Al'adzkiya International of Computer Science and Information Technology (AIoCSIT) Journal
Vol. 2, No. 1, May 2021, pp. 7∼13
E-ISSN: 2722-0001

Network Disaster Recovery Design Using Hot Standby Router Protocol (HSRP)

Abdul Rachman Harahap[1], Tommy[2], Divi Handoko[3]
[1,3]Informatics Engineering Department, Universitas Harapan Medan, Indonesia

ABSTRACT

Computer network infrastructure located in a certain area is inseparable from possible disasters such as natural disasters caused by geological and demographic factors, fire - be it environmental factors or human error, or attacks on systems such as viruses or worms. Therefore, in building a network infrastructure we also need a network backup plan and recovery in the event of a disaster on the network infrastructure that supports the delivery of information. The backup network infrastructure must be in a different location with the main network infrastructure to anticipate major disasters. This research will implement the Hot Standby Router Protocol (HSRP), which is designed to support irregular IP traffic failures under certain circumstances. The purpose of this research is to implement Disaster Recovery Plans on technology related to network recovery, Provide recommendations for Disaster Recovery Institutions. The softaware used is GNS3.
Keyword: Network, Backup, HSRP

Corresponding Author:
Abdul Rachman Harahap,
Informatics Engineering Department,
Universitas Harapan Medan,
Jalan H.M.. Joni No.70C, Indonesia.
Email: utaritari986@gmail.com

1. INTRODUCTION

Deep networks are crucial in disaster recovery(Spoon et al., 2020). A system running in an agency will depend on a network that processes this information. Information is one of the most basic human needs(Iivari et al., 2020). Currently, users of information are not only those who are capable. With the cheapening of information facilities and support, the current alternative communication that can overcome limitations such as distance is the use of international computer networks or commonly known as the Internet(Sumbodo et al., 2017).

Disaster Recovery Plan (DRP) is a set of documents that defines every activity, action and procedure that must be carried out by all stakeholders involved in order to save assets in the sector owned by information technology(Sahebjamnia et al., 2015). Before creating a DRP, the most important thing that must be done is to apply risk management. By implementing risk management, the risks in the Data Center and Network can be easily identified(Santoso & Ernawati, 2017). Disasters that occur can have a direct or indirect impact on the operations of an organization or agency. Organizations or agencies must be prepared to face the impact that occurs due to the disaster, the impact of the disaster varies greatly, such as the interruption of computer networks, the interruption of IS / IT services, the cessation of electricity, suppliers that stop the supply of their products, absence of employees, damaged public facilities, late payment of salaries so on(Maliki, 2010). Computer network infrastructure located in a certain area cannot be separated from the possibility of being hit by disasters such as natural disasters caused by geological and demographic factors, fires caused by environmental factors or human error, or attacks on systems such as viruses or worms. Therefore, in building a network infrastructure, a network backup and recovery plan is also needed in the event of a disaster on the network infrastructure that supports the delivery of information. Backup Network infrastructure must be located different from the main network infrastructure to anticipate major disasters. In failure in the network infrastructure(Haryadi, 2019).

Hot Standby Router Protocol (HSRP) is designed to support irregular IP traffic failures under certain circumstances(Sheghdara & Hassine, 2020). In particular, the protocol protects against

subsequent host failures when the source host cannot dynamically learn the IP address of the next hops. The protocol is designed for use over multiple access, multicast or LAN networks(Lane et al., 2007). HSRP is not assumed to be a substitute for the existing dynamic router discovery mechanism and these protocols should be used instead whenever possible(Puspitasari et al., 2020). Large host group implementations that do not support Dynamic Hop Next Discovery that are capable of configuring a default router. HSRP provides a service to those who have lost their way to an objective(Akmaludin et al., 2019).

In research (Puspitasari et al., 2020)conducted research on failures in data exchange caused by network device failures. This research was conducted at PT Indonesia Power Jakarta Pusat where there is a network system failure during the exchange due to a malfunction of the WAN Optimizer or router. Therefore, the implementation of HSRP is needed. With this implementation it can improve the quality of computer networks and overcome network failures. Besides that there is also research (Pratama, 2019) designing and implementing HSRP on the Thin Client network that will ensure the convenience and smooth flow of the internet and make the use of electrical power as efficiently as possible.

From the background explanation that has been explained, the problem in this study is to develop a system that can perform network disaster recovery by implementing the hot standby routing protocol as a technique in disaster recovery.

2. RESEARCH METHOD

A. Design Process Stage

The system design stage is the initial stage of designing a disaster recovery network using HSRP. This design is done to determine network conditions in general and to determine the order of work that will be carried out in designing a system. In network design, there are several things that need to be prepared so that the system can run properly. The parts that must be prepared include a computer or laptop to build a network using the HSRP in the Packet Tracer network simulator software.

B. Process Analysis Stage

The analysis process stage is the analysis stage of data collection or defining requirements specifications, the function to be made is focused on the system requirements to be delivered. This is to make it easier to design a disaster recovery network using HSRP and then analyze the security of the network. The steps taken to analyze this network system are as follows.

1. Identifying problems regarding network disaster recovery using HSRP.
2. Understanding the work of the existing system, namely to be able to find out the problems that arise in an old network system, it is necessary to have an understanding of the work or operation of the network, so that it can be seen the needs needed and will be developed on the system to be designed.

C. Function Analysis

Functional analysis is intended to identify specifications or features that a person will have in implementing network disaster recovery using HSRP.

1. On the HSRP network, the Cisco standard redundancy protocol will function which defines a Router that automatically takes over if another router fails.
2. Router functions to connect between clients with other routers.
3. There are 6 computers that are used as clients.

D. Network Topology Design

In designing a system that is built using 4 routers. The following is the topological design that the author designed in figure as follows.

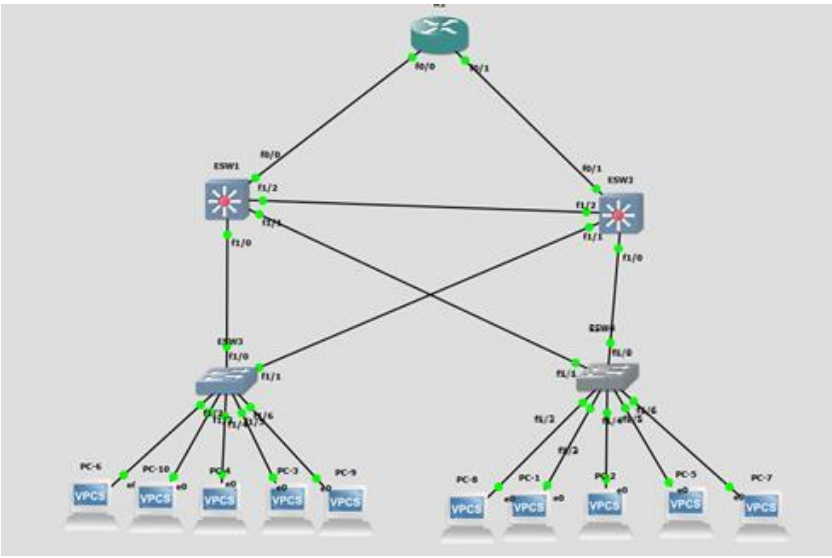


Fig 1. Network Topology Design

In the figure, there are 4 designed topologies of type 3720 that connect the network operation center division room to the operation maintenance division room. In the topology there are 2 switches that function to connect between computers and other computers and there are 8 clients / PCs.

3. RESULTS AND DISCUSSION

This section will implement and test the system. This stage is carried out after the design is completed and will then be implemented in the network simulator. After implementing it, the system is tested and the deficiencies in the network are seen for further network protocol development.

A. HSRP Network Configuration

HSRP is a Cisco proprietary redundancy protocol for establishing tolerant default gateways. Version 1 of the protocol is described in RFC 2281. There is no RFC for protocol version 2. The protocol specifies a framework between network routers to achieve a failover default gateway if the primary gateway becomes inaccessible, in close association with fast-converging routing protocols such as EIGRP or OSPF. HSRP routers send multicast Hello messages to other routers to inform them of their priority (which router is preferred) and status (Active or Standby).

1. Network on Router 1

In the configuration of network router 1 in setting the ip address, the command is carried out.

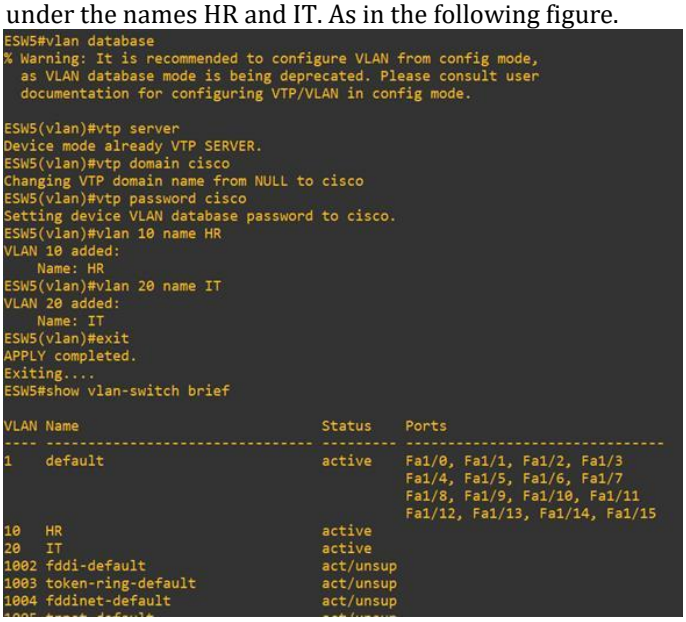
```
R2(config)#track 11 rtr 11 reachability
R2(config-track)#exit
R2(config)#ip sla 12
R2(config-ip-sla)#icmp-echo 12.12.12.2
R2(config-ip-sla-echo)#frequency 5
R2(config-ip-sla-echo)#timeout 5000
R2(config-ip-sla-echo)#threshold 100
R2(config-ip-sla-echo)#ip sla schedule 12 life forever start-time now
R2(config)#ip sla 12
Entry already running and cannot be modified
       (only can delete (no) and start over)
       (check to see if the probe has finished exiting)

R2(config)#ip sla schedule 12 life forever start-time now
Cannot modify schedule. Operation may have started.

R2(config)#track 12 sla 12 reachability
                        ^
% Invalid input detected at '^' marker.

R2(config)#track 12 rtr 12 reachability
R2(config-track)#exit
R2(config)#ip route 0.0.0.0  0.0.0.0 11.11.11.2 track 11
R2(config)#ip route 0.0.0.0  0.0.0.0 12.12.12.2 track 12
R2(config)#exit
```

Fig 2. Router Settings 1

The description of figure explains that router 1 uses the function of IP SLA which ischeck the status of an object in an unlimited or limited time period. Most often used is by pinging the destination address to check its updown status. or to measure quality parameters such as jitter, latency, round trip time (RTT) and others, IP SLA sends it "robots" many times and makes accurate statistics.

2. Network configuration on multilayer switch 1

In the multilayer switch network configuration is done by creating a virtual local area network, in this study the vlan is used under the names HR and IT. As in the following figure.



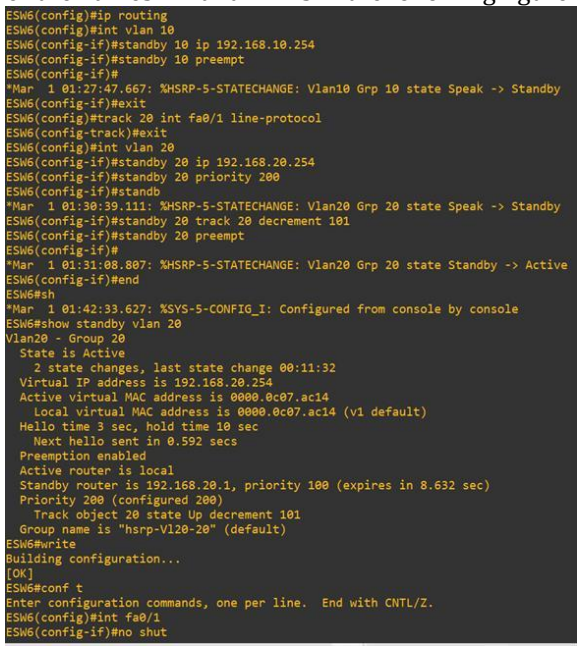
```
ESW5#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

ESW5(vlan)#vtp server
Device mode already VTP SERVER.
ESW5(vlan)#vtp domain cisco
Changing VTP domain name from NULL to cisco
ESW5(vlan)#vtp password cisco
Setting device VLAN database password to cisco.
ESW5(vlan)#vlan 10 name HR
VLAN 10 added:
    Name: HR
ESW5(vlan)#vlan 20 name IT
VLAN 20 added:
    Name: IT
ESW5(vlan)#exit
APPLY completed.
Exiting....
ESW5#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
10   HR                               active
20   IT                               active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
```

Fig 3. Network configuration at multilayer switch 1

The caption in figure explains that a multilayer switch must be given a working vlanprovides a method for dividing one physical network into many broadcast domains. VLANs allow multiple virtual LANs side by side in a switch.

3. Network configuration on multilayer switch 2

In the multilayer switch network configuration is done by creating a virtual local area network, in this study the vlan is used under the names HR and IT. As in the following figure.



```
ESW6(config)#ip routing
ESW6(config)#int vlan 10
ESW6(config-if)#standby 10 ip 192.168.10.254
ESW6(config-if)#standby 10 preempt
ESW6(config-if)#
*Mar  1 01:27:47.667: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
ESW6(config-if)#exit
ESW6(config)#track 20 int fa0/1 line-protocol
ESW6(config-track)#exit
ESW6(config)#int vlan 20
ESW6(config-if)#standby 20 ip 192.168.20.254
ESW6(config-if)#standby 20 priority 200
ESW6(config-if)#standb
*Mar  1 01:30:39.111: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
ESW6(config-if)#standby 20 track 20 decrement 101
ESW6(config-if)#standby 20 preempt
ESW6(config-if)#
*Mar  1 01:31:08.807: %HSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
ESW6(config-if)#end
ESW6#sh
*Mar  1 01:42:33.627: %SYS-5-CONFIG_I: Configured from console by console
ESW6#show standby vlan 20
Vlan20 - Group 20
  State is Active
    2 state changes, last state change 00:11:32
  Virtual IP address is 192.168.20.254
  Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.592 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.20.1, priority 100 (expires in 8.632 sec)
  Priority 200 (configured 200)
    Track object 20 state Up decrement 101
  Group name is "hsrp-Vl20-20" (default)
ESW6#write
Building configuration...
[OK]
ESW6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW6(config)#int fa0/1
ESW6(config-if)#no shut
```

Fig 4. Network configuration at multilayer switch 1

4. IP at Router 1

The show ip configuration displays the ip configuration on the router device in implementing the HSRP network using the following command.

R3 # do sh int brief

The main purpose of the following command is to display information from a port that is equipped with an ip address. This command is similar to the show ip interface command but the result of this command is a brief display of the layer 3 (network) conditions of all interfaces. view image.

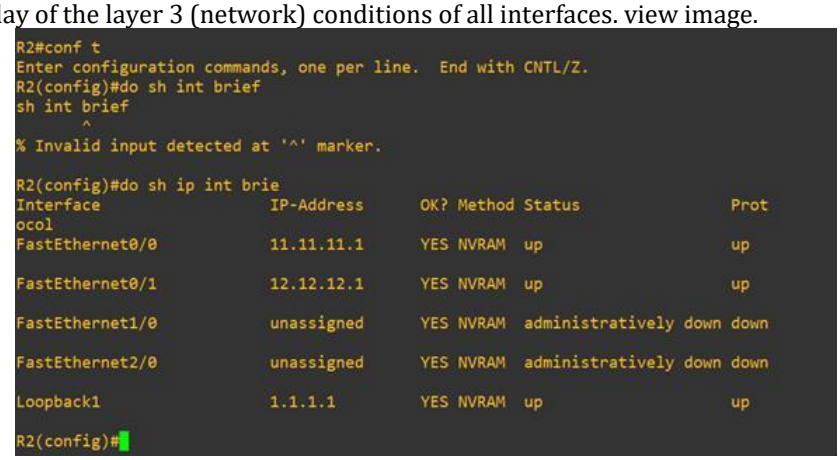


Fig 5. Ip at Router 1

The description of figure will explain the main purpose of the show ip command on the router to show back the ip address used by the client or host that has been configured to ensure that the entire client or host pc is running properly.

5. Running Config

The running config configuration will display the configuration know the configuration of a router and switch. on the router device in implementing the HSRP network using the following command.

R3 # show running config

In a simulation problem, this command is useful for knowing the configuration of a router and switch. After running this command, you can see the wrong or less configuration of a router or switch, as in the following figure.

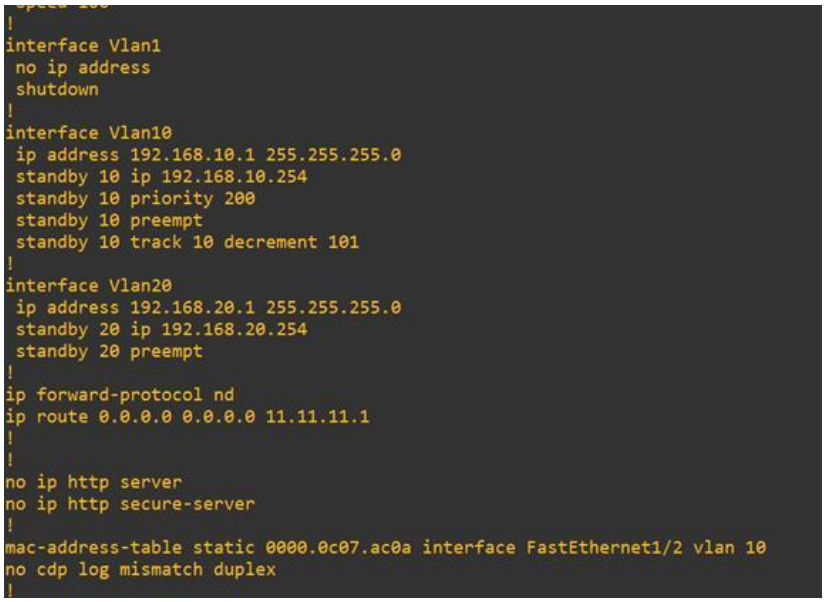


Fig 6. Running Configuration

The description of figure will explain the Display This command serves to view the configuration that has been set in a Cisco switch or router that is running.

B. Configure IP Address

In the ip address configuration, the address will be started with the command command on each computer. Here is the command to add an ip address:

PC-1> Sh ip
PC-1> Ip add 11.0.0.3 255.255.255.0 11.0.0.1

Display the IP address configuration as a configuration performed on a computer device that will connect each computer on the network. Here is a picture of the ip address configuration display.

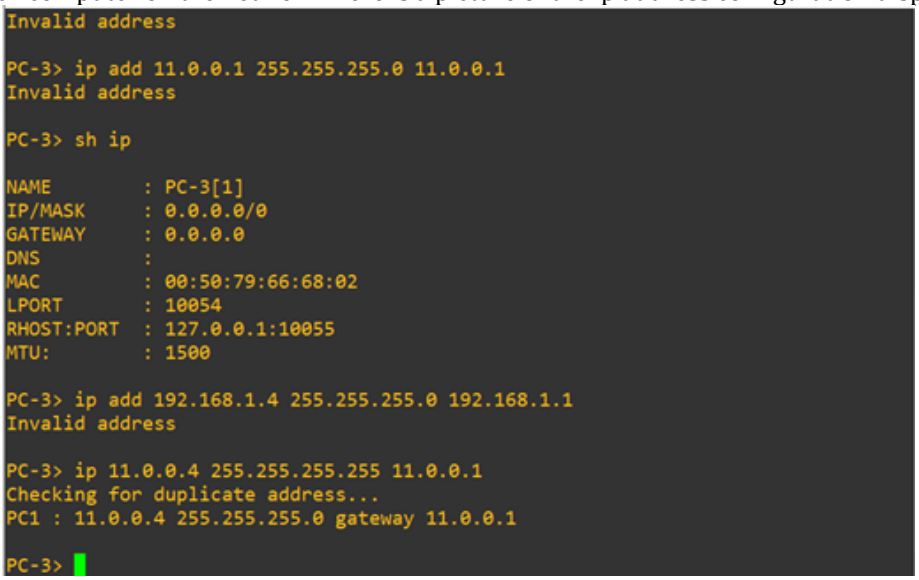


Fig 7. IP Address Configuration

The caption in figure will explain that the address of each computer to make it easier for the network to recognize all the client or host computers that have been installed.

C. Connection Test When the Multilayer Switch is Deactivated

To prove that HSRP can work properly, testing is done by deactivating the multilayers switch then pinging the router, to do this the following command is required.

PC # ping 1.1.1.1

If when the connection test results are successful, the connection using HSRP is successful, the display will be as shown below.

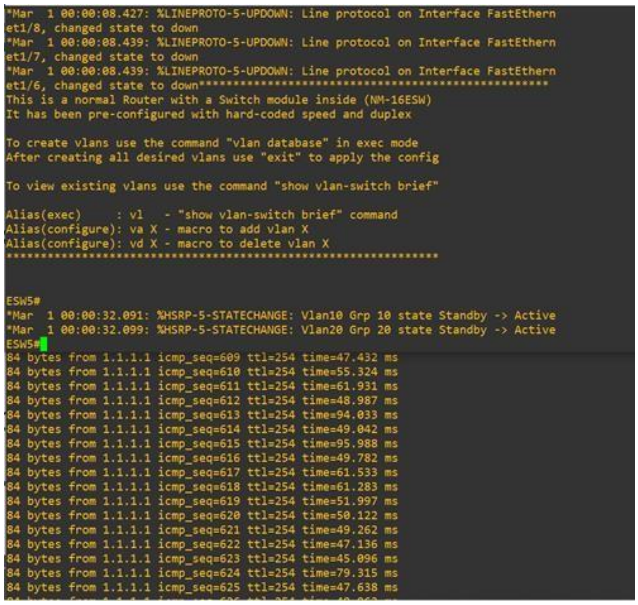


Fig 8. Test Connection When Multilayer Switch on Disable

4. CONCLUSION

Based on the research that has been done, the following conclusions are obtained:

1. With the implementation of the Disaster Recovery Plan on network recovery related technologies, it is possible to determine which path is best to reach the destination in the event of a problem on the main line.
2. This research has succeeded in implementing the hot standby routing protocol as a technique in disaster recovery which functions to exchange paths when a disaster occurs.

REFERENCES

Akmaludin, A., Mt, A., Masruroh, S. U., & Sc, M. (2019). Evalusi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming. *CyberSecurity Dan Forensik Digital*, *2*(1), 43–51.

Haryadi, E. (2019). Infrastruktur Jaringan Komputer dan VMware Untuk Mendukung Implementasi Manajemen Persediaan Barang. *Sainstech: Jurnal Penelitian Dan Pengkajian Sains Dan Teknologi*, *29*(1), 9–15. https://doi.org/10.37277/stch.v29i1.311

Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care? *International Journal of Information Management*, *55*(June), 102183. https://doi.org/10.1016/j.ijinfomgt.2020.102183

Lane, R. G., Daniels, S., & Yuan, X. (2007). An empirical study of reliable multicast protocols over Ethernet-connected networks. *Performance Evaluation an International Journal*, *64*(3), 210–228. https://doi.org/10.1016/j.peva.2006.05.013

Maliki, I. (2010). Manajemen Risiko Teknologi Informasi Untuk Keberlangsungan Layanan Publik Menggunakan Framework Information Technology Infrastructure Library (ITIL ver 3.0). *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, *2010*(Snati).

Pratama, E. K. (2019). IMPLEMENTASI HOT STANDBY ROUTER PROTOCOL CISCO PADA JARINGAN THIN CLIENT. *Jurnal AKRAB JUARA*, *4*(4), 160–168. http://repositorio.unan.edu.ni/2986/1/5624.pdf

Puspitasari, A., Hairistryan, H., & Nasution, R. (2020). Implementasi Hot Standby Router Protocol (Hsrp) Pada Pt Indonesia Power Jakarta Pusat. *JIKA (Jurnal Informatika)*, *4*(2), 55. https://doi.org/10.31000/jika.v4i2.2611

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273. https://doi.org/10.1016/j.ejor.2014.09.055

Santoso, H. B., & Ernawati, L. (2017). Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus : Universitas Kristen Duta Wacana). *Jurnal Informatika Dan Sistem Informasi (JUISI) Universitas Ciputra*, *03*(02), 8–17.

Sheghdara, M., & Hassine, J. (2020). Automatic retrieval and analysis of high availability scenarios from system execution traces: A case study on hot standby router protocol. *Journal of Systems and Software*, *161*. https://doi.org/10.1016/j.jss.2019.110490

Spoon, J., Hunter, C. E., Gerkey, D., Chhetri, R. B., Rai, A., Basnet, U., & Dewan, A. (2020). Anatomy of disaster recoveries: Tangible and intangible short-term recovery dynamics following the 2015 Nepal earthquakes. *International Journal of Disaster Risk Reduction*, *51*, 101879. https://doi.org/10.1016/j.ijdrr.2020.101879

Sumbodo, B. A. A., Dharmawan, A., & Faizah, F. (2017). Implementasi Teknologi Internet Sebagai Solusi Pengentasan Masalah Komunikasi di Desa Nyamuk, Kecamatan Karimunjawa, Kabupaten Jepara. *Jurnal Pengabdian Kepada Masyarakat (Indonesian Journal of Community Engagement)*, *2*(2), 189–203. https://doi.org/10.22146/jpkm.15654