DYNAMIC RECONFIGURATION WITH VIRTUAL LANS

[1]Engr. Md. Mustafa Kamal
Director General (DG), Bangladesh Telecommunication Regulatory Commission (BTRC)
[2]Mahbub UL Alam
Assistant Vice President, ITS Flora Telecom Limited
[3]Md. Nesar Rahman
System Administrator, Bangladesh Army
[4] Sah Riyadh Hasan Rana
System & Support Engineer, East Coast Group.
[5]Ayesha Siddika
Assistant Professor, Dept. of CSE
World University of Bangladesh (WUB)

Abstract

This project purpose is Dynamically Reconfiguration the Virtual LAN with the redundancy network line. In a Network Topology where use redundancy network line which is configured by dynamically. That means the redundancy network line will be working dynamically. For this dynamic reconfiguration, use BGP & Static routing protocol. If the BGP protocol failed or not working, then Static routing will be working. It's working on two different offices like main office & branch office which connected with two different ISP. Branch office connected with Main office by two ISP which one ISP is primary network line & another is redundancy network line. And all routers are configured by BGP & Static routing protocol. If one ISP network line is down, then another ISP network line is working dynamically. So that there is no network interruption between two offices.

Keywords: Dynamic, Virtual LAN, BGP, ISP

Introduction

All organizations that depend on Internet for sales revenue or business continuity require internet redundancy. Downtime lowers productivity, yields losses and painfully affects the company's reputation. Our project is Redundancy network line by Dynamically Reconfiguration with virtual lans. Our project introduces the new network line which is not interrupt in the network lines. In our Network Topology we use redundancy network line which is configured by dynamically. That means the redundancy network line will be working dynamically. Border Gateway Protocol (BGP) to get rid of multiple internet redundancy issues and generate significant results for your company. BGP is a critical instrument for attaining those goals. The connection to two or more ISPs is known as multi homing. As you multi home, BGP operates on your routers and delivers redundancy by determining on which ISP delivers the most effective path. For this dynamic reconfiguration, we use BGP & Static routing protocol. If the BGP protocol failed or not working, then Static routing will be working. We are working on two different offices like main office & branch office which connected with two different ISP. Branch office connected with Main office by two ISP which one ISP is main network line & another is redundancy network line. And all routers are configured by BGP & Static routing protocol. If one ISP network line is down, then another ISP network line is working dynamically. So that there is no network interruption between two offices. BGP represents the internet routing protocol. It acts similar to Routing Information Protocol (RIP), however, instead of choosing the shortest path based on hops, it makes a decision relying on the shortest Autonomous System (AS) path.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

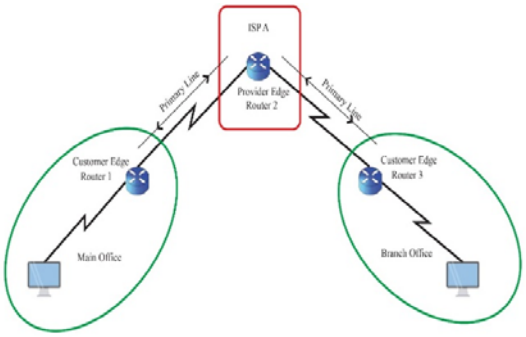
Objectives

1. Dynamic configuration in the network devices is the ability to modify and extend a network system while it is running.
2. Dynamically reconfiguration is added with network redundancy network line.

Scope of the project

In this project, we configured only BGP routing protocol in our network topology. But there is many scopes to configure other routing protocols. We establish primary link along with secondary link through two different ISP provider. Here, there is option to use more redundancy network link if the organizations need. To eliminate single points of failure for networking, each subnet accessed by a cluster node is required to have redundant network interfaces. Redundant cables are also needed to protect against cable failures. Each interface card is connected to a different cable, and the cables themselves are connected by a component such as a hub or a bridge. This arrangement of physical cables connected to each other via a bridge or concentrator or switch is known as a bridged net. We establish our small network through BGP. But BGP is the best routing protocol for the big network in different locations. Our project network topology or concepts can renewable or efficiency for any organizations. They can customize their own network through our network topology. IP addresses can be associated with interfaces on a bridged net. An interface that has an IP address associated with it is known as a primary interface, and an interface that does not have an IP address associated with it is known as a standby interface. Standby interfaces are those which are available for switching by Service guard if a failure occurs on the primary. When Service guard detects a primary interface failure, it will switch the IP addresses and any associated connections from the failed interface card to a healthy standby interface card. So, these points are the scope of our project.

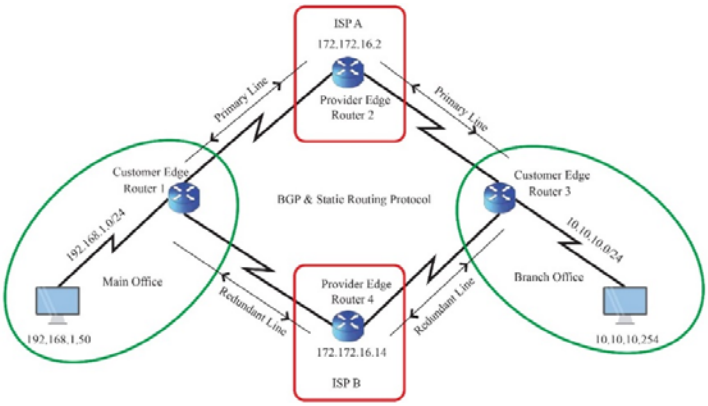
Problem Statement



Here Fig. 1, this is our problem statement which is showing the primary network link between two offices. One is Main office & another is Branch office and they have connected with ISP A. Here Main office side is customer edge router 1 and Branch office side is customer edge router 3. And they are connection with ISP A which is provider edge router 2. The link between Main office to ISP A and ISP A to Branch office is the primary link. By this primary link they are communicating with each other. This is the only one link between them to communicate. If the primary link is down physically like cable cut or ISP A problem, then whole communication between two offices are getting interruption & down. That's why this is our problem statement of project. If we make redundancy or secondary link with the primary link, then this interruption of two offices are not happened. This is our problem statement and we solve this problem with the redundancy link. Every company always need to connect or communicate with their branch office. So that they need smooth & no interruption link between their offices. For this problem we make a solution which is redundancy link means another ISP link between two offices. If they need, we can make more redundancy link between two offices.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Network Topology



Here Fig. 2, the network topology our project, that means how our solution of problem statement work. First we show details about this network topology. Second we show how network topology work. We have two offices, one is main office and another is branch office. Then we have two providers, one is ISP A and another is ISP B. Suppose we have four routers, customer edge router 1 and 3 & provider edge router 2 and 4. That means two are customer edge router which is situated in main office and branch office. Customer edge router 1 is in the main office and customer edge router 3 is in the branch office. Then provider router 2 is in the ISP A and provider edge router 4 is in the ISP B. And all the routers are configured by BGP routing protocol & static routing. Here main office and branch office are connected with ISP A and ISP B where ISP A is the primary network link and ISP B is the secondary or redundant link. **Main office server pc ip address is 192.168.1.50 and Branch office user pc ip address is 10.10.10.254. Then ISP A, provider edge router 2 ip address is 172.172.16.2 and ISP B, provider edge router 4 ip address is 172.172.16.14. Router 2 and 4 using same range ip address. As our project, we are using mikrotik router.** If the branch office user pc wants to establish network or get some files from the main office server pc, then are connected through the primary link ISP A. If any trouble gets occurred to establish the connection between two offices through primary link ISP A, then dynamically ISP B establish the link or connection between two offices. We are using BGP protocol in our network topology. That means all routers are configured by BGP. As BGP is the best routing protocol among others. Anyone can use another routing protocol without BGP. But BGP is the perfect routing protocol in this scenario. So this our Network Topology for our problem statement.

The Basics of Network Redundancy

Network redundancy is an integral part of an enterprise business communications plan. A redundancy or disaster recovery plan identifies the critical components of the network where a failure would cause significant outages. In the event of a failure with these various communications links or devices, redundancy allows your network to remain in service by providing alternative communications paths and backup equipment.

Direct Cost - The direct expense outlay to accomplish a given activity. Direct costs would include the cost to detect and control the incident, possible equipment damage, and cost of third parties contracted to help resolve an unplanned outage.

Indirect Cost – The amount of time, effort, and other organizational resources spent, but not as a direct cash outlay. Indirect costs would include the time to recover lost or damaged mission-critical data as well as user and IT productivity loss.

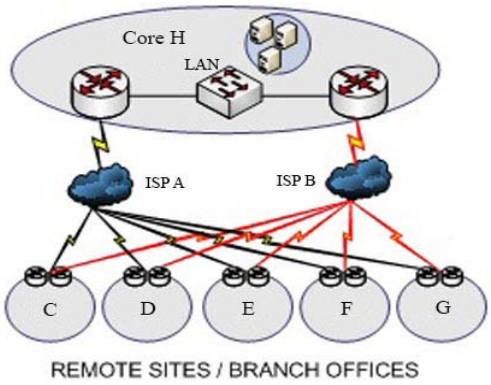
Opportunity Cost - The cost associated with lost business opportunities as a result of reputation diminishment after the outage. Opportunity costs would include lost revenues and related business consequences. Lost revenues come from the current and potential customers' inability to access core systems like VoIP or email during the outage period. The consequences a business could face due to an outage would be reputational damages, customer churn, and loss of business opportunities.

Avoid scenarios where your staff indicate, "The server(s) is down! The Internet is down," and then wondering what other fallout occurred due to a network failure. There are different types of redundancy

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

options that are available for your business and in your provider's network; you just have to determine which one would be the right fit for your network. We have included some for you to review:

Importance of Network Redundancy



Today's networks are high-tech and most times high speed. Common to most Wide Area Network (WAN) designs is the need for a backup to take over in case of any type of failure to your main link. A simple scenario would be if you had a single T1 connection from your core site to each remote office or branch office you connect with. In this section we will explore this scenario and other scenarios to help you design and plan for a backup solution that you can count on and one that is cost effective and will not break the bank. Here you have multiple remote sites connecting to a core (or multiple core) locations. Redundant links provide an alternate solution to main link failure on your WAN and provide remote site access to core resources. You should also consider failover technologies. Must like server clustering, network equipment can also failover to other devices (such as routers, switches, firewalls, etc.) if configured to do so. For example, a Cisco router can be configured with Hot Standby Router Protocol (HSRP). Servers can be clustered and load balanced for any failover scenario you can think of. With Windows Hyper-V, VMware and Citrix virtualization solutions, you can create a design where any failure can be dealt with automatically keeping operations running in the case of any disaster. It's important for VPN clients to be able to access corporate resources as well, whether on the road or in a home-based office. That being said, you should consider reviewing your VPN concentrator redundancy as well. If you need two core based units for this strategy, make sure that they also know how to fail over from one to the other in time of need. Once you have considered your design after full analysis and implemented it, you need to test it thoroughly and then document the procedures. After that, you need to continue to test and update the documentation especially as new technologies are added to your architecture, or as your architecture grows such as adding new sites. Now that we have talked about the importance of redundancy, especially in the network.

Test Plan – put together a plan that covers the details of a failover scenario so you can test for it. To do this, detail all of the architecture to be tested and failover manually to see how the solution works. Make sure you test applications, routing paths, time/speed/bandwidth usage and accuracy. Test for fail-back as well and how the main link when it becomes available can resume the role of the primary link.

Network Monitoring – your network monitoring solution should help you become aware of a main link failure. Using technologies such as ICMP and SNMP, you can continuously monitor your uptime and be alerted when there is a change in any device, link or solution.

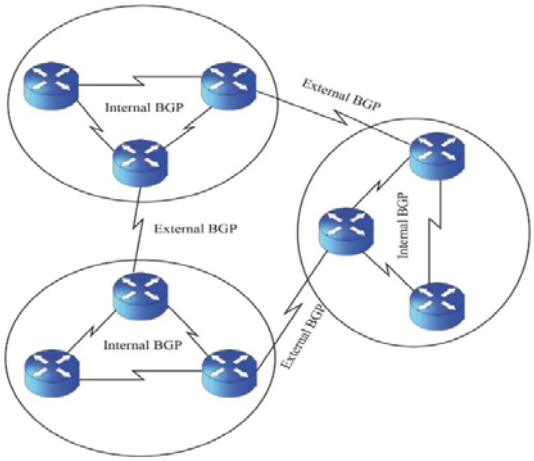
Disaster Recovery Plan – a plan should in place, and if not, added immediately. This plan should outline the Business Continuity Planning and Incident Response Planning are part of this DR plan. How the business will continue to operate, as well as who will react to the problem and follow it through until normal operations are restored. In this article, we looked at adding redundancy into your network.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Purpose of Border Gateway Protocol

Border Gateway Protocol (BGP) advertises, learn, and choose the best paths inside the wide internet. When two ISPs connected, they typically use BGP to exchange routing information. The ISPs of the world wide exchange routing information with one or more than one ISPs. [28] BGP defines in two classes for neighbours.

1. **Internal BGP** (iBGP) operates within the same autonomous system.
2. **External BGP** (eBGP) operates in between the multiple autonomous system.



BGP features

1. BGP is an open standard protocol.
2. EBGP designed for inter-AS domain routing to scale huge network like internet.
3. Its support classless, VLSM, CIDR, auto and manual summary.
4. Updates are incremental and trigger BGP send updates to manually defined neighbor as unicast.
5. BGP is application layer protocol uses TCP for reliability, TCP port 179.
6. Metric is attributes.
7. Administrative distance is 20 for external updates (eBGP) and 200 for internal updates (iBGP).

Deploying BGP for redundant IP connectivity

All organizations that depend on Internet for sales revenue or business continuity require internet redundancy. Downtime lowers productivity, yields losses and painfully affects the company's reputation. In this blog we describe how to setup Border Gateway Protocol (BGP) to get rid of multiple internet redundancy issues and generate significant results for your company. BGP is a critical instrument for attaining those goals. The connection to two or more ISPs is known as multi homing. As you multi home, BGP operates on your routers and delivers redundancy by determining on which ISP delivers the most effective path.

How to configure BGP

BGP represents the internet routing protocol. It acts similar to Routing Information Protocol (RIP), however, instead of choosing the shortest path based on hops, it makes a decision relying on the shortest Autonomous System (AS) path. Autonomous System Numbers are associated with the BGP routing domains. These numbers are assigned by the Regional Internet Registries (RIR), such as the American Registry of Internet Numbers (ARIN), Réseaux IP Europeans (RIPE), etc. When you have an understanding of the BGP basics, it becomes fairly simple to configure a multi homed network. If you currently have your main Internet connection setup, follow these common steps to implement BPG multi homing:

1. Acquire your ASN from RIR.
2. Acquire IP address space from your RIR.
3. If you are using a static route to link to your provider when you are single-homed, then no BGP routes are sent to you. Assuming that, you will need to ask your provider to send you BGP routes. (You're ASN and the remote router's neighbour address will be required by the provider) The static route can

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

be removed once you get the provider's BGP routes in your routing table and start using BGP to advertise your network.
4. Connect to a second provider once you are multi homed on a single router. The secondary provider will also require your ASN and your neighbour address.
5. You will be able to see the routes from each of the providers within your router's BGP table. In BGP, the route with the shortest AS path is considered to be the most effective. The route with the shortest AS path will be mentioned in your routing table.

Using Border Gateway Protocol: Operating BGP routes is a great benefit as well as a great responsibility. Being a BGP neighbour, you are obliged to:

1. Keep your network stable. Your network punctuations are advertised to other routers out there.
2. Advertise only a set of IP addresses that you own. Advertising other addresses could lead to Internet service loss for someone else's entire network.
3. Multi homing necessitates a sophisticated network configuration. Therefore, all the aspects of BGP must be thoroughly inspected prior to engaging in BGP routing.
4. The entire Internet's BGP table is enormous, and when you are multi homed, you have several duplicates of that. Your routers should have sufficient memory capacity to store that much data.

It is fair to consider that with BGP selecting the shortest path, a nearer location must result in superior stability and a steady performance. Since BGP is focused on reachability and its own stability, traffic may only be rerouted in case of hard failures. Hard failures are total losses of reachability as opposed to degradation. This means that
even though service may be so degraded that it is unusable for an end user, BGP will continue to assert that a degraded route is valid until and unless the route is invalidated by a total lack of reachability. BGP as a dynamic routing protocol reacts only in cases of total failure. That is why installation of intelligent routing systems.
Virtualization Support: Static routes support virtual routing and forwarding (VRF) instances. VRFs exist within virtual device contexts (VDCs). By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF.

BGP Process Architecture

This chapter is aimed at introducing the basics of the Border Gateway Protocol used in inter- domain routing. The terminology and the concepts presented in this chapter are used through- out the work to describe the multipath extensions for BGP. The Border Gateway Protocol (hereafter BGP) is the de-facto standard for advertising reachability information in the Internet, where several independent organizations interconnect to create a large scale net- work and profit from the exchanged traffic between end-hosts. Those organizations are the so-called Internet Service Providers (i.e. ISPs). Each ISP runs one or more Autonomous Systems (i.e. AS) or domains, which are networks that hauls traffic according to an economic- driven policy. The AS networks interconnect among them and exchange traffic. When the exchanged traffic between two Assess is uneven or one of them has a better location in the network (e.g. a main provider or tier-1), it is said that they keep a transit relation, one AS plays the role of the provider, offering hauling service towards a destination to the other AS, its customer. The provider charges a per-bit rate to the customer for the coursed traffic from and to the customer network. On the other hand, when the exchanged traffic is roughly the same or both Assess are of similar importance, the two Assess have a peering relation, they both act as peers without charging each other.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

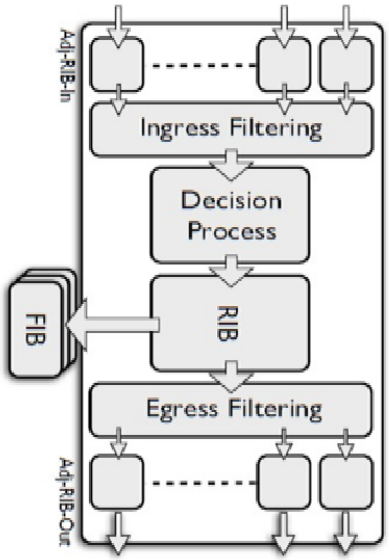


Figure: BGP Process Architecture

1. Keep paths with highest LOCAL_PREF value
2. Keep paths with shortest AS path
3. Keep paths with lowest ORIGIN value
4. For each advertising AS, select the path with lowest MED value
5. If there is a remaining path with session TYPE eASSM, delete paths with TYPE iASSM
6. Keep paths with lowest IGP cost
7. Keep paths with lowest BGP_ID
8. Select the path advertised from the lowest network address

Table 1: BGP Decision Process

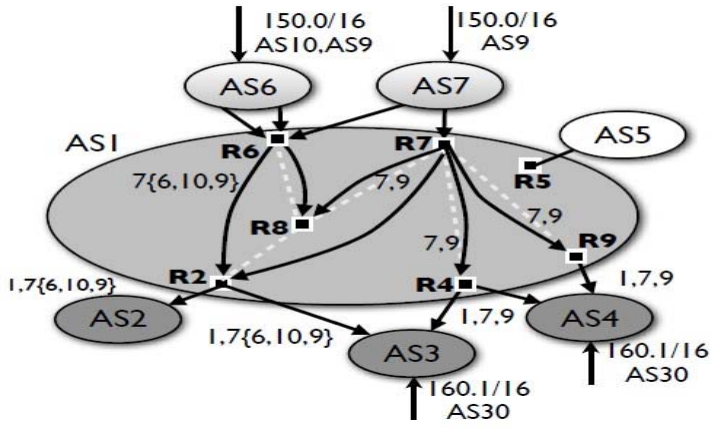
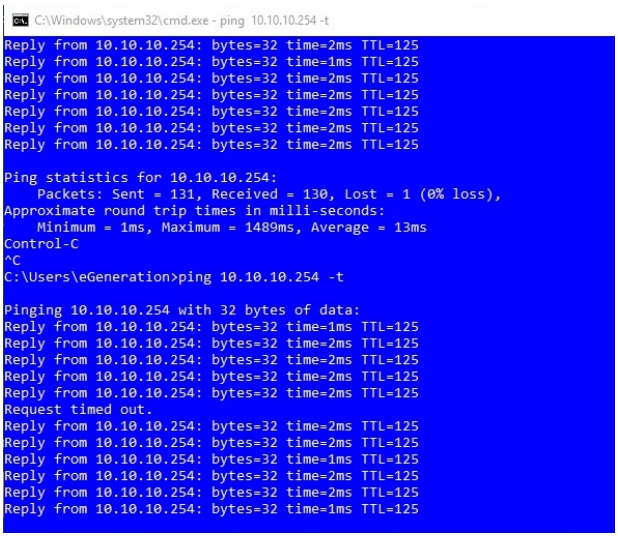


Figure: Model of a transit AS with Path ASSEMBLER Routers

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

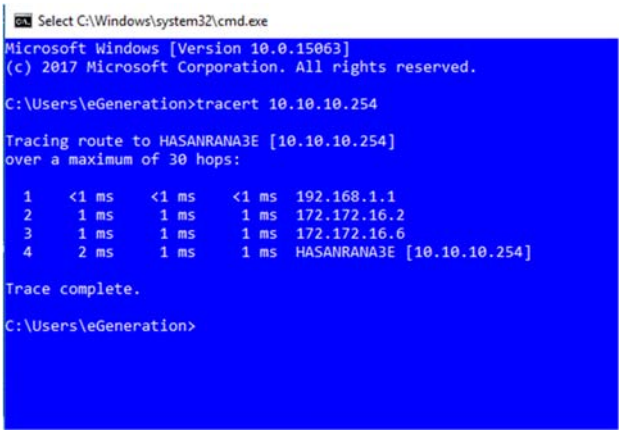
Ping & Traceroute

Figure: Router 1 to Router 3 Ping Traceroute



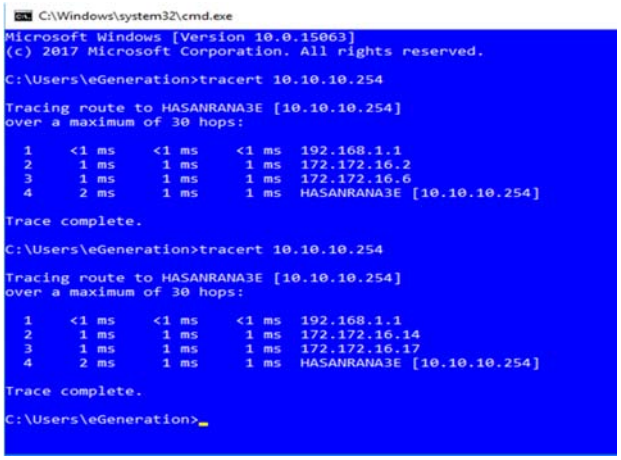
Here Fig. this is the ping traceroute from customer edge router 1 to customer edge router 3.

Figure: Router 1 to Router 3 primary link Traceroute



Here Fig. this is the ping traceroute of primary link from customer edge router 1 to customer edge router 3.

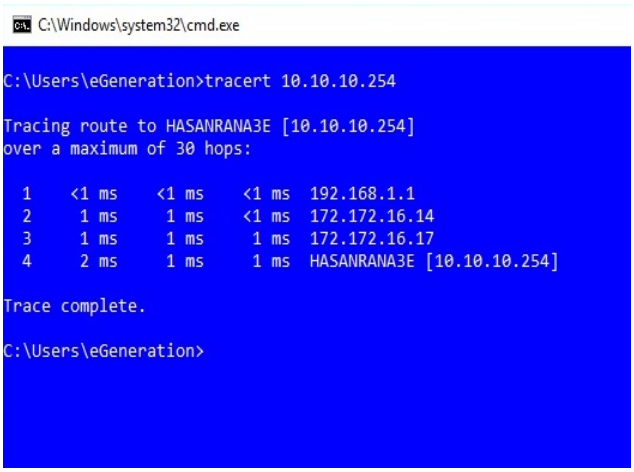
Figure: Router 1 to Router 3 Redundant Link Traceroute



Here Fig. this is the ping traceroute of redundant link from customer edge router 1 to customer edge router 3.

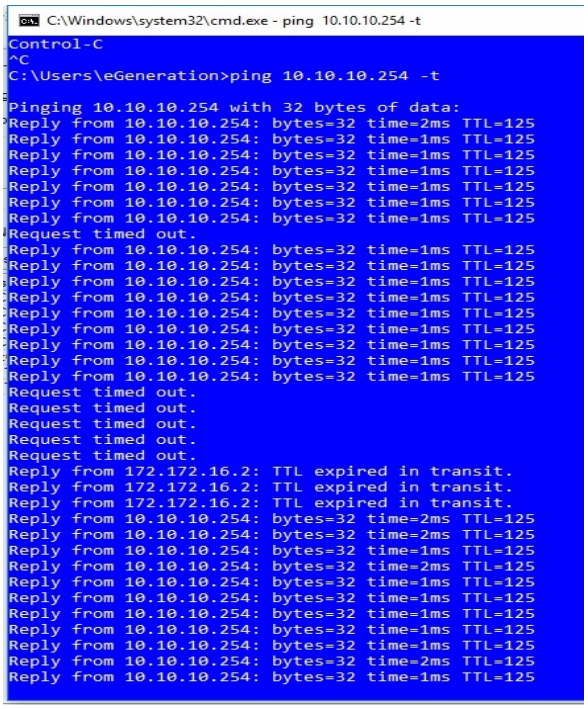
https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure: Router 1 to Router 3 Redundant Network Line Traceroute



Here Fig. this is another ping traceroute of redundant network link from customer edge router 1 to customer edge router 3.

Figure Router 1 to Router 3 Full Ping Traceroute



Here Fig. this is the full ping traceroute from customer edge router 1 to customer edge router 3 where primary link and redundant link work.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Conclusion

The underlying concept behind network redundancy is to provide alternate paths for data to travel along in case a cable is broken or a connector accidentally unplugged. However, Ethernet as standard cannot have rings or loops in the network as this will cause broadcast storms and can ultimately cause the network to stop working. An Ethernet network cannot have two paths from point A to point B without a mechanism in place to support this type of topology. To achieve redundancy, the network infrastructure (switches) must support redundancy protocols designed to negate the usual problems of putting loops into an Ethernet network, maintaining a default data path and switching to an alternate one when a fault occurs.

The most relevant BGP-compatible multipath inter-domain routing proposals with ASSEMBLER and presents the conclusions of this work. Alternative protocols that require a global upgrade of the network (see for instance [5]) are not considered in this discussion. The first set of solutions comparable to ASSEMBLER achieve backwards compatibility using BGP to exchange the primary path (ensuring backwards compatibility) and they use a parallel protocol or BGP extension to advertise additional paths. This is the case of R-BGP, which advertise failover paths [8] to achieve fast recovery. BGP Add-Paths [6] is another solution in which routers add a new BGP capability to incrementally advertise extra paths. Finally, MIRO [33] relies also on an additional negotiation of paths.

Limitation

In our project scenario, the redundancy network link is good for the huge network locations or branches offices of the organizations. But we are unable to show or project in huge network for shortage of router.

Future Work

In order to complete and extent the research work initiated by this thesis, there are some open questions that can serve as the base for future research work. Of special interest are the interoperability aspects. For instance, large ISP do not have a planar architecture for their border routers. The reason behind this is the scalability of the system, since a planar architecture implies that the full-mesh of iBGP between border routers grows exponentially with the size of the network and the system may get to a saturation point in terms of connections and internal churn. ISPs avoid that situation by introducing special nodes called route reflectors which help to reduce the amount of existing connections creating a hierarchy. Typically, the portion of border routers per route reflectors is 10 to 1, the border routers keep only one connection to the route reflector and the full-mesh is only created among the reflectors, which reduces the scalability problem. It could be interesting to perform an analysis of the possible effects that introducing ASSEMBLER inside and AS may have if legacy route reflectors are present.

Another interesting interoperability analysis could be the interactions with BGP Add Paths, such that the architecture of the AS would be inter-domain routers, internally communicated using Add-Paths and using ASSEMBLER to communicate with external ASes that do not support multipath. A transition analysis between these technologies could be interesting as well. The design of traffic engineering techniques that exploit the advantages of using multipath routing is also an open question. It is an intuition of the author that multipath should provide more flexible and finer granularity in the handling of traffic, reducing in some cases the inter domain churn and achieving fast convergence when local failures occur.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

J. verma, k. desai, “Image to sound conversion.” International journal of advance research, Volume 1, Issue 6, November 2013.

M. Vaibhav, V. Govekar, P. Meenakshihttp, “A Smart Reader for Blind People.” International Journal of Science Technology & Engineering, Volume 5, Issue 1, July 2018.

N. Harum, N. Zakaria, Z. Ayop, S. Anawar, “Smart Book Reader for Visual Impairment Person using IoT Device.” International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019.

P. Deole, S. Kulkarni, “A wearable device for the visually impaired.” International Journal of Infinite Innovations in Technology, Volume-IV, Issue-II, October 2016.

R. Duraisamy, S. Manohara, “A Smart Reader for Visually Impaired People.” International Journal of Latest Engineering and Management Research, Volume 03, Issue 10, October 2018

Shilkrot, J. Huber, M. Wong, P. Maes, “A Wearable Device to Explore Printed Text on the Go.” Conference on Human Factors in Computing Systems, April 2015.

S. Muralidharan, D. Venkatesh, J. Pritmen, “Reading Aid for Visually Impaired People.” International Journal of Advance Research, Ideas and Innovations in Technology, Volume 4, Issue 2, 2018.

S. Prasanna, B. Bernadine Infenta, S. Maria Keerthana, S. Maria Vincent, “Book Reader using Raspberry Pi.” International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, April 2018.

Zhiming Liu, Yudong Luo, J. Cordero and Y. Shen (2016), “A Wearable Text Reading Assistive System for the Blind and Visually Impaired.” International Conference on Real-time Computing and Robotics, June 2016.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

APPENDIX

Router – 1 Configuration:

```
# jan/01/2002 02:10:34 by RouterOS 6.31
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
   management-protection=allowed mode=dynamic-keys name=profile1 \
   supplicant-identity=""
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n disabled=no frequency=2447 \
   mode=ap-bridge security-profile=profile1 ssid=MICT wireless-protocol=\
   nv2-nstreme-802.11
/ip pool
add name=dhcp_pool1 ranges=192.168.1.2-192.168.1.254
add name=dhcp_pool2 ranges=192.168.1.2-192.168.1.254
/ip dhcp-server
add address-pool=dhcp_pool1 name=dhcp1
add address-pool=dhcp_pool2 disabled=no interface=ether3 name=dhcp2
/routing bgp instance
set default as=21 redistribute-other-bgp=yes
set admin access=\
   own-routers,own-users,own-profiles,own-limits,config-payment-gw
/ip address
add address=172.172.16.1/30 comment="router 2 port 2" interface=ether2 \
   network=172.172.16.0
add address=192.168.1.1/24 interface=ether3 network=192.168.1.0
add address=172.172.16.13/30 comment="router 4 port 4" interface=ether5 \
   network=172.172.16.12
/ip dhcp-server network
add address=192.168.1.0/24 gateway=192.168.1.1
/ip route
add disabled=yes distance=1 dst-address=10.10.10.0/24 gateway=172.172.16.2
add disabled=yes distance=11 dst-address=10.10.10.0/24 gateway=172.172.16.14
/routing bgp network
add disabled=yes network=10.10.10.0/24 synchronize=no
/routing bgp peer
add name="Router 1" out-filter=out remote-address=172.172.16.2 remote-as=20 \
   ttl=default
add name=Router4 remote-address=172.172.16.14 remote-as=24 ttl=default
set db-path=user-manager
```

Router – 2 Configuration:

```
# jan/02/1970 00:40:07 by RouterOS 6.29.1
# software id = AVD9-AF20
#
/interface wireless
set [ find default-name=wlan1 ] l2mtu=1600 ssid=MikroTik
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ppp profile
set [ find name=default ] name=default
set [ find name=default-encryption ] name=default-encryption
/routing bgp instance
set default as=20 redistribute-other-bgp=yes
/ip address
add address=172.172.16.2/30 interface=ether2 network=172.172.16.0
add address=172.172.16.5/30 interface=ether3 network=172.172.16.4
/ip route
add check-gateway=ping distance=1 gateway=172.172.16.1
add disabled=yes distance=1 dst-address=10.10.10.0/24 gateway=172.172.16.6
/routing bgp peer
add name=Router2 remote-address=172.172.16.1 remote-as=21 ttl=default
add name=Router3 remote-address=172.172.16.6 remote-as=22 ttl=default
/system identity
set name=Router2
/system routerboard settings
set cpu-frequency=650MHz protected-routerboot=disabled
/tool romon port
add disabled=no
```


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Router – 3 Configuration: # jan/02/1970 00:36:59 by RouterOS 6.43.16 # software id = RZB2-N2YQ # # model = RouterBOARD 750 r2 # serial number = 67D40636D847 /interface wireless security-profiles set [find default=yes] supplicant-identity=MikroTik /ip pool add name=dhcp_pool0 ranges=10.10.10.2-10.10.10.254 /ip dhcp-server add address-pool=dhcp_pool0 disabled=no interface=ether5 name=dhcp1 /routing bgp instance set default as=22 redistribute-other-bgp=yes /ip address add address=172.172.16.6/30 interface=ether3 network=172.172.16.4 add address=10.10.10.1/24 interface=ether5 network=10.10.10.0 add address=172.172.16.17/30 comment="From Mikrotik 4" interface=ether4 \ network=172.172.16.16 /ip dhcp-server network add address=10.10.10.0/24 gateway=10.10.10.1 /ip route add check-gateway=ping distance=1 gateway=172.172.16.5 add check-gateway=ping distance=2 gateway=172.172.16.18 /routing bgp network add network=10.10.10.0/24 synchronize=no /routing bgp peer add name=Router3 remote-address=172.172.16.5 remote-as=20 ttl=default add name=Router4 remote-address=172.172.16.18 remote-as=24 ttl=default /system identity set name=Router3	**Router – 4 Configuration:** set [find default=yes] supplicant-identity=MikroTik /routing bgp instance set default as=24 redistribute-other-bgp=yes set admin access=\ own-routers,own-users,own-profiles,own-limits,config-payment-gw /ip address add address=172.172.16.14/30 interface=ether4 network=172.172.16.12 add address=172.172.16.18/30 interface=ether5 network=172.172.16.16 /ip route add distance=1 gateway=172.172.16.13 add disabled=yes distance=1 dst-address=10.10.10.0/24 gateway=172.172.16.17 /routing bgp peer add name=Router1 remote-address=172.172.16.13 remote-as=21 ttl=default add name=Router3 remote-address=172.172.16.17 remote-as=22 ttl=default /system identity set name=Router4 /system lcd set contrast=0 enabled=no port=parallel type=24x4 /tool user-manager database set db-path=user-manager

https://sites.google.com/site/ijcsis/
ISSN 1947-5500