Dashboard for Monitoring Network Operations

Eka Stephani Sinambela
Department of Computer Network Technology, Del Institute of Technology

Keywords:

SNMP
Dashboard
Monitoring using SNMP

ABSTRACT

Network devices such as server, router, printer that operated in the company or an organization, should be monitored and managed well, to guarantee reliability, and availability of networks. The operational network devices are not only monitored in event of problems, but should be monitored periodically and reported centrally.

In order to achieve the objective, we need a monitoring application to monitor the operation of network devices that usually termed as "Monitoring". Not only by using monitoring application, but also the important thing is to show all the monitoring result on the dashboard.

Periodically monitoring can be run by using monitoring application and centralize reporting can be visualized by using dashboard application. The result of real-time monitoring devices will be displayed as a graph or tables in a dashboard.

In this research, the development both applications use the Object Oriented Concept and network protocol that called SNMP (Simple Network Management Protocol), which is used for getting information of network device, hereinafter referred to as managed devices. Some devices information, produced by using SNMP are devices connectivity, service connectivity, and devices utility.

The outcome of this research is the application of monitoring and dashboard application that are highly expected to help network administrator to identify network devices problems, so that problems can be solved with the right solution, and effectively.

Corresponding Author:

Eka Stephani Sinambela,
Department of Computer Network Technology,
Del Institute of Technology,
Jalan Sisingamangaraja Desa Sitoluama, Laguboti, Kabupaten Tobasa, Sumut, Indonesia.
Email: eka@del.ac.id

1. INTRODUCTION

Monitoring is a routine process to collect data periodically, because checking the status of all network devices one by one is impossible. Network operation must be monitored to insure the reliability and availability of network and not only monitored when the problem happen, but must be monitored periodically with centralized reporting. Mostly, the result of network monitoring is visualized in different reporting. So there is possibility, all the network devices are not monitored periodically, and even are not observed at all.

This research will focus on monitoring activity and centralized reporting, with three main parameters, they are devices connectivity, service connectivity, and devices utility. All the information of network devices will be collected by using a network protocol called SNMP (Simple Network Management Protocol) and will be visualized on a dashboard. This research gives more flexibility for network administrator to register all their network devices and to determine the OID (Object Identifier) of all devices that will be monitored in the monitoring application that has been built.

All data obtained in the real-time from the network devices is critical data. So, a network administrator should be aware and responsive in all data changes, although not all situations require ongoing moment-to-moment awareness. To support this awareness situation, dashboard designed with well designed.

Only what necessary appears on the dashboard, it is not cluttered or distractingly decorated, and display on one page.

2. RESEARCH METHOD

This research begins with determining the information or data to be retrieved from the managed devices that will be analyzed. After the stages of data analyst, then proceed with the application requirement analysis, followed by the implementation stage. The applications built using OOP concepts, with Java programming, open source software Style Scope, and DBMS mySQL Server. Due to limited access to managed devices, then sample data to accomplish this research, retrieved from a web server.

2.1. SYSTEM ARCHITECTURE

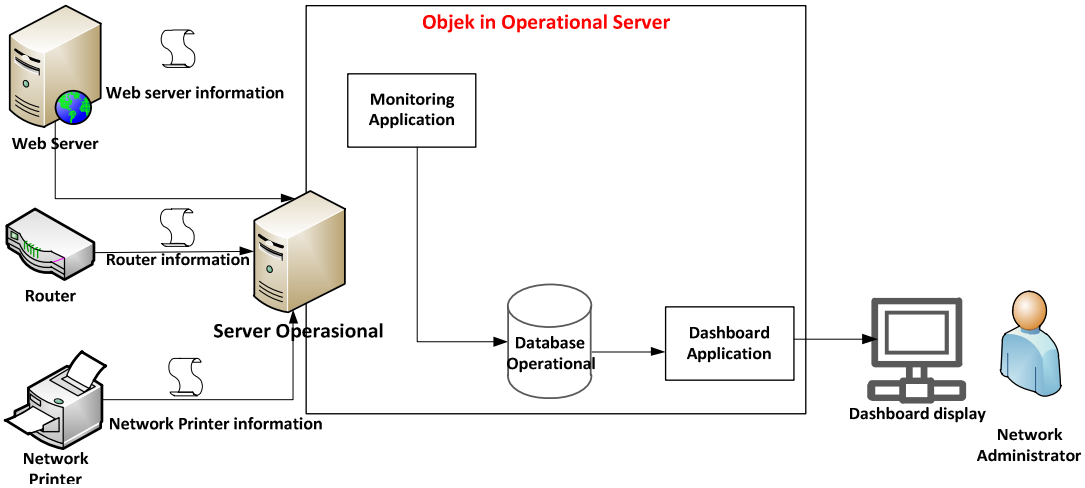

Figure 1. System Architecture

In (Figure 1) Web server, router, and network printer are few examples of devices which are monitored called managed devices. There are two parts of application that are independent in server operational; they are monitoring application and dashboard application. Monitoring application functions as a data collector from managed devices, and supplier data into database operational, whereas Dashboard application functions as data receiver from database operational and will display the data on the dashboard.

2.2. APPLICATION DESCRIPTION

Based on system architecture in (Figure 1) there are two main applications, they are dashboard application and monitoring application, which are described below.

a. Monitoring Application

SNMP protocol in monitoring application, using a database of device object Identifier (OID) called Management Information Base (MIB). At MIB there is a list of unique OID for each managed devices, which is written as decimal number, separated by using a point, for example 1.3.6.1.4.1.2682.1. SNMP agent must be installed by network administrator in all managed devices and, the version of SNMP manager must ensure equal to, or compatible with SNMP Manager. The SNMP manager and SNMP agent communicate by using service provided by TCP/IP protocol. Information exchange between SNMP manager and SNMP agent occurs at the transport layer by using access port. SNMP manager using random port of machine to request information to SNMP agent, and to respond request from SNMP manager, SNMP agent using UDP port 161. The flow of retrieve information by SNMP manager to SNMP agent, illustrated in flowchart below.

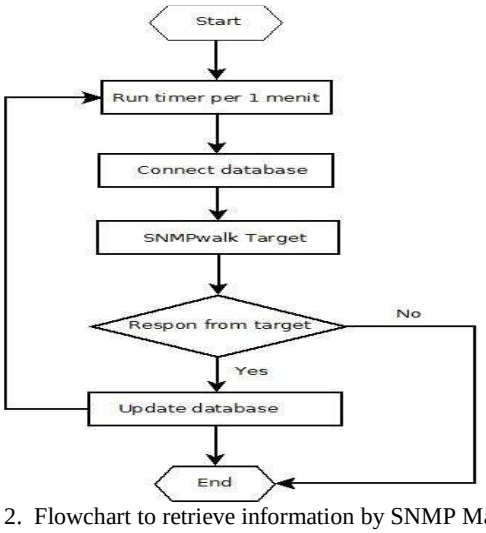

Figure 2. Flowchart to retrieve information by SNMP Manager

The explanation of flowchart are:

1. Timer will be run every one minute, activating SNMP manager.
2. SNMP manager build connection to database, for getting IP address of SNMP agent, and OID.
3. SNMP manager runs command GetNext as snmpwalk.
4. SNMP agent responds the request, and sends information, then saves the information into database.

All of device information retrieved by using monitoring application are device connectivity, service status, device utility, and type of operating system, explained detail as below.

1. Device Connectivity
   Information retrieved from managed devices such as server, router, firewall, and printer is up or down status. If the connectivity status is up, then the device is connected to network, and vice versa.
2. Service Status
   Service monitored is the service that runs in managed devices, such as squid service that runs in proxy server, sharing file service in file server, http service in web server, and printing service that runs in a network printer.
3. Network Device Utility
   The utility Information monitored from network device is CPU utility, memory, and disk utility. The attribute of each utility is the total CPU, memory capacity, and disk capacity that has been used and still available.
4. Operating System
   Information taken from the operating system is the name and the version of operating system installed, for example the operating system a server is Ubuntu and the version is 10.04.

b. Dashboard Application

Dashboard application is the application for displaying data (all devices information) that are supplied from database operational illustrated in Figure 3.

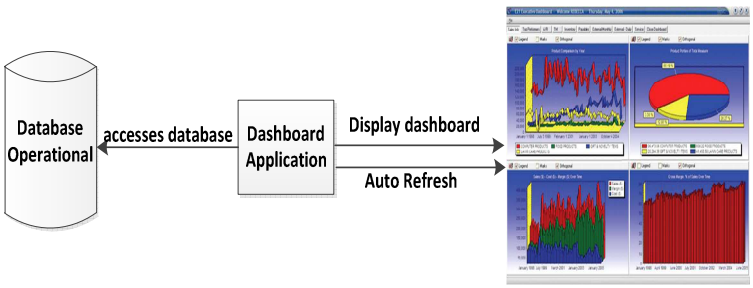

Figure 3. Process flow of dashboard application

The explanation of Figure 3 are:

1. Dashboard application accesses database operational as data supplier.
2. Then, it shows and classifies it as monitored resources.
3. Application will be run auto refresh as periodically to update data in dashboard.

The process of updating data on the dashboard starts from the process of retrieving information from managed devices by SNMP manager, storing data into database, and displaying the data back to the dashboard. Periodic checking needed to do the whole process and it is estimated that the minimum time to do the whole process is 54 µs, based on the following calculation.

1. Based on the result of data capturing from managed devices, the minimum size of packet or data is less than 1 KB (1024 bytes), transmitted via UTP cable with speed 100 Mbps. We need to calculate the time of packet transmission in this following way.
   Packet Transmission Time = Packet Size / Bit rate
   = 1024 * 8 bit / (100 000 000 bit/s)
   = 8.192 µs
2. Signal propagation that occurs in the physical media used for data transmission, also affects the transmission time. The propagation speed of communication via UTP using copper cables is in the range 2×10^8 m/s, while the maximum distance of UTP is 100 meters, therefore we need to calculate the maximum link propagation delay in this following way.
   Maximum Propagation Delay= Distance / propagation speed
   = 100 m / (200 000 000 m/s)
   = 0.5 µs
3. After calculating point 1 and 2, we need to calculate packet delivery time, which is calculated from the first bit to the last bit transmitted, by total the transmission time and propagation delay, in this following way.
   Maximum Packet delivery time = Transmission time + propagation delay
   = 8.192 µs + 0.5 µs
   = 8.692 µs (rounded to 9 µs)
4. We need packet delivery time to calculate roundtrip time. Roundtrip time is the starting time of data transmission from sender, until a response receives from receiver. Therefore, periodic checking done by SNMP manager adjusted with roundtrip time, calculated in this following way.
   Roundtrip time* = 2 * *packet delivery time
   = 2 * 9 µs
   = 18 µs
5. Dashboard application run auto refresh function to update real-time data in dashboard, by setting the refresh interval or periodic checking time. It is estimated that maximum time to insert data into database is 18 µs, and maximum time to access operational database is 18 µs. So, we need to calculate refresh interval time, in this following way.
   Refresh interval= Roundtrip time + time to insert database + time to access database
   = 18 µs + 18 µs + 18 µs
   = 54 µs

3. RESULT AND ANALYSIS

This research produces application monitoring and dashboard that can be accessed by network administrator, who has full access to managed application, such as register all network devices, and register OID of network devices, as shown in Figure 4 and Figure 5.

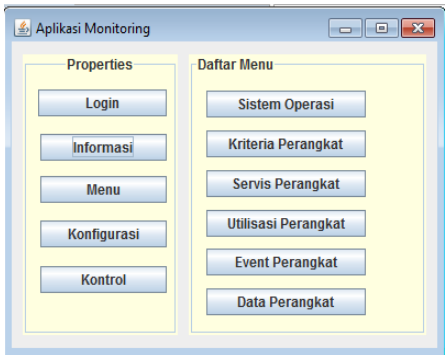

Figure 4. Main Menu Monitoring Application

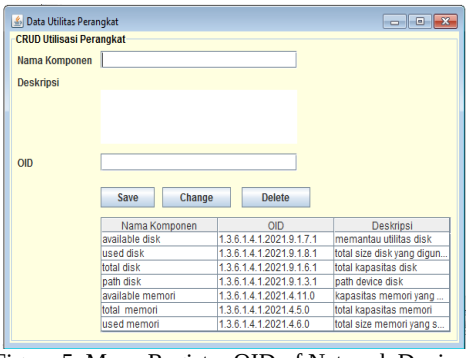

Figure 5. Menu Register OID of Network Devices Component

Dashboard as the result of monitoring process will be displayed in one layer in the form of graphs and table, by using dashboard application Style Scope Free Edition as shown in Figure 6. Information

displayed in dashboard is the information of device connectivity, service status, and device utility by using queries that retrieve data from database operational, displayed on one page dashboard.

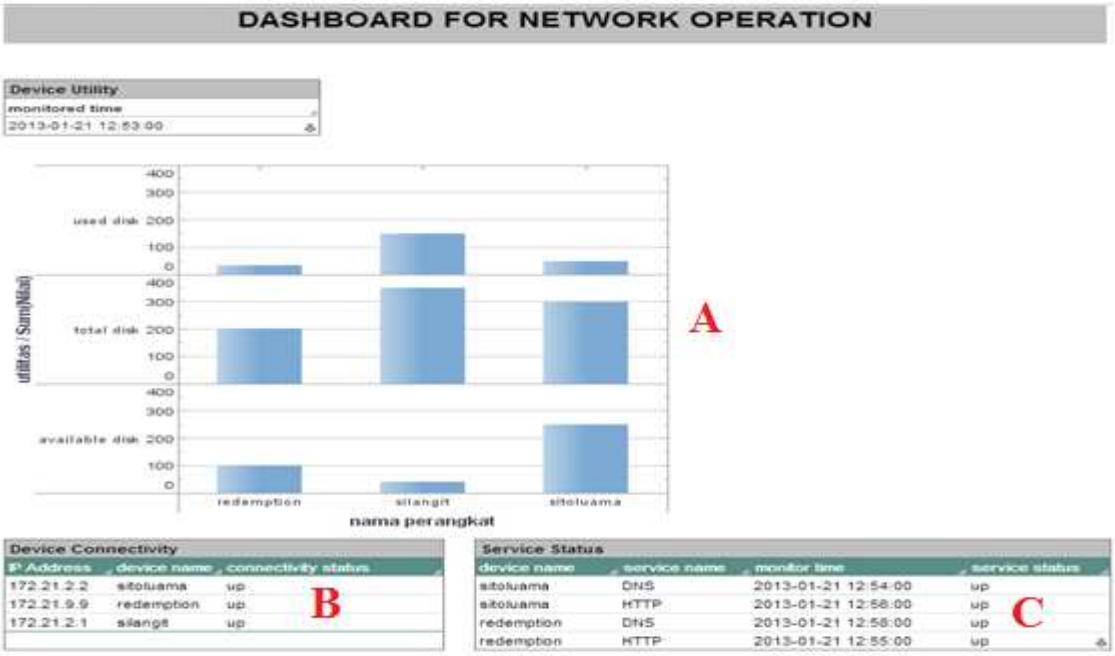

Figure 6. Dashboard Display

Display dashboard consists of three components, with detailed specification as follows:

1. First component is display device utility.
   This component display about device utility information consists of device name, IP Address, OID name, monitored time, and total utility. All information displayed in the form of graphs and table, as shown in point A in **Figure 4**. Testing conducted to obtain data from device, do the following ways.
   a. In the below command mentioned OID 1.3.6.1.4.1.2021.91.8.1 which is use to check used space disk.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.4.1.2021.9.1.8.1
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 61513592
```

   b. In the below command mentioned OID 1.3.6.1.4.1.2021.9.1.7.1 which is use to check available disk.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.4.1.2021.9.1.7.1
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 82549088
```

   c. In the below command mentioned OID 1.3.6.1.4.1.2021.91.6.1 which is use to check total disk.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.4.1.2021.9.1.6.1
UCD-SNMP-MIB::dskTotal.1 = INTEGER: 151772320
```

   d. In the below command mentioned OID 1.3.6.1.4.1.2021.91.8.1 which is use to check the location of disk.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.4.1.2021.9.1.3.1
UCD-SNMP-MIB::dskDevice.1 = STRING: /dev/sda1
```

2. Second component is service status.
   The second component display about device service status, consists of device name, IP Address, service name, monitored time, and status service connectivity. All information displayed in the form of table, as shown in point C in **Figure 4**. Testing conducted to obtain data from device, do the following ways.
   In the below command mentioned OID 1.3.6.1.4.1.8072.1.3.2.2.1.21 which is use to check service status of http server. If the value of http_pid is active(1), it indicates that the http server service status is up.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.4.1.8072.1.3.2.2.1.21
NET-SNMP-EXTEND-MIB::nsExtendStatus."httpd_pids" = INTEGER: active(1)
```

3. Third component is device connectivity
   The third component display about device connectivity, consists of IP Address, monitor time, and status connectivity, whether down or up. All information displayed in the form of table, as shown in point B in **Figure 4**. Testing conducted to obtain data from device, do the following ways.
   In the below command mentioned OID 1.3.6.1.2.1.2.2 which is use to check device connectivity. If the value of MIB ifAdminStatus.2 that related to ethernetCsmacd on MIB ifType2 is up(1), it indicates that the device connectivity is up.

```
[root@nm ~]# snmpwalk -v 1 -c nm-del localhost .1.3.6.1.2.1.2.2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 16436
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 10000000
IF-MIB::ifSpeed.2 = Gauge32: 100000000
IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING: 0:16:76:39:4:f3
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
```

4. CONCLUSION

The research with entitled “Dashboard for monitoring network operations”, produce two dependent applications named, monitoring application and dashboard application. Monitoring application is a desktop application, which aims to monitor all network devices, in accordance with device OID that has been registered in application. Data that has been obtained from monitoring process will be saved in database operational, that useful as an intermediary between monitoring application and dashboard application.
Dashboard Application accesses the real-time data from database operational, and display it in the form graphs and table. This dashboard will help network administrator to know quickly about their network operation status, and do fast handling if there are any problems are detected.

However this research needs further development to reorganize dashboard, to make interactive display. All data that related to status service, and device connectivity, should be illustrated by on or of icon with a specific color. So, it will help network administrator to identify faster about the status of service and device connectivity by looking at icon than reading text.

ACKNOWLEDGEMENTS

I would like to express my thanks to my adviser Ms. Inggriani Liem, Mr. Arief Zulianto, and Mr. Yudi Satria Gondokaryono that give me advice and conduct me to finish this research and also to my colleagues on network department, who reviews this paper content and give valuable suggestions.

REFERENCES

[1] S. Few, “Dashboard Design for Real-Time Situation Awareness”, Inova Solutions, 2007.
[2] B.A. Forouzan and S. C. Fegan, “Data communications and networking”.
[3] T. Schenk, “Red Hat Linux: System Administration”, Techmedia, America, 2000.
[4] S. Few, “Information Dashboard Design”, O’Reilly, 2006.
[5] Tutorial Net_SNMP, http://www.net-snmp.org/wiki/index.php/Tutorials, accessed on November 15th 2012.

BIBLIOGRAPHY OF AUTHORS

Eka Stephani Sinambela, a teaching assistant in Del Polytechnic of Informatics. She granted the Diploma 4 of Computer Engineering and Networking in 2013 at Bandung Institute of Technology.
Her research interests are mainly on networking programming, data communication, and networking development.