PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING JARINGAN MENGGUNAKAN ICINGA DAN POWERDNS DI PT. PACIFIC TELEMATIKA INDONESIA

Selamet Puji Ramadhan

Informatic Engineering – Indonesian Computer University
Jl. Dipatiukur 112-114 Bandung
E-mail : selamet.ramadhan@gmail.com

ABSTRACT

PT. Pacific Telematika Indonesia is a company engaged in the field of information technology. one of the services provided is the Internet Service Provider (ISP) in addition to the aforementioned service PT. Pacific Indonesia Telematics has colocation services, namely placing the computer server rack customers PT. Pacific Indonesia Telematika are used by agencies of Government, private or individual. In keeping the network conditions found some problems, namely the difficulty of monitoring the condition of the network against the changes that occur as the network status changes from life to death and vice versa. These conditions are not entirely due to the limitations of Technical control Network System which must supervise & by way of checking the condition of the server one by one. In addition, countermeasures against the server if you experience interference, is still done manually.
Based on this it takes a network monitoring system that can be used to resolve the issue. With the aim to facilitate the Technical Network System in network monitor & and can cope with the problems against the server if you experience interference, by way of transfer of the DNS path towards alternative server called DNS failover. The system is implemented using Application Programming Interface (API) as a bridge for communication between the Monitoring System network with the Domain Name System
Based on the results of testing that can be done tlah inferred that a Network monitoring system implemented can be used this way by the companies to monitor the server. And facilitate technical network system as well as and DNS Failover is implemented can tackle problems occurred. If problems occur on the server.

Keywords : Network Monitoring System, DNS Failover, API.

1. INTRODUCTION

This section will describe on about background problems, goals and purpose.

1.1 Background

PT. Pacific Telematika Indonesia is a company engaged in the field of information technology, one of the services provided is the Internet Service Provider (ISP) in addition to the aforementioned service PT. Pacific Telematika Indonesia has colocation services, namely placing the computer server rack customers PT. Pacific Telematika Indonesia are used by more than 30 users, be it the Government, private agencies or individuals. In providing service to customers, the company is constantly working to improve existing networks and systems, it is to provide the best service to customers. In keeping the network conditions found some problems, namely the difficulty of monitoring the condition of the network against the changes that occur as the network status changes from live to die and vice versa, conditions that lead to the occurrence of dead tissue, mong other damages that occur in the software or hardware of software for experiencing the bug that is not known from where the cause, and on the hardware such as ethernet often die and the occurrence of unstable voltage, such as going on a date 28 November 2016 at 20:00 WIB. ertainly the condition effect on Service service given to customers. These conditions are not fully observed, due to the limitations of the Technical Network & System who should oversee by means of checking the condition of the server one by one. This resulted in the handling of a server performance is not optimal. One system that can be used to condition a stable network is using a Network Monitoring System.

Based on the interviews that have been made against Technical Network & System in PT. Pacific Telematika Indonesia, then it needs a system that can monitor the condition of the network in one zone server, because all this time to find out the condition of the network just by doing the examination of software or hardware that are reviewed manually. In addition the need for mechanisms of countermeasures against the server if you experience interference, with the transfer of the line against DNS server alternative called DNS failover. Because when there is a dead server configuration required a diversion against the server experiencing

disturbances for redirected towards alternative server configuration however is still done manually. This proved less effective because it is not given against redirection handling server remember DNS changes take time known as the Time To Live (TTL), that resulted in the recovery of server downtime depends by the set time. The TTL has a span of, example of reference time to refresh DNS takes 86400 seconds or 24 hours [1].

One of the tools of Network Monitoring Systems namely, ICINGA, monitoring systems are network is open source so it can be configured to suit your needs, its uses, among others, to monitor network conditions in the complex environment in some locationsICINGA also generates performance data from the results of monitoring to reporting. ICINGA is able to monitor everything that is connected to the network that will be signed, otherwise it can send notifications if there is a change of status and ICINGA enables multithreaded. DNS failover DNS changes is a mechanism of a server to another server, one of the tools for DNS i.e. PowerDNS PowerDNS nameserver is authoritative, advanced with high performance. can read information from MySQL, Oracle, PostgreSQL and other databases. PowerDNS to use for DNS records to support DNS Failover mechanism.

Based on the results of the testing that has been done can be concluded that the Network Monitoring System implemented can be used by the company to monitor the server and simplify the Technical Network System, as well as DNS & Failover is implemented can tackle problems occurred. If problems occur on the server.

1.2 Purpose dan Objective

Then the point of this research is to design and implement a network monitoring system using discusses the ICINGA server as the monitoring system network and the DNS Server as the PowerDNS. As for the goals to be achieved in this research is to facilitate technical network system in monitoring & network conditions that would be able to cope with the problems that will occur.

1.3 Network Management

Network management consists of a set of functions to control, plan, allocate, deploy, coordinate and monitor network resources. Network management used to be a consideration in many network architecture. For example, most of the network architecture and design were developed without thinking about the user, which is generally true until a few years ago. Consider the changes that have recently been made in the SNMP security. Today, and in the future, the network is a resource that should be measured and verified integrity. The architecture of network management, as with other components of architecture, beginning with requirements and analysis of flow [5]. Areas that should be addressed during the analysis process include:

a. Select the network management protocol.
b. Implementing high-level asset management as part of network management architecture.
c. reconfigure network often to meet the requirements of change.
d. monitoring of the entire system from one location or device.
e. Testing service provider in accordance with service level agreements Service Level Agreement (SLA) and policies.
f. performance monitoring to avoid problems.
g. the Out-of-band access requirements.

Began defining and characterizing management for network architecture, and how to plan for monitoring, configuration, and troubleshooting network plan. then check the requirements of network management protocols and instrumentation. This will cause consideration to develop network management architecture [5]. Network management can be seen as a structure consisting of several layers:

a. business management: the management aspects of the business network for example, management of budget resources, planning, and agreements.
b. Service Management: service delivery management to users for example, these service providers will include the access bandwidth management, data storage and application delivery.
c. network management: management of all network devices across the network.
d. Elements management: managing a similar collection of network devices such as routers or access customer management system.
e. management of network elements: management of individual network devices for example, a single router, switch or hub.

In Figure 1, is a top-down approach, with the most abstract components (business management) at the top of the hierarchy, and the most tangible component of specified (network-element management) at the bottom of the hierarchy. This is shown in Figure 1. In line with that, because the components become more abstract, that the way they are applied and measured (information element) changed. Thus, at the bottom of this hierarchy (network-Network, element, element), management applied with variables and parameters, while at the top of this hierarchy (business services), management is applied in a more abstract, using the policy.

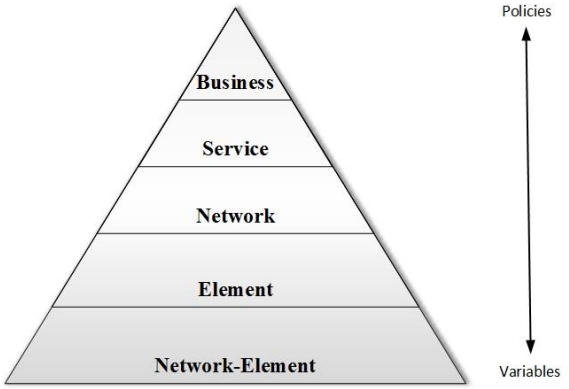


Figure 1 Network Management Hierarchy [5]

Common to all the components of the architecture, and we will find that the policy can be used for each component. network management can be divided into two basic functions: transport management information across systems, and management information element Figure 1. These functions, as shown in Figure 1, consist of various tasks the monitoring, configuration, troubleshooting, and planning done by the users, administrators, and network personnel. One of the first challenges in developing the architecture of network management is to define what network management really means to organizations that will perform tasks and receive the service-i.e. the end, user, or customer, of the system [5]. There are four categories of network management tasks, in accordance with the four tasks that were mentioned:

1. Monitoring to action notifications notifications.
2. Monitoring for trend analysis and planning.
3. Reconfigure the network parameters.
4. Troubleshooting the network.

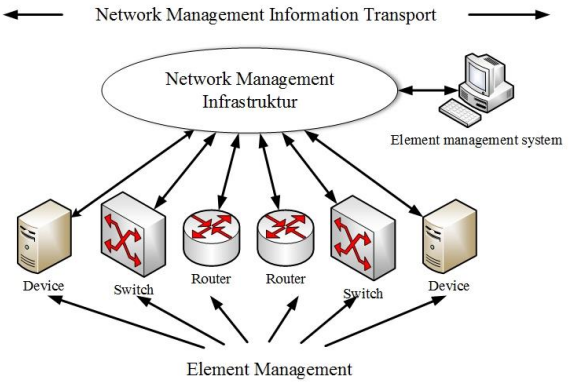


Figure 2 Network management is composed of managing elements and transporting management data [5]

1.4 Network Monitoring System

Network monitoring system is one of the system from the network management function describing the condition of a system, which continuously monitors the condition of the network by checking specific span of time, be it hardware or software conditions to monitor, for example, check the availability of the monitored devices whether on or off status, so that in case of disorders known as soon as possible by making the notification to a Technical Network & System.

There are two main approaches that are commonly used in monitoring the performance of network services support QoS (Quality of Service) to determine if the SLA (Service Level Agreement) have been met:

a. Passive network monitoring: with passive network monitoring, network devices to record statistics on the network traffic, that can provide an indication of the status of a particular network element. Polling intervals are typically used to collect this data for reporting and analysis. This is a small part that looks at each device in isolation; by looking at some of the elements of an aggregate view of the status of the network, network services can be inferred. Passive network monitoring does not require any extra would be used for the purpose of measuring traffic.
b. monitoring active network: Unlike passive monitoring, active surveillance involves the delivery of additional traffic to the network. synthetic test stream consisting of a "probe" packet is sent across the network solely for the purpose of knowing the characteristics of network performance; analysis of the flow of the accepted use for this characterization. active surveillance giving the size of a small part of SLA (Service Level Agreement) that reports the network performance is measured in a number of network elements as a system.

1.5 Domain Name System

Domain Name System (DNS) is a service directory search that provides mapping between host names on the Internet and the numerical address. DNS is critical to the function of the internet. It is defined in RFC 1034 and RFC 1035. DNS consists of four elements [3]:

a. the DNS Domain name space: using tree-structured namespaces to identify resources on the Internet.
b. DNS database: conceptually, each node and leaf in the name of the structure of the namespace tree set of information (e.g., IP address, the type of resource) are contained in the resource record (RR). A collection of all the RRS are organized into distributed database.
c. Name servers: a server is a program that stores information about the part of the tree structure of domain names and the associated RRS.
d. Resolvers: these are programs that extract information from name servers in response to client requests. The typical client is a request

for the IP address that corresponds to a particular domain name.

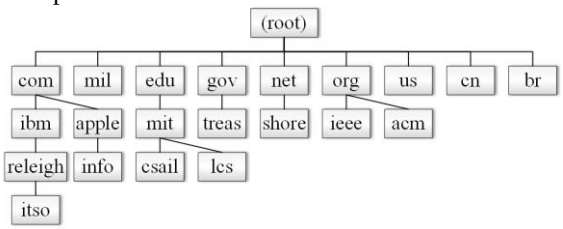


Figure 3 Portion of Internet Domain Tree [3]

1.6 JSON (JavaScript Object Nation)

JSON (JavaScript Object Nation) adalah is a lightweight data interchange format, easy to read and written by humans, as well as easily translated and made (generate) by computer. This format is based on the JavaScript programming language, Standard ECMA-262 3rd Edition-December 1999. JSON is a text format that is not dependent on any programming language because it uses the style language that is commonly used by programmers family C include C, C++, C #, Java, JavaScript, Perl, Python etc. Because of these properties, making it ideal as a JSON data exchange language [6].

1.7 API (Application Programming Interface)

Application programming interface (API) Application programming interface (API) is a set of commands, functions, components, and protocols provided by the operating system or a specific programming language that can be used by programmers when building software

In a programming required at least thousands of system call per second therefore many programmers who use fire. In the API there are functions/commands for the replacing language used in system calls with a language that is easier to understand by the programmer. Function that is created by using the API will then call the system call corresponds to system operations. No possibility of system call of the same name with the name of the API.

1.8 Centos

CentOS Linux distribution (from the Community ENTerprise Operating System) is an enterprise-class linux is freely available, open source operating system which is derived from the source code of Red Hat Enterprise Linux (RHEL) and developed and maintained by the project CentOS. The CentOS Project is more than just a Linux distribution. Project members work to provide support, training materials, and in the future even the certification. Although at the point of the project is the distribution of CentOS, CentOS Project covering the entire ecosystem of software developers and projects [7].

1.9 LAMP

Lamp (Linux, Apache, PHP, MariaDB) is a free software package, free in the sense of use, study, copy, modify, copy or sell software, users do not need to ask permission from anyone. Picture LAMP Architecture can be seen in Figure 4.

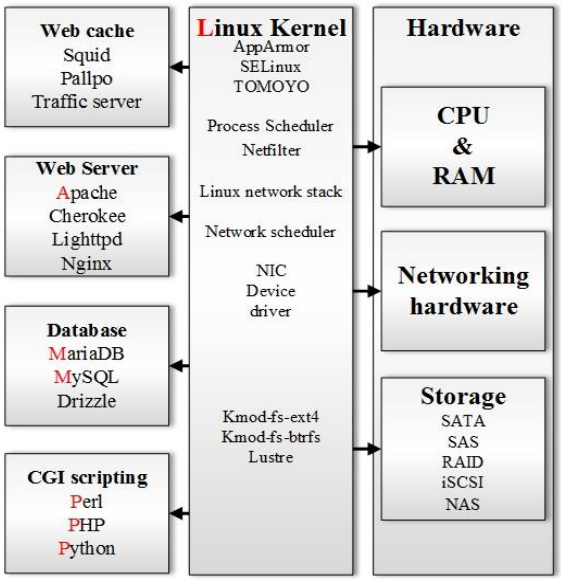


Figure 4 Architecture LAMP

1.10 ICINGA

ICINGA is one of the tools of the network monitoring system are open source so it can be configured to suit your needs, its uses, among others, to monitor network conditions in the complex environment in some locations, can give the user notification if a network resource monitor dies, also generate performance data for reporting. with a high level of flexible ICINGA is able to monitor everything that is connected to the network that you want to handle [8]. Architectural drawings ICINGA can be seen in Figure 5.

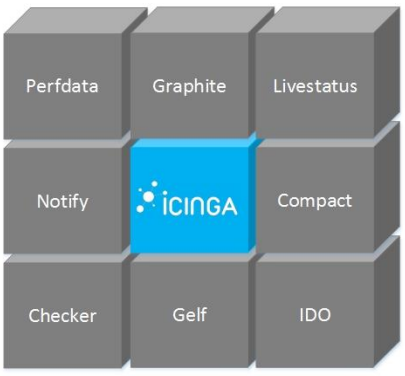


Figure 5 Architecture ICINGA

1.11 PoworDNS

PowerDNS Recursor is a high-end, high-performance finishing with the server name that the DNS resolution power of at least a hundred million customers. Utilizing multiple processors and

supports the ability of the same powerful scripting is turned from Authoritative Server, giving the Recursor performance, while retaining the flexibility in the deployment of the DNS for the modern that requires [9].

PowerDNS which used to function as a DNS server and make use of the APIS for media control over DNS, and PowerDNS has several advantages such as support for standard relavan, with measures of anti-spoofing, reconfiguration without downtime, utilization of PowerDNS to enable Dynamic DNS Updates aimed at DNS Failover.

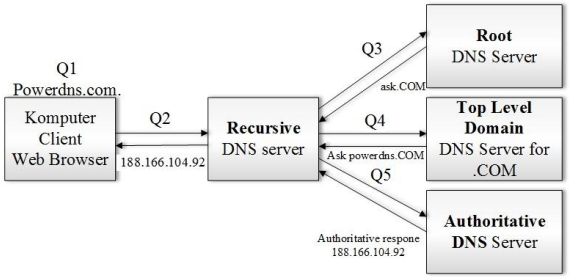


Figure 6 Mechanism DNS

From Figure 6 can be explained from the DNS client query mechanism until the client gets a response from the DNS Authoritative. Explanation step is as follows:

a. open the Web Browser and the Client wants to access the domain powerdns.com (Q1). Operating systems and Web browsers determine whether knowing the domain powerdns.com. If you don't know, the operating system asks the DNS Server to resolve them. Operating systems do demand for Recursive DNS servers.
b. the Recursive DNS Server does recognize your domain powerdns.com if no DNS Server performs Recursive DNS Root Server demand for (Q3).
c. Root DNS servers provide responses do not know the domain powerdns.com but the Root DNS servers know where can find DNS Server COM.
d. Recursive DNS servers store all information from the DNS Root Server, put in the cache and then perform a query against DNS Server COM (Q4).
e. COM DNS servers provide responses do not know the domain DNS Server but powerdns.com COM know where can find the domain powerdns.com.
f. DNS Recursive Server stores all information from the DNS Server cache and put him into the COM then do demand for Authoritative DNS servers (Q5).
g. Authoritative DNS servers provide feedback to know the domain powerdns.com and provide information IP Address that can be accessed by a Web Browser
h. Recursive DNS servers store all information from Authoritative DNS servers to place it in the cache and then give an answer to the operating system.
i. Later operating systems provide against a Web Browser.
j. Web browser then make connections against IP address and request the web page for the domain powerdns.com

1.12 Kali Linux

Time Linux is a Debian-based Linux distro intended for penetration testing and security audit. It contains several hundred times the tools that lead to a variety of tasks such as information security, penetration testing, security research, computer forensics and Reverse Engineering. Time Linux was developed, funded and managed by the security offensive, leading information security training company [10].

2 RESEARCH CONTENTS

System analysis at this stage is to identify problems that occur in the scope of the research includes hardware and software. This analysis is required as a basis for the design of the stages of the system and to determine the needs of the system to be applied.

2.1 Analysis Of The Problem

The problem of the research is how to facilitate the Technical Network System in managing network & handled can then tackle the problem that occurred.

2.2 Aanalysis of system running and Problem

Analysis of the system running and the issue at this stage is to give an overview of the running system, can be seen in Table 2.1.1.

Table **Kesalahan! Tidak ada teks dari gaya yang ditentukan dalam dokumen.**.1 Identification Of Problems

The Object	System Running	Problems
Inspection connection	Done manually, by doing the testing against the host or service one by one	Requires a lot of time to test the availability of host or service problem in the response makes it difficult
The logging host and service conditions	there is no	The unavailability of documentation of the circumstances of the network
Notification	there is no	There is no

System		documentation of the reporting State of the network
Condition monitoring devices on the network	Perform remote SSH port through device one at a time	Hard to do on many devices within the routine
recovery system	Configuration manually	Hard to do because it requires time in the transfer server

After identifying the problem then the next filing system which offered to resolve the problems, can be seen on the chart Table 2.1.2

Table **Kesalahan! Tidak ada teks dari gaya yang ditentukan dalam dokumen.**.2 The System Offered

The Object	System Running	Sistem Ditawarkan
Inspection connection	Done manually, by doing the testing against the host or service one at a time with	An examination of the entire host and service automatically
The logging host and service conditions	there is no	Automatic logging against conditions and hosted services
Notification System	there is no	Email-based notification provides the notification related to the existing conditions to Technical Network & System
Condition monitoring devices on the network	Perform monitoring devices one by one	Monitoring distributed throughout all the devices automatically
recovery system	Done manually	The response automatically with DNS Failover method

2.3 Analysis Of System Architecture

Analysis of system architecture is useful for describing how the monitoring system will be applied and describe the interaction between components of the architecture in it, for more details you can see in Figure 7.

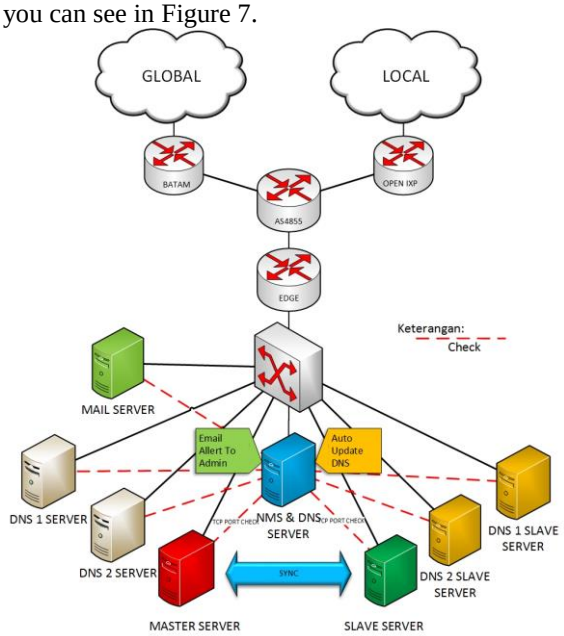


Figure 7 Network System Architecture

2.4 Analysis of the Hardware and Software Requirements

This step describes the hardware and software requirements as well as the required parameters related to support at the stage of implementation.

1. Hardware/hardware requirement referred to in this research is a set of computers that installed operating system will be in use to do the implementation. The hardware that is needed can be seen on table 2.1.3.

Table **Kesalahan! Tidak ada teks dari gaya yang ditentukan dalam dokumen.**.3 Minimum Hardware Requirements

Hardware	Specifications
Processor	Intel Pentium Dual-Core 800MHz
Ram	3 GB
Harddisk	40 GB
Monitor	CRT/LCD minimum resolusi 1024x768
Mouse+Keyboard	-

2.5 Communication System Design

At this stage the design of communication between system describes how working in the communication between the Monitoring System network with the Domain Name System. Design of communication between Systems can be seen in Figure 8.



Figure 8 Communication Between The System

in Figure 8 describes the communication that is done by a system of Monitoring network with the Domain Name System, is carried out by making use of API as a medium to communicate to DNS changes.

2.6 Notification System Design

At this stage the design notification system describes the inner workings of a notification when there is a change of status. The Notification System design can be seen in Figure 9.

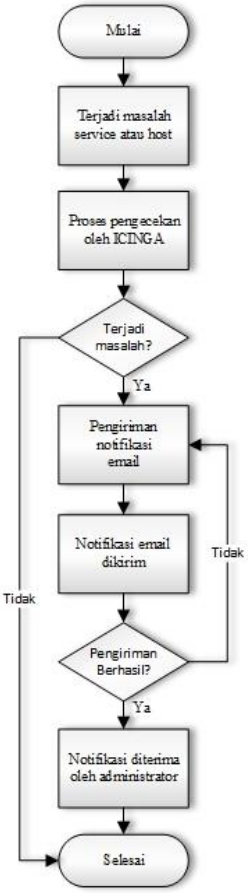


Figure 9 Email Notification Flowchart

2.7 Design of the DNS Failover Method

At this stage the design of DNS Failover describes the inner workings of fixing servers that are experiencing interference. Designing DNS Failover can be seen in Figure 10.

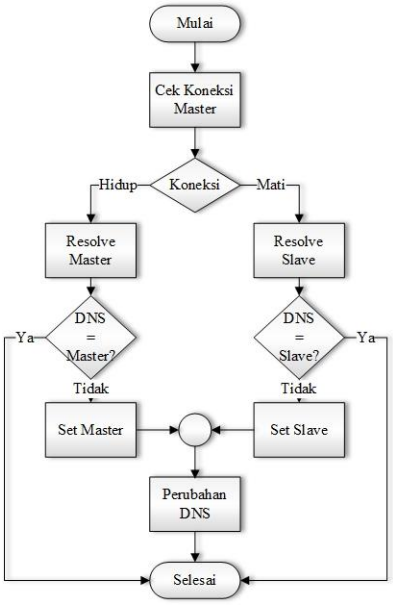


Figure 10 Flowchart DNS Failover

2.8 Environment Implementation

Environment implementation of environmental requirements is include hardware or software that are recommended to run or access the system.

1. Hardware Environment

   The following are the specifications of the hardware used in the running system, hardware that is needed can be seen in table 2.1.4.

Table **Kesalahan! Tidak ada teks dari gaya yang ditentukan dalam dokumen.**.4 Hardware Implementation

No.	Hardware	Specifications
1	Processor	i5 3.30 Ghz
2	RAM	4GB
3	Harddisk	250 GB
4	Monitor	CRT/LCD minimum resolusi 1024x768
5	Mouse+Keyboard	-

2. Environmental Software

   the specification of the software used in the running of the system, the software that is needed.

2.9 System Testing

The test system is the stages to test the system that has been implemented, with the aim to find a shortage nor excess in the system. Testing conducted include parameters and components associated with the system of Monitoring the network and DNS Failover.

2.10 Test Plan

The plan was a way of testing that will be done to ensure that the system has been implemented to meet the requirements that have

been designed before. At the stage of testing done functional tests for which there has been appropriate or there is still a shortage.

2.11 Testing Scenarios

The test scenario explains the sequence of testing to be performed on software that has been implemented. Scenario testing will be undertaken to focus on the problems that occur. It will be made two test scenarios that will do that is testing with the manual and the testing with tools. The test scenarios include:

1. Skenario manual, dengan mematikan *service http* server master yang berkaitan dengan *triger* DNS Failover, dilakukan secara manual terhadap *service* tersebut.
2. Skenario *tools*, dengan menggunakan *tools* yang dilakukan dengan mengirimkan beban *trafic* terhadap server master. Detail dari skenario pengujian *trafic* dapat dihihat pada. Adapun besaran paket adalah *KiloByte*.

Table **Kesalahan! Tidak ada teks dari gaya yang ditentukan dalam dokumen.**.5 Testing Traffic

No	Percobaan	Jumlah paket	Ukuran Paket (KB)	Port
1	Experiment ke-1	10	50	80
2		10	60	80
3		10	70	80
4		10	80	80
5		10	90	80
6		10	100	80
7		10	120	80
8	Experiment ke-2	100	50	80
9		100	60	80
10		100	70	80
11		100	80	80
12		100	90	80
13		100	100	80
14		100	120	80
15	Experiment ke-3	1000	50	80
16		1000	60	80
17		1000	70	80
18		1000	80	80
19		1000	90	80
20		1000	100	80
21		1000	120	80
22	Experiment ke-4	10000	50	80
23		10000	60	80
24		10000	70	80
25		10000	80	80
26		10000	90	80
27		10000	100	80
28		10000	120	80
29	Experiment ke-5	100000	50	80
30		100000	60	80
31		100000	70	80
32		100000	80	80
33		100000	90	80
34		100000	100	80
35		100000	120	80
36	Experiment ke-6	1000000	50	80
37		1000000	60	80
38		1000000	70	80
39		1000000	80	80
40		1000000	90	80
41		1000000	100	80
42		1000000	120	80
43	Experiment ke-7	1000000	50	80
44		1000000	60	80
45		1000000	70	80
46		1000000	80	80
47		1000000	90	80
48		1000000	100	80
49		1000000	120	80

2.12 System Testing

Following are the results of the testing that has been be scenario on the previous discussion.

1. The first test will be conducted in the form of the simulation when the service is shut down manually which later monitoring system will check availability of http service that runs against a master http server service is shut down.
2. The second test will be conducted in the form of the simulation when the service was given a high traffic load with tools that would monitoring system will check the availability of the service that runs against the service server traffic load high burdened. The test is a type of attack against a computer or server known DDoS (Distributed Denial of Service attacks) and spend the bandwidth resource owned by the master server. By using DDoS tools as goldeneye tools and Linux as the operating system.

2.13 Testing Evaluation

Based on the results of the testing that was done, whether tlah testing conducted both manual testing with a conclusion that can be drawn:

1. Functional monitoring system that exists on a network running in accordance with the design that has been created before, in the handling of errors that exist on the system.
2. The capability of the system in tackling the problems of DNS Failover can be seen that the system can cope with fast time set.

3 CLOSING

3.1 Conclusion

Based on the results of the research and testing that is performed on a system tlah Network Monitoring System using ICINGA using Failover DNS and PowerDNS some conclusions can be drawn as follows:

1. Network Monitoring system implemented can be used by the company to monitor the server.
2. Network Monitoring system implemented can make Technical Network System in monitoring & network conditions and help cope with the problems that will occur.

3.2 Suggestion

As for suggestions for the development of the Monitoring System Network are as follows:

1. Development of Monitoring System Network further so that it can be used for all the zone server.
2. Log results from ICINGA can be used for the development of value-added information in network management.

DAFTAR PUSTAKA

[1] P. Beertema, "Common DNS Data File Configuration Errors," Oktober 1993. [Online]. Available: https://tools.ietf.org/html/rfc1537.

[2] Sugiyono, "Perspektif Metode Penelitian Kualitatif dan Kuantitatif," dalam Metode Penelitian Kuantitatif Kualitatif dan R&D, Bandung, Alfabeta, 2014, p. 4.

[3] W. Stallings, Data and Computer Communications (Tenth Edition), Tenth edition penyunt., New Jersey: Pearson Prentice Hall, 2014, p. 917.

[4] W. Stallings, Data and Computer Communications (Eighth Edition), Pearson Prentice Hall, 2006.

[5] I. B. J. E. A. F. C. F. H.-G. H. J. D. M. Sebastian Abeck, Network Management, Elsevier, 2009.

[6] JSON, "Introducing JSON," [Online]. Available: http://www.json.org/json-id.html.

[7] T. V. R. A. Peter Membrey, The Definitive Guide to CentOS, Apress, 2009.

[8] ICINGA, "About Icinga 2 : Icinga web," [Online]. Available: http://docs.icinga.org/icinga2/latest/doc/module/icinga2/toc#!/icinga2/latest/doc/module/icinga2/chapter/about-icinga2#what-is-icinga2. [Diakses 5 Oktober 2016].

[9] PowerDNS, "PowerDNS Recursor," [Online]. Available: https://www.powerdns.com/recursor.html.

[10] Kali Linux, "Introduction Kali Linux," [Online]. Available: http://docs.kali.org/introduction/what-is-kali-linux.