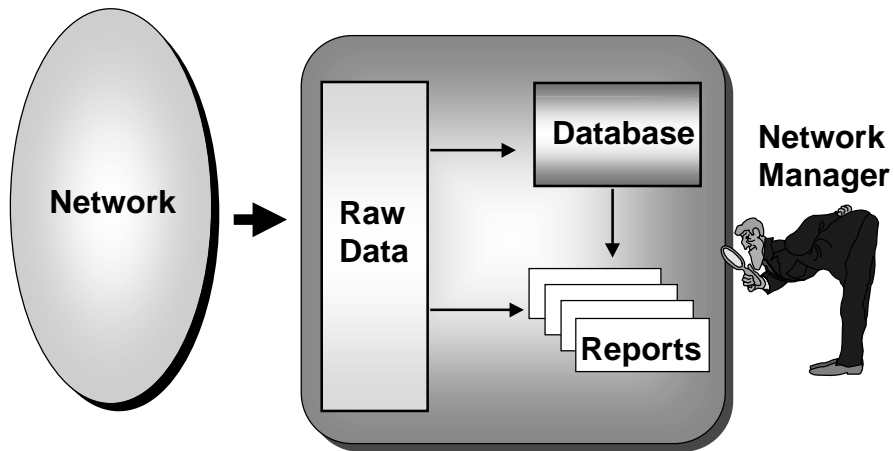


Network Management & Troubleshooting

This presentation covers some of the basic concepts of network management. Some troubleshooting tools are explained: ping, traceroute, telnet and netstat. Then, the basics of SNMP are discussed with emphasis on how PSINet utilizes SNMP.

PSINet *Network Management*



Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.2

Data originates in the network. This data is relayed to the **Network Management Station** or NMS, a device tasked with monitoring the network.

The NMS processes the raw data into a database. The raw data and database information are utilized to create reports that can be examined by the network manager.



PSINet *Network Management*

- Goals**
 - Provide network information
 - Fix problems
 - Identify potential problems
- Facets of network management**
 - Data collection
 - Real-time management
 - Fire fighting

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.3

Networks need to be managed to keep users happy and productive. Network management can provide information about the network, identify and fix current problems and track trends to predict potential future problems.

Network management can be divided into three general areas: data collection, real-time management and fire fighting.

- Possible statistics to be collected
 - Usage
 - Link status
 - Routing
- Reports
 - Textual and graphical
 - Different levels of detail & time periods
- Garbage in - garbage out

Data collection and analysis are required to identify current problems and to predict future network trends.

The exact data that will be needed three months from now is not known, so as much data as possible should be collected and maintained. What doesn't seem important now may be vital in the future.

Data should be kept as long as possible in order to track trends and analyze change. However, there is a trade-off between the amount of data you wish to collect and maintain and the amount of data you will find useful.

You may wish to maintain login histories for a year. However, this may not be practical given system constraints. Also, you may not need to maintain this information for such an extended period of time.

Some information that can be collected:

Usage: of bandwidth, of services, of machine time, etc.

Changes in link status: new connections, connections that have gone away, flapping.

Routing changes: changes in traffic patterns can be indicative of problems.

To get the most out of your data, you should look at it from different perspectives: graphical and textual, daily and monthly, per user and per department, etc.

As with all data, if the data is inaccurate, any conclusions you draw through analysis of the data will also be inaccurate.

Real-Time Management

- Global picture of the current state of the network
- Monitor & react to the changing state
- Graphical tools
- Different levels of granularity
- Areas requiring real-time management
 - Network links
 - Network routing
 - End systems

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.5

Real-time management is necessary to manage the changing state of the network. For example, if usage of a particular service machine increases dramatically, real-time management is necessary to react in a timely manner.

PSINet monitors usage of service machines such as DNS resolvers, authentication machines and USENET servers. This allows the system administration team to react to changes in the network before customers are aware of any problems.

- Routing metrics
- Path taken by packets
- Routing problems
 - Routing loops
 - Black holes

Routing information also provides information about the state of the network. Changes in metrics indicate changes in the state of the network. Similarly, if packets begin taking a different path, something has changed on the network to result in this behavior.

Routing problems are generally due to:

Routing loops

One gateway is passing a packet to another gateway which is in turn passing the packet back to the first gateway; the packet never reaches the destination. Routing loops can contain more than two gateways.

Black holes

Some device is advertising a route to a network that it can't actually reach. Packets for this destination are forwarded incorrectly to this device and thus, never reach the destination.



End Systems

- Load
 - On the network
 - On the end systems
- Types of network utilization
 - Mail
 - File Transfers
 - Remote Terminal
 - Domain Name Service
- Users

End systems also need to be monitored and managed. This is not system administration; end systems need to be monitored based upon their effect on the network as well as the network's effect on the end system. Some of the aspects of end system management are network load (both the load placed on the network due to system use and load placed on the system due to the network), types of network utilization (services offered and utilized), and system users (remote and local).



Traditional Tools

- Ping, traceroute, telnet, netstat
- Not true network management tools

Some commonly used troubleshooting tools are ping, traceroute, telnet and netstat. These are not true network management tools, but they can provide a basic picture of where the problem may be.

- PING: Packet INternet Groper
 - Term coined by Dave Mills of the University of Delaware
- ICMP echo request and ICMP echo reply
- Round trip times are computed.
- Tests IP connectivity.
- Does NOT test services or TCP.

PING is an *ICMP* (Internet Control Message Protocol) echo request and echo reply pair. The source host sends an *ICMP* echo request to the destination. The destination in turn sends an *ICMP* echo reply. When the source receives the reply, it calculates and reports the round trip time - the amount of time it took to receive the request combined with the amount of time it took for the source to receive the reply sent by the destination.

Ping is a tool that tests IP connectivity since *ICMP* packets are IP packets. Ping does not test *TCP* or any particular services such as e-mail.



Sample Ping

```
> ping uu4.psi.com 56 5
PING uu4.psi.com: 56 data bytes
64 bytes from uu4.psi.com (38.146.21.2): icmp_seq=0. time=94. ms
64 bytes from uu4.psi.com (38.146.21.2): icmp_seq=1. time=90. ms
64 bytes from uu4.psi.com (38.146.21.2): icmp_seq=2. time=91. ms
64 bytes from uu4.psi.com (38.146.21.2): icmp_seq=3. time=96. ms
64 bytes from uu4.psi.com (38.146.21.2): icmp_seq=4. time=96. ms

----uu4.psi.com PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 90/93/96
```

This is sample output from a ping. The 56 is the packet size and the 5 is the number of packets to be sent; syntax may vary from system to system.

This ping was sent from a host on PSINet in Troy, NY, to another PSINet host in Santa Clara, CA.



Sample Ping

```
> ping rpi.edu 56 5
PING rpi.edu: 56 data bytes
64 bytes from rpi.edu (128.113.1.7): icmp_seq=0. time=56. ms
64 bytes from rpi.edu (128.113.1.7): icmp_seq=1. time=64. ms
64 bytes from rpi.edu (128.113.1.7): icmp_seq=2. time=63. ms
64 bytes from rpi.edu (128.113.1.7): icmp_seq=3. time=59. ms
64 bytes from rpi.edu (128.113.1.7): icmp_seq=4. time=51. ms

----rpi.edu PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 51/58/64
```

This ping was sent from the same PSINet host in Troy, NY, to a non-PSINet host in Troy, NY.



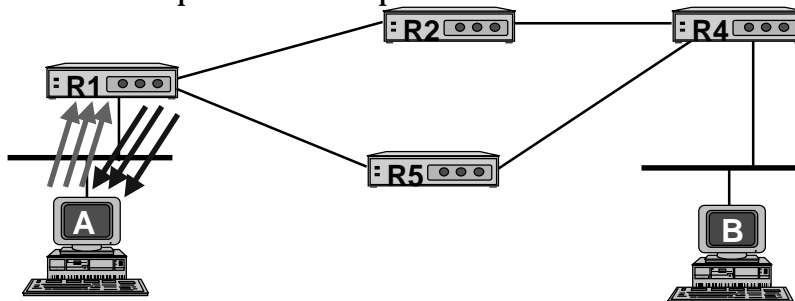
Traceroute

- Coded by Van Jacobson of LBL
- Uses the ICMP TTL Exceeded message.
- Possible path
- UDP Ports 33410-33524

Traceroute also utilizes ICMP packets and thus tests IP connectivity, not TCP or any particular service. In addition to determining whether or not a particular host is reachable, traceroute also reports a possible path packets may take to reach the destination. Traceroute utilizes the TTL or time-to-live parameter of a IP packet.

PSINet *Traceroute from A to B*

- ❑ Send 3 packets to host B with TTL of 1.
 - ❑ R1 sends TTL_EXCEEDED error to A.
 - ❑ Error includes IP Address of R1.
 - ❑ Compute round trip time.



Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

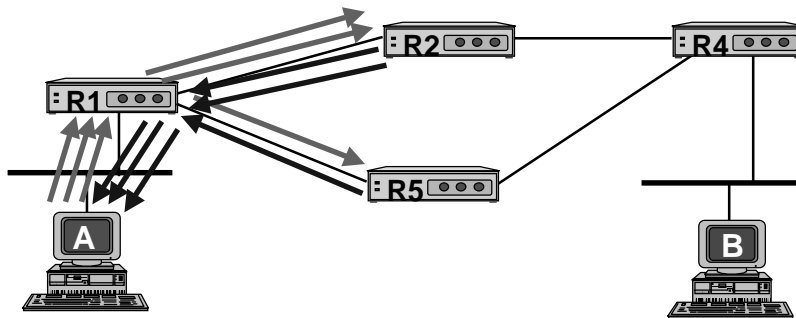
T08.13

If A issues a traceroute to B, A sends 3 packets to B with a TTL of 1. Thus the packets will expire at the first IP hop.

In the above example, R1 is the first hop. When the packet reaches R1, the TTL is decremented and the packet expires. R1 thus drops the packet and returns a TTL_EXCEEDED message to A.

PSINet *Traceroute from A to B*

- ❑ Send 3 packets to host B with TTL of 2.
- ❑ TTL_EXCEEDED errors returned.



Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

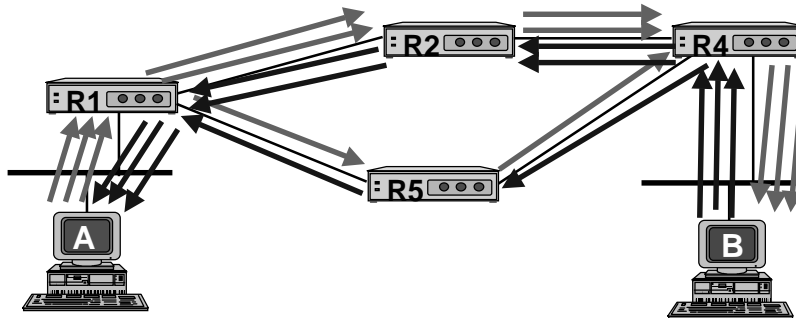
T08.14

A then sends 3 packets to B with a TTL of 2. These packets will expire at the second IP hop from the source to the destination. Again, an ICMP message will be returned to A indicating that the TTL has been exceeded.

Note that each of the three packets can follow a different path depending upon the network topology.

PSINet *Traceroute from A to B*

- And so on and so on, until the destination is reached.



Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.15

This process continues until B receives the packet. The packet is sent to an invalid, high-numbered port. Thus, when the packets arrive at B, an error is returned to A indicating an unreachable port.



Sample Traceroute

```
> traceroute uu4.psi.com
traceroute to uu4.psi.com (38.146.21.2), 30 hops max, 40
byte packets
 1 136.161.2.1 (136.161.2.1) 11 ms 3 ms 3 ms
 2 poproom.psi.net (136.161.17.1) 11 ms 3 ms 2 ms
 3 core.net222.psi.net (38.1.2.4) 98 ms 158 ms 104 ms
 4 uu4 (38.146.21.2) 90 ms 90 ms 117 ms
```

This is a traceroute from a PSINet host in Troy, NY, to a PSINet host in Santa Clara, CA.

Notice that in addition to reporting the path, the round trip time of each packet is also calculated. A single packet does not actually make the round trip. The source sends one packet to the destination, somewhere along the path the TTL expires, and an ICMP error is returned to the source. A round trip value is computed for each of the three packets sent at each step.



Sample Traceroute

```
> traceroute rpi.edu (128.113.1.7), 30 hops max, 40 byte packets
 1 136.161.2.1 (136.161.2.1) 2 ms 2 ms 2 ms
 2 poproom.psi.net (136.161.17.1) 2 ms 2 ms 2 ms
 3 ne.sc.psi.net (38.1.3.1) 85 ms 21 ms 31 ms
 4 east.ext.sc.psi.net (38.1.3.6) 94 ms 22 ms 40 ms
 5 sl-mae-e-f0/0.sprintlink.net (192.41.177.241) 57 ms 37 ms 58 ms
 6 sl-dc-8-H1/0-T3.sprintlink.net (144.228.10.41) 36 ms 37 ms 32 ms
 7 ny-dc-1-F0/0.nysernet.net (144.228.20.110) 46 ms 42 ms 39 ms
 8 ny-syr-2-H1/0-T3.nysernet.net (169.130.1.93) 42 ms 43 ms 56 ms
 9 ny-syr-1-F0/0.nysernet.net (169.130.30.1) 58 ms 68 ms 67 ms
10 ny-alb-2-H1/0-T3.nysernet.net (169.130.1.21) 59 ms 96 ms 67 ms
11 169.130.22.6 (169.130.22.6) 69 ms 64 ms *
12 vccfr2.its.rpi.edu (128.113.100.246) 65 ms 64 ms 70 ms
13 rpi.edu (128.113.1.7) 75 ms 64 ms 64 ms
```

This is a traceroute from a PSINet host in Troy, NY, to a non-PSINet host in Troy, NY. Notice that the packets travel all the way to Washington, DC, even though both hosts are in the same Upstate New York city. This is because the two hosts access the Internet through two different Internet Service Providers and MAE-East is the location of the closest peering point for these two providers.



Sample Traceroute

```
> traceroute 38.2.190.62 30 hops max, 40 byte packets
 1 host2.abci.net (207.211.42.254) 3 ms 3 ms 3ms
 2 206.171.145.33 (206.171.145.33) 9 ms 8 ms 9 ms
 3 snfc21-ign0.pbi.net (206.13.4.8) 9 ms 9 ms 11 ms
 4 165.87.225.6 (165.87.225.6) 11 ms 10 ms 9 ms
 5 sfo-uunet.ca.us.ibm.net (165.87.225.25) 11 ms 12 ms 10 ms
 6 Fddi0.CR2.SFO1.Alter.Net (137.39.41.38) 10 ms 11 ms 10 ms
 7 133.Hssi4-0.CR2.TCO1.Alter.Net (137.39.71.70) 76 ms 78 ms 80ms
 8 312.atm3-0.br1.tco1.alter.net (137.39.13.9) 113 ms 80 ms 77 ms
 9 mae-east.psi.net (192.41.177.245) 87 ms 219 ms 93 ms
10 sw.sc.psi.net (38.1.3.4) 214 ms (ttl=244!) 319 ms (ttl=245!) *
11 sw.sc.psi.net (38.1.3.4) 174 ms * *
12 * * 38.1.24.3 (38.1.24.3) 152 ms
13 38.217.6.1 (38.217.6.1) 194 ms * *
```

This is a traceroute from an off-PSINet host to a PSINet router. Notice that the path goes through MAE-East (step 9) on the East coast of the US.



Sample Traceroute

```
> traceroute 207.211.42.1 30 hops max, 40 byte packets
 1 38.1.24.1 72 msec 100 msec 16 msec
 2 NW.SC.PSI.NET (38.1.3.3) 208 msec 20 msec 24 msec
 3 * SAN-JOSE3.CA.ALTER.NET (198.32.136.42) 40 msec 40 msec
 4 HSSI1-0.PALO-ALTO2.CA.ALTER.NET (137.39.101.162) 52 msec * *
 5 * * *
 6 197.HSSI4-0.CR1.SFO1.ALTER.NET (137.39.71.162) 148 msec * *
 7 FDDI0.GW1.SFO1.ALTER.NET (137.39.41.35) 184 msec 172 msec
   172 msec
 8 * 165.87.225.26 148 msec 156 msec
 9 SFO-PACBELL-POP-SF.CA.US.IBM.NET (165.87.225.5) 156 msec
   136 msec 144 msec
10 SNFC21-IGN1.PBI.NET (206.13.4.9) 140 msec 140 msec 156 msec
11 * * 206.171.145.34 140 msec
12 HOST.ABC.NET (207.211.42.1) 156 msec * 160 msec
```

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.19

A traceroute from the same PSINet router to the same off-PSINet host.

Notice that traffic is sent through the Northwest interconnection point (step 2).

Asymmetric traceroutes can be indicative of a problem. One ISP feels the best route between the two hosts is on the East coast while the other ISP prefers the West coast to exchange traffic between these two hosts.

This example also illustrates what happens when traceroute packets are lost. Lost packets are represented by an asterisk.

- Test TCP connectivity
- May be able to ping, but not telnet.
The opposite could also be true.
- Preliminary connectivity tests on network services.
 - telnet *hostname port*
- Port 23

In addition to verifying IP connectivity, **telnet** verifies TCP connectivity. TELNET is a service that, by default, utilizes TCP port 23. The ability to ping does not imply the ability to telnet nor does the ability to telnet imply the ability to ping.

TELNET also allows basic testing of TCP services such as SMTP mail, USENET news, http server, etc. To test a particular service on a particular host, telnet to the host at the port the service is provided on.



Sample Telnet: SMTP

```
>telnet support.psi.com 25
Trying 136.161.2.3 ...
Connected to support.psi.com.
Escape character is '^]'.
220-support.psi.com Sendmail 8.6.12/PSI ready at
    Tue, 19 Mar 1996 08:59:10 -0500
220 ESMTP spoken here
>quit
221 support.psi.com closing connection
Connection closed by foreign host.
```

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.21

The TELNET to port 25 results in an SMTP (in this case Sendmail) banner indicating that the host is servicing incoming SMTP connections. SMTP commands can be entered at this prompt.



Sample Telnet: SMTP

```
>telnet www.psi.net 25
Trying 38.8.8.2 ...
telnet: connect to address 38.8.8.2:
  Connection refused
Trying 38.8.64.2 ...
telnet: connect: Connection refused
telnet> quit
```

Notice that in the first instance, the TELNET connection to port 25 (the SMTP port) is denied. This implies that either the host is unreachable or SMTP is not enabled. Ping can be used to determine whether or not the host is reachable.



Sample Telnet: NNTP

```
>telnet client1.news.psi.net 119
Trying 38.8.205.2 ...
Connected to client1.news.psi.net.
Escape character is '^]'.
200 client1 InterNetNews NNRP server
    INN 1.4 20-Mar-93 ready (posting ok).
quit
205
Connection closed by foreign host.
```

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.23

Other services, such as USENET News and World Wide Web can also be tested using this technique.



Routing Tables

- Routing table information
 - Default route
 - Other routes
 - Flags
 - Metrics

Netstat allows you to determine the status of routing information. Very often it is used during the initial configuration of a device to determine whether or not the default route has been set correctly.

Different platforms and devices use different commands to display routing information. Netstat may not be the command you need to enter to display routing information.



Sample Netstat: Host

```
>netstat -rn
```

Routing tables

<u>Destination</u>	<u>Gateway</u>	<u>Flags</u>	<u>Refcnt</u>	<u>Use</u>	<u>Interface</u>
127.0.0.1	127.0.0.1	UH	2	6447019	lo0
default	136.161.2.1	UG	233	155553887	le0
136.161.2.0	136.161.2.3	U	5	4137645	le0

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.25

This example is the routing information from a UNIX host.

The **Flags** indicate whether the entry is Up or Down and also whether it applies to a Gateway or Host. **Refcnt** indicates the current number of active uses for this particular route. The **Use** column displays the number of packets sent along the route and the **Interface** indicates which interface should be used for the indicated route.

Different hosts have different routing capabilities.

Macintosh machines do not route and thus do not require a command to display the routing tables.

Windows based machines display the routing table when the **route print** command is entered at the MS-DOS prompt.

Different flavors of UNIX generally use a variation of the **netstat** command.



Sample Netstat: Router

```
Command> show routes
```

<u>Destination</u>	<u>Gateway</u>	<u>Flag</u>	<u>Met</u>	<u>Interface</u>
0.0.0.0	38.145.250.1	NS	1	ether0
204.242.154.65	204.242.154.65	HL	1	ptp1
206.0.40.1	206.0.40.1	HL	1	ptp3
199.100.86.1	199.100.86.1	HL	1	ptp2
192.246.3.3	192.246.3.3	HL	1	ptp22
192.246.3.0	192.246.3.3	NS	1	ptp22
206.0.40.0	206.0.40.1	NS	1	ptp3
199.100.86.0	199.100.86.1	NS	1	ptp2
204.242.154.0	204.242.154.65	NS	1	ptp1
38.145.250.0	38.145.250.126	NL	1	ether0

Copyright © 1997 PSINet Inc. Confidential and Proprietary Information T08.26

This slide illustrates the routing information that is obtained when the **show routes** command is entered on a Livingston router.

The **Destination**, **Gateway** and **Metric** have the same meaning that has been used in the two routing presentations (Introduction to Routing and Routing Protocols). The **Interface** indicates which interface on the router the route should utilize. The **Flag** indicates whether the router is for a Network or a Host and also whether it was Learned or Static (part of the router configuration).

Syntax for routers supported by PSINet:

Ascend	Ethernet - Routes
Cisco	show ip route
Livingston	show routes
MicroRouter 990i	show ip routing
Morning Star	netstat -rn
Nethopper	netstat -r
Netopia	<i>currently unavailable</i>
Proteon	*talk 5 + protocol ip IP config> dump

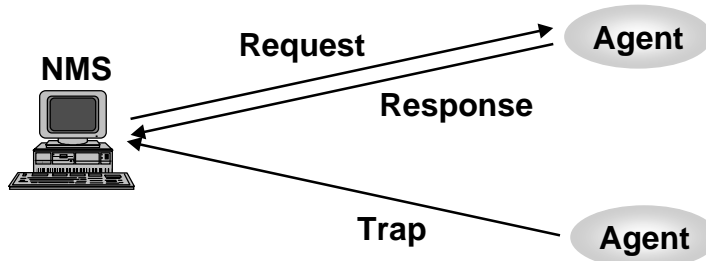
- Simple Network Management Protocol
- RFC 1157
- Three out of the four authors are connected with PSINet:
 - Mark Fedor, Marty Schoffstall, James Davin
- Developed to manage TCP/IP networks
- SNMP reports of router utilization are provided to PSINet leased line customers.

SNMP was developed to fill a need for real network management abilities. The tools we already discussed, ping, traceroute, telnet and netstat, are not true network management tools, but they are all that was available at one time.

Three of the four authors of RFC 1157 are connected with PSINet.

For leased line customers, PSINet will monitor the traffic and errors seen on your router interfaces. A report will be e-mailed to you every morning summarizing network activity for the previous day. In addition, weekly summary reports will also be sent. This service is provided free of charge.

- Request/response transactions between an NMS and an agent



This diagram illustrates the basic operation of SNMP. The NMS (Network Management Station) initiates most of the SNMP interaction. The NMS requests information or action from an agent. The agent responds by returning the requested information or completing the action and returning acknowledgment.



SNMP Terms

- Device, element, entity
 - Part of a network
- Agent
 - Program
- Network Management Station (NMS)
 - Managing entity
- Manager
 - Management software

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.29

Some SNMP terminology:

Device, element, entity

Some device on the network that you would like to manage and/or monitor remotely.

Agent

Program that runs on a device that allows it to be monitored and managed.

Network Management Station (NMS)

A network device that is responsible for the maintenance of the network.

Manager

Program that runs on the NMS allowing the NMS to manage and monitor other network devices that are running agent software.

- Management Information Base (MIB)
 - Collection of variables
- Structure of Management Information (SMI)
 - Format of variables in the MIB
- Set
 - Request to change a variable
- Poll
 - Request to report value of a variable
- Trap
 - Unsolicited exception condition report

More terminology:

Management Information Base (MIB)

A collection of variables whose values taken together represent the state of the device.

Structure of Management Information (SMI)

The building blocks of the MIB. Each MIB variable must be of a particular type. The possible types are determined by the SMI. For example, the MIB variable IP address is made up of four octets; an octet is defined by the SMI.

Set

A request to the agent to change the value of a particular MIB variable.

Poll

A request to the agent to report the value of a particular MIB variable.

Trap

Unsolicited information sent by the agent to the NMS to report an error condition or problem.

- Reside on the managed entity
- Responsible for:
 - Answer requests
 - Perform set operations
 - Generate traps

Recall that the **Agent** is a program running on a network device that allows the device to be remotely managed.

The main responsibilities of the agent are:

Answer requests

When the NMS requests a particular piece of information, the agent must find the correct value and respond to the query.

Perform set operations

When the NMS requests the agent change the value of a particular variable, the agent must satisfy the request.

Generate traps

When the agent discovers a problem or exception, it should report this to the NMS by sending an unsolicited trap.



SNMP Managers

- Direct the remote management
- Responsibilities are:
 - Issue polls
 - Process poll responses
 - Issue sets
 - Process traps

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.32

Recall that a **Manager** runs on the NMS and allows the NMS to manage agents running on other network devices. Some of the responsibilities of the Manager are:

Issue polls

Query agents for particular information when necessary. Polls are used to collect data about the state of the network devices.

Process poll responses

Something must be done with all the information provided by the various network agents. It is the responsibility of the manager to process this information.

Issue sets

When deemed necessary, the manager may issue a **set** requesting an agent to change the value of a particular variable. For example, if an agent responds with inconsistent data, the manager may conclude that a system restart is necessary. To accomplish this, the manager may request the agent set the “time to reset” variable to 10 seconds.

Process traps

When the NMS receives a trap from an agent, it indicates a problem. The manager must process the trap and determine the appropriate response to repair the problem.



SNMP & Security

- Each set/poll is authenticated.
 - Community name
- User Datagram Protocol (UDP) - port 161
- PSINet polling machines
 - 38.8.0.0 network
- PSINet testing machines
 - 136.161.0.0 network

To ensure that set requests and queries are coming from appropriate locations, they are authenticated using a community name which is basically a password. Much damage can be done with SNMP sets. Set (write) and poll (read) requests can utilize separate community names. Unless you are utilizing an NMS, SNMP set access should be disabled on your router.

If you chose to implement packet filters on your router and you want to receive SNMP reports from PSINet, you must allow UDP traffic on port 161. If you wish to implement further security, you can restrict polls to PSINet's polling machines (on the 38.8.0.0 network) and PSINet's support machines (on the 136.161.0.0 network) where testing is performed.



SNMP Configuration

- Cisco Router

- Enable mode

```
conf t
snmp-server community xxxxxx RO
^Z
write mem
```

- xxxxxx is the community name
- RO - read only

Commands to implement SNMP monitoring on a Cisco router.



SNMP Configuration

Livingston Router

```
set SNMP on
set SNMP readcommunity xxxxxx
add SNMP writer none
save all
```

- xxxxxx is the community name
- write enabled by default (private)

Commands to implement SNMP monitoring on a Livingston router.

Notice that when you enable read access to a Livingston router, you also enable write access with a default community name of private. You should turn write access off using the **add SNMP writer none** command.



SNMP Configuration

- Morning Star Router
 - snmpd.conf file
 - xxxxxx 0.0.0.0 read**
 - xxxxxx is the community name
 - Read access enabled by default (public)

Commands to implement SNMP monitoring on a Morning Star router.
By default, the read community name is public.



SNMP Configuration

- Compatible Systems MicroRouter
- Available in version 3.0.4 & up
 - set sys domain xxxxxx**
 - save**
- xxxxxx is the community name
- No *set* access available yet

The Compatible Systems MicroRouter 900i has read-only SNMP capabilities starting with version 3.0.4.



SNMP Configuration

Proteon Router

* talk 6

Config> Protocol SNMP

SNMP> delete community *public*

SNMP> add community *xxxxxx*

SNMP> exit

Control-P

Restart the router

SNMP is on by default (*public*)

xxxxxx is the community name

SNMP configuration for a Proteon router.



SNMP Configuration

- PSINet needs to know:
 - Serial IP address
 - Community name
 - Interface(s)
 - E-mail address for reports

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.39

In order to begin monitoring your router with SNMP, PSINet needs the following information:

Serial IP address

We already know this.

Community name

We will provide you with a suggestion, but we need to agree. Password exchange cannot be done via fax or e-mail but must be done over the telephone.

Interface(s) to be monitored

We can determine this as long as we know the serial IP address and the community name.

E-mail address for the reports

We recommend you receive these reports via e-mail, so you need to tell us where to send them.



Sample Poll

```
>snmpperfmon -c public new-york.psi.net  
SNMPPerfMon v1.0 Copyright (C) PSI, Inc. 1990
```

<u>interface IP address & #</u>	<u>Pkts In</u>	<u>Pkts Out</u>	<u>Octets In</u>	<u>Octets Out</u>
38.145.213.3 1	1,285,143	45,535,808	78,566,373	3,406,778,969
38.1.10.213 2	525,512,215	478,164,724	1,188,422,212	1,938,487,207
38.3.213.1 4	141,106,058	132,136,306	413,988,978	2,056,231,999
38.146.91.1 5	51,498,527	49,599,766	2,512,024,032	188,373,920

Polling in progress. Wait.

Interval: 60

Polling done.

Display: Value

UP: k DOWN: j LEFT: h RIGHT: l QUIT: q

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.40

This tool is used by PSINet to report the interfaces on the router and the amount of traffic that each interface has seen.

Different SNMP implementations and packages will have different command sets. Check your SNMP package for these implementation details, features and capabilities.



Sample Query

```
>snmplookup
      snmplookup Version 3.2
      Copyright (C) PSI, Inc. 1990
      default community name is public
      default timeout is 10 seconds
      default number of recv retries is 1
      default prefix is _iso_org_dod_internet

snmp> agent new-york.psi.net
snmp> community public
snmp> mquery
```

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.41

Another tool used by PSINet provides the entire MIB of information. There is much more information than is shown here. Notice that the type of router and the version of software is reported as is the amount of traffic seen by each interface.



Sample Query

```
mgmt_mib_system_sysDescr_0 4000 Software (XX-K),  
Version 9.1(7.3), MAINTENANCE INTERIM TEST SOFTWARE  
Copyright (c) 1986-1993 by cisco Systems, Inc.  
Compiled Tue 21-Sep-93 06:42 by kmac  
_mgmt_mib_system_sysObjectID_0 1 3 6 1 4 1 9 1 5  
_mgmt_mib_system_sysUpTime_0 0x385e5feb 945709035  
_mgmt_mib_system_sysContact_0  
_mgmt_mib_system_sysName_0 nycwtg_4000.psi.net  
_mgmt_mib_system_sysLocation_0  
_mgmt_mib_system_sysServices_0 0x6 6  
_mgmt_mib_interfaces_ifNumber_0 0x5 5
```

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.42

This is just some of the output returned by the snmplookup tool. Notice that the type of router and version of software can be determined using SNMP.



Sample Query

```
_mgmt_mib_interfaces_ifTable_ifEntry_ifDescr_1 Ethernet0  
_mgmt_mib_interfaces_ifTable_ifEntry_ifDescr_2 Serial0  
_mgmt_mib_interfaces_ifTable_ifEntry_ifInOctets_1  
0x4aed4a9 78566569  
_mgmt_mib_interfaces_ifTable_ifEntry_ifInOctets_2  
0x476b047f 1198195839  
_mgmt_mib_interfaces_ifTable_ifEntry_ifOutOctets_1  
0xcb144b18 3407104792  
_mgmt_mib_interfaces_ifTable_ifEntry_ifOutOctets_2  
0x7413fb3e 1947466558
```

More information returned by snmplookup. This is the information PSINet uses to create SNMP reports for customers: packet and kilobit information in and out for each interface.



Sample Report

Report Period Begins: 12/06/96 0000 GMT

Report Period Ends: 12/07/96 0000 GMT

Interface: sample-lan.eth

Time	Kbits/sec		Packets		Errors	
	In	Out	In	Out	In	Out
[cut]						
1900	2.20	0.27	2461	1845	0	0
2000	21.03	1.30	18525	11323	0	0
[cut]						
2300	0.35	2.90	2360	3142	0	0

Max Input Rate of 44.58 Kbits/sec on 12/06/96 2000 GMT.

Max Output Rate of 11.30 Kbits/sec on 12/06/96 2300 GMT.

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.44

This is one part of a sample report. A similar section is reported for each interface that is being monitored. The report is broken down into hours and reports the packets and kilobytes in and out of each router interface during the hour.

When considering what is “in” and what is “out” for each interface, picture yourself inside the router. Thus a packet from the Internet destined for your internal network will come “in” the serial interface and will go “out” the LAN interface. Similarly, a packet from your internal network that is destined for the Internet will come “in” the LAN interface and will go “out” the serial interface.



Sample Report

Interface: sample-atlanta.ds0

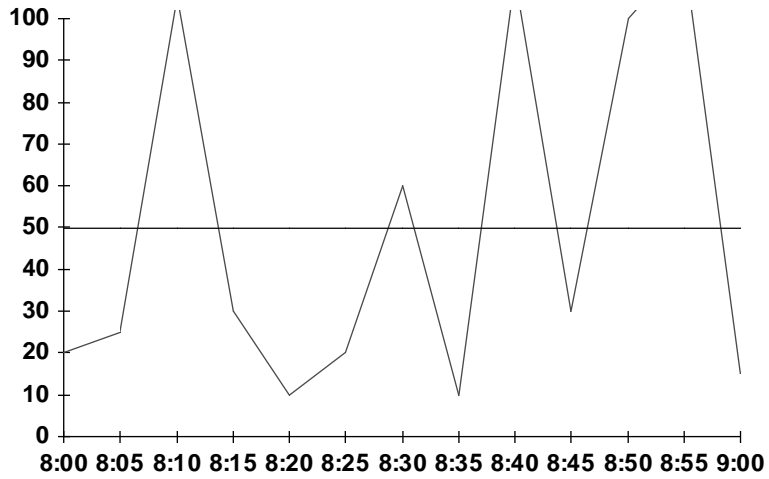
Time	Kbits/sec		Packets		Errors	
	In	Out	In	Out	In	Out
[cut]						
1900	1.47	2.25	1844	2459	0	0
2000	2.82	21.31	11320	18522	0	0
[cut]						
2300	9	14	3	3	0	0

Max Input Rate of 12.44 Kbits/sec on 12/06/96 2300 GMT.
Max Out. Rate of 45.16 Kbits/sec on 12/06/96 2000 GMT.

PSINet's SNMP reports contain a section for the Ethernet interface and another section for the serial interface.



50%: A Problem



Copyright © 1997 PSINet Inc.

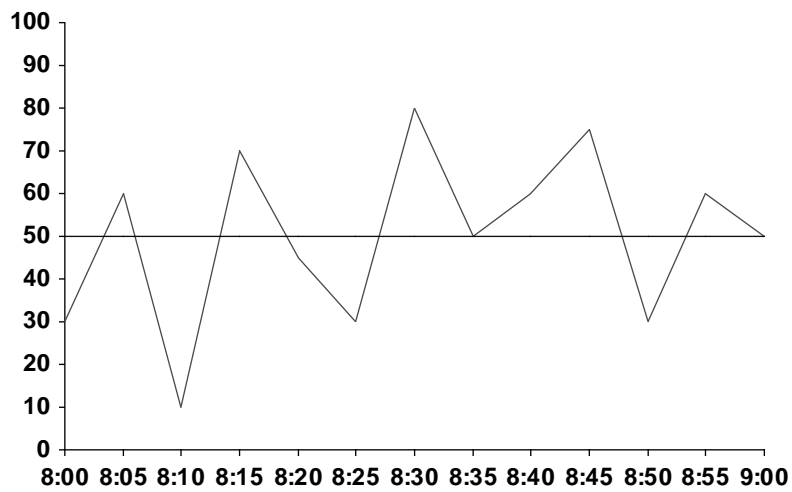
Confidential and Proprietary Information

T08.46

The above graph of 50% usage over the course of an hour illustrates how 50% usage can be indicative of a problem. Usage is bursty and exceeds the available bandwidth during different sections of the hour.



50%: No Problem



Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.47

The above graph illustrates 50% usage over an hour that is not indicative of a problem. At all times, there is sufficient bandwidth to meet the requirements of usage.

Given the bursty nature of Internet traffic, it is likely that 50% usage indicates time of bandwidth saturation.



What is available?

- <http://www.castlerock.com/>
 - Windows - SNMPc
- <http://www.snmp.com>
 - Commercial software for a variety of platforms
 - Other snmp information
- <http://www.desktalk.com/>
 - TRENDSnmp+

Here are some packages and web sites with SNMP information. PSINet has not certified these packages. Thus, we have not verified their functionality nor do we know how to configure or maintain these packages. You should analyze your needs and the packages available before purchasing any SNMP software.



Put it all together

- I can't pull up my web page from an off-net site.
 - Can you ping the web server?
 - ✓ Yes. Can you telnet to port 80? ←
 - ✓ Yes. Can you issue web commands?
 - ✓ Yes. Should be able to pull up your web page.
 - ✗ No. Web server software is not operating.
 - ✗ No. Web server not accepting connections.
 - ✗ No. Can you traceroute to the web server?
 - ✓ Yes. Go to the telnet step above.
 - ✗ No. Where does the traceroute stop?
This is where the problem is.

Copyright © 1997 PSINet Inc.

Confidential and Proprietary Information

T08.49

Here is an example showing how to use troubleshooting tools to determine where a problem exists.



Questions?

