Deployment of a Backbone operator and BGP traffic Engineering

Yannick Malong[1,2], Ebenezer Maka Maka[1,2], Samuel EKE[2], Basile Emmanuel Assiga Ateba[2], Daria Tonye[2]
[1]Department of Computer Engineering and Telecommunications, National Higher Polytechnic School of Douala, University of Doula,
[2]Laboratory of Energy, Materials, Modeling and Method

Abstract— This paper study the most appropriate way for an Internet access service provider (FAI) to guarantee each of its customers continuous access to the Internet in any circumstances without having to modify, to redo the Network configurations. The goal of all operator is being able to make profit while winning in notoriety, it should enforce to satisfy its customer base. As a result, the choice of protocols to be implemented is of capital importance. Throughout our study, we have interested in static routing and the Dynamic Ringation Protocol Bagging Gateway Protocol (BGP) in setting up an operator network connected to several Internet Service Provider (ISP). Thus, using the Enterprise Network Simulation Platform (eNSP) and ne work scan Wireshark. We have at first, put in place a network heart Operator connected to nodes of outflows to the internet then, study the behavior of the exchanges between our network heart and the different nodes output to the Internet before and after link removal using the Internet Control Message Protocol (ICMP). In a second time we analyzed the flux data generated before and after deleting each link. For this purpose, it stems that unlike a static routing that requires manual intervention in a tilting process, the dynamic routing protocol (BGP) has many assets, including its ability to adapt to any changes in the network topology (addition or deletion of one or more equipment(s)), the possibility of manipulating routes of incoming and outgoing traffic from the network through attributes he has. It offers greater control routes in our network with less latitude time than when using a manual process in case of failover.

Index Terms— BGP, continuity, Dynamic routing, eNSP, ISP, static routing, tilting
,

1 Introduction

Today, operators communication systems must face many requirements to meet their clients. The dependence of the companies at the Internet because of the many services that are exploited make it the most important. Also, the interruption of this such short access is, may paralyze the activities of its operators. Making the choice of routing protocols to implement very determining in the process of deploying a network ISP; which one must be capable to guarantee the continuity of services to its customers by optimizing the use of resources in the network. The Internet is composed of separate routers, named autonomy ous system (AS) [1]. These AS are connected to each other in the world and it is this set that forms the Internet network through which the different users can communicate.

To send information in networks, two possibilities are offered to us: we can also use a routing static protocol and a dynamic routing protocol. Also, what type of routing would be the most suitable in a tilting process Internship?

Throughout our work, we will put in place an operating network consisting of two main parts: a first part representing the operator private operator (AS 65001) and a second part illustrating the public network. The private network is that part of the backbone (network heart operator) and different covers that are grafted; the public part of it is consisting of the different nodes out of the output to the Internet. In our tests, we will simulatefour main points (ISP) representing each of the different AS. So, we will come out with the advantages of static routing and its limits. Then we will look at the RSVP-TE signaling protocol associated with MPLS for routing inside the backbone operator. The Gateway Protocol Border (BGP) as to it will be used in an environment of multihoming to different networks of transitions or ISP. Subsequently, we will study the behavior of incoming / outgoing traffic of our backbone before and after removal of the links between AS. Finally, we will be able to make a small interpretation of them.

2 Static Routing

A routing protocol is this mechanism that transferring IP packets through different networks according to a routing algorithm. The use of railway static areas has many benefits among which [2] [3]**:**

- The Conservation of the Routing Resources: No Central Processing Unit (CPU) is used, only to perform calculations or analyze the network for the router update;
- A The Security: Allows us to ensure communication between the different nodes of the network (controlled road used) and the availability of the bandwidth for important applications because, we have a precise map of routes in the reswater. Guests will have specific routes for each communication. The use of static routes remains a solution allowing the operator to restore access to the Internet for its customers by modifying oneself the routes.

Nevertheless, it requires delicacy, excellent knowledge of the network because, poor manipulation can cause huge damage in this way as well:

- The Maintenance is difficult: The process of adding static routes in a routing table is manual. In addition, when an error occurs in the network or the topology changes, static routes can not change automatically and must always be modified manually;
- It does not offer us optimal control opportunities for

routes in the network during the movement of the prefixes (definition of new routes), it flows a great period during which customers will not be able to access the different Internet services

3 Resource Reservation Protocol: RSVP

The RSVP protocol is this user-oriented resource booking protocol Datagram Protocol (UDP). It is used in the establishment Entity of a specific path with bandwidth constraints. In order to transmit the labels at the same time, an extension has been assigned to take care of traffic engineering: we are talking about RSVP-TE. Although this protocol offers a best control of the network thanks to pre-established routes, it is on the other hand very gourmand in resource and is done abandoned for the implicit routing protocol Label distribution protocol LDP (Label Distribution Protocol). However, for small networks, the RSVP-remains the best choice possible.

4 BGP et Routage inter-AS

The Gateway Protocol Border (BGP) is an Internet traffic protocol on the Internet used by operators and ISPs. It is used for the exchange of routes between separate networks on which administrative control is available. Also, it allows the exchange of routing information, network accessibility (called prefixes) between Autonomous Systems(AS). It is designed for the support of large volumes of data and has extensive opportunities for choice of the best road. Still called path protocol (path Vector protocol), the BGP bases routing decisions on trails, the attribution of prefixes and a set of selection rules defined by the AS Director. A AS can work well using the default static routes provided by the operator, it is not necessary for him to receive a full-routing. Thus, the transition network (ISP) will be re-announced the routes learned from this AS to the rest of the Internet and the definition of routes for the traffic of the latter [4]. Nevertheless, in the measure or we want to perform an automatical tilting or a balance of charge, BGP remains the best choice. In multi-homing with the use of the BGP, a better control of traffic charge balancing and redundancy becomes possible [5].

5 Requirements of production

Our realization does not at any time have interest at the service operated in the Backbone. We will focus mainly on interconnection (communication) of the different ends of our network and the behavior of the borrowed routes. Our setting in place answer to the following requirements:

- Explicit routing: The heart of our network will take charge of the Protocol of RSVP-TE signaling and the CSPF algorithm. Using the latter, we have defined routes (tunnels) responding to a bandwidth constraint. As a result, the reservation of resources from one end of the network to another is made via a bandwidth control available. The borrowed routes will be those with the necessary resources for the support of the traffic. The control route follows an order of priority predefined;
- Integration of IPv6: It will be a larger Internet access. It is indeed a solution for bearing a possible exhaustion of IPv4 addresses. Because, unlike the IPv4 which is coded on 32 bits, the IPv6 is encoded on 128 bits so can manage some greater number users;
- The choice of the best way: according to the constraints fixed for each customer (VPN), shorter path to the gateways (IGWs) before moving in the public part of the network. Indeed, to optimize the traffic of the Backbone to the IGWs, the resources reservations will follow a priority predifined order;
- Dynamic routing: our architecture must be able to adapt to any system changes in the minimum time without intervention of a network administrator. To be done, it supports the dynamic routing at the level of IGWS to ensure a rapid tipping of an ISP to another in case of necessity.

6 Scenario in the private part of the network

As for the operation and effectiveness of our backbone or dorsal epine, we will implement the MPLS which reveals many advantages in TE compared to the traditional routing [6] and the IS-IS link protocol that is prove to be the most adequate because, it is both faster and more reliable than OSPF for network security [7]. We are particularly using ISIS-TE to be able to take charge of traffic engineering and CSPF algorithm for the support of the bandwidth. A minimal bandwidth will be required for each traffic according to the different customers (in our case, we took a bandwidth inter-provision of 100mbit). The bandwidth necessary for the traffic of our client is 20Mbit.

The different traffic will follow the routes as defined on the diagram below: The Green routes will always be a priority, in case of unavailability of the latter caused by a deficiency of resources or by a bread of the link, the traffic is automatically tilted to the secondary itinerary represented in orange.

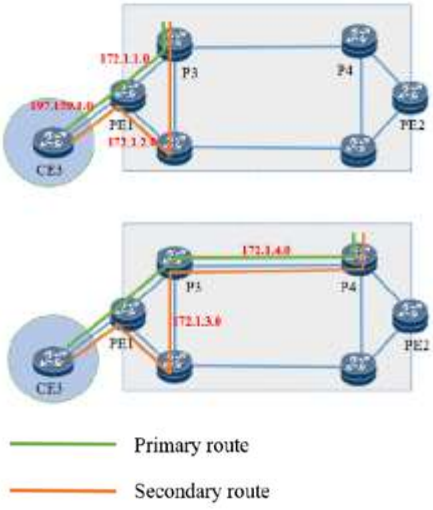


Fig. 1 Operator private network

7 Scenario in the public part of the network

Out of our Backbone, especially to connect the different CEs and IGWs, we use the OSPF (ISPFv2, OSPFv3) link protocol (OSPFv3). OSPFv3 will allow us to support the IPv6. The role of the routing protocol between EC and PE will be the exchange of existing roads in different customers. In this case, the choice of the protocol imports may. One can also choose a remote protocol to such as RIP, RIPV2 or even static routing.

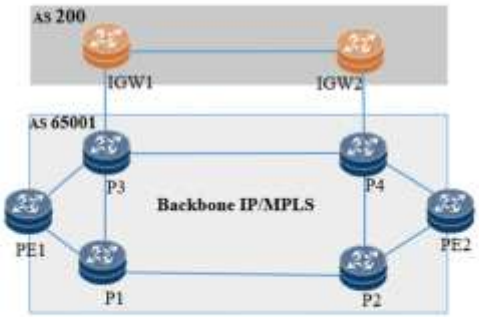


Fig. 2 Operator network

In the scenario represented by the figures below below ouroperator network has two gateways (IGW1, IGW2). These two gateways are connected to four nodes output to the Internet (ISPs) by what, the packages of the different customers will transit for achieving DRE the Internet and vice versa. The definitions different routes fingerprints by customer's traffic are configured using the BGP attributes.

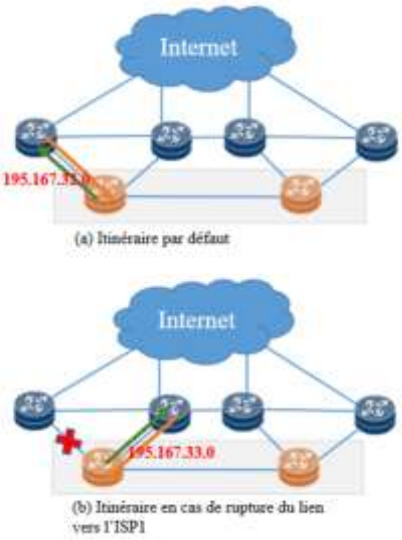
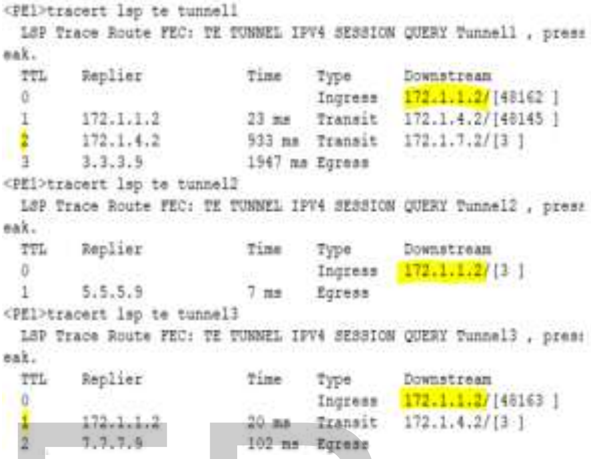

Internet
195.167.33.0
(a) Itinéraire par défaut
Internet
195.167.33.0
(b) Itinéraire en cas de rupture du lien vers l'ISP1

Fig. 3 External operator traffic

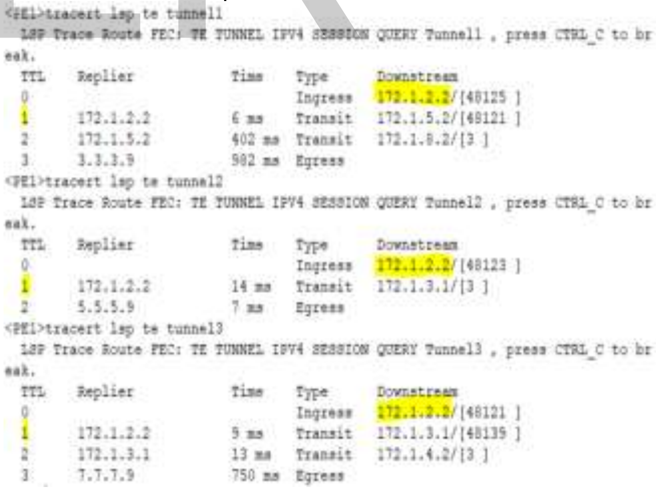
Firstly, the packages from a post (client) connected to our operator networkwill contact the Internet using the right route that is defined as default with a local preference value above that of all others. In our scenario the default route is that passed through the ISP1. To this efFet, the incoming traffic as the outgoing of the network operator will always go through the node ISP1 (this as long as it will be operational). In a second time we proceed to a break in the link to the ISP1, footprint traffic for this purpose the second routes that is the one to the ISP2. We are interested in particular to attributes preferably local and AS-Path to be able to manage the outgoing traffic and in the operator network respectively. Tests are also performed using the poste (Customer) that is grafted to our operator network.



```
<PE1>tracert lsp te tunnel1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.1.2/[48162 ]
  1      172.1.1.2          23 ms   Transit   172.1.4.2/[48145 ]
  2      172.1.4.2          933 ms  Transit   172.1.7.2/[3 ]
  3      3.3.3.9            1947 ms Egress
<PE1>tracert lsp te tunnel2
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel2 , press
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.1.2/[3 ]
  1      5.5.5.9            7 ms    Egress
<PE1>tracert lsp te tunnel3
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel3 , press
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.1.2/[48163 ]
  1      172.1.1.2          20 ms   Transit   172.1.4.2/[3 ]
  2      7.7.7.9            102 ms  Egress
```

Fig. 4 PE1 routing table before deleting the link to P3

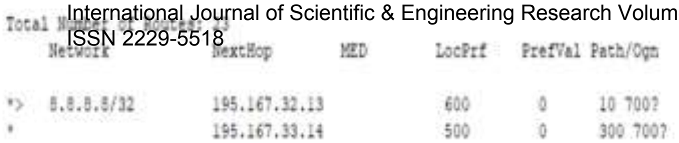
The routes that interest us here are those generated by the tunnels 2 and 3 correspond to traffic internet.



```
<PE1>tracert lsp te tunnel1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press CTRL_C to br
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.2.2/[48125 ]
  1      172.1.2.2          6 ms    Transit   172.1.5.2/[48121 ]
  2      172.1.5.2          402 ms  Transit   172.1.8.2/[3 ]
  3      3.3.3.9            982 ms  Egress
<PE1>tracert lsp te tunnel2
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel2 , press CTRL_C to br
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.2.2/[48123 ]
  1      172.1.2.2          14 ms   Transit   172.1.3.1/[3 ]
  2      5.5.5.9            7 ms    Egress
<PE1>tracert lsp te tunnel3
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel3 , press CTRL_C to br
eak.
  TTL    Replier            Time    Type      Downstream
  0                                 Ingress   172.1.2.2/[48121 ]
  1      172.1.2.2          5 ms    Transit   172.1.3.1/[48135 ]
  2      172.1.3.1          13 ms   Transit   172.1.4.2/[3 ]
  3      7.7.7.9            750 ms  Egress
```

Fig. 5 PE1 routing table after removal of the link to P3

Figure 4 is an extract of the different tunnels a PE1. Figure 5 is a capture of the same tunnels at PE1 after deleting node P3.



```
Total Number of Routes: 13
    Network            NextHop        MED       LocPrf    PrefVal Path/Ogn

*>  8.8.8.8/32         195.167.32.13             600        0      10 700?
*                      195.167.33.14             500        0      300 700?
```

Fig. 3 Routes BGP towards Internet

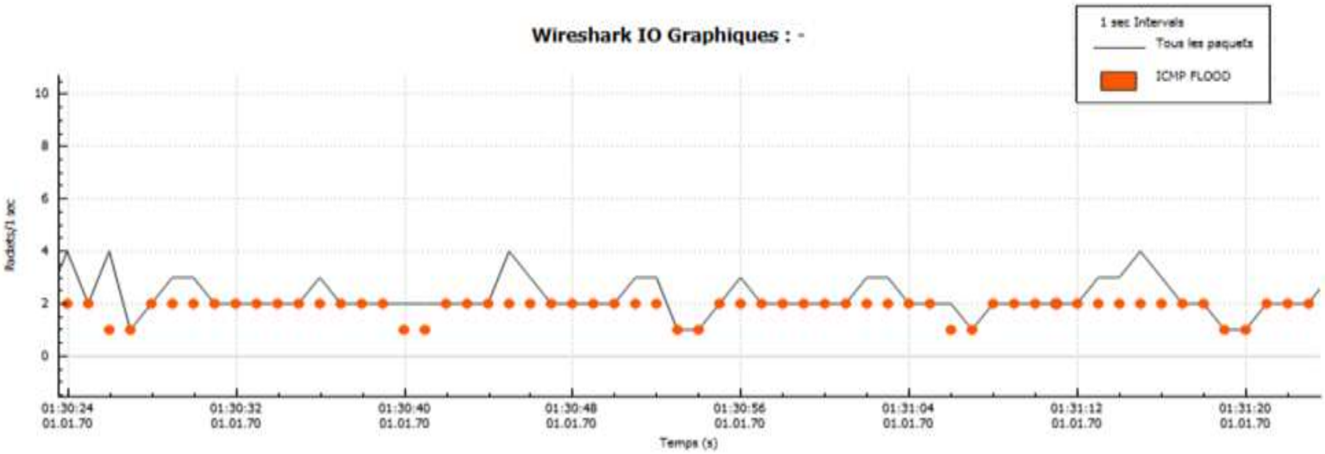
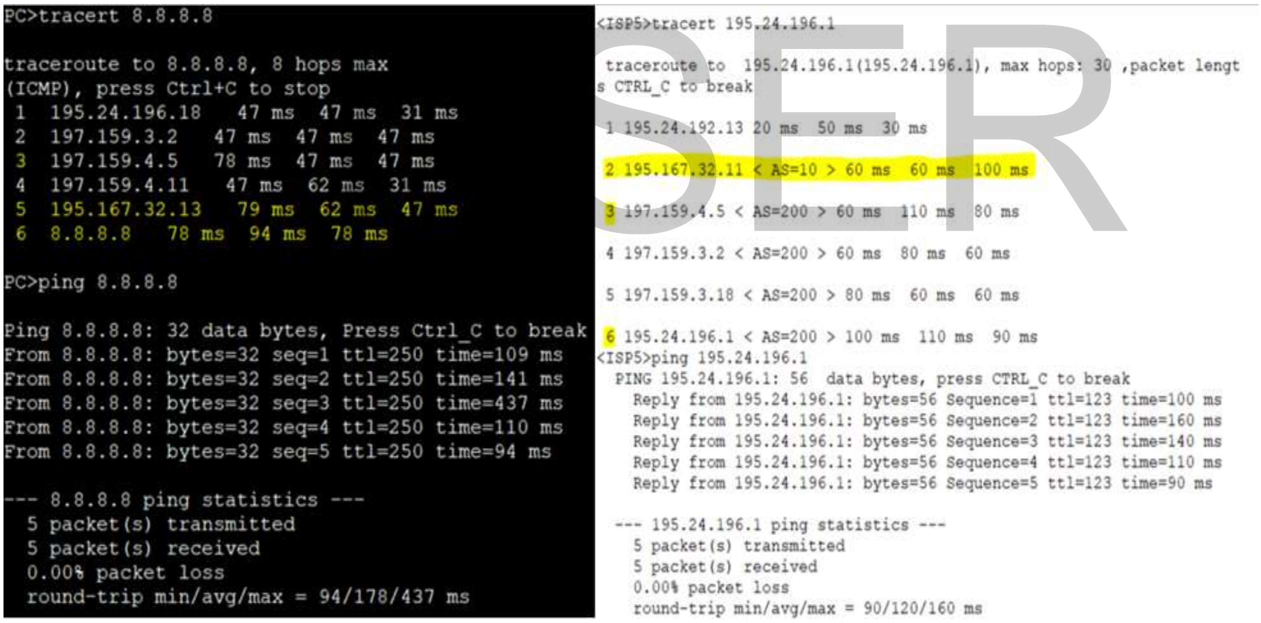


Fig. 4 ICMP stream generated by the PE1 and Internet exchanges

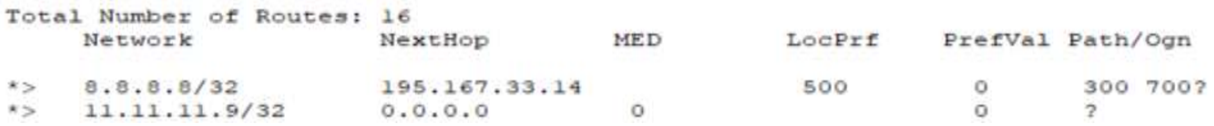
The Figure 6 is an extract of the BGP routing table executed at the IGW1, Figure 7 is a capture of the ICMP stream of the post-traffic to the BGP realised by the help of the capture tool Wireshark.



```
PC>tracert 8.8.8.8

traceroute to 8.8.8.8, 8 hops max
(ICMP), press Ctrl+C to stop
 1  195.24.196.18   47 ms  47 ms  31 ms
 2  197.159.3.2    47 ms  47 ms  47 ms
 3  197.159.4.5    78 ms  47 ms  47 ms
 4  197.159.4.11    47 ms  62 ms  31 ms
 5  195.167.32.13    79 ms  62 ms  47 ms
 6  8.8.8.8    78 ms  94 ms  78 ms

PC>ping 8.8.8.8

Ping 8.8.8.8: 32 data bytes, Press Ctrl_C to break
From 8.8.8.8: bytes=32 seq=1 ttl=250 time=109 ms
From 8.8.8.8: bytes=32 seq=2 ttl=250 time=141 ms
From 8.8.8.8: bytes=32 seq=3 ttl=250 time=437 ms
From 8.8.8.8: bytes=32 seq=4 ttl=250 time=110 ms
From 8.8.8.8: bytes=32 seq=5 ttl=250 time=94 ms

--- 8.8.8.8 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 94/178/437 ms
```

```
<ISP5>tracert 195.24.196.1

 traceroute to  195.24.196.1(195.24.196.1), max hops: 30 ,packet lengt
s CTRL_C to break

 1 195.24.192.13 20 ms  50 ms  30 ms

 2 195.167.32.11 < AS=10 > 60 ms  60 ms  100 ms

 3 197.159.4.5 < AS=200 > 60 ms  110 ms  80 ms

 4 197.159.3.2 < AS=200 > 60 ms  80 ms  60 ms

 5 197.159.3.18 < AS=200 > 80 ms  60 ms  60 ms

 6 195.24.196.1 < AS=200 > 100 ms  110 ms  90 ms
<ISP5>ping 195.24.196.1
  PING 195.24.196.1: 56  data bytes, press CTRL_C to break
    Reply from 195.24.196.1: bytes=56 Sequence=1 ttl=123 time=100 ms
    Reply from 195.24.196.1: bytes=56 Sequence=2 ttl=123 time=160 ms
    Reply from 195.24.196.1: bytes=56 Sequence=3 ttl=123 time=140 ms
    Reply from 195.24.196.1: bytes=56 Sequence=4 ttl=123 time=110 ms
    Reply from 195.24.196.1: bytes=56 Sequence=5 ttl=123 time=90 ms

  --- 195.24.196.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 90/120/160 ms
```

Fig. 8 Tests Routes on the PC and the Internet



```
Total Number of Routes: 16
      Network            NextHop          MED         LocPrf     PrefVal  Path/Ogn

*>    8.8.8.8/32         195.167.33.14                500          0       300 700?
*>    11.11.11.9/32      0.0.0.0           0                       0       ?
```

Fig. 9 BGP routes to the Internet after removal of the link to the ISP1

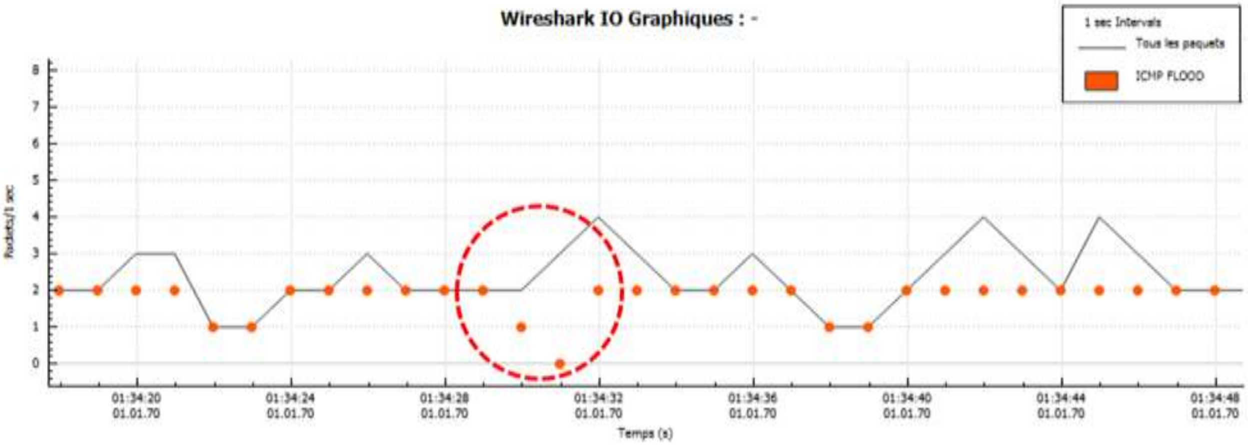
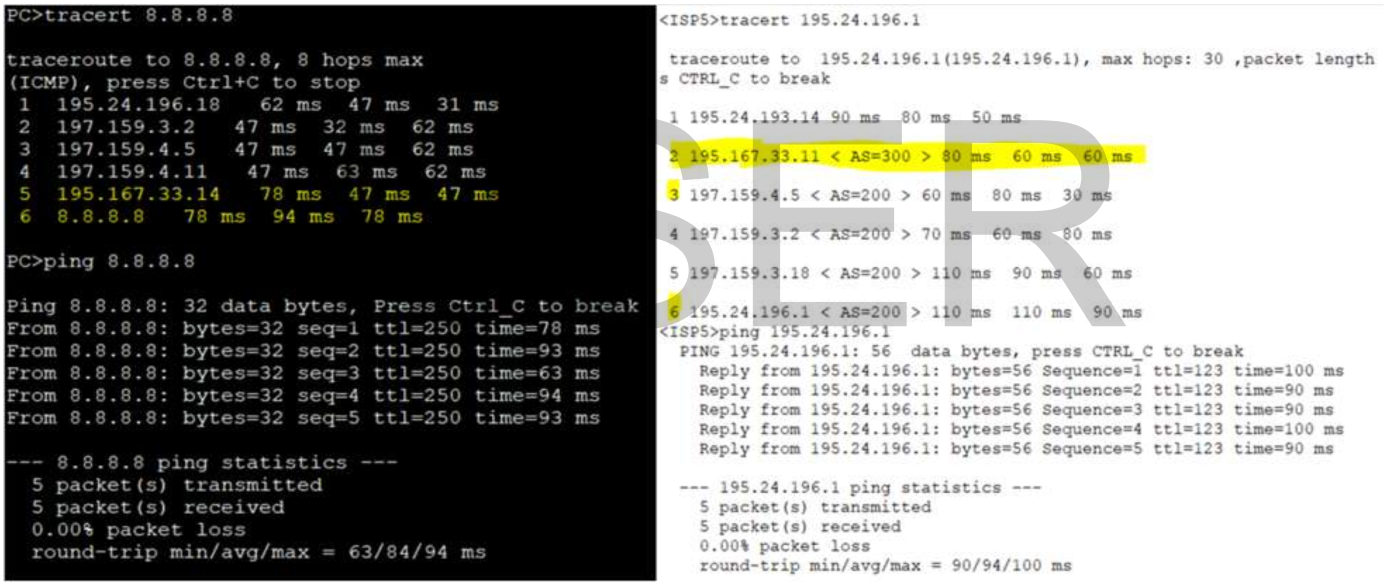


Fig. 10 ICMP flow generated by PE1 and Internet exchanges after breaking the link to ISP1



```
PC>tracert 8.8.8.8

traceroute to 8.8.8.8, 8 hops max
(ICMP), press Ctrl+C to stop
 1  195.24.196.18   62 ms  47 ms  31 ms
 2  197.159.3.2   47 ms  32 ms  62 ms
 3  197.159.4.5   47 ms  47 ms  62 ms
 4  197.159.4.11   47 ms  63 ms  62 ms
 5  195.167.33.14   78 ms  47 ms  47 ms
 6  8.8.8.8   78 ms  94 ms  78 ms

PC>ping 8.8.8.8

Ping 8.8.8.8: 32 data bytes, Press Ctrl_C to break
From 8.8.8.8: bytes=32 seq=1 ttl=250 time=78 ms
From 8.8.8.8: bytes=32 seq=2 ttl=250 time=93 ms
From 8.8.8.8: bytes=32 seq=3 ttl=250 time=63 ms
From 8.8.8.8: bytes=32 seq=4 ttl=250 time=94 ms
From 8.8.8.8: bytes=32 seq=5 ttl=250 time=93 ms

--- 8.8.8.8 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 63/84/94 ms
```

```
<ISP5>tracert 195.24.196.1

 traceroute to  195.24.196.1(195.24.196.1), max hops: 30 ,packet length
s CTRL_C to break

 1 195.24.193.14 90 ms  80 ms  50 ms

 2 195.167.33.11 < AS=300 > 80 ms  60 ms  60 ms

 3 197.159.4.5 < AS=200 > 60 ms  80 ms  30 ms

 4 197.159.3.2 < AS=200 > 70 ms  60 ms  80 ms

 5 197.159.3.18 < AS=200 > 110 ms  90 ms  60 ms

 6 195.24.196.1 < AS=200 > 110 ms  110 ms  90 ms
<ISP5>ping 195.24.196.1
  PING 195.24.196.1: 56  data bytes, press CTRL_C to break
    Reply from 195.24.196.1: bytes=56 Sequence=1 ttl=123 time=100 ms
    Reply from 195.24.196.1: bytes=56 Sequence=2 ttl=123 time=90 ms
    Reply from 195.24.196.1: bytes=56 Sequence=3 ttl=123 time=90 ms
    Reply from 195.24.196.1: bytes=56 Sequence=4 ttl=123 time=100 ms
    Reply from 195.24.196.1: bytes=56 Sequence=5 ttl=123 time=90 ms

  --- 195.24.196.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 90/94/100 ms
```

Fig. 11 Tests Routes on the PC and the Internet

The Figure 9 is an extract from the routing table ICMP Flow Features to the BGP Internet Based to the IGW1 after delete Directed using the capture of tool Wireshark Link to ISP1, Figure 10 is a capture of the moment of the breaking link to the ISP1.

8 Interpretations of results

The Figure 4 and Figure 5 show us Respectively the routes taken by the existing tunnels in PE1. We can notice that inFigure 1, all traffic passes through the PE1-P3 (172.1.1.0). Following the deletion of the PE1-P3 link, the traffic will now be routed to the PE1-P5 link (172.1.2.0). Note that the reservation of resources follows this priority (PE1-P3, PE1-P5-P3) therefore, insufficient resourcesnecessary for the evacuation of data can also be at the root of this failover.

In the IGW1 routing table obtainede in Figure 6 before deleting the node ISP1, we can notice that two-trained trails are available (195.167.32.13 And 195.167.33.14). The first with for destination the ISP1 and the other going to the ISP2. In our case, the link to ISP1 is a priority because it has a local preference value above that to the ISP2. Traffic uses the link to the default ISP1 for Vacuum are traffic.

In Figure 7, it can be clearly noted that the ICMP stream generated by exchanges between our post and the Internet is periodic.

In Figure 9, we can notice that a route to the Internet has only been available. This is a justifia by the fact that the link is not removed to the ISP1 given by the address 195.167.32.13 For this purpose, traffic switches to ISP2 195.167.33.14. Figure 10 as to it, contrary to Figure 7, presents a sudden drop in the ICMP stream (zone areaCurly red), this flow is subsequently reestablishing after a few seconds. Following the breakage of the link to ISP1, the traffic will be interrupted the tipping time to the ISP2 (time relatively short of 3s). We note that the BGP has the capecity to adapt this in seconds (case of our simulation) to changes in the network is the deletion of the link to the ISP1. Also, using these different attributes, it can easily control the incoming and outgoing traffic of our reservesTo the development, facilitating the maintenance and management of the latter.

9 Conclusion

In order to ensure continuous access to the Internet, the operator must be able to provide the possible failure of a material or software component. To get to it, it would be necessary to be available to the customer a multitude of itineraries to different Internet output points. Thanks to this multitude of itineraries, customers will always have an evacuation solution of their traffic to the Internet and vice versa. In effect, it is possible for a multi-homed operator with forwarding agent to achieve a tilting by having only static routes uses. It can simply use the default static routes provided by its transparencies (ISPs). Nevertheless, unlike a dynamic routing that can adapt to all system changes, static routes refer to routes that are manually added to the routing table. An error in the network can delay the bottom of the binding and thus interrupt the services for a longer or less long time. Although they are simple to configure, static routes require permanent control of administrators. Everything is done manually and in repeated ways. To this end, the use of the dynamic routing protocol is properly the best choice for the handling of inter-AS roads and the guarantee of continuity to the Internet because it may adapt to any changes of the topology of the network offering greater control of routes borrowed from incoming and outgoing traffic in the network.

References

[1] Cisco (2016) Load Sharing with BGP in Single and Multihomed Env ronments, Document ID 13762. Cisco Systems, Inc. All Rights Reserved. Updated 22 June 2016

[2] Protocoles de routage-RIP, OSPF, BGP, Toutain, Laurent and Isabelle Chrisment, LORIA and McKeown, Nick

[3] Ashutosh Sharma, Rajiv kumar, Realistic Comparison of Performance Parameters of Static and Dynamic Unicast Routing over Mesh Topology, International Journal of Scientific & Engineering Research, Volume 6, Issue 12, December-2015

[4] Sarah Nataf, BGP et l'interconnexion des réseaux. Technical report, Institut Mines Telecom, 2014

[5] Ahmed, Muhammed Zaharadeen and AbdallahHashim, Aisha Hassan and Khalifa, OthmanOmran and Salami, Momoh. J. E. Border Gateway Protocol to provide failover in multihoming environment, International Journal of Information Technology. article,9, p 33–39, 2017

[6] Akshay, Pooja Ahlawat, Comparison between Traditional IPNetworks/Routing and MPLS, International Journal of Scientific Engineering and Research (IJSER), Volume 3 Issue 3, March 2015

[7] AfNOG, Introduction to IS-IS. Technical report, AfNOG Dakar, 2018

[8] IETF. Rfc 5305- IS-IS Extensions for Traffic Engineering, October, 2008

[9] Josselin VALLET, Optimisation dynamique des réseaux IP/MPLS. PhD thesis, Institut National des Sciences Appliquées de Toulouse (INSA de Toulouse), 2015

[10] J. W. Steward," BGP4 inter-Domain Routing in the Internet", Addison-Wesley, 1999

[11] Philip Smith, BGP for Internet Service Providers, January, 2003

[12] IETF. Rfc 4271, A Border Gateway Protocol 4 (BGP-4), January, 2006, p. 23

[13] Ludwig, Christian, Traffic engineering with BGP, Seminar Internet Routing; Technical University Berlin: Berlin, Germany, p.1–10, 2009

[14] APNIC-eLearning. Technical report, BGP Attributes, 2017

[15] Reabellejoyce, reabelle JOYCE INTES BLOG, THE ARCHITECTURE OF THE INTERNET, https://reabellemyblog.wordpress.com/2016/01/05/the-architecture-of-theinternet- 2/, The Network Architecture Networks must support a wide range of applications and services, as well as operate over many different types of physical infrastructures. The term network architecture, in, urldate = 2020-10-15, jan, 2016

[16] MICHEAL, qu'est ce que VRF: Virtual Routing and Forwarding, 2012,

[17] IEEE. Nykvist, Johan and Carr-Motykova, Lenka, Simulating convergence properties of BGP. Proceedings. Eleventh International Conference on Computer Communications and Networks, p124–129, 2002

[18] IETF. Rfc 6445- Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute, November, 2011

[19] IETF. Rfc 5712- MPLS Traffic Engineering Soft Preemption, January, 2010, p. 5

[20] IETF. Rfc 5305- IS-IS Extensions for Traffic Engineering, October, 2008

[21] NE40E Product Documentation. Technical Support, Huawei Technologies

[22] Guide de configuration-MPLS, Huawei. Technical Support, support.huawei.com

[23] Guillon Samuel. Robin David, Ressource ReSerVation Protocol-Traffic Engineering, 2005,