INTELLIGENT REQUEST TRACKING AND NETWORK MONITORING SYSTEM

MUHAMMAD INAYATULLAH BABAR[1], SYED WAQAR SHAH[1], SAHAR NOOR[2], RAFIULLAH KHAN[1], RIFAQAT ZAHEER[1], MUHAMMAD AKMAL[1] and MUHAMMAD ALI RAZA[1]

[1] *Department of Electrical Engineering, University of Engineering & Technology, Peshawar – Pakistan.*
[2] *Department of Mechanical Engineering, University of Engineering & Technology, Peshawar – Pakistan.*

ABSTRACT

This paper is about efficient and effective monitoring of the network switches of an organization such that as soon as problem arises to any of the switch, the ticketing system will automatically send email or SMS to the responsible person specifying the problem and the specific switch that has got the problem. If the administrator is busy or does not resolve the problem within an hour, the same ticket will be sent to 2nd responsible person based upon priority. So this system is an automatic network monitoring and reporting back system rather than manually monitoring all the switches thus reducing human labor and time in monitoring all switches of a huge network. Request Tracker (RT) software is heavily used worldwide and can be configured and customized to any location and is capable of handling large-scale operations. RT has essential functionality like it provides several interfaces (Web, CLI, e-mail, etc.), multiuser, different levels(admin, general user, queues etc), authentication and authorization, event history, handles dependencies, notifications.RT ticketing system can be configured according to the requirements in Linux environment and can be interfaced with another software called Nagios. Nagios can be programmed to build the network topology and applying different services on switches that are to be monitored.Nagios monitors the network and send notifications when any of the switch goes down. Such notifications will generate tickets in RT which will be sent via email to the network administrator.

Key Words: **Network Monitoring, Nagios, Network Switches, Reporting Back System, Request Tracker**

Citation: Babar, M.I., S.W. Shah, S. Noor, R.U. Khan, R. Zaheer, M. Akmal and M.A. Raza. 2013. Intelligent request tracking and network monitoring system. Sarhad J. Agric. 29(1):151-162.

INTRODUCTION

This paper is designed to give some insight into the procedures used to implement the intelligent RT ticketing system for network monitoring. This ticketing system is intelligent in a sense that it can specify which switch has got the problem, where the problem has occurred in the topology and what will be the effects on other switches e.g., if a parent switch is damaged or stopped functioning then all of its child switches will become unreachable and email will be sent only for the parent switch.Large organizations network usually consists of a large number of switches, so the task to manually monitor all of the network switches of such a huge network is inefficient and very time consuming. An automatic network monitoring and reporting back system helps the responsible person to quickly find the switch that has got problem and stop functioning due to any reason.

The ticketing system has great importance for an organization. Now the question arises why the ticketing system is an important for an organization, (organization may be of anything). In an organization, people have a lot of work to perform, salesmen in organization needs to sell the stuff, clients must be satisfied and employees are needed to provide services to the clients. Software or hardware problems need to be detected, fixed and everyone in organization must be informed that the problem has been fixed. Useless stuff needs to be disposedoff. At the end the responsible person have to know who needed what, the person who did it, when it completed and what extra need to be done, that's why ticketing system is important. Ticket is a piece of information or request that is to be tracked by ticketing system, when something new comes in organization, a ticket will be assigned with an id number specifying that exact thing.

The following parts when combined, form a true general ticketing system. These are the backbones of a general ticketing system:

i. Register an event or a ticket
ii. Assign an owner, or person responsible, to the ticket
iii. Assign additional interested parties to the ticket
iv. Track changes to the ticket
v. Inform interested parties of these changes

vi. Launch activity based on ticket status and/or priority
vii. Report on status of one or more ticket(s)—an overview
viii. Finish with, or close, the ticket

A ticketing system has many users in many different situations e.g. a few of them are listed below.

i. Network Security
ii. Engineering (Bug Tracking)
iii. Customer Service
iv. Sales Lead Tracking

MATERIALS AND METHODS

RT Ticketing System

RT (Request Tracker) is an open source, enterprise-grade ticketing system.It's function, at a most basic level, is to keep track of tickets, each of which represents a task to be completed, a conversation to be held, or a similar 'trackable'items. RT has many advantages over the other ticketing systems, most notably its open architecture and email friendly interface. RT is developed by Best Practical, Inc. New York University currently has a "bronze" support contract with best practical, allowing for a set of amount of questions to be asked per year.RT was first released by Jesse Vincent, in 1996.To distribute, develop and support the package Jesse Vincent created Best Practical Solution LLC.RT main display page is shown in Fig.1.

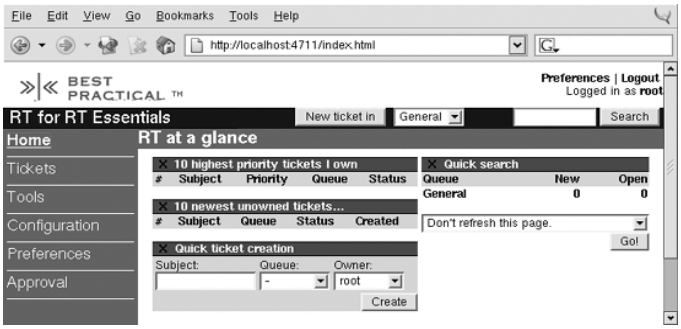

Fig.1. RT home page

Some important features of a true ticketing system are

i. Accessibility
ii. Ease of use
iii. Multiuser
iv. Ability to track history
v. Immutable history
vi. Flexible views
vii. Access control
viii. Dependency management
ix. Notifications
x. Customizable workflow

RT is designed not only to handle all the scenarios explored above, but its adoptability makes it friendlier for the beginners.RT can be installed on different operating systems like various distribution of Linux, Unix and window etc.RT uses several databases such as MYSQL, ORACLE and POSTGRESQL etc. Finally RT uses a language called Perl which is used for customization of RT.RT exists with the support of users and developers community having active mail lists. Because it is open source software, so everyone can modify it according to its own requirement.

RT software is a distribution under the GNU General Public License. RT is developed in Perl language and it is supported by Apache web server and MYSQL,ORACLE etc databases are used to store its data.Named user can access it through web based interface while public users can access it through guest login. But mostly email is preferred as the primary interface for public users.The email interface provides support for email auto-responses,attachments and customization of the subject name. RT uses a back-end database, a perl-based main engine, and front-end web and mail

interfaces. Aliases are used for all interaction with RT that is used to pipe with a perl program so therefore any Mail Transfer Agent "MTA" is used for mail gateway.

RT INSTALLATION REQUIREMENTS

Best practical does not explicitly list hardware requirements for RT. However, since it is database driven application, it is logical to assume that greater the amount of RAM and CPU available to RT, the smoother it will run. But it has a number of software dependencies. RT requires the following main dependencies (which have further dependencies) to be installed before RT installation.

i. Perl 5.8.3 or Later.
ii. RT is all about its Database. Several Databases are available e.g. MySQL 4.0.14 or later, PostgreSQL 7.2 or later, Oracle 9iR2 or later, SQLite etc. RT runs equally well on MySQL and PostgreSQL. Oracle support is relatively new, but it should be as stable as the MySQL and PostgreSQL.MySQL is the easiest supported database to set up and maintain therefore is more preferred than any other database.
iii. A Web Server. Apache 2.x with mod_perl 2.x or Apache 1.x or 2.x with the FastCGI module.

RT makes heavy use of freely available Perl libraries available on the CPAN. To make the installation process somewhat smoother, Best Practical has created a (mostly) automated procedure using the CPAN.pm module to download and install libraries from CPAN. RT can be installed on Windows environment (but not used for production purpose), Ubuntu, Redhat, and Fedora. Ubuntu and Fedora have packages that make installation a bit easier. Before configuring RT via the web interface, it is necessary to understand the following basic concepts:

i. User - A person who has an RT account and password. Rights can be granted to users on a global or per-queue basis.
ii. Groups - A collection of Users. Rights can be granted to groups on a global or per-queue basis.
iii. Rights - The abilities granted to users and/or groups on a global or queue basis. RT provides many different types of rights.
iv. Queue - The central administrative domain of RT. The queue is the organizational container of a collection of tickets waiting to be worked on. Queues often correspond to groups of services, groups of machines, or organizational units. The creation and naming of queues will depend on how the organization splits its work flow.
v. Ticket - The central object in RT. Each ticket defines a task to do or a problem to solve. One ticket is opened for each issue, regardless of how many notes or interactions happen with users about said issue. A ticket includes associated metadata such as an owner, watchers, status, and queue.
vi. Ticket Watcher - Someone interested in keeping track of the ticket. The owner and requestor(s) of the ticket automatically become watcher. The additional watcher categories are Cc (The person or people who receive copies of any replies that go to the requestor. Someone on the Cc list sees email but may not have permission to modify the ticket) and AdminCc(that also gets copies of comments and are usually permitted to modify the ticket).
vii. Time worked - The amount of time spent on the ticket.
viii. Time left - The amount of time left to work on the ticket.
ix. Ticket priority - The importance of a ticket, represented as a numerical scale from 0-99, with 99 being the highest priority. The initial and final ticket priorities should follow a predetermined company-wide standard. By setting a final priority, RT makes a ticket's priority increase or decrease as its due date draws closer.
x. Scrips– Triggers, that take a specified action automatically in response to a given condition. As with templates, scrips can be created and applied on a global or queue basis. Custom scripts can be formed after installation like templates. A number of default scrips are available in fresh installed RT.

RT Installation Procedure

RT can be installed on any Linux distribution e.g. Red Hat, Fedora, Ubuntu etc. Ubuntu is preferred because it provides automatic installation of many of the RT dependencies. RT installation procedure on Ubuntu 8 is given below:

```
#apt-get update
# apt-get install rt3.6-apache2
# apt-get install request-tracker3.6 rt3.6-clients
# apt-get install apache2-doc postfix mysql-server \
lynx  libdbd-pg-perl
```

While configuring mysql server it will prompt to enter new password for mysql "root" user. Enter password

(e.g.“innovation”) and press enter. Again enter the password (“innovation”) and press enter.

During Postfix configuration installation will prompt and provide the following options with details.

i. No configuration
ii. Internet sites
iii. Internet with smarthost
iv. Satellite system
v. Local Only

Select any option according to organization requirements. e.g. select “ Internet Sites ”.Again During Postfix configuration it prompt to enter System mail name.System mail name also known as fully qualified domain name, provides the global access. It is a fully qualified Domain Name. Fully Qualified Domain Name provides the global access. For testing purposes if RT is installed on the same machine as administrator PC, it can be selected as “localhost".

Duringconfiguring request tracker installation will prompt to enter $rtname. It is the RT instance name. Enter suitable name “RT.Hostname” as name for this RT instance.

Then the installation will prompt for “Handle RT_siteconfig.pm Permissions?” Two options (YES and NO) are available.Select “YES” option. Finally enter the choice for “Configure database for request tracker 3.6 with dbconfig-common?”.Select “YES” option for ease.

```
 # apt-get installlibapache-dbi-perl
# cp /etc/request-tracker3.6/RT_SiteConfig.pm \
     /etc/request-tracker3.6/RT_SiteConfig.pm.orig
# vi /etc/request-tracker3.6/RT_SiteConfig.pm
```

Compare the lines in the file with what is shown below. Remember to remove any leading'#' on a line to uncomment the line. Make the changes that are suggested. A number of these items will likely already be correctly set.

Hostname = machine's hostname like "pc1", "pc2", etc.
FQDN=FullyQualified Domain Name like" nwfpuet.edu.pk" or “localhost”

```
Set($rtname, 'RT.Hostname');
Set($Organization, 'RT.Hostname.FQDN’);

Set($CorrespondAddress , rt@Hostname.FQDN);
Set($CommentAddress , rt-comment@Hostname.FQDN);

# THE WEBSERVER:

Set($WebPath , "/rt");
Set($WebBaseURL , "http://Hostname.FQDN/rt");

Set($DatabaseType, $typemap{mysql} || "UNKNOWN");

Set($DatabaseHost, 'localhost');
Set($DatabasePort, '');

Set($DatabaseUser , 'root');
Set($DatabasePassword , 'root password');

Set ($DatabaseName, '/rtdb') if "mysql" eq "sqlite3";
Set ($DatabaseName, 'rtdb');
```

Save the file and exit. Now do the following:

```
# rt-setup-database-3.6 --action init --dba root --dba-password 'Enter-Password'
# cd /etc/apache2/sites-available/
# vi default
```

In the file add the line:

Include "/etc/request-tracker3.6/apache2-modperl2.conf"

Just before the </VirtualHost> directive near the end of the file works fine.Saveand exit from the file.

Now it is important to verify that two Apache modules are enabled.

```
# a2enmod perl
# a2enmod rewrite
# /etc/init.d/apache2 restart
# a2enmod rewrite
```

Now install Request Tracker FAQ Manager module for Request Tracker

```
# apt-get install rt3.6-rtfm
```

Choose "Allow" when asked for "Permission to modify the Request Tracker database: Options provide are 1.allow 2.prompt 3. deny

Restart Apache to be sure that all changes are noted.

```
# /etc/init.d/apache2 restart
```

RT is now installed successfully. In the web browser go to:

http://Hostname.FQDN/rt

Log in as user id "root" with password of "password". (Fig.2) Change the root password in the preferences link and start using Request Tracker.

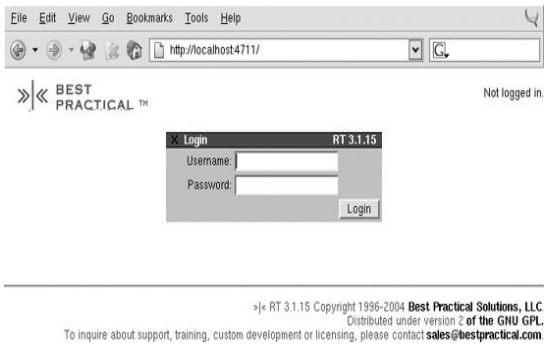

Fig. 2. RT login box

NAGIOS Monitoring System

Nagios is a web based,open source software used for system and network monitoring application.It observes services and hosts and informing network administrator when some change occur in the network. Basically Nagios is designed for working under linux environment but it also run under other platforms as well.Nagios is relative scalable, manageable and secure. Nagios powerful features are availability of its Best documentation, Good log and database system, Nice, informative and attractive web interface, Very flexible, Automatic alerts sending if condition changes, Various notification options (Email, pager, mobile phoneetc). Check on host and services are carried out by Nagios Monitoring daemon with external "plugins" to provide the complete status of the network.

When the problems occurred in the network,Nagios daemon will send message to the network administrator in different forms such as email,sms,instant message etc.Web interface of Nagios provides information about the current status,history and reports.Nagios software is distributed under the GNU General Public License.Various services like HTTP,SMTP,NNTP,POP3 and Ping etc.Also host resources like CPU load,disk and memory usage can be monitored using Nagios.Nagios Plug-in design facilitates users to create their services and hosts checks.Nagios can be used to build the complete network topology so child parent relationship exist between network nodes. Parent host in Nagios also has the ability to find and differentiate the down and unreachable host.Nagios host status details screen is shown in Fig.3

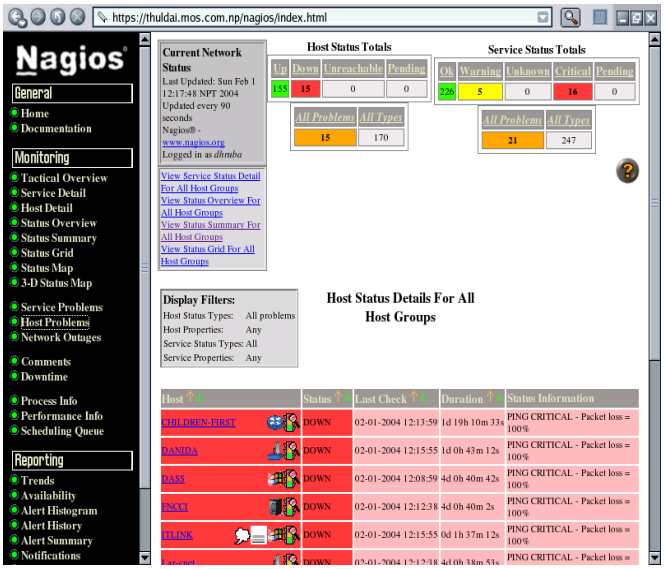

Fig.3. Nagios host status details screen

In order to run Nagios, TCP/IP should be configured as most service checks will be performed over the network and it also required a machine running Linux (or UNIX variant) and a C compiler.

The present condition of host and services is decided by two factors.The status of host and service (i.eUP,DOWN,CRITICAL,UNREACHABLE,etc) and the type of state(i.e SOFT STATE AND HARD STATE). State types play an important role in monitoring and alerting process. They specify the execution of event handlers and timings of sent out notification.

i. Service and Host Check Retries- In order to prevent false alarms, Nagios allows to define how many times a service or host check will be retried before the service or host is considered to have a real problem. The maximum number of retries before a service or host check is considered to have a real problem is controlled by the <max_check_attempts> option in the service and host definitions, respectively. Depending on what attempt a service or host check is currently on determines what type of state it is in.

ii. Soft States- Soft states occur for services and hosts when a service or host check results in a non-OK state and it has not yet been (re)checked the number of times specified by the <max_check_attempts> option in the service or host definition. This is called a soft error state...When a service or host recovers from a soft error state. This is considered to be a soft recovery.The soft error or recovery is logged if log_service_retries or log_host_retries options are enabled in the main configuration file.

iii. Hard States- Hard states occur for services when a service check results in a non-OK state and it has been (re)checked the number of times specified by the <max_check_attempts> option in the service definition. This is a hard error state.When a service recovers from a hard error state. This is considered to be a hard recovery.When a service check results in a non-OK state and its corresponding host is either DOWN or UNREACHABLE.

iv. Hard State Changes- Hard state changes occur when a service or host...
   a. Changes from a hard OK state to a hard non-OK state
   b. Changes from a hard non-OK state to a hard OK- state

c. Changes from a hard non-OK state of some kind to a hard non-OK state of another kind (i.e. from a hard WARNING state to a hard UNKNOWN state)

v. Hard State Events- If a hard state change has occurred and the service or host is in a non-OK state then the hard service or host problem is logged and Event handlers are executed to handle the hard problem for the service or host. Contacts will be notified of the service or host problem (if the notification logic allows it).But if a hard state change has occurred and the service or host is in an OK state then the hard service or host recovery is logged and Event handlers are executed to handle the hard recovery for the service or host. Contacts will be notified of the service or host recovery. And if a hard state change has NOT occurred and the service or host is in a non-OK state then contacts will be re-notified of the service or host problem. Ifa hard state change has NOT occurred and the service or host is in an OK state nothing happens. This is because the service or host is in an OK state and was the last time it was checked as well.

RESULTS AND DISCUSSION

NAGIOS CONFIGURATION

According to the network, define all of the hosts or switches in the /etc/nagios3/conf.d/ directory.Keep the file name for each host same as the hostname in the file. Sample entry is shown below:

cd /etc/nagios3/conf.d/

Now define the switch with name switch1.cfg

viswitch1.cfg

define host {
use generic-host
host_nameswitch1
alias switch1 of the network
address_____ [switch1 IP address here]
parents switch1's parent name here

}

Save and quit. Similarly define all of the switches and build a complete network topology. Sample topology in nagios is shown in Fig.4

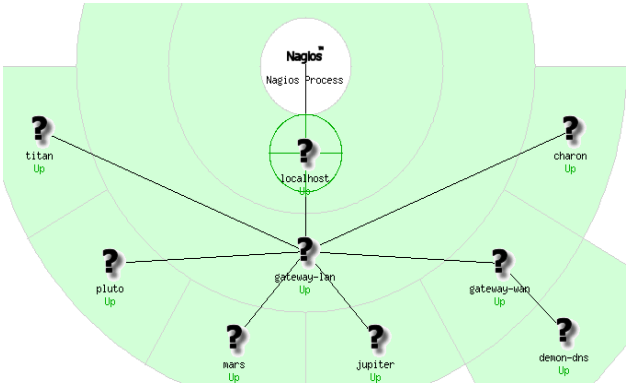

Fig.4. Status map of a network in Nagios

Now make a new group with the name of hostgroup and include the defined host into it.Modifyhostgroups_nagios2.cfg file and insert a new group:

edit hostgroups_nagios2.cfg

```
definehostgroup {
hostgroup_name  servers
alias           organization switches
members         switch1
}
```

Associate some services to that host

```
# cd  /etc/nagios3/conf.d/
# vi services_nagios2.cfg
```

Locate the portion called "check that ssh services are running",and modify the text:

```
hostgroup_namessh-servers
to
hostgroup_namessh-servers, servers
```

Make sure that the configured file is correct

```
# nagios3 -v /etc/nagios3/nagios.cfg
```

It should return zero warnings and errors.

Now Restart Nagios

```
# /etc/init.d/nagios3 restart
```

In order to check the ping service, edit the file as

```
# vi services_nagios2.cfg

# check that ping-only hosts are up

define service {
hostgroup_name                ping-servers,servers
service_description           PING
check_command       check_ping!100.0,20%!500.0,60%
use                           generic-service
notification_interval0 ; set > 0 ifre-notification is
                                        required
}
```

Change the contents of the file contacts_nagios.cfg with

```
# contacts.cfg

define contact{
   contact_name                    rt
   alias                           rt
   service_notification_period     24x7
   host_notification_period        24x7
   service_notification_options      w,u,c,r
   host_notification_options       d,r
   service_notification_commands  notify-service-                    by-email
```

```
host_notification_commands      notify-host-by-                                    email
emailrt@Hostname.FQDN

}

define contact{
contact_name            root
alias                   Root
service_notification_period     24x7
host_notification_period        24x7
service_notification_options        w,u,c,r
host_notification_options       d,r
service_notification_commands   notify-service-                                by-email
host_notification_commands      notify-host-by-                                    email
email                   root@localhost
}


define contact{
contact_name                Admin-name
alias                   Admin.name
service_notification_period     24x7
host_notification_period        24x7
service_notification_options    w,u,c,r
host_notification_options       d,r
service_notification_commands   notify-service-                                by-email
host_notification_commands      notify-host-by-                                email
email                       Admin-email-add
}
```

CONTACT GROUPS

```
 definecontactgroup{
contactgroup_name  admins
alias         Nagios, Administrators
members       root,Admin-name,rt
 }
```

The file "/etc/nagios3/conf.d/services_nagios2.cfg"include information about the service check running on each group(not individual devices)The simpler example is shown below:

```
# check that ping-only hosts are up
   define service {
hostgroup_name              ping-servers,servers
service_description         PING
check_commandcheck_ping!100.0,20%!500.0,60%
use                         generic-service
notification_interval0 ; set > 0 if  to be   renotified
}
```

The file "/etc/nagios3/conf.d/extinfo_nagios2.cfg" determine information about each device in each define group.For example:

```
#vi extinfo_nagios2.cfg
# Extended Host and Service Information

      definehostextinfo {
```

```
hostgroup_name      servers
icon_image          base/ubuntu.png
icon_image_alt          Debian GNU/Linux
        vrml_image          ubuntu.png
statusmap_image     base/ubuntu.gd2
notes_url           http://Hostname.FQDN/rt
        }
```

In order to ensure that the host is added ,use the web interface (http://localhost/nagios3)

Go to the file command.cfg by
#vi /etc/nagios3/commands.cfg

Changethe following two commands with:

service_notification_commands withnotify-service-by-email

host_notification_commandswith notify-host-by-email

Now ensure that the configuration is correct:

```
 # nagios3 -v /etc/nagios3/nagios.cfg
```

The following should return zero warnings and errors.

Now Restart Nagios
/etc/init.d/nagios3 restart

Cisco Switch Configuration

Since Nagios is used to monitor different services and Hosts so switches in the network should be configurable and different services should be applied on them e.g. PING, SSH etc. In order to configure the switch take the following steps

i. First connect the one end of console wire to the switch and the other end with the serial port of PC.
ii. Turn on the switch.
iii. Open hyper terminal in the PC using the link start/all programme/accessories/communications/Hyperterminal
iv. Give name for the project after clicking on the terminal
v. Select No for automatic initial configuration.
vi. Write ‘enable’ in the hyperterminal page
vii. Write ‘config t’
viii. Then interface fastethernet 0/1
ix. Press enter
x. Then no shut
xi. Press Enter
xii. Then, press ctrl z on the keyboard to come out from enable mode.Then, write memory

The above procedure is used to configure one port (0/1 , means port number one), it should be repeated 24 times for configuring 24 ports in the switch (by writing interface fastethernet 0/2 , 0/3 ,0/4,……..); but there is an easy way in which all the ports can be configured by a single command ,for that just make a little change in step of “ interface fastethernet 0/1” as follows;
interface range fastethernet 0/1 – 24.

There are various switch configuration modes e.g. user mode, privileged mode,interfaceand global configuration mode. User enter into privileged mode by using "enter" command.The sign of privileged mod is "#".The list of privileged mode command is determined by using "?" command."Disable" command isused to go back from privileged mode user mode. The sign of user mode is ">".To configure aswitch,first enter into privileged mode and then enter to global configuration mode. Now assign nameto switch.

```
> enable
# configure terminal
(config)# hostname SWITCH
Use exit or ctrl-z to get out of configuration mode.
SWITCH (config)# exit
SWITCH #
On switch type 'show running-config' to see the active configuration.
SWITCH #show running-config
```

Assign the TCP/IP protocol configuration to the switch e.g. Assigning an IP address of 172.16.1.72 with a subnet mask of 255.255.0.0 and default gateway of 172.16.1.1 takes the following steps:

i. > enable
ii. # configure terminal
iii. (config)# hostname SWITCH
iv. SWITCH (config)# enable password cisco
v. SWITCH (config)# interface vlan1
vi. SWITCH (config-if)# ip address 172.16.1.72 255.255.0.0
vii. SWITCH (config-if)# no shutdown
viii. SWITCH (config-if) # exit
ix. SWITCH (config) # ip default-gateway 172.16.1.1

On switch, issue the show interface vlan1 command to ensure that TCP/IP configuration are ok;

i. SWITCH # show interface vlan1
ii. SWITCH # show interfaces

To remove the switch IP address, use the command " noip address" command in interface configurationmode.Similarly in order to remove default gateway address,use the command "no ip default-gateway" in global configuration mode.

NAGIOS Interfacing with RT

In order to interface Nagios with RT,an alias is required using rt-mailgate program in order to provide interface between Nagios and RT.Alias is created in /ete/aliases such as:

```
# vi /etc/aliases
```

Insert the following text into the bottom of file:

rt: "|rt-mailgate --queue 'Queue name' --action correspond --urlhttp://Hostname.FQDN/rt"

rt-comment: "|rt-mailgate --queue 'Queue name' --action comment --url http://Hostname.FQDN/rt"

These lines provide information to the rt-mailgate to send all mails to root@localhostto the 'Queue name' account instead.

Save the configuration and quit the file Now usethe command:

```
# newaliases
```

Openthe RT instance.

```
http://Hostname.FQDN/rt
```

Now sign in as a "root" user.

Go to the link “Configuration”,”Queue”,New queue” in RT.Now create the Queue in RT with the same name as specified in /etc/aliases file.

Now assign required user right to the root user.For this go to link of “User Rights”.In order to make it simple, assign all the user rights to the root user. Similarly go to “Group Right”, assign all the group rights as well.In order to display a created Queue on the main page of RT,restart the RT software.

Now ticket is formed in RT when nagios generate an alert.Notice in thenagios file /etc/nagios3/conf.d/contacts_nagios3.cfg,the nagios send an alert when the host is in “down” or “d” state or when the service is in “critical” or “c” stateetc.In this file a line:

notification_interval 0

determine that Nagios will generate only one email per critical or down state.If this is other than zero then Nagios will send multiple email per state but it is good to use this equal to zero.Now check whether rt-Mail-gate(which is a part of rt3.6-clients) is functioning correctly. For this write the following command in the terminal

echo “testing rt” | mail -s 'testing rt- Mail-Gate' rt@Hostname.FQDN

then check RT software. It should generate ticket in RT with the subject “testing rt-Mail-Gate”.Now attempt to generate a ticket in RT,this is possible by generating Nagios alert through plugging out the network cable of a switch so that it appears to be down. The ticket in RT will then send email to all watchers of the specified queue in aliases file.

CONCLUSION AND RECOMENDATIONS

This paper presents an automatic network monitoring and reporting back system which is much more efficient than manual monitoring system. For networks consisting of a large number of switches, manual monitoring will be very time consuming, inefficient and difficult to find out exact location where problem exist. But in this automatic monitoring system, the administrator has to check only his emails. Whenever problem occurs anywhere in the network, email will be sent to administrator specifying the location of problem and also effects on other network switches e.g. some switches will become unreachable because they are the child switches of the problematic switch. An alternate option of informing the administration of the problem is the use of GSM module for sending SMS which further improves the efficiency as compared to emails.

REFERENCES

Schubert M., A. Hay, D. Bennett, J. Strand, J. Ginesl. 2008. Nagios3 Enterprise Network Monitoring: Designing Configurations for Large Organizations, Chap:2; pp.25-84

Chamberlain, D., R. Foley, D. Rolsky, R. Spier, J. Vincent. 2011. RT Essentials: Installation, Chap.2:pp. 9-18

Request Tracker Software, Available at http://bestpractical.com/rt/, Latest version of RT,

Nagios Software, Available at http://nagios.org/download

Nagios to Monitor Remote Linux Server, Available at http://www.kernelhardware.org/nagios-nrpe-to-monitor-remote-linux-server/Monitoring systems using Nagios,

Nagios Alerts via SMS, Available at http://barryodonovan.com/index.php/2007/05/19/nagios-sms-kapow

http://ubuntu.com/GetUbuntu/download/Cisco Switch configuration, lab_16_catalyst_2950_switch_configuration.pdf