Fast-Recovery and Optimization Multipath Circuit Networks Environments Using Routing Policies Different Administrative Distance and Internal BGP

1st Hillman Akhyar Damanik
Faculty of Information Technology Budi Luhur University
Jakarta, Indonesia
hillman.akhyardamanik@budiluhur.ac.id

***Abstract*—Heterogeneity of Service Provider network connectivity on increasingly complex transmission networks and multilink transmission networks, so a link recovery system is needed that can minimize link and circuit link failures. Management of large distributed link connectivity and transmission line infrastructure with various business services that require link recovery systems when primary links fail or interrupt their paths. Increased internet and network coverage in terms of speed and cost efficiency of services to end-to-end latency, for customer service quality of service. The research objective was to implement and model Flexible Failover Using Routing Policies Different Levels of the BGP Hierarchy, for a Multipath environment for failure recovery processes with routing between BGP Autonomous System Internal and Policies Terms. Fast link failure and recovery mechanism in dealing with link failures and link congestion in service provider backhaul networks, at layer 3 and layer 2 by implementing BGP peering sessions with Routing Policies Different Levels of the BGP Hierarchy. The results obtained from the modeling that will be carried out in a multipath link environment, show and periodically generate the intervals obtained in the graph and test with the MRTG monitoring tool, have a direct average correlation with link failures. Failed link or node on primary link fails, secondary link is active and ready to perform recovery, then on tertiary link by selecting round-robin method to perform recovery. The process of removing the recovery link from the obtained results is 0-5.0-10 m/s.**

Keywords—i-BGP, Policy Subroutines, MEN, Match Prefix (Route Filters), Routing Policies

I. INTRODUCTION

I. INTRODUCTION

Fast recovery from link failure is a very popular topic in IP networks. Implementing fast recovery in Ethernet Networks is a complex issue because its implementation is based on the destination MAC address, which does not have the same hierarchical nature as that implemented in Layer 3 in the form of an IP network [1]. Ethernet business services and public cloud accesses have grown at a double digit rate over the last few years, and there is no end in sight of the development and pace of today's technology [2]. Offering lower cost-per-bit and bandwidth scalability, Metro-Ethernet's popularity is also driven by the unprecedented growth in network traffic. Metro Ethernet has been able to reproduce to meet these needs thanks in part to the MEF Forum's CE 2.0 specification. These standards enable providers to grow their business by linking their performance-assured services across local, regional, national, and international networks. In turn, the Metro-Ethernet (MEN) connectivity business service has to date been the fastest growing of all market segments for service providers on the network both in terms of the number of connection endpoints and volume of network traffic supported and to be deployed. Routing Policies Different Levels of the BGP Hierarchy with a combination of policy subroutines and internal BGP methods are modeled to minimize and develop fast recovery link, and convergence on networks and anticipate network failures at fast time intervals. In the BGP Internal Policy, a set of rules or policies has been provided, how to determine how the Autonomous System (AS) Number can direct the traffic process both when traffic enters and leaves the internet or between AS (Internal-BGP) numbers. Implementation of policy routing in research, with internal BGP protocol, where routes are selected and advertised with neighbors [3] [4]. Internal BGP peering session will be interconnected between two internal peers that have Autonomous System 45699 [5]. The BGP implementation method is used for two or more gateways when the packet originates from the source address, or for sending the packet to the destination in case of information exchange. ISP and NAP providers in using and utilizing the BGP protocol method are for the distribution of information, routes between domains to the internet [6] [7].

In this research we also present the Routing Policies of Different Levels of the BGP Hierarchy in the environment in the service provider's backhaul transmission, a test that will be carried out on AJN's corporate infrastructure. This research presents the modeling and routing protocol scheme for Layer 3 Internal Border Gateway Protocol (i-BGP) which is combined with a chain of route policy decisions and policies subroutines policy statement term on the sending process that forwards data traffic communications from the end point to the service provider router. Tolerance to connection errors is highlighted in challenges on multipath or multilink networks. Internal BGP methods and concepts and the decision chain and route policy subroutines, will be used in the Metro environment and the results will provide reliability in ensuring the delivery of user traffic. The implementation of this routing policy will outline the failure technique and link recovery process intervals and to provide link reliability for multipath networks as well as to provide network scalability and performance. The AS Number value used is ASN 45669.The technique used to test and analyze the results of link failures on primary, secondary and tertiary links will be carried out with the sub-interface port setup process. The testing technique is done by disabled and deactivated each sub-interface port, assuming that the configuration has failed. It then sends an echo reply (ICMP) packet on each link with 40Mbps of traffic coming from the remote customer. The test phase and test results will be

explained and displayed on MRTG, so that the results can be mapped in real-time and graphic. The topological in Figure 1 will be implemented for Routing Policies Different Levels of the BGP Hierarchy.

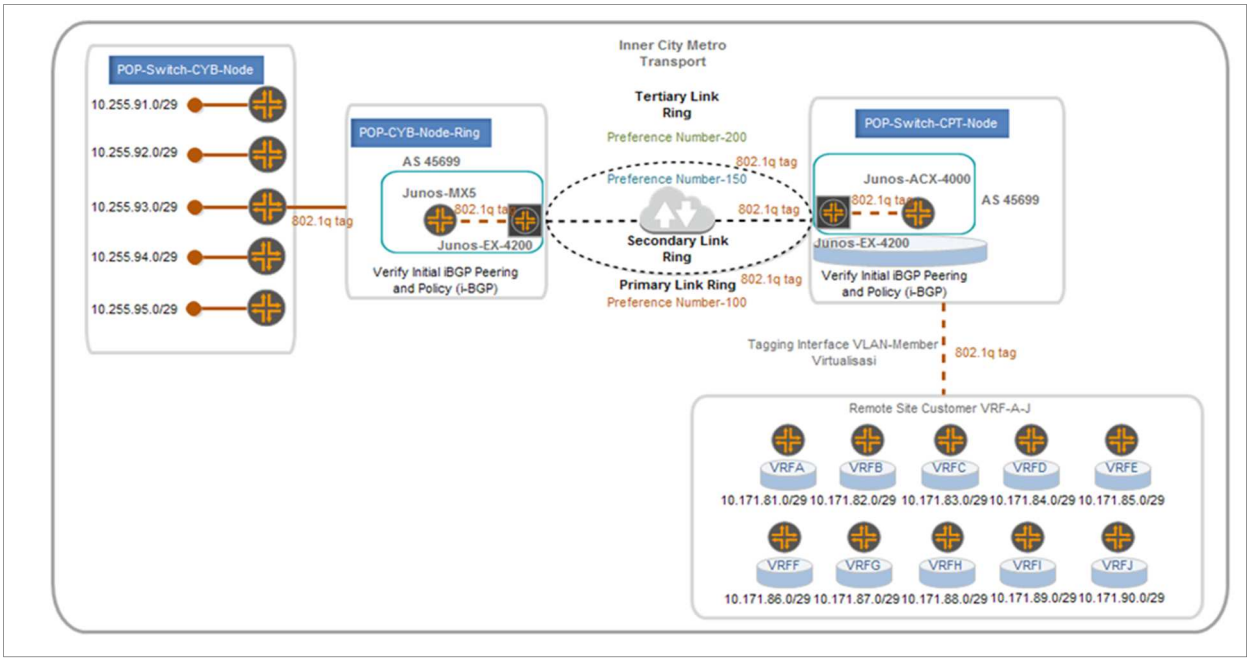

Figure. 1. Topological Physic Design and Modeling Flexible Failover

II. PROPOSED METHOD AND CONFIGURATION SCHEME

The design and modeling of architectural systems in this study uses real tools intended to test whether the theories and algorithms on the internal Border Gateway Protocol (i-BGP) and policy subroutines can be combined with the following models and schemes [8]:

- Verify that the next hop can reach the destination to carry remote site traffic by selecting the link path with the lowest preference value (routing protocol process preference) can select routing first even if other preferences are active or operational.
- Traffic routing that has failed (link down) will recover (for example, because the primary link is down by a routing policy or because the next hop is inaccessible) which has a preference of 100 will overwrite a higher preference (Preference secondary link with a value of 150) and so next until another preference value is specified.

Design and modeling architecture is also in order to handle and adapt to dynamic prefix address conditions. Designing and modeling of architectural systems also requires a server that functions as a bandwidth usage traffic analysis for ICMP packets when the link is down or fails [9] [10] [11]. Router RB-951Ui-2HND will enable remote site device, later on this device will be configured as many as 10 remote site customers virtually using VLAN-ID. And each remote site will be configured with an IP address with the subnet prefix /29. Furthermore, the remote site customer uplink backhaul device will be used by the Router RB1100 device. In this device, 5 IP addresses will be configured as the main backhaul for the 10 remote sites. Between remote site and Core edge remote site will pass the metro service provider link which is modeled by Multipath link.

Design and modelling of architectural system on physical devices, use are real devices intended to test. Device specifications will be described in table 1 below.

TABLE I. Hardware instrument Design and Specifications

Hardware Instrumentation Design and Specifications	
Hardware	**Device Function**
JUNOS ACX4000 and JUNOS MX5	- Session peering BGP internal. - Evaluating complex cases using policy chains and subroutines, route filter and routing policy match conditions
RB951Ui-2HND Router	Remote Customer Site
RB1100 Series	Backhaul Customer Site
Server Monitoring System	System Monitoring Tool MRTG Cacti (Traffic inbound and Outbound)

A. Scheme Route Policy Chain and Subroutine

Route policy chain shows how the routing policy chain is evaluated. This routing policy consists of several terms. Each term consists of conditions and a match action to be applied to the matched route. Referring to the policy routing policy subroutine yields the final result of true or false via matching and policy entry actions. Policy entry action "Accept" will evaluate to true, and policy entry action

"Reject" will evaluate to false. When the policy subroutine is configured to reject a route, the Accept action state can be used as a possible configuration in the subroutine's match criteria to return a correct match, and the reject action state can be applied in the main policy entry [12]. If a match is not found during the evaluation of one or more routing policies, the final evaluation will return the acceptance or rejection given by the default behavior based on the destination and or source import/export policy type. Modeling and the Route Policy Chain and Subroutine scheme in this study, functions as a routing policy matching process in the applied IBGP routing [13]. The modeling and techniques introduced to provide compatibility for each route will be combined with the routing policy match conditions, firewall filters, route preferences, chain policies, and policy statements, and are described in the flowchart representation in Figure 2 [15].

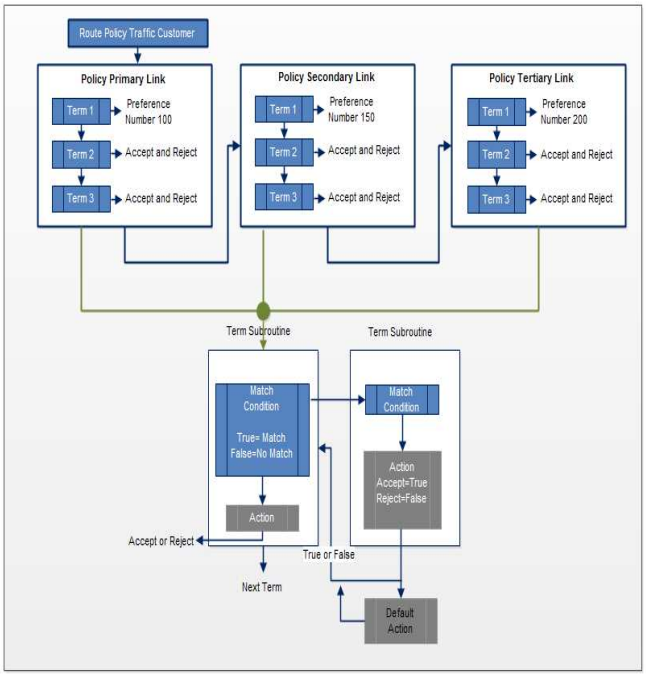

Figure. 2. Scheme of Route Policy Chain and Subroutine in Multipath Metro Environment

B. Failover Scheme Configuration

The main objective of this research is to provide the results of how the failover function is available in the Carrier Ethernet Backhaul (Metro-E) on the circuit link path of the Service Provider (SP) [15]. Topology scheme design and configuration to be modeled originates from remote sites VRF A to VRF J, passes through i-BGP filtering process and policy subroutines to service providers and goes to Backhaul customer sites that have been allocated. Then the bandwidth allocation on the backhaul carrier ETHERNET on the circuit link path at the Service Provider (SP) is 40 Mbps. This pipe bandwidth width will carry traffic from the customer site to the customer's backhaul. Application Layer 2 802.1q tag is used to process the ongoing traffic to determine the route on the transmission line. Layer 3 service will carry all customer site traffic and process the running traffic to determine the route to the predetermined preferences, namely in preference 100 (primary link), preference 150 (secondary link) and preference 200 (tertiary link).

The detailed process can be seen and illustrated in Figure 3 below. The standard port configuration interface for each port will be tagged to carry traffic to the communication to be integrated with BGP internals. On the router side, AS numbers will be allocated to each link group primary link, secondary link and tertiary link with each AS number is 45699. Internal BGP work process will function as a failover link and will be managed by internal BGP peering sessions and policy subroutines with preference value.

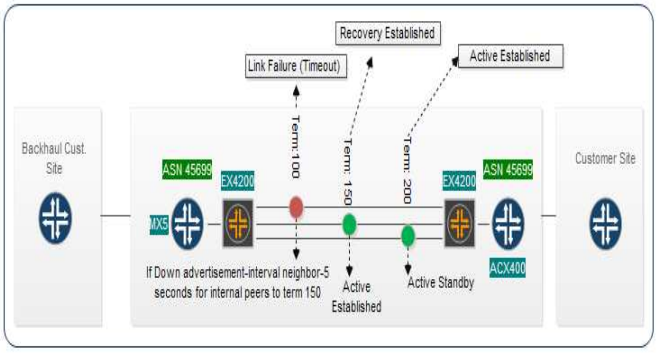

Figure. 3. Design and Modeling of customer site to edge core Failover Carrier System on the circuit link path

Testing will provide specific results and find out how the failover function is implemented on Metro-E links, especially on Service Providers (SP), by applying and combining Layer 2 (802.1Q Tag) and Autonomous System Internal (I-BGP). The testing process and results analysis, from network failures on the primary link, secondary link and tertiary link will be simulated by performing, on each of the sub interface ports (JUNOS ACX4000 and JUNOS MX5): ge-0/0/0.261, ge-0 /0/0.262, ge-0/0/0.263 and ge-1/1/0.261, ge-1/1/0.262, ge-1/1/0.263. There are several tests that can be done, in this research test, we tested the link failure on the failover technique by sending an echo reply (ICMP) packet, deactivating the port (deactivate). The first test step is to port (disable) the sub-interfaces (JUNOS ACX4000 and JUNOS MX5).

TABLE II. Routing Rules and Priority Rules.

SRC AS 45699	DEST 45699	Distance Preference	Priority	Term
10.167.69.2/29	10.167.69.1/29	100	1	Primary Link
10.167.70.2/29	10.167.70.1/29	150	2	Secondary Link
10.167.71.2/29	10.167.71.1/29	200	3	Tertiary Link

Configuration design and network topological concepts that are modeled, for Multipath or multilink environments for failure recovery processes with routing between AS Numbers, the modeling and concepts that we have integrated in this research, present and implement fast-state link failure and recovery mechanisms in terms of handling link failures and connecting traffic. The route selection for the failover technique that is applied is based on several parameters,

namely the source-address and destination-address (neighbor) and the preference value.

Procedure:

First, the router on each Internal BGP peering group will choose the most specific routing rule with the DST-address neighbor with the result active:

```
10.167.69.1 45699 57306 56985 0 3 2w4d2h Establish
  inet.0: 0/2/0/0
10.167.70.1 45699 57306 56986 0 2 2w4d2h Establish
  inet.0: 0/2/0/0
10.167.71.1 45699 57306 56984 0 2 2w4d2h Establish
  inet.0: 0/2/0/0
```

Then, the router will see the value in the preference parameter of each internal routing rule-BGP group between neighbors, the smaller the preference value, the rule will be used. The operational preference value is 100.
If, there are several routing rules with a specific DST-address and a similar preference, the router will select Random (round robin). This research paper aims to provide specific results and find out how the failover or link redundancy function is applied to the backhaul of a provider or Service Provider (SP), as a technique that can be used for the sustainability of backhaul nodes, in guaranteeing Network Availability and Level Agreement to customers, with implementing Policy Subroutines and IBGP techniques.

The sequence of steps that must be carried out in the test is:

- term preference (value preference = 100): link port main interface configuration is disabled: ge-0/0 / 0.261. Traffic will be monitored within that time period, whether the traffic will immediately switch to the secondary link.
- term preference (value preference = 150): main interface configuration disables link ports: ge-0/0 / 0.262. Traffic will be monitored within that time period, whether the traffic will immediately switch to the tertiary link.
- term preference (value preference = 200): Main interface configuration disables link ports: ge-0/0 / 0.263. Traffic will be monitored within that time period, whether the traffic will move to the main link. When the main link is in a state and status up. If the link or interface node fails, the link active state (Up) will perform a recovery.

C. Circuit Ethernet Ring Transmission (802.1Q in 802.1Q) for Primary, Secondary and Tertiary Links Scheme

The 802.1Q tag for the primary link is applied to the Junos EX 4200 Switch. The 802.1Q tag is useful for transmitting Layer 2 metro Layer 2 802.1Q tag, used to process traffic customer to determine the route on the transmission line.

- The process of configuring and implementing the 802.1Q tag for the primary link is applied to the Junos EX 4200 Switch.
- The 802.1Q tag is useful for transmitting Layer 2 (L2) metro links P2P for connectivity on the sub-interface from POP-Switch-CPT to POP-Switch-CYB.
- Application Layer 2 802.1Q tag, used to process customer traffic to determine the route on the transmission line.

```
user@POP-Switch-CPT> show configuration interface subinterface_vlan
    interfaces {
      ge-0/0/0 {
        vlan-tagging;
        unit 0 {
     description 802.1Q Tag Link;
          vlan-id vlan;
          family inet {
            address address;
       }
```

The 802.1Q tagged transmission virtualization. The configuration and implementation is modeled as shown in Figure 4.

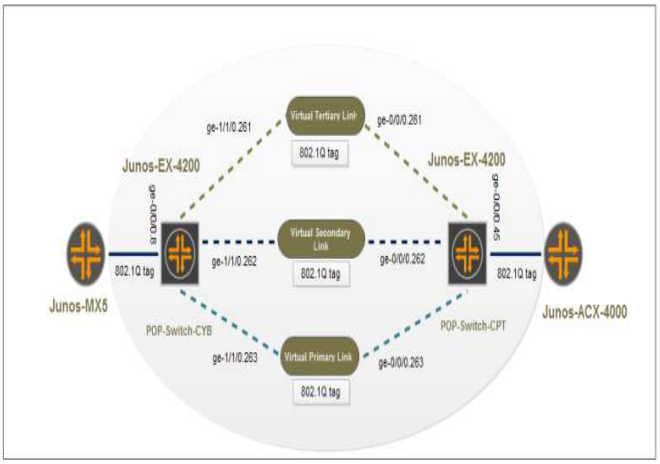

Figure. 4. Schematic and Modeling of 802.1Q tags in a Metro-Ethernet Multipath Environment

D. Internal Border Gateway Protocol (IBGP) Scheme

The standard configuration of interface ports for each port will be marked to carry traffic to the communication to be integrated with internal BGP. On the Junos ACX4000 and MX5 router, AS Number will be allocated to each primary link, secondary link and tertiary link group, 45699. The internal BGP working process will serve as a failover link and will be managed by the internal BGP peering session to represent route policy chain routing and subroutines.

The i-BGP peer verified initial route reflection will route customer traffic with the following scheme:

- Term 1 (preference 100) Junos-ACX-4000 router advertises customer traffic from routing peer-as 45699 with IP Address 10.167.69.2/29 to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.69.1/29.

- Term 2 (preference 150) Junos-ACX-4000 router advertises customer traffic from routing peer-as 45699 with IP Address 10.167.70.2/29 to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.70.1/29.
- Term 3 (preference 200) Junos-ACX-4000 router advertises customer traffic from routing peer-as 45699 with IP Address 10.167.71.2/29 to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.71.1/29.

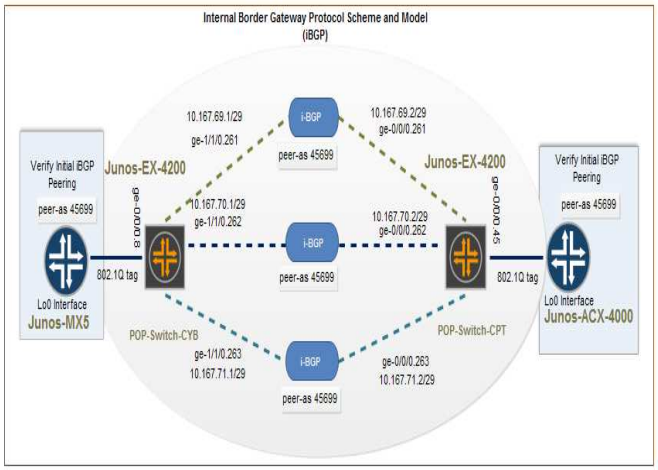

Figure. 5. Configuration Modeling and Implementation of Internal Border Gateway Protocol (IBGP)

Figure 5 shows the i-BGP peering Junos-ACX-4000 as an internal peer that is fully connected to the Junos-MX5. When a Junos-ACX-4000 router advertises a route to Junos-MX5, the Junos-ACX-4000 router established its neighbor advertisements, which in turn, established the route to the remaining routers within the AS. Route reflection allows routes to be propagated AS.

- Junos-ACX-4000 router advertises a route to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.69.0/29.
- Junos-ACX-4000 router advertises a route to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.70.0/29.
- Junos-ACX-4000 router advertises a route to Junos-MX5 with peer-as 45699 via IP Address on subnet 10.167.71.0/29.

```
</neighbor>
</group>
<group>
<name>i-BGP-Metro-Primary-Failover-Link</name>
<type>internal</type>
<peer-as>45699</peer-as>
<neighbor>
<name>10.167.69.1</name>
</neighbor>
</group>
<group>
<name>i-BGP-Metro-Secondary-Failover-Link</name>
<type>internal</type>
<peer-as>45699</peer-as>
<neighbor>
<name>10.167.70.1</name>
</neighbor>
</group>
<group>
<name>i-BGP-Metro-Tertiary-Failover-Link</name>
<type>internal</type>
<peer-as>45699</peer-as>
<neighbor>
<name>10.167.71.1</name>
</neighbor>
```

The scripting excerpt above from the configuration and implementation of the Internal Border Gateway Protocol (iBGP) for each link, primary link, secondary link and tertiary link is applied to the Junos ACX-4000 router. The internal BGP workflow will act as a failover link and will be managed by the AS 45699 internal BGP peering session to represent the routing of the route policy chain and subroutines.

Referring to the policy subroutine route result of True or False through policy entry matching and action. The accept policy entry action evaluates to True, and the reject policy entry action evaluates to False. When a policy subroutine is configured to reject a route, the accept action state can be used as a possible configuration within the subroutine match criteria to return a true match, and the reject action state can be applied in the main policy entry.

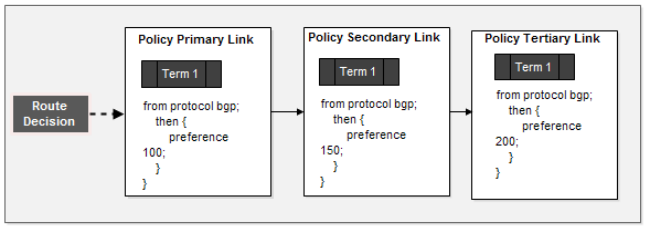

Figure. 6. Route Policy Chain and Subroutine Modeling and Schematic

III. TESTING AND ANALYSIS INTEGRATE POLICY SUBROUTINES AND INTERNAL BORDER GATEWAY PROTOCOL

A. Data Rate Primary, Secondary and Tertiary ∑ (Receive Inbound Traffic and Outbound Traffic).

1. Primary Link ∑ (Receive Inbound and Transmit Outbound)

Figure 4 (MRTG Cacti) shows the date 2021/08/12 at 20:16:30. Traffic (incoming and outgoing traffic) on the primary link (preference 100), traffic drop traffic on 10/12/2020 at 20:16:30. Simulation is done by disabling the port (ge-0/0 / 0.261) on the primary link. Then the BGP Protocol will detect a failure on the primary link. First, the router on each Internal BGP peering group will choose the most specific routing rule with the neighbor address of the destination with the result active (Up/Up). Then internal BGP through the policy preference value will see the value in the preference parameter of each internal group routing

rule-BGP between neighbors, the smaller the preference value, the rule to be used.

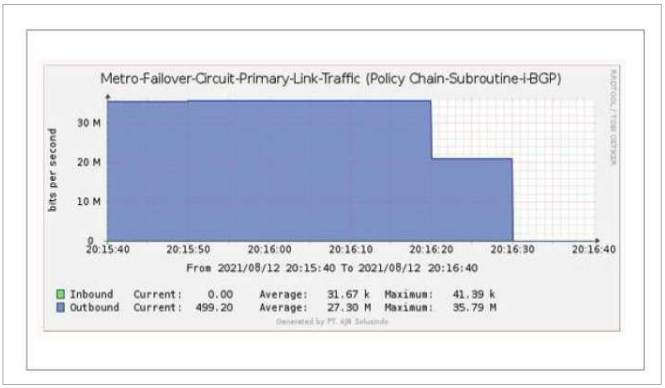

Figure. 7. ∑ Graph of traffic index data rate traffic primary link (process drop link: 20:16:30)

Figure 5 (MRTG Cacti) shows that in 2021/08/12 at 20:16:20, the secondary link line has received traffic graphs inbound as well when the primary link has decreased traffic/drop or a down status on the interface (ge-0/0/0.261). Received traffic reaches 20 Mbps at the same time when the main link traffic drops at 20:16:20 and at 20:16:30 the traffic on the secondary link has reached 40 Mbps in 5 seconds. Then at 20:16:40 the traffic on the secondary link has reached 40 Mbps, with the total allocated bandwidth. When the secondary link is active, it does auto recovery of traffic from the primary link.

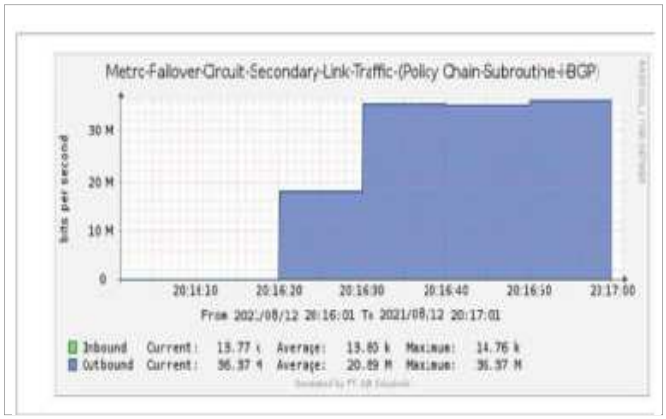

Figure. 8. ∑ Graph of traffic index data rate secondary link

Figure 6 (MRTG Cacti) below shows the test was carried out on 2021/08/12 at 20:22:20 secondary link line, deactivated (disable port) the ge-0/0/0.262 interface. Traffic (incoming) on the secondary link path (preference term 150) will experience a drop in traffic (assumed to experience interference on the secondary Metro link). Drop the link on 2021/08/12 at 20:22:20 with disabled status (test with port shutdown). The BGP protocol and the term 150 preference value on the tertiary link will detect a failure on the neighbor link, namely the secondary link.

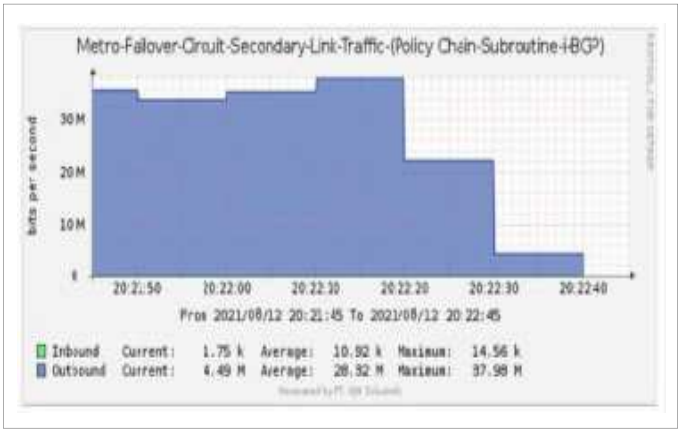

Figure. 9. ∑ Graph of traffic index data rate secondary link (process drop link)

Figure 7 shows that on 2021/08/12 at 20:22:20, the tertiary link has received traffic (inbound / incoming) at the same time when the secondary link has dropped traffic, this is done by disabled / deactivated port ge-0/0 / 0.262. The traffic on the received tertiary link reached 12 Mbps at the same time as the decrease in secondary link traffic at 20:22:20 and at 20:22:30 the traffic on the tertiary link reaches 30 Mbps in 10 seconds. Then at 20:22.40 the traffic on the tertiary link has reached 40 Mbps, with the total bandwidth allocated to the implemented multipath link.

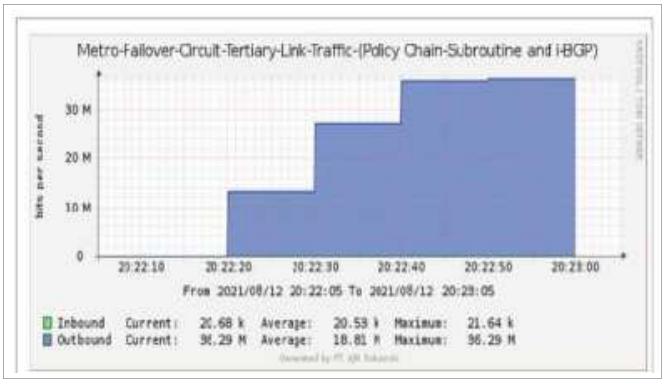

Figure. 10. ∑ Graph of traffic index data rate tertiary link (the tertiary link path has received traffic)

IV. CONCLUSION

Failure Recovery and Optimization Schemes by applying Routing Policies Different Levels of the BGP Hierarchy policy subroutines and Internal Border Gateway Protocol (IBGP), for failure detection on the redundancy path that has been integrated into this study, presents a link failure mechanism with fast conditions in terms of handling failed links, congestion and recovery processes at backbone service providers and customer companies. network (CE), to the core edge (PE) provider to the uplink CE, with testing in this research, will give specific results and find out how the failover function is applied to Metro-E backhaul, especially on Service Provider (SP), by implementing and combines Layer 2 (802.1) Q Tag) and Internal Autonomous System (I-BGP). Research testing can determine the learning process

of BGP's internal algorithm and policy subroutines, which exchange update packages with connected neighbors. Process if the error or link failure is found again, action will be taken and notification is sent to active neighbors. So that link recovery from primary link to secondary link and tertiary link does not take a long time, the link selection process will be carried out randomly with a round robin algorithm. The results obtained from the modeling that will be carried out in a multipath link environment, show and periodically generate the intervals obtained in the graph and test with the MRTG monitoring tool, have a direct average correlation with link failures. Link failure or node on primary link fails, secondary link is active and ready to perform recovery, then on tertiary link by selecting round-robin method to perform recovery. The process of moving the link recovery from the yield is only from 0-5 m/s to 0-10 m/s until the link that takes over is fulfilled. The process by which this value is obtained from the parameters of the CACTI monitoring chart which can be seen in each explanation and result obtained.

V. ACKNOWLEDGMENT

The author would like to thank the Directorate General of Higher Education (DIKTI) for providing financial support and assistance for beginner research, 2020.

VI. REFERENCES

[1] A. Pratap Naidu, M.V.R Maneesha. 2014. Fast Recovery from Link Failures in Ethernet Networks. International Journal of Research in Modern Engineering and Emerging Technology. (IJRMEET) ISSN: 2320-6586.

[2] Juniper Networks, Modified 2019, Capitalizing on the Fast-Growing Ethernet Business Services Market. (https://www.juniper.net/us/en/solutions/metro/metro-ethernet/, Access: August 2, 2019).

[3] Abu Hena Al Muktadir, Kenji Fujikawa, Hiroaki Harai, (2016). "Route advertisement policies for border gateway protocol with provider aggregatable addressing" High Performance Switching and Routing (HPSR) 2016 IEEE 17th International Conference on, pp. 42-48.

[4] Damanik, H. (2020). Scalable Resilient Internal BGP: Fast Recovery Mechanism Provide Multi-link Environment Carrier Ethernet Backhaul. In Proceedings of the 1st International Conference on IT, Communication and Technology for Better Life - ICT4BL, ISBN 978-989-758-429-9, pages 197-208.

[5] Vissicchio, S., Cittadini, L., & Di Battista, G. (2015). On iBGP Routing Policies. IEEE/ACM Transactions on Networking, 23(1), 227–240.

[6] Santhosh, S., Dakshayini, M., Tech, M., & Student, C. N. E. (2016). Effect of Route Reflection on IBGP Convergence and an approach to reduce convergence time, 4(8), 4530–4535.

[7] Imelda Ristanti Julia, Hendra Bayu Suseno, Luh Kesuma Wardhani, Dewi Khairani, Khodijah Hulliyah, Asep Taufik Muharram, "Performance Evaluation of First Hop Redundancy Protocol (FHRP) on VRRP HSRP GLBP with Routing Protocol BGP and EIGRP", Cyber and IT Service Management (CITSM) 2020 8th International Conference on, pp. 1-5, 2020.

[8] Usino, Wendi; Damanik, Hillman Akhyar; Anggraeni, Merry (2019). Improving Internal BGP Provide Fast Failover in Multihoming Environment Mobile Backhaul. Journal of Physics: Conference Series, 1201(), 012016–.

[9] Zhang, Y., Cao, C., Wang, J., & Tang, X. (2014). International Journal of Electronics and Communications (AEU) GPON-based transmission hierarchy for metro ring networks AEUE - International Journal of Electronics and Communications, 68(6), 528–533.

[10] Mliki, H., Chaari, L., & Kamoun, L. (2014). A Comprehensive Survey on Carrier Ethernet Congestion Management Mechanism. Journal of Network and Computer Applications.

[11] Medhi, D., Ramasamy, K. (2018) Network Routing (Second edition) Algorithms, Protocols, and Architectures. Pages 286-333.

[12] Moubarak, M. T., Elbayoumy, A. D., & Megahed, M. H. (2017). Design and implementation of BGP novel control mechanism (BGP-NCM) based on network performance parameters.

[13] Noor, A., Derisba, M., (2013). Fail-stop failure recovery in neighbor replica environment. The 3rd International Symposium on Frontiers in Ambient and Mobile Systems (FAMS). 1040 – 1045.

[14] Juniper Networks, Modified 2019,Understanding How a Routing Policy Chain Is Evaluated,[pdf],(https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-routing-policies-chain-evaluation-method.html, Access: August 2, 2019).).

[15] Alcatel-Lucent, 2019, Unicast Routing Protocols Guide R14.0.R1, [pdf], (https://infocenter.nokia.com/public/7750SR140R Access: August 2, 2019).