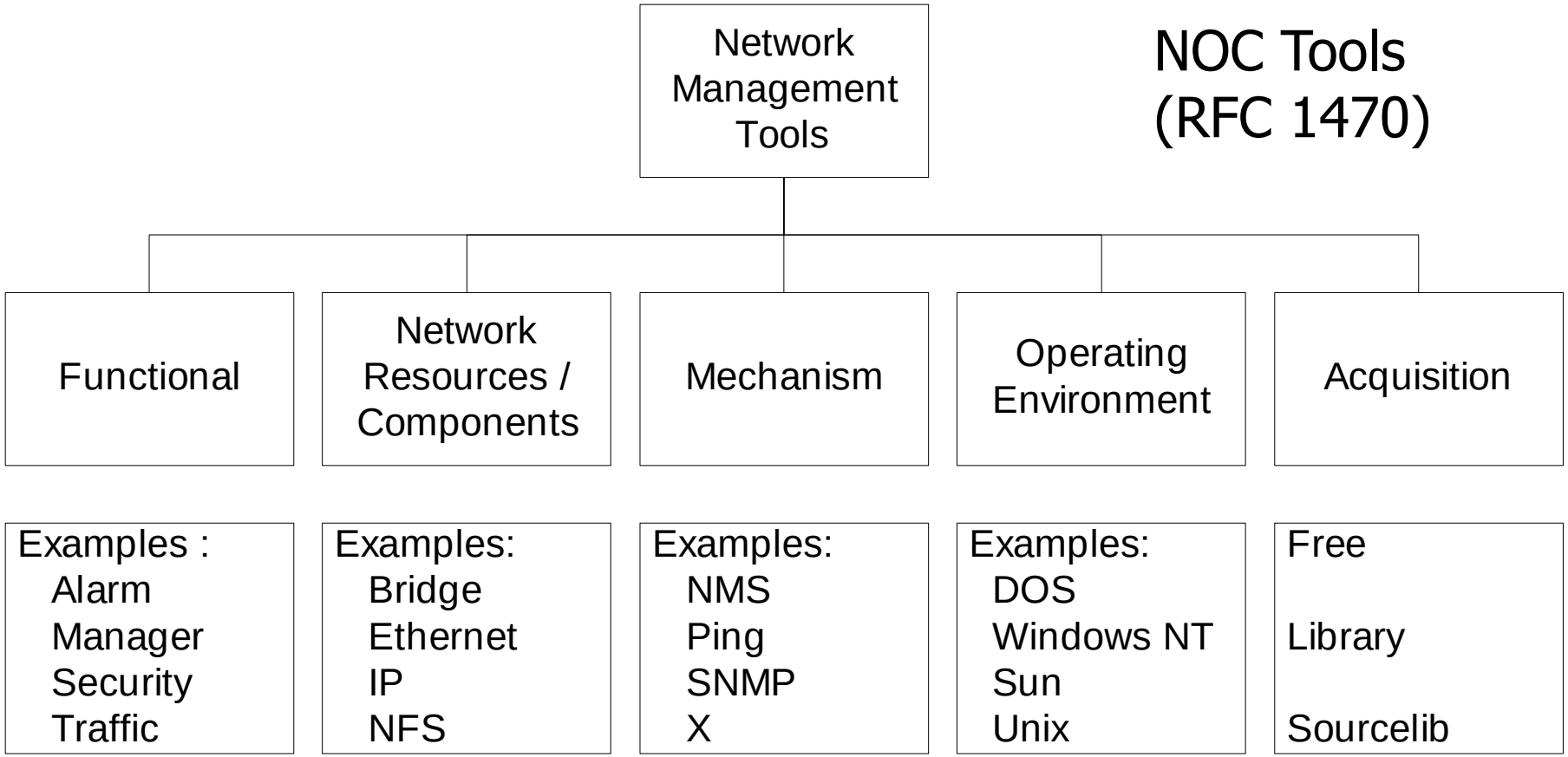
NM tools And Systems

Eng. Maha Jeha

NM Tools and Systems

1. Network Management Tools
2. Network Statistics Measurement Systems
3. Network Management Systems
4. System Management
5. Enterprise Management Systems

1. Network Management Tools

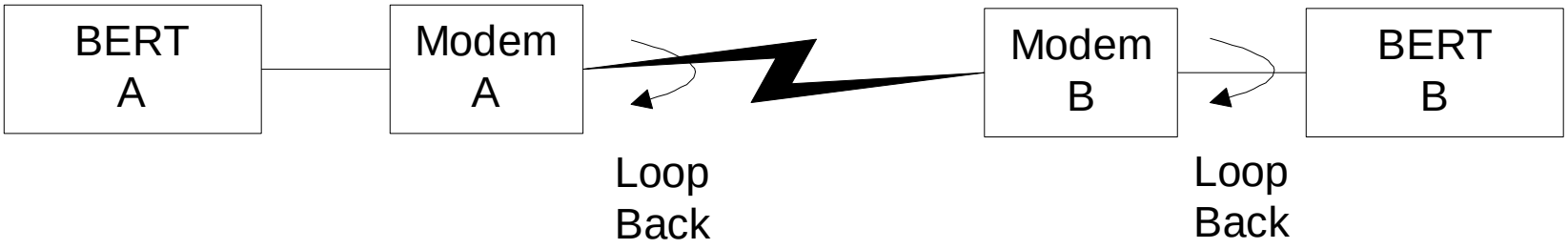


ftp://wuarchive.wustl.edu/doc/noctools/

Network Monitoring Tools

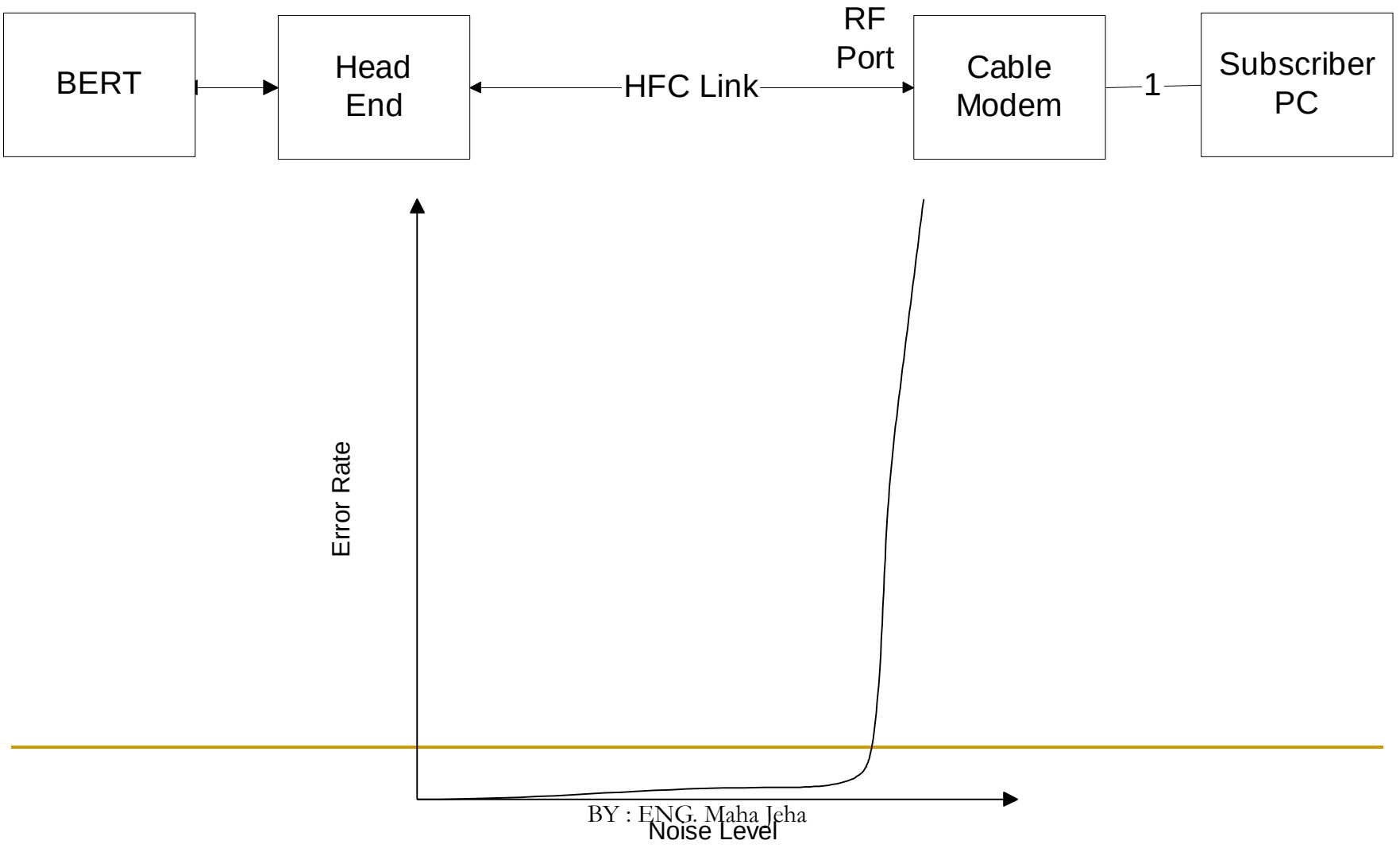
- SLAC, Stanford University
  - http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
- www.SNMPLink.org
  - http://www.snmplink.org/Tools.html
- ***SimpleWeb***
  - http://www.simpleweb.org/software/

Bit Error Rate Tester



- Physical layer monitoring tool
- Important for WAN and Broadband access
- Generates and detects bits
- Bit error rate (BER) is calculated by comparing the transmitted pattern with received pattern
- BER can be measured for a modem or two modems and the link in between

BERT in HFC / LAN Environment



Status Monitoring Tools

Table 12.5 Status Monitoring Tools

NAME	OPERATING SYSTEM	DESCRIPTION
Ifconfig	UNIX	Obtains and configures networking interface parameters and status
ping	UNIX Windows	Checks the status of node / host
nslookup	UNIX Windows NT	Looks up DNS for name-IP address translation
dig	UNIX	Queries DNS server
host	UNIX	Displays information on Internet hosts / domains

ifconfig

- Used to assign/read an address to/of an interface
- Option -a is to display all interfaces
- Notice two interface loop-back (lo0) and Ethernet (le0)

```
[/home/teachers/ycchen]ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
le0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 163.22.20.16 netmask ffffff00 broadcast 163.22.20.255
```

ifconfig le0 down
ifconfig le0 163.22.20.16 netmask 255.255.255.0 broadcast 163.22.20.255

Ping

- Most basic tool for internet management
- Based on ICMP ECHO_REQUEST message
- Available on all TCP/IP stacks
- Useful for measuring
  - Connectivity
  - Packet loss rate
  - Round trip time
- Can do auto-discovery of TCP/IP equipped stations on single segment

nslookup

- An interactive program for querying Internet Domain Name System servers
- Converts a hostname into an IP address and vice versa querying DNS
- Useful to identify the subnet a host or node belongs to
- Lists contents of a domain, displaying DNS record

Traffic Monitoring Tools

Name	Operating System	Description
ping	UNIX Windows	Used for measuring roundtrip packet loss
bing	UNIX	Measures point-to-point bandwidth of a link
etherfind	UNIX	Inspects Ethernet packets
snoop	UNIX	Captures and inspects network packets
tcpdump	UNIX	Dumps traffic on a network
getethers	UNIX	Acquires all host addresses of an Ethernet LAN segment
iptrace	UNIX	Measures performance of gateways

Packet Loss Measurement

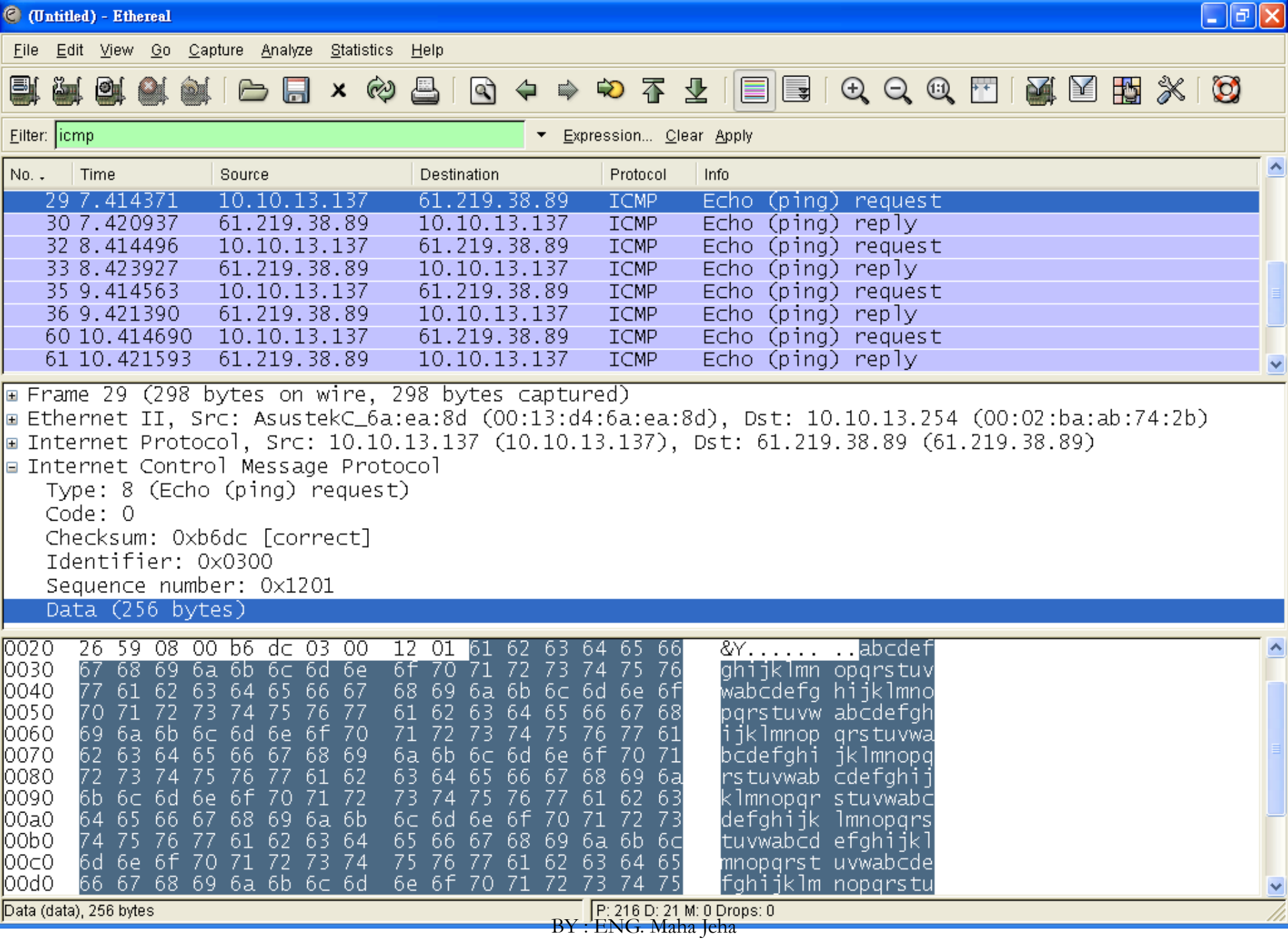
netman: ping -s mit.edu
PING mit.edu: 56 data bytes
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=0. time=42. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=1. time=41. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=2. time=41. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=3. time=40. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=4. time=40. ms

----mit.edu PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 40/40/42

ping

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] destination-list

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue -
                    type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

```
C:\>ping -n 10 -l 256 www.hinet.net

Pinging www.hinet.net [61.219.38.89] with 256 bytes of data:

Reply from 61.219.38.89: bytes=256 time=7ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=9ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=9ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=6ms TTL=242
Reply from 61.219.38.89: bytes=256 time=37ms TTL=242

Ping statistics for 61.219.38.89:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 37ms, Average = 9ms
```

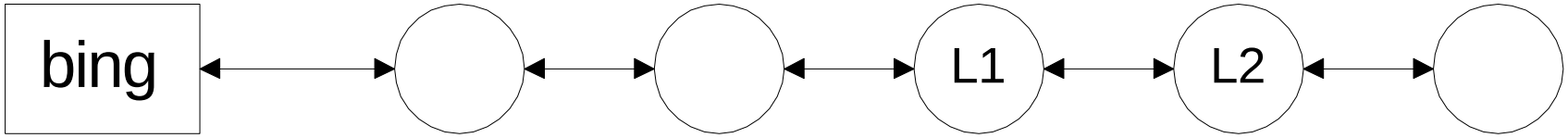


BY : ENG. Maha Jeha

```
C:\>ping -n 2 -r 5 www.ncnu.edu.tw

Pinging www.ncnu.edu.tw [163.22.4.67] with 32 bytes of data:

Reply from 163.22.4.67: bytes=32 time=2ms TTL=126
    Route: 10.10.1.248 ->
           163.22.4.254 ->
           163.22.4.67 ->
           163.22.1.253 ->
           10.10.13.254
Reply from 163.22.4.67: bytes=32 time=15ms TTL=126
    Route: 10.10.1.248 ->
           163.22.4.254 ->
           163.22.4.67 ->
           163.22.1.253 ->
           10.10.13.254

Ping statistics for 163.22.4.67:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 8ms
```

bing

bing 163.22.18.110 203.64.255.90



- Used to determine throughput of a link
- Uses icmp_echo utility
- Knowing packet size and delay, calculates bandwidth
- bing L1 and L2 and the difference yields the bandwidth of link L1-L2
- Bandwidth of link L1-L2 could be higher than the intermediate links.

ftp://ftp.funet.fi/pub/networking/management/bing-1.0.4.tar.gz

http://spengler.econ.duke.edu/~ferizs/bing.txt

snoop

- Puts a network interface in promiscuous mode
- Logs data on
  - Protocol type
  - Length
  - Source address
  - Destination address
  - Reading of user data limited to superuser

Network Routing Tools

Table 12.7 Route-Monitoring Tools

Name	Operating System	Description
netstat	UNIX / Windows	Displays the contents of various network-related data structures
arp rarp	UNIX, Windows 95/x/00NT	Displays and modifies the Internet-to-Ethernet address translation tables
traceroute tracert	UNIX Windows	Traces route to a destination with routing delays

netstat

```
C:\>netstat -n -a
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1234           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1235           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1236           0.0.0.0:0              LISTENING
  TCP    163.31.153.68:1234     163.22.3.4:80          ESTABLISHED
  TCP    163.31.153.68:1235     163.22.4.67:80         ESTABLISHED
  TCP    163.31.153.68:1236     163.22.4.67:80         SYN_SENT
  UDP    0.0.0.0:135                *:*
  UDP    0.0.0.0:445                *:*
  UDP    0.0.0.0:38037              *:*
  UDP    127.0.0.1:1230             *:*
  UDP    163.31.153.68:500          *:*
```

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

-a Displays all connections and listening ports.

-e Displays Ethernet statistics. This may be combined with the -s option.

-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

C:\>**netstat -s -p TCP**

TCP Statistics for IPv4

```
  Active Opens                            = 904
  Passive Opens                           = 13
  Failed Connection Attempts              = 25
  Reset Connections                       = 189
  Current Connections                     = 3
  Segments Received                       = 61946
  Segments Sent                           = 53891
  Segments Retransmitted                  = 249
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	94ASUS3705:1502	euler.im.ncnu.edu.tw:telnet	ESTABLISHED
TCP	94ASUS3705:1976	giant.ccserver.ncnu.edu.tw:epmap	TIME_WAIT
TCP	94ASUS3705:1977	giant.ccserver.ncnu.edu.tw:1025	TIME_WAIT
TCP	94ASUS3705:1980	giant.ccserver.ncnu.edu.tw:1025	TIME_WAIT
TCP	94ASUS3705:1981	giant.ccserver.ncnu.edu.tw:1025	TIME_WAIT
TCP	94ASUS3705:1982	giant.ccserver.ncnu.edu.tw:ldap	TIME_WAIT
TCP	94ASUS3705:1984	giant.ccserver.ncnu.edu.tw:ldap	TIME_WAIT
TCP	94ASUS3705:1985	giant.ccserver.ncnu.edu.tw:microsoft-ds	TIME_WAIT
TCP	94ASUS3705:1990	giant.ccserver.ncnu.edu.tw:ldap	TIME_WAIT
TCP	94ASUS3705:4558	localhost:4559	ESTABLISHED
TCP	94ASUS3705:4559	localhost:4558	ESTABLISHED

C:\>**netstat -b**

```
C:\> netstat -b -v
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	94ASUS3705:1502	euler.im.ncnu.edu.tw:telnet	ESTABLISHED	528
[telnet.exe]				
TCP	94ASUS3705:2136	66.102.7.99:http	ESTABLISHED	988
[firefox.exe]				
TCP	94ASUS3705:2176	216.239.57.99:http	ESTABLISHED	988
[firefox.exe]				
TCP	94ASUS3705:2181	ip172.puli04.ncnu.edu.tw:554	ESTABLISHED	3016
[wmplayer.exe]				
TCP	94ASUS3705:4558	localhost:4559	ESTABLISHED	988
[firefox.exe]				
TCP	94ASUS3705:4559	localhost:4558	ESTABLISHED	988
[firefox.exe]				

C:\>**netstat -r**

```
C:\> route print
```

Route Table

==========

Interface List

0x1 ..... MS TCP Loopback interface

0x10003 ...00 12 f0 9c 1d 2e ..... Intel(R) PRO/Wireless 2200BG Network Connection

0x10004 ...00 13 d4 6a ea 8d ..... Realtek RTL8139 Family PCI Fast Ethernet NIC

==========

==========

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.10.13.254	10.10.13.137	20
10.10.13.0	255.255.255.0	10.10.13.137	10.10.13.137	20
10.10.13.137	255.255.255.255	127.0.0.1	127.0.0.1	20
10.255.255.255	255.255.255.255	10.10.13.137	10.10.13.137	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	10.10.13.137	10.10.13.137	20
255.255.255.255	255.255.255.255	10.10.13.137	10.10.13.137	1
255.255.255.255	255.255.255.255	10.10.13.137	10003	1

Default Gateway: 10.10.13.254

==========

Persistent Routes:

None

traceroute/tracert

tracert www.hinet.net

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

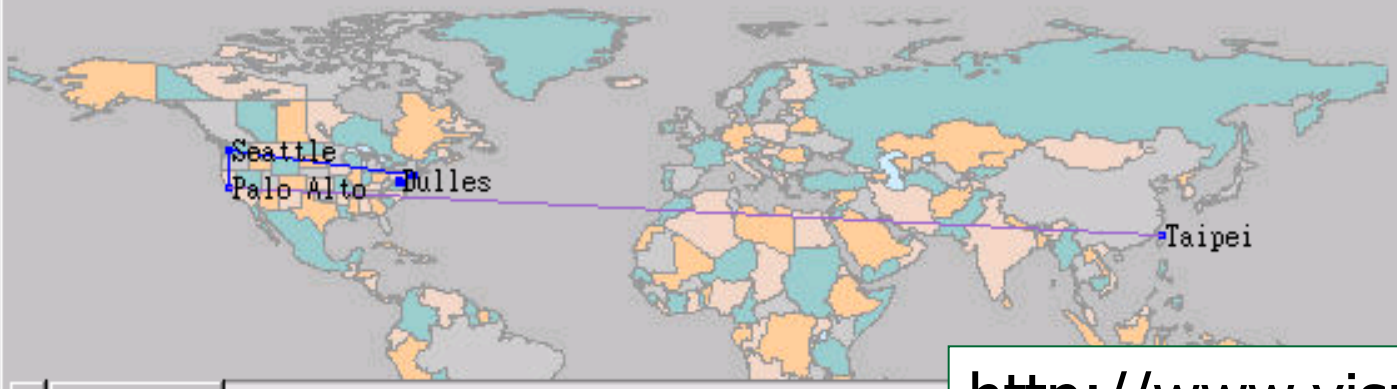
-d	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target.
-j host-list	Loose source route along host-list.
-w timeout	Wait timeout milliseconds for each reply.

```
C:\>tracert www.yahoo.co.jp

Tracing route to www.yahoo.co.jp [203.216.247.225]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  gateway.puli13-10-10.ncnu.edu.tw [10.10.13.254]
  2    <1 ms     1 ms    <1 ms  ip253.puli01.ncnu.edu.tw [163.22.1.253]
  3    <1 ms    <1 ms    <1 ms  ip105.puli18-10-10.ncnu.edu.tw [10.10.18.105]
  4    <1 ms    <1 ms    <1 ms  ip110.puli18.ncnu.edu.tw [163.22.18.110]
  5     2 ms     1 ms     1 ms  ip098.puli255-64-203.ncnu.edu.tw [203.64.255.98]
  6     6 ms     3 ms     3 ms  140.128.251.38
  7     3 ms     3 ms     2 ms  10G-10GE-CHT-P1.TCC-NCHUE.twaren.net [211.79.60.145]
  8     4 ms     4 ms     5 ms  10G-POS-CHT-P1.HCC-TCC.twaren.net [211.79.59.161]
  9     6 ms     6 ms     6 ms  10G-POS-CHT-P1.TPC-HCC.twaren.net [211.79.59.154]
 10     6 ms     6 ms     6 ms  211.79.59.98
 11    56 ms    19 ms     6 ms  202.169.174.58
 12    59 ms    60 ms    60 ms  202.169.174.41
 13    66 ms    74 ms    70 ms  AS9607-2.ix.jpix.ad.jp [210.171.224.205]
 14    62 ms    61 ms    62 ms  ge-1-0-0.edge09.colo01.bbtower.ad.jp [211.14.3.200]
 15    60 ms    62 ms    61 ms  yahoo-7.demarc.colo01.bbtower.ad.jp [211.14.30.1]
 16    62 ms    62 ms    60 ms  202.93.95.194
 17    60 ms    60 ms    60 ms  203.216.238.154
 18    63 ms    60 ms    62 ms  f6.top.vip.tnz.yahoo.co.jp [203.216.247.225]

Trace complete.
```

VisualRoute from win10115.iad.dn.net

Enter Host/URL: www.im.ncnu.edu.tw <-- 163.31.153.68 Stop Snap... *

Ho	%Lc	IP Address	Node Name	Location	ms	Graph	Network
0		161.58.180.113	win10115.iad.dn.net	Dulles, VA,		0 438	Verio, Inc.
1		161.58.176.129	-	Englewood,	0		Verio, Inc.
2		161.58.156.140	-	Englewood,	64		Verio, Inc.
3		129.250.27.190	ge-1-3-0.r00.stngva01.us.bb.	Sterling, V.	0		Verio, Inc.
4		129.250.2.145	p4-2-3.r02.mclnva01.us.bb.ve	Mclean, VA,	0		Verio, Inc.
5		209.133.31.105	above-verio-oc3.iad.above.ne	Vienna, VA,	0		Abovenet Communications, Inc.
6		208.185.0.142	core4-core3-oc48.iad1.above.	Vienna, VA,	0		Abovenet Communications, Inc.
7		208.184.233.62	lga1-iad1-oc192-2.lga1.above	New York, N	0		Abovenet Communications, Inc.
8		216.200.127.66	sea1-lga1-oc48.sea1.above.ne	Seattle, WA	62		Abovenet Communications, Inc.
9		64.125.31.94	main1-core3-oc48.sea4.above.	Seattle, WA	62		Abovenet Communications, Inc.
10		216.200.249.94	ixnet-abovenet.pao1.above.ne	Palo Alto,	147		Abovenet Communications, Inc.
11	10	210.70.55.17	Internet-TANet.edu.tw	Taipei, Tai	276		TAKMING JUNIOR COLLEGE OF COMMERCE
12	30	203.72.38.120	TANet-NCHU.edu.tw	(Taiwan)	268		CHIAO TUNG UNIVERSITY
13	30	140.128.248.253	rsp8.nchu.edu.tw	(Taiwan)	355		Ministry of Education Computer Center
14	30	140.128.254.13	-	(Taiwan)	299		Ministry of Education Computer Center
15	30	163.22.49.22	-	(Taiwan)	328		Ministry of Education Computer Center
16	30	203.64.255.105	ip105.puli255-64-203.ncnu.ed	(Taiwan)	365		National Chi Nan University
17	20	203.64.255.97	ip097.puli255-64-203.ncnu.ed	(Taiwan)	338		National Chi Nan University
18	50	163.22.1.252	ip252.puli01.ncnu.edu.tw	(Taiwan)	336		Ministry of Education Computer Center
19	20	163.22.20.16	www.im.ncnu.edu.tw	(Taiwan)	339		Ministry of Education Computer Center



http://www.visualroute.com/

警告: Applet 視窗

BY : ENG. Maha Jeha

Network Management Tools

- SNMP command tools
- MIB Walk
- MIB Browser
- snmpsniff

SNMP Command Tools

- snmptest
- snmpget
- snmpgetnext
- snmpset
- snmptrap
- snmpwalk
- snmpnetstat

Network Status

- Command: snmpnetstat host community
- Useful for finding status of network connections

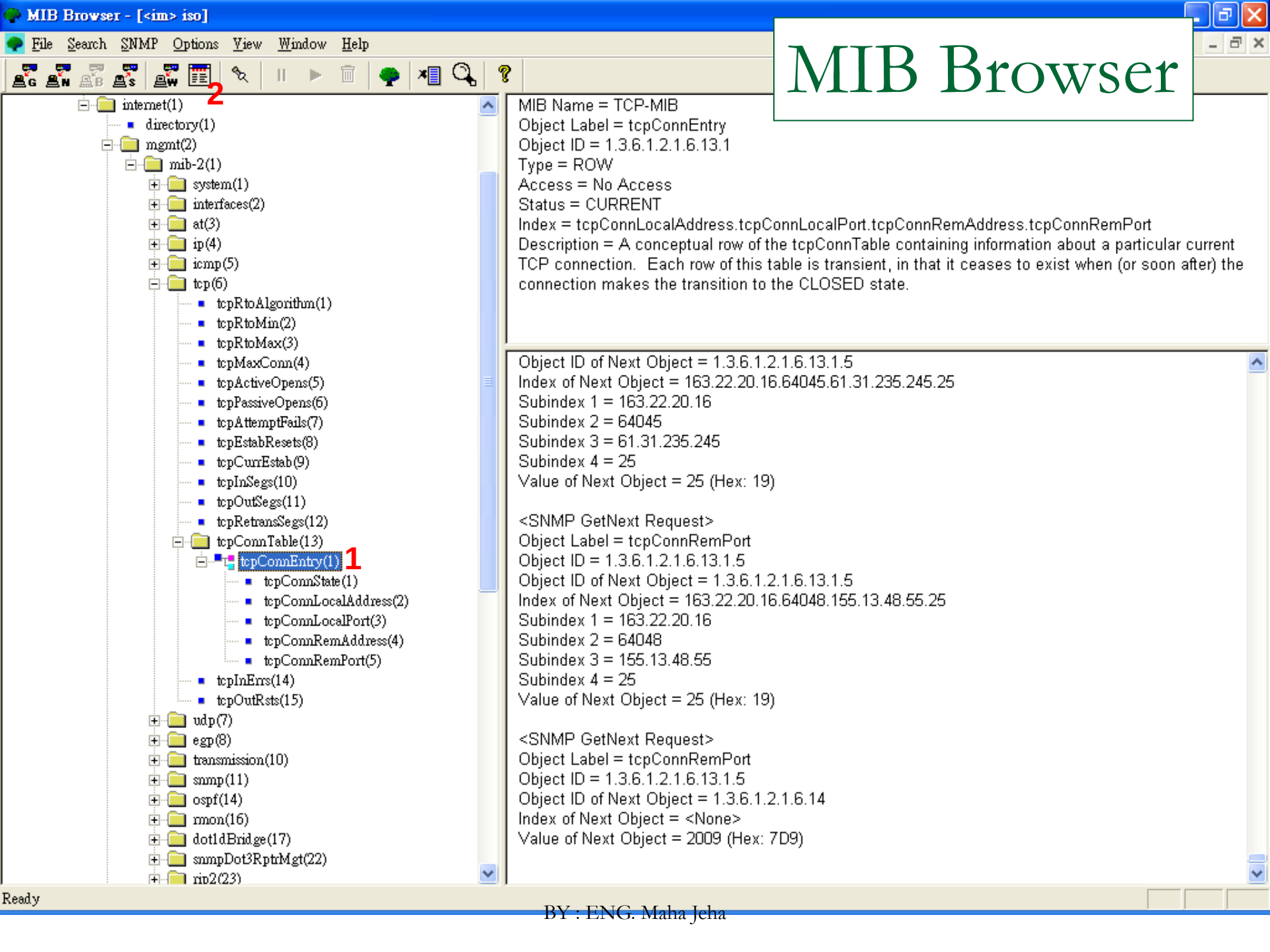
```
% snmpnetstat noc5 public
Active Internet Connections
Proto Recv-Q Send-Q  Local Address Foreign Address (state)
tcp   0  0        *.*                *.*                CLOSED
tcp   0  0  localhost.46626   localhost.3456     ESTABLISHED
tcp   0  0  localhost.46626   localhost.3712     ESTABLISHED
tcp   0  0  localhost.46626   localhost.3968     ESTABLISHED
tcp   0  0  localhost.46626   localhost.4224     ESTABLISHED
tcp   0  0  localhost.3456    localhost.46626    ESTABLISHED
tcp   0  0  localhost.3712    localhost.46626    ESTABLISHED
tcp   0  0  localhost.3968    localhost.46626    ESTABLISHED
tcp   0  0  localhost.4224    localhost.46626    ESTABLISHED
tcp   0  0  noc5.41472        noc5.4480          ESTABLISHED
tcp   0  0  noc5.41472        noc5.4736          ESTABLISHED
tcp   0  0  noc5.4480         noc5.41472         ESTABLISHED
tcp   0  0  noc5.4736         noc5.41472         ESTABLISHED
```

SNMP Browser

- Command: snmpwalk host community [variable name]
- Uses Get Next Command
- Presents MIB Tree

SNMP Sniff

- *snmpsniff -I interface*
- A tool in Linux / FreeBSD environment
- Puts the interface in promiscuous mode and captures snmp PDUs.
- Similar to *tcpdump*


MIB Browser - [<im> iso]
File Search SNMP Options View Window Help
2
internet(1)
directory(1)
mgmt(2)
mib-2(1)
system(1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
tcpRtoAlgorithm(1)
tcpRtoMin(2)
tcpRtoMax(3)
tcpMaxConn(4)
tcpActiveOpens(5)
tcpPassiveOpens(6)
tcpAttemptFails(7)
tcpEstabResets(8)
tcpCurrEstab(9)
tcpInSegs(10)
tcpOutSegs(11)
tcpRetransSegs(12)
tcpConnTable(13)
tcpConnEntry(1)
1
tcpConnState(1)
tcpConnLocalAddress(2)
tcpConnLocalPort(3)
tcpConnRemAddress(4)
tcpConnRemPort(5)
tcpInErrs(14)
tcpOutRsts(15)
udp(7)
egp(8)
transmission(10)
snmp(11)
ospf(14)
rmon(16)
dot1dBridge(17)
snmpDot3RptrMgt(22)
rip2(23)
MIB Name = TCP-MIB
Object Label = tcpConnEntry
Object ID = 1.3.6.1.2.1.6.13.1
Type = ROW
Access = No Access
Status = CURRENT
Index = tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort
Description = A conceptual row of the tcpConnTable containing information about a particular current TCP connection. Each row of this table is transient, in that it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state.
Object ID of Next Object = 1.3.6.1.2.1.6.13.1.5
Index of Next Object = 163.22.20.16.64045.61.31.235.245.25
Subindex 1 = 163.22.20.16
Subindex 2 = 64045
Subindex 3 = 61.31.235.245
Subindex 4 = 25
Value of Next Object = 25 (Hex: 19)
<SNMP GetNext Request>
Object Label = tcpConnRemPort
Object ID = 1.3.6.1.2.1.6.13.1.5
Object ID of Next Object = 1.3.6.1.2.1.6.13.1.5
Index of Next Object = 163.22.20.16.64048.155.13.48.55.25
Subindex 1 = 163.22.20.16
Subindex 2 = 64048
Subindex 3 = 155.13.48.55
Subindex 4 = 25
Value of Next Object = 25 (Hex: 19)
<SNMP GetNext Request>
Object Label = tcpConnRemPort
Object ID = 1.3.6.1.2.1.6.13.1.5
Object ID of Next Object = 1.3.6.1.2.1.6.14
Index of Next Object = <None>
Value of Next Object = 2009 (Hex: 7D9)
Ready

MIB Browser

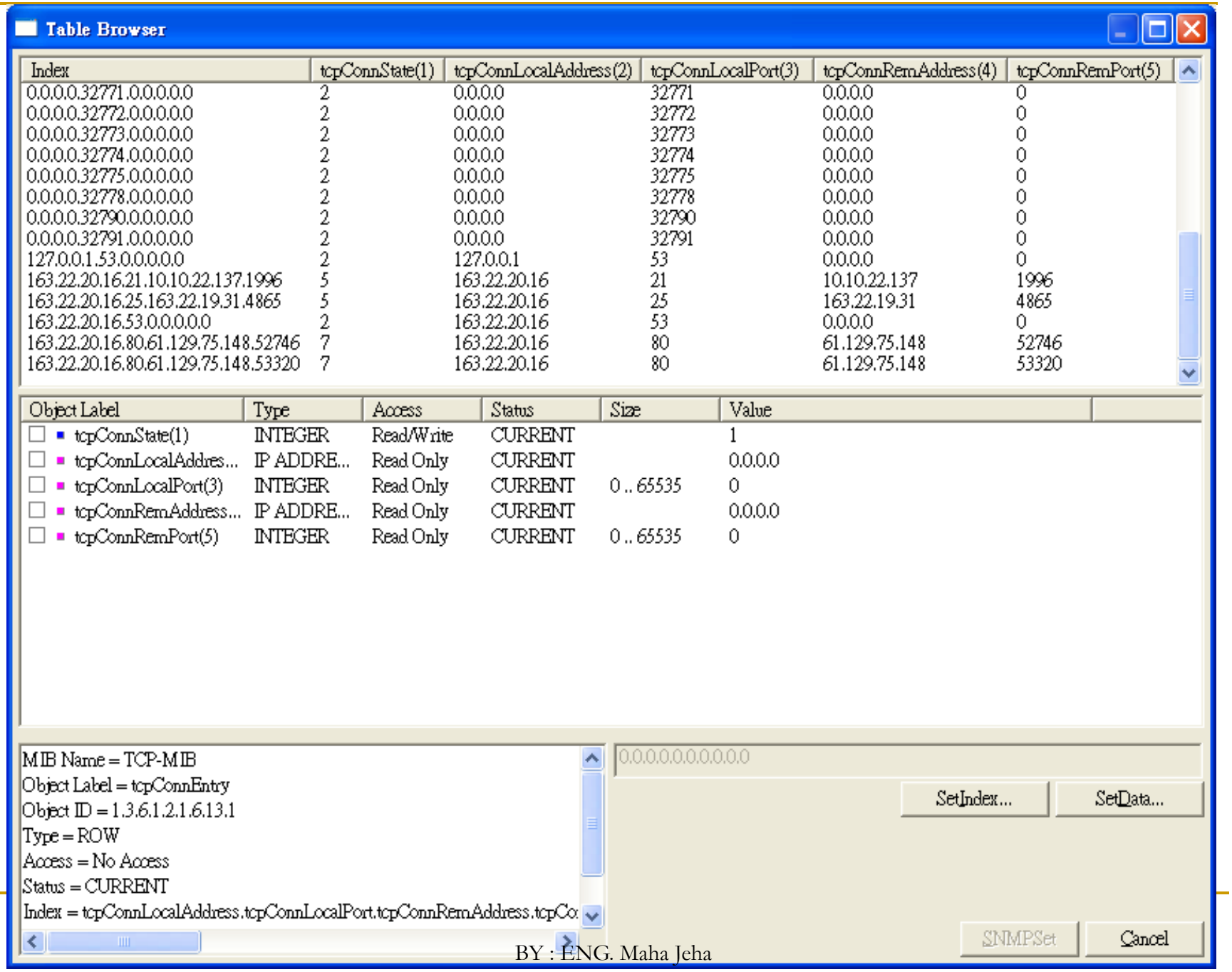
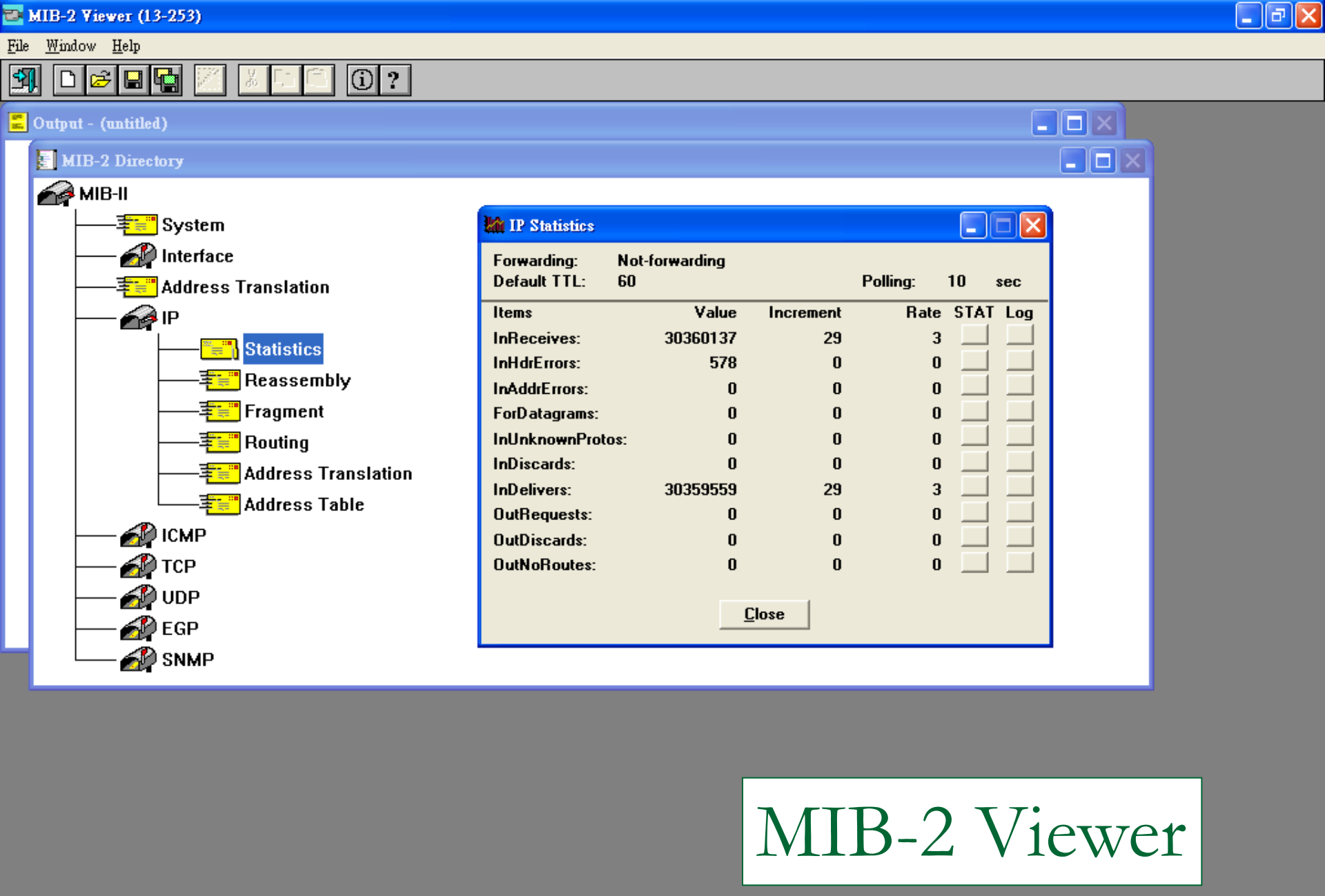


Table Browser
Index
tcpConnState(1)
tcpConnLocalAddress(2)
tcpConnLocalPort(3)
tcpConnRemAddress(4)
tcpConnRemPort(5)
0.0.0.0.32771.0.0.0.0.0
2
0.0.0.0
32771
0.0.0.0
0
0.0.0.0.32772.0.0.0.0.0
2
0.0.0.0
32772
0.0.0.0
0
0.0.0.0.32773.0.0.0.0.0
2
0.0.0.0
32773
0.0.0.0
0
0.0.0.0.32774.0.0.0.0.0
2
0.0.0.0
32774
0.0.0.0
0
0.0.0.0.32775.0.0.0.0.0
2
0.0.0.0
32775
0.0.0.0
0
0.0.0.0.32778.0.0.0.0.0
2
0.0.0.0
32778
0.0.0.0
0
0.0.0.0.32790.0.0.0.0.0
2
0.0.0.0
32790
0.0.0.0
0
0.0.0.0.32791.0.0.0.0.0
2
0.0.0.0
32791
0.0.0.0
0
127.0.0.1.53.0.0.0.0.0
2
127.0.0.1
53
0.0.0.0
0
163.22.20.16.21.10.10.22.137.1996
5
163.22.20.16
21
10.10.22.137
1996
163.22.20.16.25.163.22.19.31.4865
5
163.22.20.16
25
163.22.19.31
4865
163.22.20.16.53.0.0.0.0.0
2
163.22.20.16
53
0.0.0.0
0
163.22.20.16.80.61.129.75.148.52746
7
163.22.20.16
80
61.129.75.148
52746
163.22.20.16.80.61.129.75.148.53320
7
163.22.20.16
80
61.129.75.148
53320
Object Label
Type
Access
Status
Size
Value
tcpConnState(1)
INTEGER
Read/Write
CURRENT
1
tcpConnLocalAddres...
IP ADDRE...
Read Only
CURRENT
0.0.0.0
tcpConnLocalPort(3)
INTEGER
Read Only
CURRENT
0 .. 65535
0
tcpConnRemAddress...
IP ADDRE...
Read Only
CURRENT
0.0.0.0
tcpConnRemPort(5)
INTEGER
Read Only
CURRENT
0 .. 65535
0
MIB Name = TCP-MIB
Object Label = tcpConnEntry
Object ID = 1.3.6.1.2.1.6.13.1
Type = ROW
Access = No Access
Status = CURRENT
Index = tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpCo
0.0.0.0.0.0.0.0.0.0
SetIndex...
SetData...
SNMPSet
Cancel

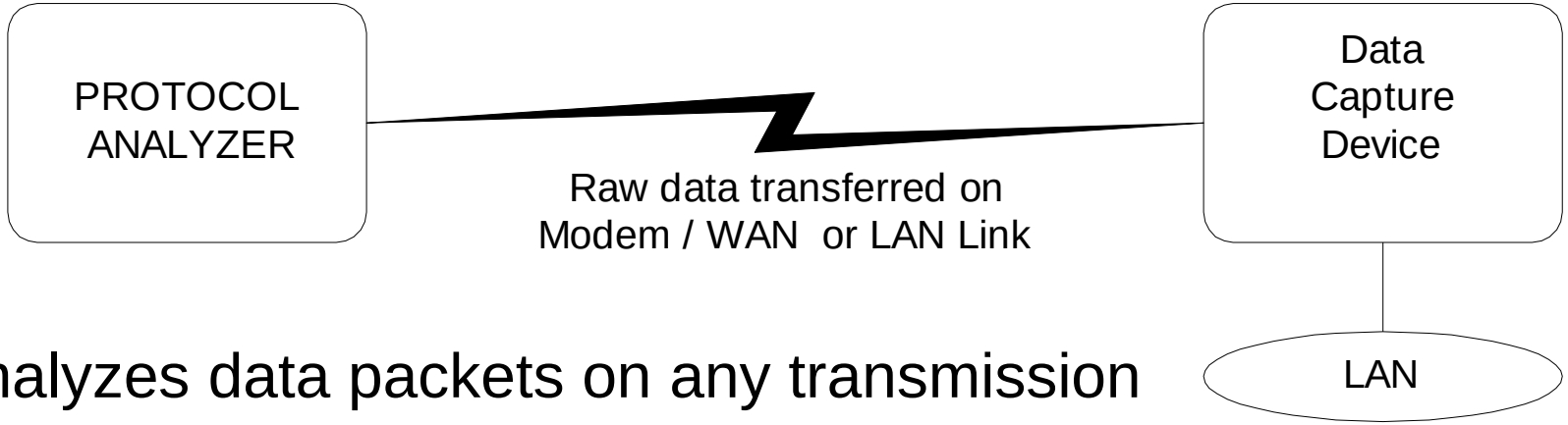

MIB-2 Viewer (13-253)
File Window Help
Output - (untitled)
MIB-2 Directory
MIB-II
System
Interface
Address Translation
IP
Statistics
Reassembly
Fragment
Routing
Address Translation
Address Table
ICMP
TCP
UDP
EGP
SNMP
IP Statistics
Forwarding: Not-forwarding
Default TTL: 60
Polling: 10 sec
Items Value Increment Rate STAT Log
InReceives: 30360137 29 3
InHdrErrors: 578 0 0
InAddrErrors: 0 0 0
ForDatagrams: 0 0 0
InUnknownProtos: 0 0 0
InDiscards: 0 0 0
InDelivers: 30359559 29 3
OutRequests: 0 0 0
OutDiscards: 0 0 0
OutNoRoutes: 0 0 0
Close

MIB-2 Viewer

SMC EliteView

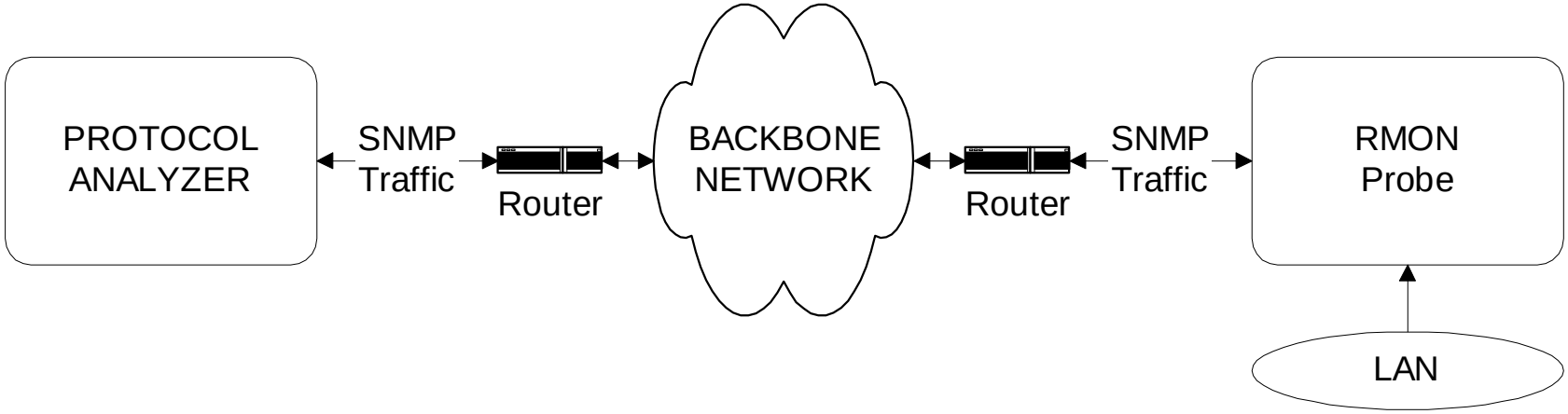
- EliteView
  - http://www.im.ncnu.edu.tw/~ycchen/nm/EliteView.zip

Protocol Analyzer



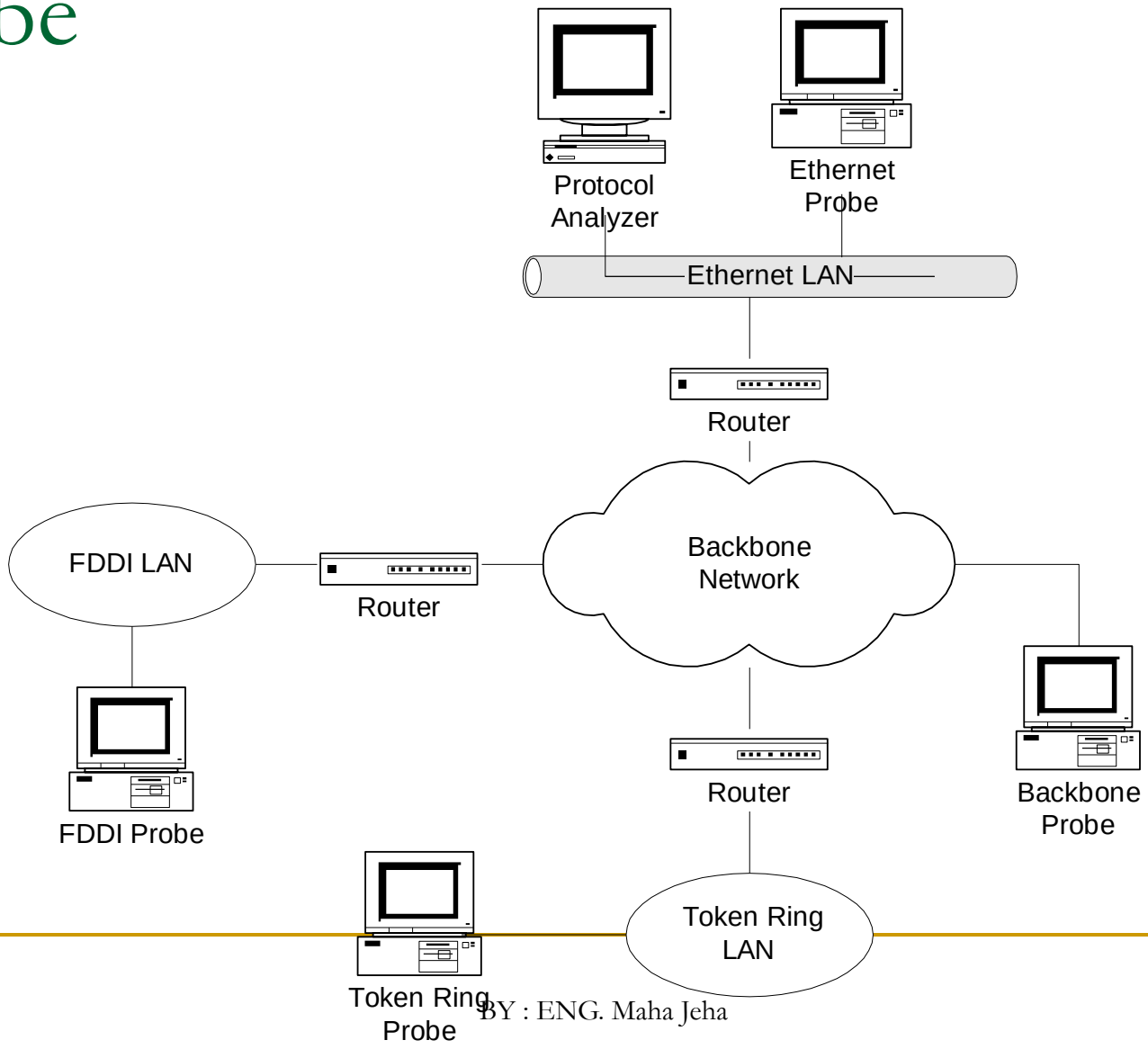
- Analyzes data packets on any transmission line including LAN
- Measurements made locally or remotely
- **Probe** (data capture device) captures data and transfers to the protocol analyzer (no storage)
- Data link between probe and protocol analyzer either dial-up or dedicated link or LAN
- Protocol analyzer analyzes data at all protocol levels

RMON Probe



- Communication between probe and analyzer is using SNMP
- Data gathered and stored for an extended period of time and analyzed later
- Used for gathering traffic statistics and used for configuration management for performance tuning

Network Monitoring with RMON Probe



Network Statistics

- Protocol Analyzers
- RMON Probe / Protocol analyzer
- MRTG (Multi router traffic grouper)
- Home-grown program using *tcpdump*

History: All (10.10.22.18)

File Polling View Control! Help

Polling done

	Sample Idx	Interval Start	Drops	Bytes	Packets	Broadcasts	Multicasts	CRC/Aligns	Undersizes
34	18462	2006/5/26 00:27:58	0	172010	823	159	14	0	
35	18463	2006/5/26 00:28:28	0	182564	1066	136	13	0	
36	18464	2006/5/26 00:28:59	0	176808	1058	147	31	0	
37	18465	2006/5/26 00:29:29	0	165675					
38	18466	2006/5/26 00:29:59	0	152619					
39	18467	2006/5/26 00:30:30	0	178769					
40	18468	2006/5/26 00:31:00	0	182645					
41	18469	2006/5/26 00:31:31	0	205430					
42	18470	2006/5/26 00:32:01	0	209947					
43	18471	2006/5/26 00:32:32	0	173539					
44	18472	2006/5/26 00:33:02	0	163971					
45	18473	2006/5/26 00:33:33	0	170199					
46	18474	2006/5/26 00:34:03	0	166988					
47	18475	2006/5/26 00:34:33	0	172809					
48	18476	2006/5/26 00:35:04	0	174563					

History: Control Table

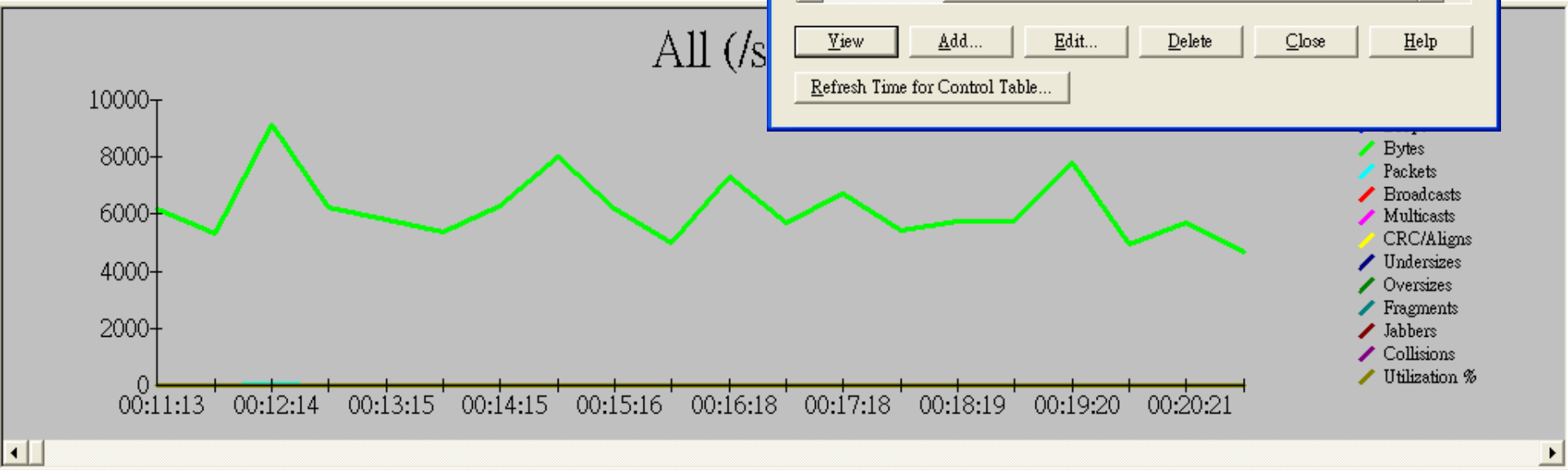
Total: 48 Read Status: Done

Control Table:

(I)ndex /	(O)wner	Requested	Granted	Interval	Status
1	monitor	50	50	30	Valid
2	monitor	50	50	1800	Valid
3	monitor	50	50	30	Valid
4	monitor	50	50	1800	Valid
5	monitor	50	50	30	Valid
6	monitor	50	50	1800	Valid
7	monitor	50	50	30	Valid

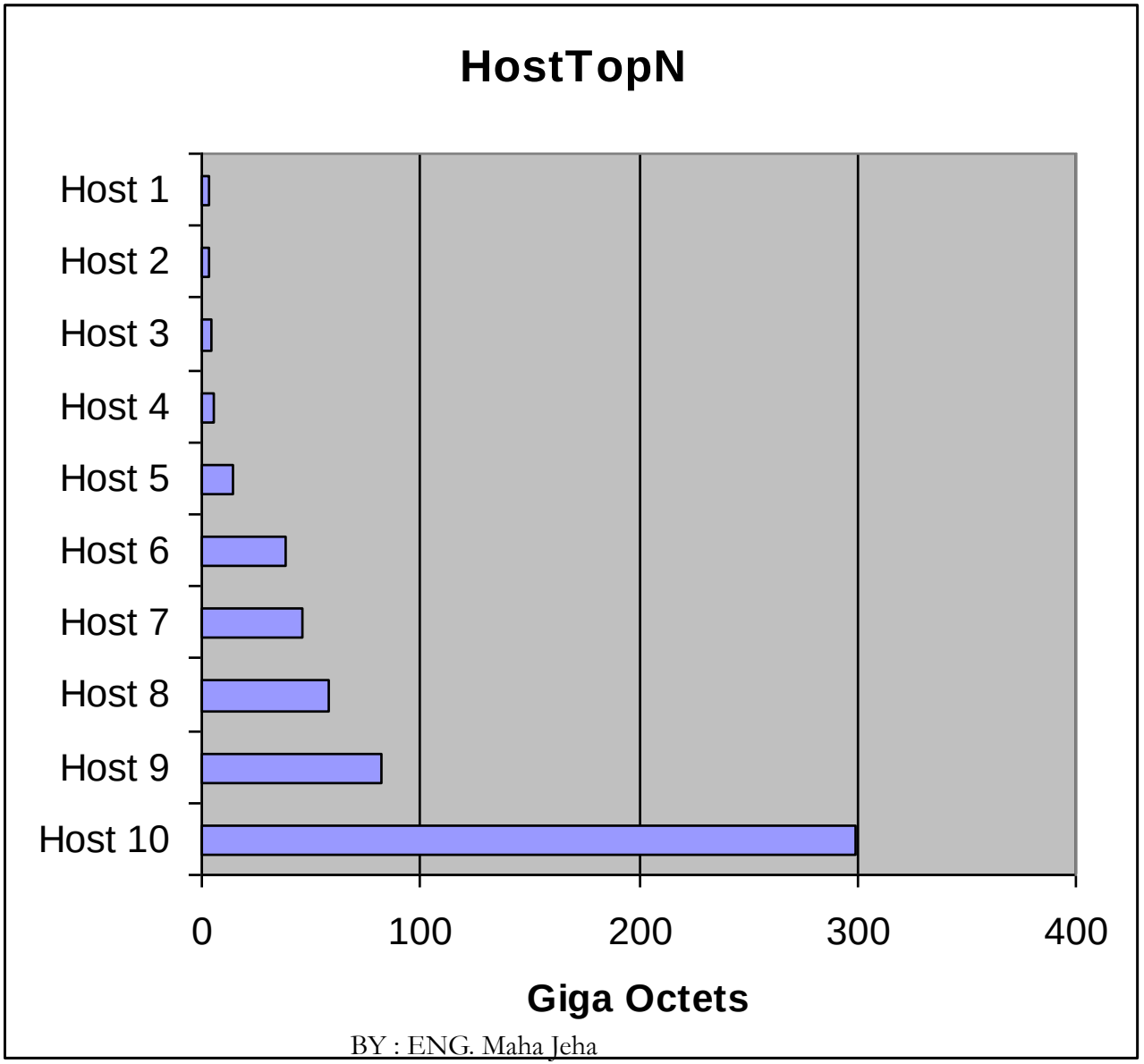
View Add... Edit... Delete Close Help

Refresh Time for Control Table...

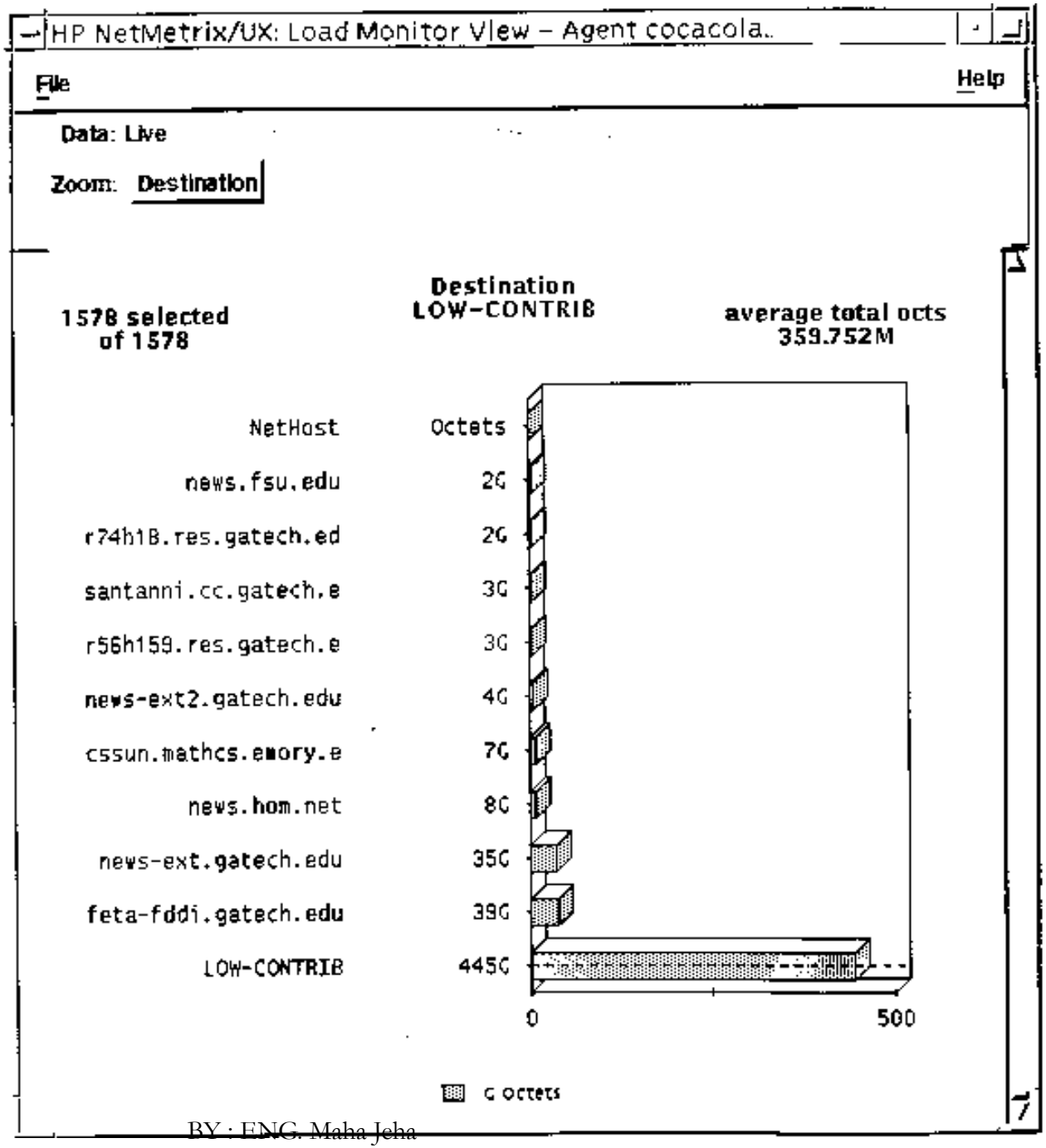


Ready | Control Index: 1 | Interface: 1 | Interval: 30 | Speed: 100 M | Owner: monitor

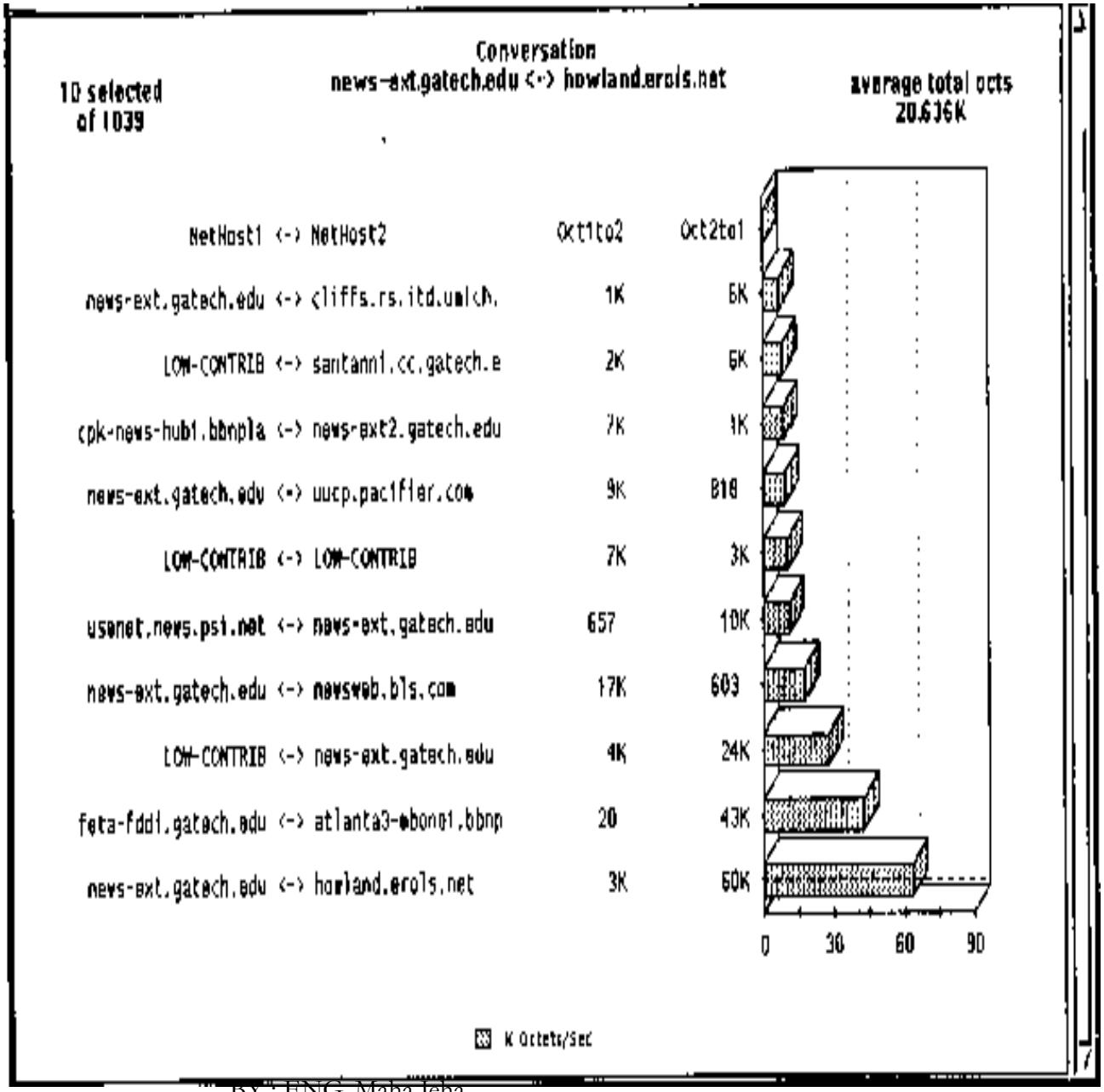
Traffic Load: Source



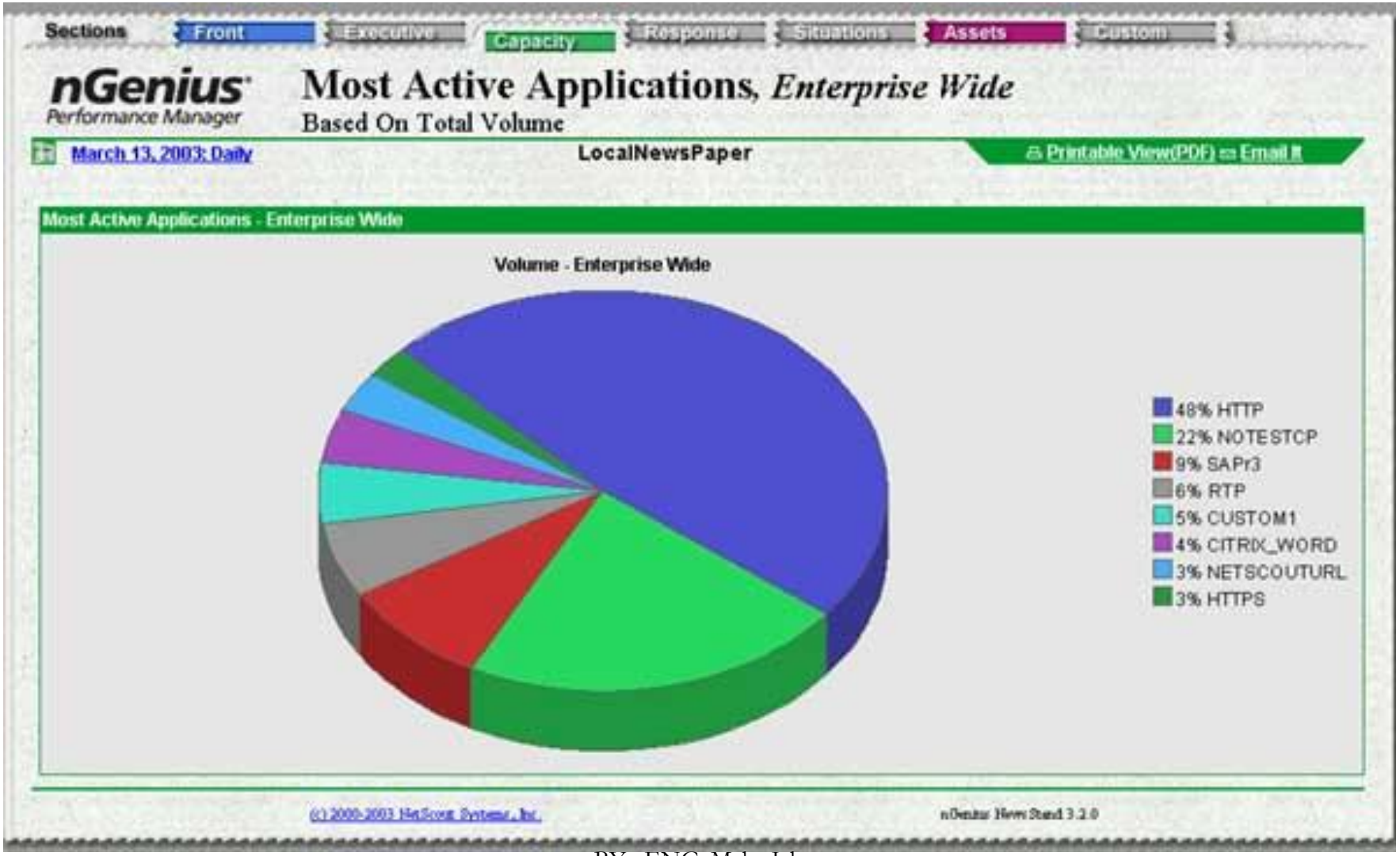
Traffic Load: Destination



Traffic Load: Conversation



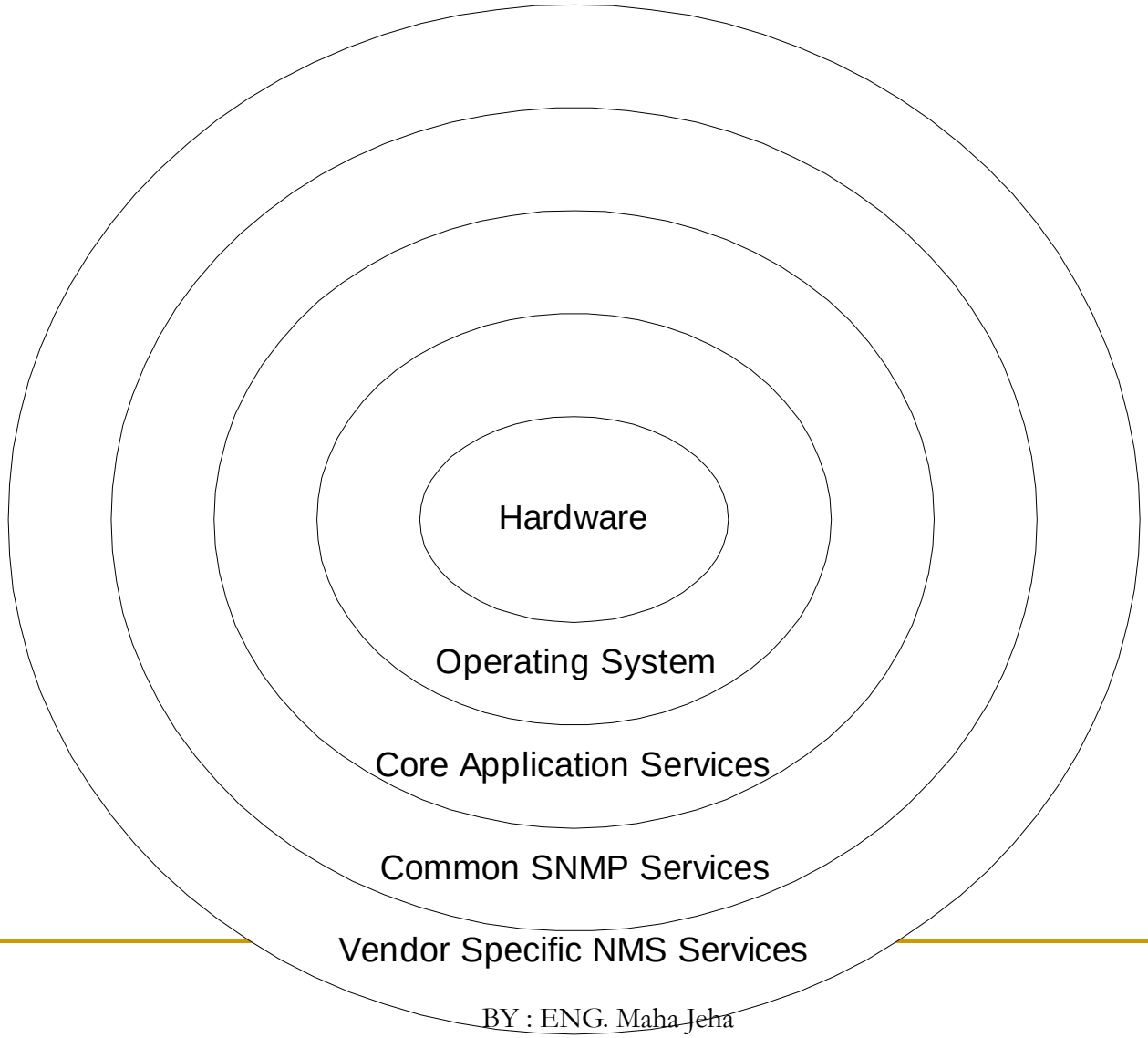
Protocol Distribution



Enterprise Management

- Management of data transport
  - IBM Netview, Sun Solstice, HP OpenView, Cabletron Spectrum
- Systems management
  - CA Unicenter and Tivoli TME
- Network and systems management
  - Partnerships
- Telecommunications management
  - TMN, Operations systems
- Service management and policy management

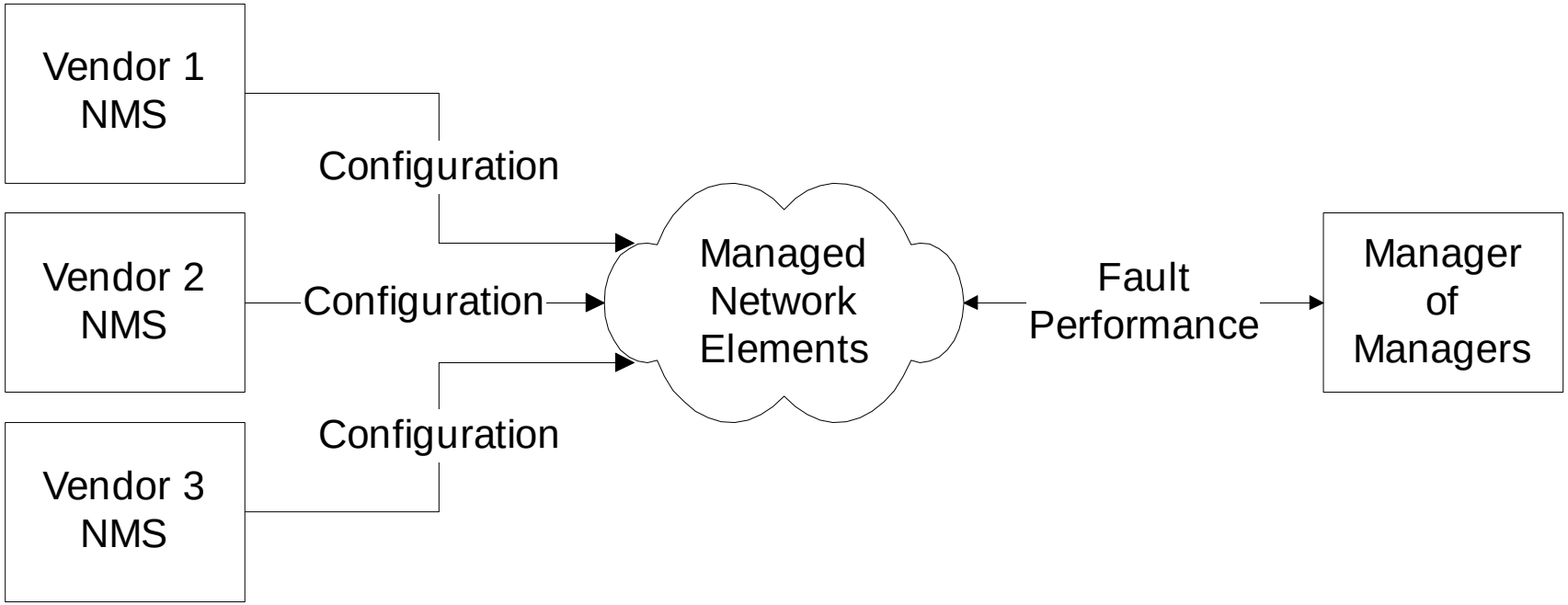
NMS Components



NMS Components

Component	Service	Example
Hardware	Processor Monitor Mouse and Keyboard Communications	Sun Sparc HP 9000 PC
Operating system	OS services	UNIX LINUX / FreeBSD Solaris MS Windows 95 / 98 / NT
Core application services	Display GUI Database Report generation Communication services	OpenView SunNet Manager Solstice Enterprise Manager MS Windows
Common SNMP services	SNMPv1 messages SNMPv2 messages MIB management Basic SNMP applications 3rd party NMS API	SNMPc OpenView Network Node Manager Cabletron Spectrum Enterprise Manager IBM NetView SunNet Manager Solstice Enterprise Manager
Vendor-specific NMS services	MIB management SNMP applications	CiscoWorks Transcend
	Config. management Physical entity display	Spectrum Element Manager / Spectrum Portable Management Application

Multi-NMS Configuration



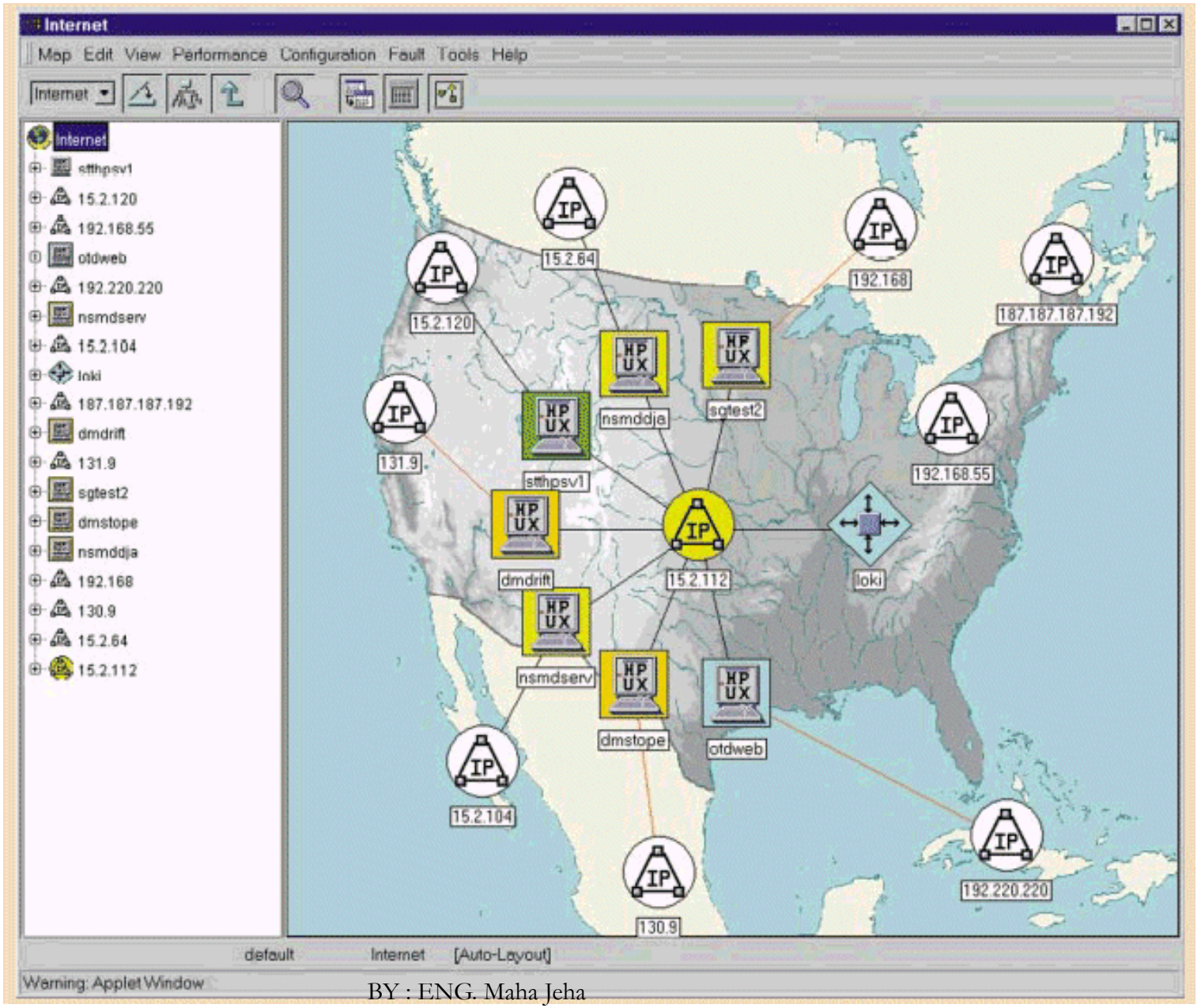
Network Configuration

- Configure agents
- Configure management systems
- Community administration parameters
  - Community name
  - MIB view
  - Trap targets
- Auto-discovery : Scope

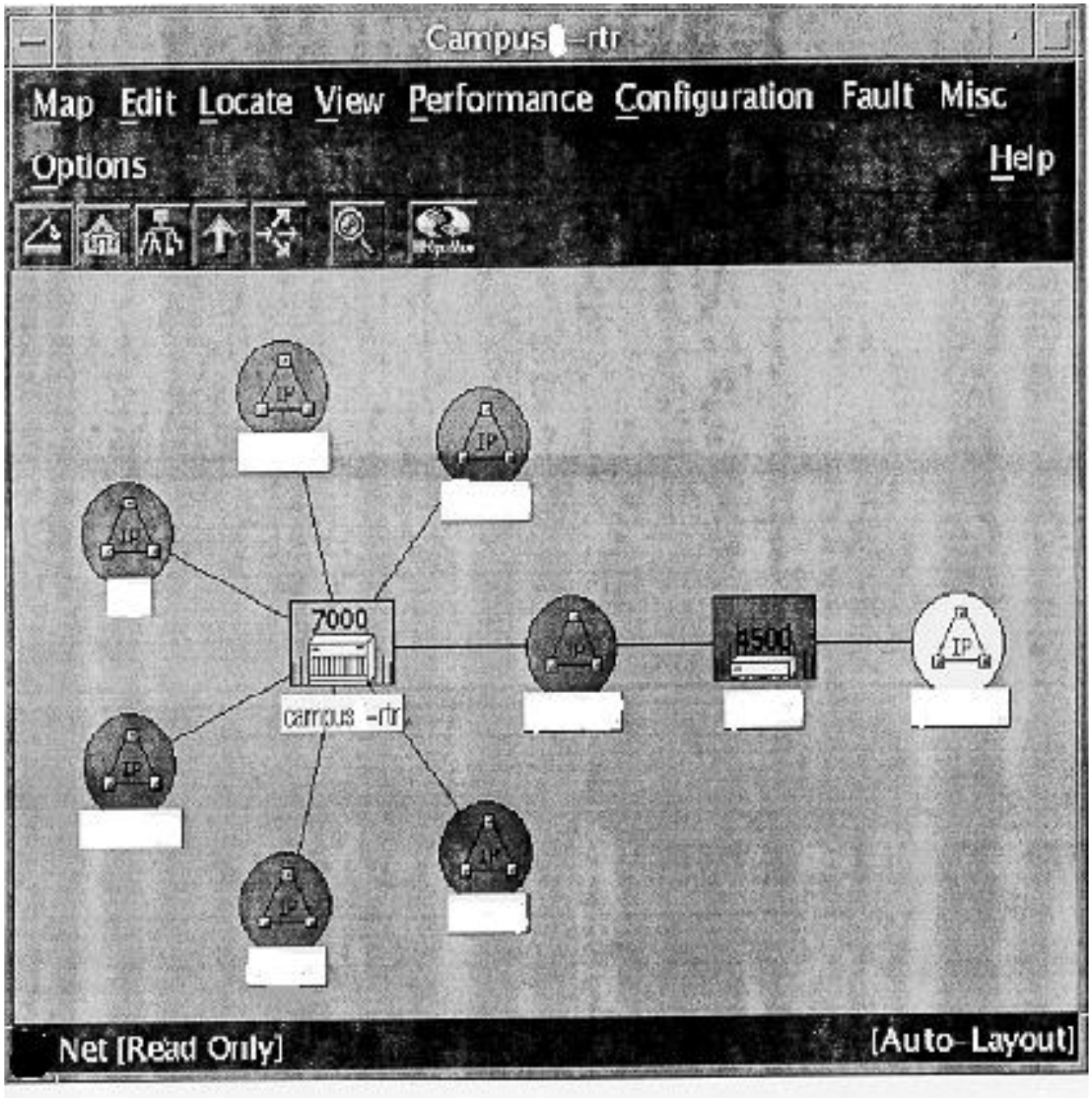
Network Monitoring

- By polling
- By traps (notifications)
- Failure indicated by pinging or traps
- Ping frequency optimized for network load vs. quickness of detection
- trap messages: *linkdown, linkUp, coldStart, warmStart, etc.*
- Network topology discovered by auto-discovery

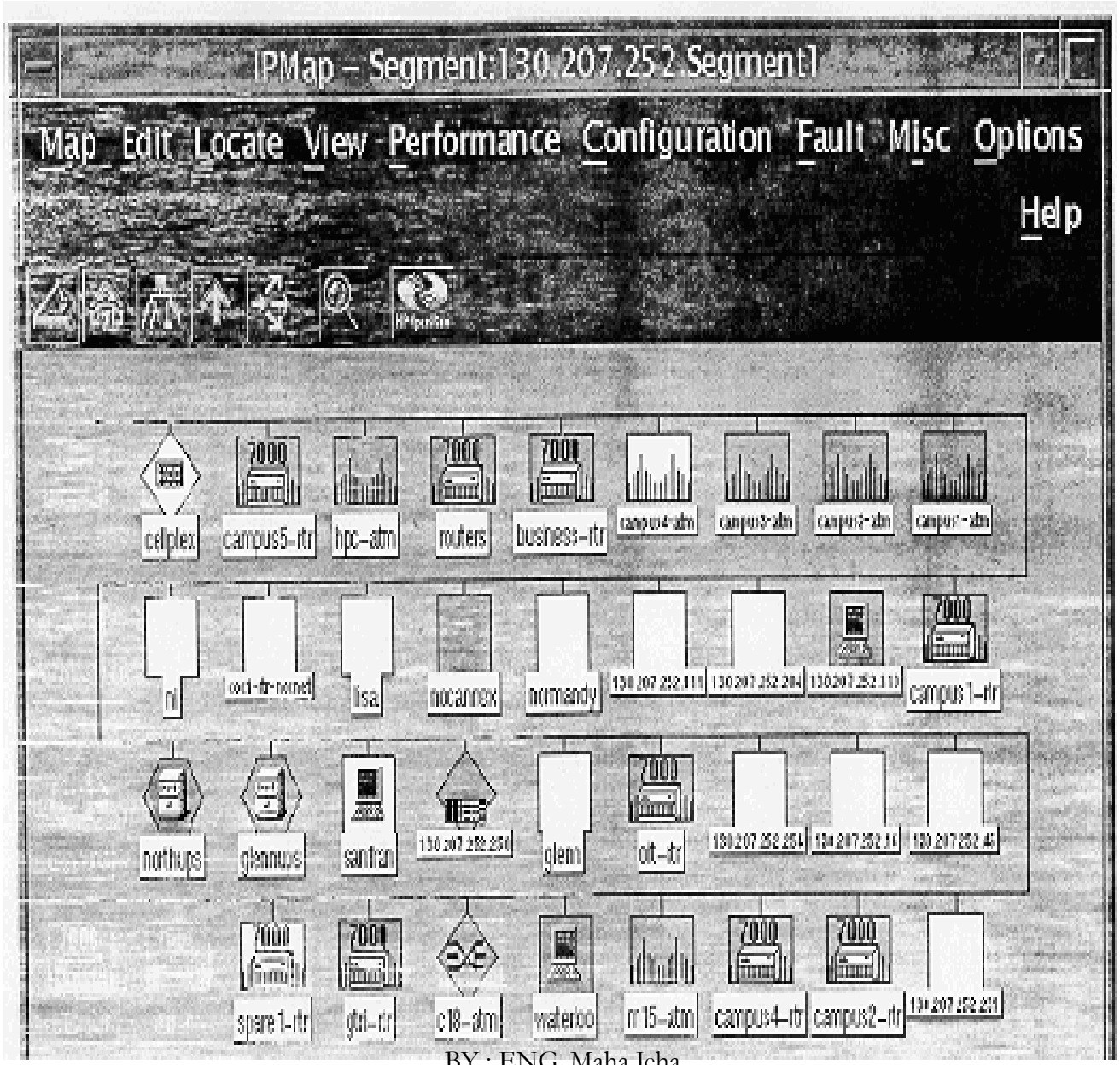
Global View


Internet
Map Edit View Performance Configuration Fault Tools Help
Internet
Internet
stthpsv1
15.2.120
192.168.55
otdweb
192.220.220
nsmdserv
15.2.104
loki
187.187.187.192
dmdrift
131.9
sgtest2
dmstope
nsmddja
192.168
130.9
15.2.64
15.2.112
15.2.64
192.168
187.187.187.192
15.2.120
nsmddja
sgtest2
131.9
stthpsv1
192.168.55
dmdrift
15.2.112
loki
nsmdserv
dmstope
otdweb
15.2.104
130.9
192.220.220
default
Internet
[Auto-Layout]
Warning: Applet Window

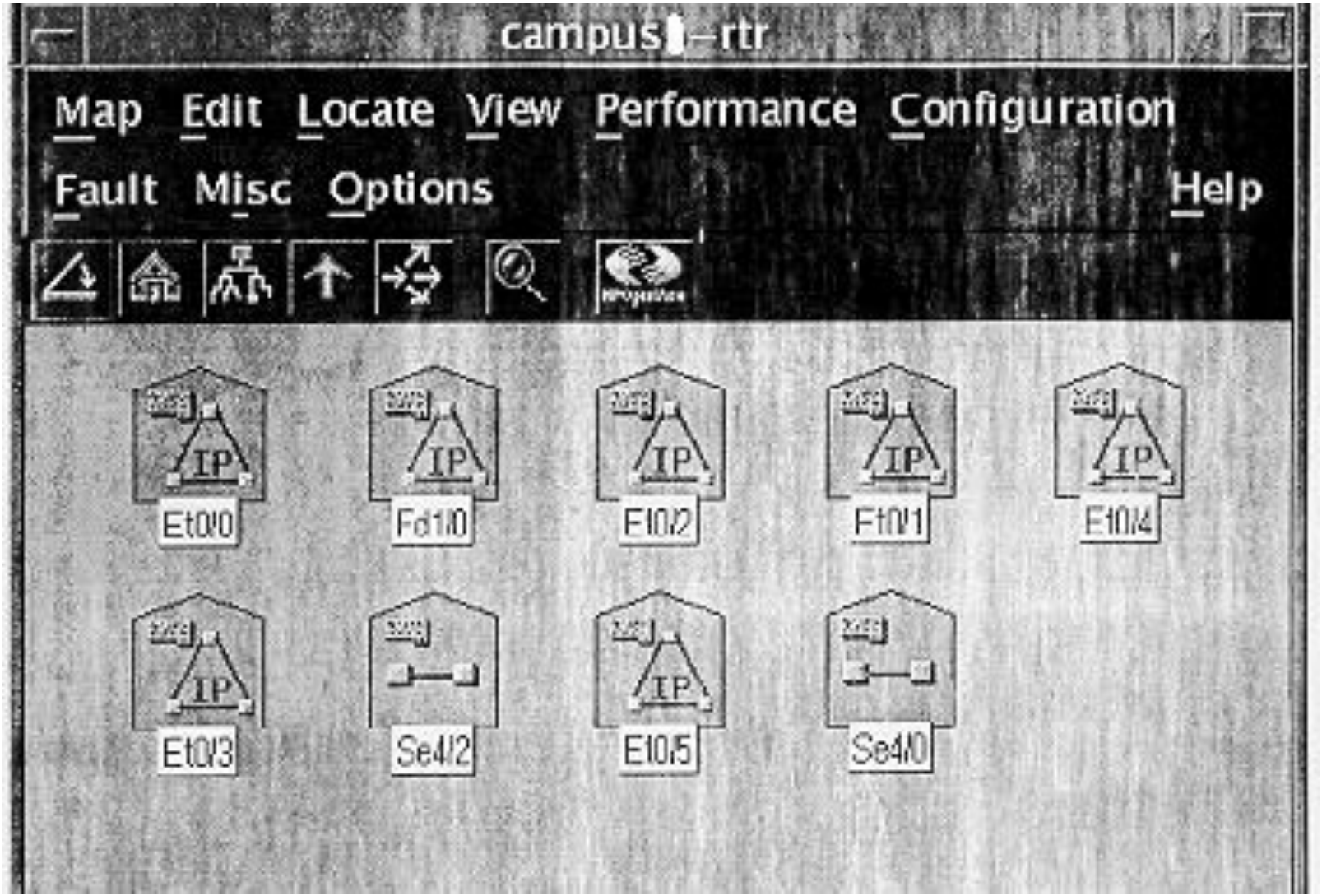
Domain View


Campus -rtr
Map Edit Locate View Performance Configuration Fault Misc
Options
Help
7000
campus -rtr
8500
IP
Net [Read Only]
[Auto-Layout]

Segment View



Interfaces View



Node Discovery In a Network

- Node Discovery
  - Given an IP Address with its subnet mask, find the nodes in the same network.
- Two Major Approaches:
  - Use ICMP ECHO to query all the possible IP addresses.
  - Use SNMP to query the ARP Cache of a node known

Use ICMP ECHO

- Eg: IP address: 163.25.147.12

  Subnet mask: 255.255.255.0
- All possible addresses:
  - 163.25.147.1 ~ 163.25.147.254
- For each of the above addresses, use ICMP ECHO to inquire the address
- If a node replies (ICMP ECHO Reply), then it is found.

Use SNMP

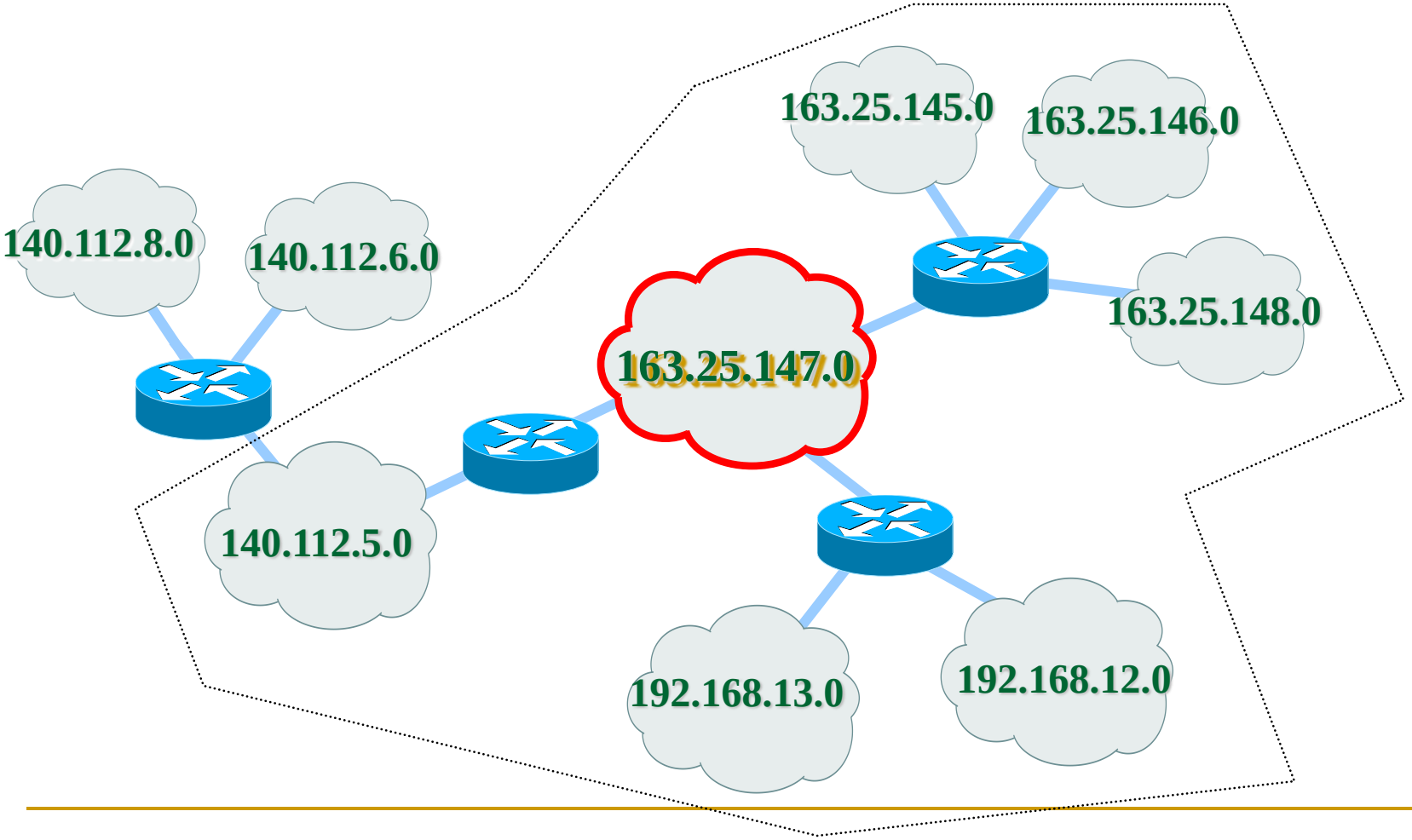
- Find a node which supports SNMP
  - The given node, default gateway, or router
  - Or try a node arbitrarily
- Query the *ipNetToMediaTable* in MIB-II IP group

ipNetToMediaIfIndex	ipNetToMediaPhysAddress	ipNetToMediaNetAddress	ipNetToMediaType
1	00:80:43:5F:12:9A	163.25.147.10	dynamic(3)
2	00:80:51:F3:11:DE	163.25.147.11	dynamic(3)

Network Discovery

- Network Discovery
  - Find the networks to be managed with their interconnections
- Given a network, find the networks which directly connect with it.
- Recall that networks are connected via routers.
- Major Approach
  - Use SNMP

Discovering Networks



A Network Discovery Algorithm

1. First use a node discovery algorithm to find all the nodes in the network.
2. For each discovered node, use SNMP to query the ipAddrTable of MIB-II IP group

ipAdEntAddr	ipAdEntIfIndex	ipAdEntNetMask	ipAdEntBcastAddr	
163.25.145.254	1	255.255.255.0	163.25.145.255	…
162.25.146.254	2	255.255.255.0	163.25.146.255	…
162.25.147.254	3	255.255.255.0	163.25.147.255	…

3. Query the corresponding entries in ipRouteTable to verify the above addresses

ipRouteTable

Destination	Interface	Next Hop	Routing Type	Routing Protocol	Subnet Mask
0.0.0.0	173	192.192.45.252	indirect(4)	netmgmt(3)	0.0.0.0
192.192.45.0	173	0.0.0.0	direct(3)	local(2)	255.255.255.0
192.192.108.64	139	0.0.0.0	direct(3)	local(2)	255.255.255.192
192.192.108.192	132	0.0.0.0	direct(3)	local(2)	255.255.255.192
192.192.109.0	137	0.0.0.0	direct(3)	local(2)	255.255.255.0
192.192.110.0	134	0.0.0.0	direct(3)	local(2)	255.255.255.0
192.192.162.0	173	192.192.45.252	indirect(4)	rip(8)	255.255.255.0
203.71.252.0	142	0.0.0.0	direct(3)	local(2)	255.255.255.192
203.71.252.64	143	0.0.0.0	direct(3)	local(2)	255.255.255.192
203.71.252.128	144	0.0.0.0	direct(3)	local(2)	255.255.255.192
203.71.252.192	133	0.0.0.0	direct(3)	local(2)	255.255.255.192
203.71.253.0	137	192.192.109.254	indirect(4)	rip(8)	255.255.255.0
211.22.243.0	173	192.192.45.204	indirect(4)	rip(8)	255.255.255.0

Commercial NMS & System Solutions

- Enterprise NMS
  - Hewlett-Packard OpenView
  - Sun SunNet Manager
  - IBM Netview
  - Cabletron Spectrum Enterprise Manager
- Low End NMS
  - SNMPc
- System & Network Management
  - Computer Associates Unicenter TNG
  - Tivoli TME / Netview
  - Big Brother
  - Spong