Cisco IOS Features used for QOS analysis and implementation

Tsvetomir Tsvetanov[1] and Nikolay Manolov[2]

Abstract - **IT managers and network administrators are constantly faced with managing critical business applications across their network infrastructure. Management tasks include troubleshooting network performance problems, capacity analysis and planning, internal accounting of service usage and service billing to company departments. The key to effectively managing network performance and utilization is the ability to measure, quantify and analyze enterprise traffic across the network. This paper describes the use of Cisco NetFlow and network probes for building analysis charts, as well as a practical example of easiest way to utilize protocol information.**

Keywords – **Cisco IOS NetFlow feature, network management**

I. INTRODUCTION

The trends in information and communication technologies to transfer multimedia data, including online audio and video conference streams, in same way of batch interactive data streams raise new problem field waiting for fast and adequate decisions. In the end of 90-es dominating type of services was text and graphical web contents. New age of communications enjoined new technologies in addition of standard e-mail, web-forum, IRC and other similar.

Enhancing effective management and utilizing internetworks Cisco Systems Company offers an ability to measure, quantify, and analyze enterprise traffic across the network.

Typically, such information is gained via 2 methods built-in Cisco IOS:

1. Network probes are used to continuously collect RMON2 statistics (such as, volume, rate, Top N Talkers, etc) about network and application traffic as it flows through the network. This raw data is then mined and analyzed in order to extract information to guide engineering and administrative processes.
2. Cisco's NetFlow data collection technology provides the data necessary to effectively analyze, trend and baseline application data as it passes through the network. NetFlow data can be created by Cisco routers and switches within the network and exported to a reporting package to provide the information necessary to manage critical business applications.

[1] Tsvetomir I. Tsvetanov is with Bulgarian Telecommunication Company – Intranet Department, blvd.Sh.Prohod #69, 1574 Sofia, Bulgaria, z_zvetanov.cits@btk.bg

[2] Nikolay D. Manolov is with Bulgarian Telecommunication Company – Intranet Department, blvd.Sh.Prohod #69, 1574 Sofia, Bulgaria, ndm_w@abv.bg

II. IMPORTANCE OF TRAFFIC ANALYSIS

Traffic analysis builds the foundation upon which successful and proactive network management is possible. It provides precise information as to the existence and behavior of applications and network protocols including the following key elements:

- Volume and rate measurements by application, host and conversation. These measurements allow network administrators to trend growth and to identify abnormal occurrences within the network. (e.g. virus attacks performing Denial of Services on network devices)
- Customizable groupings of network traffic by business units, geography, IP subnets, etc. These groupings of network traffic allow network administrators to associate network traffic with business entities and functions, and trend growth per grouping.
- Customizable filters and exceptions based on network traffic. Such filters and exceptions provide network administrators with alarm notifications in the event of abnormal occurrences in the network.
- Baselining to identify and trend usage statistics and report changes in network or application usage.
- Customizable time-periods to support workday reporting. This provides network administrators the ability to schedule recurring network tasks (such as data backups, database synchronizations, batch processes, etc.) at off-peak hours and to analyze statistics for a given set of business hours.

This information can be used to identify, plan and execute network based projects such as capacity planning and management, network readiness assessments for new business application rollouts, accounting functions on network usage, removing unwanted traffic, managing necessary and optional applications, planning and implementing QoS, and performing budget assessments for future network equipment and support. Without precise and comprehensive knowledge of the presence and behavior of application protocols on a network, network and application performance can be unpredictable, unacceptable and costly. Network administration and engineering changes become reactive. Additionally, costs for rolling out new applications, or adding new sites could well exceed projected values. This could wreak havoc on IT budgets, which could be avoided with usage based planning and accounting.

III. CISCO NETFLOW

Cisco has taken a novel approach to network instrumentation by adding the NetFlow feature set to its routers. NetFlow gives a Cisco router the ability to collect IP network traffic data. Utilizing a router as a probe to gather NetFlow data has the following advantages:

- Low capital investment – The majority of networks are already instrumented with Cisco routers. Customers must simply turn NetFlow on each of the routers in order to start measuring traffic to those routers.
- Simple configuration – configuring NetFlow involves a few global commands and an interface command for each interface running NetFlow.
- Completeness of data – NetFlow measures and reports automatically on all application traffic (most probe solutions require that each probe be configured to look for each traffic type).
- Low lifecycle maintenance - NetFlow capabilities are tied to Cisco router hardware/software maintenance.

However, the following should also be considered when looking to deploy NetFlow:

An increase in CPU utilization on the configured routers (The amount of increase on router CPU utilization varies by router platform and the number of flows traversing the router.)

- An increase in network traffic along the path between the configured routers and the NetFlow harvesters.
- A less significant increase in network traffic along the path between the NetFlow harvesters and the management/reporter console.
- Only IP traffic is supported!

IV. HOW CISCO'S NETFLOW WORKS

NetFlow enables Cisco routers to track unicast IP packets as they enter the router through an interface. As the name implies, NetFlow tracks IP packets on a "per flow" basis. A flow is made up of unidirectional flow of data having two endpoints as individually identified by a combination of the following seven criteria items:

- Source IP address
- Destination IP address
- Source port number (TCP, UDP)
- Destination port number (TCP, UDP)
- Layer 3 protocol type (IP, ICMP)
- Type of Service (ToS) byte (0-7)
- Input logical interface

Any difference in these seven criteria distinguishes one flow from another.

When enabling NetFlow on a Cisco router, a NetFlow cache is built by the router to track flows as they enter the router. The NetFlow cache contains 64-byte records (one per flow) that describe each respective flow. The default size of the NetFlow cache is dependent on the router platform and/or the amount of memory in the router. The information contained in each NetFlow record is somewhat similar, but varies by NetFlow version number.

V. NETFLOW SYSTEM FOR TRAFFIC ANALYSIS

According to Cisco, a complete NetFlow system should contain the components as shown in Figure 1.

Figure 1 : NetFlow Infrastructure

- **NetFlow data export devices** – Cisco switches and routers. Captures NetFlow statistics for ingress IP traffic and export data to a collection device.
- **NetFlow data collector –** Software performing data collection, filtering and aggregation.
- **NetFlow analyzer –** The user interface to collected data. Enables user to retrieve and display NetFlow collected data, based on several criteria.

There are number of commercial NetFlow collectors and analyzers available from Cisco, NetQoS, Apogee, HP and Concord.

VI. EXPORTING NETFLOW DATA

The routing device checks the NetFlow cache once per second and expires the flow in the following instances:

- Transport is completed (TCP FIN or RST).
- The flow cache has become full.
- The inactive timer has expired after 15 seconds of traffic inactivity.
- The active timer has expired after 30 minutes of traffic activity.

NetFlow data is exported in one of four formats: Version 1, Version 5, Version 7, and Version 8. In all versions, the datagram consists of a header and one or more flow records (see Table 1 and Table 2). The Version 5 format adds BGP AS information and flow sequence numbers. The Version 7 format is used only on Catalyst switches. Cisco IOS NetFlow aggregation maintains one or more extra flow caches with different combinations of fields that determine which traditional flows are grouped together. These extra flow caches are called aggregation caches. Version 8, a new data export version format, has been added to support data exports from aggregation caches. This leads to reduced bandwidth requirement and reduced NetFlow workstation requirements. In version 9 Cisco will implement flexible export format and support for MPLS, multicast and BGP Next Hop.

TABLE 1
VERSION 1 HEADER FORMAT

Bytes	Content	Description
0-1	version	NetFlow export format version number (in this case, the number is 1).
2-3	count	Number of flows exported in this packet (1 to 24).
4-7	sysUptime	Number of milliseconds since the routing device was last booted.
8-11	unix_secs	Number of seconds since 0000 UTC 1970.
12-15	unix_nsecs	Number of seconds since 0000 UTC 1970.

TABLE 2
VERSION 1 FLOW RECORD FORMAT

Bytes	Content	Description
0-3	srcaddr	Source IP address.
4-7	dstaddr	Destination IP address.
8-11	nexthop	IP address of the next hop router.
12-13	input	Simple Network Management Protocol (SNMP) index of the input interface.
14-15	output	SNMP index of the output interface.
16-19	dPkts	Packets in the flow.
20-23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24-27	first	SysUptime at start of flow.
28-31	last	SysUptime at the time the last packet of flow was received.
32-33	srcport	TCP/UDP source port number or equivalent.
34-35	dstport	TCP/UDP destination port number or equivalent.
36-37	pad1	Pad 1 is unused (zero) bytes.
38	prot	IP protocol (for example, 6 = TCP, 17 = UDP).
39	TOS	IP ToS.
40	flags	Cumulative OR of TCP flags.
41	tcp_retx_cnt	Number of mis-sequenced packets with delay > 1 second.
42	tcp_retx_secs	Cumulative seconds between mis-sequenced packets.
43	tcp_misseq_cnt	Number of mis-sequenced packets seen.
44-47	reserved	Unused (zero) bytes.

VII. NETFLOW APPLICATION

As NetFlow is activated on appropriate router interfaces and export function is up and running, using a simple command application (Figure 2) NetFlow data is collected within a period of time and is stored into relational database or into plain text file/s. Result analysis performs, aided by relations of data stored, which is the way to trend and monitor enterprise traffic. All information presents in a user-friendly graphic style by web application or other GUI. Graphics and text result summaries the points and time, where and when is recommended applying prioritization techniques performed in router IOS.

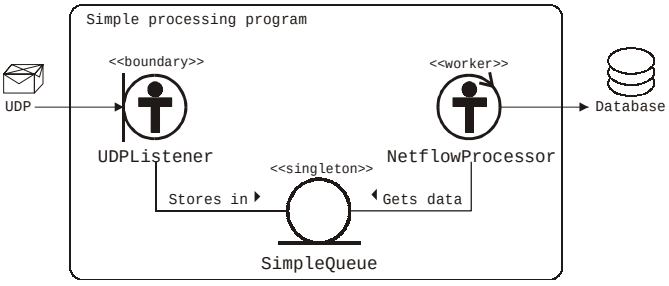

Figure 2 : Application UML diagram

Data storage and monitoring can be done via two scenarios:

- Data is stored within a 24-hour period and using additional processes stored data is aggregated following previously well defined plan for creating significant sections (database table joins). Aggregated in that manner data leaves for additional trending within a larger periods of time: couple of days, a week or a month.
- Data is stored into a relational database within a longer time period, e.g. month, and finally the NetFlow application generated interactively online DB queries for significant table joins.

Based on NetFlow data collection and aggregated data network managers get a picture which kind of internetwork and enterprise applications is used between sets of subnetworks and specific nodes. In enterprises implemented policy-based routing network engineers and administrators can have real information of load in logical circuits. In that way NetFlow analyzer application is a tool for designing a reliable and load balanced network. Assume that we chance on a multiple interconnections at core/backbone network as shown in Figure 3. As the network grows and changes its topology it is possible to misbalance the traffic shaping doesn't matter it was previously well balanced. Adding or modifying services supplied by enterprise servers attached at stub subnetworks of backbone routers can be reason of change of traffic characteristics, so policy-routing is no more properly working. In enterprises quickly growing and altering, in cases of designing new network implementation, when preparing test plans for innovations, NetFlow application analyzer helps engineers to commit trends, points of weakness, and fields of redesign.

Furthermore, modern networks transfer still more multimedia content. Audio, video and telephony services are routed together with batch interactive data. Having NetFlow collection process engineers can afford designing more intelligent software that provides an advisory capabilities such as report suggestion for QoS implementation, for new load balance design, and for bandwidth utilization.

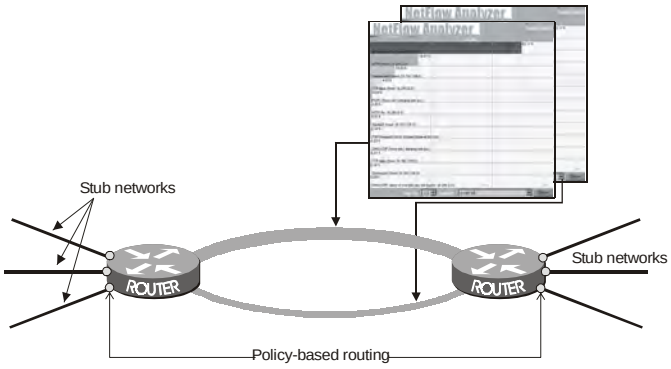

Figure 3: Multiconnected backbone network

VIII. BENEFIT FOR BILLING/ACCOUNTING

NetFlow captures and exports detailed measurements including intra-company, supplier and customer traffic volume and application usage patterns for billing/accounting and network planning purposes.

Customer benefits by pay for only the required bandwidth being utilized. The customer (and the service provider) also benefits by receiving detailed usage measurements via NetFlow data export and by easy reconfiguration to higher service levels when required. For example - time and usage based billing via NetFlow measurements provide the service provider with a means of encouraging (or shifting) demand during periods of light network loading by offering off peak discount pricing. Traffic classes and prioritization allow the network operator to encourage the customers to classify their traffic and then to transport the highest value bits during peak usage periods and heavy congestion conditions.

IX. CONCLUSION

Cisco IOS QoS services and NetFlow data collection and export capabilities provide a new paradigm for ISP's to efficiently monitor network operations, drilldown to diagnose and resolve network troubles and provide both internal personnel and customers with data concerning service level agreement metrics. ISPs may now utilize a flow-based paradigm to visualize traffic flows in the network including aggregate traffic flows, flows by application and flows by class of service. Enhanced network monitoring based on layer 3 services MIBs will also provide the capability to observe bandwidth allocation and excess usage.

In addition with IP Account and RMON2 features of Cisco IOS NetFlow is a powerful tool for monitoring and management of complex enterprise networks. It gives managers and engineers a key for flexible and vivid trend and performance management and utilization of their enterprises internetworks.

REFERENCES

[1] Cisco® NetFlow or RMON2: NetQoS White Paper, http://www.netqos.com

[2] Advanced QoS Services for the Intelligent Internet, Cisco White Paper, www.cisco.com