



國立勤益科技大學
電子工程研究所碩士班

碩士論文

節省檢修時間之前瞻性整合管理系統研究
**A Proactive Integrated Management System to
Save Troubleshooting Time**

研究生：邱顯錦

指導教授：陳瑞茂 博士

中華民國九十九年六月

授權書

(碩士論文)

本授權書所授權之論文為本人在國立勤益科技大學(學院)電子工程系所
光電產碩組98學年度第2學期取得碩士學位之論文。

論文名稱：節省檢修時間之前瞻性整合管理系統研究

同意 不同意

本人具有著作財產權之論文全文資料，授予行政院國家科學委員會科學技術資料中心、國家圖書館及本人畢業學校圖書館，得不限地域、時間與次數以微縮、光碟或數位化等各種方式重製後散布發行或上載網路。本論文為本人向經濟部智慧財產局申請專利的附件之一，請將全文資料延後兩年後再公開。(請註明文號：)

同意 不同意

本人具有著作財產權之論文全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限地域與時間，惟每人以一份為限。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未勾選，本人同意視同授權。

指導教授姓名：陳瑞文

研究生簽名：邱顯錦

學號：497T2003

(親筆正楷)

(務必填寫)

日期：民國 99年 7月 28日

1. 本授權書請以黑筆撰寫並影印裝訂於書名頁之次頁。
2. 授權第一項者，請再交論文一本予畢業學校承辦人員或逕寄 106-36 台北市和平東路二段 106 號 1702 室 國科會科學技術資料中心 王淑貞。(本授權書諮詢電話：02-27377746)
3. 本授權書於民國 85 年 4 月 10 日送請內政部著作權委員會(現為經濟部智慧財產局)修正定稿。
4. 本案依據教育部國家圖書館 85.4.19 台(85)圖編字第 712 號函辦理。

碩士論文電子檔案上網授權書

(提供國家圖書館辦理電子全文授權管理用)

本授權書所授權之論文為授權人在國勤益科技大學(學院)電子工程系
所光電產研組 98 學年度第 2 學期取得 碩 士學位之論文。

論文題目: 節省檢修時間之前瞻性整合管理系統研究

指導教授: _____

茲同意將授權人擁有著作權之上列論文全文(含摘要),非專屬、無
償授權國家圖書館及授權人畢業學校之圖書館,不限地域、時間與
次數,以微縮、光碟或其他各種數位化方式將上列論文重製,並得
將數位化之上列論文以上載網路方式,提供讀者基於個人非營利性
質之線上檢索、閱讀,或並下載、列印。

上列論文為授權人向經濟部智慧財產局申請專利之附件或相關文件之
一(專利申請案號: _____),請於兩年後(即 101 年 7 月
28 日後)再將上列論文公開或上載網路。

授 權 人

姓 名: 邱景錦 (請簽名並蓋章)

身分證字號: N121993002

地 址: 台北市西七路三段301231号1F

電 話: 04-24616638

傳 真: _____

E-MAIL: justinnal@ms76.hinet.net

中 華 民 國 99 年 7 月 28 日

國立勤益科技大學
研究所碩士班
論文口試委員會審定書

本校 電子工程系 碩士班 邱顯錦 君

所提論文 **A Proactive Integrated Management System to
Save Troubleshooting Time**

合於碩士資格水準，業經本委員會評審認可。

論文口試委員會：

召集人：

連高國

委員：

連高國

陳瑞文

王川木

指導教授：

陳瑞文

所

長：

電子工程系
主任 陳文淵

中華民國九十九年七月三日

節省檢修時間之前瞻性整合管理系統研究

學生：邱顯錦

指導教授：陳瑞茂 博士

國立勤益科技大學

電子工程研究所碩士班

摘要

隨者網際網路快速發達，我們作息與網路息息相關。網際網路已經成為一種通用名詞。現在有許多商業交易透過網際網路來進行。同時許多的大型企業環境運作模式為 24 小時全年無休的環境之下，企業需要一種快速有效管理機制，面對嚴厲挑戰。因此如何讓網際網路提供穩定服務之探討更加熱絡，這系統必須可以對問題快速與精準作出反應。

因此企業需要一個可以有效率與有用的管理系統，已經成為重要的環節。不過，檢修對於大型系統/ 網路環境十分費時。其間需要穩固和準確的管理工具可以降低的檢修時間。SNMP(Simple Network Management Protocol)是一個管理協議，而且廣泛應用在很大程度上地用標準在 IP 網路的設備的遠距離的管理。雖然如此，在

SNMP 的 MIB(Management Information Base)裡的管理訊息可以包含在多種設備如網路設備或應用伺服器使用狀況。

在這項研究過程中，來自被管理的設備的管理訊息被整合到主動式監控管理系統。此主動式管理的機制而非被動式，如此管理訊息及時性更能掌握。在這項研究過程中，有些好處可以獲得。第一能夠容易了解管理設備使用狀態，第二能夠容易了解管理設備是否達到使用瓶頸，第三能夠協助找出故障的管理設備。

在此重申這項研究是透過 SNMP 機制及結合管理設備的Trap 功能。而且此管理系統可以再結合郵件警告系統或語音示警系統，讓系統管理者能夠及時了解管理的設備發生或在發生故障之前已經知道設備潛在問題。

關鍵詞：SNMP, MIB, proactive management system, Cacti, trap

A Proactive Integrated Management System to Save Troubleshooting Time

Student: Hsien-Chin Chiou

Advisors: Dr. Ruey-Maw Chen

Institute of Electronic Engineering
National Chin-Yi University of Technology

Abstract

People's dependence on the internet has increased apparently. It's a trend that the internet is regarded as a general term. There are business models like B2B (Business to Business), B2C (Business to Consumer) and C2C (Consumer to Consumer) running on internet. Hence, today's enterprise environment, where the business operation keeps running and the nonstop service available is required; enterprise needs a quick and accurate mechanism to face the challenges of any unexpected event. Therefore, the issue of how to tighten the "stability" of internet environment has given rise to much attention of researchers.

Restated, effective and efficient management is a vital issue. However, troubleshooting is quite time consuming for large scales system/network environment. At meantime it needs a strong and accurate management tools to reduce troubleshoot time. SNMP (Simple Network Management Protocol) is a management protocol that is widely used standard for remote management of devices in IP networks. Nevertheless, management information in MIB (Management Information Base) of SNMP agent is implemented in a variety of devices such as network equipments, application servers and others.

In this study, management information from the managed devices was integrated to provide a proactive management system. Through proactive rather than reactive management, it could offer the real benefits of management system. Some core features are presented in the proactive management system; they are easy to find out the state of managed devices, to identify the trends of operation easily and take a troubleshooting guide to predict what might go wrong.

Restated, this work incorporates SNMP mechanism as well as trap mechanism in management system. Moreover, the proposed proactive management system is able to combine an alarm system and mail system to provide an alert message to related management staffs in time, prior to the managed device being faulty.

Keyword: SNMP, MIB, proactive management system, Cacti, trap



Contents

授權書.....	I
碩士論文電子檔案上網授權書	II
論文口試委員會審定書	III
A Proactive Integrated Management System to Save Troubleshooting Time	VI
Abstract	VI
Contents	VIII
1 Introduction.....	12
1.1 Study background.....	12
1.1.1 SNMP.....	12
1.1.2 NMS.....	13
1.2 Study objective.....	14
1.2.1 Management system architecture.....	15
1.2.2 Polling versus Trap	17
1.2.3 Fault management operation.....	19
1.3 Study motivation.....	21
2 Architecture review.....	22
2.1 Management system architecture review.....	22
2.2 Requirements for effective management system.....	26
2.2.1 Customization.....	26
2.2.2 Integration.....	26
2.2.3 Scalability	27
2.3 Factor impact management scale.....	27
2.4 Applied to polling method	29
2.5 Access mechanism in SNMP	30
2.6 Integrating with the other application	31
3 Implementation	32
3.1 Prepare MIB files.....	32
3.2 Start SNMP daemon at managed agents	33
3.3 Notification operation	37
4 Function verification.....	42
4.1 About setting on Cacti	43
4.1.1 Configuration set up.....	43
4.1.2 Add on managed device to Cacti	47

4.1.3	Create Weathermap	49
4.2	Test result from Cacti monitor system	53
4.2.1	Function test from Cacti management system	54
4.2.2	Accuracy verification	58
4.3	Limitation on test environment	63
5	Management system comparison	63
6	Conclusions and feature works	66
6.1	Conclusions	66
6.2	Feature works	66
	References	68
	Appendix A	71
	Appendix B	78



Figure captions

Figure 1-1 Relationship between management system and agent	16
Figure 1-2 MIB hierarchy	17
Figure 1-3 Polling VS trap	19
Figure 1-4 Trap information	20
Figure 2-1 Data network management architecture	22
Figure 2-2 Daemon relationship	23
Figure 3-1 Enable SNMP through Web for SAN switch	36
Figure 4-1 Cacti function tabs	43
Figure 4-2 Set up function tabs	44
Figure 4-3 Alerting mail account setting	45
Figure 4-4 Mail account setting for threshold	45
Figure 4-5 Mail / DNS setting	46
Figure 4-6 Mail function verification	46
Figure 4-7 Miscellanies	47
Figure 4-8 Add on managed device through Devices menu	48
Figure 4-9 Managed device status	48
Figure 4-10 Add on one managed device and its related setting	49
Figure 4-11 Creating Weathermap	50
Figure 4-13 Assigns a new map name	51
Figure 4-14 Adds a node	52
Figure 4-15 Adds a link	53
Figure 4-15 Status of managed device	54
Figure 4-16 Displays Current CPU utilization on threshold tab	56
Figure 4-17 Displays one alert message to mail account	56
Figure 4-18 Looks up mail content	57
Figure 4-19 Shows traffic volume from map	58
Figure 4-20 Displays CPU utilization from a managed node on map	58
Figure 4-21 CPU utilization of R-443	60
Figure 4-22 CPU utilization of R-443 from Cacti	60
Figure 4-23 Processor memory usage of R-443	61
Figure 4-24 Process memory usage of R-443 from Cacti	61
Figure 4-25 CPU utilization of network server	62
Figure 4-26 CPU utilization of network server from Cacti	62

Table captions

Table 2-1 CISCO-STACK-MIB traps	24
Table 2-2 MIB Access Category	31
Table 3-1 Monitor item and threshold predefined	38
Table 3-2 List which OID supports trap feature	38
Table 5-1 Depiction of the advantage	64
Table 5-2 Benefit in different management methodology	65



1 Introduction

1.1 Study background

Today, computer is used in many areas. It is an important tool to people, especially for people who work for organizations, industry, and so forth. Almost anything can be executed or implemented by computers. Hence, out of function of computer will impact daily operation very seriously. It is hardly to make sure anything run well, a monitor mechanism must set up. Once abnormal event happened, management system should be able to alert the related message to IT staff or take the proper procedure in time. Let IT staff know what wrong it is after one alerting message sent to his /her mail account. Based on the desired management concept, a management system with proactive monitor mechanism can be built up. The management system is to reduce time of system out of service which is caused by man-made error. Meanwhile, the management system also gives a troubleshooting guide on problem solving, especially any adverse event occurred in a complicated enterprise environment.

Here are my reference resources in this study. There are almost from Web information. Today everything you want to understand or learn, it could be on internet. They are also included “Unix Fault Management” [1] and “Network Node Manager managing your network” [2] two books. Especially, in “Unix Fault Management”, there are many concepts I learned in this study in fault management. The former book does not only focus on Unix operating system, but also gives rich knowledge in fault management. The other book focuses on network management. It is a good manual to build up knowledge about the operation in how to work in management field.

1.1.1 SNMP

Simple network management protocol (SNMP) [3] [4] [5] [6] is actually used to refer to a collection of specifications for network management that includes the protocol itself, the definition of a

database, and concepts. SNMP is introduced in the 1980s. Today it is highlighted here to TCP/IP network environment. The development of TCP/IP boosts up more application of SNMP in nowadays. There are more detailed definitions in RFC [3] [7] [8] [9] [10] [11] [12]. The following addresses three basic specifications:

1. Structure and Identification of Management Information for TCP/IP based Internets (SMI): describes the common structures and identification scheme for the definition of management information used in managing in TCP/IP based internet. There is a full definition on RFC1155.
2. Management Information Base (MIB) [5] [13] for network management of TCP/IP based Internets: describes the managed objects contained in the MIB. There is a full definition on RFC1213.
3. Simple Network Management Protocol (SNMP): describes the protocol used to manage these objects. There is more a clear definition on RFC1157.

There is an enhanced feature in security and administrative capability in SNMP V3. About SNMP specification, there are more clear definitions mapping to the related RFC. In OSI definition, SNMP is designed to be an application layer that is part of the TCP/IP protocol suite. It is intended to operate over the user datagram protocol (UDP) which is a connectionless protocol. Typically, SNMP uses UDP ports 161 for the agent and 162 for the manager.

In typical SNMP use, system operators have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system (device) executes, at all times, a software component called an agent which reports information via SNMP to the management systems. Although SNMP was used only to manage network devices, such like routers, switches and hubs initially. Today SNMP is also applied in management for system, application software [15] [16] and the equipment embedded SNMP agent.

1.1.2 NMS

Network Management System (NMS) [17] [18] [19] [20] [21] [22]

[23] [24] [25] [26] [27] is responsible to collect or query the status of managed device. In the same time it also could accept trap message from managed device encountering fault and take an alerting mechanism to notify the related staff. It would save troubleshooting time. The other way is to define the threshold like CPU utilization or resources usage to specific managed devices. If the threshold is breaching, management system would send out one alerting message to the IT staff. This method provides a bottleneck monitor mechanism.

Initial state of NMS is considered as a management in network devices and seeds in the network topology. Due to IT industrial blossom, let management become more important and at meantime it could extend its power to the other device except network device. Even we could say it could provide a proactive protection in management field. Let us think about why it is proactive. To Reactive service is just offered a passive problem solving. It is not quick and in time.

Today NMS must offer the capability to find out the current state of your network and managed device firstly. It could offer the capability to optimize the network and managed device before reaching its bottleneck secondly. It offers some evident to prevent operation interrupt. Hence it could achieve an efficient and proactive management platform.

1.2 Study objective

In order to understand integrated operation theory, we must understand how to combine it into one management platform. This combination is to point out quickly what managed device is out of function and to reduce troubleshooting time. At meantime it could assist system operator to identify what wrong it is and reduce opportunity in human errors in daily operation. First we need to build up the related acknowledge and concept.

1.2.1 Management system architecture

The model of network management [2] [23] [24] [25] that is based on TCP/IP network management covering the following key components:

- management system
- management agent
- management information base (MIB)
- SNMP protocol

The management system is typically a standalone server or a station installed the related management application like NNM. It could offer data analysis, fault recovery...the related capability. It would do monitor and control the managed devices for system administrator. It also owns database for the MIB of the managed devices. Today there are different management systems on industrial technology. Their function is similar.

An agent is usually a passive entity. The management agent is managed devices with embedded agent to response to request for information and request for action from management systems. An agent becomes an active entity by emitting unsolicited messages to alert SNMP managers of obvious local events (such as a one power failure in managed device). The Figure 1-1 [2] would depict the relationship between management system and management agent.

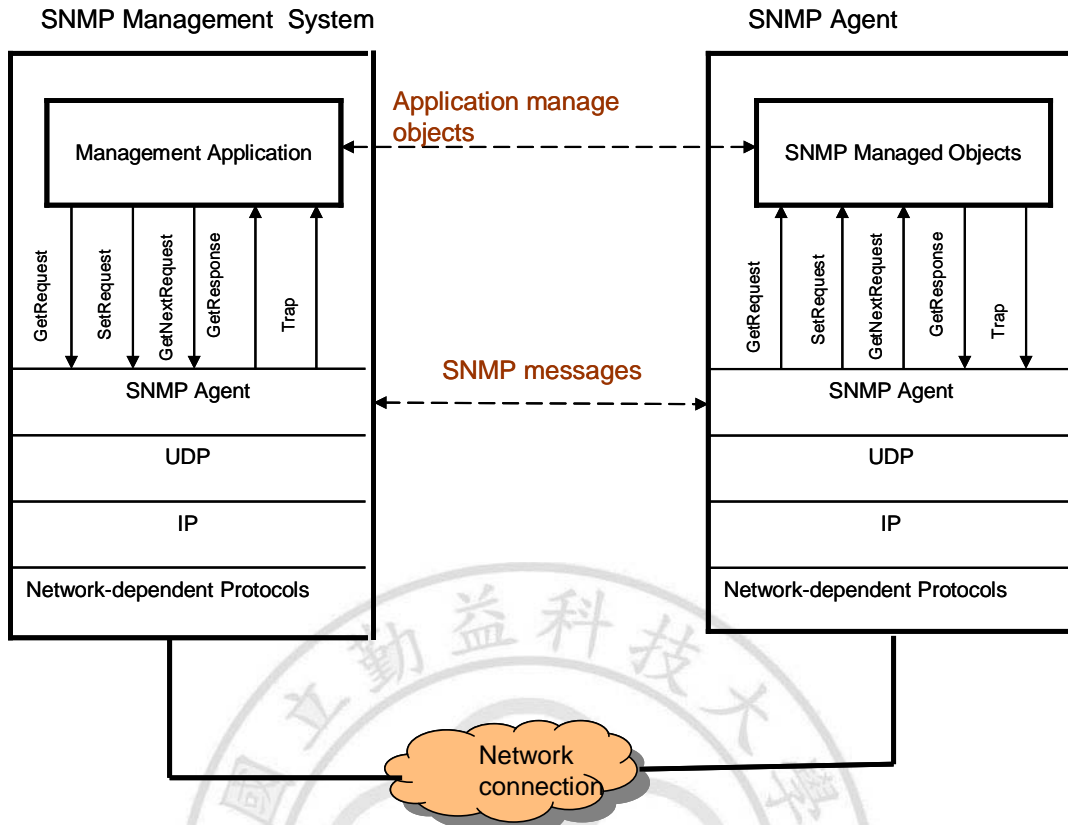


Figure 1-1 Relationship between management system and agent

A set of objects provided from vendors is referred to as a management information base. The MIB file would define specific objects for monitoring the managed device. We could say if the router's working environment would be monitored, the related MIB for working environment of this router must be loaded into management system. Figure 1-2 [1] [28] shows the MIB hierarchy. It could refer to <http://www.ietf.org> [3] to get more detailed information for RFC.

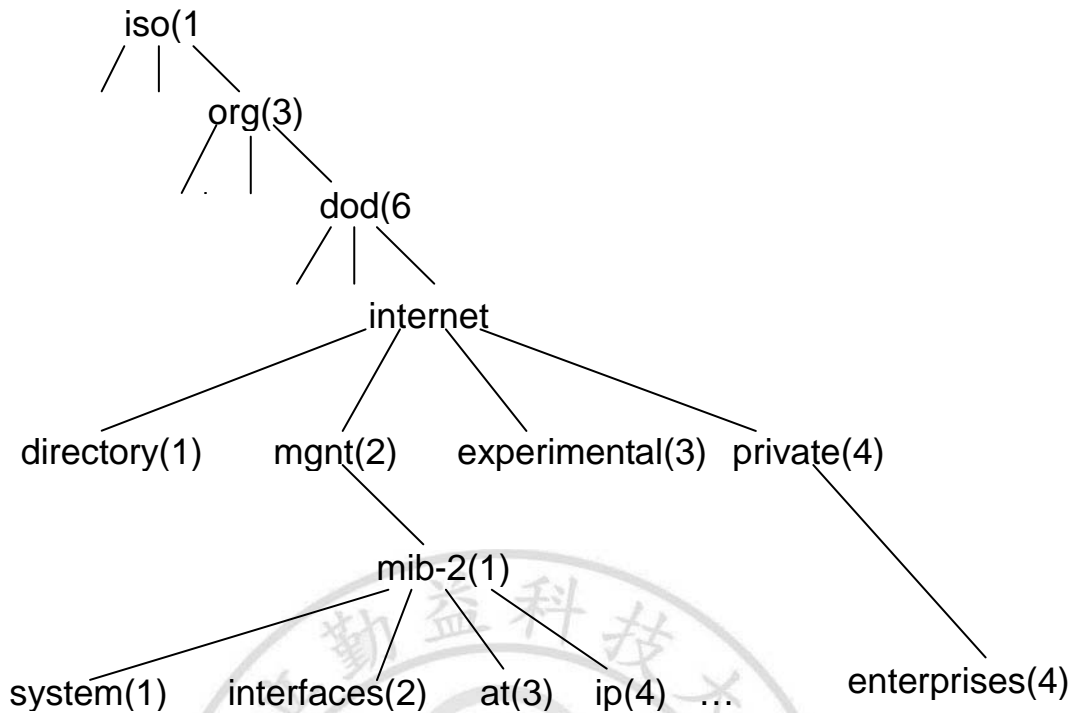


Figure 1-2 MIB hierarchy

The management system and management agent [1] [2] [6] are linked by SNMP protocol. The protocol would offer the following key function:

- Get : enables a management system to retrieve the value of object at a managed device
- Set: enables a management system to set the value of object at a managed device
- Trap: enables a managed device to notify a management system critical event occurred.

The SNMP is an application protocol that is part of the TCP/IP protocol suite. It operates over the user datagram protocol (UDP) which is a connectionless protocol. It means no handshaking mechanism on UDP. There is a tracking method involved in the entire implementation. At the meantime there is some enhancement in security.

1.2.2 Polling versus Trap

Let we think about how many managed devices will be managed

by management system in your management environment and every managed agent maintains a large number of objects. If a management system is responsible for a large number of agents, it would become an impractical implement. Then one management mechanism must be taken through polling and trap [29] [30]. The polling is through management system to periodically query the managed device to receive the status. A trap is through agent notifying the management system of unsolicited event occurred. All communication between the management system and its managed agents take place using SNMP.

At initial stage, we could define a rule which devices are managed, which items are monitored, how long it will be polled and what devices could issue trap event to management system while the device get faults. These are a basic demand to management system. It could let management system to build the baseline for your IT. Then later it could be set up alarm mechanism during breaching threshold we defined based on baseline or trap event occurring. The Figure 1-3 depicts the operation of polling and trap. It could be understood easily from the Figure 1-3 [31]. The polling operation is initiated by management system through SNMP get function to get managed device status or state. The trap operation is trigger while managed device get fault and at meantime it own the trap function. These message are operated on UDP, we could decide polling interval and how many failed polls are allowed in your management environment. These are a not standard, it just offers the guideline to lead a right track.

In general one trap is an unexpected event occurred on managed device sent to a management system. A trap is generated by SNMP agent and is sent to specific destination. There are many hardware faults signaling a trap message like fan failure, NIC card failure... etc.. The trap message contains its related information. Hence the trap message directs to management system and a management system could process trap message. It would trigger the appropriated action to notify IT staff. It lets the potential problem be solved in time.

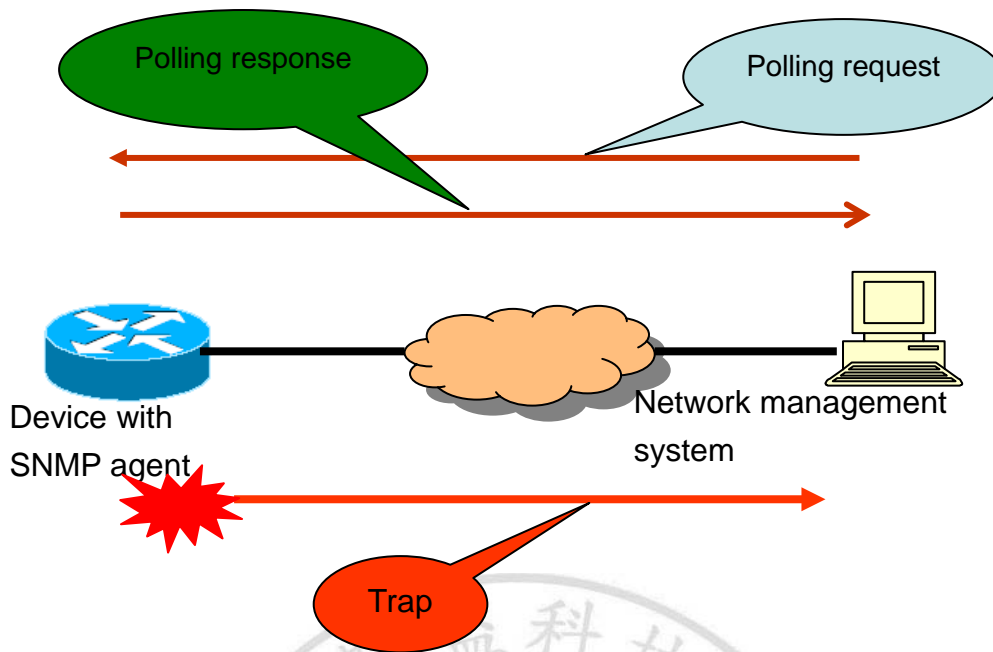


Figure 1-3 Polling VS trap

1.2.3 Fault management operation

Fault management [1] [2] operation proposed in this work is implemented by integrating both polled messages and event traps from devices. It is based on polling and trap operation. A management system would poll managed device within interval time. The polling is carried out through ICMP ping or SNMP get mechanism to acquire device's status. The ICMP ping is performed at a consistent rate that is independent of polling response time. The management system achieves this poll function using two asynchronous threads: one sends polls and the other receives poll responses. The sending and receiving threads are designed to operate asynchronously. Therefore, slow response times or excessive timeouts does not affect the polling rate. If the managed device inhibits ICMP ping function, instead the management system uses SNMP polling to get managed device's status. Meanwhile, the SNMP polling automatically switches to an alternate IP address during failures, ensuring the integrity of management system analysis. In general, the primary purpose of polling mechanism is to understand managed device's status.

We could define the threshold and enable trap function on managed devices in advance after loading MIB files into management system. Due to one event arising, trap mechanism would be triggered, the managed device will direct trap information to management system. There is one link down occurring on managed device here. The Figure 1-4 [24] [25] [31] depicts the related information contained in trap PDU would be directed to management system. The managed device already enabled link down trap feature would send the notification message agent generated to management system. At meantime management would decode the notification message and category the message and take the appropriate action predefined in the action task.

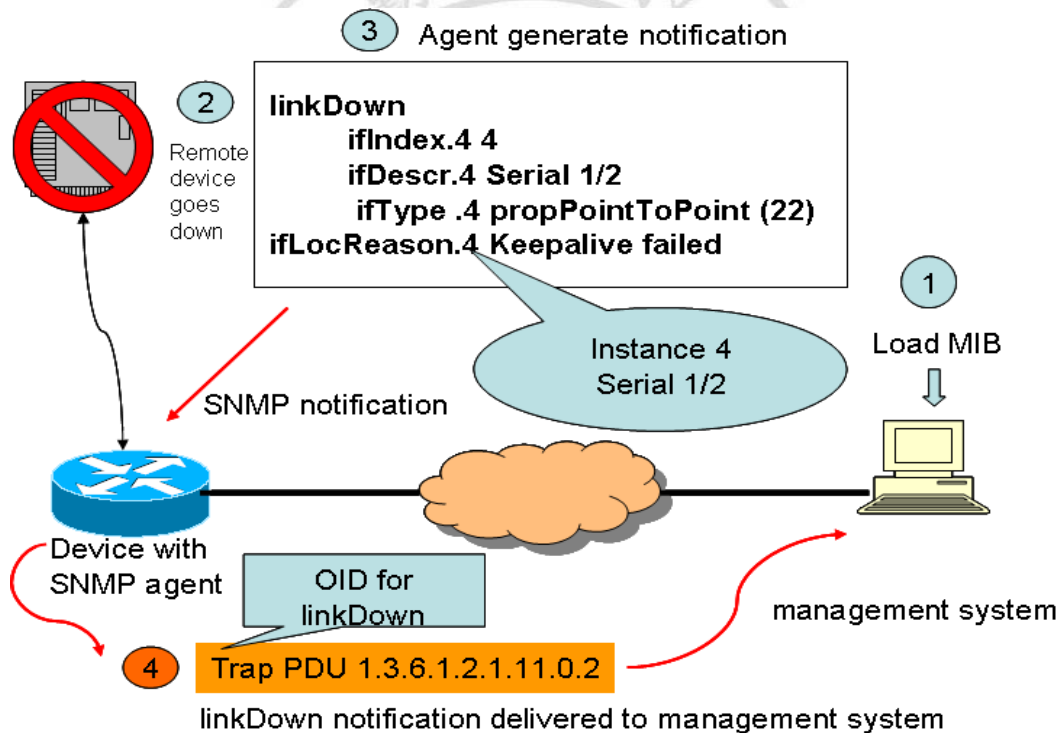


Figure 1-4 Trap information

Each trap is identified by its OID as well as generic and specific trap number. A trap message includes the address of the agent sending the event and a list of variables. The variables contained in the trap message can be used in the event message and then filter the message to take predefined action. Restated, the fault management system (event daemon) assigns the event to an event category and takes a predefined

action based on the severity configuration in the template.

1.3 Study motivation

First we talk about system administrator is responsible to maintain the system integrity and stability in data center. In early system administrator must take care of troubleshooting and problem solving to his/her management devices. But today application systems become more complicated and more tasks deployed on different machines. While one of equipment or application system stuck, it is not easy to identify which parts encounters problem within short time. It's beyond system administrator's capability to identify or recover the fault parts in short time. Hence system administrator should get the effective and powerful tools to assist him/her to short troubleshooting time. It would cover the checking the current health of the system in daily operation and troubleshoot recent events and faults that may be related connection. It would point out that operator error is the most common cause of unplanned downtime. It is to reduce the opportunity of operator error. An automatic monitor mechanism is a must after it is considered well and proved deployment. It is a necessary routine in management.

In study area, we could not manage all devices in test environment we planed. But we could think about which devices could be adopted into a management domain. Restate, the equipments, application systems or its peripherals which support SNMP daemon are adopted into managed devices.

Here is to take the opportunity to prove SNMP incorporated to a management system. Firstly it lets a proactive management system assist IT staff to reduce the pressure in daily monitor management. If the management through man power is easy to miss the checking item and it is poor in management efficiency. Secondly it is real and accurate in monitor event incoming. Due to almost equipments with redundancy mechanism, one of redundant equipment is faulty. All services keep running. It is seamless to service. Hence IT staff must exam carefully in his/ her daily check list, maybe it could be found at that day. The same check is executed on a proactive management system. The alerting

message would be sent out the related staff in time. No lag issue exists in a proactive management system.

2 Architecture review

In general we talk about network management. It would follow up ISO network management architecture. Of course its management models are flexible, not full sets of all models. It depends on your needs to add the model you need.

2.1 Management system architecture review

Fault management [23] [24] [25] is one of the ISO management models. The ability of the fault management is to detect, isolate, notify, correct faults encountered in managed devices. Figure 2-1 shows a reference architecture that should be the minimal solution for managing a data network.

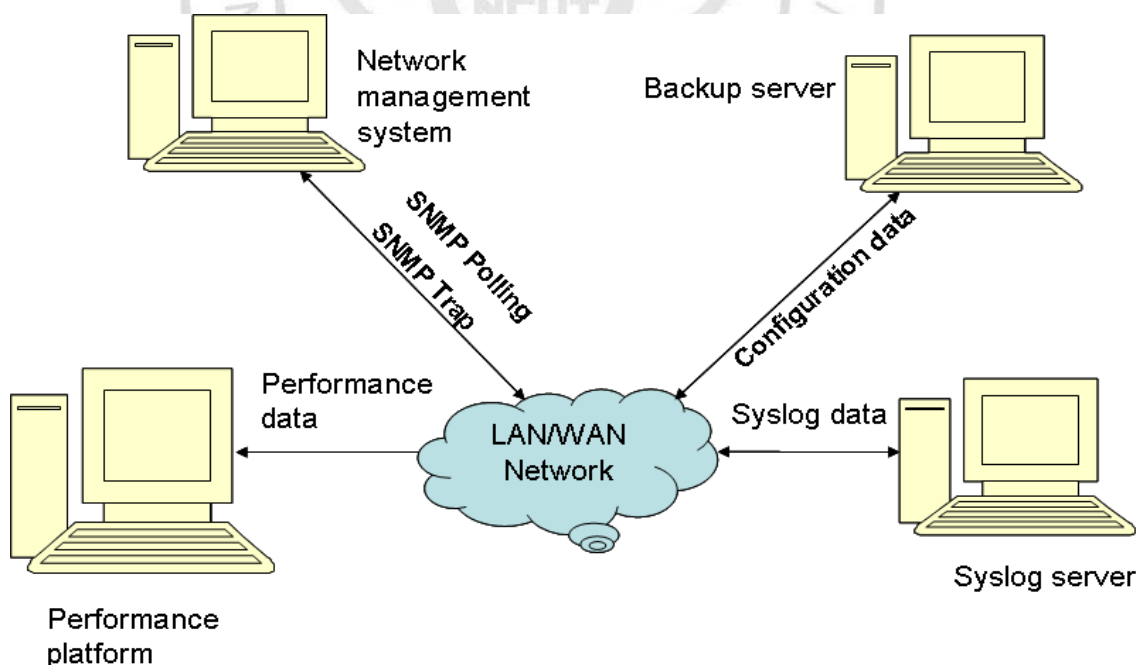


Figure 2-1 Data network management architecture

Fault management is perhaps the most widely implemented component of the ISO network management elements, since network

device faults may cause downtime of the network or unacceptable network degradation. One NMS can be deployed in enterprise network or campus network. Then, the NMS could receive and process events from network elements in the managed network. Meanwhile, events from servers and the other critical resources are forwarded to the NMS platform for processing. Usually, the NMS platform includes the following processing functions and Figure 2-2 [2] [25] depicts these daemons' relationship.

- Network discovery processing
- Topology mapping processing
- Event handler processing
- Performance data collecting and a graphical processing
- Management data browser

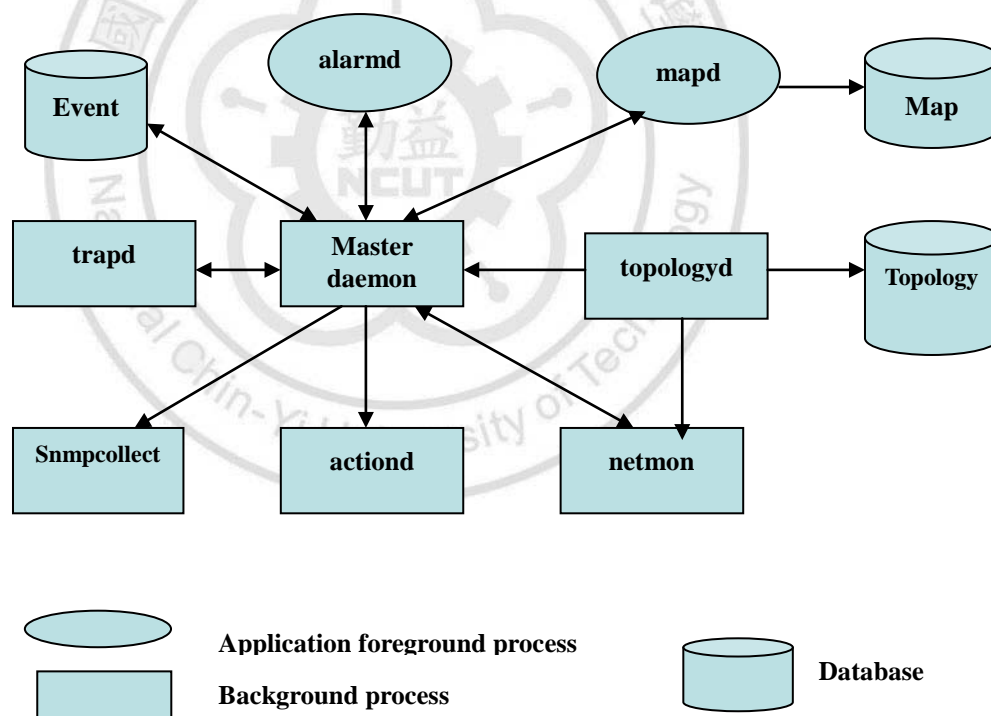


Figure 2-2 Daemon relationship

The management platforms monitor the status of managed devices through browser interface. The key issue of the network management is the ability to detect problems quickly.

Therefore, how fast to poll a managed device is needed to be determined. Moreover, to ensure various alerts from managed devices are interpreted correctly by the NMS platform based on the MIB file is important. These MIB files can be downloaded from managed devices provider web site.

The target of fault management is to detect, isolate, notify, and correct faults encountered in the network. Managed devices are capable of issuing alerting messages when a fault occurs on the systems. An effective fault management system consists of several subsystems. Fault detection is accomplished through below when the devices send SNMP trap messages, SNMP polled messages, remote monitoring (RMON) thresholds, and *syslog* messages. A management system would alert network administrator when a fault occurs and hence corresponding troubleshooting actions can be taken.

Traps are used to indicate devices status. Hence, traps must be enabled consistently on managed devices. It is important to check and update the configuration file to ensure the proper decoding of traps. Table 2-1 [13] [31] lists used CISCO-STACK-MIB traps that are supported as displayed in description example.

Table 2-1 CISCO-STACK-MIB traps

traps	description
moduleUp	The agent entity has detected that the moduleStatus object in this MIB has transitioned to the ok (2) state for one of its modules.
moduleDown	The agent entity has detected that the moduleStatus object in this MIB has transitioned out of the ok (2) state for one of its modules
chassisAlarmOn	The agent entity has detected that the chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has transitioned to the on (2) state. A chassisMajorAlarm indicates

	<p>that one of the following conditions exists:</p> <ul style="list-style-type: none"> ■ Any voltage failure ■ Simultaneous temperature and fan failure ■ One hundred percent power supply failure (two out of two or one out of one) ■ Electrically erasable programmable read-only memo (EEPROM) failure ■ Nonvolatile RAM (NVRAM) failure ■ MCP communication failure ■ NMP status unknown <p>A chassisMinorAlarm indicates that one of the following conditions exists:</p> <ul style="list-style-type: none"> ■ Temperature alarm ■ Fan failure ■ Partial power supply failure ■ Two power supplies of incompatible type
chassisAlarmOff	<p>The agent entity has detected that the chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has transitioned to the off (1) state.</p>

According to Table 2-1, administrator staffs determine which corresponding trap MIB must be loaded into management system for managed devices. Restated, to look up the related information on provider website is required. For example, if network administrator wants to monitor HP-UNIX servers on a management system, who must have a private HP-UNIX MIB provided by HP. The HP-UNIX MIB contains important information about the users, jobs, file system, memory, and processes of a system. Then, network administrator could set a threshold for a trap of how busy the managed system is on a management system. Furthermore, the management system can alert message to the management staffs when the trap value beaches the setting threshold for managed devices.

2.2 Requirements for effective management system

The ultimate goal of the proposed integrated management system is to provide the accurately discovering and fault correction. Its benefit is to reduce the effort in troubleshooting and management. According to experiences, an effective management system requires a synergy and flexibility among customization, integration and scalability [1] [2] [25] [26].

2.2.1 Customization

Communication networks of a corporation can be viewed as operating strategic tools used to gain advantage over competitors. The network services must be able to adapt to new requirements and accommodate new applications. Similarly, public service providers must strive to offer a high quality service to their customer and it is basic to meet their service level agreement with their clients.

Although it could offer an excellent infrastructure, one service in their infrastructural platforms is out of service, avoiding human error in monitor mechanism and save time in troubleshooting time, it is a necessary management mechanism. Therefore, management system is allowed to be tailored on what kind of service is needed to be monitored in gaining more efficient response. Hence, it is the best management tools to be easy to adapt to custom-made depending on the real environment.

2.2.2 Integration

A management system is used on managing network devices in common situation. However, system servers starting up SNMP daemon and equipments embedded SNMP agent are able to be integrated into one management system. Meanwhile, appropriate MIB files from device provider are loaded into a management system. Accordingly, staff member can monitor all equipments through a common and unified application platform. Meanwhile, a collective procedure in fault

management for a variety of systems and equipments can be used. Therefore, the predefined action related to any fault occurred could be applied to reduce operator error. Moreover, the proposed management system is able to combine alert system with email system or voice system to be a more proactive way in notifying staff member and hence reducing troubleshooting time. Restated, an integrated management system can greatly promotes management efficiency.

Furthermore, the ability of consolidating data from diverse equipments allows to develop a specific application such as performance analysis, data flow volume monitoring. Valuable information through designed application interface can be provided.

Meantime it could propagate the related message into mail system or voice system in time according to information severity received by management system. These messages are filtered to meet the back end equipment, let alarm system be triggered in time.

2.2.3 Scalability

The use of Local Area Networks (LANs) to meet corporate communication needs is growing up at a rapid pace. A large number of these LANs are glued together into Wide Area Networks (WANs) using high speed backbone networks, bridging and routing technology. WAN may span geographical areas in scope and use facilities and services provided in many different countries. The requirements on management system increase as networks grow. Therefore, a management system must be able to support a different architecture to work on different scenario environments. Restated, a management system can be applied to either centralized management or distributed management.

2.3 Factor impact management scale

We already know the traps that are defined by SNMP are initiated by managed devices. Its sending frequency is seldom and few. The chance is only device with setting trap function out of service. But management system is actively gathers managed devices through

polling method. Furthermore, if polling is only done to managed device, the management system could not be alerted the status change on managed devices in time.

Hence polling mechanism would be deployed. The polling policy is needed for the frequency with which polling is done by the management system. The issue is related to the scope of the network and there the number of agents that could be effectively managed by the management system. There is no standard, just a guideline here, because performance will depend on the processor speed of the management system, right traffic volume on network interface, the congestion level in your managed network and others. However, we can do is to gather from the simple formula that gives some idea of the scale of what is possible.

To simplify the issue, let us suppose management system could handle one agent at a time. That is, when the management system polls an agent, it must wait for the response of agent. Then it continues next polling to the other agent. Based on the simplified scenario, we can determine the maximum number of agents that management system engaged in full-time can handle the polling. The following equation would be stated in the desired polling time, SNMP servers could handle the number of agents:

錯誤! 尚未定義書籤。

$$N \leq \frac{T}{\Delta}$$

Where

N = number of agents

T = desired polling interval

Δ = average time required to perform a single poll

One popular example to explain the polling issue is as follows. The example is provided in Ben-Artzi, Candna, and Warriar (1990) [32]. The example consists of a single local area network, where each managed device is polled every 15 minutes (typically used today). Assuming processing times on the order of 50 ms and a network delay of about 1 ms (packet size of 1,000 bytes, no significant network congestion), then Δ is approximately 0.202 sec. Then we could get the approximate number of agents.

錯誤! 尚未定義書籤。錯誤! 尚未定義書籤。

$$N \leq \frac{(15 \times 60)}{0.202} \approx 4,500$$

Therefore under the assumption, one SNMP server could handle a maximum of 4,500 devices in local network environment. If a WAN environment will be covered in management domain, its network latency is worse than local network. The device quantity will be reduced. However, a distributed architecture can be deployed to overcome the issue.

There are some limitations on SNMP except polling issue. The following address these limitations of SNMP;

- It runs UDP protocol, there is no acknowledged mechanism.
- It is a not good way to retrieve large volumes of data information. But it is a suited way to query the status of managed devices.
- SNMP MIB is not already resident on management system. It would impact the accurate message decoded.

Based on the understanding, what scale it would be managed and what field it could be used the implementation is easy to plan. Next section would address polling issue more detailed.

2.4 Applied to polling method

Last section it already addresses that polling interval would affect management scale. In general management system would take SNMP polling [6] [29] [31] to managed devices on its management domain. It uses an SNMP poller that is synchronous and multithreaded. The SNMP poller uses 10 synchronous polling threads default. The SNMP poller supports the following SNMP versions:

- SNMP V1
- SNMP V2C
- SNMP V3 (security only, no data encryption)

On management system it would define which MIB of

managed agent would be polled periodical interval, hence only those MIB variables needed for analysis are polled. Due to SNMP polling is a synchronous mechanism. If one device is no response to the polling, it would let polling throughput down. To overcome the drawback, it could adopt ICMP. The ICMP poller is asynchronous and does not slow down, even in the event of a managed device.

2.5 Access mechanism in SNMP

In SNMP, it takes set, get, trap three commands to exchange or change information with management system. But what way is used on access control each other. SNMP is defined in RFC 1157 that provides only a limited capability for access security. It adopts the concept of community.

A SNMP community is a relationship between a SNMP manager and a SNMP agent that defines access-control, authentication. They must be defined at SNMP agent. Hence the community name is unique in management domain. The same name may be used by different agents. The management system communicates with managed agent with the same community name defined at the agent. The community name could be used to trigger the authentication procedure. But more secure authentication mechanism will be covered in SNMP v3.

By defining more one community name at local agent, then agent can provide different categories of MIB access privilege to management system. The access control has two categories. Table 2-2 shows the relationship between MIB access category and SNMP access mode [6] [25] [31].

Table 2-2 MIB Access Category

MIB Access Category	SNMP Access mode	
	Read-only	Read-Write
Read-only	get and trap	get and trap
Read-Write	get and trap	get, set and trap
Write-only	get and trap, the value is implementation-specific	get, set and trap, the value is implementation-specific for get and trap only
Not accessible	unavailable	Unavailable

Hence a community profile is related with each community defined by an agent, it takes the combination of SNMP community and an SNMP community profile to achieve access control mechanism. Restate it again, the community names defined at agent and assign the different access privilege through different name. At meantime management system must be aware of these community names.

2.6 Integrating with the other application

In real environment, we must think more to create a full set of monitor mechanism in management domain. It is a complex task. A management system is built up in management domain, how to outcome the event or message into action item. Hence predefined SOP will be helpful to do recovering action during event coming. The following application will be linked to a management system [2] [25] [26].

- Log server:

As we know SNMP protocol operates on UDP which is a connectionless. It is just to make sure all events will be handled later. The log server will provide a platform to trace what kind of error encountered.

- Mail alerting function:

The message from the managed device is needed to tailor and direct the filtered message into mail receiver

predefined in configuration file.

- Voice alarm system:

The fault severity is high, it needs a quickly response. It could through alarm system to call pager or phone system to deliver a key message. It could let system operator notify what managed device is out of service.

Based on the infrastructure, it is better to build up redundancy system in management system in management domain.

3 Implementation

3.1 Prepare MIB files

Before launching the installation, it should understand what devices will be monitored through management system and their MIB files are downloaded or not. And we must consider which MIB files are important to your monitor mechanism. At meantime you must understand these managed devices supporting trap operation or not. If it could, you could enable the trap function in the same.

How to get the related MIB files from vendor's corporate URL is a key issue. For example, one system operator wants to monitor the performance of the Cisco router. He/She must download the following MIB files into management system; The following MIB files let system operator to understand the network traffic trends and plan the capacity of the network.

- `cpmCPUTotal5secRev (.1.3.6.1.4.1.9.9.109.1.1.1.1.6)`: The overall CPU busy percentage in the last five seconds period.
- `cpmCPUTotal1minRev (.1.3.6.1.4.1.9.9.109.1.1.1.1.7)`: The overall CPU busy percentage in the last one minute period.
- `cpmCPUTotal5minRev (.1.3.6.1.4.1.9.9.109.1.1.1.1.8)`: The overall CPU busy percentage in the last five minutes period.

3.2 Start SNMP daemon at managed agents

We already decide which devices are monitored by management system. Hence the SNMP agent of managed devices will be checked. It is needed to startup its agent. Almost devices are not started up SNMP agent service in default. You must enable or modify its SNMP configuration file, then restart it. Examples are referred as below.

A. Setting in Cisco router or Cisco switch

Here we would take one Cisco 6509 example [21] [31]. The following are issued the related commands under configuration mode. It is sure that there is a little difference between different IOS versions and different product models.

```
snmp-server community test123 RO
snmp-server host 10.10.10.1 test123
snmp-server ifindex persist
snmp-server trap-source Vlan12
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps chassis
snmp-server enable traps module
snmp-server enable traps casa
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vldelete
snmp-server enable traps slb real virtual csrp
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps c6kxbar swbus
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps bridge
snmp-server enable traps stpx
snmp-server enable traps flash insertion removal
snmp-server enable traps bgp
```

```
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
```

B. Setting in Window based OS

How to Configure SNMP Agent Information is from Microsoft Web site. To configure SNMP agent information [33] [34]:

1. Click Start, point to Control Panel, point to Administrative Tools, and then click Computer Management.
2. In the console tree, expand Services and Applications, and then click Services.
3. In the right pane, double-click SNMP Service.
4. Click the Agent tab.
5. Type the name of the user or administrator of the computer in the Contact box, and then type the physical location of the computer or contact in the Location box.

These comments are treated as text and are optional.

6. Under Service, click to select the check boxes next to the services that are provided by your computer. Service options are:
 - Physical: Specifies whether the computer manages physical devices, such as a hard disk partition.
 - Applications: Specifies whether the computer uses any programs that send data by using TCP/IP.
 - Datalink and subnetwork: Specifies whether this computer manages a TCP/IP subnetwork or datalink, such as a bridge.
 - Internet: Specifies whether this computer acts as an IP gateway (router).
 - End-to-end: Specifies whether this computer acts as an IP host.
7. Click OK.

C. Setting in HP-UNIX

How to Configure SNMP Agent Information is from HP Web site. To configure SNMP agent information for HP UNIX environment [1]:

1. To edit the `snmpd.conf` file under `/etc/SnmpAgent.d`

directory. The following configurable values are in the `snmpd.conf` file;

■ `get-community-name`

It is to specify community name for the agent. The agent responds to SNMP GetRequests with this community name. It is allowed to configure the agent to respond to more than one get community name. If a community name is not entered, the agent does not respond to SNMP GetRequests.

■ `set-community-name`

It is to specify community name for the agent. The agent responds to the SNMP SetRequests and SNMP GetRequests with this community name. It is allowed to configure the agent to respond to more than one set community name. If a set community name is not entered, the agent will not respond to SetRequests.

■ `trap-dest`

It is to specify a system where traps are sent. This system is usually the IP address of the management system.

■ `location`

It is to specify the physical location of the managed agent.

■ `contact`

It is to specify the person responsible for this managed agent and information on how to contact this person.

2. Start SNMP daemon again

D. Setting in Brocade SAN switch

First logged into administrator account, SNMP setup would be completed through the `snmpconfig` command or web tools. The following parameters would be provided and discussed [35];

1. SNMP V1 configuration parameters

The parameter will be covered community name and the IP

- address of the trap recipient.
2. Trap recipient severity level
The trap is linking with the event's severity level. There are six severity level supported here.
 3. SNMP V3 configuration parameters
Two user roles supported respectively to snmpadmin and snmpuser. The snmpadmin user provides read-write access and the snmpuser user provides read-only access.
 4. AccessControl configuration parameters
The function is like ACL of router. It is provide an access mechanism to restrict SNMP set/get/trap operations.
The Figure 3-1 is through web tools to enable SNMP. You could finish the setting easily, then moving to the modified column and change the related field in SNMP tab.

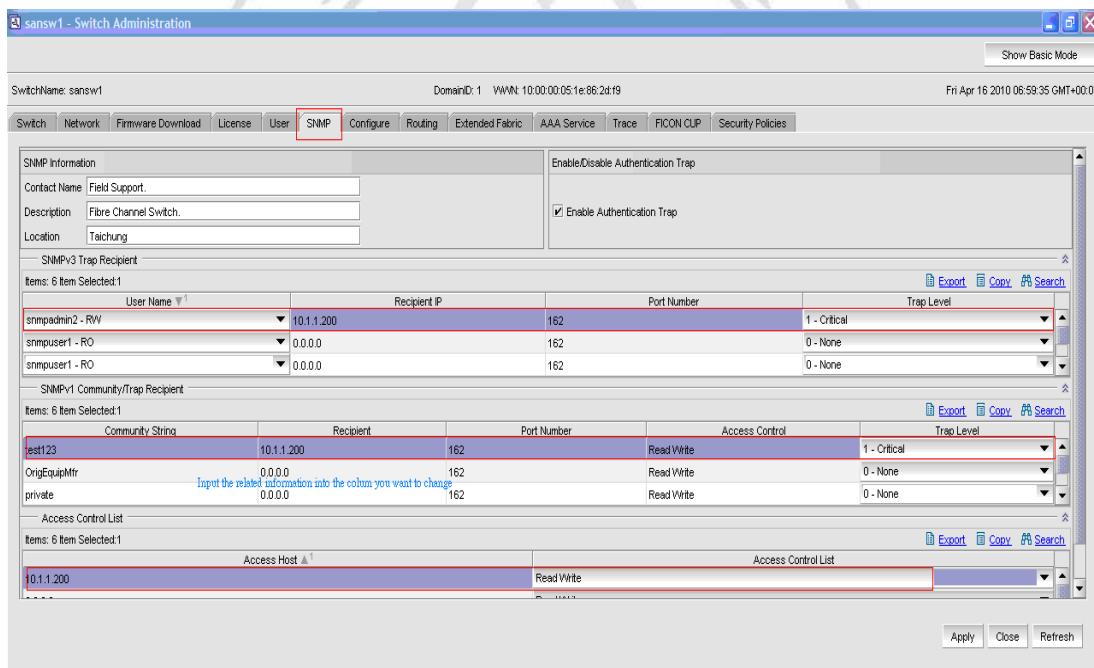


Figure 3-1 Enable SNMP through Web for SAN switch

E. Setting in APC UPS

There is an example of AP 961X card network management card installed APC UPS [36].

- 1: Assign IP address to this management card first
- 2: From browser the IP address with administrator account

- 3: To choose network>SNMPv1>options under administration
- access
To enable SNMP v1 access as a method of communication with the device.
 - access control
To provide the following answer for this access control
 - ◆ NMS IP address
 - ◆ community name
 - ◆ access type: read, read/write
- 4: Or to choose network>SNMPv3>options under administration
- access
To enable SNMP v1 access as a method of communication with the device.
 - user profile
To define user profiles to comply with security needs.
 - access control
To provide the following answer for this access control
 - ◆ NMS IP address
 - ◆ community name
 - ◆ access type: read, read/write
- 5: To choose SNMP trap through Notification>Event Action>options under administration
- To add trap receiver
 - To run under SNMP v3, please choose user profile for this setting.

3.3 Notification operation

As the managed device encounters problem or abnormal status, what information will be sent to the related staff in time through predefined threshold on management system or enable on managed agent? Let the message become a meaningful input to management staff is necessary. Hence, the message flowed out agent will be filtered and then notification message is neat and clear to explain what problem encountered on managed device. Table 3-1 [2] [25] [27] [36] will

depict which item on managed device will be monitored and trigger alarm mechanism reaching the threshold value on predefined on management system. Then Table 3-2 [13] [31] depicts what OID on managed device supports trap function and action taken by alert.pl file. There are so many managed devices supporting trap function. Here is only to take some examples. Trap function of managed devices do not enable on default, they must be referred to administration guide of managed device to get more detailed information.

Table 3-1 Monitor item and threshold predefined

Item name	Interval	threshold	Rearm	Used on
CiscoCpmCPUTotal5min %	1200	≥ 20	≤ 15	Monitor CPU utilization on network
Disk usage rate%	1800	> 70	≤ 60	Monitor disk usage
Free Memory usage rate%	900	≤ 30	≥ 40	Monitor memory free status
cpqHoCpuUtilThirtymMin%	900	> 60	≤ 50	Monitor CPU utilization on server

Table 3-2 List which OID supports trap feature

Event Name	OID	Alarm catalog	Action
Cisco_Link_Down	.1.3.6.1.6.3.1.1.5.3. 1.3.6.1.4.1.9	Interface Link Trap Alarms	alert.pl \$N \$r \$1
Cisco_Link_Up	.1.3.6.1.6.3.1.1.5.4. 1.3.6.1.4.1.9	Interface Link Trap Alarms	alert.pl \$N \$r \$1
chassisAlarmOn	.1.3.6.1.4.1.9.5.0.5	Status Alarms	alert.pl \$N \$r "The trap signifies that the agent entity has detected the chassisAlarmOn."

Event Name	OID	Alarm catalog	Action
chassisAlarmOff	.1.3.6.1.4.1.9.5.0.6	Status Alarms	alert.pl \$N \$r "The chassisAlarm status is back to normal."
ciscoEnvMonTemperatureNotification	.1.3.6.1.4.1.9.9.13.3.0.3	Status Alarms	alert.pl \$N \$r "Temperature is \$2 Celsius Degrees and Status is \$3"
ciscoEnvMonFanNotification	.1.3.6.1.4.1.9.9.13.3.0.4	Status Alarms	alert.pl \$N \$r "FAN Status is \$2"
ciscoEnvMonRedundantSupplyNotification	.1.3.6.1.4.1.9.9.13.3.0.5	Status Alarms	alert.pl \$N \$r "The redundant power supply fails."
stpInconsistencyUpdate	.1.3.6.1.4.1.9.9.82.2.0.1	Status Alarms	alert.pl \$N \$r "A Update notification is sent by spanning tree. (\$1)"
stpRootInconsistencyUpdate	.1.3.6.1.4.1.9.9.82.2.0.2	Status Alarms	alert.pl \$N \$r "Spanning tree detect a loop topology.(\$1,\$2)"
stpLoopInconsistencyUpdate	.1.3.6.1.4.1.9.9.82.2.0.3	Status Alarms	alert.pl \$N \$r "An loop-inconsistency of spanning tree disappears. (\$1, \$2)"
c2900BroadcastStorm	.1.3.6.1.4.1.9.9.87.2.0.2	Status Alarms	alert.pl \$N \$r "The broadcastStorm notification is generated.(\$1)"
cHsrpStateChange	.1.3.6.1.4.1.9.9.106.2.0.1	Status Alarms	alert.pl \$N \$r "HSRP Status Change, \$1"
cefcModuleStatusChange	.1.3.6.1.4.1.9.9.117.2.0.1	Cisco Default Trap	alert.pl \$N \$r "cefcModuleStatusChange: \$1,\$2"
cefcPowerStatusChange	.1.3.6.1.4.1.9.9.117.2.0.2	Status Alarms	alert.pl \$N \$r "Operational FRU Power Status is \$1 and Administratively desired FRU Power Status is \$2"
communicationLost	.1.3.6.1.4.1.318.0.1	APC UPS Alarms	alert.pl \$N \$r "Communication lost between the agent and the UPS."

Event Name	OID	Alarm catalog	Action
upsOverload	.1.3.6.1.4.1.318.0.2	APC UPS Alarms	alert.pl \$N \$r "The UPS has sensed a load greater than 100 percent of its rated capacity."
upsDiagnosticsFailed	.1.3.6.1.4.1.318.0.3	APC UPS Alarms	alert.pl \$N \$r "The UPS has failed its internal selftest."
upsDischarged	.1.3.6.1.4.1.318.0.4	APC UPS Alarms	alert.pl \$N \$r "The UPS batteries are discharged."
upsOnBattery	.1.3.6.1.4.1.318.0.5	APC UPS Alarms	alert.pl \$N \$r "\$1"
smartBoostOn	.1.3.6.1.4.1.318.0.6	APC UPS Alarms	alert.pl \$N \$r "\$1"
lowBattery	.1.3.6.1.4.1.318.0.7	APC UPS Alarms	alert.pl \$N \$r "\$1"
powerRestored	.1.3.6.1.4.1.318.0.9	APC UPS Alarms	alert.pl \$N \$r "Returned from battery backup power; utility power restored."
upsBatteryNeedsReplacement	.1.3.6.1.4.1.318.0.17	APC UPS Alarms	alert.pl \$N \$r "\$1"
hardwareFailureBypass	.1.3.6.1.4.1.318.0.20	APC UPS Alarms	alert.pl \$N \$r "The UPS is on bypass due to an internal fault."
softwareBypass	.1.3.6.1.4.1.318.0.21	APC UPS Alarms	alert.pl \$N \$r "UPS put on bypass by user via software or front UPS panel."
switchedBypass	.1.3.6.1.4.1.318.0.22	APC UPS Alarms	alert.pl \$N \$r "UPS put on bypass by user."
returnFromBypass	.1.3.6.1.4.1.318.0.23	APC UPS Alarms	alert.pl \$N \$r "The UPS has returned from bypass mode."
bypassPowerSupplyFailure	.1.3.6.1.4.1.318.0.24	APC UPS Alarms	alert.pl \$N \$r "The base module bypass power supply needs repair."
smartAvrReducing	.1.3.6.1.4.1.318.0.31	APC UPS Alarms	alert.pl \$N \$r "\$1"

Event Name	OID	Alarm catalog	Action
smartBoostOff	.1.3.6.1.4.1.318.0.34	APC UPS Alarms	alert.pl \$N \$r "\$1"
smartAvrReducingOff	.1.3.6.1.4.1.318.0.35	APC UPS Alarms	alert.pl \$N \$r "\$1"
temperatureThresholdViolation1	.1.3.6.1.4.1.318.0.59	APC UPS Alarms	alert.pl \$N \$r "\$1"
temperatureThresholdViolationCleared1	.1.3.6.1.4.1.318.0.60	APC UPS Alarms	alert.pl \$N \$r "\$1"
temperatureThresholdViolation2	.1.3.6.1.4.1.318.0.63	APC UPS Alarms	alert.pl \$N \$r "\$1"
temperatureThresholdViolationCleared2	.1.3.6.1.4.1.318.0.64	APC UPS Alarms	alert.pl \$N \$r "\$1"
batsSourceSwitched	.1.3.6.1.4.1.318.0.126	APC UPS Alarms	alert.pl \$N \$r "The Automatic Transfer Switch has switched source."
batsPowerSupplyFailure	.1.3.6.1.4.1.318.0.134	APC UPS Alarms	alert.pl \$N \$r "The Automatic Transfer Switch Power Supply has failed."
rxPDUCoolingFanAlarm	.1.3.6.1.4.1.318.0.336	APC UPS Alarms	alert.pl \$N \$r "Cooling fan failure."
rxPDUTransformerTempAlarm	.1.3.6.1.4.1.318.0.338	APC UPS Alarms	alert.pl \$N \$r "Transformer temp alarm."
upsInternalOverTemperature	.1.3.6.1.4.1.318.0.353	APC UPS Alarms	alert.pl \$N \$r "\$1"
upsInternalOverTemperatureCleared	.1.3.6.1.4.1.318.0.354	APC UPS Alarms	alert.pl \$N \$r "\$1"
upsInverterOverTemperature	.1.3.6.1.4.1.318.0.504	APC UPS Alarms	alert.pl \$N \$r "\$1"
upsInverterOverTemperatureCleared	.1.3.6.1.4.1.318.0.505	APC UPS Alarms	alert.pl \$N \$r "\$1"
upsBypassRelayFault	.1.3.6.1.4.1.318.0.622	APC UPS Alarms	alert.pl \$N \$r "A bypass relay (or its driver) has a fault."
SNMP_Link_Down_SSLVPN	.1.3.6.1.6.3.1.1.5.3	SSLVPN	alert.pl \$N \$r \$1

Event Name	OID	Alarm catalog	Action
SNMP_Link_Up_SSLVPN	.1.3.6.1.6.3.1.1.5.4	SSLVPN	alert.pl \$N \$r \$1

About action item with options parameter, it will depend on a managed device what message will be sent out. Please refer to appendix A as one Perl template file. There are options parameters used in action task, please refer to appendix B.

4 Function verification

Now that we've looked at definitions, it's easier to see how SNMP operates in a network. In its simplest form, an SNMP agent is loaded on a host with the appropriate MIB components. MIB components include the SNMP MIB, and may include RMON extensions, private MIB extensions, or a combination.

In this study it would be helpful to monitor production devices in time and to get an alert message when managed devices encountered fault. The evident message would assist in troubleshooting. Here we would set up one test environment to verify the monitor mechanism. Due to budget issue, it could not verify possible managed device discussed in this paper. The test environment is quite simple. We still believe their operation theory is similar. Hence it works in this test. The result would be proved in the possible managed devices. Below are we would verify parts;

- monitor status of managed devices
- monitor threshold of managed devices
- Build up network map
- alarm through mail mechanism

In this study it would be adopted Cacti system as test framework. It is a quite popular monitor system. It could be executed on Linux OS. The monitor mechanism is similar with HP OpenView network node manager. The test is focus on operation theory proven, not additional customization.

4.1 About setting on Cacti

The following paragraphs describe the related setting on Cacti monitor system. Initially it starts setting tab from Web login to set the related settings we want to.

4.1.1 Configuration set up

This figure 4-1 depicts how to setup in Cacti from web interface under configuration field to choose setting menu.

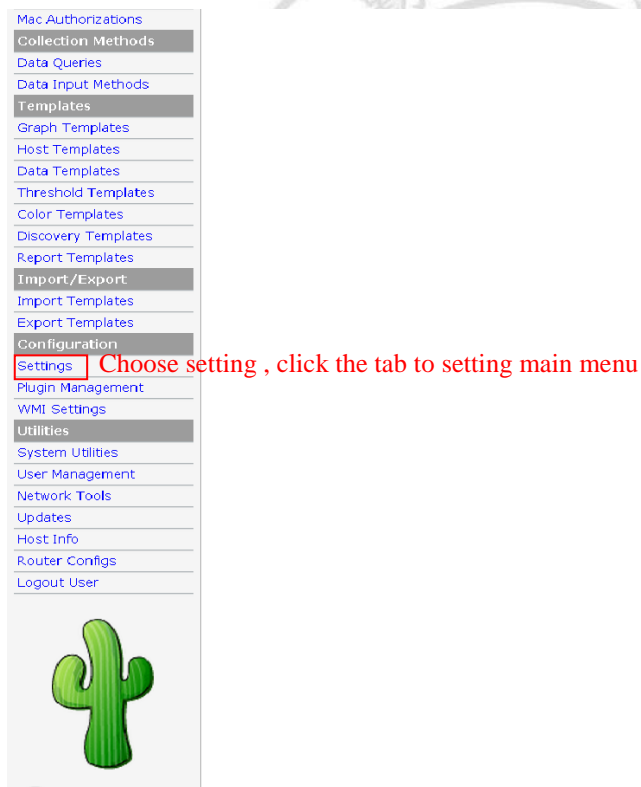


Figure 4-1 Cacti function tabs

In setting function, the page displays for every setting Cacti could support. Every tree is for different function and feature supporting. Here is an example to set up an alert system through mail, then respectively to define Alerting/Threshold, Mail/DNS,

and Misc. three trees. Please refer to Figure 4-2. More detailed procedures are in Figures 4-3, 4-4 and 4-5. About the related fields in every setting; please refer to Cacti Web to get the information.

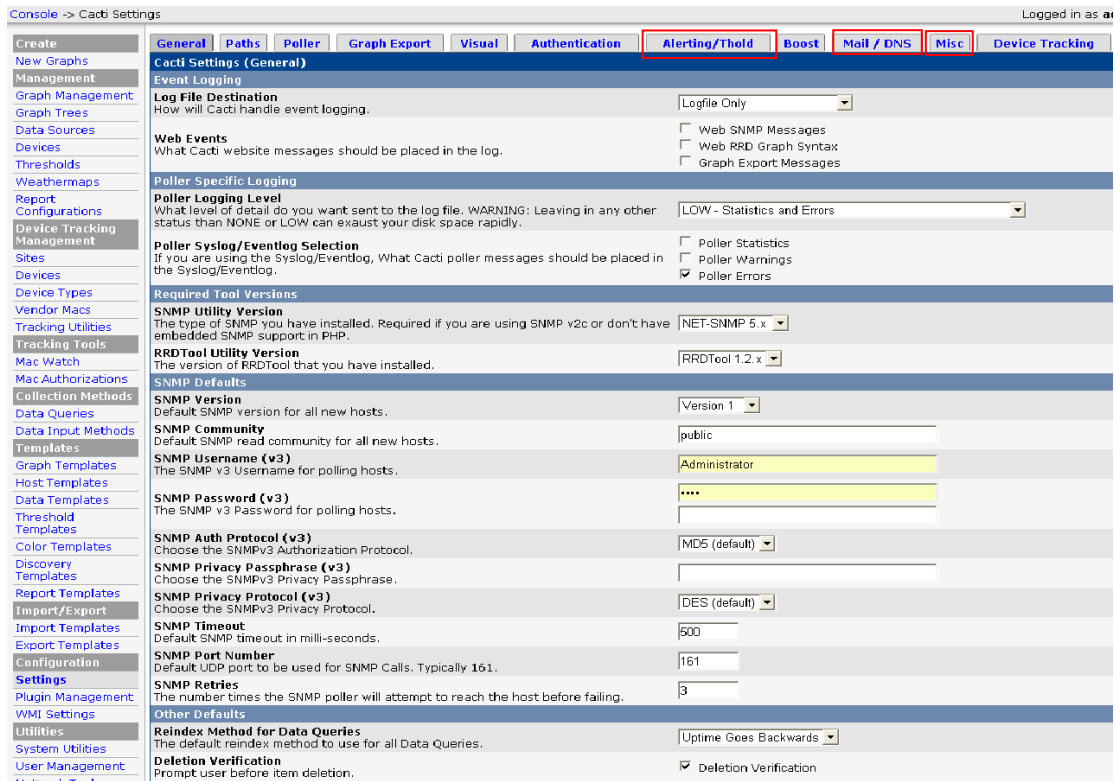


Figure 4-2 Set up function tabs

■ Alerting/Threshold setup

Console -> Cacti Settings Logged in as ad

General Paths Poller Graph Export Visual Authentication Alerting/Thold Boost Mail / DNS Misc Device Tracking

Cacti Settings (Alerting/Thold)

General

Disable all thresholds
Checking this box will disable alerting on all thresholds. This can be used when it is necessary to perform maintenance on your network. Disable all thresholds

Base URL
Cacti base URL

Syslogging
These messages will be sent to your local syslog. If you would like these sent to a remote box, you must setup your local syslog to do so. Syslogging

Syslog Level
This is the priority level that your syslog messages will be sent as.

Syslog Facility
This is the facility level that your syslog messages will be sent as.

Thresholds per page
Number of thresholds to display per page

Log Threshold Breaches
Enable logging of all Threshold failures to the Cacti Log Log Threshold Breaches

Log Threshold Changes
Enable logging of all Threshold changes to the Cacti Log Log Threshold Changes

Default Alerting Options

Dead Hosts Notifications
Enable Dead/Recovering host notification Dead Hosts Notifications

Dead Host Notifications Email
This is the email address that the dead host notifications will be sent to. **One mail account assignment**

Send alerts as text
If checked, this will cause all alerts to be sent as plain text emails with no graph. The default is HTML emails with the graph embedded in the email. Send alerts as text

Weekend exemptions
If this is checked, thold will not run on weekends. Weekend exemptions

Default Trigger Count
Number of consecutive times the data source must be in breach of the threshold for an alert to be raised

Re-Alerting
Repeat alert after specified number of cycles.

Alert Text Message
This is the message that will be displayed at the top of all threshold alerts (255 Char MAX). HTML is allowed, but will be removed for text only emails. There are several descriptors that may be used.
<DESCRIPTION> <HOSTNAME> <TIME> <URL> <GRAPHID>
<CURRENTVALUE> <THRESHOLDNAME> <DSNAME> <SUBJECT> <GRAPH>

Default Baseline Options

Figure 4-3 Alerting mail account setting

Utilities System Utilities User Management Network Tools Updates Host Info Router Configs Logout User

Default Baseline Options

Baseline notifications
Enable sending alert for baseline notifications Baseline notifications

Default Baseline Trigger Count
Number of consecutive times the data source must be in breach of the calculated baseline threshold for an alert to be raised

Baseline reference in the past default
This is the default value used in creating thresholds or templates.

Baseline time range default
This is the default value used in creating thresholds or templates.

Baseline deviation percentage
This is the default value used in creating thresholds or templates.

Emailing Options

From Email Address
This is the email address that the threshold will appear from. **One mail account assignment**

From Name
This is the actual name that the threshold will appear from.

Figure 4-4 Mail account setting for threshold

■ Mail/DNS setting

General Paths Poller Graph Export Visual Authentication Alerting/Thold Boost Mail / DNS Misc Device Tracking Reports

Cacti Settings (Mail / DNS) Send a Test Email

Emailing Options

Test Email
This is a email account used for sending a test message to ensure everything is working properly.

Mail Services
Which mail service to use in order to send mail.

From Email Address
This is the email address that the email will appear from.

From Name
This is the actual name that the email will appear from.

Word Wrap
This is how many characters will be allowed before a line in the email is automatically word wrapped. (0 = Disabled)

Sendmail Options

Sendmail Path
This is the path to sendmail on your server. (Only used if Sendmail is selected as the Mail Service)
[OK: FILE FOUND]

SMTP Options

SMTP Hostname
This is the hostname/IP of the SMTP Server you will send the email to.

SMTP Port
This is the port on the SMTP Server that SMTP uses.

SMTP Username
This is the username to authenticate with when sending via SMTP. (Leave blank if you do not require authentication.)

SMTP Password
This is the password to authenticate with when sending via SMTP. (Leave blank if you do not require authentication.)

DNS Options

Primary DNS IP Address
Enter the primary DNS IP Address to utilize for reverse lookups.

Secondary DNS IP Address
Enter the secondary DNS IP Address to utilize for reverse lookups.

DNS Timeout
Please enter the DNS timeout in milliseconds. Cacti uses a PHP based DNS resolver.

The button is to verify mail

Figure 4-5 Mail / DNS setting

Herein, we verify mail function, Figure 4-6 is received mail through mail test

寄件者	主旨	收件日期
SG	SG - CPU Utilization - CPU1 [cpu] is still above threshold of...	2010/5/18 下午 06:17
Mail Delivery Subsystem	Warning: could not send message for past 4 hours	2010/5/20 上午 01:20
freeangel	Cacti Test Message	2010/5/17 下午 05:58
freeangel	Cacti Test Message	2010/5/15 下午 12:09

寄件者: freeangel 收件者: s39517026@student.ncut.edu.tw
主旨: Cacti Test Message

This is a test message generated from Cacti. This message was sent to test the configuration of your Mail Settings.

Your email settings are currently set as follows

Method: SMTP
Host: localhost
Port: 25
Authentication: false

----- Information from ESET NOD32 Antivirus, version of virus signature database 5120 (20100517) -----

The message was checked by ESET NOD32 Antivirus.

<http://www.eset.com>

Figure 4-6 Mail function verification

■ Miscellanies

Under Misc function tab, it is to define syslog events here, not focus on configuration backup notification on routers in Figure 4-7.

Syslog Events	
Refresh Interval This is the time in seconds before the page refreshes. (1 - 300)	300
Syslog Retention This is the number of days to keep events. (0 - 365, 0 = unlimited)	30
From Email Address This is the email address that syslog alerts will appear from.	s39517026@student.ncut.edu.tw
From Display Name This is the display name that syslog alerts will appear from.	SG
Plugin Updates	
Update Scan Interval The amount of time in between checking for Updates.	Never
Network Weathermap	
Page style How to display multiple maps.	Thumbnail Overview
Thumbnail Maximum Size The maximum width or height for thumbnails in thumbnail view, in pixels. Takes effect after the next poller run.	250
Refresh Time How often to refresh the page in Cycle mode. Automatic makes all available maps fit into 5 minutes.	Automatic
Output Format What format do you prefer for the generated map images and thumbnails?	PNG (default)
Map Rendering Interval How often do you want Weathermap to recalculate it's maps? You should not touch this unless you know what you are doing! It is mainly needed for people with non-standard polling setups.	Every Poller Cycle (default)
Quiet Logging By default, even in LOW level logging, Weathermap logs normal activity. This makes it REALLY log only errors in LOW mode.	Quiet
Router Configs	
TFTP Server IP Must be an IP pointing to your Cacti server.	
Backup Directory Path The path to where your Configs will be backed up, it must be the path that the local TFTP Server writes to.	/var/routerconfigs [OK: DIR FOUND]
Email Address Email address to send the nightly backup email to. Comma delimitate any extra email addresses.	s39517026@student.ncut.edu.tw
From Address Email address the nightly backup will be sent from.	s39517026@student.ncut.edu.tw
Retention Period The number of days to retain old backups.	30
Realtime Graphs	

Figure 4-7 Miscellanies

4.1.2 Add on managed device to Cacti

The first step to creating graphs for your network is to add a device for each managed devices that you want to create graphs for. A managed device must specify important information such as the network hostname, SNMP parameters, and host type. To manage devices within Cacti, click on the Devices menu item. Then to Click Add will generate a new device form. Description and Hostname are the only two fields that require your input beyond the defaults. If the type of managed device is defined under the host template dropdown, be sure to select it here.

The steps are referred to Figures 4-8, 4-9 and 4-10.

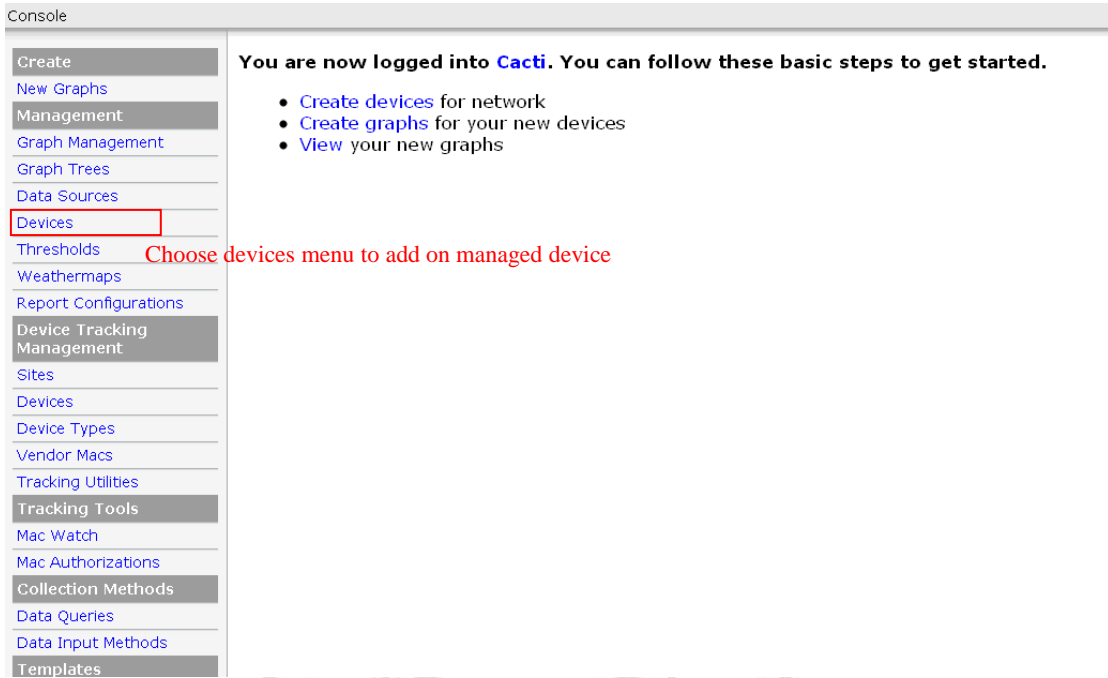


Figure 4-8 Add on managed device through Devices menu

Look up which device already would be included and it is easy to understand managed device's status in Figure 4-9. Then through Add tab button, it is to add on device you want to manage through Cacti.

Add on managed device

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability
10.10.10.251(R-443)	10	6	7	Up	0	10.10.10.251	1.99	2.97	100
140.128.72.1(SHO)	12	5	6	Down	21	140.128.72.1	3.42	3.78	99.57
140.128.86.254	13	6	7	Down	21	140.128.86.254	3.42	4.34	99.62
140.128.87.132	4	2	2	Down	21	140.128.87.132	2.49	1.98	99.6
140.128.87.254	7	6	7	Down	21	140.128.87.254	3.45	4.43	99.57
140.128.88.254	6	8	21	Down	21	140.128.88.254	3.45	4.22	99.56
192.168.2.253(R-443)	11	5	6	Up	0	192.168.2.253	1.75	2.49	100
Chin	8	4	4	Up	0	10.10.10.49	0.5	0.92	59.1
csieserver	5	4	7	Down	21	140.128.87.131	2.22	1.66	99.58
Networkserver	1	7	8	Up	0	10.10.10.3	0.32	0.54	100
SG	2	6	6	Up	0	10.10.10.1	0.5	0.59	99.99
SSR	14	2	2	Up	0	10.10.10.254	1.31	1.29	99.91
TKT	3	6	6	Up	0	10.10.10.2	1.08	0.85	99.2

Figure 4-9 Managed device status

To add on one managed device from add tab, then modify which items will be monitored in Figure 4-10.

SG (10.10.10.1)

SNMP Information
 System: Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE -
 Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)
 Uptime: 484152812 (56 days, 0 hours, 52 minutes)
 Hostname: FREEANGEL
 Location:
 Contact:

* Create Graphs for this Host
 * Data Source List
 * Graph List

Devices [edit: SG]

General Host Options

Description
Give this host a meaningful description.

Hostname
Fully qualified hostname or IP address for this device.

Host Template
Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host.

Disable Host
Check this box to disable all checks for this host. Disable Host

Monitor Host
Check this box to monitor this host on the Monitor Tab. Monitor Host

Down Host Message
This is the message that will be displayed when this host is reported as down.

Availability/Reachability Options

Downed Device Detection
The method Cacti will use to determine if a host is available for polling.
NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Timeout Value
The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.

Ping Retry Count
The number of times Cacti will attempt to ping a host before failing.

SNMP Options

SNMP Version
Choose the SNMP version for this device.

SNMP Community
SNMP read community for this device.

SNMP Port
Enter the UDP port number to use for SNMP (default is 161).

SNMP Timeout
The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

Maximum OID's Per Get Request
Specified the number of OID's that can be obtained in a single SNMP Get request.

Associated Graph Templates

Graph Template Name	Status
1) Host MIB - Logged in Users	Not Being Graphed
2) Host MIB - Processes	Is Being Graphed (Edit)

Add Graph Template:

Associated Data Queries

Data Query Name	Debugging	Re-Index Method	Status
1) SNMP - Get Mounted Partitions	(Verbose Query)	Uptime Goes Backwards	Success [6 Items, 3 Rows]
2) SNMP - Get Processor Information	(Verbose Query)	Uptime Goes Backwards	Success [4 Items, 4 Rows]
3) SNMP - Interface Statistics	(Verbose Query)	Uptime Goes Backwards	Success [14 Items, 2 Rows]
4) Win Services	(Verbose Query)	Uptime Goes Backwards	Success [108 Items, 54 Rows]

Add Data Query: Re-Index Method:

Figure 4-10 Add on one managed device and its related setting

4.1.3 Create Weathermap

It's useful for management staff to understand the traffic volume between two managed devices. It could gather which managed devices are necessary to display the traffic volume currently and build up the map. Below are to create one weathermap to meet management staffs need. First to choose weathermaps menu from console is like Figure 4-11.

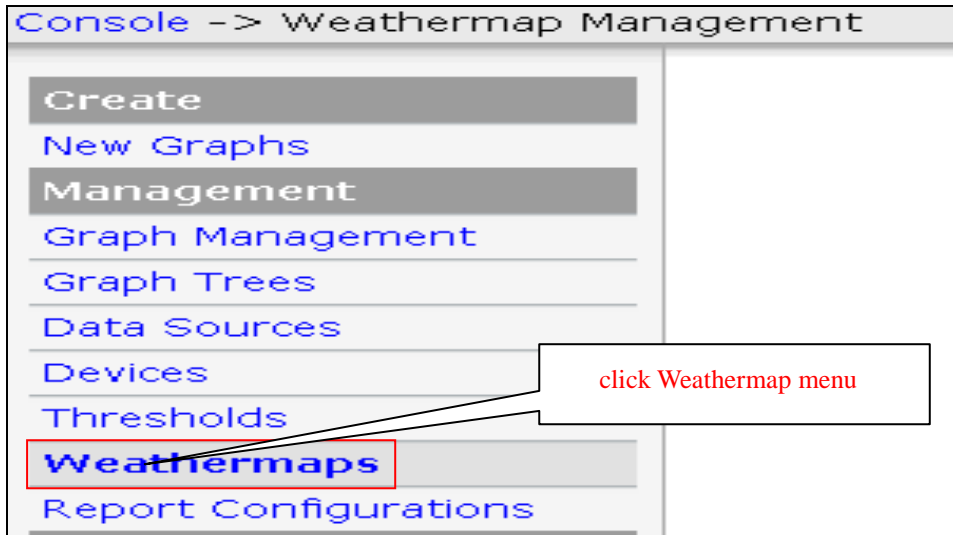


Figure 4-11 Creating Weathermap

Weathermaps					Add
Config File	Title	Active	Sort Order	Accessible By	
CSIE	Network Weathermap	Yes	↑↓	admin	✘

Recalculate All Maps NOW

(Experimental - You should NOT need to use this normally)

Create a new weathermap

Local Documentation -- Weathermap Website -- Weathermap Editor -- This is version 0.95b

Figure 4-12 Creates a new weathermap

Below procedure is to assign a new weathermap and create it.

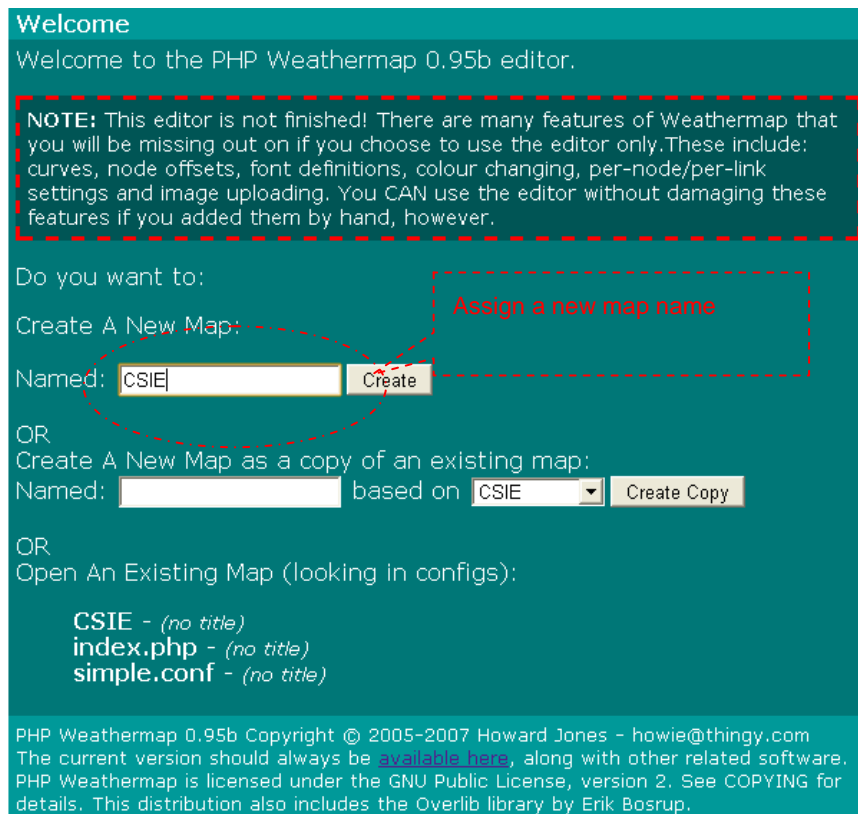


Figure 4-13 Assigns a new map name

After creating a new configuration file of weathermap, it could continue to add which nodes you want to join the map and the link of node. Please refer to Figures 4-14 and 4-15 respectively to add node and add its link.

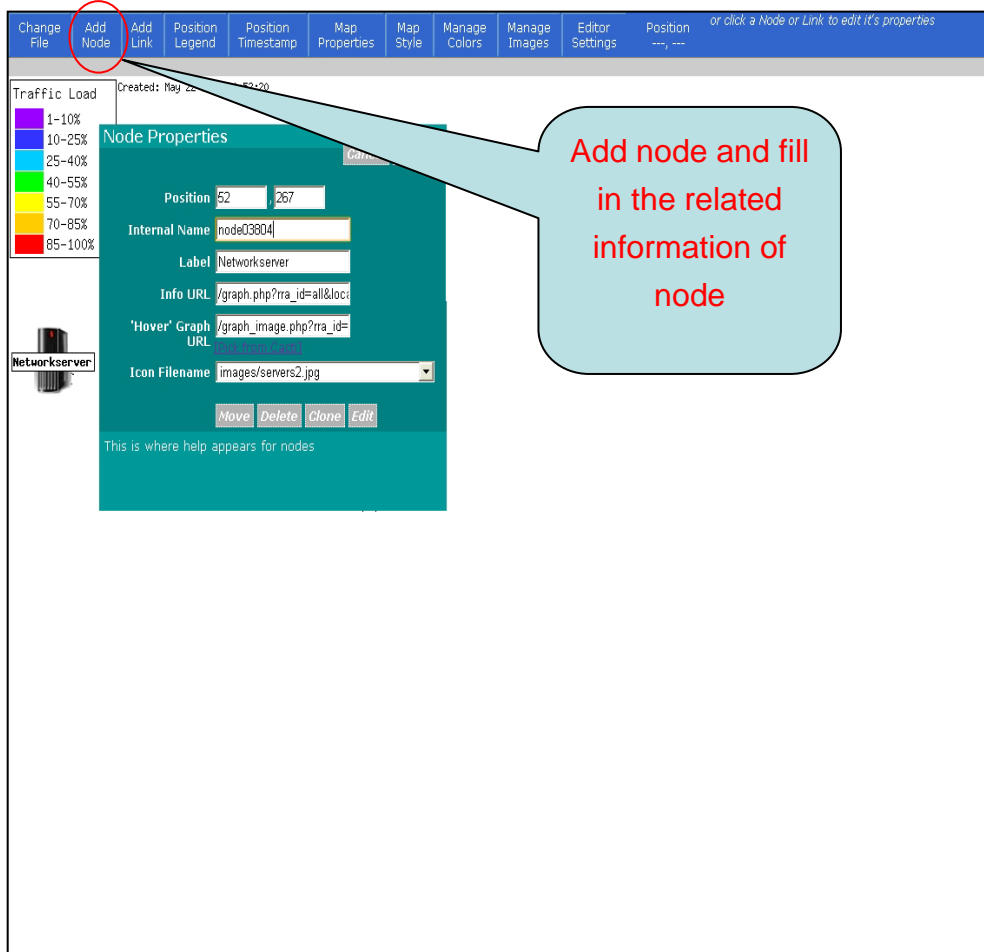


Figure 4-14 Adds a node

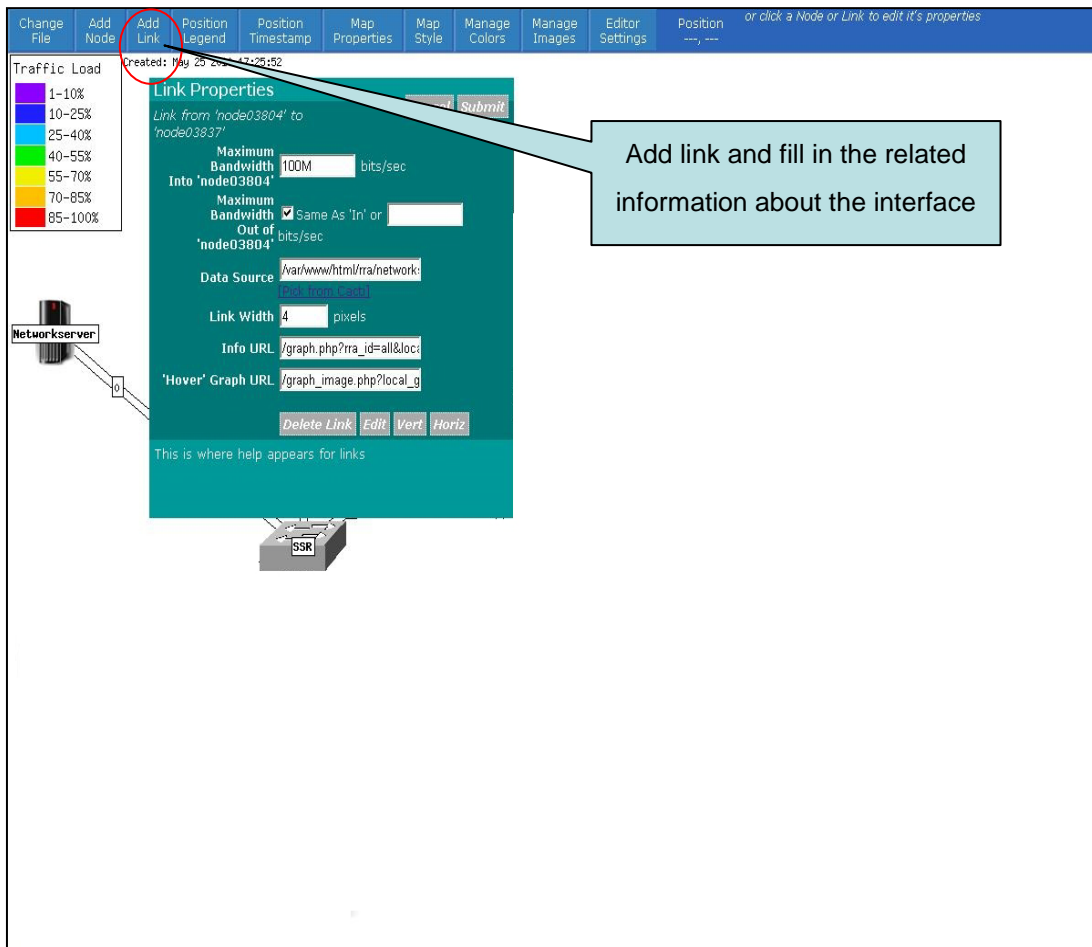


Figure 4-15 Adds a link

In this section, we almost complete the settings for the test environment. We would set some scenarios in test environment to proof the result from Cacti management system.

4.2 Test result from Cacti monitor system

This section would focus on proof the result. At meantime we would verify the test qualification from server or device side. Below tasks would be completed in this test.

- monitor status of managed devices
- monitor threshold of managed devices
- build up network map
- alarm through mail mechanism

We would verify the tasks in this study. Every task would cover its scenario,

purpose and test result. Restate our test background. Although it does not all devices, its operation is similar. These results are still proofed and applied to daily management.

4.2.1 Function test from Cacti management system

1: The task is monitor status of managed devices

■ Scenario:

The test is to monitor the status of managed device from Cacti management system. At meantime we would shutdown some managed devices, to observe what response is in Cacti.

■ Purpose:

The purpose is clear and simple. It could be applied to daily management to managed device's status change or not.

■ Result:

The result we do From Cacti management system is able to monitor status of managed device in short time. The Figure 4-15 depicts the status of managed device. From color change, it shows which managed node is up or down.

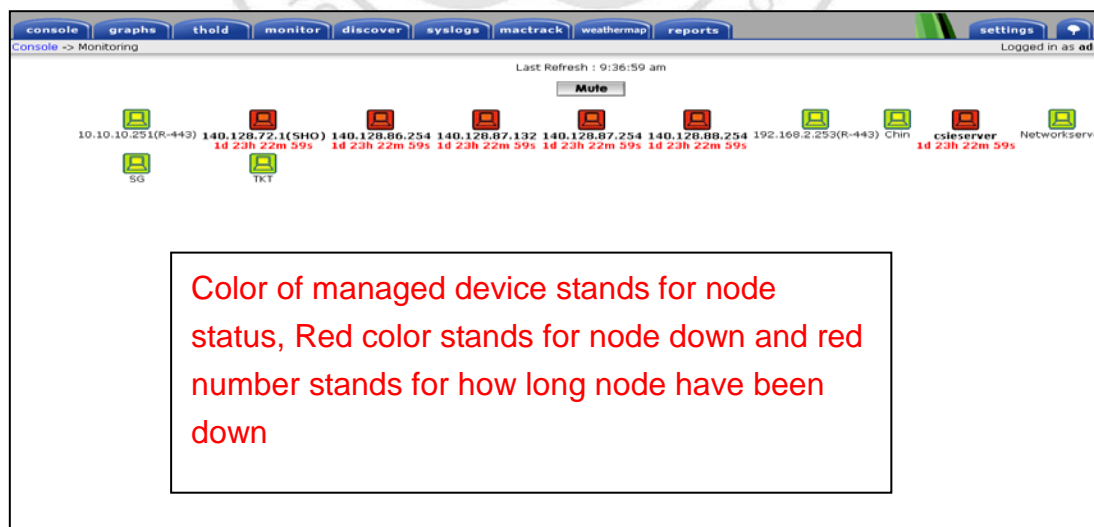


Figure 4-15 Status of managed device

2: The task is to setup the threshold of managed device and build up

an alert mechanism.

■ Scenario:

The test is to verify the function of the threshold mechanism and understand what method is used while reaching the threshold. We also set its threshold to 5 every 5 minutes average for CPU on 192.168.2.253(R-443) router. Of course it would be defined its own threshold.

■ Purpose

The purpose is to build up one mechanism to reach its threshold on managed device. The mechanism is to join one alert message sent to the related staff. Let the management system become more proactive to fault handling.

■ Result

The threshold on managed device reaches its setup value. The alert mechanism would be triggered through mail sent to the mail account. Below is the test result. Figure 4-16 depicts current CPU reached the threshold defined in threshold setting of the device Figure 4-17 depicts the alert message would be sent to the predefined mail account. Figure 4-18 depicts to exam the mail content.

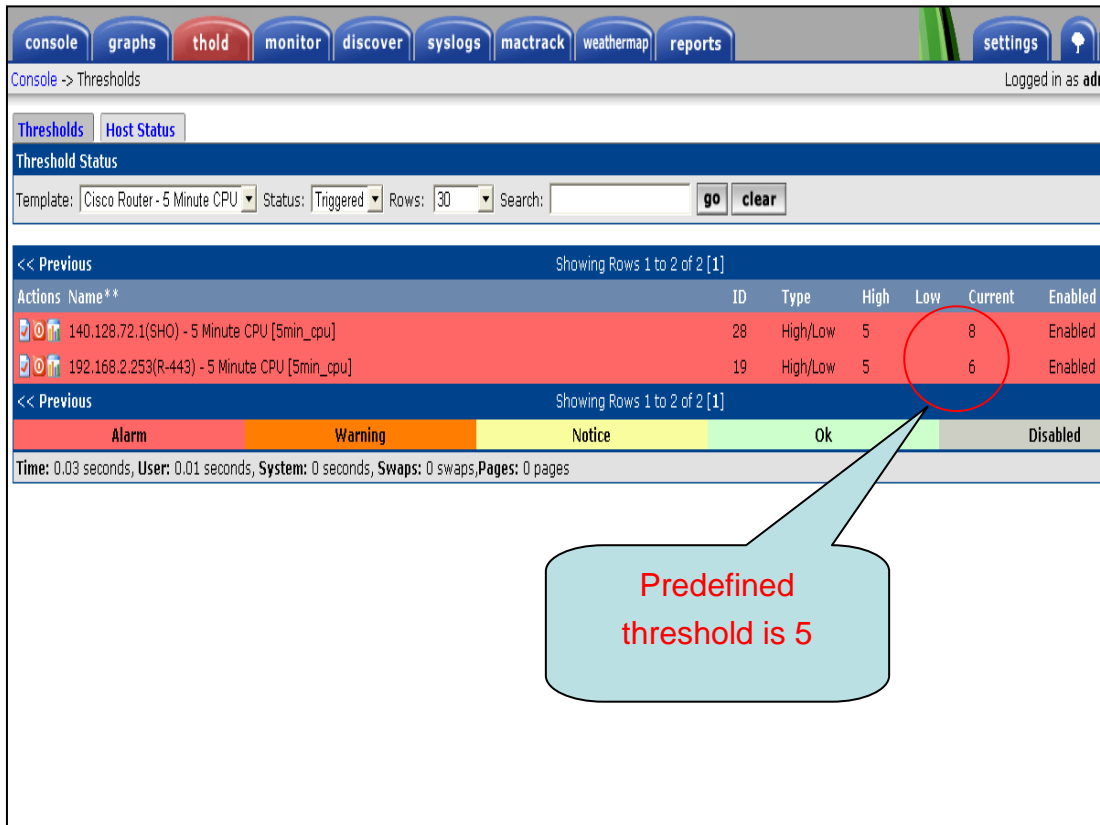


Figure 4-16 Displays Current CPU utilization on threshold tab

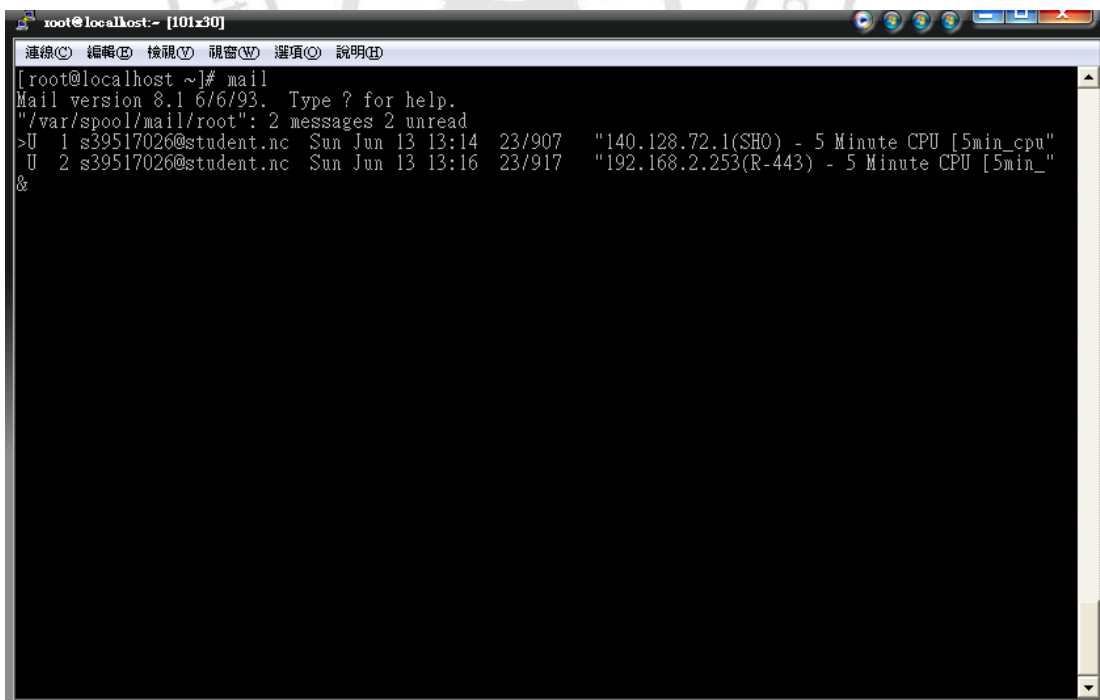
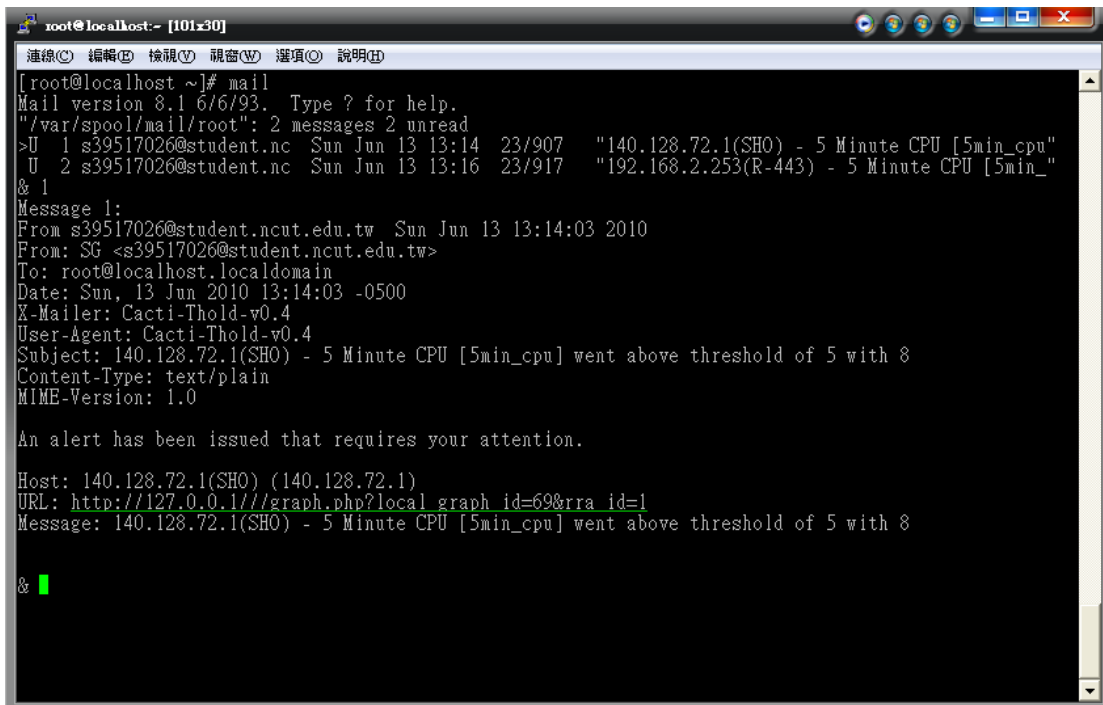


Figure 4-17 Displays one alert message to mail account



```
root@localhost:~# mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/spool/mail/root": 2 messages 2 unread
>U 1 s39517026@student.nc Sun Jun 13 13:14 23/907 "140.128.72.1(SHO) - 5 Minute CPU [5min_cpu"
  U 2 s39517026@student.nc Sun Jun 13 13:16 23/917 "192.168.2.253(R-443) - 5 Minute CPU [5min_"
  & 1
Message 1:
From s39517026@student.ncut.edu.tw Sun Jun 13 13:14:03 2010
From: SG <s39517026@student.ncut.edu.tw>
To: root@localhost.localdomain
Date: Sun, 13 Jun 2010 13:14:03 -0500
X-Mailer: Cacti-Thold-v0.4
User-Agent: Cacti-Thold-v0.4
Subject: 140.128.72.1(SHO) - 5 Minute CPU [5min_cpu] went above threshold of 5 with 8
Content-Type: text/plain
MIME-Version: 1.0

An alert has been issued that requires your attention.

Host: 140.128.72.1(SHO) (140.128.72.1)
URL: http://127.0.0.1//graph.php?local\_graph\_id=69&rra\_id=1
Message: 140.128.72.1(SHO) - 5 Minute CPU [5min_cpu] went above threshold of 5 with 8

&
```

Figure 4-18 Looks up mail content

3: The task is to build up network map

■ Scenario:

The test is to build up one map suit for your network topology. The topology information will contain information we need in management and troubleshooting assistance.

■ Purpose

It is used on to get more information in management and assist in troubleshooting. At meantime it could create one baseline to traffic volume, CPU utilization, memory usage... etc. It is used to plan to upgrade or add on device in the future.

■ Result

From this test, it could understand the network topology, the traffic volume between the managed nodes and the CPU utilization of managed node. It means the information is valuable to management and troubleshooting. Figure 4-19 shows the traffic volume between node04080 and node09623. Figure 4-20 depicts

the CPU utilization of this managed node

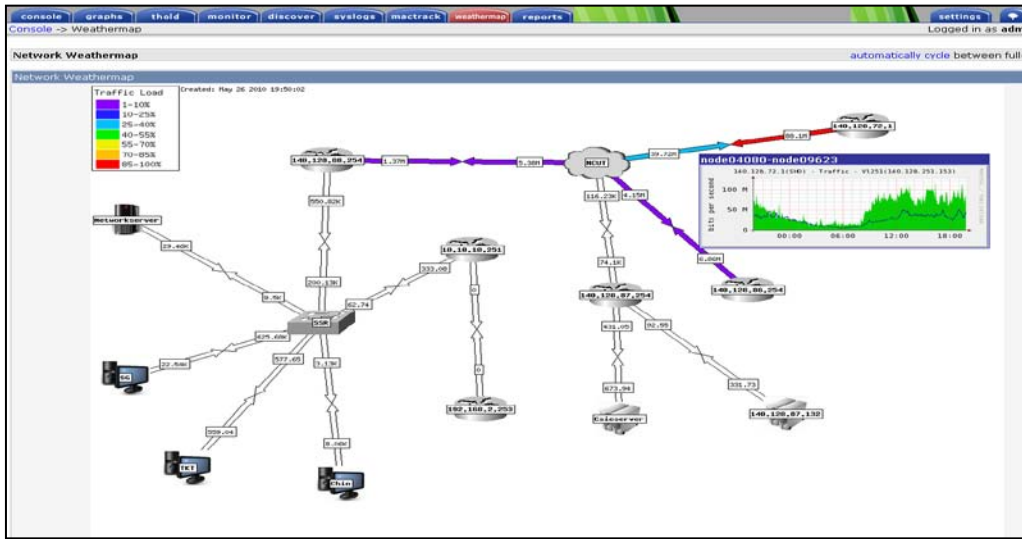


Figure 4-19 Shows traffic volume from map

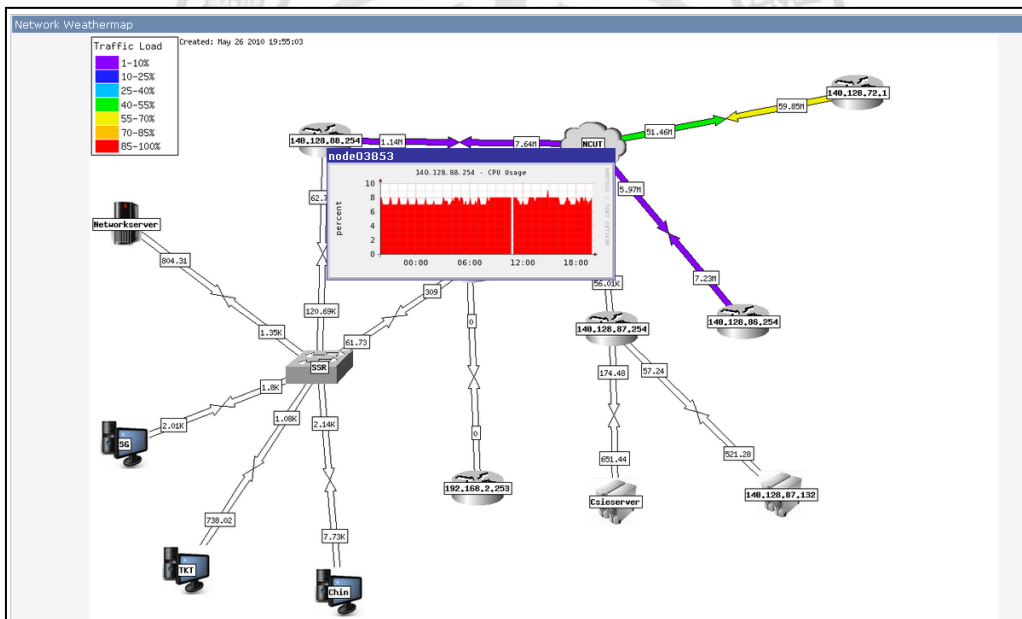


Figure 4-20 Displays CPU utilization from a managed node on map

4.2.2 Accuracy verification

In the section we would proof the data from Cacti management system is accurate or not. It's more accurate, it is more reliable in management. Here is to explain why it verifies the accuracy in this item. Any action would be launched before production. They must make sure

it is right and accurate to the action. Especially in management, it is used in 7X24 monitor mechanism. If it is any errant in management, it would loss the reliability in daily operation. Any differentiated value is not allowed in management sector. If the differentiation exists, it must stop any alarm or alert to this item before why it is dipped out. Firstly it could take a investigation in this MIB and the related setting on management system to understand what wrong it is. It is a easy way to query the MIB to issue “snmpwalk” command to get the current value. Secondly it is to inquire the information of this MIB from the original vendor. It is a fast way to get your answer fro the original vendor. Thirdly this is an unsupported in measured value from MIB that it is being monitored. Try to the other way to meet the requirement of production. Of course it seldom occurs. In production environment, any action must be verified to make sure it is accurate and reliable. It takes the opportunity to emphasize the reliability in management.

Here is to take three comparisons on CPU utilization and memory usage on router and CPU utilization on server. Below is its comparison. Figure 4-21 and Figure 4-22 depict the comparison for CPU utilization on router. Figures 4-23 and 4-24 depict the comparison for memory usage on router. Figures 4-25 and 4-26 depict the comparison for CPU utilization on server.

■ comparison for CPU utilization on router

The CPU utilization of router_192_168_2 is 6 % every 5 minutes average from “show process cpu” command. At the same its CPU utilization from Cacti also display 6 % every 5 minutes average. Two values from different ways to get are the same.

```

c:\ Telnet 192.168.2.253
router_192_168_2#show proc cpu
CPU utilization for five seconds: 7%/0%; one minute: 6%; five minutes: 6%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min   TTY Process
 1         0         13         0  0.00%  0.00%  0.00%  0 Chunk Manager
 2         0        51264         0  0.00%  0.00%  0.00%  0 Load Meter
 3         0         1         0  0.00%  0.00%  0.00%  0 CEF RP IPC Backg
 4      224170      30410      7371  0.00%  0.09%  0.06%  0 Check heaps
 5         8         42        190  0.00%  0.00%  0.00%  0 Pool Manager
 6         0         2         0  0.00%  0.00%  0.00%  0 Timers
 7         0         1         0  0.00%  0.00%  0.00%  0 Net Input
 8         0         1         0  0.00%  0.00%  0.00%  0 Crash writer
 9        42        4316         9  0.00%  0.00%  0.00%  0 ARP Input
10         0         1         0  0.00%  0.00%  0.00%  0 CEF MIB API
11         0         1         0  0.00%  0.00%  0.00%  0 AAA_SERUER_DEADT
12         0         2         0  0.00%  0.00%  0.00%  0 AAA_high-capacit
13         0         1         0  0.00%  0.00%  0.00%  0 Policy Manager
14        17         6      2833  0.00%  0.00%  0.00%  0 Entity MIB API
15         0         1         0  0.00%  0.00%  0.00%  0 IFS Agent Manage
16         8        4280         1  0.00%  0.00%  0.00%  0 IPC Dynamic Cach
17         0         1         0  0.00%  0.00%  0.00%  0 IPC Zone Manager
18        319      252939         1  0.00%  0.00%  0.00%  0 IPC Periodic Tim
19         0         1         0  0.00%  0.00%  0.00%  0 IPC Managed Time
20        231      252939         0  0.00%  0.00%  0.00%  0 IPC Deferred Por
21         41      17108         2  0.00%  0.00%  0.00%  0 IPC Seat Manager
22         0         1         0  0.00%  0.00%  0.00%  0 IPC Session Serv
23       1913      252939         7  0.00%  0.00%  0.00%  0 Dynamic ARP Insp
24         0         1         0  0.00%  0.00%  0.00%  0 ARP Snoop
25       3908      252916        15  0.00%  0.00%  0.00%  0 GraphIt
26         0         2         0  0.00%  0.00%  0.00%  0 XML Proxy Client
27         0         1         0  0.00%  0.00%  0.00%  0 Critical Bkgn
28       1014      205780         4  0.00%  0.00%  0.00%  0 Net Background
29         0         1         0  0.00%  0.00%  0.00%  0 IDB Work
30         0         12         0  0.00%  0.00%  0.00%  0 Logger
31       3607      252912        14  0.00%  0.00%  0.00%  0 TTY Background
32      11074      252939        43  0.00%  0.00%  0.00%  0 Per-Second Jobs
33      76456      4320      17698  0.00%  0.02%  0.00%  0 Per-minute Jobs
34         17         6      2833  0.00%  0.00%  0.00%  0 IF-MGR control p
35         0         7         0  0.00%  0.00%  0.00%  0 IF-MGR event pro
36         0         1         0  0.00%  0.00%  0.00%  0 AggMgr Process
37       9280      51124        181  0.00%  0.00%  0.00%  0 Compute load avg
38         0         1         0  0.00%  0.00%  0.00%  0 Transport Port A
39       3133      76634         40  0.00%  0.00%  0.00%  0 HC Counter Timer
40         0         1         0  0.00%  0.00%  0.00%  0 SFF8472
41        420      5098202         0  0.00%  0.00%  0.00%  0 DownWhenLooped
42         0         1         0  0.00%  0.00%  0.00%  0 HRPC lpip reques
43         0         2         0  0.00%  0.00%  0.00%  0 HLP/IP Sync Proce
44         0         1         0  0.00%  0.00%  0.00%  0 HULC ASP Process
45         0         1         0  0.00%  0.00%  0.00%  0 Hule LED Alchemy
46         0         1         0  0.00%  0.00%  0.00%  0 HRPC asic-stats
47         0         1         0  0.00%  0.00%  0.00%  0 HRPC hsm request
48         0         7         0  0.00%  0.00%  0.00%  0 Stack Mgr
49        218         6      36333  0.00%  0.00%  0.00%  0 Stack Mgr Notifi
50      40436     1332814        30  0.00%  0.04%  0.00%  0 RedEarth Tx Mana
51      10908     10114258         1  0.00%  0.00%  0.00%  0 RedEarth Rx Mana
52         0         1715         0  0.00%  0.00%  0.00%  0 HULC Thermal Pro
53      347639     13625056        25  0.15%  0.11%  0.11%  0 Fifo Error Detec
54         0         3         0  0.00%  0.00%  0.00%  0 Adjust Regions
55      12079      252927        47  0.00%  0.00%  0.00%  0 hrpc -> response
56         214        51139         4  0.00%  0.00%  0.00%  0 hrpc -> request
57        2150        51139        42  0.00%  0.00%  0.00%  0 hrpc <- response

```

Figure 4-21 CPU utilization of R-443

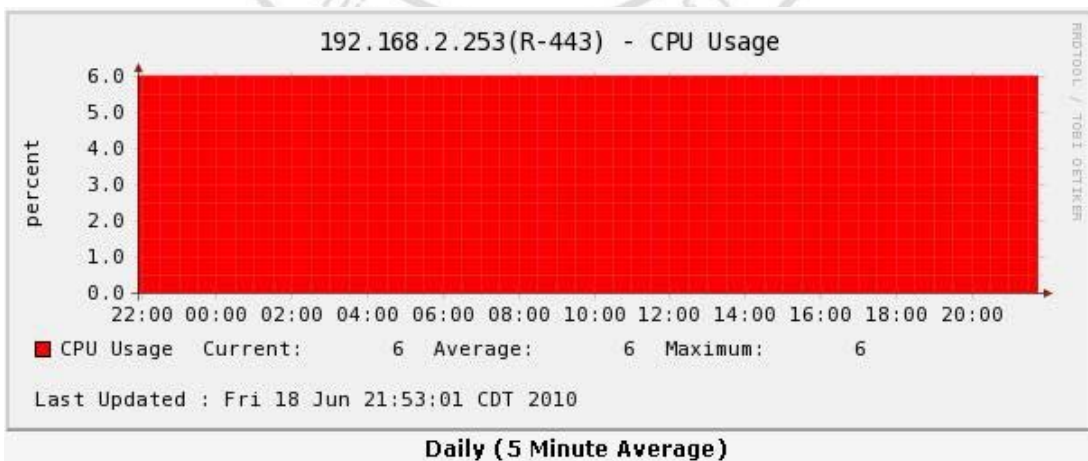


Figure 4-22 CPU utilization of R-443 from Cacti

- comparison for processor memory usage on router

From “show process memory” command, the used memory is 18430620 bit. From Cacti system it shows the memory usage is 18.43 Mbit currently (18.43*1000000=18430000). Two values from different ways to get are quite close.

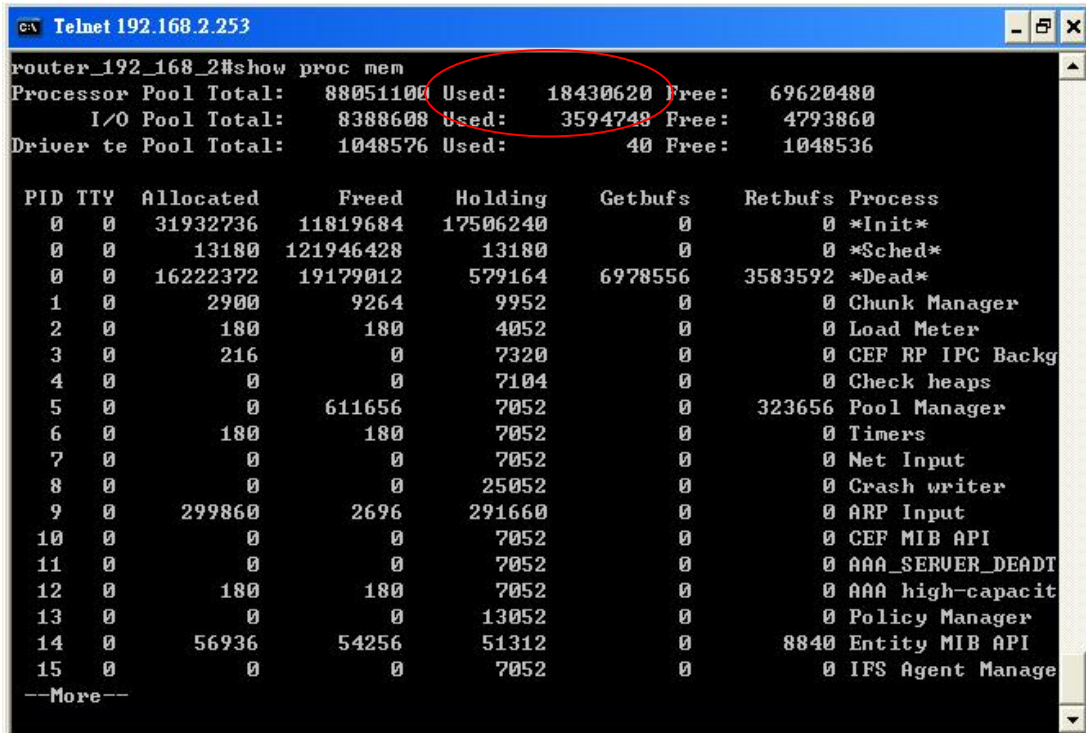


Figure 4-23 Processor memory usage of R-443

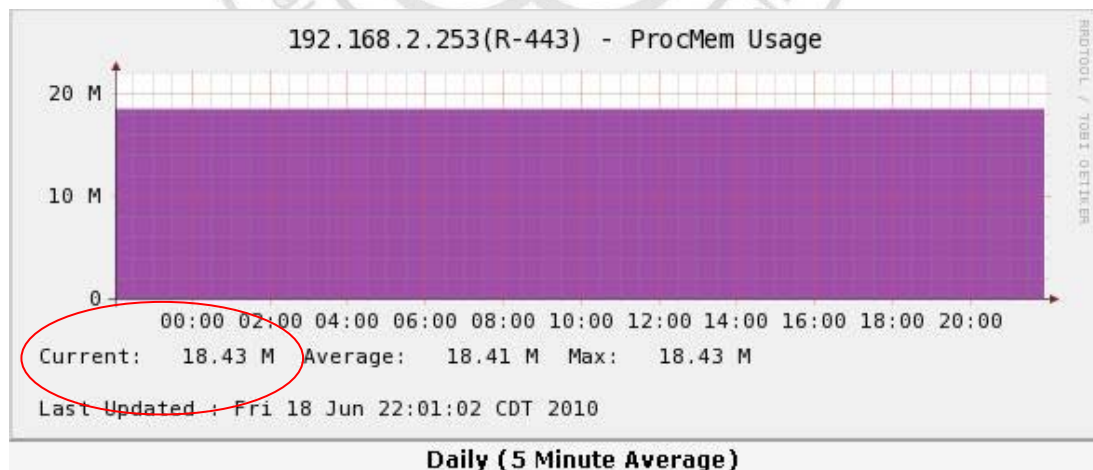


Figure 4-24 Process memory usage of R-443 from Cacti

- comparison for CPU utilization on server

The CPU utilization on network server is 25 % through top

command. The CPU utilization of network server displays almost 25 % on Cacti management system.

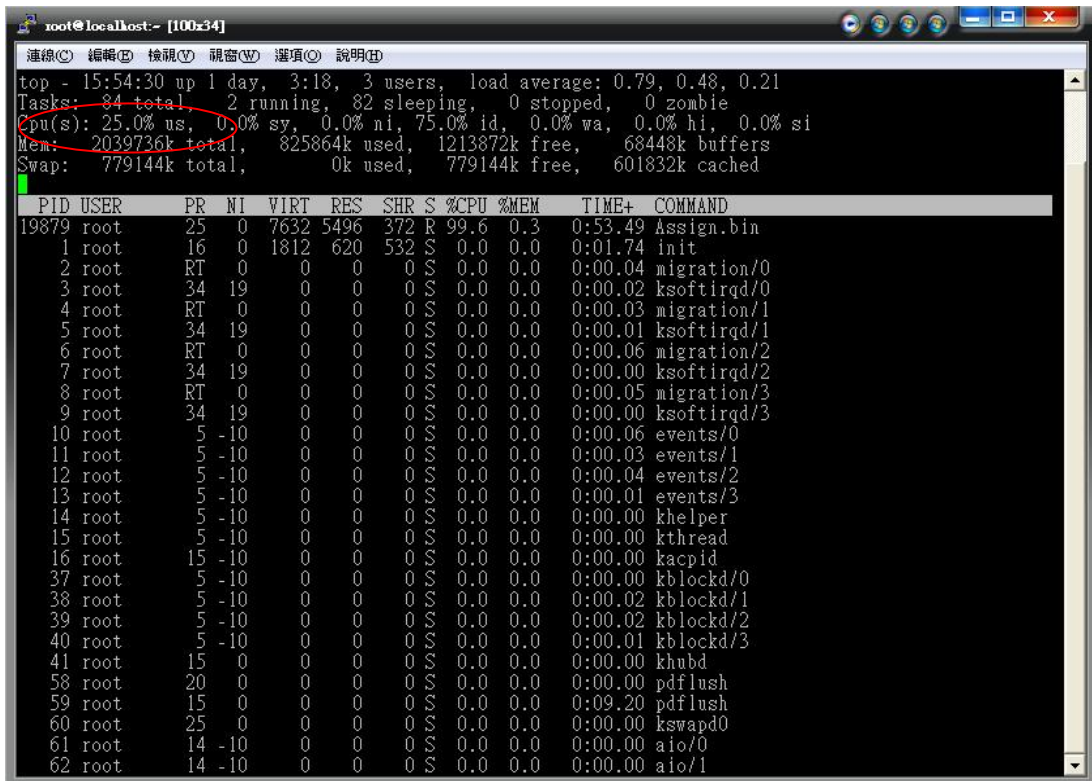


Figure 4-25 CPU utilization of network server

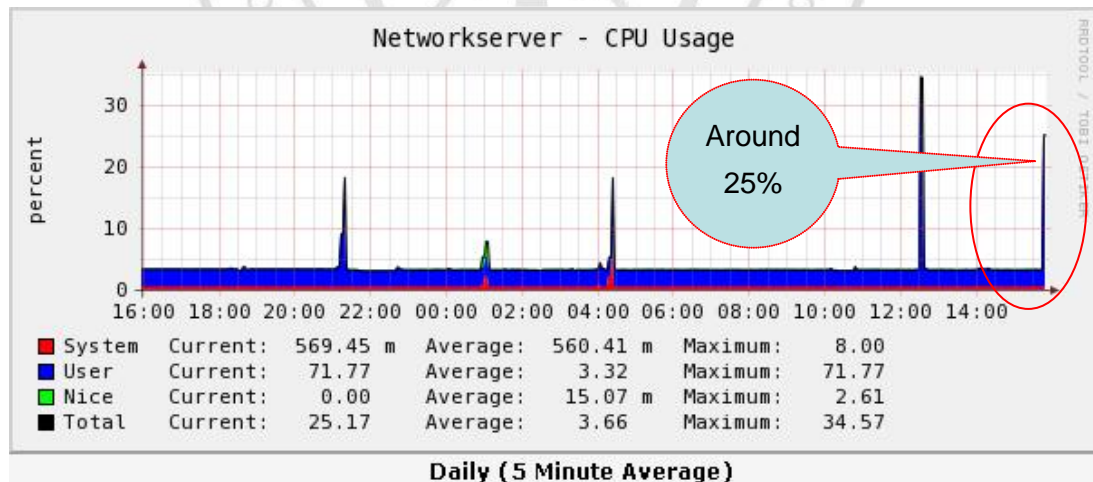


Figure 4-26 CPU utilization of network server from Cacti

From these tests and comparison, we know Cacti management system almost could meet our setup goal. It could be used on management system to assist daily operation. It's able

to reduce the burden of man power in management through pre-defined rule.

4.3 Limitation on test environment

It is simple and clear in test environment. It's just to prove the operation is workable or not. In real environment, probes or multiple management systems may be used in remote sites to limit WAN-based SNMP communication. In typically probes would collect SNMP, RMON and process the data collected. Remote management system may also relay information to one or more centralized management systems. It is also scalable on its architecture.

The other is a trap operation. Cacti management system runs well in different management fields which include traffic monitor, CPU utilization, topology discovery... etc. But it's not good at trap handling. In fact we focus on how to centrally manage in managed devices with multi-platforms in this Lab.

5 Management system comparison

In this study, an integrated proactive management system is provided to use a common management platform to manage any devices, such as network equipments, application servers and equipment with SNMP agent enabled. The purpose is to provide a central management platform to easily access the related message from fault devices or potential event on occurring on managed devices. The IT staff does not inspect any log or message to every device IT staff manages.

In early IT environment without management system, IT staff must inspect any suspected device step by step through his/her personally experience to dip out the root cause. Below procedures are used to troubleshoot on server step by step;

- 1: To log into the suspected system by one experienced staff
- 2: To check logs or messages under the proper directory

3: Maybe it needs more resource to decode the error message or the staff is not good at this parts.

4: Maybe it is not a root cause in this server impacted by the device

5: Probably repeat these checking on the other device until root cause found.

It could take much time in troubleshooting compared with proactive management system. Here is to take a comparison between smart human being and a proactive management system. Detailed comparison shows on Table 5-1.

Table 5-1 Depiction of the advantage

Method	IT staff	Proposed proactive management system
Measured item		
Efficiency to one managed device	Fair, minutes per target	Excellent, seconds per target
Troubleshooting time	More than 30 minutes	Less than 5 minutes depends on time resolution
Accuracy	Human error	After proof, approach to 100% accuracy
Managed domain	Around 50-100 managed devices	More than 200 managed devices
Judgment credit	Learned capacity	Follow up policy rule

Therefore one integrated proactive management system processes any events incoming from managed devices in one common event handling. The event handling is served through FIFO mechanism. It is easily understood event happened orderly and the topology map exist in the management system. It is

useful information to catch up the relationship each other in short time.

In general it is hardly to find what wrong it is in redundancy mechanism. To daily operation is no impact if backup mechanism is out of service. It must be through daily check to find these problems. Management system would monitor the managed device in time and get ready to process trap message from a fault managed device. It could save time and recover human error to managed devices.

With this proposed scheme, the fault identification and hence the troubleshooting time can be greatly reduced. Table 5 displays the comparison among different management schemes. In Table 5-1, the “✓” symbol indicates the benefit is to let IT staff know faulty device through an alerting mechanism in time. Meanwhile, the “x” symbol stands for the lags occurs in event handling.

Table 5-2 Benefit in different management methodology

NMS supported Managed devices	No NMS	NMS only	Integrated MS
Device itself monitor	✓	✓	✓
Managed network device	x	✓	✓
Managed sever	x	x	✓
Managed SAN switch	x	x	✓
Managed storage controller	✓(like itself monitor)	x	✓
Managed process daemon	✓(like daemon checking)	x	✓

There are many equipments supporting SNMP agent used in IT filed. It is a necessary to integrate into a management system to gain to its benefit.

6 Conclusions and feature works

In this study, a proactive integrated management system is suggested for fault management operation and effective management system. The goal of this work is to greatly save troubleshooting time and reduce man power in management.

6.1 Conclusions

According to the comparison among management systems, the proposed scheme is a lightweight management system to provide effective and efficient management on internet servers and network devices. However, the deployed management system has to be tailored to the dedicated communication environment.

The management system would incorporate alarm system or mail system depending on event severity level to take the appropriate action in time. It could save event troubleshooting time and it could reduce production loss. From management view, the management system would be a good sentry. It needs to incorporate a powerful alarm utility to join into a proactive management system. That's a total solution to management system.

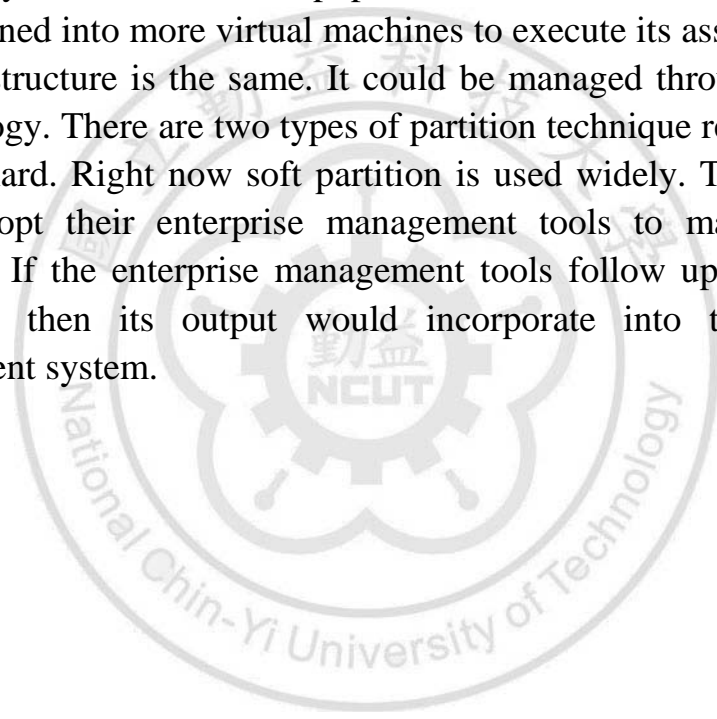
In general the factor that is a single point failure in management system would be considered. If the budget is allowed, the redundancy of management system would be implemented. The disaster site is a good place to locate the other management system.

6.2 Feature works

Here is to restate alarm system deployed in management domain.

It's a critical factor to decide how fast the event message be sent to the related IT staff. Then it could be a bi-direction mechanism. The information delivered to IT staff will be reviewed in implement stage. If the description message about the incoming event is not clear to IT staff. It must be revised for the description in test stage. After all tests in your plan pass, the management system would be launched to production. The other is tracking mechanism. It means how long it does not get response. The notification mechanism should set a higher priority and send to the higher level IT staff. These factors will be considered one by one. A management system will become more perfect and reliable through different views to implement.

Today virtual machine is popular. First it is a real machine would be partitioned into more virtual machines to execute its assignment jobs. The infrastructure is the same. It could be managed through the same methodology. There are two types of partition technique respectively to soft and hard. Right now soft partition is used widely. These vendors would adopt their enterprise management tools to manage virtual machines. If the enterprise management tools follow up SNMP RFC definition, then its output would incorporate into the proactive management system.



References

- [1] Brad Stone and Julia Symons, *Unix fault management- a guide for system administrators*, Prentice Hall, 1996.
- [2] HP OpenView network node manager managing your network
HP OpenView solutions reference guide
- [3] SNMP related information, <http://www.ietf.org>
- [4] Management in Sun web,
<http://java.sun.com/j2se/1.5.0/docs/guide/management/SNMP.htm>
[1](#)
- [5] Essential SNMP on Oreilly web
information <http://oreilly.com/catalog/esnmp/chapter/ch02.html>
- [6] William Stallings, *SNMP, SNMPv2 and CMIP- The practical guide to network management standards*, Addison Wesley, 1993
- [7] Structure and identification of management information for TCP/IP based internets, <http://www.javvin.com/protocol/rfc1155.pdf>
- [8] A simple network management protocol, <http://www.javvin.com/protocol/rfc1157.pdf>
- [9] Introduction to SNMP v2, <http://www.javvin.com/protocol/rfc1441.pdf>
- [10] Management information base network, <http://www.javvin.com/protocol/rfc1156.pdf>
- [11] User-based security model (USM) for SNMP v3, <http://www.javvin.com/protocol/rfc3414.pdf>
- [12] SNMP applications, <http://www.javvin.com/protocol/rfc3413.pdf>
- [13] About download MIB for Cisco devices <http://www.cisco.com/public/sw-center/netmgmt/mtk/mibs.shtml>
- [14] About configure SNMP on Oracle http://download.oracle.com/docs/cd/E11857_01/em.111/b16244/chap2.htm
- [15] Network management in Oracle http://www.oracle.com/corporate/press/2008_feb/united-illuminating.html
- [16] Discuss monitor

- tools, <http://www.monitortools.com/snmp/>
- [17] About alert in Whatsup web, <http://www.whatsupgold.com/technology/network-management/alert-center/index.aspx>
- [18] About monitor in solarwinds, http://www.solarwinds.com/products/freetools/network_device_monitor/
- [19] How to choose network management system http://www.computerworld.com/s/article/9000849/How_To_Choose_A_Network_Management_System
- [20] Network management system in Huawei http://www.huawei.com/core_network/products/ngn/manager_n2000_operation_support_system.do?card=1
- [21] SNMP network tools on Linux system <http://linas.org/linux/NMS.html>
- [22] OpenNMS demo <http://demo.opennms.org/opennms/login.jsp;jsessionid=1kuevzrzk3oyp7bfyyg4pacfq>
- [23] Network management system in Cisco http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml
- [24] NNM in HP <http://www.openview.hp.com>
- [25] NNM smart plug-in for LAN/WAN in HP https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-119^2521_4000_100
- [26] Cacti information <http://www.cacti.net/index.php>
- [27] Perl script in Cacti forum <http://forums.cacti.net/about663.html&highlight>
- [28] About MIB browser, <http://www.oidview.com/oidview.html>
- [29] Behrouz A. Forouzan, *TCP/IP protocol suite* (second edition), McGraw-Hill, 2003.
- [30] Mark A. Miller, *Troubleshooting TCP/IP- analyzing the protocol of the Internet*, Prentice Hall, 1995.
- [31] Configure SNMP in Cisco http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080662d15.html
- [32] Ben-Artiz, A.; Canada, A.; and Warriar, U., "Network

Management of TCP/IP networks, “ IEEE network Magazine, July, 1990.

- [33] SNMP message in
Microsoft [http://technet.microsoft.com/en-us/library/cc783142\(WS.10\).aspx#w2k3tr_snmp_how_oqdv](http://technet.microsoft.com/en-us/library/cc783142(WS.10).aspx#w2k3tr_snmp_how_oqdv)
- [34] SNMP architecture in
Microsoft [http://technet.microsoft.com/en-us/library/cc783142\(WS.10\).aspx#w2k3tr_snmp_how_syhu](http://technet.microsoft.com/en-us/library/cc783142(WS.10).aspx#w2k3tr_snmp_how_syhu)
- [35] SNMP setup for SAN switches
in <http://community.brocade.com/message/2400#2400>
- [36] SNMP setup for APC UPS in
APC <http://www.apc.com/search/results.cfm?qt=snmp>



Appendix A

Below is a Perl template file. It could be referred to join into alarm system, if the NNM will be integrated with automation system.

```
use FindBin;
use lib "$FindBin::Bin/site/lib";
use Time::localtime;

#####
##
# Get Today (YYYY-MM-DD) and Time (YYYY/MM/DD HH:MM:SS)
#####
##
$tm = localtime(time);
$tod = sprintf("%04d-%02d-%02d", $tm->year+1900, $tm->mon+1, $tm->mday);
$now = sprintf("%04d/%02d/%02d %02d:%02d:%02d", $tm->year+1900,
$tm->mon+1, $tm->mday, $tm->hour, $tm->min, $tm->sec);

#####
##
# Get environment attributes
#####
##
$envfile = "D:/NNM_action/alarm_test.env";
open ENVFILE, "< $envfile" or die "Couldn't open $envfile for reading: $!\n";
foreach $line (<ENVFILE>) {
    chomp $line;
    @TIBCO_BIN = split /=/, $line if ( $line =~ /\bTIBCO_BIN\b/ );
    @BLAT_EXE   = split /=/, $line if ( $line =~ /\bBLAT_EXE\b/ );
    @MAIL_SRV   = split /=/, $line if ( $line =~ /\bMAIL_SRV\b/ );
    @LOG_DIR    = split /=/, $line if ( $line =~ /\bLOG_DIR\b/ );
    @MAIL_LIST  = split /=/, $line if ( $line =~ /\bMAIL_LIST\b/ );
```



```

}
close ENVFILE;

#####
##
# Main
#####
##
my ($eventName) = shift;
my ($source) = shift;

#####
##
# Get mail information
#####
##
$mailto = getValue(@MAIL_LIST[1], $eventName);
$mailfrom = "staff.alarm@alarm_test.com";

if ( $mailto eq "" ) {
    $mailto = "staff.alarm@alarm_test.com";
}

if ( $eventName =~ /\bCisco_Link_Down\b/ || $eventName =~
\bSNMP_Link_Down_SSLVPN\b/ ) {
    $ifIndex = @ARGV[0];
    $ifName = ifAttr($source, "ifName", $ifIndex);
    $ifAlias = ifAttr($source, "ifAlias", $ifIndex);
    $mailsub = "NNM: $now, $source interface $ifName is down, description is
    $ifAlias";
    $mailmsg = "NNM: $now, $source interface $ifName is down, description is
    $ifAlias";
    $smstext = "NNM: $now, description is $ifAlias";
    $alcsmsg = "$source interface $ifName is down, description is $ifAlias";
    sendMail($mailto, $mailfrom, $mailsub, $mailmsg);
    sendsms($smstext);
    sendalcs($alcsmsg, "CiscoLNKDOWN", $ifAlias);
} elsif ( $eventName =~ /\bCisco_Link_Up\b/ || $eventName =~

```

```

/\bSNMP_Link_Up_SSLVPN\b/ ) {
    $ifIndex = @ARGV[0];
    $ifName = ifAttr($source, "ifName", $ifIndex);
    $ifAlias = ifAttr($source, "ifAlias", $ifIndex);
    $mailsub = "NNM: $now, $source interface $ifName is up, description is
$ifAlias";
    $mailmsg = "NNM: $now, $source interface $ifName is up, description is
$ifAlias";
    $smstext = "NNM: $now, description is $ifAlias";
    $alcsmsg = "$source interface $ifName is up, description is $ifAlias";
    sendMail($mailto, $mailfrom, $mailsub, $mailmsg);
    sendsms($smstext);
    sendalcs($alcsmsg, "CiscoLNKUP", $ifAlias);
} elsif ( $eventName =~ /\bOV_Message\b/ ) {
    $mailsub = "NNM: $now, HP Systems Insight Manager Event Alert: @ARGV[1],
ID: @ARGV[0]";
    $mailmsg = @ARGV[2];
    sendMail($mailto, $mailfrom, $mailsub, $mailmsg);
} elsif ( $eventName =~ /\bOV_Duplicate_IP_addr\b/ ) {
    $mailsub = "NNM: $now, node @ARGV[0] and @ARGV[2] have Duplicate IP
address.";
    $mailmsg = "Duplicate IP address: node @ARGV[0] reported having @ARGV[1],
but this address was previously detected on node @ARGV[2].";
    sendMail($mailto, $mailfrom, $mailsub, $mailmsg);
} else {
    $mailsub = "NNM: $now, $source @ARGV[0]";
    $mailmsg = "NNM: $now, $source @ARGV[0]";
    sendMail($mailto, $mailfrom, $mailsub, $mailmsg);
    sendsms($mailmsg);
}

#print "Script is done.\n";
close LOGFILE;

exit 0;

## All sub

```

```

#####
##
# trim space
#####
##
sub trim {
    #my $out = $_[0];
my $out = shift;
    $out =~ s/^\s+//;    # trim left
    $out =~ s/\s+$//;    # trim right
    return $out;
}

#####
##
# Get interface attributes
# Usage: ifAttr(source nodename, attribute name, interface index)
# Example: ifAttr("xxx", "ifName", 1)
#           return -> Fa0/1
#####
##
sub ifAttr {
    my ($srcnode, $attr, $ifIndex) = @_;
    chomp(my $tmp = `snmpget -c alarm_test $srcnode $attr.$ifIndex`);
    @src = split /:/, $tmp;
    return trim(@src[2]);
}

#####
##
# Get value from file
# Usage: getValue(file name, attribute name)
# Example: getValue("maillist.txt", "OV_IF_Down")
# Mail List Format: OV_IF_Down=receiver1@domain,receiver2@domain
#####
##
sub getValue {

```

```

my ($cfgfile, $cfgname) = @_;
$match_found = 0;
open CFGFILE, "< $cfgfile" or die "Couldn't open $cfgfile for reading: $!\n";
while (defined ($line = <CFGFILE>) && $match_found == 0) {
    if ($line =~ /\b$cfgname\b/) {
        chomp $line;
        @tmp = split /=/, $line;
        $match_found = 1;
        $ss = @tmp[1];
    }
}
close CFGFILE;
return $ss;
}

#####
##
# Get real message from message format file
# Usage: getMsg(message name,message array)
# Example: getMsg("OV_IF_Down", @array)
# Message Template: OV_IF_Down=$arg1$ interface $arg2$ is down, description
# is $arg3$
#####
##
sub getMsg {
my ($msgkey, @msgarr) = @_;
    @arr = split /\$/, getValue(@MSG_FILE[1], $msgkey, "=");
    $out = "";
    for ($i=0; $i<=$#arr; $i++) {
        if ($i%2 == 0) {
            $out = "$out@arr[$i]";
        }
        else {
            $out = "$out@msgarr[$i/2]";
        }
    }
}
return $out;
}

```

```

#####
##
# Send mail by blat.exe
# Usage: sendMail(to, from, subject, message body)
#####
##
sub sendMail {
    my ($to, $from, $sub, $body) = @_;
    $args = "- -to \"$to\" -f \"$from\" -server @MAIL_SRV[1] -subject \"$sub\" -body
    \"$body\"";
    system(@BLAT_EXE[1], $args);
    #print "@BLAT_EXE[1] $args\n";
    writeLog("sendMail - $body");
}

#####
##
# Send sms
# Usage: sendsms(sms text)
#####
##
sub sendsms {
    my ($sms) = shift;
    $cmd = "@TIBCO_BIN[1]/tibrvsend.exe \"NNM.ALM\" \"$sms\"";
    system($cmd);
    writeLog("NNM.ALM - $sms");
    #print "$cmd \n";
}

#####
### Send alcs
# Usage: sendalcs(text, alarmid, eqpid)
#####
##
sub sendalcs {
    my ($alarmText, $alarmId, $eqpId) = @_;
    $alcs = "sysid=\"NNM\" timestamp=\"$now\" alarmText=\"$alarmText\"

```

```

alarmId="\$alarmId\"   eqpId="\$eqpId\" ";
$cmd = "@TIBCO_BIN[1]/tibrvsend.exe \"alarm_test.T1.PROD.ALCS.NNM\"
\"$alcs\"";
system($cmd);
writeLog("alarm_test.T1.PROD.ALCS.NNM - $alarmText");
#print "$cmd \n";
}

```

```
#####
```

```
##
```

```

# Write log
# Usage: writeLog(message text)
#####

```

```
##
```

```

sub writeLog {
my ($log_msg) = shift;
$logfile = "@LOG_DIR[1]/$tod.log";
open LOGFILE, ">> $logfile" or die "Couldn't open $logfile for writing: $!\n";
$sold_fh = select(LOGFILE); # switch to LOGFILE for output
print "$now\t$log_msg\n";
select($old_fh); # return to original output
close LOGFILE;
}

```

Appendix B

There are some sequential attribute variables binding to an SNMP trap. Herein, the following \$ variables are used to access the sequential attributes that were received with the event. Each event has attributes associated with it (possibly none). They are accessed using the \$n notation, where n is the positional attribute, with 1 being the first possible attribute. The printing format is based on the ASN.1 type of the attribute. These attributes are equivalent to the variable bindings in an SNMP trap. Below table lists its related arguments.

\$[arg]

argument	description
\$#	Print the number of attributes in the event
\$*	Print all the attributes as [seq] name (type): value strings, where seq is the attribute sequence number
\$n	Print the nth attribute as a value string
\$-n	Print the nth attribute as a name (type): value string
\$+n	Print the nth attribute as a name: value string
\$>n	Print all attributes greater than n as value strings; useful for printing a variable number of arguments
\$>0	is equivalent to \$* without sequence numbers, names, or types
\$>-n	Print all attributes greater than n

	as [seq] name (type): value strings
\$>+n	Print all variables greater than n as name: value strings

