JPPI Vol 11 No 2 (2021) 121 - 136

Jurnal Penelitian Pos dan Informatika

32a/E/KPT/2017

e-ISSN 2476-9266
p-ISSN: 2088-9402

Doi: 10.17933/jppi.v11i2.338

Implementation of Backoff Algorithm Bidirectional Forwarding Detection (BFD) and MPLS VRF for Fast Recovery Mechanism End-to-End Multi-Circuit (E2E)

Hillman Akhyar Damanik [1] Merry Anggraeni[2]

Fakultas Teknologi Informasi Universitas Budi Luhur[12]
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta 12260[12] Indonesia

hillman.akhyardamanik@budiluhur.ac.id[1]

Received: 15 September 2021 ; Revision: 27 December 2021; Accepted: 27 December 2021

Abstract

Implementing and modeling a multi-circuit backbone technology in a service provider environment, for a multi-circuit link method with a fast recovery and redundancy process, is one of the most useful and promising developments and trends in building a policy system for mapping packet paths for future systems generation. The use of streaming video conferencing, mobile user devices and mobility, the shift from TDM networks to IP based, cloud computing services, smart cities, and the Internet of Things (IoT), and Content Delivery Network (CDN) are the main generators of growth. Failure mechanism and fast recovery of link failure in connectivity tested using liveness with minimum link primary value intervals (10), secondary links (20) and tertiary links (30). The smaller the interval value in the policy specified in the preference, the rule will be used or take the recovery path link action first. The process that will be experienced when the main link fails be connected or active on the secondary link. The learning process of the back-off algorithm then exchanges update packages with interconnected neighbors. The next process is 10 seconds to receive traffic from a failed link. The failure transfer link to the process will not take time, can be interpreted as a 0-1 process, and there is no packet drop and loss on the link that performs the recovery process.

Keywords: *BFD, MPLS, Failover, Availability, VRF*

INTRODUCTION

Bidirectional Forwarding Detection (BFD) is protocol that can be used for flexible connectivity, the back-off algorithm process contained in BFD is very high availability and quite simple, but too complex for some running applications to configure (Ahmed et al., 2017). Therefore it will be rarely used by the service provider for all its features and in many cases some parts will be omitted. In the concept of BFD technology you can set a timer for fast convergence, for example in MPLS it can be configured to use an off interval of only one or three seconds. The problem however is that all of these protocols were never really designed for sub-second failover. Hello packets contained in BFDs and such are processed by the control plane so there is some overhead. BFD is designed to be fast, the packets can be processed by multiple port interface modules or line cards so there is not much that can cause overhead.

The influence of the development of information and communication technology in all fields of activity and ways of human live, has formed more stringent requirements for indicators of reliability, high availability in handling and recovery of modern communication networks (Ahmed et al., 2017; Damanik, H, 2020).

Implementing and modeling technology in a service provider environment, for the Multi-circuit link method with the process of fast recovery and redundancy, is one of the most useful and promising developments and trends in building a packet path mapping policy system for the next generation. The use of video streaming, device and user mobility, the shift from TDM networks to IP, cloud computing services, smart cities, and the Internet of Things (IoT), Content Delivery Network (CDN) are the main generators of that growth (Anwar, 2019). For service provider network connectivity from core backbone to customers, network connection downtime of only a few minutes a month can cause huge losses, based on Service Level Agreement (SLA).

The this paper proposes a model and method that can support both certain infrastructure choices from real service provider networks, which originate from CPE (Customer Premises Equipment) Routers to Premises Enterprise (PE) Routers networks. Or it can be used on two different network gateway providers, for failure and recovery of links and nodes in link links. The methods and schemes in this paper, we study and present the impact of applying policies and rules on BFD, routing traffic in the Customer Premises Enterprise (CPE) environment through the PE network, by applying Bidirectional Forwarding Detection (BFD) and integrating it with the Multiprotocol Labeling Switching (MPLS) method, Multiprotocol Label Switching (MPLS), will engineer traffic patterns from CPE to PE by assigning short labels to network packets. The advantage with this paper model and scheme is that MPLS does not depend on any routing table or routing protocol and can be used for unicast packages (Wendi Usino et al., 2019; Siqueira et al., 2019; Ahmed and Nawari, 2016; Zemtsov, 2019).

Automatically BFD operation, will exchange the hello BFD packet at the specified time interval to detect failures and neighbor link errors, if they do not receive a reply after a predetermined interval. The configured BFD detection timer are 10 s (primary link), 20 s (secondary link) and 30 s (tertiary link) intervals interval. So the back-off algorithm will increase the reception interval at the transmission, from the BFD instance to the session flap (online: juniper.net, 2021). With the timer values already defined, we will analyze the direct average correlation with failure of links on the primary link, secondary link and tertiary link. So it will get:

- If a node failure primary link fails, then the secondary link is an active status and ready recovery.
- If a node failure in secondary link, tertiary is in the active status and is ready to recover.
- If a node failure in tertiary link, then primary link is active and ready to perform a recovery. and so on by choosing the round-robin method for recovery.
- When a link or interface node fails, the active status link (Up) will restore. The Figure 1 below shows the procedure for simulating and testing link and node failures and recovery.

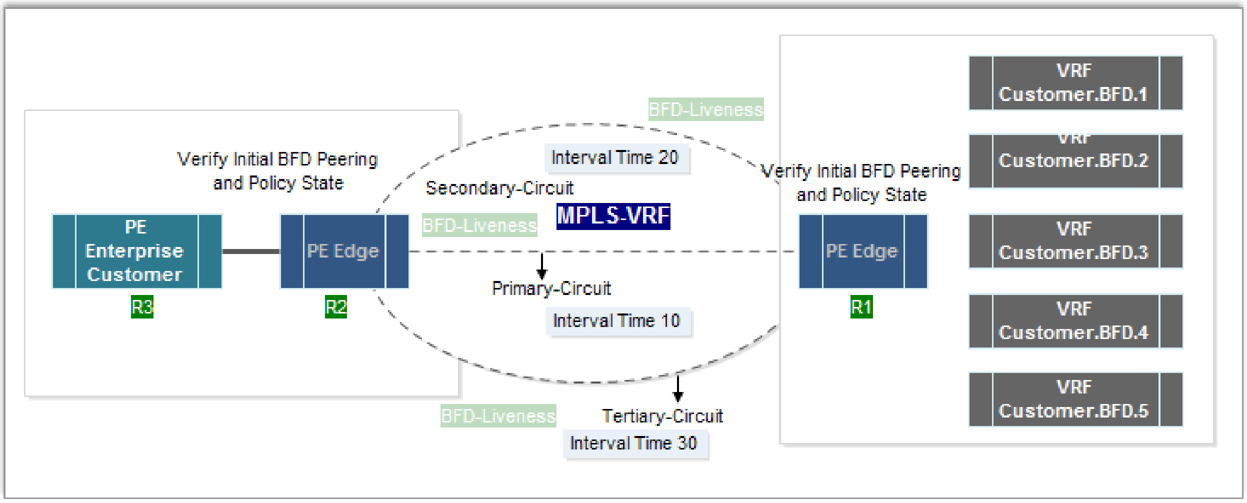

Figure 1. BFD Schema for BFD for Multi-Circuit Route path for Faster Failure Detection

METHODOLOGY

1. Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection Protocol (BFD) enables rapid detection of communication failures between neighboring device systems. In this paper BFD will implement a detection designed to provide fast forwarding path failure detection times for media types, topology, and routing protocols. In addition to detecting fast track forward failure failures, MFD provides a failure detection method that is consistent with implementing interval timers, so convergence times will be consistent and predictable (Muthumanikandan et al, 2017; Aijaz and Kulkarni, 2017).

Failures on each link are handled using a few sessions interval (30s) MFD which is managed by sending hello messages in the network of neighboring nodes. The neighboring node that matches the specified configuration can have clock a that is synchronized to detect failure (Kim et al., 2017). The BFD technique that will be proposed is as follows:

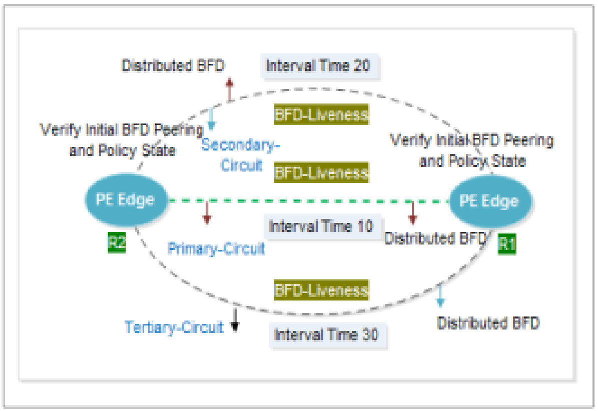

Figure 2 Architecture for providing BFD Fast Recovery Mechanism Provide Multi-Circuit

2. Multiprotocol Label Switching (MPLS) Schema

The labeling mechanism in the MPLS scheme allows network connectivity to improve routing path performance, thereby increasing service quality to data traffic (Tariq et al., 2015). The LDP (Label Distribution Protocol) core network service provider will segment labels between routers, where the signaling protocol runs on devices configured for MPLS support (Ravi et al., 2017).

In the schema applied in this paper, MPLS and LDP Configuration to start TCP packet exchange across LDP interfaces on the same port interface as the loopback interface. The packets will form a TCP-based LDP session to exchange MPLS information in the destination network, on a point-to-point interface (Yadav et al., 2017; Sun, 2013). Then in the MPLS scheme the criteria that must be met are:

- All traffic is forwarded by forwarding the standard IP from the Customer Edge (CE) router to the PE Edge router.
- PE Edge router will create an LSP over the network.
- PE Edge routers receive traffic from CE, and do a route lookup. The lookup will generate the next hop LSP, the LSP process will continue along the traffic.
- Traffic reaching the PE Edge router goes out, and the PE Edge router will bring up the MPLS label and resume traffic with the routing used.

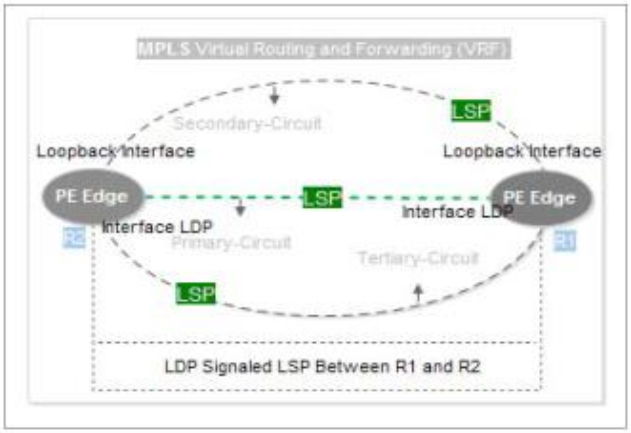

Figure 3. MPLS Fast Recovery Mechanism Provide Multi-Circuit

3. Virtual Routing Forwarding

One of the most important and highly available MPLS applications is VPN or Virtual Private Network which provides layer 3 protocol or VPN network layer for service providers that ensures private and secure transport of traffic from one customer to another with virtualized routing through the provider's network service. In supporting several customers who are at the provider and each customer requests a different service such as having a secure, reliable, private and fast connection, MPLS VPN has a concept called a Virtual Router called a VRF (Virtual Routing and Forwarding) table. The concept of VRF technology or Virtual Routing and Forwarding which allows routers to have multiple routing tables or multiple VPNs in router and at the same time because they are in the same router and with the help of VRF different subscribers can use the same IP address Subnet connect to the same MPLS service provider network (Yadav et al., 2016; Mehraban et al., 2018).

The concept of VRF (Virtual Routing Forwarding) Customer Edge (CE) - or as VRF-lite is a concept where PE functionality is extended to CE routers by virtualization. Multi-VRF routers can run and implement multiple routing protocol instances with neighboring routers with overlapping address spaces configured on different VRF interface instances (Chandana et al., 2017) Implementation of the routing instance interface is a collection of schemas of the routing table, parameters of the routing protocol and interface. Its purpose is to control information in the routing table.

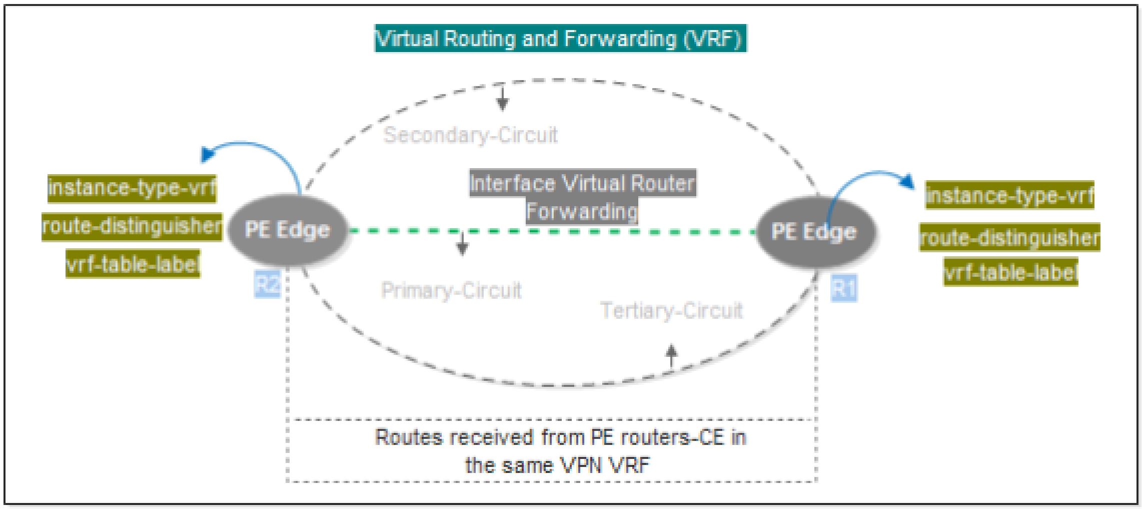

Figure 4. Virtual Routing and Forwarding (VRF) Schema

4. Hardware and Software Instrumentation

The integration design and system model and research design specifications are modeled as shown in table 1. The model network configuration design resembles end-to-end (E2E) connectivity from remote customer sites to the enterprise.

Hardware and Software Instrumentation

Hardware	Device Function	Software Monitoring
Junos ACX4000	Router PE	MRTG Cacti
Routerboard 450	Virtualisasi Remote Site Customer	
RB1100 Power PC	Router Enterprise Cutomer	
HP Lenovo Server	MRTG Cacti Monitoring	

IPv4 will be allocated as in table 2. Failover analysis for Peer IP Address will use number and term preference values. Table 2 contains some route rules and priority rules with multiple IP Peer BFD Addresses.

PE Edge R1 (Junos ACX4000)		PE Edge R2 (Junos ACX4000)	
Sub Interface	IP Address	Sub Interface	IP Address
ge-0/0/0.415	10.167.69.2/29	ge-1/1/0.415	10.167.69.1/29
ge-0/0/0.416	10.167.70.2/29	ge-1/1/0.416	10.167.70.1/29
ge-0/0/0.417	10.167.71.2/29	ge-1/1/0.417	10.167.71.1/29

Table 3 the configured BFD detection timer interval.

Interface	Term	Priority	Min Interval
Untagged	Primary Link	1	10
Untagged	Secondary Link	2	20
Untagged	Tertiary Link	3	30

The main concept of BFD operation is automatically, it will exchange hello BFD packets at specified time intervals to detect neighbor link failures and errors, if they do not receive a reply after a predetermined interval. The configured BFD detection timers are 10 seconds (primary link), 20 seconds (secondary link) and 30 seconds (tertiary link) intervals. So that the back-off algorithm will increase the reception interval on the transmission, from the BFD instance to the session flap [6]. With the timer values already defined, we will analyze the direct average correlation with link failure on primary, secondary and tertiary links.

The scheme and methodological application of this research paper is to study, propose, implement and develop a high availability failure policy on links, integrated in Multiprotocol Label Switching (MPLS) and Virtual Routing and Forwarding (VRF) in directing distribution and carrying backhaul traffic at a backhaul service provider service connectivity with policy statements in the link recovery process and link path failure link. The following is explained the methodology that will be applied is as follows:

5. Evaluating Match Bidirectional Forwarding Detection (BFD) Schema

The method to be used is to evaluate the complex connectivity on the service provider network by using a series of chains in the scheme, namely by determining 30 millisecond interval value, the detection time of the BFD session on the path link failure, determining the interval value at each hop on MPLS VRF. In table 4 shows how the link path routing policy will be evaluated. The routing process policy for failed link paths consists of several terms. Then each term consists of conditions and actions that are suitable to be applied to each match route, with the following policies:

Procedure: Value interval failure detection and actions to apply next hop:

- `Set` minimum acceptance interval value for failure detection on each routing path, including the minimum acceptance interval statement that is 30 milliseconds in the BFD configuration. This value will represent the minimum routing path interval for receiving replies from neighbors who are with it by creating a BFD session. Hierarchy level `[routing-optionsstatic route destination-prefix bfd-liveness-detection minimum-interval]`.
- `Set` detection time of the BFD session to adapt to the same value when the log message is sent. The detection time will be based on the `multiplier` of the minimum `receive-interval` and transmit-interval that is configured. Then the minimum acceptance interval value is 30 milliseconds and the `multiplier` is 3 (3 is the default value), the total detection time is 90 milliseconds.
- `Set` route with the `next hop`. Each subsequent route hop has a minimum-interval Bidirectional Forwarding Detection (BFD) value to be activated.
- `Set` PE Edge Router to have a route on each path with the next three possible hops. The next three hops are defined using the three hop statements that are on each VRF interface and are enabled for the three connection ends.

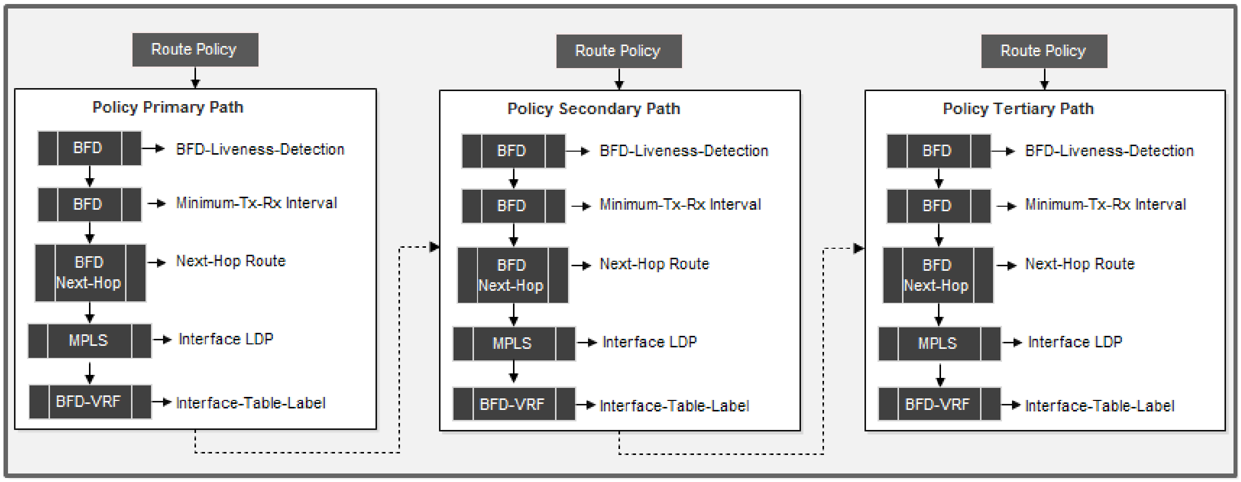

Figure 5. Proposed interval failure detection and actions schema

RESULT AND ANALYSIS

1. Configuration Collection of Match Prefixes (Route Policy Match Conditions) Scheme

BFD integration runs independently of other (routing) protocols. Once up and running, we will configure the MPLS VRF protocol to use BFD for link failure detection instead of the mechanism itself. When the primary link fails, the BFD will inform the protocol, and so on until the tertiary link.

Table 5 we set a timer for fast convergence, with the MPLS VRF configurable to use 10s (primary link), 20s (secondary link) and 30s (tertiary link) off intervals. Hello packets and such are processed by the control plane so there is some overhead. BFD is designed to be fast, the packets are processed by the three sub interfaces of the interface module or line card so there is not much overhead. When the link fails, BFD will inform the protocol. Here’s how you can visualize is:

```
protocols {
    mpls {
        interface interface;
        interface loopback;
BFD-Patch-Circuit {
instance-type vrf;
interface [sub-interface];
interface [sub-interface];;
interface [sub-interface];;
interface [sub-interface];;
route-distinguisher (as-
number:id|ip-address:id);
vrf-target target:(as-
number:id|ip-address:id);
vrf-table-label;

qualified-next-hop ip-address {
bfd-liveness-detection {
minimum-interval 10;
}
qualified-next-hop ip-address {
bfd-liveness-detection {
minimum-interval 20;
}
qualified-next-hop ip-address {
bfd-liveness-detection {
minimum-interval 30;
                    }
                    }
                }
```

2. Testing and Analysis Integrate Bidirectional Forwarding Detection (BFD) and MPLS VRF Fast Recovery Mechanism

The process of increasing Bidirectional Forwarding Detection (BFD) for the Fast Recovery Mechanism on the link path will provide a Multi-Link Environment Carrier Ethernet. Schema model specifications and topology configuration will be modeled as figure 6. Model design and topology scheme configuration will be modeled from the P2P PE router to each customer's CPE. The bandwidth allocation provided on the transmission link is 50 Mbps, this bandwidth will bring traffic to all customers to the backhaul router provider (ISP).

Customer Edge (CE) VRF (Virtual Routing and Forwarding) Applications - or as VRF-Lite - is a concept where PE functionality to customers is extended to CE routers by virtualization. Multi-VRF routers can run and implement multiple routing protocol instances with neighboring routers with overlapping address spaces configured on different VRF interface instances. Then integrated with Multiprotocol Label Switching (MPLS) and Virtual Routing and Forwarding (VRF) in directing distribution and carrying backhaul traffic in a service provider service connectivity with a policy statement in the recovery process link and path link failure. BFD services will carry all site traffic remotely. The detailed process can be seen and illustrated in Figure 6 below. Standard configuration of interface ports for each port will be marked to carry traffic to the communication that will be integrated with the BFD model. On the router side, BFD numbers will be allocated to each primary, secondary and tertiary link group.

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 service provider, by applying Bidirectional Forwarding Detection (BFD). The process carried out for testing and analyzing the results of link failures on primary, secondary and tertiary links will be carried out with configuration on each port sub-interface: ge-0/0/0.415,ge-0/0/0.416,ge-0/0/0.417. Some of the testing done is sending an echo reply (ICMP) packet and charging each link path with traffic that originates from a remote customer of 50Mbps. Table 6 sequence of steps to be taken in testing is:

- First term (Interval time=10): configure primary link port deactivate interface: ge-0/0/0.415. Traffic will be monitored in span of time, whether traffic will immediately switch to the secondary link.
- Second term (Interval time=20): Configure the primary link port deactivate interface: ge-0/0/0.416. Traffic will be monitored in span of time, whether traffic will immediately switch to the tertiary link.
- Third term (interval time=30): configure the primary link port deactivate interface: ge-0/0/0.417. Traffic will be monitored in span of time, whether traffic will immediately switch to the primary link. When the primary link is in a state and status up.
- When a link or interface node fails, the active status link (Up) will do the recovery.

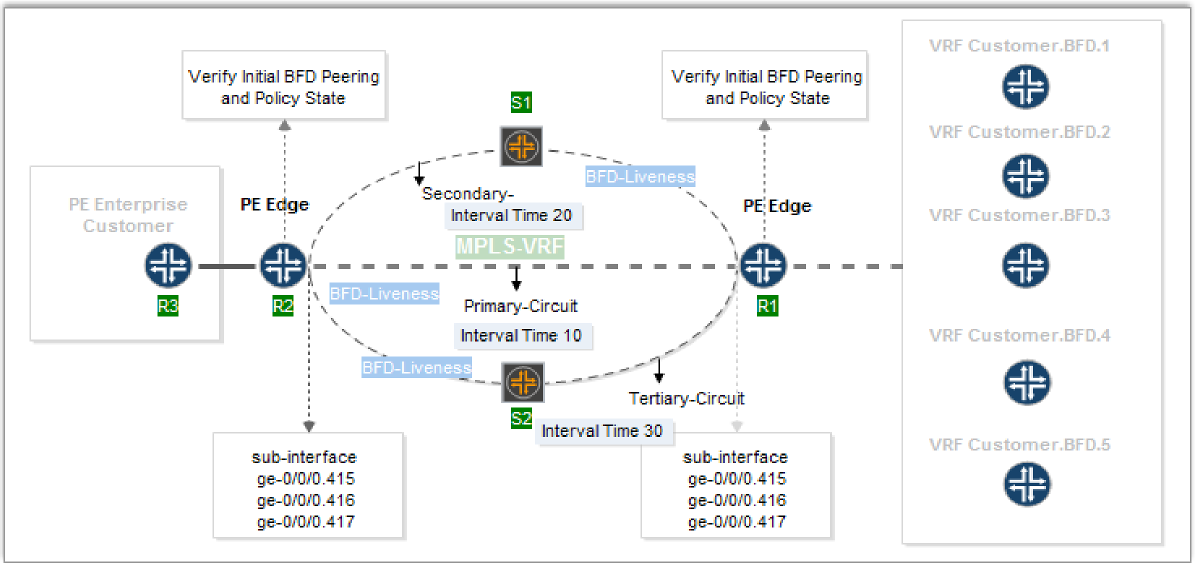

Figure 6. Integrate Bidirectional Forwarding Detection (BFD) and MPLS VRF Fast Recovery Mechanism Provide Multi-Circuit

The topology in figure 6 will perform the route selection process for failover and will be based on several parameters, namely destination-address (neighbor and peering) from R1 to R2. Table 7 the time interval values for each of these parameters have been explained as follows:

Functionality and Failure Recovery Procedure:

1. First Term: Peer Interface P2P IP Address in every router sub interface that peeks into select a routing rule with a specific value for destination address.
2. Second Term: IP Peer P2P router interface BFD address will be value in time interval (BFD-Liveness) parameters of each routing rule, the smaller the preference, the action will be used in the routing process.

Table 7 will explain the procedure for the link when it fails and the node between the testing process R1: ge-0/0/0.415 ge-0/0/0.416 ge-0/0/0.417 and R2: ge-1/1/0.415 ge -1/1/0.416 ge-1/1/0.417.

Table 8 procedure for the link R1: ge-0/0/0.415

```
R1:configure
Entering configuration
mode
:deactivate interfaces
ge-0/0/0.415
:show interfaces ge-0/0/0.415
##
## inactive: interfaces
ge-0/0/0.415
##
description
Primary-Link-Preference-
Interval-time 10
vlan-id 415;
family inet {
    address
10.167.69.1/29;
```

Table 9 procedure for the link R1: ge-0/0/0.416

```
R1:configure
Entering configuration
mode
:deactivate interfaces
ge-0/0/0.416
:show interfaces ge-0/0/0.416
##
## inactive: interfaces
ge-0/0/0.416
##
description
Primary-Link-Preference-
Interval-time 20
vlan-id 416;
family inet {
    address
10.167.70.1/29;

}

    }

}
```

Table 10 procedure for the link R1: ge-0/0/0.417

```
R1:configure
Entering configuration
mode
:deactivate interfaces
ge-0/0/0.417
:show interfaces ge-0/0/0.417
##
## inactive: interfaces
ge-0/0/0.417
##
description
Primary-Link-Preference-
Interval-time 30
vlan-id 417;
family inet {
    address
10.167.71.1/29;

}

    }

}
```

Table 11 Results of date and time of failover link implementation from primary link to secondary link.

Path	Date and Failure Time	Status	Status Recovery	Date and Time Recovery
Primary Link BFD-Liveness	2/26/2021 21:40	ICMP Timeout	Running Interval time 10	2/26/2021 21:40
Secondary Link BFD-Liveness	2/26/2021 21:43	ICMP Timeout	Running Interval time 20	2/26/2021 21:43
Tertiary Link BFD-Liveness	2/26/2021 21:44	ICMP Timeout	Running Interval time 30	2/26/2021 21:44

The testing steps and results will be explained and displayed in the Cacti MRTG, so the results can be mapped in graphical form and in real-time time and traffic will be seen. Some actual and real-time testing techniques, when a link or interface node fails, the secondary link will be recovered within a few seconds. The figure below shows the procedure for simulating and testing links as well as node failures and recovery.

The link failover implementation process will be carried out by performing a failure response time on the link, then it will be seen how long the response time will be when the link fails. Then all VRF BFD customers will send traffic simultaneously through the primary link (interval time 10). Interface ge-0/0/0.415 on R1 on the link serves to channel data traffic and other interface links as a backup if the main link (interval time 10) fails. Test transfer traffic and failover response time (ICMP Packet), will be tested how long the BFD failover response will take, or when the data path is moved from BFD-Liveness (interval time 10) to the second BFD-Liveness, with conditions, primary BFD-Liveness and BFD -Secondary liveness will be active.

Table 12 Procedure Send ICMP packets

Procedure:

- Send ICMP packets using the command "PING and COUNT = 10000" from the customer VRF BFD to neighbor R3 (PE-Enterprise Customer) as shown below, so that the timeout can be seen.
  ```
  Hostname: PE-Enterprise
  Customer: ping detail
  10.11.5.10 no-resolve rapid
  count 10000
  ```
- Term interval time 10 R1 lines (Primary Link) used to send ICMP packets to R3, type the command: `-traceroute monitor (IP Address PE-Enterprise Customer) source (IP Address BFD Customer.`
- At the same time, disable/deactivated is the primary link (interval time 10) as if the primary link is in an incorrect state or there is a disruption in its path, which is used to send ICMP PE-Enterprise Customer packets with the command type:

Table 13 configuration recovery link (automatic switching)

```
R1:configure
Entering configuration
mode
:deactivate interfaces
ge-0/0/0.415
:show interfaces ge-0/0/0.415
##
## inactive: interfaces
ge-0/0/0.415
##
description
Primary-Link-Preference-
Interval-time 10
vlan-id 415;
family inet {
    address
10.167.69.1/29;

}
    }
}
```

In the output below, sending ICMP packets from the main link path (interval time 10) i.e `10.167.69.2` changes using secondary link (interval time 20) line `10.167.70.2.`

```
>tool traceroute monitor 10.11.5.9
src-address 10.17.248.9
Tracing route to 10.11.5.9 over 10 max jump
1 1 ms 1 ms 1 ms 10.17.248.9
2 12ms 11ms 12ms 10.12.1.2
3 3ms 2ms 2ms 10.167.70.2
4 8ms 2ms 2ms 172.30.0.57
5 1ms 2ms 2ms 10.11.5.10
Trace complete.
```

At the same time the ICMP packet delivery command indicator will seen in R2, looks like command output above. A packet loss does not occur when there is automatic switching from primary link (interval time 10) to Secondary Link (interval time 20) by error.

Traffic flow testing will be carried out by VRF subscribers. BFD will send traffic simultaneously through the main link (10 intervals of time), each BFD customer will send TCP traffic of 10Mbps. The ge-0/0/0.416 interface on R1 on the link serves to pass data traffic and another ge-0/0/0.417 link as secondary if the primary link (10 time intervals) fails, and so on, the ge-0/0/ interface 0.417 (30 time interval) as a backup in case the secondary link (30 time interval) fails.

Table 14 show configuration customers BFD will send traffic. The traffic transfer test on the failover link test, will be tested how long the BFD failover response will last, or when the data path is moved from BFD-Liveness (10 time intervals) to the second BFD-Liveness, with the conditions, primary BFD-Liveness and Secondary BFD-Liveness will be active.

Procedure:

- At the same time, disable/deactivated is the primary link (interval time 10) as if the primary link is in an incorrect state or there is a disruption in its path, which is used to send TCP Packet PE-Enterprise Customer packets with the command type:

```
>tool bandwidth-test 10.11.5.10
protocol=tcp local-udp-tx-
size=1500 remote-udp-tx-size=1500
direction=receive local-tx-
speed=10M remote-tx-speed=10M
random-data=yes
```

The testing steps and results will be explained and displayed in the Cacti MRTG, so the results can be mapped in graphical form and in real-time time and traffic will be seen.

3. Data Rate Primary, Secondary and Tertiary ∑ (Receive Inbound and Transmit Outbound).

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

Figure 7 below shows 02/26 2021 at 21:40:50 traffic in and out on the primary link (interval 10), has decreased traffic and down on 02/26 2021 at 21:40:40 due to deactivate status. The BFD protocol will detect failures in the network, primary link (interval-time 10). In BFD operations, switching will exchange hello BFD packets at the specified 20-time interval, as a secondary link and detect neighbor failure (primary link) if, at 20-time intervals do not receive a reply, the BFD failure detection timer will provide faster failure detection.

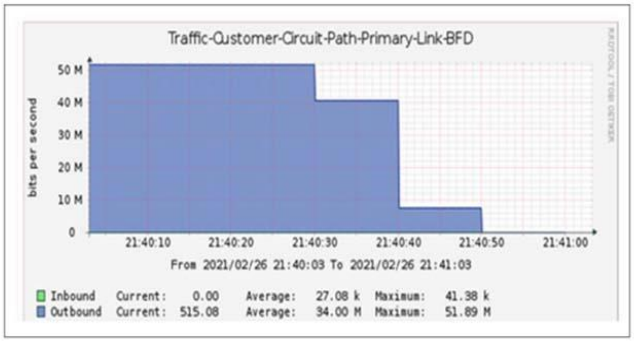

Figure 7 ∑ Graph of traffic index data rate primary link (process drop traffic)

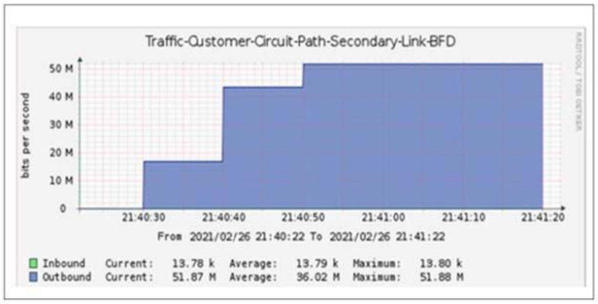

Figure 8 ∑ Graph of traffic index data rate secondary link

Figure 8 shows that on 26/02 2021 at 21:40:30, the secondary link path has received traffic (RX) at the same time, when the primary link has fallen traffic. Received traffic reached 20 Mbps at the same time that the main link had a traffic drop at 9:40:30 p.m. in 10 seconds at 9:40:40 pm the traffic on the secondary link has reached 40 Mbps in 10 seconds. Then at 9:40:50 p.m., traffic on the secondary link line has reached 50 Mbps, with the total bandwidth allocated.

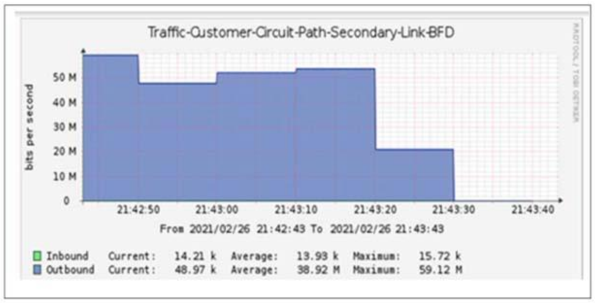

Figure 9 ∑ Graph of traffic index data rate secondary link (process drop link)

Figure 9 above shows the test done again on the secondary link path (interval time 20). On 26/02 2021 at 21:43:20. Incoming and outgoing traffic on the secondary link path (interval 20), experienced decrease in traffic (deactivated sub interface) and the traffic dropped on 6/02 2021 at 21:43:30. Due to disable status (test with shutdown sub interface). The BFD protocol on the tertiary link will detect failures in neighboring network, on a tertiary link (30 interval time).

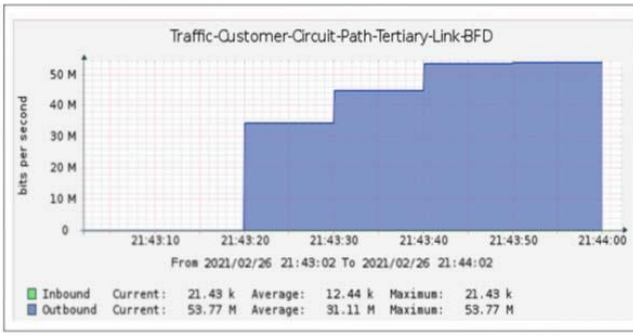

Figure 10 ∑ Graph of traffic index data rate tertiary link

Figure 11 shows that on 26/02 2021 at 21:43:20, tertiary link path has received traffic (RX) concurrently the time when the secondary link went down traffic. Received traffic reaches 30 Mbps. in seconds when the secondary link had a traffic drop at 9:43:20 p.m. Gradually at 21:43:30 the traffic on the tertiary link had reached 45 Mbps in 10 seconds. Then at 21:43:40, the traffic on the tertiary link has reached 50 Mbps, with the total bandwidth allocated.

CONCLUSIONS

The modeling and concept of detecting failure on a circuit link for path redundancy that we integrate into this paper presents a fast state link failure mechanism in terms of dealing with failed links, bottlenecks, and recovery processes in backbone service providers and customer enterprises (CE), to the backbone provider edge (PE) upwards to the CE uplink, by incorporating MPLS Virtual Routing Forwarding (VRF) with Bidirectional Forwarding Detection Mechanism (BFD). When the primary link experiences a link failure, each session (neighbor) in the Session BFD will return a secondary link, with a higher value after the BFD value of the primary link interval time 10, i.e. interval time 20 (secondary link), and so also when the secondary link fails, then the BFD Liveness of the tertiary link (interval time 30) will automatically restore the link. The results and modeling the results show that the average recovery time of the failure mechanism at each link is significantly faster for recovery. Processed to be experienced when the main link fails, the main link will be connected or active (created) on a secondary link and tertiary links. The process of learning the back-off algorithm then exchanges update packets with interconnected neighbors. The next process is 10 seconds to receive traffic from failed links. Transfer failure link to the process will not take time, can be interpreted as 0-1 second process, and no packets dropped and loston the link that performs the restore process.

REFERENCES

W Ahmed, O Hasan, U Pervez, J Qodir., "Reliability modeling and analysis of communication networks", Journal of Network and Computer Applications, 78, 191-215, 2017.

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.

Anwar, U. (2019). Performance Analysis and Functionality Comparison of FHRP Protocols. 2019 IEEE11th International Conference on Communication Software and Networks (ICCSN), 111–115.

Usino, W., Damanik, H.A., & Anggraeni, M. (2019). Improving Internal BGP Provide Fast Failover in Multihoming Environment Mobile Backhaul.

Siqueira, D., Pinheiro, T., Dantas, J., & Maciel, P. (2019). Dependability Evaluation in a Convergent Network Service using BGP and BFD Protocols. 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), 2378–2383.

R. Ahmed, E. Alfaki and M. Nawari, "Fast failure detection and recovery mechanism for dynamic networks using software-defined networking," 2016 Conference of Basic Sciences and Engineering Studies (SGCAC), Khartoum, 2016, pp. 167-170.

Zemtsov, A. (2019). Performance Evaluation of First Hop Redundancy Protocols for a Computer Networks of an Industrial Enterprise. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (Far East Con), 1–5.

Juniper Documentation (Understanding Bidirectional Forwarding Detection (BFD)), Feb 2021 [Online]. Available:https://www.juniper.net/documentation.

V. Muthumanikandan, C. Valliyammai and S. Harish, "Link Failure Detection and Alternate Path Tracing in OpenFlow Based Ethernet Networks," 2017 Ninth International Conference on Advanced Computing (ICoAC), Chennai, 2017, pp. 352-356.

Aijaz, A., & Kulkarni, P. (2017). Protocol Design for Enabling Full-Duplex Operation in Next-Generation IEEE 802.11 WLANs. IEEE Systems Journal, 1–12.

Tariq M. Almandhari, Fahad A. Shiginah," A performance Study Framework for Multi-protocol Label Switching (MPLS) Networks", 8th IEEE GCC Conference and Exhibition, Muscat, Oman, 1-4 February, 2015.

Ravi Kumar CV, Dhanumjayulu C, Bagubali A and Bagadi KP," Architecture for MPLS L3 VPN Deployment in Service Provider Network", Journal of Telecommunications System & Management 2017, 6:1.

Snehal Yadav and Amutha Jeyakumar," Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator", IEEE WiSPNET 2016.

Ming-song sun ,wen-Hao Wu,"Engineering Analysis and Research of MPLS VPN" IEEE 2013 Harban,China.

S. Yadav and A. Jeyakumar, "MPLS multi-VRF design and implementation using GNS simulator," 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, 2016, pp. 962-966.

S. Mehraban, K. B. Vora and D. Upadhyay, "Deploy Multi Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF)," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 543-548.

B. H. Chandana, P. Darsini and M. Devi Prasad, "Inter-Provider VPN network using back-to-back VRF and MP-eBGP method," 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, 2017, pp. 358-363.