DEVELOPMENT OF A TELECOMMUNICATION-BASED FAILOVER SYSTEM TO REDUCE TRANSACTION DISRUPTION ON EDC DEVICES AT SPBU PERTAMINA

[1]**Muhammad Kalam Kahfi,** [2]**Dhoni Putra Setiawan,** [3]**Harfan Hian Ryanu**
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**kalamkahfi@student.telkomuniversity.ac.id**, [2]**setiawandhoni@telkomuniversity.ac.id,**
[3]**harfanhian@telkomuniversity.ac.id**

Abstract

Currently, Pertamina has implemented a cashless transaction system in their SPBU, using *Electronic Data Capture* (EDC) devices in its operation. However, this device has several weaknesses, one of which is the dependence on a stable network connection, which is still a challenge in certain areas.

The proposed solution to address these weaknesses is the creation of a failover system, which will automatically switch the network to a backup network if the main network is disrupted so that the EDC devices can continue to operate until the main network is restored. This system will hopefully reduce the experienced downtime when there is a network disruption, increasing the reliability of the cashless transaction system used in the SPBU.

Implementation and testing of the proposed failover design shows that the system is able to switch to the backup network in 435ms when the main network experiences disruption, and quickly return to the main network in 36ms once the disruption ends. This switching time should be quick enough to maintain the connectivity during operations with only minimal delays.

Keywords: *EDC, Failover, SPBU*

1. Introduction

Pertamina has implemented a cashless transaction system in their SPBU, using Electronic Data Capture (EDC) devices to process the payments. The operation of this transaction system relies on constant and uninterrupted network connection to communicate with the bank provider servers.

Should any kind of network interruptions occur, the system will be disconnected to the servers, and the transaction process will not be able to continue. These kinds of network disruptions increase wait time, disrupt the flow of vehicle queue, and lower customer's satisfaction on the cashless transaction system of the SPBU.

Therefore, this research intended to implement a failover system in the transaction system of the SPBU, as it is able to reduce risks of transaction failure, and increase the efficiency of operations. Research was conducted by observing one SPBU of its cashless transaction system and during its usage, and then designing a failover system to be integrated with it. Once the design is implemented, it is then tested on a live simulation.

2. Basic Theory

2.1. Telecommunication

Telecommunication is the process of transmitting information in the form of electromagnetic signals from one location to another through various transmission media, such as cables, radio waves, or optical fibers[1].

In the EDC system, telecommunications are used to send transaction data to the bank server or payment service provider by utilizing an internet connection. This connectivity is often realized through GSM, Wi-Fi, or Ethernet networks, depending on the available infrastructure[2].

2.2. EDC Device

Electronic Data Capture (EDC) devices are electronic devices designed to process payment transactions using debit cards, credit cards, or other cashless payment methods. This device has become one of the main solutions in supporting the ease and speed of financial transactions, both in the retail sector, public services, and other business sectors.

EDC devices work by reading data from payment cards, either through chips, magnetic strips, or contactless technologies such as Near Field Communication (NFC). The data received by the EDC device is then sent via a telecommunications network to the bank's server or payment service provider for verification. This process involves strong data encryption to ensure the security of customer information. Once the data is verified, the system will send a real-time approval or rejection response, so that transactions can be completed in seconds[1].

2.3. Failover

Failover is a mechanism in network and telecommunication systems designed to maintain service continuity when there is a disruption to the main path. The failover process works automatically by replacing the failed main path with a previously prepared backup path. With this mechanism, operational disruptions can be minimized so that services continue to run smoothly.

In telecommunication-based systems, failover is a reliable solution to overcome various risks of connectivity disruptions that can affect service quality[3].

2.4. Failover System Supporting Technologies

To ensure the failover system can run effectively and minimize disruption in the transaction process, a number of supporting technologies need to be implemented. These technologies are designed to maintain stability and continuity of connectivity, even in emergency conditions or disruptions to the main network. Some supporting technologies that can be implemented in the failover system are routers with Dual SIM capability[5], network load balancer[4], and Dynamic DNS technology[3].

2.5. Disruptions in Cashless Transactions

Disruptions in transactions made through EDC (Electronic Data Capture) machines can occur due to various factors, which have the potential to hinder the payment process and harm related parties. One of the main factors that cause disruptions in EDC transactions is problems with the internet network connection.

When the EDC device cannot connect to the bank server or payment service provider, the data verification and transaction approval process cannot be carried out in real-time. This can cause transactions to be delayed, or even fail completely. This network disruption can be caused by problems with the local network (such as broken cables or damaged switches), or with a wider internet connection such as an outage from the internet service provider (ISP) [1].

3. System Design

The proposed design for the failover system is expressed through this block diagram:

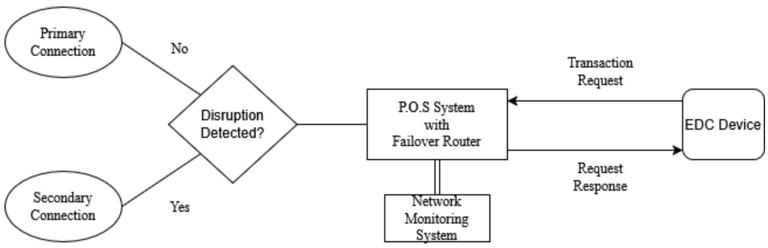


Image 1. Block Diagram of Proposed System.

The system monitors the condition of the main network and identifies disruptions or quality degradation that can affect transaction performance. When a disruption is detected and confirmed, the system will automatically switch the network. The failover router switches the connection from the main network to the backup network to ensure that transactions continue to run smoothly

After the switch is made, the system enters the network stabilization stage, where the switch distributes the connection to the connected devices, including the EDC device. This ensures that all devices can function optimally again even if there is a disruption to the main network.

The integration of the failover system to the existing transaction system within the SPBU is expressed through this diagram:

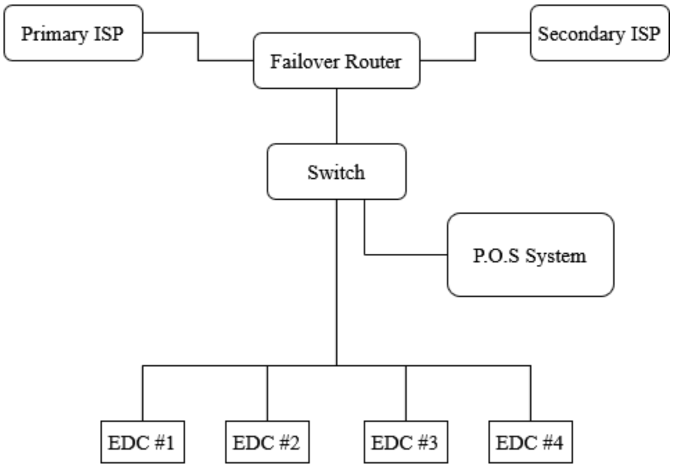


Image 2. Diagram of Cashless Transaction System after Failover System Integration.

The components required for the failover system, along with their specifications, can be seen in the table below.

Table 1. Failover System Components and Specifications.

Component	Hardware Specification
Internet Service Provider (ISP)	Internet service with minimum speed of 10 Mbps (recommended to be higher to support several EDC devices).
Failover Router	- Dual-WAN support for primary and backup connections.
	- Minimum routing speed of 1 Gbps.
	- Supports automatic failover protocol.
	- Minimum RAM of 128 MB.
4G/5G Modem	- Supports LTE/5G network with download speed up to 1 Gbps.
	- Compatible frequency with local network.
	- Port Ethernet for connection to router.
Broadband Modem	- Minimum connection speed of 50 Mbps.
	- Supports IPv4/IPv6 protocols.
	- Port Ethernet for connection to router.
Network Switch	- Type: Unmanaged or managed switch.
	- Port count: 8-16 Gigabit Ethernet ports.
	- Port speed: 1 Gbps per port.
	- Supports QoS (Quality of Service) technology.
EDC Device	- Supports TCP/IP communication protocol.
	- Processor: ARM Cortex or equal.
	- Connectivity: LAN/WiFi.
	- High operational durability for commercial use.

4. System Implementation

4.1 System Installation

The system, which has been designed according to Image 2, is then installed and integrated to the SPBU's digital transaction system.

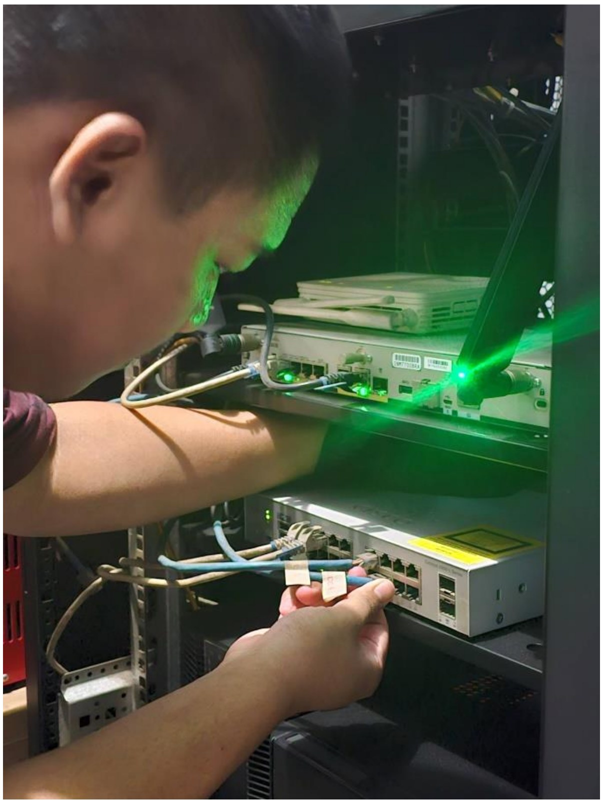


Image 3. Instalation Process of Designed Failover System.

The main components that are installed, along with each of its specifications, are as follows:

1. Router

Image 4. Installed Router.

The router used is CISCO ISR 1100 Series, with model code C1111-4PLTEEA, with specifications listed at the table below:

Table 2. Specifications of the Installed Router.

WAN Support	Dual (2) WAN
WAN Throughput	1889 Mbps
IPv4 Throughput	1372 Mbps
Automatic Failover Protocol	Hot Standby Router Protocol

RAM Size	4GB

Within the system, this router functions as the failover device, managing the primary and secondary connections and performing network swaps whenever necessary.

2. Switch

Image 5. Installed Switch.

The switch used is CISCO Catalyst 2960-L, with model code WS-C290L-16TS. The specifications of which is listed on the table below:

Table 3. Specifications of the Installed Switch.

Switch Type	Managed
Ethernet Port Count	16
Ethernet Port Speed	1000 Mbps
QoS Features	Load Balancing, Dynamic Host Configuration Protocol

Within the system, this switch functions as a load balancer, ensuring network traffic is evenly distributed across all of the operating EDC devices.

The total cost of the installed device, and the monthly operational cost, can be seen on the tables below.

Table 4. Installation Cost.

Router	Rp20.500.000
Switch	Rp12.000.000
Total Cost	Rp32.500.000

Table 5. Monthly Operational Cost.

AstiNet 50Mbps Monthly	Rp5.615.000
XL Business Monthly	RP1.000.000
Total Monthly Cost	RP6.615.000

4.2 System Testing

4.2.1 Automatic Failover Testing

The testing for the failover feature is done in a live simulation test. This is done by manually disconnecting the primary ISP from the Failover Router to simulate network outage and observing the connection through the network switch using a simple network monitoring tool.

Other than testing the automatic failover function of the router, this test also measures the time it takes to complete the switch from the primary to the secondary ISP, and the time it takes to complete the switch back to the primary ISP once the connection has recovered. The results for this test are shown below.

Table 6. Test Results for Automatic ISP Switching of Failover System.

Automatic ISP Switching	Time (ms)
Primary to Secondary	435
Secondary to Primary	36

4.2.2 Network Performance Testing

The connection performance of the primary and secondary ISP is also measured for comparison and analysis. The parameters measured include packet loss, round-trip-times (RTT), latency, jitter and throughput. The results for the measurements are displayed below.

Table 7. Network Performance Test Results.

Parameter measured	Primary ISP	Secondary ISP
Packet Loss	0%	0%
Minimum RTT	8ms	8ms
Maximum RTT	16ms	9ms
Latency	10ms	8ms
Jitter	2ms	0.1ms
Measured Throughput	41.41Mbps	22.88Mbps

4.3 Analysis

From the results of the test that has been performed and the measurements that have been taken, some key points can be made. These include:

1.) The automatic failover system in the Failover Router is working as intended, as it is capable of switching to the secondary ISP when the primary ISP is intentionally disconnected as part of the test.
2.) The time it takes for the failover system to switch to the secondary ISP is significantly longer than the time it takes to switch back to the primary ISP. This is most likely caused by a couple of factors, such as instability on the connection causing a delay or the configuration of the router used for the secondary ISP. Despite this, the switch to the secondary ISP still happens within acceptable times, of <500ms (or less than half a second).
3.) The primary ISP and secondary ISP both perform similarly, with the primary only experiencing slightly more latency and jitter than the secondary, and both in minimal amounts. Measured throughput of the connection from both ISPs is adequate for transactional purposes. Both also experience zero packet loss, which is a sign of an overall healthy network connection.

Analysis of these key points indicates that the failover system that has been implemented into the digital transaction system of SPBU Pertamina has been successful in its purpose. The automatic failover is able to recover the network connection when the primary ISP experiences outage or failure within an acceptable time frame, allowing continued usage of the EDC devices until it recovers from aforementioned outage, and for transactions to continue smoothly.

Compared to a digital transaction system before the failover system is implemented, which has no backup ISP and will fail whenever the primary experiences any sort of failure, this is a significant improvement on network reliability and sustainability. Both of the ISPs chosen and implemented with this system also meet the requirements for operation of the EDC devices.

5. Conclusion and Suggestions

Based on the results of the conducted research, test, and analysis, these conclusions can be made:

1.) The telecommunications-based network failover system has been successfully developed as a solution to the issues of connection instabilities and network outages during the operation of EDC devices, both of which negatively impact the reliability and smoothness of cashless transactions within Pertamina’s SPBU, by switching to a backup secondary network when the primary network experiences disruption.
2.) Through the test that simulates a network disruption event, the failover system is deemed effective at maintaining stable network connection during any transactions made using the EDC devices,

able to switch between networks at less than half a second (<500ms) at the slowest and less than 50ms at the fastest. This allows the transactions to continue with minimal or close to no disruptions that would otherwise cause a failure.

3.) The primary factor that affects the failover system is the overall quality and stability of the connection from the ISPs used as primary and secondary/backup networks. Another factor that could affect the failover system is the configuration of the router used to connect the ISP network to the failover system.

Based on the results of the research, test, and analysis that has been performed, a couple of suggestions for further research are also given, which are as follows:

1.) Utilization of more than two internet service providers can increase the reliability and the success rate of the failover system, by providing a tertiary backup network for cases when the secondary backup network also experience disruptions.

2.) Further research into optimal configurations for the network devices supporting the failover system.

3.) The addition of an electrical-based failover system, such as an Uninterruptible Power Supply (UPS), to be deployed alongside the telecommunications-based failover system to further ensure the operational continuity of the digital transaction system during power disruption.

References

[1] A. Tanenbaum and D. Wetherall, Computer Networks, 5th ed. Upper Saddle River, NJ: Pearson, 2011.

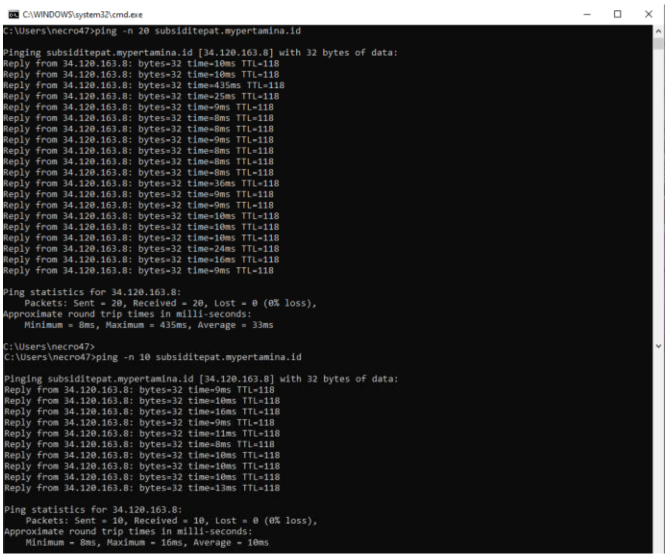
[2] G. Held, High-Speed Networking: A Systematic Approach to High-Bandwidth Low-Latency Communication. Hoboken, NJ: Wiley, 2009.

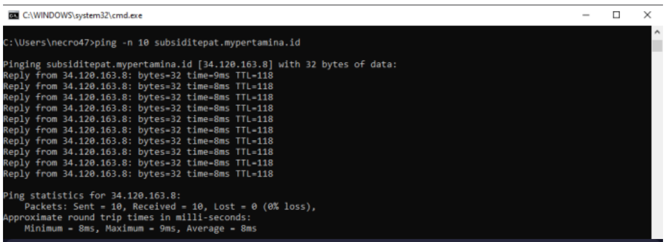
[3] M. Badrul dan A. Akmaludin, "Implementasi Automatic Failover Menggunakan Router Mikrotik untuk Optimalisasi Jaringan," Jurnal PROSISKO, vol. 6, no. 2, pp. 82-90, Sept. 2019. p-ISSN: 2406-7733, e-ISSN: 2597-9922.

[4] R. Rosmegawati, S. M. L. Tobing, dan D. A. S., "Pengaruh Teknologi Informasi, Sistem Pembayaran, Promosi Terhadap Kepuasan Pembeli dan Efeknya pada Loyalitas Pembeli," Jurnal Akuntansi FE-UB, vol. 16, no. 2, pp. 24-38, Okt. 2023.

[5] T. Sasidhar, V. Havisha, S. Koushik, M. Deep, and V. K. Reddy, "Load balancing techniques for efficient traffic management in cloud environment," International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 3, pp. 963–973, Jun. 2016, doi: 10.11591/ijece.v6i3.7943

Attachments





```
C:\WINDOWS\system32\cmd.exe

C:\Users\necro47>ping -n 10 subsiditepat.mypertamina.id

Pinging subsiditepat.mypertamina.id [34.120.163.8] with 32 bytes of data:
Reply from 34.120.163.8: bytes=32 time=9ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118
Reply from 34.120.163.8: bytes=32 time=8ms TTL=118

Ping statistics for 34.120.163.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 9ms, Average = 8ms
```