An Efficient Network Monitoring Systems

The term „network monitoring" describes a system that continuously monitor the whole network topology for jamming, slowing down or failing components and notifies the network responsible person via email, sms or other alarms in case of any problem.

Large organizations always require fast and efficient network monitoring system which reports to the network administrator as soon as a network problem arises. This paper presents an effective and automatic network monitoring system that continuously monitor all the network switches and inform the administrator by email or SMS when any of the network switch goes down. This system also points out problem location in the network topology and its effect on the rest of the network. Such network monitoring system uses smart interaction of Request Tracker (RT) and Nagios software's in Linux environment. The network topology is built in Nagios which continuously monitor all of the network nodes based on the services defined for them. Nagios generates a notification as soon as a network node goes down and sends it to the RT software. This notification will generate a ticket in RT database with problematic node information and its effect on the rest of the network. The RT software is configured to send the ticket by email and SMS to the network administrator as soon as it is created. If the administrator is busy at the moment and does not resolve the ticket within an hour, the same ticket is automatically sent to the second network responsible person depending upon the priority defined. Thus, all persons in the priority list are informed one by one until the ticket is resolved.

An efficient and automatic network monitoring is always required for large organizations like universities, companies and other business sectors where the manual network monitoring is very difficult [1],[2]. Since large organizations have a big network topology, the manual network monitoring causes waste of time to point out problem location [3]. The Multi Router Traffic Grapher (MRTG) has been extensively used for network traffic load monitoring. MRTG generates graph for all the nodes of the network topology from which the traffic load information can be accessed [4]. It consists of perl script which uses simple network management protocol (SNMP). Manual monitoring of all nodes of a huge network with MRTG is inefficient and time consuming. The network monitoring scheme presented in this paper, make use of the smart interaction of Request Tracker (RT) and Nagios software to obtain an intelligent and automatic network monitoring system. This system is intelligent in a sense that it can specify the problem location in the network topology as well as its effect on the other nodes. If a parent node stops functioning then all the child nodes also become unreachable but problem notification of only parent node is sent to the administrator.

Thus, this efficient network monitoring and reporting back system quickly inform the administrator about the network problem location [5]. The role of network monitoring is performed by the nagios software [6]. The whole network topology is constructed in nagios [7]. The administrator apply different services on the network nodes that are to be monitored by nagios software. Nagios continuously monitors all network nodes and generate notification when a node goes down after making a pre-defined number of attempts [8],[9]. The key role in network management is performed by the RT software which manage the tickets generated by the nagios software. RT is heavily used worldwide and can be customized and configured according to the organization needs.

Network monitoring systems & tools

Three kinds of tools

1. Diagnostic tools – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools

2. Monitoring tools – tools running in the background (" daemons" or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.

3. Performance Tools

Key is to look at each router interface (probably don't need to look at switch ports).

Two common tools:

-Netflow

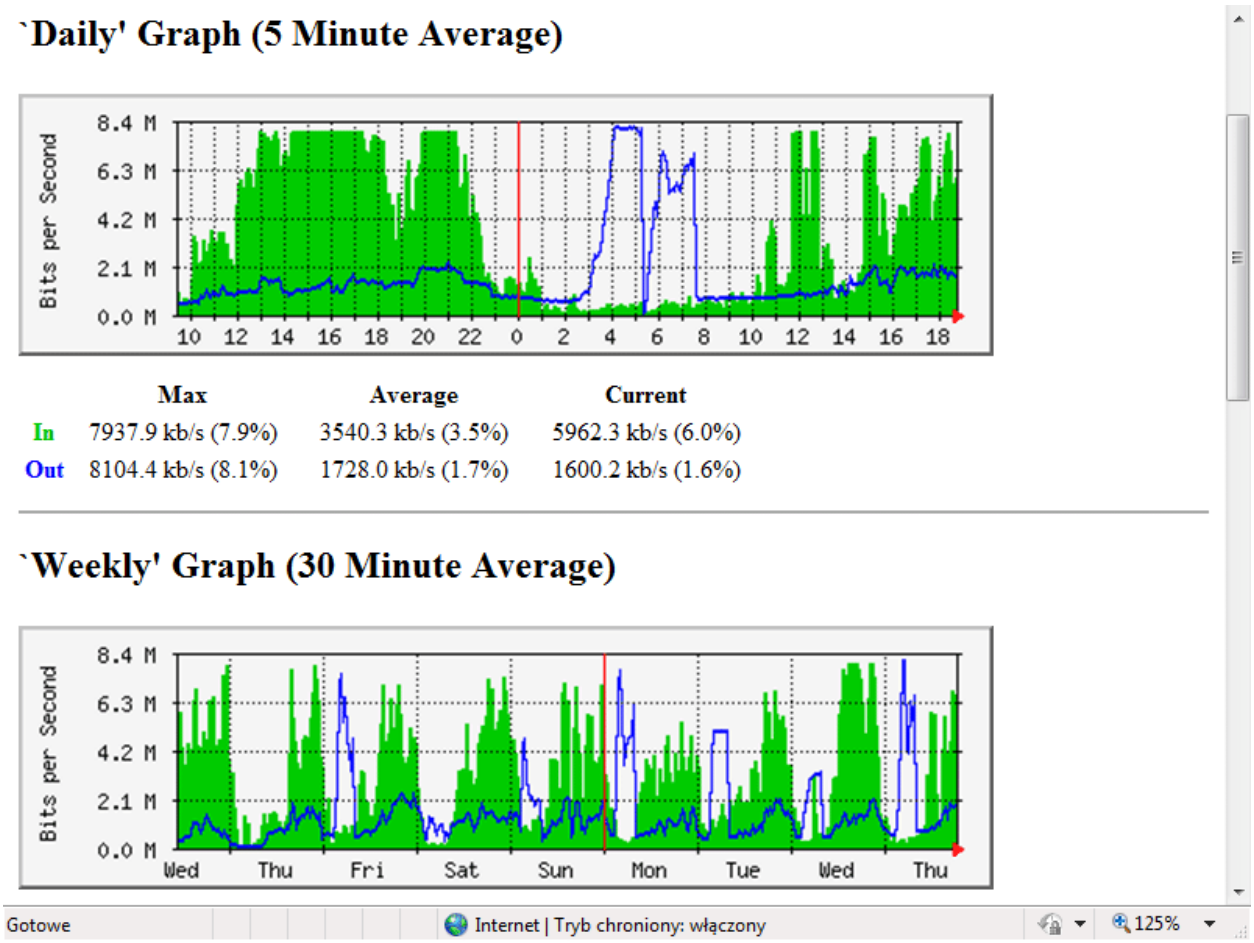
-MRTG (Multi Router Traffic Grapher)

What is NetFlow and how does it work?

NetFlow is a network protocol used to monitor the flow of traffic over the network. By analyzing NetFlow data, you can get a picture of how network traffic flows across your network, including source, destination, congestion points, and volume. Using a NetFlow monitoring solution can help you analyze flow records to understand and optimize traffic within the network, so you don't spend money on additional bandwidth that is not needed.

Multi Router Traffic Grapher **(MRTG)**

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic. These graphs are embedded into webpages which can be viewed from any modern Web-browser. In addition to a detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last five weeks and the last twelve months. This is possible because MRTG keeps a log of all the data it has pulled from the router. This log is automatically consolidated so that it does not grow over time, but still contains all the relevant data for all the traffic seen over the last two years. This is all performed in an efficient manner. Therefore you can monitor 200 or more network links from any halfway decent UNIX box



Active tools

- **Ping** – test connectivity to a host

- **Traceroute** – show path to a host

- **MTR** – combination of ping + traceroute

- **SNMP** collectors (polling)

Passive tools

- log monitoring, SNMP trap receivers, NetFlow

Automated tools

- **SmokePing** – SmokePing is a network latency monitoring tool that uses ICMP Echo requests (ping) and other types of probes to measure, record, and display network latency, packet loss, and other network performance metrics over time

- **MRTG/RRD** – record and graph bandwidth usage on a switch port or network link, at regular intervals.

Network & Service Monitoring tools

- **Nagios** – server and service monitor: Monitors network services and alerts you to issues before they become critical.

 Can monitor pretty much anything

 HTTP, SMTP, DNS, Disk space, CPU usage, ...

 Easy to write new plugins (extensions)

- Basic scripting skills are required to develop simple

monitoring jobs – Perl, Shell scripts, php, etc...

- Many good Open Source tools

 Zabbix, ZenOSS, Hyperic, OpenNMS ..

Automation Tools:

- **Ansible:** Automates configuration management, application deployment, and task execution across your network.
- **Puppet:** Manages and automates the configuration of your network services.
- **Chef:** Automates the management of infrastructure, including network devices.

Security Best Practices:

- **Regular Updates:** Keep network services and devices updated with the latest security patches.
- **Firewalls and Access Controls:** Implement firewalls and access controls to protect network services.
- **Monitoring and Alerts:** Set up monitoring and alerts for unusual activity that may indicate security issues.

Backup and Recovery:

- Regularly back up configuration files and important data.
- Have a disaster recovery plan in place to quickly restore services in case of failures.

Wireshark

Wireshark is one of the best open source network packet analyser that will try to capture network packets and tries to display that packet data as detailed as possible.

Some Intended Purposes

- Network administrators use it *to troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol internals*

Features

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs
- Import packets from text files containing hex dumps of packet data
- Display packets with very detailed protocol information
- Save packet data captured
- Export some or all packets in a number of capture file formats
- Filter packets on many criteria
- Search for packets on many criteria
- Colorize packet display based on filters
- Create various statistics

SNMP – Simple Network Management

Protocol

- Industry standard, hundreds of tools exist to exploit it

- Present on any decent network equipment

 Network throughput, errors, CPU load, temperature, ...

- UNIX and Windows implement this as well

 Disk space, running processes, ...

Suppose an organization runs an email service for its employees. Managing this network service would involve:

- **Configuration:** Setting up the email server with appropriate settings.
- **Monitoring:** Using tools like Nagios to monitor server uptime and email delivery rates.
- **Maintenance:** Regularly updating the email server software to protect against vulnerabilities.
- **Troubleshooting:** Diagnosing issues such as email delivery failures or server outages.
- **Security:** Implementing spam filters and security protocols to prevent unauthorized access.
- **Scaling:** Adding more resources as the number of users grows.
- **Backup:** Ensuring that email data is backed up regularly.
- **Documentation:** Keeping records of configurations, incidents, and maintenance activities.

Best Practices for Managing Network Services:

1. **Regular Updates:**
    - Keep all network services and associated software up-to-date with the latest patches and updates.
2. **Automation:**
    - Use automation tools to handle routine tasks, reducing the likelihood of human error and increasing efficiency.
3. **Proactive Monitoring:**

- Implement proactive monitoring to detect and resolve issues before they impact users.

4. **Redundancy and Failover:**
   - Set up redundant systems and failover mechanisms to ensure high availability and reliability.

Ticketing systems

Why are they important?

- Track all events, failures and issues Focal point for helpdesk communication Use it to track all communications

- Both internal and external Events originating from the outside:

- customer complaints

Events originating from the inside:

- System outages (direct or indirect)

- Planned maintenances or upgrades – Remember to

notify your customers!

Use ticket system to follow each case, including internal communication between technicians

 Each case is assigned a case number

 Each case goes through a similar life cycle:

- New

- Open

- ...

- Resolved

- Closed