MONITORING AND MANAGEMENT THE ENTERPRISE NETWORK VIA PRIME NETWORK

Yensira Tantitakurn[1] and Khanista Namee[1]

[1]Department of Information Technology, Faculty of Industrial Technology and Management,
King Mongkut's University of Technology North Bangkok, Prachinburi, Thailand
Emails: 5606021612138@Fitm.Kmutnb.ac.th, Khanista.N@Fitm.Kmutnb.ac.th

ABSTRACT

This research implements Prime Network to assist in the management of monitoring and diagnostic systems, the network devices in the enterprise network is across the country. This system can operate as a hierarchy. A notification is sent to the network admin when a problem occurs in the network. Moreover, This is an excellent tool to monitor new diagnostic problems in large networks, to prevent problems that might occur in a timely manner. The results of this implementation show that the Prime network supports applications on the network very well with high performance.

Index Terms–*Prime Network; Network Monitoring; Enterprise Network Monitoring*

1. INTRODUCTION

To monitor network devices in the huge network is a tricky management because this type of network can have up to 1000 devices. The question is, how can we manage all of them? If a problem occurs in a large network, how do we know? How do we locate where the problem is? It can occur at any location where the device is. The device problem could be in another province, and far away, how are we going to deal with this problem? Also, if the bandwidth on the network is unusual, how do we know? Identifying the issue quickly will enable administration to manage the problem in a timely manner. According to the study, there is software that helps in managing these issues. This software is the Prime Network.

The objective of this research is to implement Prime network to a large network. In our experiment, the testing network offers the leading telecommunication company in Thailand. There are hundreds of devices in the network covering Thailand. This telecommunication company had a major requirement to provide network monitoring of the Prime Network and is able to manage the whole network system. Also, they want to monitor the performance of the devices within the network more effectively. Including, an alert to the administrator completely without flaws or weaknesses in the monitoring system. Many devices within the network, each device is different location. If without the monitoring system, it makes network Admin act tough in order to check for defects or damage within the network.

The rest of this paper is organized as follows. Section II provides a brief overview of some software which had to be implemented within this research. Then, in Section III, the system designs of hardware and software components are presented in detail. The experimental deployment and measurement results are presented in Section IV to demonstrate the design. Finally, conclusions are drawn in Section V and following with acknowledgement in Section VI.

2. BACKGROUND

This section will describe the literature review and theories related to this research.

2.1. Prime Network

Prime Network is Cisco software used for inspection or monitoring of network. It will also detect errors within the network and notify the network administrator. The monitoring program will reduce the burden on system administrators to monitor the network. If there are any error events or device events occur on the network, it will inform the administrators to know whether it is caused by a general or device log. Each event report will have the status of the network. The report will show the result of the error, if there is serious damage to the system or not. The function of the Prime Network is a hierarchy. It can divide into the Gateway and Unit Prime Network [1].

Prime Network is a program that can monitor the status of the network and is responsible for a thorough check of devices in the system, which will divide both the logical and physical check in to the device within the network. The system is designed for very large networks.

The Prime Network server is divided into two parts: Prime Network Unit and Prime Network Gateway. Both parts have a different functionality.

2.1.1. Prime Network Gateway

This part is a command of the system to monitor network equipment and will be responsible for direct contact with the administrator. When administrators want to direct or control the management system, it will work through the

Agent and will connect directly to the Prime Network Gateway. After that, the Prime Network Gateway orders to the Prime Network Unit in order to request or look up various device parameters within the network.

2.1.2. Prime Network Unit

Its task is to mediate between Prime Network Gateway and the devices within the network. The function of Prime Network Unit will be responsible for Telnet SSH to the network devices within the system and is responsible for monitoring the status of the devices through the protocol SNMP Polling, a protocol for monitoring devices and networks. There are 2 types of SNMP protocol for monitoring the transmission of data within network: Trap and Polling [2].

Trap is sent from the device to an administrator without a direct request from the Prime Network Unit, which sends status information while the device within the system has problems or damage.

Polling is a monitoring device within the system used by requesting the status of the Prime Network Unit, but must be ordered by the administrator or the time to submit Log for the defects or status of the network.

In this research, we implement the Prime Network to assist in the monitoring system and network, which helps administrators manage the enterprise network more easily. In this way, the administrator will not need to monitor the network devices by themselves. In this experiment, the network is very large. There are hundreds of network devices, devices located in remote areas as well.

2.2. SNMP (Simple Network Gateway Protocol)

SNMP stands for Simple Network Management Protocol, a network protocol in the application layer and is part of the TCP / IP protocol suite. The internet and intranet network using TCP / IP protocols with a variety of network devices and brands. The standard network management protocol that works efficiency is SNMP protocol.

Service and network management require different equipment and are part of a collaborative network management system, we call the Agent. The agent as part of the software in the devices that connects to the network with the main computer systems in one machine to manage and administer networks known as NMS (Network Management System). NMS serves as the control center and watched network with an alert [3]. When any part of a network malfunctions or crashes, administrators know immediately and are able to fix the problem quickly.

Therefore, the system administration and network management will be successful depending on the agent within the network devices. The agent also has storage inside. The data stored is called MIB (Management Information Base.) Each device on the network will have its own data stored on their MIB. Hence, the NMS sent questions to the agent for requesting the data which is stored in the MIB database. Submitting questions and getting answers shall be based on the format of standard protocols which is SNMP protocol [4].

2.3. UCS Server

A UCS server can be created by combining the processing, network, storage systems and virtualization together with comprehensive management system performance. This is a revolutionary technology of Data Center altogether.

2.4. SecureCRT

This program is used for Remote Login to a UNIX operating system server and other network devices that support Remote Protocol such as FTP, Telnet, SSH and etc. Moreover, it supports Serial Protocol. This software is designed as a Graphic Interface Mode which is easy to use. In this research, we use Secure CRT software which enables the configuration of devices on the network. Including access to the remote server to configure or install an additional package to the server.

2.5. VMware ESXi

The VMware ESXi is a simulation software that simulates an operating system as a virtual machine. The idea is for using one server (hardware) to create many virtual machines with a variety of operating systems. By using VMware ESXi, the system can operate faster than conventional computers. However, this must be based on the number of resources within a server. The VMware ESXi supports all VMware vSphere Client and the ability to work independently because it does not have to run on other operating systems. Another advantage is that VMware ESXi consumes little system resources. In this research, we us ESXi operating system to manage servers by working as a virtual server. The ESXi manages the resource of the system most effectively.

2.6. VMware vSphere Client

The VMware vSphere Client is a product of VMware, one of the key variables in the system of Server Virtualization. This is part of SDDC (Software-Defined Data Center) consists of three main systems, Server Virtualized, Network Virtualized and Storage Virtualized. To manage the servers with virtualization within ESXi, which is a program used to control the ESXi operating system. In order to create or edit a Guest within internal server and Snapshot of information on a Guest were also able to do so through the VMware vSphere Client, etc. (Snapshot is to collect data over time, for the prevention or errors to the system in the future. When a problem occurs, it can be traced back to the same data within the system at the time of the Snapshot.) In this research, we use VMware vSphere Client to access the Virtual Server to accommodate the users so it can be easily handled with Virtual Servers inside.

3. SYSTEM DESIGN AND IMPLEMENTATION

In this experiment, the system will monitor an enterprise network system. This is the prime network monitoring functionality of the device within the network more effectively and will alert to the system administer completely without flaws or weaknesses in the monitoring system. There are many devices within the network, each device is different location. Without this system, the monitor and network admin act tough in order to check for defects or damage within the network. There are 7 steps as following [5].

3.1. Survey Network Infrastructure

To simulate real network, we need to monitor the system or network infrastructure. The simulation system should have a process or format similar to the real network, to be able to monitor the replication needs.

3.2. Examine the operation of the monitoring system in real network problems

When monitoring the network device problems or damages, the system will generate Trap reported to Prime Network Gateway using a Trap SNMP protocol, which is sent from the device itself. This information will be sent in real time to alert to the administrator. For the operation Poll, generated by Poll SNMP protocol. The benefit of Poll is to see the Log of equipment which will be delivered from around based on administrator-defined. In order to keep the device or Syslog, but will not get the information real time as SNMP Trap, which studies this process. It is very important in the analyze system and their problems.

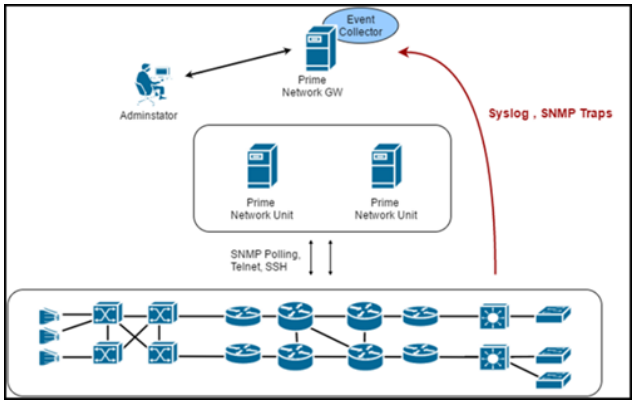

Figure 1. Shows the layout of the monitor.

3.3. Learning how to install the Prime Network

Study Guide to install Cisco Prime Network 4.2.2 to prepare to install the server to the study prior to the actual installation. Once installed, which makes it really makes installation faster or cause trouble to install, and will cause less expertise in server and so on [6].

3.4. Learning how to monitor the network via the Prime Network

Learning about the operation of the Prime Network in order to learn the process of monitoring, investigating, and learn how to verify the network devices. What is the protocol used to request information from the device? If a problem does occur, how does it report that problem to administrator? Also, how does the system generates Trap notifications for sending to the Prime Network Gateway?

3.5. Studying about an operation of Virtual Server on ESXi operating system

Studies in the Virtual Server function of ESXi, however, that the allocation of resources to give each Guest and learn how to manage Guest within ESXi. The ESXi can be supported by the operating system for a variety of Guest Operating System. Also, the ESXi can enhance the efficiency of Guest from the original by allocation of resources to the limit as high as 128 CPUs RAM 4 TB. For example, the ESXi is a Hypervisor software application, which installed on the server hardware, and serves as the operating system that runs between the Virtual Machine.

3.6. Survey the network devices

Studying and monitoring equipment to see the needs of the organization and use the network to achieve the highest performance according to user requirements. This is important because if the network does not meet the needs of customers, it may be the result of a system crash or monitor. Therefore, it is necessary to explore and determine the needs and the actual system. When the survey is complete, it is necessary to examine the inside of the organization. There is not a device that can replace it. Also, be sure to configure the devices and connections within the system, in order to simulate a real system.

3.7. To determine the IP Address and manage a resource for servers

Table 1 is designed to monitor system resources by Cisco Prime Network Unit, which is to support the functioning of the systems stability. There must be a speed monitoring system. The memory must have enough space to store the data from the monitoring system. Including processing, it can be processed efficiently and in accordance with the speed of the system to avoid flaws or weaknesses in the system.

Table 1. Details the resources of the server as Prime Network Unit.

Virtual Server Name	CPU	RAM	Storage
Prime Network Unit 1	2 core	32 GB	500 GB
Prime Network Unit 2	2 core	32 GB	500 GB

Table 2 is the design stage that assigns IP Addresses to the server. There are two parts that have to be assigned: Management IP and OS IP. The Management IP is intended for use in the management of UCS Server by web browsers. This is a feature of the UCS Server, it has come out with a lot of features for managing the server.

Another part is designed to be part of the operating system in use for OS IP connectivity between servers. However, the operating system ESXi is also used for the management of Virtual Server within the system software vSphere Client which IP Address is essential. Moreover, it is a Gateway for a Virtual Server that is used to connect to a server or external network device.

Table 2. Details the defined IP Address with UCS Server.

Devices	Types	IP	Netmask
UCS Server Gateway	Manage IP	192.168.0.200	/24
	OS IP	192.168.0.33	/24
UCS Server Unit	Manage IP	192.168.0.201	/24
	OS IP	192.168.0.31	/24

Table 3 IP Address is designed for servers as Prime Network Unit, which is used for connections between servers and devices within the system for monitoring and mandated by the administrator through the Prime Network Gateway.

Table 3. Details the defined IP Address to a Virtual Server Unit.

Virtual Server Name	IP	Netmask
Prime Network Unit 1	192.168.0.34	/24
Prime Network Unit 2	192.168.0.35	/24

4. RESULTS

Results from the experiment in each section can be displayed as follows.

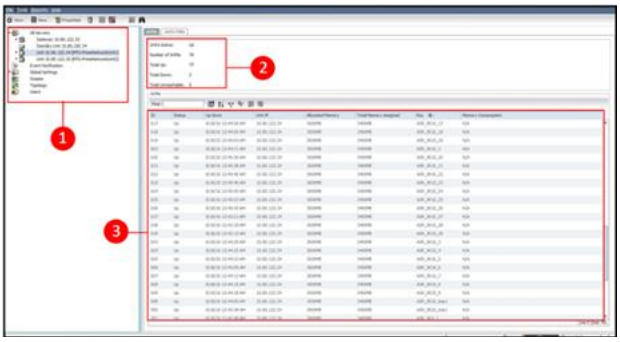

Figure 2. Shows the first page of the Prime Network for administration.

The Figure 2 shows the first interface for administrators who can manage and organize the server of Prime Network for the whole system. Each parts of this interface will be described as following.

1) Shows the server where it is each the Prime Network Gateway and Unit.

2) Shows the status of the server on which to monitor, which is called AVM. The AVM are divided into ID. The AVM in each ID will be responsible for maintaining the device in several parts on the network.

3) Shows the list of devices that each AVM controls and the details of each device.

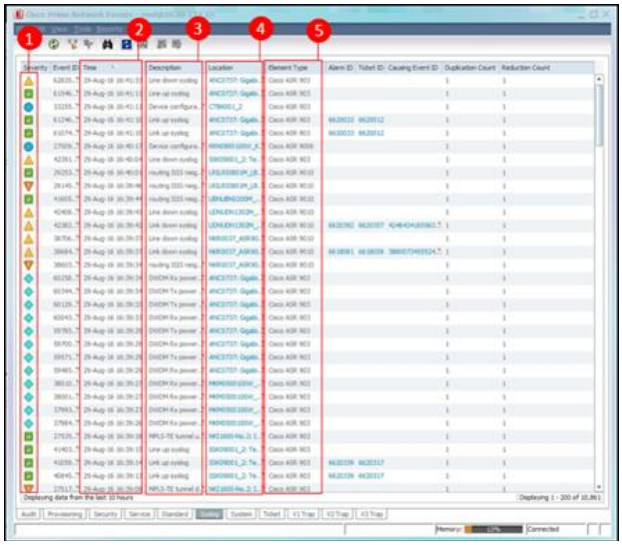

Figure 3. Shows the results of the Event List as Syslog.

This section is the interface of the Event, which shows every event that happens within the system. The information contained in Event information will be sent by network devices such as router and switch. The Event that was reported to the Gateway can divided into 2 types.

1) Data is sent from the device when an action or event takes place on the device. A device Log will be sent to Prime Network immediately.

2) Data from the Poll from the server to the storage device Log and report to the Prime Network, data administrator will then analyze.

The system will separate sections of the event list displayed in of the Syslog and Trap separately in order to easily manage the problem with ease of administration.

In the Figure 3, the interface is divided into five parts.

1) *Severity*: this part shows the type of data source or Log display, which is separated into 5 levels.

1.1) Information: Log on as general information.

1.2) Warning: A warning of this type or that type of Log that the device may not be aware of the risks.

1.3) Minor: Log Error within the device, which is beginning to result in a total system crash.

1.4) Major: it is a problem which can be solved, such as the Port Down, Protocol Down and so on.

1.5) Critical: to express the problem directly from the device. This is a serious problem such as a card damage.

2) *Time*: it is the time to send Log or Event. It will be a time to measure the performance of the system, whether it, can be solved quickly or not. Also, if the system can back to normal faster or not.

3) *Description*: A detailed description of the Log. What type of Log? The internal details of updates to the Event, or what happened.

4) *Location*: The Log reports where the device is, and from which part of the device. Such as an update to the name of the Router Interface Gi 0/1 to AYT2004.

5) *Element Type*: to tell the type of equipment that is up Log identifies what types of models.

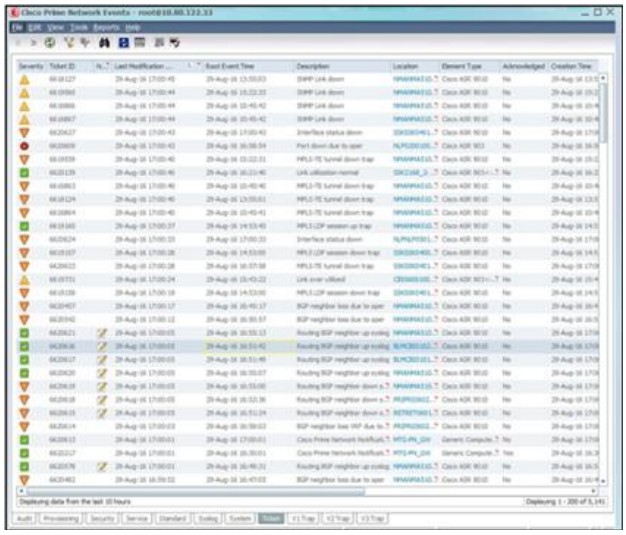

Figure 4. Shows List of Ticket.

Figure 4 shows a portion of the Ticket List, which will reduce the complexity of the system and Ticket. The Event will show the Location or Device name. When the Trap from the device, it will be open Ticket was a problem with the Trap and be a solution or an Event with solutions such Ticket will matching with the Event. Then the system will shut the Ticket down.

The Prime Network will generate the Ticket number automatically by comparing with the calibration of the equipment and device description. The way will make the system more stable and can control every devices and links.

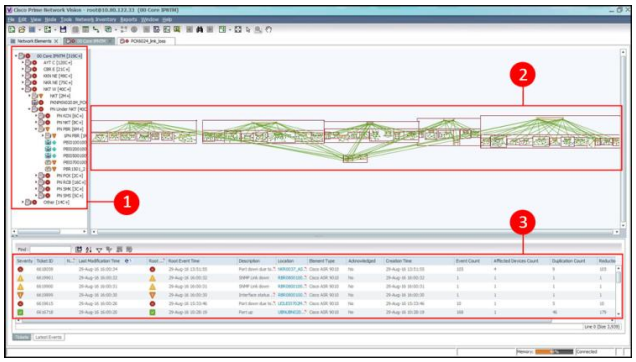

Figure 5. Shows the Topology Monitor's Vision (1).

This interface shows a topology of the network, Prime Network monitoring by mapping between physical and logical devices topology. This makes it easier to see and be able to see an overview of your network. This is suitable for working with larger networks because it allows for easier administration. The Figure 5 is divided into three parts.

1) Shown, Lists all devices within the network, this will display as hierarchy. It is divided into zones before narrowed down to the local device.

2) Shown, logical devices in the network, which is topology that shows the connection between the devices. When the administrator wants to add a new device to the system, just add the new device into this topology, then the Prime Network will Poll to that device and build a link itself automatically according to the physical structure of the network.

3) Shown, all Events going in all of the networks, which are both Poll and Trap, which will run through the SNMP protocol for monitoring.

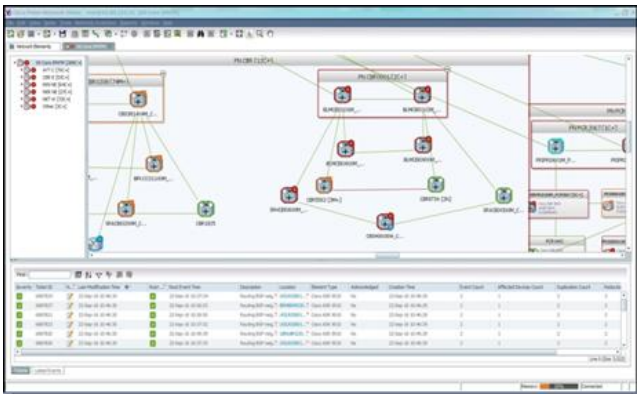

Figure 6 shows the Topology Monitor's Vision (2).

Figure 6 has the information details like in the Figure 5, however the topology in Figure 6 expanded view of a deeper level. Hence, it can show the device, distribute and access in each province.

5. CONCLUSION

This research implements Prime Network to assist in the management of monitoring and diagnostic systems that cover a very large area. The network used in experimental research is a network of a company that provides telecommunications services around the country. Network coverage across the country are required to monitor the network devices within the network. The results of this implement show that the Prime network supports applications on the network very well with high performance. A notification to the network admin when a problem occurs in the network. Moreover, it is an excellent tool to monitor new diagnostic problems in large networks, to prevent problems that might occur in a timely manner.

This system can operate as a hierarchy. The connection is complemented by Prime Network Gateway, which is responsible for the user interface directly. If the administrator wants to see the Log, it will connect the Prime Network Unit for requesting Log from them. Every process will work through the Gateway. The Prime

Network Unit is responsible for Poll to devices on the network, and then sends the information to the Prime Network Gateway, which Prime Network Unit as an intermediary between Prime Network Gateway to monitor the devices on the network. From the results, this system can monitor and manage all network devices on the enterprise network efficiency.

6. ACKNOWLEDGEMENT

This research could not have been completed successfully without supporting from Department of Information Technology, Faculty of Industrial and Technology Management at King Mongkut's University of Technology North Bangkok. We would like to deliver our greatest appreciation for their support.

REFERENCES

[1] Cisco [White Paper], "Immediate Network Synchronization with Low Overhead: Cisco Prime Network Reduced Polling VNE," Cisco Public Information, 2012.
[2] Cisco, "Service Provider Cuts Management Cost and Risk," Cisco Public Information, 2013.
[3] Rick Fletcher, Prakash Banthia, "Distributed remote monitoring (dRMON) for networks," 3Com Corporation, 2000.
[4] Hugh S. Njemanze, Pravin S. Kothari, "Real time monitoring and analysis of events from multiple network security devices," Patents, 2008.
[5] Chakchai So-In, "A Survey of Network Traffic Monitoring and Analysis Tools," 2006.
[6] Cisco, "Cisco Prime Network Installation Guide, 4.3," Cisco Public Information, 2016.