In chapter 9: do not consider slides from 37 to 96, so do not consider

- MIB Engineering
- 。 NMS design

Chapter 9

Network Management Tools, Systems, and Engineering

Basic Network Software Tools

- Status monitoring tools
- Traffic monitoring tools
- Route monitoring tools

Notes

- Basic tools are available as
 - Part of the Operating System
 - Add-on applications

2

Status Monitoring Tools

 Table 9.1 Status-Monitoring Tools

NAME	OS	DESCRIPTION
Ifconfig	UNIX	Obtains and configures networking
		interface parameters and status
ping	UNIX	Checks the status of node / host
	Windows	
nslook-	UNIX	Looks up DNS for name-IP address
up	Windows	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 (hme0)

Notes

netman: ifconfig -a Example:

lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232 inet 127.0.0.1 netmask ff000000

hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING, MULTICAST> mtu 1500 inet 192.207.8.31 netmask fffff00 broadcast 192.207.8.255



Ping

- Most basic tool for internet management
- Based on ICMP ECHO_REQUEST message
- Available on all TCP/IP stacks
- Useful for measuring connectivity
- Useful for measuring packet loss
- Can do autodiscovery of TCP/IP equipped stations on single segment

Notes

Example:

% ping 205.152.8.138

PING 205.152.8.138 (205.152.8.138): 56 data bytes 64 bytes from 205.152.8.138: icmp_seq=0 ttl=17 time=14.8 ms 64 bytes from 205.152.8.138: icmp_seq=1 ttl=17 time=20.2 ms 64 bytes from 205.152.8.138: icmp_seq=2 ttl=17 time=15.7 ms 64 bytes from 205.152.8.138: icmp_seq=3 ttl=17 time=21.6 ms 64 bytes from 205.152.8.138: icmp_seq=4 ttl=17 time=20.0 ms

--- 205.152.8.138 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 14.8/18.4/21.6 ms

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
- Available with BSD UNIX; FTP from uunet.uu.net
- Available in Windows NT

Notes

Example:

noc2% nslookup 172.152.8.138 Server: ada.btc.gatech.edu Address: 192.77.147.28

Name: mani.bellsouth.net Address: 172.152.8.138

6

Domain Name Groper: dig

Used to gather lots of information on hosts from DNS

Notes

Example:

[beluga]~> dig +noc nimbus.tenet.res.in. tenet.res.in. tenet.res.in. volcano.tenet.res.in ;; Query time: 2 mse ;; SERVER: 203.199 WHEN: Fri Mar, 6	604800 604800 604800 .604800 ec 9.255.3#5	IN IN IN 3(203.199	A NS NS A	203.199.255.4 volcano.tenet.res.in. lantana.tenet.res.in. 203.199.255.3
;; SERVER: 203.199 ;; WHEN: Fri Mar 6 ;; MSG SIZE rcvd: [beluga]~>	14:12:43	`	.255.	3)

Host

- Command: host
- Displays host names using DNS
- Available from ftp.nikhef.nl:/pub/network/host.tar.Z

Notes

Example:

% host -a sun4-gw.cc.gatech.edu

Trying null domain

rcode = 0 (Success), ancount=1

The following answer is not authoritative:

sun4-gw.cc.gatech.edu 85851 IN A 130.207.111.100

Traffic Monitoring Tools

Name	Operati	Description Table 9.2 Traffic-M	onitoring Tools	
	ng System	Not	es • <i>ping</i> and <i>bing</i> used t	
ping	UNIX / Window s	Used for measuring roundtrip packet loss	 characteristics of the <i>ethereal</i> (a.k.a. <i>wires</i>) 	
bing	UNIX	Measures point-to-point bandwidth of a link	(also <i>snoop)</i> puts the mode and logs the da	
tcpdump	UNIX	Dumps traffic on a network	 <i>iptrace</i> uses NETMC produces 3 types of a 	
getethers	UNIX	Acquires all host addresses of an Ethernet LAN segment	 IP traffic Host traffic Abbreviated same 	
iptrace	UNIX	Measures performance of gateways	of packets	
ethereal, wireshark	Linux / Window s	Graphical tool to capture, inspect, and to save Ethernet packets		

to measure the propagation e transmission path

eshark), and *tcpdump* ne network interface in promiscuous data

ON program in UNIX and outputs:

mpling of pre-defined number

Packet Loss Measurement

- Command: ping
- Many options available
- Implementation varies from system to system

Notes

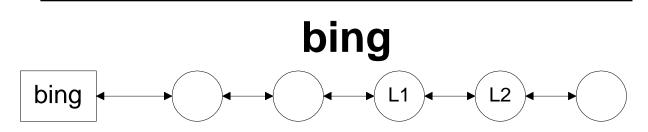
Example:

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





- 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.

Ethereal (Wireshark)

× _ =				(Untitled) - Wireshark (on 007)
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture A</u> nalyze <u>S</u> t	atistics <u>H</u> elp		
	🛍 í 🖪 🖄 🗙	2 👌 i 🗛 🔶 i	* *	🛧 🛨 i 🔲 🕞 i 🔍 🔍 🗠 📅 i 🅁 🕅 📑 🔯 i 😂
Filter:			▼ 🕈 Ex	pression 🤞 <u>C</u> lear 🤣 Apply
No. Time	Source	Destination *	Protocol	Info
15751 13.599814	10.94.12.156	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0xa62b9a27
15752 13.599997	10.94.1.1	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0xa62b9a27
15753 13.600216	Intel_93:05:cf	Broadcast	ARP	Who has 10.94.86.242? Tell 10.94.7.159
15754 13.602520	QuantaCo_bb:96:6d	Broadcast	ARP	Who has 10.94.71.187? Tell 10.94.14.107
15755 13.603665	00000001.000fb0cd6cbf	00000000.ffffffffffff	IPX SAP	Nearest Query
15756 13.604452	Wistron_9c:2b:15	Broadcast	ARP	Who has 10.94.3.229? Tell 10.94.18.116
15757 13.604575	IntelCor_28:f7:54	Broadcast	ARP	Who has 10.94.196.215? Tell 10.94.13.79
15758 13.605370	Intel_37:51:d6	Broadcast	ARP	Who has 10.94.25.45? Tell 10.94.19.149
15759 13.606849	Intel_80:ee:93	Broadcast	ARP	Who has 10.94.48.201? Tell 10.94.8.254
15760 13.607949	10.6.21.59	10.94.3.215	TCP	48966 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=115648 TSER=0 WS=5
15761 13.607974	10.94.3.215	10.6.21.59	TCP	http > 48966 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=6
15762 13.607983	Dell f2:16:e3	Broadcast	ARP	Who has 10.94.22.27? Tell 10.94.13.242
15763 13.608379	10.6.21.59	10.94.3.215	TCP	48966 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0
15764 13.608624	AsustekC 92:53:5a	Broadcast	ARP	Who has 10.94.204.43? Tell 10.94.33.110
15765 13.610549	Giga-Byt_ce:dl:c3	Broadcast	ARP	Who has 10.94.70.165? Tell 10.94.35.9
15766 13.611760	AsustekC_ef:87:30	Broadcast	ARP	Who has 10.94.81.89? Tell 10.94.19.251
▶ Frame 1 (60 bytes	s on wire, 60 bytes cap	otured)		
Ethernet II, Src:	Cisco df:64:40 (00:11	L:bc:df:64:40), Dst: I	ntel 9c:ce	5:a2 (00:19:d1:9c:c6:a2)
	, Src: 10.6.21.112 (10		Charles and the construction	
	-			(22), Seq: 1, Ack: 1, Len: 0
v Transmission Cont	LIGE FIGLOCOL, SPC POP	1; 40201 (40201), DSt 1	-ort; ssn	(22), Sey: I, ACK: I, Len: 0
0000 00 19 d1 9c c6	5 a2 00 11 bc df 64 4	0 08 00 45 10	d@E	
	0 00 3e 06 46 1c 0a 0		>. Fp.	
	0 16 57 49 28 09 71 c		NI (.q.~.F	
0030 4d 0a 27 e3 00	0 00 00 00 00 00 00 00			
	<i>.</i>			
File: "/tmp/etherXXXXL	JNr6d6" 3222 K Pack	ets: 22608 Displayed: 22	608 Marke	d: 0 Dropped: 364

Notes

12

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

Notes

Example: Options: -d for device interface and -c for counts

root@noc2:~# snoop -d hme0 -c 5 Using device /dev/hme (promiscuous mode) noc2.btc.gatech.edu -> noc4.btc.gatech.edu TCP D=22 S=1221 Ack=2845521735 Seg=24552727 Len=0 Win=7368 ? -> (multicast) ETHER Type=809B (EtherTalk (AppleTalk over Ethernet)), size = 80 bytes ? -> (multicast) ETHER Type=809B (EtherTalk (AppleTalk over Ethernet)), size = 86 bytes noc2.btc.gatech.edu -> 199.77.147.255 UDP D=137 S=137 LEN=108 ? -> (broadcast) ETHER Type=8137 (Novell (old) NetWare IPX), size = 88 noc4.btc.gatech.edu -> noc2.btc.gatech.edu TCP D=1221 S=22 Ack=24552727 Seg=2845521735 Len=64 Win=8760 noc2.btc.gatech.edu -> noc4.btc.gatech.edu TCP D=22 S=1221 Ack=2845521799 Seq=24552727 Len=0 Win=7304 noc4.btc.gatech.edu -> noc2.btc.gatech.edu TCP D=1221 S=22 Ack=24552727 Seq=2845521799 Len=56 Win=8760 snoop: 5 packets captured



tcpdump

- Command: tcpdump
- Interprets and prints headers for:

Ethernet	IP	ICMP
TCP	UDP	NFS
ND	ARP	Appletalk

- Useful for examining and evaluating the TCP based traffic
- Available in UNIX system; FTP from ftp.ee.lbl.gov

Notes Example: SNMP message

14:03:36.798269 noc1.btc.gatech.edu.snmp > noc3.btc.gatech.edu.164: Community = public GetResponse(196) Request ID = 4 system.sysDescr.0 = "SunOS noc1 5.5.1 Generic_103640-08 sun4u" system.sysObjectID.0 = E:hp.2.3.10.1.2 system.sysObjectID.0 = 247396453 system.sysContact.0 = "Brandon Rhodes" system.sysName.0 = "noc1" system.sysLocation.0 = "BTC NM Lab" system.sysServices.0 = 72

Figure 5.17(b) Get-Response Message from Agent-to-Manager (After)

Network Routing *Tools*

Table 9.3 Route-Monitoring Tools

Name	Operating	Description
	System	
netstat	UNIX	Displays the contents of
		network-related data stru
arp	UNIX, Windows	Displays and modifies th
rarp	9x/00/NT	to-Ethernet address tran
		tables
traceroute	UNIX	Traces route to a destination
tracert	Windows	routing delays

Notes

various uctures ne Internetnslation

ation with

Network Status

netstat -r Routing tables

Internet:

Destination	G	ateway	Flag	s Refs	Use		Net
Default g	w.litech.net	UGC	44 541	550	de0		
172.16.15.1	g	w.litech.r	net UGF	H 0	0		de0
ah.litech.net	0	:80:48:ee	e:74:b4	UHLW	9	26536	83
uucp.litech.net	uucp.lited	ch.netU⊢	00		lo0		
sip-17.litech.net	big	UH 0	5551		ppp3		
dip-244.litech.ne				2472		de0	
univers-litech-g	w gw.litech.	net UG	GH O	47	otstat -r	de0	
194.44.232	gv	v.isr.lviv.u	ia Ugc		17183	81	ppp
OSPF-ALL.MC/	ST.NET loc	calhost	UH 1	86491	lo0		
OSPF-DSIG.MC	CAST.NE loo	calhost	UH 1	25127	lo0		

Notes

etif Expire

0 de0 202

p9

Route Tracing

- Command: traceroute (UNIX) / tracert (MS TIME-EXCEED error report
- Available in most UNIX OS
- Windows)
- ICMP Also available from uc.msc.unm.edu
- Discovers route taken by packets from source to destination
- Useful for diagnosing route failures
- Useful for detecting bottleneck nodes

Trace Route Sample 1

Tracing route to mani.btc.gatech.edu [199.77.147.96] over a maximum of 30 hops:

2 ms 3 ms 3 ms bims008001.bims.bellsouth.net [205.152.8.1] 1 4 ms 2 ms 3 ms 172.16.11.2 2 3 5 ms 4 ms 3 ms 172.16.4.2 5 ms 3 ms 3 ms bims011033.bims.bellsouth.net [205.152.11.33] 4 5 4 ms 4 ms 4 ms 205.152.13.98 Request timed out 6 * 5 ms 9 ms 12 ms 205.152.2.249 7 8 33 ms 31 ms 31 ms Hssi0-0-0.GW2.ATL1.ALTER.NET [157.130.65.229] 9 68 ms 10 ms 11 ms 105.ATM3-0-0.XR1.ATL1.ALTER.NET [146.188.232.66] 10 11 ms 14 ms 12 ms 195.ATM12-0-0.BR1.ATL1.ALTER.NET [146.188.232.49] 11 16 ms 14 ms 14 ms atlanta1-br1.bbnplanet.net [4.0.2.141] 12 19 ms 15 ms 17 ms atlanta2-br2.bbnplanet.net [4.0.2.158] 13 21 ms 56 ms 328 ms atlanta2-cr99.bbnplanet.net [4.0.2.91] 14 17 ms 18 ms 17 ms 192.221.26.3 15 32 ms 20 ms 18 ms 130.207.251.3 16 20 ms 17 ms 17 ms mani.btc.gatech.edu [199.77.147.96] Trace complete

Trace Route Sample 2

Tracing route to mani.btc.gatech.edu [199.77.147.96] over a maximum of 30 hops:

1	3 ms		ms bims008001.bims.bellsouth.net [205.152.8.1]
2	3 ms	3 ms 2	ms 172.16.11.2
3	5 ms	4 ms 4	ms 172.16.4.2
4	5 ms	3 ms 4	ms bims011033.bims.bellsouth.net [205.152.11.33]
5	7 ms	4 ms 4	ms 205.152.13.98
6	* *	* R	equest timed out
7	9 ms	8 ms 9	ms 205.152.2.249
8	228 ms	214 ms	191 ms 206.80.168.9
9	230 ms	246 ms	234 ms maeeast.bbnplanet.net [192.41.177.2]
10	243 ms	222 ms	212 ms vienna1-nbr2.bbnplanet.net [4.0.1.93]
11	230 ms	213 ms	202 ms vienna1-nbr3.bbnplanet.net [4.0.5.46]
12	247 ms	227 ms	236 ms vienna1-br2.bbnplanet.net [4.0.3.149]
13	228 ms	235 ms	238 ms atlanta1-br1.bbnplanet.net [4.0.2.58]
14	*	257 ms	238 ms atlanta2-br2.bbnplanet.net [4.0.2.158]
15	225 ms	234 ms	233 ms atlanta2-cr99.bbnplanet.net [4.0.2.91]
16	240 ms	229 ms	251 ms 192.221.26.3
17	235 ms	245 ms	225 ms 130.207.251.3
18	*	268 ms	243 ms mani.btc.gatech.edu [199.77.147.96]

Trace complete

SNMP Tools

- SNMP command-line tools
- SNMP MIB Browser with graphical interface
- snmpsniff: Linux/Free BSD based tool. Reads PDUs

Notes

Many tools available on public domain.

SNMP Command Tools

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

- Test tool is an interactive tool to get values of several managed objects, one at a time.
- Get, Get-next and Set are the SNMP commands that we learned under SNMP architecture / messages. Execution of these will return an SNMP Response message.
- SNMPWalk uses snmpgetnext to trace the entire MIB.
- Network status command is used to test the status of network connections of a host.

SNMP Get Command

% snmpget noc5.btc.gatech.edu public system.sysDescr.0

system.sysDescr.0 = OCTET STRING: "SunOS noc5 5.6 Generic_105181-03 sun4u"

Notes

• Note that the value 0 at the end of the object id indicates that it is a single-valued scalar.

SNMP Get Next Command

% snmpgetnext noc5.btc.gatech.edu public interfaces.ifTable.ifEntry.ifIndex.1

interfaces.ifTable.ifEntry.ifIndex. 2 = INTEGER: 2

Notes Snmpget host community OID

SNMP Set Command

• Command: snmpset host community

Network Status

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

% snmpnetstat noc5 public

		nternet Connecti	ons cal Address Foreig	In 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	00	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

Notes

199.77.147.182: sysDescr.0 : SunOS noc5 5.6 Generic_105181-03 sun4u sysObjectID.0: 1.3.6.1.4.1.11.2.3.10.1.2 sysUpTime.0 : 8d 22:21:53.74 sysContact.0: sysName.0: noc5 sysLocation.0: sysServices.0:72 sysORLastChange.0 : 0d 0:00:00.00

Figure 9.8 MIB Browser Example (text based) for System Group

SNMP Sniff

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

Protocol Analyzer

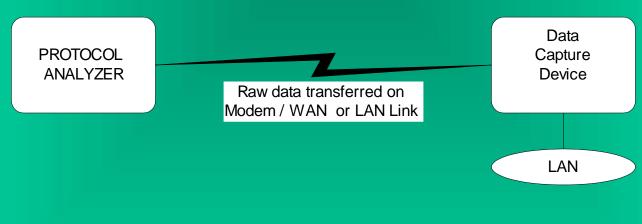


Figure 9.9 Basic Configuration of a Protocol Analyzer

- 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

PROTOCOL ANALYZER SNM Traffic Router Router SNM Traffic Router Composition LAN Network A SNM Probe LAN Network A Stand • HP NetM • Comm analyze • Data gath period of ti • Used for for config

Figure 9.10 Protocol Analyzer with RMON Probe

Network Associates Sniffer

Notes

Stand-alone and Networked
HP NetMetrix / HP OpenView

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

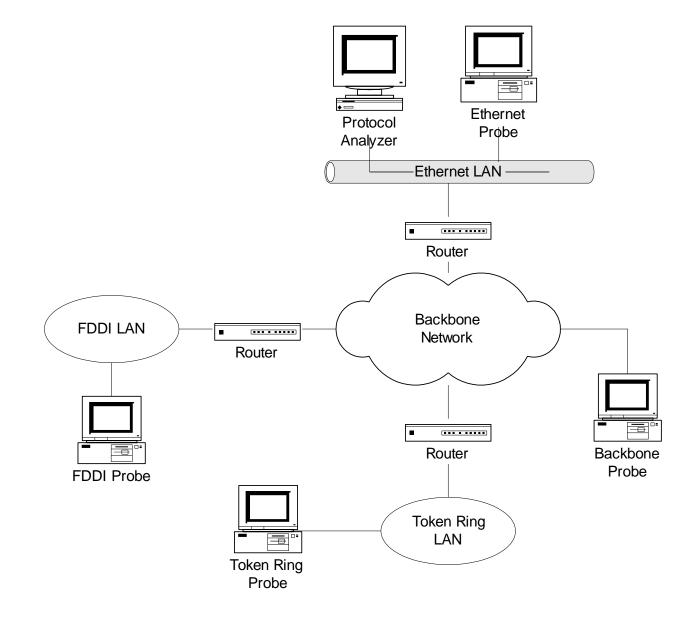


Figure 9.11 Monitoring of Total Network with Individual RMON Probes

Network Statistics

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

Notes

31

Traffic Load: Source

) Data: Live 1		
com: Source		
1609 selected of 1609	Source LOW-CONTRIB	average total octs 352.831 M
NetHost	Octets	1
cssun.mathcs.emory.e	3G 🛛	
r39h178.res.gatech.e	зс 📲	
cpk-news-hub1.bbnpla	4G	
r32h 177.res.gatech. e	5¢ 🖞	
howland.erols.net	140	
collegepk-mbone1.bbn	ЗВС	
r74h18.res.gatech.ed	46G 🗾	
santanni.cc.gatech.e	586	1
news-ext.gatech.edu	826	
LOW-CONTRIB	2990	
	р <u>е</u> 0	300

Figure 9.12 Load Statistics: Monitoring of Sources

Traffic Load: Destination

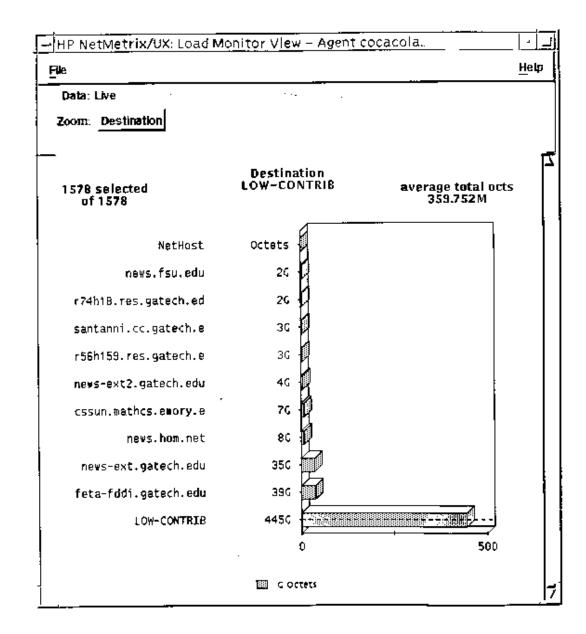


Figure 9.13 Load Statistics: Monitoring of Destinations

Network Management: Principles and Practice © Mani Subramanian and T. A. Gonsalves 2010

Traffic Load: Conversation

Data: Live Dom: Conversation				
10 selected of 1039	Conve news-axt.gatech.edu 4	rsation (•) howland.e	rois.net	average total octs 20.636K
NetHost1 <-> No	otHost2	0xt1to2	Oct 2to1	
newsrext.gatech.edu <-> <	liffs.rs.itd.umlch.	1K	ык 🗗	
LON-CONTRIB (-) \$	antanni.co.gatech.e	2K	r (2	
opk-news-hubi.bbnpla <-> n	ws-axt2.gatech.edu	7к	к 🛃	
news-ext.gatech.edu <-> u	cp.pacifier.com	9 K	818	
LOM-CONTRIB (-> L	OM-CONTRIB	7K	ж 🕎	
usenet.news.psi.net <-> n	evs-ext, gatech, edu	657	10K	7
ng¥s-ext.gatech.edu <-> n	evsveb,bls,com	17K	603	
ton⊢contrib (-> n	eus-ext.gatech.eóu	4Ķ	24K	
feta-fddi.gatech.edu <-> a	tlanta3-ebone1.bbnp	20	43К 🏧	
news-ext.gatech.edu <-> h	am)and.erols.net	3K	EOK THE	36 60 9D

Figure 9.14 Load Statistics: Monitoring of Conversation Pairs

Network Management: Principles and Practice © Mani Subramanian and T. A. Gonsalves 2010

Protocol Distribution

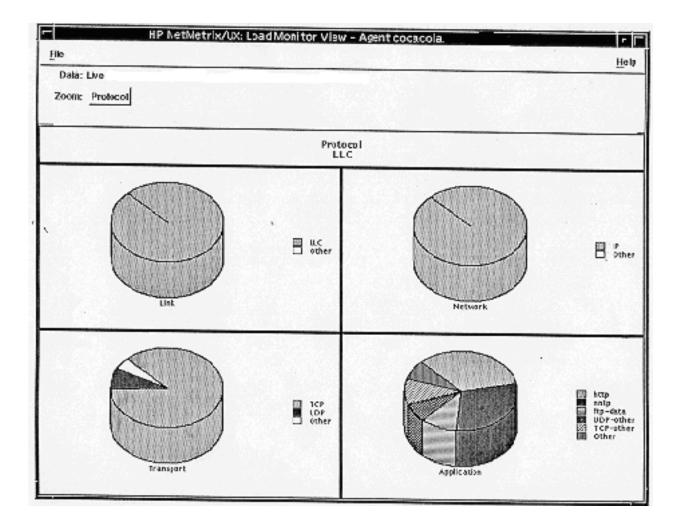


Figure 9.15 Protocol Distribution (NetMetrix)

MRTG

• Multi Router Traffic Grouper (Oeticker and Rand)

- www.ee.ethz.ch/stats/mrtg/
- Generates graphic presentation of traffic on Web
 - Daily view
 - Weekly view
 - Monthly view
 - Yearly view



MIB Engineering

- In chapter 9: do not consider slides from 37 to 96, so do not • consider
 - **MIB** Engineering
 - NMS design