ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Automatic Traffic Management and Congestion Avoidance

Hemlata[1]
Deptt. Of Comp. Sci. & Engg.
SKITM, (MD UNIVERSITY)
Bahadurgrh, India

V. K. Pandey[2]
Deptt. Of Comp. Sci. & Engg.
SKITM, (MD UNIVERSITY)
Bahadurgrh, India

Abstract: ***As company intranets continue to grow it is increasingly important that network Administrators are aware of and have a handle on the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic. This paper discusses monitoring, analysis of network traffic, congestion avoidance. It gives an overview of the monitoring, analysis techniques of network traffic, congestion avoidance techniques including the Qos, EEM scripting.***

Keywords: Network monitoring, network analysis, active monitoring, congestion avoidance, QOS, EEM Scripting, TCL.

I. INTRODUCTION

Network traffic can be defined in a number of ways. But in the simplest manner we can define it as the density of data present in any Network. In any computer Network, there are a lot of communication devices trying to access resources and at the same time getting requests to carry out some work for some other device .Also at the same time certain types of communication devices may be busy to respond to the request being made to them. So there is lot of information exchange in the Network in form of request, response and control data. This data is basically in the form of a huge number of packets floating around in the Network. This huge amount of data acts as a load on the Network, which results in slowing down the operations of other communication devices. Due to this there is a lot of delay in communication activities. This ultimately results in congestion of the Network.

Controlling network traffic requires limiting bandwidth to certain applications, guaranteeing minimum bandwidth to others, and marking traffic with high or low priorities. This exercise is called traffic management. In this research paper discuss overview of techniques used for monitoring, analysis network traffic and congestion avoidance techniques by using Qos, EEM Scripting and TCL.

II. DESCRIPTION OF NETWORK MONITORING AND ANALYSIS TECHNIQUES

1. Importance of Network Monitoring and Analysis

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised.

2. Monitoring and Analysis Techniques

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

Monitoring Techniques are used:-

Router Based Monitoring Techniques

Router Based Monitoring Techniques are hard-coded into the routers and therefore offer little flexibility. A brief explanation of the most commonly used monitoring techniques is given below. Each technique has undergone years of development to become a standardized model.

3. Simple Network Monitoring Protocol (SNMP) RFC 1157

SNMP is an application layer protocol that is part of the TCP/IP protocol suite. It allows Administrators to manage network performance, find and solve network problems, and plan for network growth. It gathers traffic statistics through passive sensors that are implemented from router to end host. While two versions exist, SNMPv1 and SNMPv2.

There are 3 key components to SNMP: Managed Devices, Agents, and Network Management Systems (NMSs).

The Managed Devices contain the SNMP Agent and can consist of routers, switches, hubs, pHs, printers, and items such as these. They are responsible for collecting information and making it available to the NMSs.

The Agents contain software that have knowledge of management information and translates this information into a form compatible with SNMP. They are located on a managed device.

The NMSs execute applications that monitor and control the managed devices. Processing and memory resources that are needed for network management are provided by the NMSs. A minimum of one NMS must exist on any managed network. SNMP can act solely as a NMS or an agent, or can perform the duties of both.

SNMP uses four protocol operations in order to operate: Get, Get Next, Set, and Trap.

4. .Remote Monitoring (RMON) RFC 1757

RMON [Cisco5506] enables various network monitors and console systems to exchange network-monitoring data. It is an extension of the SNMP Management Information Database (MIB). Unlike SNMP that must send out a request for information, RMON is able to set alarms that will monitor the network based on certain criteria. RMON allows Administrators to manage local networks as well as remote sites from one central location. It monitors at the Network Layer and below. RMON has 2 versions RMON and RMON2 this paper only deals with RMON. RMON2 allows for monitoring of packets on all network layers. It focuses on IP traffic and application level traffic.

RMON [RMON] uses 9 different monitoring groups to obtain information about the network.

Statistics - stats measured by the probe for each monitored interface on this device

History - records periodic statistical samples from a network and store for retrieval

Alarm - periodically takes statistic samples and compares them with a set of thresholds for event generation

Host - contains statistics associated with each host discovered on the network

Huston - prepares tables that describe top hosts

Filters - enable packets to be matched by a filter equation for capturing events

Packet capture - captures packets after they flow through the channel

Events - controls generation and notification of events from a device

Token ring - supports token ring

5. Non-Router Based Techniques

Although non-router based techniques are still limited in their abilities they do offer more flexibility than the router based techniques. These techniques are classified as either active or passive.

Active Monitoring

Active monitoring [Active06] transmits probes into the network to collect measurements between at least two endpoints in the network. Active measurement systems deal with metrics such as:

Availability

Routes

Packet Delay

Commonly used tools such as ping, which measures delay and loss of packets, and trace route which helps determine topology of the network, are examples of basic active measurement tools. They both send ICMP packets (probes) to a designated host and wait for the host to respond back to the sender. Figure 4 is an example of the ping command that uses active measurements by sending an Echo Request from the source host through the network to a specified destination. The destination then sends an Echo Response back to the source it received the request from.

Passive Monitoring

Passive monitoring unlike active monitoring does not inject traffic into the network or modify the traffic that is already on the network. Also unlike active monitoring, passive monitoring collects information about only one point in the network that is being measured rather than between two endpoints as active monitoring measures..

III. DESCRIPTION OF CONGESTION AVOIDANCE

What is Network Congestion

Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity. Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load. This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

Quality of Service

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by providing the following services:

» Supporting dedicated bandwidth

» Improving loss characteristics

» Avoiding and managing network congestion

» Shaping network traffic

» Setting traffic priorities across the network

In general, edge routers perform the following QoS functions:

» Packet classification

» Admission control

» Configuration management

In general, backbone routers perform the following QoS functions:

» Congestion management

» Congestion avoidance

IV. CONGESTION AVOIDANCE

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before it becomes a problem. These techniques are designed to provide preferential treatment for premium (priority) class traffic under congestion situations while concurrently maximizing network throughput and capacity utilization and minimizing packet loss and delay. WRED and DWRED are the Cisco IOS QoS congestion avoidance features.

WRED

WRED, the Cisco implementation of RED, combines the capabilities of the RED algorithm with IP Precedence to provide preferential traffic handling for higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service. WRED is also RSVP-aware. WRED is available on the Cisco 7200 series RSP.

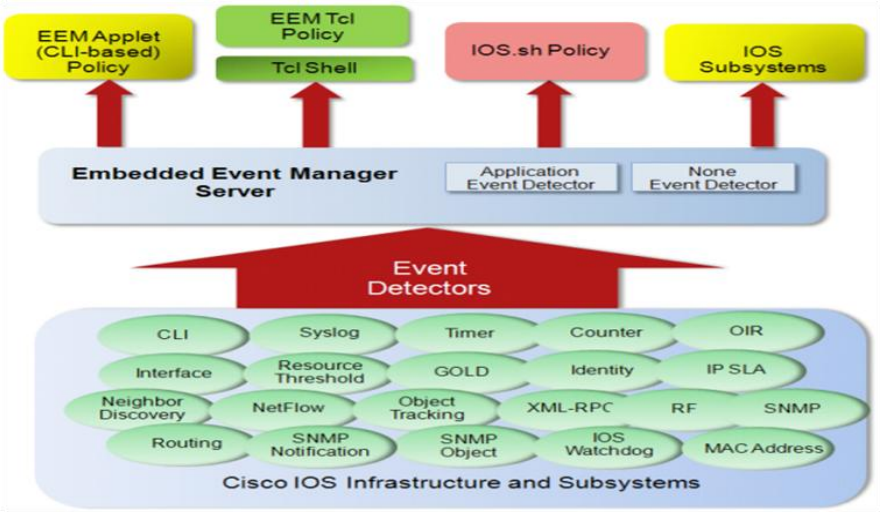
DWRED

DWRED is the Cisco high-speed version of WRED. The DWRED algorithm was designed with ISP providers in mind; it allows an ISP to define minimum and maximum queue depth thresholds and drop capabilities for each class of service.

DWRED, which is available on the Cisco 7500 series routers or the Cisco 7000 series router with RSPs is analogous in function to WRED, which is available on the Cisco 7200 series RSP.

V. EMBEDDED EVENT MANAGER (EEM)

The EEM(Embedded Event manager is a software component of Cisco IOS, XR, and NX-OS makes life easier for administrators by tracking and classifying events that take place on a router and providing notification options for those events. EEM allows you to automate tasks, perform minor enhancements and create workarounds EEM is a policy-driven process by means of which faults in the Cisco IOS software system are reported through a defined application programming interface (API). The EEM policy engine receives notifications when faults and other events occur. EEM policies implement recovery on the basis of the current state of the system and the actions specified in the policy for a given event.



There are two independent pieces: Applets and Scripting

» Applets are a collection of CLI commands

» Scripts are actions coded up in TCL(interpreter language)

EEM uses event detectors and actions to provide notifications of those events:

EEM detectors can be:

1) SNMP:-Monitoring SNMP objects.

2) Syslog:-Responds to various syslog messages, allowing for matching on regular expressions.

3) Counter: Monitoring and responding to interface counter when cross threshold settings.

4) CLI events: Screening CLI input for a regular expression match.

5) None: This event detector is use to test EEM script/applet using "event manager run" command.

6) Timers :(Countdown, watchdog and CRON)

7) IP SLA and Netflows events.

EEM Actions can be:

1)Sending a email messages

2)Executing a Cisco command.

3)Generating SNMP traps

4)Reloading the router

5)Generating priotized syslog messages

VI. EEM SCRIPT USING TOOL COMMAND LANGUAGE(TCL)

All Embedded Event Manager scripts are written in Tcl. Tcl is a string-based command language that is interpreted at run time. The version of Tcl supported is Tcl version 8.3.4 plus added script support. Scripts are defined using an ASCII editor on another device, not on the networking device. The script is then copied to the networking device and registered with EEM. Tcl scripts are supported by EEM. As an enforced rule, Embedded Event Manager policies are short-lived run time routines that

must be interpreted and executed in less than 20 seconds of elapsed time. If more than 20 seconds of elapsed time are required, the maxrun parameter may be specified in the event_register statement to specify any desired value.

EEM policies use the full range of the Tcl language's capabilities. However, Cisco provides enhancements to the Tcl language in the form of Tcl command extensions that facilitate the writing of EEM policies. EEM allows you to write and implement your own policies using Tcl. Writing an EEM script involves:

» Selecting the event Tcl command extension that establishes the criteria used to determine when the policy is run.

» Defining the event detector options associated with detecting the event.

» Choosing the actions to implement recovery or respond to the detected event.

VII. CONCLUSION

Network Management Systems today, need to deliver scalable, reliable and highly available management solutions with a rich set of features; and no doubt some of the available NMS applications are very promising in their deliverables. But the need doesn't stop here, even with very definitive NMS. Reason being, there are significant efforts & resources need to be involved in order to work on the information received from the NMS.

Nevertheless, automation always remained captivating in the networking world & so in the NMS.

TCL (Tool Command Language) is one the very good **cross-platform scripting that** runs on Windows, Macintosh, and nearly every imaginable Unix platform. It provides high-level API's that let you write code that works the same — everywhere. Importantly, Cisco IOS Scripting with TCL provides the ability to run Tool Command Language (TCL) commands from the Cisco IOS command-line interface (CLI). We can have some really interesting automatic traffic management/diversion TCL policies implemented straight into the devices which can invoke in tandem with EEM

References

1. [Cisco5606] Cisco Systems, " Simple Network Management Protocol", Internetworking Technologies Handbook, Chpt 56, 1992--2006 http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
2. [Cisco5506] Cisco Systems, "Remote Monitoring", Internetworking Technologies Handbook, Chpt 55, 1992--2006 http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm
3. [LowekampZangrilli04] Lowekamp, Bruce B; Zangrilli, Marcia, "Using Passive Traces of Application Traffic in a network Monitoring system", IEEE Computer Society 2004 http://portal.acm.org/citation.cfm?id=1033294
4. [Agarwal03] Agarwal, Deb; Gonzalez, Jose Maria; Jin, Goujun; Tierney, Brian, "An Infrastructure for Passive Network Monitoring of Application Data Streams", Proceedings of the 2003 Passive and Active Monitoring Workshop http://www.pam2003.org
5. [UnivPenn02] Anagnostakis, K.G.; Ioannidis, S. ; Miltchev, S. ; Greenwald, M. ; Smith, J.M. (University of Pennsylvania), "Efficient Packet Monitoring for Network Management" Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2002 http://citeseer.ist.psu.edu/anagnostakis02efficient.html
6. [Tierney04] Tierney, Brian L, "Self-Configuring Network Monitor A High Performance Network Engineering Proposal: Network Measurement and Analysis", For the period June 1, 2001 - May 31, 2004 http://dsd.lbl.gov/Net-Mon/SCNM-proposal.pdf
7. [NetflowWhitePaper05] "Traffic Analysis with Netflow WhitePaper", 2005 http://manageengine.adventnet.com/products/netflow/Traffic_Analysis_with_Cisco_Netflow.pdf [NetflowAbout06] "About Cisco Netflow", 2006 http://manageengine.adventnet.com/products/netflow/cisco-netflow.html

