. A. Abdulvasea, N. Zhuven. Analysis of promising approaches to improving the reliability of convergent corporate communication networks. *T-Comm*. 2015. Vol. 9, no. 12, pp. 44-51.