Study of the impact of routing and the profoundness of GRE tunnels on the performance of the transmission of real time applications in IP networks

Dounia EL IDRISSI[1], Najib ELKAMOUN[2], Fatima LAKRAMI[3], and Rachid HILAL[3],

Chouaib Doukkali University, STIC *Laboratory*, El Jadida, Morocco

Summary
This paper studies the impact of varying GRE tunnel proprieties on the performance of the transmission of real time application in IP networks. It focuses on studying the impact of both the profoundness of the tunnel by increasing the number of crossed routers and routing protocol combination used to disseminate data through GRE tunnel. Results evinces the limits of using GRE tunnels in IP networks, it exhibits the best routing schema to use, especially for real time traffic.

Key words:
Routing protocols, Tunnel GRE, EIGRP, OSPF, RIP, QoS, Opnet.

1. Introduction

Tunnel allows the user to connect to another user (in other private networks for example) over the Internet or another public network with the security and functionality available so far only on private networks. It makes possible to pass directly from one point to another, without having to suffer the pangs of traffic on the surface.
They propose a method to link "directly" two remote private networks, through an inter-network as complex as the Internet. There are many ways to make tunnels. PPP can be considered as a tunnel in configurations such as PPPoE or PPPoA. These are tunnels on layer 2 of the OSI model, in the same way as L2TP (Layer 2 Tunneling Protocol), used on operators' networks, implemented in non-unbundled ADSL connections. At level 3, there are also several solutions, such as PPTP (Point-to-Point Tunneling Protocol), or tunnels over IPSec.
GRE or Encapsulation Generic Routing is a tunneling protocol that allows to encapsulate any packet of the network layer. The original package is the payload of the final package. For example, tunnel servers that encrypt data can use GRE over the Internet to secure Virtual Private Networks. Making a tunnel through networks involves establishing and maintaining a logical connection between two points.
Through this logical connection, data will be sent using a tunnel protocol. A GRE tunnel is the easiest way to create a tunnel between two points. This tunnel makes it possible to encapsulate in the network layer (level 3 OSI) any IP packet. We are interested in this paper to the practical study of GRE tunnels, and to evaluate their performance by varying several network parameters and evaluating their impact such as the combination of routing protocols and the profoundness of the network.
The main goal is to define the best routing combination for better performance and to highlight GRE tunnels limits in a general case of study. The rest of the paper is organized as follows: section 2 presents an overview of the tunneling technology. In section 3, the GRE tunnels are explained and detailed. A brief review of routing protocols in wired networks and in tunnels is presented in section 4. Section 5 resumes the context of study, simulations and results. Section 6 concludes the paper.

2. Tunneling Overview

Tunnels provide a way to transport protocols not supported by the underlying network infrastructure[1]. They are primordially deployed when the crossed network doesn't support the protocol being transported or cannot perform packets dissemination due to lack or the absence of informations about routing mechanism or addressing types (public versus private) or even the traffic type (multicast or broadcast).
In general, tunnels are especially used to connect remote, geographically separated sites over an existing network, most notably routing over a public infrastructure (such as the Internet). When used in such context, tunnels create VPN connection between two or multiple remote sites. In this case, a new header is used for encapsulating packets destined to remote private networks, the same header that is used to across the public network (internet).[2]
The principle of Tunnels is to create a virtual network (overlay network) on top of a physical underlying infrastructure (underlay network), to provide a logical interface that emulates a direct physical link connecting the two sites.
The tunnel interface proceeds first by encapsulating the traffic of the original protocol, intending to cross the network, using an intermediate protocol. The intermediate protocol is then encapsulated inside a transport protocol, which is used to pass through the underlying infrastructure

Manuscript received July 5, 2018
Manuscript revised July 20, 2018

(for example internet) [3]. Traffic that enters the tunnel is then forwarded, in a transparent way from the underlying infrastructure.
It is received on the other end to be decapsulate and further processed. The crossed network devices do not examine or check the original packet's IP header or their payload.

3. Review Of GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol developed originally by Cisco, in order to enable the encapsulation of a wide variety of protocols of network over point-to-point links.
A GRE tunnel is also used when packets need to be transmitted from one network to another while crossing a public or insecure as the Internet. The principle of GRE, is to create a virtual tunnel between two routers, packets are then sent through the created GRE tunnel. The diagram below shows the encapsulation procedure of GRE packet from the moment it traversers the first router and accesses the tunnel interface:

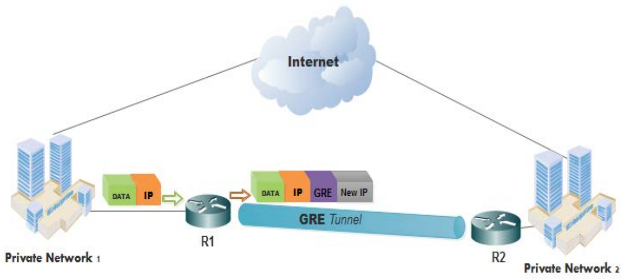

Fig. 1 Encapsulation process of GRE packet as it traversers the router and enters the tunnel interface.

In fact, GRE's support multiple protocols and packet types which makes it desirable for solving many problems faced when trying to establish VPNs across the Internet. However there is a big issue when using tunnels, in fact the private addressing used by enterprises cannot be routed across the public Internet.
GRE poposes to solve this problem by encapsulating the IP header with private addressing inside another packet that uses an other IP header that uses public addressing. When it comes to routing, as known hello messages used by IGPs to discover neighbors are sent as multicast, and the IGP adjacencies are limited to directly connected neighbors. When an IGP tries to discover neighbors, by default, it will multicast hello messages out to all of the interfaces on which it is enabled.
However in certain situations, multicast transmission or routing multicast traffic is not supported by GRE tunnels, as the same as for the public Internet or when using IPsec VPN tunnels. Additionally, even if this limitation were skirted, IGPs enable to form adjacencies only with directly connected neighbors. GRE can also be used to solve two problems; firstly, GRE supports multicast traffic by allowing transport of hello messages generated by an IGP to be transported through the GRE tunnel across the underlying infrastructure as a unicast packet.
Secondly, GRE configuration creates a logical direct connection between two sites over the underlying infrastructure. the control plane of the IGP consider two equipment to be directly connected (form an adjacency) when they are able to exchange hello messages and therefore they can form an adjacency. In addition, GRE is suitable for time sensitive and bandwidth sensitive applications [4].

4. Routing Protocols

Routing protocols are used to calculate route on a network, in function of a set of metrics in order to determine the best route or to privilege a path among others. In function of the mechanism used to calculate routes, we can distinguish many routing protocols, that belongs to different families. There are various numbers of static and dynamic routing protocols, but the selection of appropriate routing protocol for a given network architecture is the most important for routing performance.
The right choice of routing protocol depends on several parameters, related to both network specifications and application requirements [5]. Actually, the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) are considered as the pre-eminent routing protocols used for transmitting real-time traffic. The EIGRP protocol is distance-vector protocol developed by cisco and is based on Diffusing Update Algorithm (DUAL).
On the other hand, OSPF is a link-state interior gateway protocol based on Dijkstra algorithm (Shortest Path First Algorithm). EIGRP and OSPF are dynamic routing protocols used in practical networks to disseminate network topology to the adjacent routers. This work is based on the evaluation of combinations involving EIGRP and OSPF. A number of simulations have been done in order to compare different routing protocols.
The obtained results showed that EIGRP and OSPF can be qualified as "better" routing protocols comparing with others.

4.1 RIP

The Routing Information Protocol (RIP) is a distance-vector based algorithm. RIP is one of the first routing protocols used on TCP/IP. Data packets are sent through the network using UDP. Each router using this protocol has limited knowledge of the network around it.

This simple protocol uses a hop count mechanism to determine the optimal path for routing packets [6]. A maximum value of 16 hops is employed in to avoid routing loops, and thus limiting the size of the networks that uses this protocol to disseminate their data. The popularity of this protocol is principally due to its simplicity (algorithm) and it's easy configuration.
However, It has some disadvantages, for an example a slow convergence time, and a limitation of scaling up due the limitation of maximum hope number. So, this protocol performed well for small networks.

4.2 EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a routing protocol developed by Cisco based on their original IGRP protocol.
EIGRP is an IP distance routing protocol with optimization to minimize routing instability due to both topology change, bandwidth utilization, and router processor power. EIGRP uses a hybrid routing that relies on distance and link state vectors.
EIGRP uses several metrics to evaluate paths, these metrics are mainly the bandwidth, the memory as well as the overhead of the processors.
The EIGRP works quite differently from the IGRP. In fact, the EIGRP routing protocol is considered as an advanced distance vector routing protocol compared to IGRP, it belongs to also to link state protocol family due its manner of updating neighbours and treating routing information [7].
EIGRP offer a rapid convergence time, Compared to a simple distance vector protocols, in plus of many other advantages [7].

4.3 OSPF

OSPF (Open Shortest Path First) belongs to link state routing protocol family, that is used to distribute information inside of the single Autonomous System [8]. the principle of it's functioning is that each router determines first the state of its links with its one hope neighbouring routers; and then broadcasts routing information to all the routers belonging to the same zone.
This information enables to form a routing database, which must be the similar for all routers from the same zone. In fact, a stand-alone system (AS) consists of several zones, which means that all of these databases must form the topology of the whole AS.

4.4 Routing in GRE tunnel

To configure a GRE tunnel implies the creation of a tunnel interface, which is in fact a logical interface, which means that it does not really exist, at the physical level. The second step consists on configuring the tunnel endpoints for the tunnel interface.

The endpoints here signifies the source and destination of the tunnel, the source is represented by the couple {ip-address | interface-type} and the tunnel destination by : {host-name | ip-address}, this commands must be entered under the interface configuration mode while configuring the tunnel[9]. The following example illustrates the manner of creating a simple GRE tunnel between two endpoints and the necessary steps and to create and verify the GRE tunnel between two given networks. Router1's and Router2's Internal subnets(192.168.1.0/24 and 192.168.2.0/24) are communicating with each other using GRE tunnel that crosses a public network (internet) internet. Both Tunnel interfaces addresses belongs to 172.16.1.0/30 network.

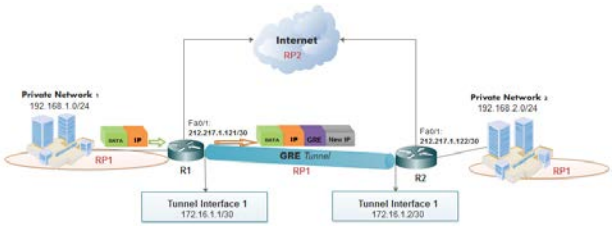

Fig. 2 The studied network topology Encapsulation.

In the ideal case, the private network and the tunnel use the same routing protocol. However, in some cases, the routing protocol used in the private network is different from that used in the public one, the latter is the one that will necessarily be used in the tunnel.
This difference gives rise to certain problems of propagation of the routing information during the passage of the private addresses to the public ones.

5. Context of Study

In order to evaluate the performance of the GRE tunnel, a contextualization was previously defined, beginning by defining a reference for the study. In this work, the reference is presented by the absence of the tunnel and by the use of the static routing.
The study was carried out by considering two major network configuration parameters, the combination of the routing protocols used for the private and public network, and the profoundness of the network. Speaking of depth, it is defined by the number of routers crossed between the two communicating ends of the network. The two main objectives defined by this work are presented by the definition of the best configuration of the network in terms of the choice of routing, and secondly, the delineation of the limits of use of the tunnels, by an evaluation of the scalability through the increase of the Number of users connected to the tunnel.

For the routing protocols used in this study context, the choice has been made for RIP, OSPF and EIGRP, since they are the most deployed protocols in actual implementations.

6. Simulation And Results

Simulation are performaned using OPNET modeler 14.5[10], the results are presented for the following configurations: Number of users (1 => 35).
Combination of routing protocols: STS: Tunnel-free static routing.

TRO: Tunnel OSPF (private) / RIP (public).
TOR: RIP tunnel (private) / OSPF (public).
TOE: EIGP Tunnel (Private) / OSPF (public).
TEO: OSPF Tunnel (Private) / EIGRP (public).

Performance metrics are presented by Delay and packet Loss rate, in terms of increasing user's number and modifying the routing schema.

6.1 Delay

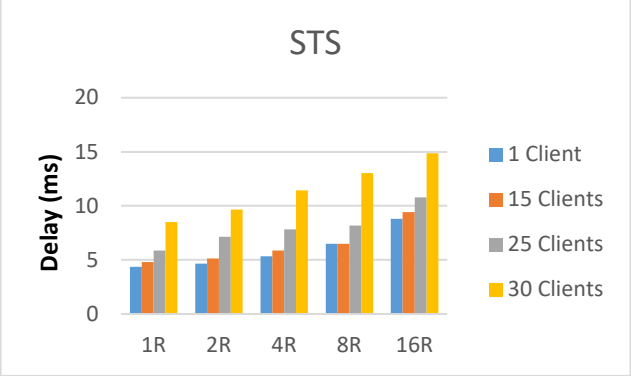

Fig. 3 Delay of videoconference for Tunnel-free and static routing.

Fig.3 shows the evolution of the delay according to the number of users for different profoundness, for a reference scenario with static routing, and no tunnel. It is clear that the delay increases with profoundness and the number of users.

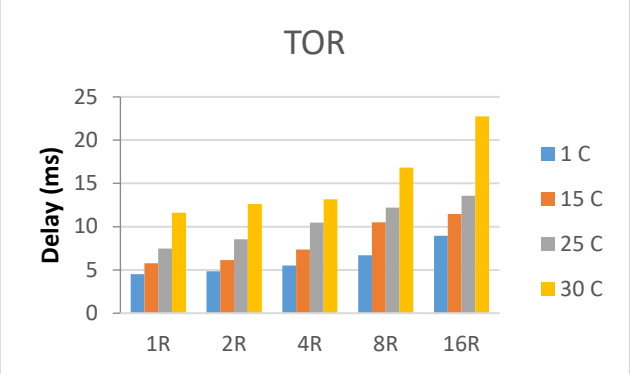

Fig.4 Delay of videoconference for Tunnel OSPF (private) / RIP (public).

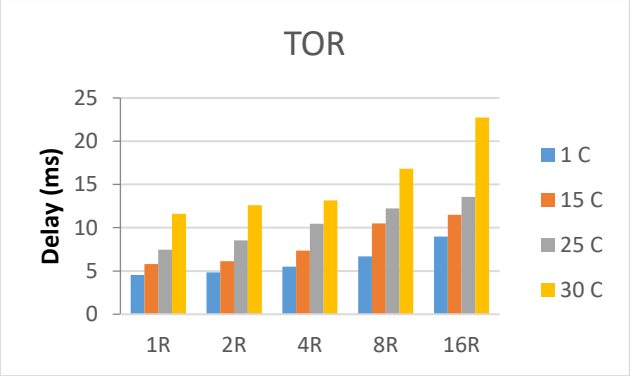

Fig.5 Delay of videoconference for Tunnel RIP (private) / OSPF (public).

In the same manner, Figure.4 and Figure.5 show that the delay of the videoconference increases with the number of router crossed by the tunnel.

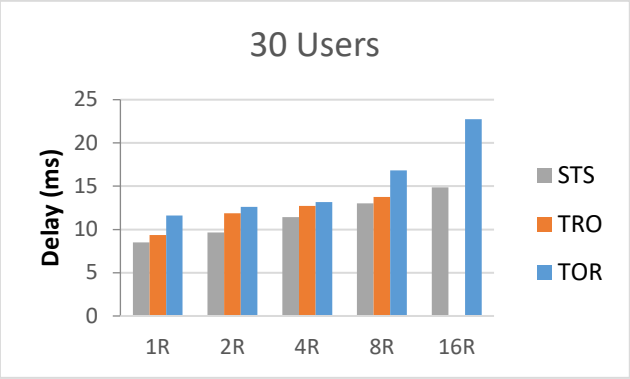

Fig.6 Delay of videoconference for 30 users.

Fig.6 demonstrates that the combination of routing protocols also affects the delay, in addition to the depth of the number of users.

Compared to the reference scenario, the TRO case (RIP (public), OSPF (private)) shows the best performance in comparison with TOR.
This increase can be explained by frequent and periodic updates of the RIP routing protocol (each 30sec) which forces the OSPF routing protocol, used in the public network, to encapsulate and decapsulation a large number of update messages of RIP. The case of the profoundness of 16 routers has not been reported, due to the limitation of the maximum number of hops of RIP routing protocol, that cannot exceed 16.

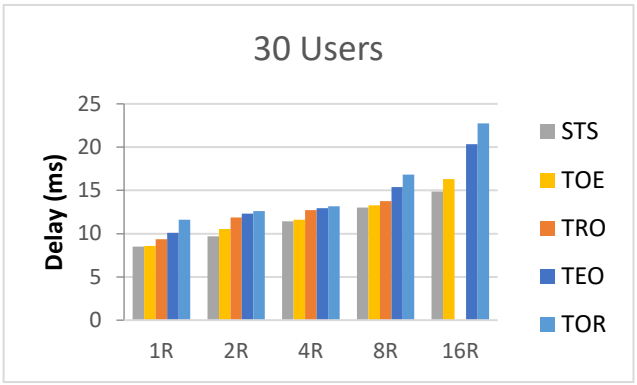

Fig 7 Delay of videoconference for 30 users.

Fig. 7 gives the results of comparison of the delay, this time including scenarios of routing combinations with EIGRP. As shown by the same figure, the delay increases in parallel for different scenarios up to a profoundness of 4 routers. For 8 and 16 routers, the TOE scenario (OSPF (public)/EIGRP (private)) manifests the best delay compared to the others. The reference scenario (STS) always gives the best results.

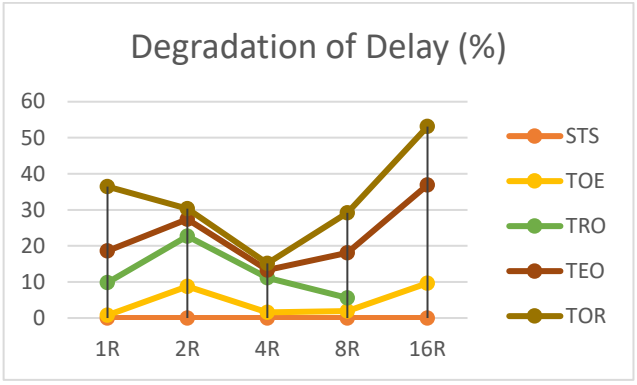

Fig.8 Degradation of delay for different scenario.

Fig.8 represents the degradation of delay for different combination of routing according to the profoundness of the network in term of the number of routers crossed by the tunnel. The calculation of the degradation was made using the STS scenario as a reference.

The remark made when examining the results is that the rate of degradation changes in parallel for all combination of routing protocols in the following order: STS, TOE, TRO, TOE, TOR. Which means that the depth obviously impacts the performance of the tunnel in terms of the delay.

6.2 Packet loss

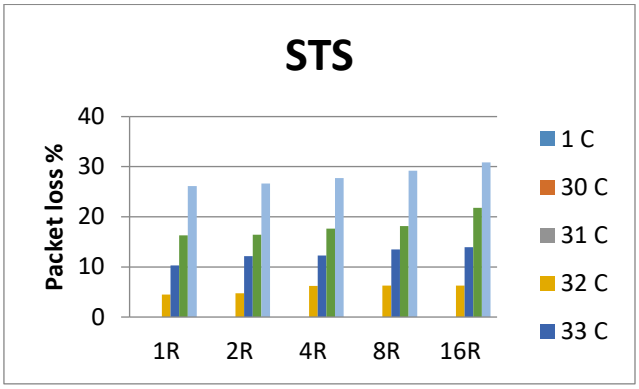

Fig.9 Packet loss of videoconference for Tunnel-free and static routing.

Figure 9 represents the evolution of packet loss rate according to the increase of the number of users and routers. As shown, this metric increases with the two parameters: users and routers. For the STS scenario, the loss rate is zero for a number of customers less than 32. The upper limit is 30%.

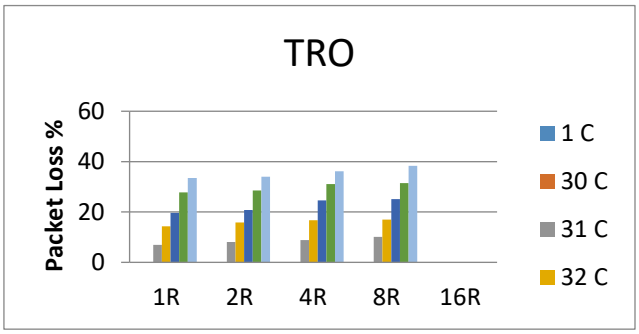

Fig.10 Packet loss of videoconference for Tunnel OSPF (private) / RIP (public).

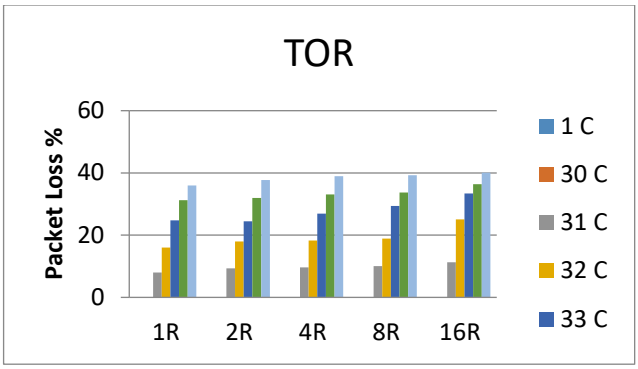

Fig.11 Packet loss of videoconference for Tunnel RIP (private) / OSPF (public).

Looking at Fig.10 and 11, the remark that can be drawn is that losses begin to appear starting from 31 users for both the TOR and TRO combinations. However, in comparison with the STS scenario, losses evolve more rapidly when increasing the profoundness of the network and number of users. The limit reached for 16 routers and 35 users is 40%.

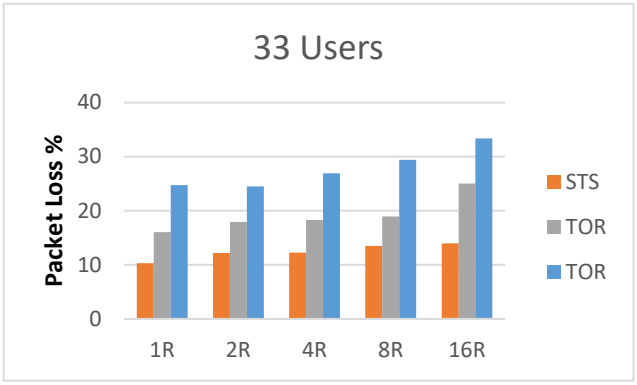

Fig.12 Packet loss of videoconference for 33 users.

Fig.12 shows clearly the notable difference in performance for the three routing combinations considered in this case, in terms of measuring the packet loss rate. The best values are obtained for STS and TRO. TOR is more sensitive to the variation of the profoundness of the network for a given number of users, in this case 33 users.

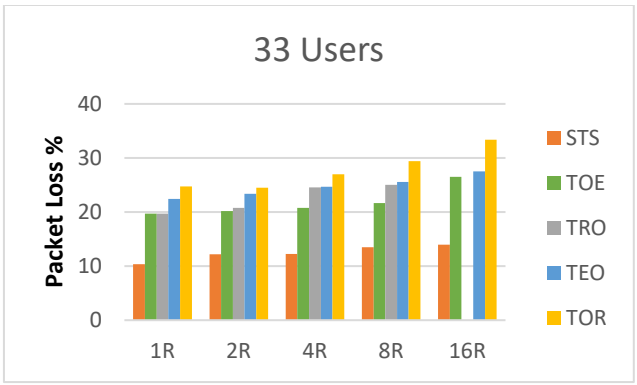

Fig.13 Packet loss of videoconference for 33 users.

The performance study was extended to examine the case of EIGRP. The latter experiment is considered by combining EIGRP with OSPF. The obtained results confirm the following classification in terms of the increase in the packet of loss rate: STS, TOE, TRO, TEO, TOR.

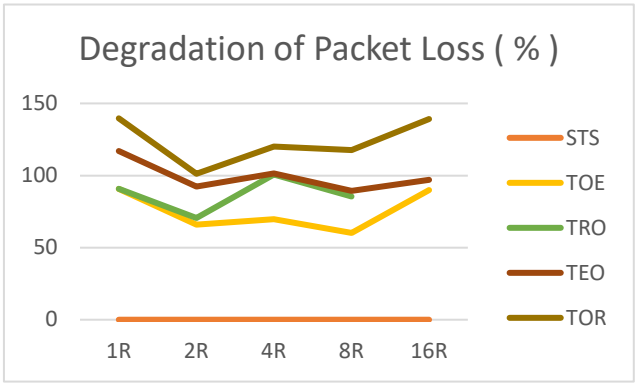

Fig.14 Degradation of Packet loss.

In the same way as for the delay, the calculation of the degradation of the loss rate was made using the STS scenario as a reference. The remark made when examining the results is that the rate of degradation changes in parallel for all combination of routing protocols in the following order: STS, TOE, TRO, TOE, TOR. Which means that the profoundness of the network obviously impacts the performance of the tunnel in terms of packet loss rate.

In fact, EIGRP has the advantage over RIP is that when a change occurs, only the changes made to the routing tables are propagated, not the entire routing table. This reduces the load that the routing protocol generates in the network itself. Without forgetting that the updates via the HELLO packets for EIGRP are carried out every 60 seconds for the links with low bandwidth, which spares the OSPF protocol of frequent encapsulations and decapsulations, as it was the case for RIP (30 sec with it propagates the routing table's tatotality).

It is for these reasons that the TOE combination gives the best performance in comparison with the others. The case of the absence of the Tunnel is always the best, which is quite normal.

7. Conclusion

This work presents a series of performance examinations of GRE tunnel in a context of real deployment, being the most commonly tunneling protocol used in reality, it was imperative to be able to determine its best configuration but also its limits with respect to a reference scenario.
The simulations have proved that the best routing scheme for this study is the one involving EIGRP as a routing protocol in the private network and the OSPF in the public one (TOE). Performance degradations were more noticeable starting from 33 users for the STS scenario and 32 for the others. These results lead to new prospects for improving the performance of this type of tunnel, especially when it comes to scaling. The next work is obviously oriented in this direction.

References

[1] I. Coonjah, P. C. Catherine, and K. M. Sunjiv Soyjaudah, "A VPN framework through multi-layer tunnels based on OpenSSH", International Conference on Computing Communication & Automation, 2015.
[2] A. Asadi, M. Eskandar, R. Syed, and M. Bahareh. Zarei, "Performance Analysis of VOIP over GRE Tunnel", I. J. Computer Network and Information Security, November.2015.
[3] X. Wang, D. Liu, H. Cao, and H. Xia, (2017), "Traffic flow redirection between border routers using routing encapsulation", 2017.
[4] S. Jahan, S. Rahman, and S. Saha, "Application Specific Tunneling Protocol Selection for Virtual Private Networks", January. 2017.
[5] D. El Idrissi, N. Elkamoun, F. Lakrami, and R. Hilal, "Performance Comparison of Protocols Combination based on EIGRP and OSPF for Real-Time Applications in Enterprise Networks", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 5, 2017.
[6] A. Iqbal, S.Liaqat, and A. Khan, "Performance Evaluation of Real Time Applications for RIP, OSPF and EIGRP for flapping links using OPNET Modeler". International Journal of Computer Networks and Communications Security, January. 2017.
[7] E. Stankoska, N. Rendevski, and P. Mitrevski, "Simulation Based Comparative Performance Analysis of OSPF and EIGRP protocols". International Conference on Applied Internet and Information Technologies, 2016.
[8] N. Absar, A. Wahab, and K. U. Sikder, "Performance Measurement of Open Shortest Path First (OSPF) Protocol in IP Networks", International Journal of Engineering Research, February.2017.
[9] S. Punithavathani, and S. Radley, "Performance Analysis for Wireless Networks: An Analytical Approach by Multifarious Sym Teredo",The Scientific World Journal, November.2014
[10] S. Adarshpal, S. Vasil, Y. Hnatyshin, "The Practical OPNET User Guide for Computer Network Simulation".

Dounia EL IDRISSI received the Master degrees, Network and telecommunication, from Faculty of sciences El Jadida in 2014. Actually a Ph.D Student on STIC Laboratory on Faculty Of sciences El Jadida, Network and Telecommunications team. Her research interest are: Routing Protocols, Tunnel , QoS of networks and networks and telecommunications.

Najib ELKAMOUN Ph.D, professor higher education degree at Faculty of sciences El Jadida.in the dept. of physics. Researcher member on STIC laboratory, header of Network and Telecommunications team. His research interest includes, NGN, MPLS, Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Rachid Hilal Ph.D, professor higher education degree at Chouaib Doukkali University. Actually a vice president of the Chouaib Doukkali University. Researcher member on STIC laboratory. His research interest includes, Hyperfrequency, amplifiers Antennas, Wireless Communications, networks and telecommunications.