CMIP Vs. SNMP : Network Management Essay, Research Paper

CMIP vs. SNMP : Network Management

Imagine yourself as a network administrator, responsible for a 2000 user

network. This network reaches from California to New York, and some branches

over seas. In this situation, anything can, and usually does go wrong, but it

would be your job as a system administrator to resolve the problem with it

arises as quickly as possible. The last thing you would want is for your boss

to call you up, asking why you haven’t done anything to fix the 2 major systems

that have been down for several hours. How do you explain to him that you

didn’t even know about it? Would you even want to tell him that? So now,

picture yourself in the same situation, only this time, you were using a network

monitoring program. Sitting in front of a large screen displaying a map of the

world, leaning back gently in your chair. A gentle warning tone sounds, and

looking at your display, you see that California is now glowing a soft red in

color, in place of the green glow just moments before. You select the state of

California, and it zooms in for a closer look. You see a network diagram

overview of all the computers your company has within California. Two systems

are flashing, with an X on top of them indicating that they are experiencing

problems. Tagging the two systems, you press enter, and with a flash, the screen

displays all the statitics of the two systems, including anything they might

have in common causing the problem. Seeing that both systems are linked to the

same card of a network switch, you pick up the phone and give that branch office

a call, notifying them not only that they have a problem, but how to fix it as

well.

Early in the days of computers, a central computer (called a mainframe) was

connected to a bunch of dumb terminals using a standard copper wire. Not much

thought was put into how this was done because there was only one way to do it:

they were either connected, or they weren’t. Figure 1 shows a diagram of these

early systems. If something went wrong with this type of system, it was fairly

easy to troubleshoot, the blame almost always fell on the mainframe system.

Shortly after the introduction of Personal Computers (PC), came Local Area

Networks (LANS), forever changing the way in which we look at networked systems.

LANS originally consisted of just PC’s connected into groups of computers, but

soon after, there came a need to connect those individual LANS together forming

what is known as a Wide Area Network, or WAN, the result was a complex

connection of computers joined together using various types of interfaces and

protocols. Figure 2 shows a modern day WAN. Last year, a survey of Fortune 500

companies showed that 15% of their total computer budget, 1.6 Million dollars,

was spent on network management (Rose, 115). Because of this, much attention

has focused on two families of network management protocols: The Simple Network

Management Protocol (SNMP), which comes from a de facto standards based

background of TCP/IP communication, and the Common Management Information

Protocol (CMIP), which derives from a de jure standards-based background

associated with the Open Systems Interconnection (OSI) (Fisher, 183).

In this report I will cover advantages and disadvantages of both Common

Management Information Protocol (CMIP) and Simple Network Management Protocol

(SNMP)., as well as discuss a new protocol for the future. I will also give

some good reasons supporting why I believe that SNMP is a protocol that all

network administrators should use.

SNMP is a protocol that enables a management station to configure, monitor,

and receive trap (alarm) messages from network devices. (Feit, 12). It is

formally specified in a series of related Request for Comment (RFC) documents,

listed here.

RFC 1089 – SNMP over Ethernet

RFC 1140 – IAB Official Protocol Standards

RFC 1147 – Tools for Monitoring and Debugging TCP/IP

Internets and Interconnected Devices

[superceded by RFC 1470]

RFC 1155 – Structure and Identification of Management

Information for TCP/IP based internets.

RFC 1156 – Management Information Base Network

Management of TCP/IP based internets

RFC 1157 – A Simple Network Management Protocol

RFC 1158 – Management Information Base Network

Management of TCP/IP based internets: MIB-II

RFC 1161 – SNMP over OSI

RFC 1212 – Concise MIB Definitions

RFC 1213 – Management Information Base for Network Management

of TCP/IP-based internets: MIB-II

RFC 1215 – A Convention for Defining Traps for use with the SNMP

RFC 1298 – SNMP over IPX (SNMP, Part 1 of 2, I.1.)

The first protocol developed was the Simple Network Management Protocol

(SNMP). It was commonly considered to be a quickly designed “band-aid” solution

to internetwork management difficulties while other, larger and better protocols

were being designed. (Miller, 46). However, no better choice became available,

and SNMP soon became the network management protocol of choice.

It works very simply (as the name suggests): it exchanges network packets

through messages (known as protocol data units (PDU)). The PDU contains

variables that have both titles and values. There are five types of PDU’s

which SNMP uses to monitor a network: two deal with reading terminal data, two

with setting terminal data, and one called the trap, used for monitoring network

events, such as terminal start-ups or shut-downs.

By far the largest advantage of SNMP over CMIP is that its design is simple,

so it is as easy to use on a small network as well as on a large one, with ease

of setup, and lack of stress on system resources. Also, the simple design makes

it simple for the user to program system variables that they would like to

monitor. Another major advantage to SNMP is that is in wide use today around

the world. Because of it’s development during a time when no other protocol of

this type existed, it became very popular, and is a built in protocol supported

by most major vendors of networking hardware, such as hubs, bridges, and routers,

as well as majoring operating systems. It has even been put to use inside the

Coca-Cola machines at Stanford University, in Palo Alto, California (Borsook,

48). Because of SNMP’s smaller size, it has even been implemented in such

devices as toasters, compact disc players, and battery-operated barking dogs.

In the 1990 Interop show, John Romkey, vice president of engineering for

Epilogue, demonstrated that through an SNMP program running on a PC, you could

control a standard toaster through a network (Miller, 57).

SNMP is by no means a perfect network manager. But because of it’s simple

design, these flaws can be fixed. The first problem realized by most companies

is that there are some rather large security problems related with SNMP. Any

decent hacker can easily access SNMP information, giving them any information

about the network, and also the ability to potentially shut down systems on the

network. The latest version of SNMP, called SNMPv2, has added some security

measures that were left out of SNMP, to combat the 3 largest problems plaguing

SNMP: Privacy of Data (to prevent intruders from gaining access to information

carried along the network), authentication (to prevent intruders from sending

false data across the network), and access control (which restricts access of

particular variables to certain users, thus removing the possibility of a user

accidentally crashing the network). (Stallings, 213)

The largest problem with SNMP, ironically enough, is the same thing that

made it great; it’s simple design. Because it is so simple, the information it

deals with is neither detailed, nor well organized enough to deal with the

growing networks of the 1990’s. This is mainly due to the quick creation of SNMP,

because it was never designed to be the network management protocol of the

1990’s. Like the previous flaw, this one too has been corrected with the new

version, SNMPv2. This new version allows for more in-detail specification of

variables, including the use of the table data structure for easier data

retrieval. Also added are two new PDU’s that are used to manipulate the tabled

objects. In fact, so many new features have been added that the formal

specifications for SNMP have expanded from 36 pages (with v1) to 416 pages with

SNMPv2. (Stallings, 153) Some people might say that SNMPv2 has lost the

simplicity, but the truth is that the changes were necessary, and could not have

been avoided.

A management station relies on the agent at a device to retrieve or update

the information at the device. The information is viewed as a logical database,

called a Management Information Base, or MIB. MIB modules describe MIB variables

for a large variety of device types, computer hardware, and software components.

The original MIB for Managing a TCP/IP internet (now called MIB-I) was defined

in RFC 1066 in August of 1988. It was updated in RFC 1156 in May of 1990. The

MIB-II version published in RFC 1213 in May of 1991, contained some improvements,

and has proved that it can do a good job of meeting basic TCP/IP management

needs. MIB-II added many useful variables missing from MIB-I (Feit, 85). MIB

files are common variables used not only by SNMP, but CMIP as well.

In the late 1980’s a project began, funded by governments, and large

corporations. Common Management Information Protocol (CMIP) was born. Many

thought that because of it’s nearly infinite development budget, that it would

quickly become in widespread use, and overthrow SNMP from it’s throne.

Unfortunately, problems with its implementation have delayed its use, and it is

now only available in limited form from developers themselves. (SNMP, Part 2 of

2, III.40.)

CMIP was designed to be better than SNMP in every way by repairing all

flaws, and expanding on what was good about it, making it a bigger and more

detailed network manager. It’s design is similar to SNMP, where PDU’s are used

as variables to monitor the network. CMIP however contains 11 types of PDU’s

(compared to SNMP’s 5). In CMIP, the variables are seen as very complex and

sophisticated data structures with three attributes. These include: 1)

Variable attributes: which represent the variables characteristics (its data

type, whether it is writable) 2) variable behaviors: what actions of that

variable can be triggered. 3) Notifications: the variable generates an event

report whenever a specified event occurs (eg. A terminal shutdown would cause a

variable notification event) (Comer, 82) As a comparison, SNMP only employs

variable properties from one and three above. The biggest feature of the CMIP

protocol is that its variables not only relay information to and from the

terminal (as in SNMP) , but they can also be used to perform tasks that would be

impossible under SNMP. For instance, if a terminal on a network cannot reach

the fileserver a pre-determined amount of times, then CMIP can notify

appropriate personnel of the event. With SNMP however, a user would have to

specifically tell it to keep track of unsuccessful attempts to reach the server,

and then what to do when that variable reaches a limit. CMIP therefore results

in a more efficient management system, and less work is required from the user

to keep updated on the status of the network. CMIP also contains the security

measures left out by SNMP. Because of the large development budget, when it

becomes available, CMIP will be widely used by the government, and the

corporations that funded it.

After reading the above paragraph, you might wonder why, if CMIP is this

wonderful, is it not being used already? (after all, it had been in development

for nearly 10 years) The answer is that possibly CMIP’s only major disadvantage,

is enough in my opinion to render it useless. CMIP requires about ten times the

system resources that are needed for SNMP. In other words, very few systems in

the world would able to handle a full implementation on CMIP without undergoing

massive network modifications. This disadvantage has no inexpensive fix to it.

For that reason, many believe CMIP is doomed to fail. The other flaw in CMIP is

that it is very difficult to program. Its complex nature requires so many

different variables that only a few skilled programmers are able to use it to

it’s full potential.

Considering the above information, one can see that both management systems

have their advantages and disadvantages. However the deciding factor between

the two, lies with their implementation, for now, it is almost impossible to

find a system with the necessary resources to support the CMIP model, even

though it is superior to SNMP (v1 and v2) in both design and operation. Many

people believe that the growing power of modern systems will soon fit well with

CMIP model, and might result in it’s widespread use, but I believe by the time

that day comes, SNMP could very well have adapted itself to become what CMIP

currently offers, and more. As we’ve seen with other products, once a

technology achieves critical mass, and a substantial installed base, it’s quite

difficult to convince users to rip it out and start fresh with an new and

unproven technology (Borsook, 48). It is then recommend that SNMP be used in a

situation where minimial security is needed, and SNMPv2 be used where security

is a high priority.

Works Cited

Borsook, Paulina. “SNMP tools evolving to meet critical LAN needs.” Infoworld

June 1, 1992: 48-49. Comer, Douglas E. Internetworking with TCP/IP New

York: Prentice-Hall,

Inc., 1991. Dryden, Partick. “Another view for SNMP.” Computerworld

December 11, 1995: 12. Feit, Dr. Sidnie. SNMP. New York: McGraw-Hill Inc.,

1995. Fisher, Sharon. “Dueling Protocols.” Byte March 1991: 183-190. Horwitt,

Elisabeth. “SNMP holds steady as network standard.” Computerworld

June 1, 1992: 53-54. Leon, Mark. “Advent creates Java tools for SNMP

apps.” Infoworld

March 25, 1996: 8. Marshall, Rose. The Simple Book. New Jersey: Prentice

Hall, 1994. Miller, Mark A., P.E. Managing Internetworks with SNMP New York:

M&T

Books, 1993. Moore, Steve. “Committee takes another look at SNMP.”

Computerworld

January 16, 1995: 58. Moore, Steve. “Users weigh benefits of DMI, SNMP.”

Computerworld

July, 31 1995: 60. The SNMP Workshop & Panther Digital Corporation. SNMP

FAQ Part 1 of 2.

Danbury, CT: http://www.www.cis.ohio-state.edu/hypertext/faq/usenet/snmp-

faq/part1/faq.html, pantherdig@delphi.com. The SNMP Workshop & Panther

Digital Corporation. SNMP FAQ Part 2 of 2.

Danbury, CT: http://www.www.cis.ohio-state.edu/hypertext/faq/usenet/snmp-

faq/part2/faq.html, pantherdig@delphi.com. Stallings, William. SNMP,

SNMPv2, and CMIP. Don Mills, Addison-Wesley, 1993. Vallillee, Tyler, web page

author. Http://www.undergrad.math.

uwaterloo.ca/~tkvallil/snmp.html VanderSluis, Kurt. “SNMP: Not so simple.”

MacUser October 1992: 237-240