International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Routing Strategy Based on Separation of Lines and Relay System in Case of Interruption of an Internet Signal

[1]BUKASA MUKENGESHAYI Jean Claude

[1]Teaching Assistant, Department of Computer Science, University of Kananga, DR Congo Email:[1]bukmjc@gmail.com

ABSTRACT

The internet connection is of interest to everyone and has become a computer means to be implemented to facilitate communication in the various sectors. The use of said connection in the company poses certain difficulties such as: the disturbance of the signal which can be due to natural or artificial disasters (torrential rain, strong wind, short circuit etc.) and this prevents the system to produce good results in a short time, from where we will make integration of several Internet access providers in a single autonomous system with a routing strategy based on the separation of lines and relays in the event of a cut or interruption of one of the Internet service providers.

Key Words –multiple ISPs in a single stand-alone, multi-homing, split-line routing system.

1. Introduction

1.1 Problematic

As part of this study, the objective is to provide a sustainable solution and remedy this difficulty, the use of various Internet access providers without coming too many financial means to buy a router for each provider. We therefore propose the establishment of a routing strategy based on the separation of lines, and the relay system in the event of interruption of the signal of one the Internet service Providers and while sharing the load and creating a fallback link for important traffic, if the primary link carrying the major application traffic fails.

Hence the questions like: why integrate several Internet access providers into a single autonomous system? Does this solution guarantee the availability of the Internet? These are the essential questions that we will try to answer in this reflection, which focuses less on the content than on the spirit of the routing strategy based on the separation of the lines and as well as the relay system in the event of an interruption of the internet signal.

Subscriber traffic flow control on service provider networks through traffic management policies and rules based on subscriber profiles. The goal is to interconnect an autonomous system with two different Internet access providers to give endurance to the network, and guarantee the high availability of the Internet in the event of failure of one of the Internet service providers, the other takes over.

Here are the criteria based on the choice of an access provider: quality of service, service offered, availability. It must guarantee an SLA for carrying a certain type of traffic by providing it with proper prioritization and routing, as well as the necessary bandwith for an optimal user experience.

1.2 Benefits of this system [1]

The exchanges of companies with their customers, suppliers and collaborators are now carried out in an integrated way thanks to the Internet and network operation. The advantage of this solution lies in the speed of exchanges and the availability of data. And has the following advantages:

- ➢ The high availability of data, that is to say: if I have a problem with one of the Internet service providers, I can switch to the second;
- ➢ Continuous communication between Internet users which allows us to stay in touch with our friends and contacts;

And for this solution we have opted for the implementation of the BGP Protocol.

2.BGP Protocol (Border Gateway Protocol)[2]

BGP is mainly used between operators and internet service providers for the exchange of routes. Most internet end users only have one connection to an internet service provider. In this case, BGP is useful because a default route is satisfactory. However, a company that is redundantly connected to several Internet service providers (multi-homing) could obtain its own autonomous system number and establish BGP sessions with each of the providers. In addition to the Internet, private IP networks can use BGP, for example to interconnect local networks using OSPF.

BGP is the routing protocol designed to exchange routing information between autonomous systems. For BGP, the different networks are organized into an Autonomous System (SA), linked by one or more links.

Within an SA, the routing is calculated with one of the protocols (RIP or OSPF). While the BGP Protocol intervenes when the route must borrow several SA. In an Autonomous System, there are one or more Edge Routers that communicate with the Edge Router(s) of neighboring SAs.

BGP therefore only takes into account SAs where transit is authorized (internet backbone networks, for example, or operator networks, subject to financial agreements). The border routers of these SAs are called BGP routers.

They calculate routes with a distance vector algorithm. Unlike RIP, they memorize the entire path and not just the first router in the path. They therefore exchange complete information, which is possible because the BGP graph is small.

A BGP router is a machine with complete communication architecture, because routing between SAs is considered an application requiring high communication reliability.

Note that there are three ways to implement theBGP [3]:

- Default route;
- Partial update;
- And full updates

a. Default route [4]:

In the implementation of BGP with the default route, at the network level we will announce the default route to reach the two Internet access providers; this means that traffic originating from the network can pass either through the first Internet access provider or through the second, and it is up to the network administrator to specify on the administrative exemption which traffic can pass only through the first ISP only. And that allows us to do load sharing.

What is very important here is that at the level of the routing table, we will have a single line, this is the default route, or two routes, i.e. the route to the first internet provider and the second line to the second. And that has the disadvantage of not being able to force the routing.

b. Partial update

In partial updates, at the router level we will not advertise the default route, i.e. part of the network to reach the Internet can be condemned to the first Internet service provider and a second part of the network to the second ISP.

And this as an advantage, you can play on the routes to join the remote networks by choosing a link.

And as a disadvantage: there is a high consumption of CPU and memory.

c. full updates

In the complete updates we give the possibility to receive all the routes coming from the Internet service providers. And it is necessary to have a router capable of supporting all the routes, especially based on the memory which can make it possible to classify all the routes of the Internet network.

3.Deployment of the solution

Scenario

With respect to the outgoing packet, we will define in the sense that half of the data from the 10.10.10.0 network will pass through the first internet service provider and the second part will pass through the second internet service provider.

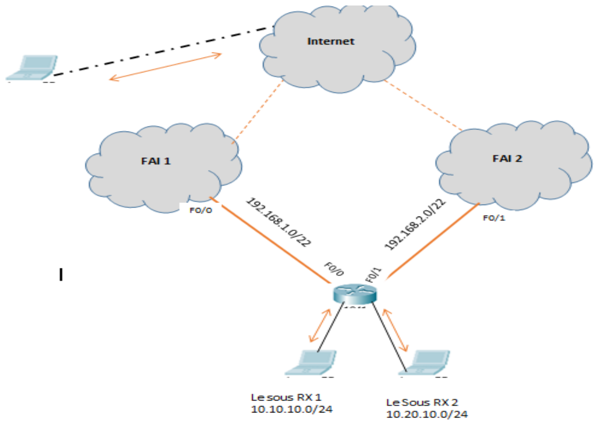
And the same principle with the 10.20.10.0 network, part of the network will go through the first internet service provider and a second part of this network goes through the second internet service provider.

Second scenario: the first internet service provider for example as it offers a better quality of service, with a large bandwidth, we will send out the most important data via this first internet service provider and the rest of the data we send on the second link (second internet service provider) and here it is for outgoing traffic.

And with regard to routing, we can force it by announcing part of the 10.10.10.0 network which can only go out on the first internet access provider, so if there is traffic destined for this network, it will go to the first Internet service provider.

And do the same on the 10.20.10.0 network with the second internet service provider.

3.1 Illustration diagrams of the solution



4.For this solution, we have implemented these few lines of configuration codes

Configuration of the first Internet Service Provider

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R_FAI1
R_FAI1 (config)#interface fastEthernet 0/0
R_FAI1(config-if)#ip address 192.168.1.1 255.255.255.252
R_FAI1(config-if)#no shutdown
R_FAI1(config-if)#exit
R_FAI1(config)#router bgp 100
R_FAI1(config-router)#neighbor 192.168.1.2 remote-ar 200
R_FAI1(config-router)#neighbor 192.168.1.2 activate
R_FAI1(config-router)#network 192.168.1.0 mask 255.255.255.252
R_FAI1     (config-router)#exit
```

Configuration router second Internet access provider

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R_FAI2
R_FAI2 (config)#interface fastEthernet 0/1
R_FAI2(config-if)#ip address 192.168.2.2 255.255.255.252
R_FAI2(config-if)#no shutdown
R_FAI2(config-if)#exit
R_FAI2(config)#router bgp 100
R_FAI2(config-router)#neighbor 192.168.2.1 remote-ar 200
R_FAI2(config-router)#neighbor 192.168.2.1 activate
R_FAI2(config-router)#network 192.168.2.0 mask 255.255.255.252
R_FAI2(config-router)#exit
```

Central Router Setup

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

// Address configuration on central router interfaces
```

```
Router(config)#hostnameR_Central
R_Central (config)#interface fastEthernet 0/0
R_Central (config-if)#ip address 192.168.1.2 255.255.255.252
R_Central (config-if)#no shutdown
R_Central (config-if)#interface fastEthernet 0/1
R_Central (config-if)#ip address 192.168.2.1 255.255.255.252
R_Central (config-if)#no shutdown
R_Central (config-if)#exit
R_Central (config)#int loopback 0
R_Central (config)#ip add 10.10.10.1 255.255.255.0
R_Central (config)#no sh
R_Central (config)#int loopback 2
R_Central (config)#ip add 10.20.10.1 255.255.255.0
R_Central (config)#no sh
```

```
//configure the BGP protocol
R_Central (config)#router bgp 200
R_Central (config-router)#neighbor 192.168.1.1 remote-ar 100
R_Central (config-router)#neighbor 192.168.1.1 activate
R_Central (config-router)#neighbor 192.168.2.2 remote-ar 200
R_Central (config-router)#neighbor 192.168.2.2 activate
R_Central (config-router)#exit
```

```
// Configuring the Default Route from the Central Router to Both Internet Service Providers
R_Central (config)#router bgp 200
R_Central (config-router)#network 192.168.1.0 mask 255.255.255.252
R_Central (config-router)#network 192.168.2.0 mask 255.255.255.252
R_Central (config-router)#network 10.10.10.0 mask 255.255.255.0
R_Central (config-router)#network 10.20.10.0 mask 255.255.255.0
R_Central (config-router)#neighbor 192.168.1.1 active-map ADvited-FAI1
R_Central (config-router)#exit
R_Central (config-router)#neighbor 192.168.2.2 active-map ADvited-FAI2
R_Central (config-router)#exit
```

Here the code explains that network traffic 10.10.10.0 only goes through the first Internet Service Provider

```
R_Central (config)#access-list 20 permit 10.10.10.0  0.0.0.255
R_Central (config)#access-list 30 permit 192.168.2.0  0.0.0.1
```

Here the code explains that we will only define the route of the network 10.20.10.0 to pass only through the second Internet Service Provider

```
R_Central (config)#access-list 40 permit 10.20.10.0  0.0.0.255
R_Central (config)#access-list 50 permit 192.168.1.0  0.0.0.1
```

5.Conclusion

The setting up of this scientific progress was made with the aim of providing a solution to the problem within companies by setting up a routing strategy based on the separation of lines and the relay system in the event of interruption of the signal from one of the internet service providers.
Knowing the consequences of this in the event of a signal break.

REFERENCES

[1]Y. Rekhter, T. Li et S. Hares, « *A Border Gateway Protocol 4 (BGP-4)* », RFC 4271, janvier 2021
[2]José DORDOIGNE, Practice network administration, Paris, ENI, 2004
[3]https://www.youtube.com/watch?v=X47V1O2Ggqk, consulted on November 25, 2021