NETWORK TRAFFIC ANALYSIS AT THE 20,000 FOOT LEVEL - OR WHERE DID ALL THIS TRAFFIC COME FROM

Henry Steinhauer
Hewitt Associates
Lincolnshire, IL, U.S.A.

Managing the Network involves a number of different views. While waiting for other Network tools to arrive, we tried out some Network Viewing methods. This paper will describe our experiences in the hope that others will also see their Network traffic from a different view.

INTRODUCTION:

While waiting for other Network products to produce results, we happened to stumble on a GNU General Public License product that anyone can install and use. (While GNU stands for Gnu Not Unix, the program will run on Unix and NT. The important point for us is the cost – free) It allows us to have a simple view of our Network traffic without getting into a lot of detail or bringing our Network down to its knees with bandwidth required for the monitoring operation. It has also allowed us to use the other tools with more success. We now know which segments to use the other tools on and expect to see some results.

BACKGROUND INFORMATION:

The background information that you need to understand to use any of the non-basic monitoring tools: RFC, SNMP, MIB and OID.

RFC – Request for Comment This is the way that the Network community creates documents to describe and share information. It includes everything from Protocols to Management issues. There is even an RFC that describes the Timeline of the Internet (RFC2235). RFCs can be requested for viewing by using either e-mail or FTP processes. The simplest approach is to send an e-mail to nis-info @ nis.nsf.net with send *rfcnnnn.txt* in the message body. An automatic responder will automatically send you the RFC back to your e-mail address.

The RFCs relating to SNMP are: RFC 1157 (where it is defined), RFC 1187 (Bulk Table Retrieval with SNMP), RFC 2011, 2012, 2013 (describe SNMPv2 – the next generation), and RFC 2273 (SNMPv3).

While you do not have to understand all the content of the RFC, it is useful to understand what they were working toward with introducing SNMP. There is a lot of useless information (mostly because it is system-specific or considerably outdated) in the RFCs, but there is also a wealth of detail. Just watch out, do not believe everything you read.

SNMP – Simple Network Management Protocol. The networking industry noted that a single management standard was required. What's more, any final solution would need to be both broad and flexible enough to cover all of the available networking and inter-network devices. SNMP emerged as a defined standard in 1988. Essentially, the standard defines two entities: a single manager and multiple agents. The manager was designed to be a dedicated workstation that would act as collection point for the management information from various network devices. The management information on each network device would be collected by the SNMP agents.

The "simple" part within SNMP relates to both its architecture and its development requirements. It is a fairly simple requirement for vendors to incorporate the required functionality defined by the SNMP specification within their networking products. From an architectural point of view, the standard is also flexible enough to facilitate the inclusion of additional management functionality as the vendors see fit to provide.

The overall operation of the SNMP standard considers the three main areas of functionality necessary for the development of an effective network management framework:

1) Identification of the items within the network that require management;
2) Identification of the information that needs to be gathered for each of these items;
3) The method for distributing this collected management information to the network manager

MIB – Management Information Base. Every SNMP managed device maintains a database that contains statistics and other data. This database is called a Management Information Base or MIB. The MIB entries have four pieces of information in them: an object type, a syntax, an Access field, and a Status field. Advantageous for us, the MIB entries are usually standardized by the protocols and follow strict formatting rules defined by Abstract Syntax Notation One (ASN.1).

OID – Object Identifier. The standardized formatting rules are described by the OID associated with the MIB tree. The use of the OID tree makes it possible to identify any object or group of objects within the management framework. The unique OID provides the necessary reference. For example, it is possible to identify all vendors of networking devices supporting SNMP under the OID { 1.3.6.1.4}. Likewise, it is possible to reference a device's IP protocol-related data under the OID {1.3.6.1.2.1.4}.

For our use we are interested in the Interface information and the number of bytes sent in or out of that interface. The MIB objects are normally named ifInOctets and ifOutOctets. If you use the MIB names, then the exact spelling and capitalization is required for the SNMP agents to know which MIB you are asking about. The OID is {1.3.6.1.2.1.2.2.1.10 and 1.3.6.1.2.1.2.2.1.16}. You can see why people create names for referring to these OID numbers. Getting the numbers just right is why we are all happy these are done with cut/paste tools today and not punched cards.

INFORMATION ON EACH NETWORKING DEVICE

Now that we have the foundation laid, we need to start looking at what is a typical campus today.

We are still a Token Ring shop for the most part. We do have E100 in some of the Server areas, but these are directly attached to E100 switches to avoid any problems with Ethernet. Within our local campus area, we have 9 buildings today. We have broken up these 9 buildings into 6 campus settings. They are far enough apart that they could not be connected with just simple Fiber runs. We had to partner with our local phone company and have a SONET connection between. This gives us 47 Mb for data with the rest of the SONET for our Voice traffic. For redundant protection, we started with two routers in each campus. The SONET is a ring so the data can travel in either direction for service. Any one of the areas could break and the other ones would still have access to all the data.

We wanted to study the traffic load by taking a simple approach to the problem, we were able to narrow the focus to just looking at the InOctets and OutOctets for each campus.

Looking at one of the Bay Routers, we have 20+ interfaces that have counters associated with them. Since we have 12 routers, that amounts to 240 interfaces that we need to gather information about. To do this, we need something automatic. There just are not enough hours in the day to gather the data by hand.

Our stated direction is to use NetView/6000 for our NetWork Management. BUT it seems each time we add devices, there is a long lag time before we can get data. Also running this 24 hours per day appears to burn up a lot of bandwidth.

We needed something simpler. One of our people happened to stumble on a product called MRTG - The Mutli Router Traffic Grapher. A tool to visualise networktraffic via a WebPage. It was being given away under the GNU license process. The price was right. See the url at *ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html*

MRTG was first written for UNIX, but also runs under NT at this point. With this information, we began another journey to explore the interfaces and LAN/WAN Devices. (Credit needs to be given to Tobias Oetiker (oetiker@ee.ethz.ch)and Dave Rand drl@bungi.com) and Stuart Schneider (schneis@testlab.orst.edu).

We were able to obtain the entire package through the Web. All zipped up with the PERL Language, MRTG source code, Binaries for a program called Rateup to create the Graphs and helper PERL programs to create the configuration input control cards.

Having worked with SAS since 1978 and having a number of other programming languages in my tool kit, learning another language did not turn me off. Also the write-ups had mentioned that you did not have to learn PERL in order to use the tool.

Why use another tool when we already had NetView/6000? We needed something that was simple enough to provide the high level overview of traffic information and still run 24 hours per day 7 days per week. MRTG met that need.

MRTG consists of a PERL script which uses SNMP to read the traffic counters of your routers (or any other SNMP device) and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs are embedded into webpages which can be viewed from any modern Web-browser. NetView/6000 still needs an X-window session for us to have access to the information and this was not exactly something that we wanted to extend over the entire network. We could put these webpages in a central place and have any location view the information without impact.

In addition to the detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last four weeks, and the last twelve months. This is possible because the data log is automatically consolidated so that it does not grow over time, but contains all the relevant data for the last two years.

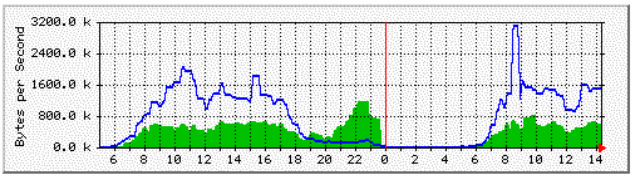
The picture demonstrates the point.

Traffic Analysis for A111

System: BCN at 3OP in Bldg 3 Overlook Point
Maintainer: Steve McCollum
Interface: A111 (7)
IP: ()
Max Speed: 19.4 MBytes/s (sonet)

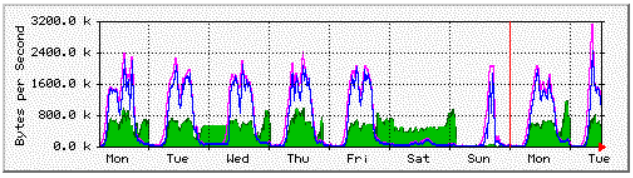
The statistics were last updated **Tuesday, 19 May 1998 at 14:24** ,
at which time **'BCN at 3OP'** had been up for **8 days, 6:36:19**.

`Daily' Graph (5 Minute Average)



Max In: 1196.0 kB/s (6.2%) Average In:416.5 kB/s (2.1%) Current In: 608.9 kB/s (
Max Out:3125.1 kB/s (16.1%) Average Out:787.5 kB/s (4.1%) Current Out:1524.8 kB/s (

`Weekly' Graph (30 Minute Average)



Max In: 1196.0 kB/s (6.2%) Average In:381.2 kB/s (2.0%) Current In: 668.5 kB/s (
Max Out:3125.1 kB/s (16.1%) Average Out:577.9 kB/s (3.0%) Current Out:1499.6 kB/s (

Figures 1 – Daily and weekly Graphs

The red vertical line represents a change in the time frame of the graph. For the daily GIF it is a change in the day; for the week GIF a change in the week; Monthly a month change; Yearly, a year change. All presented very concise and to the point.

We have implemented MRTG now for our entire campus and also all the installed wiring closet switch interfaces.. For some of our larger buildings we have two wiring closets per floor. We have placed an 8 port switch in each closet to reduce the number of stations on each physical the floor. They are still on the same logical segment, but the physical segment is no longer fighting for the same free Token. With this process of monitoring ALL the floors and closets, we are able to see if there is root cause for response time problems or slow downs.

The simple process of using SNMP to gather JUST the InOctets and OutOctets reduces the amount of traffic needed for the NetWork Management process. We can then use the other tools,

NetView/6000, Sniffer and other analyzers, on those segments where there is heavy traffic or repeated problems.

Any device that can respond to a SNMP poll for data can be monitored this way. As well as monitoring NetWare servers for traffic, we track Modem usage by counting the number of modems in use at any point in time. Thus we know when the peak load for the modems occurs and when we are starting to bump into the top of the allocated pool of devices.

Has this replaced our use of NetView/6000 ? Of course not. Has it made our use any different than before? YES. Now we can go into a segment and gather better information since we are not forced to gather large amounts of information from the entire campus.

Using MRTG has also increased the information flow between the different technical areas because we are able to see the impact of having data in a given location.

Is the server interface overloaded? Network bandwidth constrained? A given floor transferring more work than other floors? All of these questions can be answered by viewing the graphs.

CONCLUSION

Getting a handle on the traffic flows of the NetWork is not a trivial task. There are many tools that can assist with that process but they seem to also command a high price tag. Using MRTG has allowed us to gain valuable experience with the NetWork devices and also to give information back to the other technical areas. This process has increased the good will between the groups since the numbers speak for themselves. There is reduced fighting about what is happening over the NetWork. Now we can focus on why it is going over the NetWork. The focus is back on Application Analysis.

References

[Oetiker-WWW] T. Oetiker and D. Rand "Multi Router Traffic Grapher" WWW page ee-staff.ethz.ch / ~oetiker / webtools / mrtg / mrtg.html.

Questions

If you have any questions about this paper or the MRTG tool, please contact Henry Steinhauer at 1-847-295-5000 h1steinh@hewitt.com or visit the MRTG WWW page by T. Oetiker. ee-staff.ethz.ch / ~oetiker / webtools / mrtg / mrtg.html.