Implementation of Dynamic Routing OSPF and Loopback IP for Failover IBGP Connections

Wahyu Efendi
Mercu Buana University
Jalan Meruya Selatan No. 1, Kembangan, Kebon Jeruk Jakarta, Indonesia

Raka Yusuf
Mercu Buana University
Jalan Meruya Selatan No. 1, Kembangan, Kebon Jeruk Jakarta, Indonesia

ABSTRACT

The Internal Border Gateway Protocol network topology in an internet service company that is not well-designed can affect the convenience of service users such as the length of time the internet network is down when the Internal Border Gateway Protocol network has a problem. Therefore, it is necessary to design an Internal Border Gateway Protocol network topology that can meet the needs of service users. In this case, the internet connection service should always work. This study aims to build a failover system in one of the internet service providers which is PT. Quanta Tunas Abadi using the Network Development Life Cycle approach. The results of Internal Border Gateway Protocol network topology design became a proposal for the development of Internal Border Gateway Protocol networks at the PT. Quanta Tunas Abadi. The results of the implementation of a failover system using the Open Shortest Path First protocol and IP Loopback on the Internal Border Gateway Protocol network have a positive effect of being able to automatically move the Internal Border Gateway Protocol connection path within 3 seconds and the Border Gateway Protocol connection status remains established when the line of the main used is disconnected.

General Terms

Dynamic Routing Protocol, Mission Critical System

Keywords

Failover, Internal BGP, OSPF, Loopback IP

1. INTRODUCTION

An internet service provider company can use BGP connections between internal routers to distribute prefixes from the gateway router to the distribution router. If there is a disruption in the path from the gateway router to the distribution router, the BGP connection will be disconnected and the prefix cannot be distributed. In order to overcome this problem, it needs a failover system that able to move the connection path automatically between the gateway router and the distribution router when the path used is interrupted so that BGP connections are not interrupted or remain established.

This research was conducted with the aim of building a failover system using OSPF routing protocols and IP Loopback on Internal BGP networks in an internet service provider company.

In order that the writing of this study is not deviant and in accordance with the background of the problem, the authors limit the problem that only applies to OSPF dynamic routing for Internal BGP failover and uses IP loopback as IP Point to Point BGP at PT. Quanta Tunas Abadi. The author limits the scope of his research for router devices used in the Internal BGP network which is the Mikrotik router, while the routing protocol used is BGP and OSPF. Data collection in this study used observation method carried out on situations occurred when data traffic engineering in Internal BGP networks that have been prepared in such a way as to examine the mechanism in network communications.

2. RELATED WORK

According to a study conducted by B. Rifai and E. Supriyanto, OSPF has less than 5 seconds to restore a connection that has been disrupted so that it has a positive effect when it is implemented for network failover systems. The study compared the performance of a failover system built using the OSPF protocol and a failover system using the BGP protocol [1]. In this study, the authors used both protocols (OSPF and BGP) simultaneously to build an Internal BGP network failover system at PT. Quanta Tunas Abadi. According to T. Ernawati and J. Endrawan, the performance of network systems using BGP is better than without BGP. Comparison of the average latency parameter is 0% (almost no latency) which means that the access speed is faster than without BGP [2]. According to research conducted by V. Vetriselvan, P. R. Patil and M. Mahendran, and research conducted by C. Wijaya, OSPF has the lowest cost and highest throughput compared to the RIP, IGRP, and EIGRP protocols and also has the following advantages.

- OSPF is not CISCO's protocol.
- OSPF always determines loop-free routes.
- If changes occur in the network, updates are fast.
- Low bandwidth utilization.
- Supports multiple routes for single-purpose networks.
- OSPF refers to the cost of the interface.
- Supports Variable Length Subnet Mask (VLSM) [3][4][5].

According to H. A. Musril, the loopback interface is a logic and not a physical interface so that this interface is virtually non-existent. The loopback interface does not have a physical cable connected to a router or switch. The loopback interface is an interface that is never in a "down" position, while the physical interface can die or experience downtime when a wiring error occurs. So that the IP address on the loopback interface will never timeout and is very suitable to be used as a router ID [6][7].

The following innovations used in this study:

- OSPF Protocol on Internal BGP networks used for problem-solving and one of many solutions to issue network failure.
- Loopback IP addresses as an IP Point to Point for BGP connection between routers so that IP Point to Point is always active.

3. METHODOLOGY

In conducting experiments on this network system, it is necessary to do several steps to identify that the data transfer from the source to the destination was successfully carried out. If data transfer is not successful, it is necessary to make a change by using a failover system as a solution to ensure data transfer continues when a problem occurs in the data path used. In this study, the authors used the NDLC (Network Development Life Cycle) approach as the stage of the research methodology.

NDLC is a method that can be used to develop a computer network. There are 6 basic steps from NDLC as shown in Fig. 1, but as time goes by many researchers applied different steps but are still in the same stage [8].

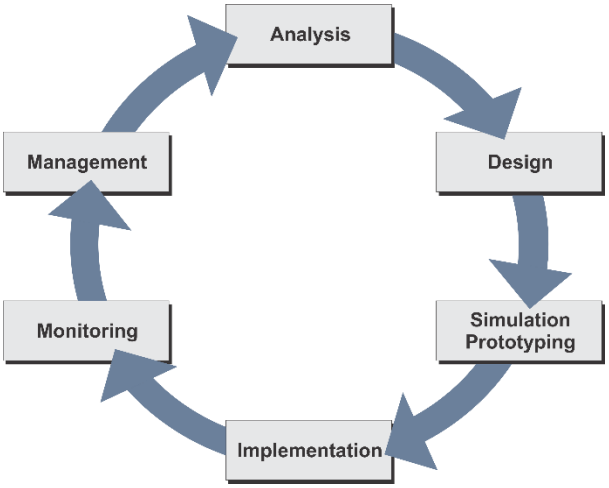


Fig 1: Network Development Life Cycle

4. USED TOPOLOGY

4.1 Initial Topology

In the initial topology as shown in Fig. 2, the connection from the router border transit to the distribution router uses Internal BGP to send the prefix received from upstream international to the router distribution through vlan-id 100 with an IP point to point 11.11.11.0/30. Then, the connection from the IIX border router to the distribution router uses Internal BGP to send the received prefix from the local upstream to the distribution router via vlan-id 200 with IP Point to point 22.22.22.0/30.

In the initial topology, if the connection from the router border transit to the distribution router is interrupted or broken, then the prefix received from upstream international cannot be sent to the distribution router because BGP between border router and transit routers is down or not established. In order to restore the BGP connection between routers that are disconnected so that it can be established again takes a long time because besides the path transfer process is still done manually by moving vlan-id 100 tagging through other channels, the advertise prefix with a prefix of around 700 thousand until the distribution router takes a long time to get full route.

4.2 Proposed Logic Topology

In order to overcome the problems in the initial topology, the author implemented OSPF dynamic routing as a failover system and used IP loopback as an IBGP IP point to point between routers as seen in Fig. 3. In the proposed topology, if the main line used experiences interference, then the IP connection point to point between the routers will move automatically through other channels so that the IBGP connection between routers remains established.

The following is the system design for the allocation of IP Address or Subnetting according to the proposed topology.

11.11.11.0/30, vlan-id 100 : OSPF IP PTP between border transit routers and distribution routers

22.22.22.0/30, vlan-id 200 : OSPF IP PTP between border IIX routers and distribution router

12.12.12.0/30, vlan-id 300 : OSPF IP PTP between border transit routers and border IIX routers

103.116.173.1/32 : IP loopback border transit routers

103.116.173.2/32 : IP loopback border IIX routers

103.116.173.3/32 : IP loopback distribution routers

The following OSPF and BGP configurations implemented on border transit routers are in accordance with the proposed logic topology design.

1 name="internal" router-id=103.116.173.1 distribute-default=never redistribute-connected=as-type-2 redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out

For OSPF configuration, the purpose of using redistributed-connected as-type-2 is to be able to also send network IP point to point BGP border transit routers with upstream transit to router distribution. It is intended that the network IP point to point is reachable on the router distribution side because in the IBGP topology applied, the gateway prefix received from the direction of the border transit router in the distribution router routing table will lead to the IP gateway on the upstream transit side (not IP point to point between router distribution and router border transit).

For BGP configurations on the side of routers transit uses route-reflector, next-hop = force-self, update-source = loopback and hold time which is 3 minutes. The following configuration was attached.

0 E name="DISTRIB" instance=higen.border.ipv4 remote-address=103.116.173.3 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=dist-in out-filter=dist-out address-families=ip update-source=loopback default-originate=never remove-private-as=yes as-override=no passive=no use-bfd=no

1 E name="IIX" instance=higen.border.ipv4 remote-address=103.116.173.2 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=iix-in

out-filter=iix-out address-families=ip update-source=loopback default-originate=never remove-private-as=yes as-override=no passive=no use-bfd=no

In the border transit routing router table presented below, it appears that there are several Google prefixes in the border transit routing table obtained from the upstream direction. The author used these prefixes to be distributed to the distribution router using the BGP protocol and used to test connections to the international. It can be seen also for IP address Loopback and internal IP from IIX routers and distribution routers already included in the routing table obtained through the OSPF protocol.

@BORDER.TRANSIT] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,

B - blackhole, U - unreachable, P - prohibit

#		DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADb	8.8.4.0/24		103.116.172.9	200
1	ADb	8.8.8.0/24		103.116.172.9	200
2	ADb	8.8.33.0/24		103.116.172.9	200
3	ADb	8.8.39.0/24		103.116.172.9	200
4	ADb	8.8.176.0/24		103.116.172.9	200
5	ADb	8.8.178.0/24		103.116.172.9	200
6	ADb	8.8.208.0/21		103.116.172.9	200
7	ADb	8.8.216.0/24		103.116.172.9	200
8	ADb	8.8.217.0/24		103.116.172.9	200
9	ADb	8.8.218.0/24		103.116.172.9	200
10	ADb	8.8.219.0/24		103.116.172.9	200
11	ADb	8.8.226.0/24		103.116.172.9	200
12	ADb	8.8.227.0/24		103.116.172.9	200
13	ADb	8.8.228.0/22		103.116.172.9	200
14	ADb	8.8.232.0/21		103.116.172.9	200
15	ADC	11.11.11.0/30	11.11.11.1	VID.100.TRANSIT...	0
16	ADC	12.12.12.0/30	12.12.12.1	VID.300.TRANSIT...	0
17	ADC	103.116.172.8/30	103.116.172.10	ether1	0
18	A S	103.116.172.96/30		103.116.172.9	1
19	ADb	103.116.173.0/24		103.116.173.3	200
20	ADC	103.116.173.1/32	103.116.173.1	loopback	0
21	ADo	103.116.173.2/32		12.12.12.2	110
22	ADo	103.116.173.3/32		11.11.11.2	110
23	ADo	103.116.173.100/30		11.11.11.2	110

The following is the IP Address, OSPF and BGP configuration on the router distribution according to the proposed topology attached.

RO-DIST] > ip address print

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	22.22.22.2/30	22.22.22.0	VID.200.DIST-IIX
1	11.11.11.2/30	11.11.11.0	VID.100.DIST-TRANSIT
2	103.116.173.101/30	103.116.173.100	bridge1
3	103.116.173.3/32	103.116.173.3	loopback

In the attachment configuration of the IP address router distribution above, there is a configuration IP address 103.116.101 / 30 installed on the bridge1 interface where the IP address used as the source address for the router test ping from the distribution towards the international when failover testing is performed. The following is the OSPF configuration on a distribution router that is not much different from the configuration on the border transit router, which uses redistributed-connected as-type-2.

1 name="internal" router-id=103.116.173.3 distribute-default=never redistribute-connected=as-type-2 redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out

For the BGP configuration, the following distribution routers use route-reflect, nexthope = force-selfe, update-source = loopback and the default 3 minutes hold time is the same as the configuration on the border transit router.

0 E name="BORDER" instance=higen.dist.ipv4 remote-address=103.116.173.1 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=border-in out-filter=border-out address-families=ip update-source=loopback default-originate=never remove-private-as=yes as-override=no passive=no use-bfd=no

1 E name="IIX" instance=higen.dist.ipv4 remote-address=103.116.173.2 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=iix-in out-filter=iix-out address-families=ip update-source=loopback default-originate=always remove-private-as=yes as-override=no passive=no use-bfd=no

The following is the routing table on the distribution router,

RO-DIST] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,

B - blackhole, U - unreachable, P - prohibit

#		DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADb	8.8.4.0/24		103.116.172.9	200
1	ADb	8.8.8.0/24		103.116.172.9	200
2	ADb	8.8.33.0/24		103.116.172.9	200
3	ADb	8.8.39.0/24		103.116.172.9	200
4	ADb	8.8.176.0/24		103.116.172.9	200
5	ADb	8.8.178.0/24		103.116.172.9	200
6	ADb	8.8.208.0/21		103.116.172.9	200
7	ADb	8.8.216.0/24		103.116.172.9	200
8	ADb	8.8.217.0/24		103.116.172.9	200
9	ADb	8.8.218.0/24		103.116.172.9	200

10 ADb 8.8.219.0/24 103.116.172.9 200

The google prefix sent by the transit router has been received by the distribution router. However, for the gateway, the IP gateway seen in the routing table above is IP 103.116.172.9. The IP gateway is a bgp IP point to point between border transit and upstream transit routers that are on the upstream side. This is because the connection between router border transit and router distribution used an internal BGP connection with the same AS number so that the as-path of the router distribution to the border transit router still reads one as-path.

The last is the OSPF and BGP configuration on the border IIX router as follows.

1 name="internal" router-id=103.116.173.2 distribute-default=never redistribute-connected=as-type-2 redistribute-static=no redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no metric-default=1 metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out

0 E name="BORDER-TRANSIT" instance=higen.iix.ipv4 remote-address=103.116.173.1 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=transit-in out-filter=transit-out address-families=ip update-source=loopback default-originate=never remove-private-as=yes as-override=no passive=no use-bfd=no

1 E name="DIST" instance=higen.iix.ipv4 remote-address=103.116.173.3 remote-as=137363 tcp-md5-key="" nexthop-choice=force-self multihop=no route-reflect=yes hold-time=3m ttl=default in-filter=dist-in out-filter=dist-out address-families=ip update-source=loopback default-originate=never remove-private-as=yes as-override=no passive=no use-bfd=no

In the OSPF and BGP configuration on border IIX routers above are also the same as configuration on router border transit and distribution routers. OSPF uses redistributed-connected as-type-2 and for BGP using route-reflect, nexthope = force-selfe, source-update = loopback and default holdtime is 3 minutes.

The border router IIX acts as a backup path between router border transit and distribution routers. When the line between the router border transit and the distribution router is interrupted, the line from the router distribution towards the international will automatically be routed through the IIX router first.

In the border IIX router routing table below, there are several google prefixes obtained from border transit routers. These prefixes must be converted to the border IIX router from the border transit router but do not need to be forwarded to the router distribution by the IIX border router. This is because the IIX border router must also get the google/international prefix from the border transit router so that the distribution router gets reachable status to the international prefix obtained from the router border transit when using the backup path.

@BORDER-IIX] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,

B - blackhole, U - unreachable, P - prohibit

#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0	ADb	8.8.4.0/24	103.116.172.9	200
1	ADb	8.8.8.0/24	103.116.172.9	200
2	ADb	8.8.33.0/24	103.116.172.9	200
3	ADb	8.8.39.0/24	103.116.172.9	200
4	ADb	8.8.176.0/24	103.116.172.9	200
5	ADb	8.8.178.0/24	103.116.172.9	200
6	ADb	8.8.208.0/21	103.116.172.9	200
7	ADb	8.8.216.0/24	103.116.172.9	200
8	ADb	8.8.217.0/24	103.116.172.9	200
9	ADb	8.8.218.0/24	103.116.172.9	200
10	ADb	8.8.219.0/24	103.116.172.9	200
11	ADb	8.8.226.0/24	103.116.172.9	200
12	ADb	8.8.227.0/24	103.116.172.9	200
13	ADb	8.8.228.0/22	103.116.172.9	200
14	ADb	8.8.232.0/21	103.116.172.9	200
15	ADo	11.11.11.0/30	12.12.12.1 22.22.22.2	110
16	ADC	12.12.12.0/30	12.12.12.2 VID.300.IIX-TRA...	0
17	ADC	22.22.22.0/30	22.22.22.1 VID.200.IIX-DIS...	0
18	ADo	103.116.172.8/30	12.12.12.1	110
19	ADC	103.116.172.12/30	103.116.172.14 ether1	0
20	A S	103.116.172.96/30	103.116.172.13	1
21	ADb	103.116.173.0/24	103.116.173.3	200
22	ADo	103.116.173.1/32	12.12.12.1	110
23	ADC	103.116.173.2/32	103.116.173.2 loopback	0
24	ADo	103.116.173.3/32	22.22.22.2	110
25	ADo	103.116.173.100/30	22.22.22.2	110

5. RESULTS AND DISCUSSION

Basically, this research changes the IP point to point that previously used an IP address with subnet / 30 installed on the interface VLAN to be an IP address with a subnet / 32 installed on the loopback interface. It was intended that if there is a disturbance caused by several things such as interface down, cable breaks, configuration errors, or other things that cause the main link to be interrupted, the IP point to point will remain active because it is attached to the loopback interface.

In the proposed logic topology, there are two routing protocols, that is BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First) where both routing protocols have their respective roles. BGP has the duty to distribute the prefix received by the router border from upstream to the distribution router and OSPF is responsible for distributing loopback IP addresses that function as BGP IP points to points between routers.

The following results are pinged and traceroute to IP 8.8.8.8 from the distribution router with source IP 103.116.173.101.

@RO-DIST] > ping 8.8.8.8 src-address=103.116.173.101

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	56	12ms	
1	8.8.8.8	56	56	12ms	
2	8.8.8.8	56	56	12ms	
3	8.8.8.8	56	56	12ms	
4	8.8.8.8	56	56	12ms	

@RO-DIST] > /tool traceroute 8.8.8.8 src-address=103.116.173.101

#	ADDRESS	LOSS	SENT	LAST	AVG
1	11.11.11.1	0%	5	0.3ms	0.4
2	103.116.172.9	0%	5	0.3ms	0.3
3	10.40.1.1	0%	5	0.4ms	1
4	43.240.229.201	0%	5	0.5ms	0.5
5	72.14.194.182	0%	5	11.9ms	12.9
6	108.170.240.161	0%	5	12.3ms	12.3
7	108.170.232.171	0%	5	12.3ms	12.3
8	8.8.8.8	0%	5	12.2ms	12.2

For the ping results from the router distribution to IP 8.8.8.8 is "replay". For the traceroute results, the first hop is directed to

P 11.11.11.1 where that IP is the IP router border transit. It can be concluded that under normal conditions the path from the distribution router towards IP 8.8.8.8 through the border transit router then to the upstream transit.

Then, the author conducted an experiment by deactivating the VLAN-id 100 on the distribution router so that the main line used was disconnected and pinged to IP 8.8.8.8 continuously at the same time to monitor the connection to google when the experiment was executed.

The following is the command to disable the VLAN-id 100 and capture the VLAN interface configuration on the distribution router.

@RO-DIST] > interface vlan disable VID.100.DIST-TRANSIT

@RO-DIST] > interface vlan print

Flags: X - disabled, R - running, S - slave

#	NAME	MTU	ARP	VLAN-ID	INTERFACE
0 X	VID.100.DIST-TRANSIT	1500	enabled	100	ether3
1 R	VID.200.DIST-IIX	1500	enabled	200	ether2

@RO-DIST] > ping 8.8.8.8 src-address=103.116.173.101

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	56	12ms	
1	8.8.8.8	56	56	12ms	
2	8.8.8.8	56	56	12ms	
3	8.8.8.8	56	56	12ms	
4	8.8.8.8	56	56	12ms	
5	8.8.8.8	56	56	12ms	
6	8.8.8.8	56	56	12ms	
7	8.8.8.8	no route to host			
8	8.8.8.8	no route to host			
9	8.8.8.8	no route to host			
10	8.8.8.8	56	56	12ms	
11	8.8.8.8	56	56	12ms	

It can be seen in the ping results above, when vlan-id 100 is deactivated to IP 8.8.8.8, there was a packet loss or time out of 3 digits then replay again. This is because the process of moving the path that was through vlan-id 100 automatically switches through vlan-id 200 and passes the border iix router.

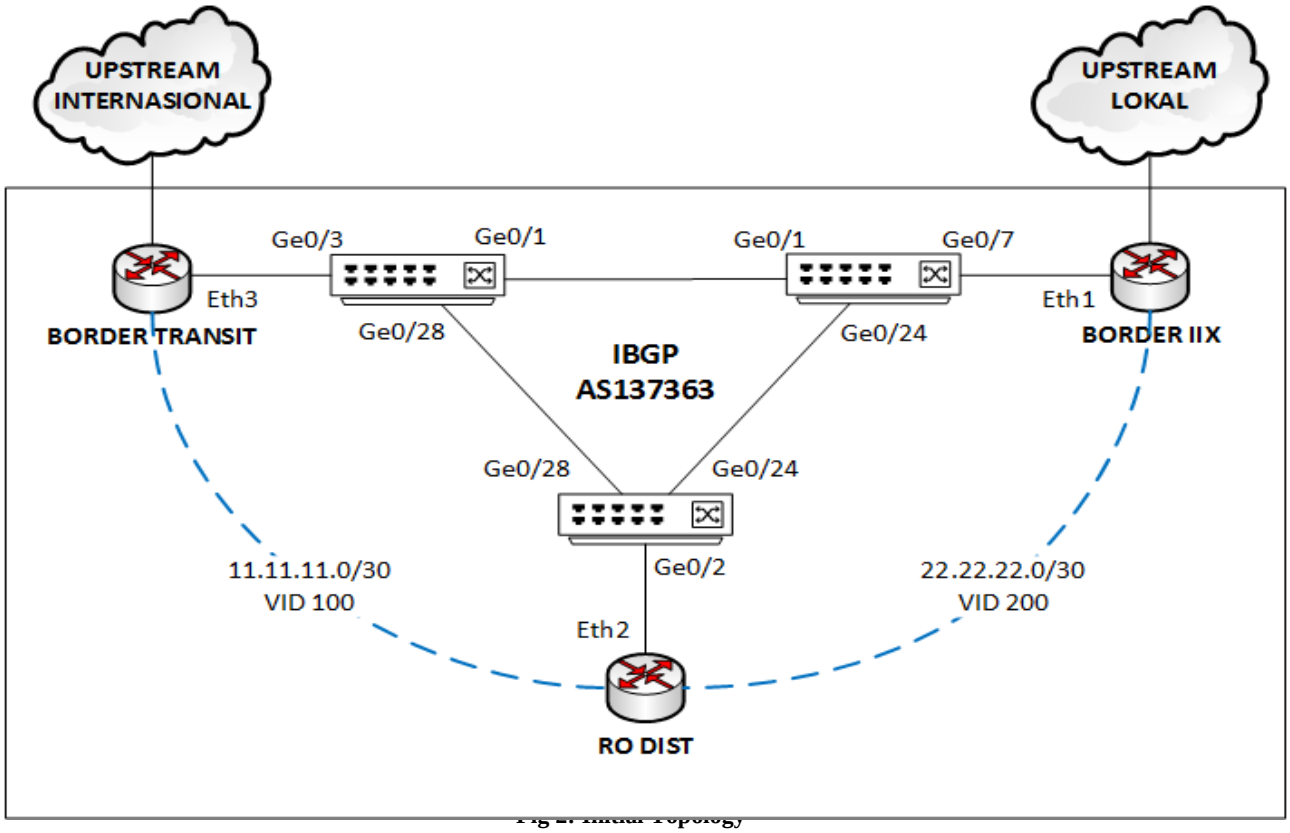
When switching paths, the BGP status between border transit routers and distribution routers is still "established" because the IP point to point connection between routers experience only three seconds of time out (packet loss). This is because BGP has a 3-minute hold time configuration where BGP status will be completely disconnected if the IP point to point time out is more than 3 minutes.

The following results are traceroute after vlan-id 100 is disabled.

@RO-DIST] > /tool traceroute 8.8.8.8 src-address=103.116.173.101

#	ADDRESS	LOSS	SENT	LAST	AVG
1	22.22.22.1	0%	3	0.3ms	0.3
2	12.12.12.1	0%	3	0.3ms	0.4
3	103.116.172.9	0%	3	0.3ms	0.4
4	10.40.1.1	0%	3	0.5ms	0.5
5	43.240.229.201	0%	3	0.5ms	0.5
6	72.14.194.182	0%	3	12.1ms	12
7	108.170.240.161	0%	3	12.4ms	12.4
8	108.170.232.171	0%	3	12.3ms	12.3
9	8.8.8.8	0%	3	12.2ms	12.2

From the results of the traceroute above, it appears in the first hop leading to IP 22.22.22.1 where the IP address is the IP address of the border IIX routers. Then, the second hop leads to the border transit IP address 12.12.12.1. From these results, it can be concluded that when the vlan-id 100 or main path was deactivated, the path from the distribution router towards IP 8.8.8.8 switches automatically through the border IIX router or backup path.



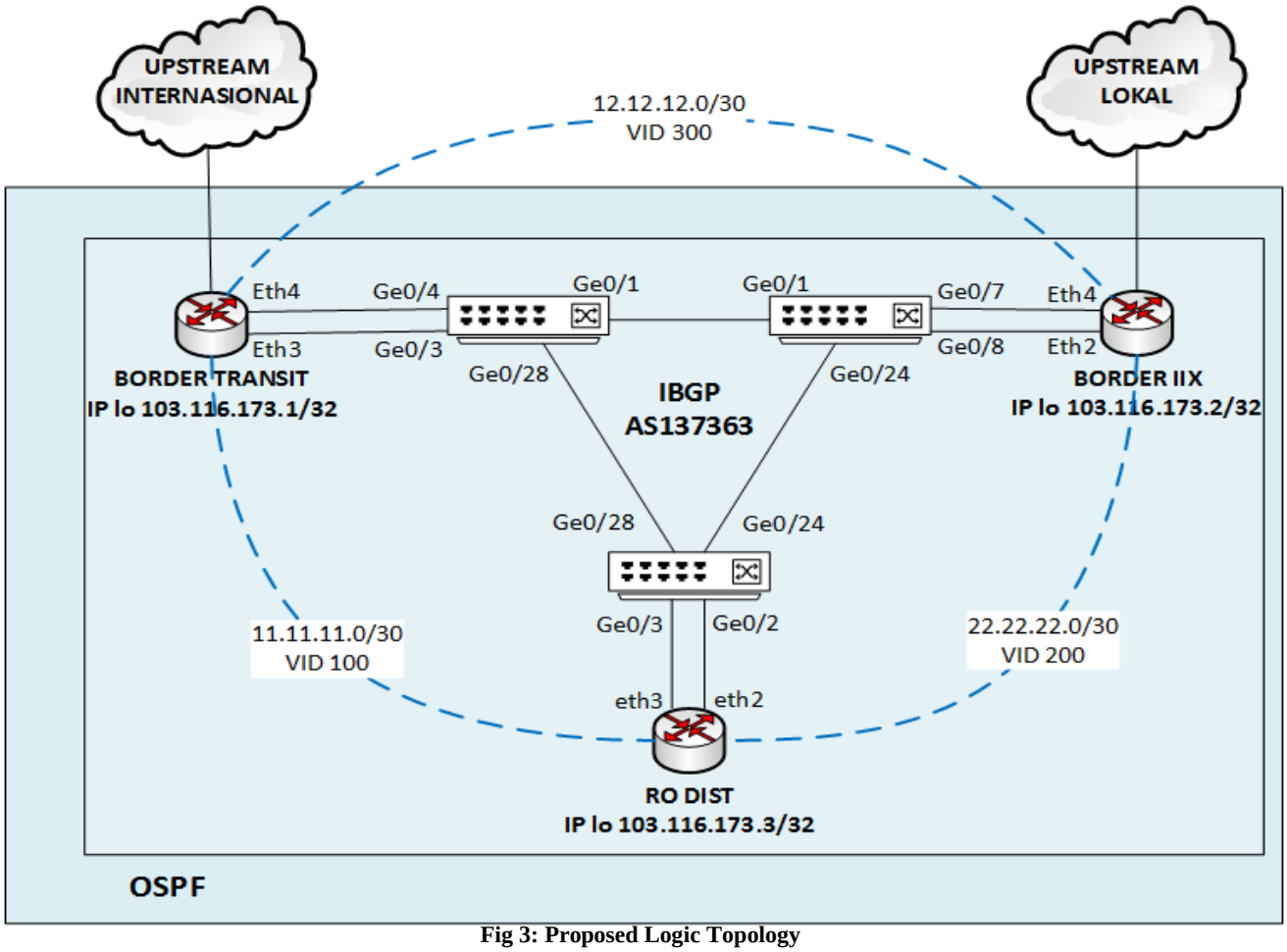


Fig 3: Proposed Logic Topology

6. CONCLUSION AND FUTURE WORK

The conclusion of this study is that the failover system was implemented using the OSPF and IP loopback protocols running well and has a positive impact on the Internal BGP network, which can move the Internal BGP connection path within 3 seconds and BGP status remains established when the main line is experienced breakdown.

For the use on large scale networks that also require greater throughput, it is recommended to use upper middle class devices such as Cisco using the EIGRP protocol.

7. ACKNOWLEDGMENTS

The author would like to thank Mercu Buana University and PT. Quanta Tunas Abadi who support this research.

8. REFERENCES

[1] B. Rifai and E. Supriyanto, "Management System Failover Dengan Routing Dinamis Open Shortest Path First Dan Border Gateway Protocol," J. Ilmu Pengetah. Dan Teknol. Komput., vol. 3, no. 1, pp. 39–46, 2017.

[2] T. Ernawati and J. Endrawan, "Peningkatan Kinerja Jaringan Komputer dengan Border Gateway Protocol (BGP) dan Dynamic Routing (Studi Kasus PT Estiko Ramanda)," Khazanah Inform. J. Ilmu Komput. dan Inform., vol. 4, no. 1, pp. 35–41, 2018.

[3] V. Vetriselvan, P. R. Patil, and M. Mahendran, "Survey on the RIP, OSPF, EIGRP routing protocols," Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 2, pp. 1058–1065, 2014.

[4] S. Shewaye and S. Mahajan, "Survey on Dynamic Routing Protocols," Int. J. Eng. Res., vol. 5, no. 1, pp. 10–14, 2016.

[5] A. Verma and N. Bhardwaj, "A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol," Int. J. Futur. Gener. Commun. Netw., vol. 9, no. 4, pp. 161–170, 2016.

[6] S. Y. Jalali, S. Wani, and M. Derwesh, "Qualitative Analysis and Performance Evaluation of RIP, IGRP, OSPF and EGRP Using OPNETTM," Adv. Electron. Electr. Eng., vol. 4, no. 4, pp. 389–396, 2014.

[7] H. Antoni Musril, "SIMULASI INTERKONEKSI ANTARA AUTONOMOUS SYSTEM (AS) MENGGUNAKAN BORDER GATEWAY PROTOCOL (BGP)," J. Nas. Inform. dan Teknol. Jar., vol. 2, no. 26181, pp. 1–9, 2017.

[8] O. P. D. Anggorowati, M. T. Kurniawan, and U. Y. K. S. H, "Desain Dan Analisa Infrastruktur Jaringan Wireless Di Pdii-Lipi Jakarta Dengan Menggunakan Metode Network Development Life Cycle (Ndlc) Design and Analysis of Infrastructure Wireless Network in Pdii-Lipi Jakarta Using Network Development Life Cycle (Nd," Telkom Univ., vol. 2, no. 2, pp. 5811–5819, 2015.

[9] M. I. Alsaydia dan O. M. Alsaydia, " Analysis and Performance Evaluation of OSPF and RIP Routing Protocol Using QualNet, " International Journal of Computer Science and Information Technologies, vol. 4, no. 3, pp. 125-132, 2016.

[10] Darmawan and T. Imanto, " Analisa Link Balancing dan Failover 2 Provider Menggunakan Border Gateway Protocol (BGP) Pada Router Cisco 7606s, " Jurnal Teknologi dan Sistem Informasi, vol. 3, no. 3, pp. 326-333, 2017.

[11] Gede Putra Yasa W, I., Adian Fatchur R, and Yuli Christyono. "Desain dan Simulasi Internal Gateway Protocol (IBGP) Menggunakan Graphical Network Simulator (Studi Kasus Pada Jaringan Universitas Diponegoro)," Transmisi, Vol. 16, no. 1, pp. 20-25, 2014.

[12] N. Zidan and M. Hamarsheh, " Implementation of Border Gateway Protocol (BGP) Attributes, " International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 5, no. 2, pp. 74-79, 2016.

[13] M. Sadikin, R. Yusuf and A. Rifai D, " Load balancing clustering on moodle LMS to overcome performance issue of e-learning system, " TELKOMNIKA, vol. 17, no. 1, pp. 131-138, 2019.

[14] B. Yuliadi and A. Nugroho, " Rancangan Disaster Recovery Pada Instansi Pendidikan Studi Kasus Universitas Mercu Buana, " JURNAL TEKNIK INFORMATIKA, vol. 9, no. 1, pp. 31-39, 2016.