SITEKIN: Jurnal Sains, Teknologi dan Industri, Vol. 21, No. 2, June 2024, pp.401 - 408
ISSN 2407-0939 print/ISSN 2721-2041 online

Implementation of Policy-Based Route and Failover with Netwatch Using Mikrotik Router on PT. Len Industrial

Werry Oki Sudi Wijaya[1], Syahril Rizal[2], Suryayusra[3], Dedi Irawan[4]
[1,2,3,4] Informatics Engineering Study Program, Universitas Bina Darma
l. General Ahmad Yani No.3, 9/10 Ulu, Seberang Ulu I District, Palembang City
Email: werrysudiwijaya@gmail.com, syahril.rizal@binadarma.ac.id, suryayusra@binadarma.ac.id,
dedi.irawan@binadarma.ac.id

ABSTRACT

Computer networks have now become a primary need for some people, be it to do work or other things. The same happened at the site office of PT. LEN Industri Palembang all employees are very dependent on public network connections or the internet to do work or communicate with sites or head offices. Sometimes the network is disrupted so that it does not allow employees to do their work. Therefore, researchers will implement policy-based route based failover which aims to separate traffic and also failover as a backup connection, this can be implemented using a built-in tool from MikroTik, namely Netwatch and also 2 ISPs that work in a way when ISP 1 experiences interference, traffic will be diverted to ISP 2 or vice versa and by using policy based route traffic on the network can be separated so that it is not Make the network choked or full traffic.

Keywords: *MikroTik, Policy Based Route, Failover, Netwatch*

Introduction

Currently technological advances are very rapid, especially in the problem of computer networks, where computer networks have now become the primary needs of every human who uses technology, as well as in using technology in the form of smartphones, computers, laptops and so on, where computer networks play an important role in the process of sending data between one device to another. Computer networks can be classified into several types, namely there are private connections and public connections [1]. Most users of smartphones, computers, laptops or other devices use public networks where they can connect to each other with users in other parts of the world. At that time computer networks play an important role, especially in terms of exchanging data and information [2].

Public networks are composed of many private networks that are connected to each other and make it a large-scale network, which is why one device can connect with other devices even though it is limited by long distances [3]. The protocol that connects these devices with each other is the Internet Protocol (IP) address, IP Address is categorized according to its place or divided into two, namely Private IP Address and Public IP Address, where the public network is composed of private IP addresses that have been configured in such a way as to connect to each other. IP addresses are owned by ISPs (Internet Service Providers) where if we want to use computer network services publicly we must subscribe or use services from ISPs [4].

Currently, public networks are widely used by all circles, as well as employees at the site office of PT. LEN Industries that use internet services as daily support at work, they usually use this internet connection to communicate between one site and another site besides that employees at the site office also use internet connections to conduct and monitor employee attendance and most critical employees at the site office take care of office administration every day including reports related to signaling obtained on that day to the head office. The use of the internet on the site office is usually there are approximately 25 users in one office, these users include technicians, engineers and office admins with different device variations, some use smartphones, laptops and also other electronic devices, all users are connected to the same internet network, both to access office work and access personal consumption such as social media and so on. Sometimes with that many users the network becomes slow.

The purpose of this study is to prevent or minimize the occurrence of problems in the network, especially if the network is disconnected or choked. By utilizing the failover method when the network is disconnected, the internet source will be redirected to the backup ISP and by applying the policy based route access method commonly used to do office work will be redirected to the backup ISP, it is expected to prevent difficulties accessing the office website due to the large number of users accessing the internet [5]–[7].

Research Methods

The research method that will be used in developing this network topology is the ADDIE method, the ADDIE development model as the name implies is a model that involves development stages with five development steps / phases including [8]: Analysis, Design, Development, Implementation and Evaluation. The ADDIE model was developed by Dick and Carry in 1996 to design a learning system [2].

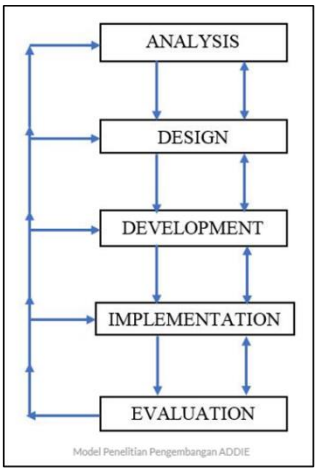

Figure 1 Research methods

Analysis

The first stage of this research first analyzes how the network conditions on the site office what are the needs and shortcomings of the site office, then it will be developed and improved through this research [9]–[14]. The needs of tools and materials needed in this study are shown in Table 1.

Table 1. Tools and materials

Tools and Materials	Specifications	Sum	Information
Laptop	Intel® Core™ i7 vPro Intel® HD Graphics 520 8 GB DDR4 14" FHD (1920 x 1080) SATA SSD 512 GB Windows 10 Pro	1 unit	Laptops play an important role in this implementation in the form of configuration, checking network connections, testing configuration results.
Mikrotik RB750Gr3	MT7621A 256 MB 8-30 V *License level* 4 RouterOS	1 unit	Mikrotik will manage the network that will be configured failover and *policy based route*
Access Point Ruijie RG-EW1200G PRO	2.4GHz: 400Mbps 5 GHz: 867Mbps *Support* 802.11a/b/g/n/ac/ac DC12V 1.5A 4 LAN *Ports* 10/100/1000M	1 unit	*Access Point* that will spread *Wi-Fi* signals to laptop and smartphone devices
ISP 1	50 Mbps	1 unit	ISP1 acts as the Main ISP
ISP 2	30 Mbps	1 unit	ISP2 acts as a Backup ISP

LAN Cable	2 Meters	3 units	On the *LAN port* on the proxy, *the access point*, ISP1 and ISP 2 will be connected directly using a LAN cable
	20 Meters	1 unit	
Winbox	*Version* 3.27	-	By using Winbox, you can configure the *Mikrotik* router with GUI *mode* quickly
Command Prompt	*Version* 10.0.19045.2604	-	Command prompt is used to check connections by using the "ping" and "traceroute" features

Design

At this design stage, developing the network that already exists at the site office of PT. LEN Industri Palembang by implementing several additions such as using 2 ISPs then implementing policy based route and failover [15]–[18]. The network design is shown in Figure 2.

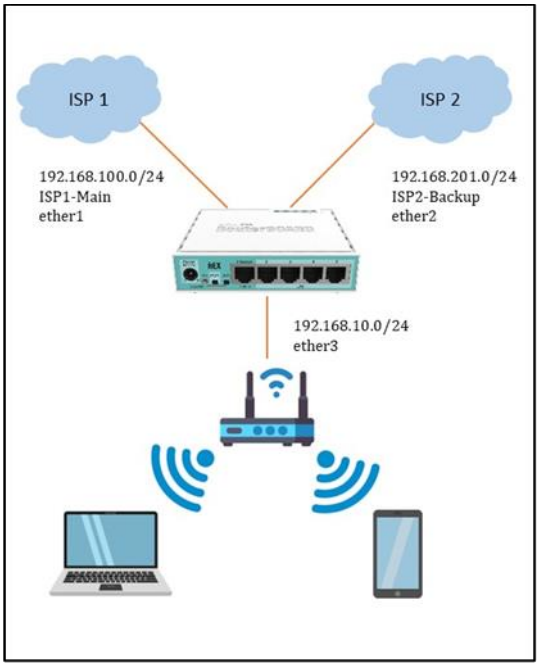

Figure 2 Topology Design

The design in Figure 2 of the two ISPs is connected to Mikrotik using a LAN cable then the internet connection obtained from the ISP will be processed by Mikrotik and spread again using an access point that is also connected using a LAN cable and the last wifi signal spread by the access point will be captured by the client.

Development

This failover uses additional tools, namely Netwatch which works by pinging continuously to a certain address, when the ping results show a time out, Netwatch will disable the routing currently used.

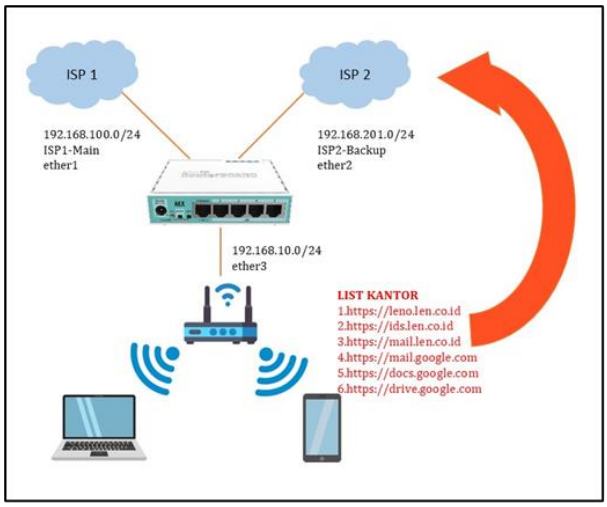

Figure 3 Policy Based Route schema

In addition to the failover method, this research will use one more method to secure the internet connection, namely separating the connection with the Policy Based Route (PBR) method which will work by filtering the office access list, if the traffic contains one of the office access lists, the traffic will lead to the ISP backup seen in Figure 3.

The routing concept used in this study is the default route, where ISP 1 with distance 1 while for ISP 2 using distance 2, Distance in routing serves to choose the path with the smallest value, if there are 2 similar destination lines, then the routing used is routing with distance 1 (ISP 1) and routing with distance 2 (ISP 2) as standby when routing on ISP 1 is off or not running, then ISP 2 routing will be active.

In addition, the routing concept used by researchers in this study is a routing mark that will lead to ISP 2, so that both ISPs continue to run simultaneously. This routing mark aims to mark any packets that pass through ISP 2, to mark these packets, the configuration point is on the mangle firewall, here the author marks 6 domains as shown in figure 3.4 then the 6 domains will be marked and will be directed to routing to ISP 2 with a distance of 1 so that when the user accesses the 6 domains will pass through ISP 2.

Results and Discussion

Implementation

The implementation stage is by configuring the basic IP Address of each ethernet port according to the topology that has been designed earlier.

1. Address=192.168.100.99/24 interface=ether1-ISP1
2. Address=192.168.201.99/24 interface=ether2-ISP2
3. Address=192.168.10.1/24 interface=ether3

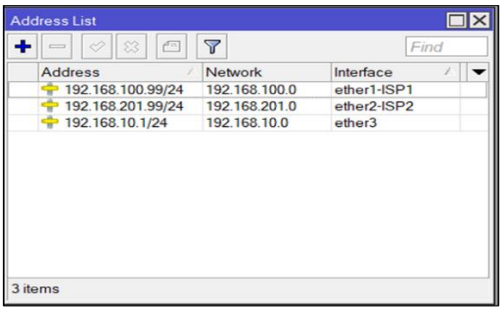

Figure 4 IP Address

On the firewall menu, mangle will add website addresses which will then be grouped into 1 to point to ISP 2, add action=add etc to address list chain=prerouting src. address list=IP Local etc. address list=! IP Local address list=List-Kantor content=leno.len.co.id to add another website is the same way, just change the content where it leads.

Add action=mark routing chain=prerouting src. address list=IP Local etc. address list=List-Office new routing mark=to-ISP2 for this configuration the purpose will redirect the office list to ISP 2.

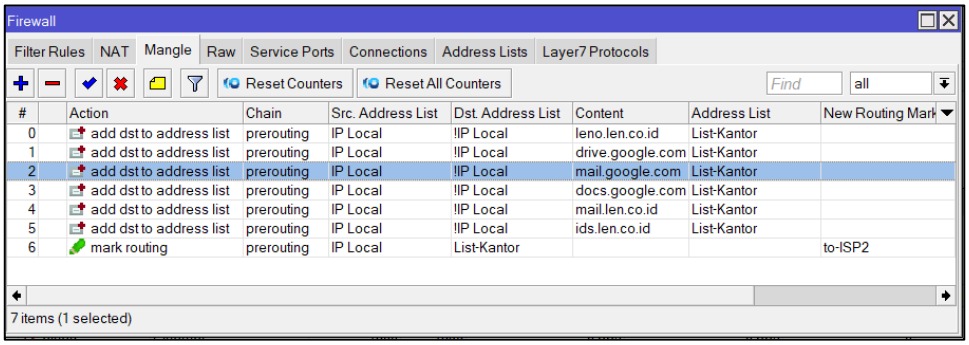

Figure 5 Mangle

In this routing section, which will redirect the mangle that has been made earlier to ISP 2.

1. etc. Address=0.0.0.0/0 gateway=192.168.100.1 distance=1 comment=Routing ISP1-Main this command as the default route that points to ISP 1 as the primary ISP
2. etc. Address=0.0.0.0/0 gateway=192.168.201.1 distance=2 comment=Routing ISP2-Backup This command is the default route that points to ISP 2 as the backup ISP
3. etc. Address=0.0.0.0/0 gateway=192.168.201.1 distance=1 routing mark=to-ISP2 comment=Routing PBR this command that says on the mangle menu has been created so that the access that has been listed earlier will lead to ISP 2
4. etc. Address=0.0.0.0/0 gateway=192.168.100.1 distance=2 comment=Routing Backup PBR this command as a backup when ISP 2 is down, the list on the mangle will point to ISP 1

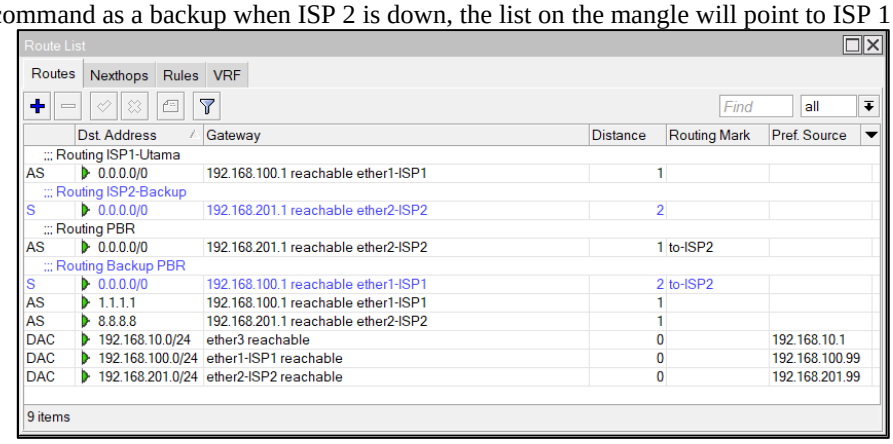

Figure 6 Route List

This netwatch tool will be in charge of monitoring by pinging the destination that has been set regularly, when ping is detected request time out then the netwatch will run a script down.

1. Host=1.1.1.1 up=/ip route set [find comment="ISP1-Main Routing"] disable=no down=/ip route set [find comment="ISP1-Main Routing"] disable=yes
2. Host=8.8.8.8 up=/ip route set [find comment="Routing ISP2-Backup"] disable=no down=/ip route set [find comment="Routing ISP2-Backup"] disable=yes
3. Host=8.8.8.8 up=/ip route set [find comment="Routing PBR"] disable=no down=/ip route set [find comment="Routing PBR"] disable=yes

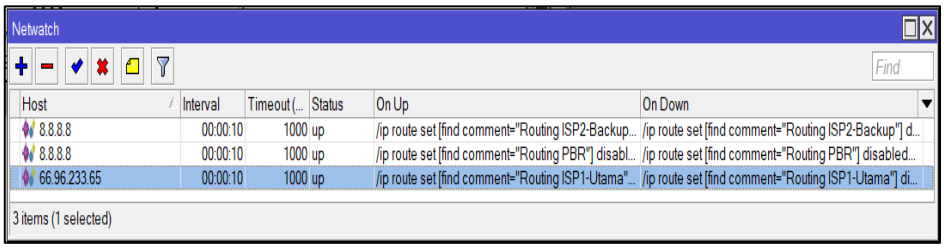

Figure 7 Netwatch

Evaluation

After implementing the topology that has been designed, there are several things that need to be done in order to test the performance of policy based route and failover.
The first attempt to tracert to the ids.len.co.id office list shows the goal is to bypass ISP 2 through ip address 192.168.201.1.

```
C:\Users\Thinkpad T460s>tracert ids.len.co.id

Tracing route to ids.len.co.id [103.233.146.13]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.10.1
  2    18 ms    27 ms    17 ms  192.168.201.1
  3    56 ms   221 ms   222 ms  192.168.121.90
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    78 ms    32 ms    72 ms  114.125.224.58
  8    44 ms    68 ms    52 ms  114.124.160.149
  9    89 ms    54 ms    48 ms  123.108.8.237
 10    43 ms    44 ms    68 ms  103.78.99.150
 11    83 ms    66 ms    76 ms  103.123.249.85
 12     *        *        *     Request timed out.
```

Figure 8 Tracert ids.len.co.id Results

On failover attempt when ISP 1 *Down* on the menu *Ping* Top view still *Replay* so *Tools* netwatch detect *Up*when *Ping* no replay then *Tools* netwatch will run the script *Down* towards *Routing* ISP 1. Then the whole load *traffic* to *internet* leads to ISP 2

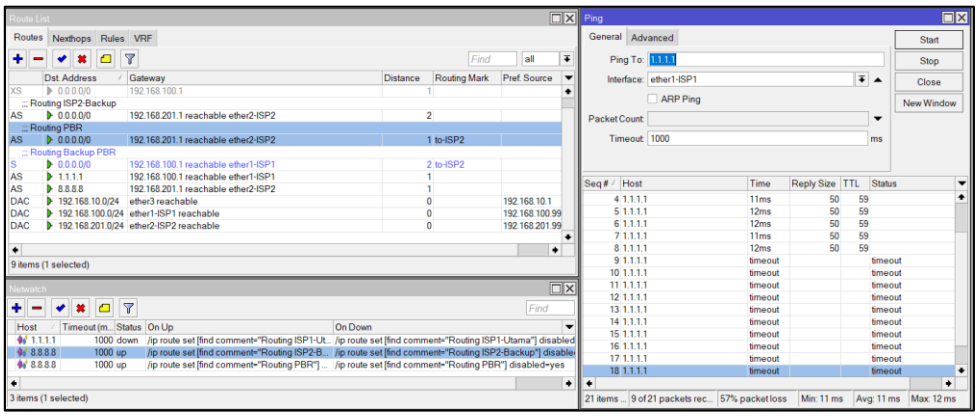

Figure 9 ISP Failover Test Results 1

Furthermore, the failover attempt when ISP 2 is down, *for how it works is still the same as ISP 1, it's just that when* ISP 2 is down *there are 2 scripts running will disable* routing *on ISP 2 and* PBR *routing*. When *PBR routing is off, the* routing *that will run is* PBR *backup routing*.

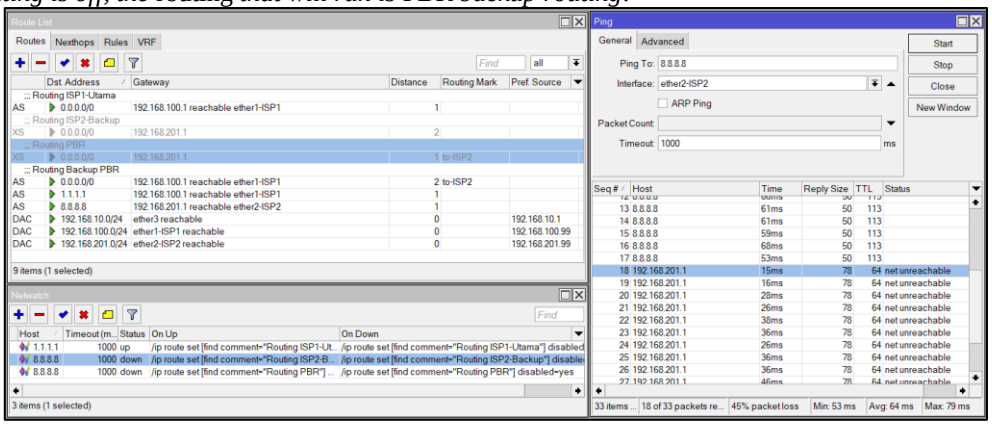

Figure 10 ISP Failover Test Results 2

After several experiments *policy based route*, where *List* The office that has been created earlier will pass ISP 2 so as to access *website* Office faster without overcrowding *traffic*, while connectivity through ISP 1 is only intended for access that is not on the mangle firewall list. This can be seen from the picture above where the three lists are listed on *mangle firewall* Namely mail.len.co.id, leno.len.co.id and ids.len.co.id, the results of experiments conducted using tools *traceroute* indicates that all websites point to ISP 2 as evidenced by passing IP 192.168.201.1 (ISP Gateway 2). As for website access other than the list on *mangle firewall*result *traceroute* leads to IP 192.168.100.1, which is *Gateway* from ISP 1.

As for the failover experiment that has been done, when ISP 1 is detected *request time out* by netwatch tools, Mikrotik will run *a disable script* on ISP 1 routing, *the result* is that all internet *access will be handled by ISP 2, while if ISP* 2 is detected down then there are 2 *routing* that will be *disabled* by *tools* netwatch is ISP 2 *routing* and *PBR Routing* so *internet* access will be handled all by ISP 1.

Here is the level of effectiveness of the two methods above, for failover to run well when one ISP is detected down, the netwatch tool will perform a disable command on the ISP routing that is down, so that the internet network can still run normally. As for the policy based route on the office list marking, namely 6 domains run well leading to ISP 2, but the access is only a little so that the connection used is only a little better subscribe to enough bandwidth to the ISP.

The shortcomings found by researchers are that when one of the ISPs goes down, the administrator must check directly on the device and also check on the configuration side, this has an impact on the down time of the related ISP, because before reporting interference to the relevant ISP, the administrator must check directly to the device.

Recommendation

Add features *Monitoring* In Mikrotik in the form of a telegram bot, the bot itself is a software that functions to execute commands that have been made by the administrator automatically and repeatedly. Telegram is an open source social media messaging platform that allows administrators to develop bots using the platform for free. The way the bot works is very simple, which only detects connections through ping that is running in real time, so when the connection experiences *request time out* then the telegram bot will send notifications in real time to telegram messages containing the Gateway IP and the status when the notification comes in. So when the administrator receives a message that occurs *request time out* then the administrator can draw conclusions as soon as possible and report the findings to the relevant ISP, so that interference with the ISP can be quickly handled by the ISP.

Conclusion

Reduce down time so that when there is a disruption the user is not too affected by the disturbance, because the internet source will immediately move if the disturbance occurs in one of the sources. In this study, even though it uses failover and 2 ISPs, all ISPs still run simultaneously. This research still has a loophole where administrators have to check devices directly when there is a disruption to one of the ISPs, which slows down the process of reporting and repairing the affected ISPs.

References

[1] B. Ilham, "Implementation of High Availability Message ISO 8583 using F5 Active-Passive Failover Method," *Int. J. Eng. Trends Technol.*, Vol. 71, No. 4, pp. 264–273, 2023, doi: 10.14445/22315381/IJETT-V71I4P223.

[2] M. Abduh, "Downtime Prevention Using Failover on IoT-based Contactless Temperature Checkers," *2022 10th International Conference on Cyber and IT Service Management, CITSM 2022*. 2022. DOI: 10.1109/CITSM56380.2022.9935842.

[3] S. H. M. Nejad, "A Novel Congestion Avoidance Algorithm Using Two Routing Algorithms and Fast-Failover Group Table in SDN Networks," *Lecture Notes in Networks and Systems*, vol. 180. Pp. 146–158, 2021. DOI: 10.1007/978-3-030-64758-2_11.

[4] K. Goravanchi, "A Divide and Conquer method with Semi-Global Failover for Software Defined Networks," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*. Pp. 1388–1397, 2021. DOI: 10.1109/CCWC51732.2021.9376136.

[5] T. Lee, "Position Fault Detection and Failover Method for UAM PMSM Control," *2021 IEEE Energy Conversion Congress and Exposition, ECCE 2021 - Proceedings*. Pp. 1627–1633, 2021. DOI: 10.1109/ECCE47101.2021.9594929.

[6] E. Ember, "Poster: Communication failover strategies for dependable smart grid operation," *International Conference on Embedded Wireless Systems and Networks*. 2021. [Online]. Available:

https://api.elsevier.com/content/abstract/scopus_id/85120718890

[7] Y. Kido, "A Development of Real-Time Failover Inter-domain Routing Framework Using Software-Defined Networking," *Advances in Intelligent Systems and Computing*, vol. 1363. Pp. 369–387, 2021. DOI: 10.1007/978-3-030-73100-7_27.

[8] K. Pakrijauskas, "Investigation of Stateful Microservice Availability During Failover," *2022 8th International Conference on Control, Decision and Information Technologies, CoDIT 2022*. Pp. 286–290, 2022. doi: 10.1109/CoDIT55151.2022.9804162.

[9] P. Weiss, "Worst-Case Failover Timing Analysis of Distributed Fail-Operational Automotive Applications," *Proceedings -Design, Automation and Test in Europe, DATE*, Vol. 2021. Pp. 1294–1299, 2021. DOI: 10.23919/DATE51398.2021.9473950.

[10] M. Abuibaid, "Edge Workloads Monitoring and Failover: a StarlingX-Based Testbed Implementation and Measurement Study," *IEEE Access*, Vol. 10, pp. 97101–97116, 2022, doi: 10.1109/ACCESS.2022.3204976.

[11] A. Leiter, "Automatic failover of 5G container-based User Plane Function by ONAP closed-loop orchestration," *Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022: Network and Service Management in the Era of Cloudification, Softwarization and Artificial Intelligence, NOMS 2022*. 2022. DOI: 10.1109/NOMS54207.2022.9789799.

[12] W. Dai, "A Tight Characterization of Fast Failover Routing: Resiliency to Two Link Failures is Possible," *Annual ACM Symposium on Parallelism in Algorithms and Architectures*. Pp. 153–163, 2023. DOI: 10.1145/3558481.3591080.

[13] H. Ben, "Design of a Scheme for Failover of Large Screen Visualization System Graphic Workstation," *2023 4th International Conference on Computer Engineering and Application, ICCEA 2023*. Pp. 328–334, 2023. DOI: 10.1109/ICCEA58433.2023.10135543.

[14] K. Sosnowski, "SURE: A Smart Failover Blockchain-Based Solution for the Recycling Reuse Process," *Electron.*, Vol. 12, No. 10, 2023, DOI: 10.3390/Electronics12102201.

[15] O. Schweiger, "Improving the Resilience of Fast Failover Routing: TREE (Tree Routing to Extend Edge disjoint paths)," *ANCS 2021 - Proceedings of the 2021 Symposium on Architectures for Networking and Communications Systems*. Pp. 1–7, 2021. DOI: 10.1145/3493425.3502747.

[16] S. H. Park, "Self-organized low-power multi-hop failover protocol for a cellular-based public safety device network," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2022.3156442.

[17] M. Terneborg, "Application agnostic container migration and failover," *Proceedings - Conference on Local Computer Networks, LCN*, Vol. 2021. Pp. 565–572, 2021. DOI: 10.1109/LCN52139.2021.9525029.

[18] P. Dharam, "A Mechanism for Controller Failover in Distributed Software-Defined Networks," *Proceedings of the 8th International Conference on Computer and Communication Engineering, ICCCE 2021*. Pp. 196–201, 2021. DOI: 10.1109/ICCCE50029.2021.9467174.