Monitoring & Measurement

In this presentation

- Introduction
- Why do we need network monitoring
- What are Network Monitoring Tools
- Bandwidth Monitoring Techniques/Services
- Setting up some monitoring Tools
- Conclusion

Introduction:- Why do we need to monitor and measure Bandwidth

- Cost of Bandwidth is expensive for developing countries
  - Bandwidth in developing countries is expensive. In a report for the Partnership for Higher Education in Africa, Mike Jensen calculates that Makerere University pays about

    $22,000/month for 1.5Mbps/768Kbps (in/out), Eduardo Mondlane pays $10,000/month for 1Mbps/384Kbps, while the University of Ghana pays $10,000/month for 1Mbps/512Kbps.

    These figures indicate that African universities, outside of South Africa, are paying over $55,000/month for 4Mbps inbound and 2Mbps outbound. These figures are about 100 times more expensive than equivalent prices in North America or Europe.

Cont…

- To Know if the ISP is providing us with the required bandwidth paid for.

- To be able to optimize the available bandwidth
  - 59% of institutions do not monitor or manage bandwidth at all (Belcher, 2005)

  - For details See the ATICS Report: www.atics.info

Why do we need network monitoring

- Network statistics (for optimization and planning)
  - Network monitoring
    - Traffic statistics (bandwidth usage, service usage, traffic distribution (e.g. local vs. remote))
  - Network optimization and hardening (to achieve responsiveness to change and growth)
    - Bottlenecks
    - Throughput
- Network mapping/inventory:
  - Identification of routers and servers (DNS, ...)
  - Mapping client characteristics (opened ports, ...

- Security
  - Identifying unofficial services or servers
  - Detection of network security violations
    - Intrusion Detection
    - Compromised Hosts
  - Protecting your network from the world
- Troubleshooting
  - Faulty Hardware
  - (No) Connectivity
  - Resource and service availability
- Accounting
  - Keep logs of users activities

Ways to improve network performance

- Upgrade infrastructure, to install faster, larger, and higher performing systems, lines and facilities.
- Look for cheaper provider and Increase/upgrade your bandwidth.
- Alternative approach
  - is to recognize that 'bandwidth' is a valuable institutional resource or asset that needs to be managed, conserved, and shared as effectively as possible.

How do we measure Bandwidth?

- Network Monitoring Tool

What are Network Monitoring Tools?

- Allows the administrator to know the health status of the network.
- It provides information about collected data and the analysis of such raw data with a view to using scarce or limited resources effectively.
- Uses network probe. Probes let you isolate traffic problems and congestions slowing your network to a crawl.

What can we use the tools for?

- Identifying unofficial services or servers
- Monitoring usage and traffic statistics
- Troubleshooting your network
- Investigating a security incident
- Keeping logs of users activities for accountability

Who? What? Where? How? When?

- Who is accessing your network?
  - students, academics, staff, visitors or others
- What are they accessing your network for?
  - academic study, social use, business use, illegal use
- Where are they accessing your network from?
  - internal, external
- How are they accessing your network?
  - remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN
- When did they access your network?
  - today, yesterday, last week, last month…

Network Monitoring Techniques

- Fraleigh et al, (2001) describe two techniques for network measurement.
- Active Measurement
- Passive Measurement

Active vs. Passive

- Active – relies upon data gathered from probe packets injected into the network.
- Passive – relies upon data gathered from active network traffic.

Active and Passive Tools

Network Monitoring Tools

http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#ping

Passive Network Monitoring Tools

- Multi-Router Traffic Grapher

Is a tool for monitoring traffic loads on a network link. MRTG generates HTML pages that provide a live, visual representation of the network traffic.

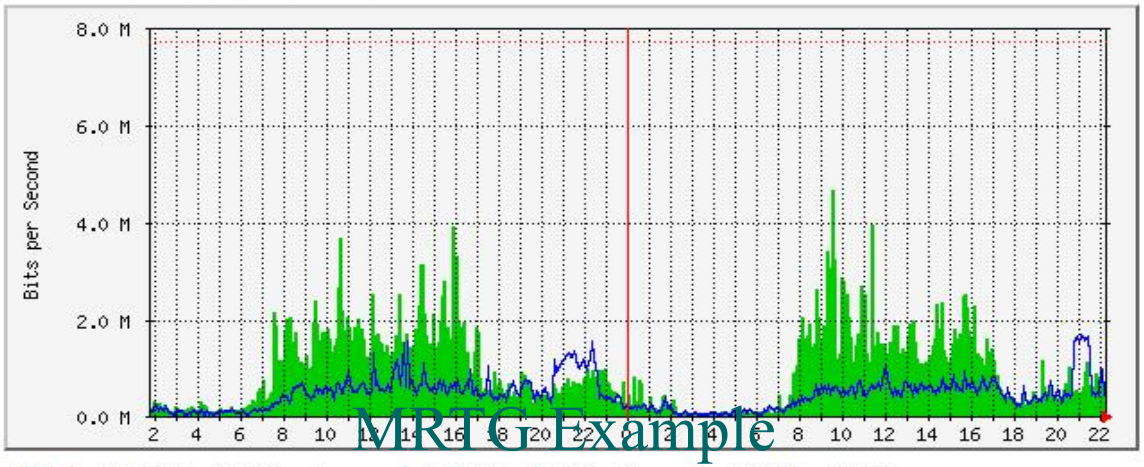
It can be used to monitor any SNMP MIB.

Limitations

- It cannot provide information that shows which host or application may be causing a traffic bottleneck.
- MRTG does not provide information about traffic type or protocol statistics

MRTG Example

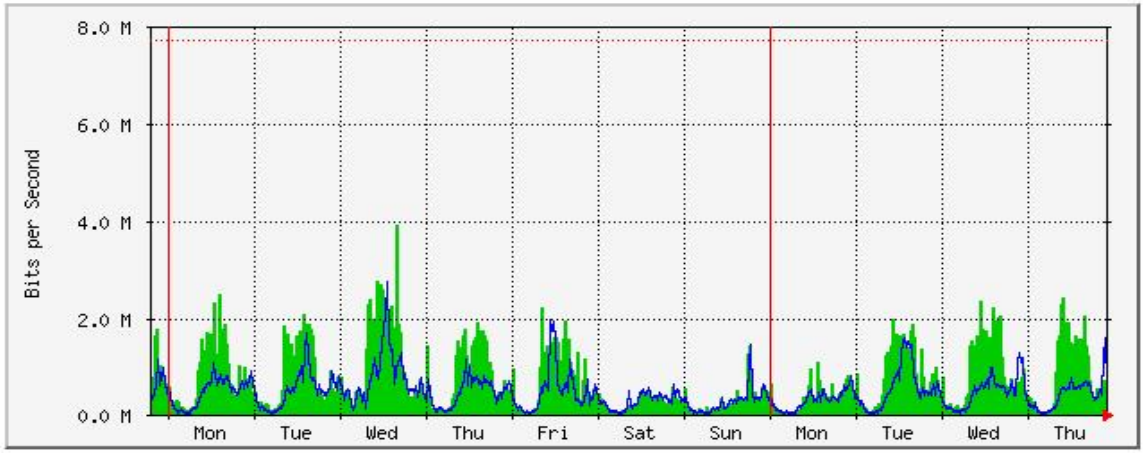
`Daily' Graph (5 Minute Average)



MRTG Example

Max In:4679.7 kb/s (60.6%) Average In:917.1 kb/s (11.9%) Current In:455.3 kb/s (5.9%)
Max Out:1672.4 kb/s (21.7%) Average Out: 465.4 kb/s (6.0%) Current Out:547.1 kb/s (7.1%)

`Weekly' Graph (30 Minute Average)



Max In:3925.6 kb/s (50.8%) Average In:734.2 kb/s (9.5%) Current In:670.7 kb/s (8.7%)
Max Out:2728.5 kb/s (35.3%) Average Out:464.0 kb/s (6.0%) Current Out:559.3 kb/s (7.2%)

Cont…

- Etherfind
  - The software opens the network card in the promiscuous mode and writes a summary line of each packet to a file.
  - Information include protocol type, size, source and destination addresses.
  - The tool extract information from each packet. The data is presented as a text-based user interface
  - Only users with root permission can access the tool.

CONT……

- NFS watch
  - It monitors all incoming network traffic destined to NFS file servers, and divides it into several categories. The number and percentages of packets received is displayed on the screen
  - This tool was originally designed to monitor a single host

CONT…

- TCPdump
  - Uses the packet capture library (libpcap).
  - Prints the headers of packet on a network interface, user analyses network status using this header manually
  - Has many option for capturing raw data, but it does not provide any analysis capability for the captured data.

CONT…..

- Argus
  - It is a generic auditing tool.
  - It runs as an application level daemon, promiscuously reading network packets from a specified interface
  - it generate network traffic audit records for the network activity.
  - it extract info from each packet in promiscuous mode, save the info to a file and later analyzes the file
  - It shows information about protocols, but does not show source or destination host information, it only provides a text based user interface.

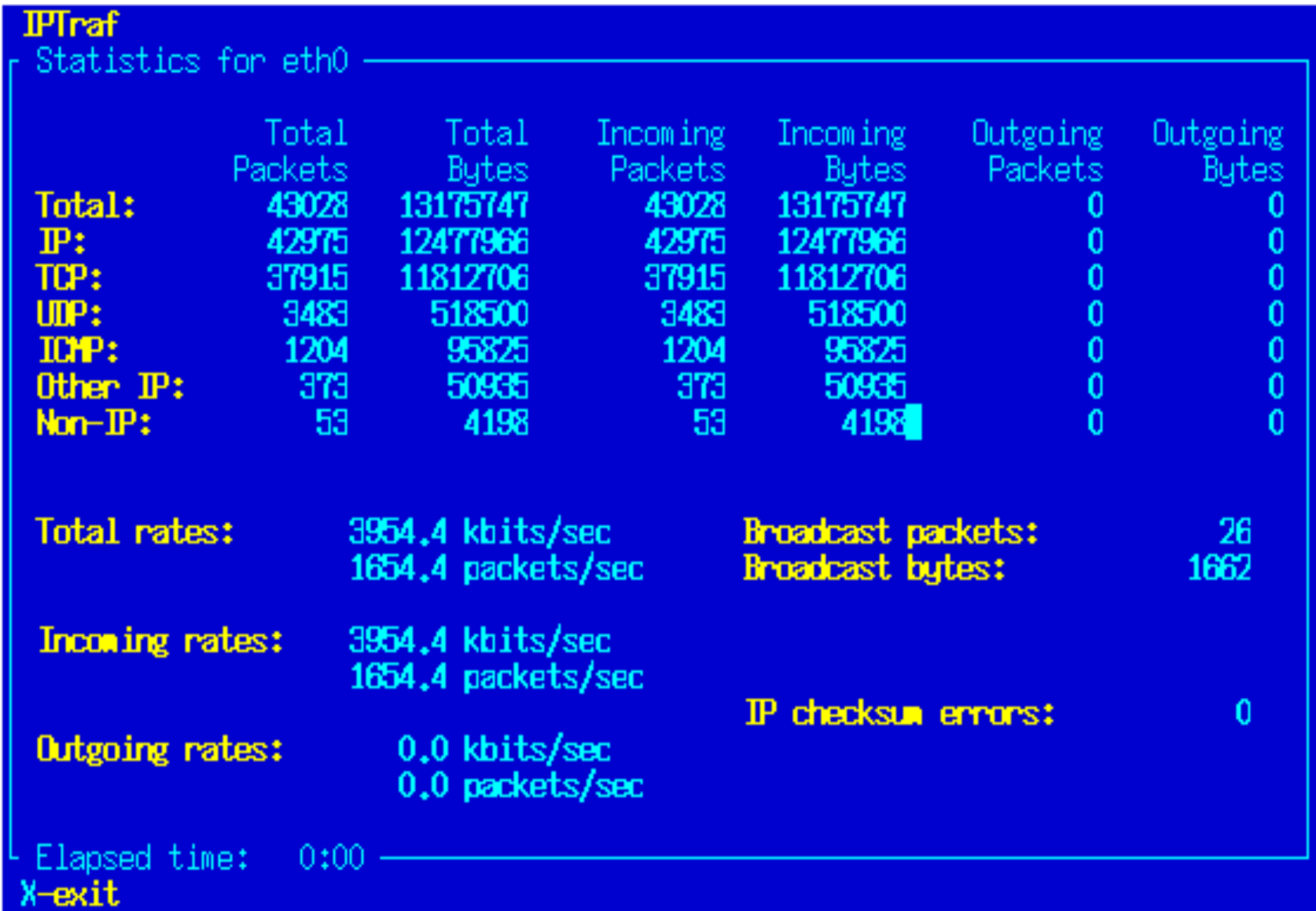
CONT…

- Etherload
  - It is a freely LAN traffic analyzer for MS-DOS with an Ethernet or Token Ring controller
  - It basically captures each packet running through a LAN and provides various information on the packet.
  - It can be used to check which host is generating the most traffic, which host is sending to which host, and what kind of protocols are in use in a specific Ethernet segment
  - Since it is DOS based it provides character-based user interface for displaying traffic information

CONT…..

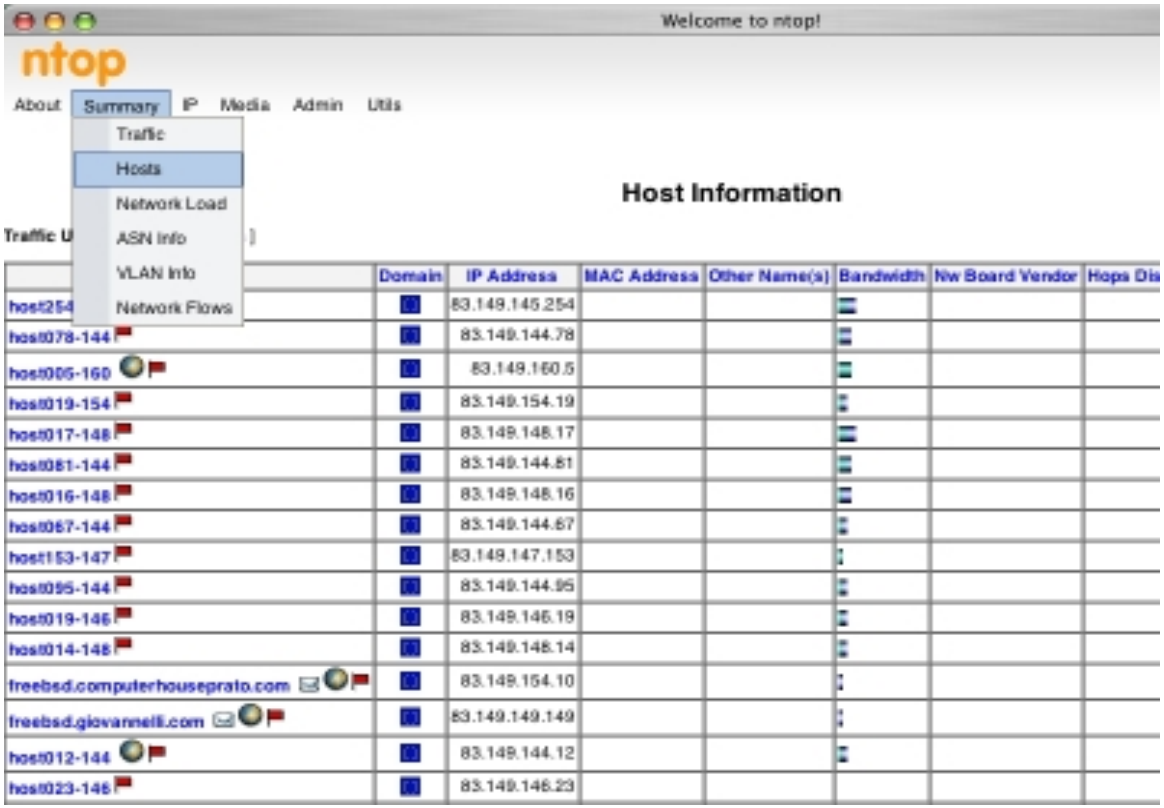
- IPTraf
  - IPTraf is a console-based network statistics utility for Linux. It gathers a variety of figures such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte count

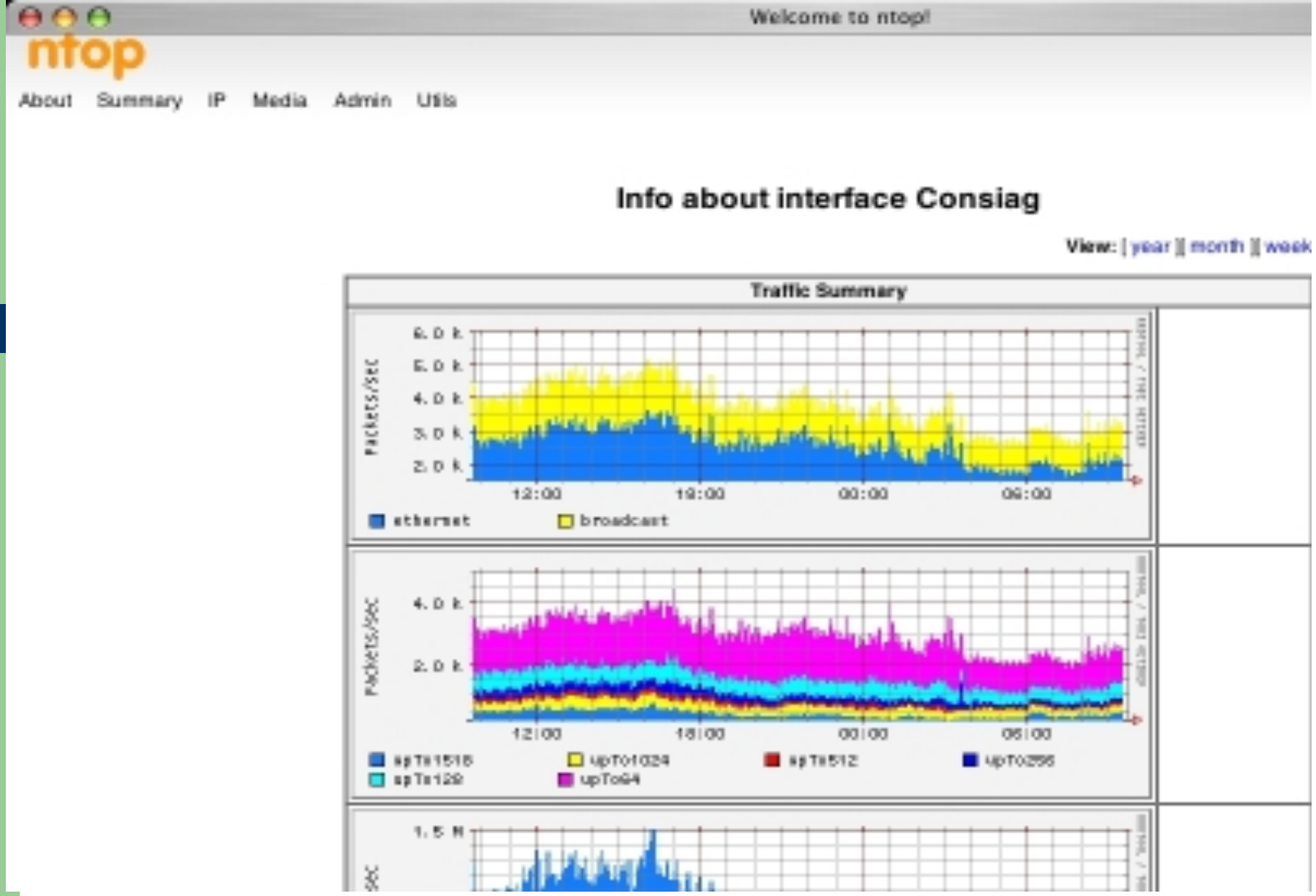
  - **Protocols Recognized**
  - IP
  - TCP
  - UDP
  - ICMP
  - IGMP
  - IGP
  - IGRP
  - OSPF
  - ARP
  - RARP


IPTraf
Statistics for eth0
Total Packets
Total Bytes
Incoming Packets
Incoming Bytes
Outgoing Packets
Outgoing Bytes
Total: 43028 13175747 43028 13175747 0 0
IP: 42975 12477966 42975 12477966 0 0
TCP: 37915 11812706 37915 11812706 0 0
UDP: 3483 518500 3483 518500 0 0
ICMP: 1204 95825 1204 95825 0 0
Other IP: 373 50935 373 50935 0 0
Non-IP: 53 4198 53 4198 0 0
Total rates: 3954.4 kbits/sec
1654.4 packets/sec
Broadcast packets: 26
Broadcast bytes: 1662
Incoming rates: 3954.4 kbits/sec
1654.4 packets/sec
IP checksum errors: 0
Outgoing rates: 0.0 kbits/sec
0.0 packets/sec
Elapsed time: 0:00
X-exit

CONT……

- NTOP
  - ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does. ntop is based on libpcap and it has been written in a portable way in order to virtually run on every Unix platform and on Win32 as well.
  - ntop users can use a a web browser (e.g. netscape) to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status.

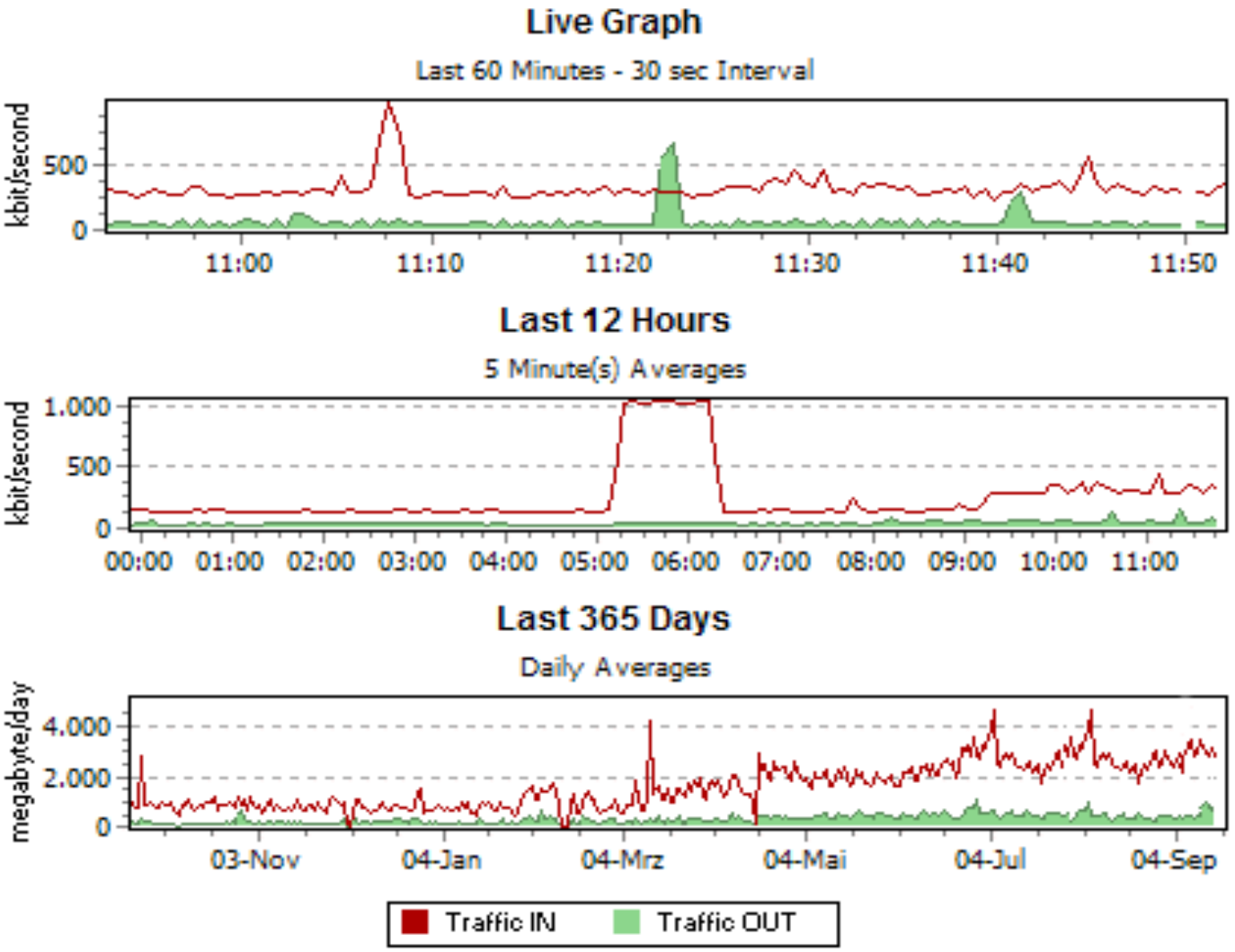

Welcome to ntop!
ntop
About
Summary
IP
Media
Admin
Utils
Traffic
Hosts
Network Load
ASN Info
VLAN Info
Network Flows
Host Information
Traffic U
Domain
IP Address
MAC Address
Other Name(s)
Bandwidth
Nw Board Vendor
Hops Dis
host254
83.149.145.254
host078-144
83.149.144.78
host005-160
83.149.160.5
host019-154
83.149.154.19
host017-148
83.149.148.17
host081-144
83.149.144.81
host016-148
83.149.148.16
host067-144
83.149.144.67
host153-147
83.149.147.153
host095-144
83.149.144.95
host019-146
83.149.146.19
host014-148
83.149.148.14
freebsd.computerhouseprato.com
83.149.154.10
freebsd.giovannelli.com
83.149.149.149
host012-144
83.149.144.12
host023-146
83.149.146.23


Welcome to ntop!
ntop
About
Summary
IP
Media
Admin
Utils
Info about interface Consiag
View: | year | month | week
Traffic Summary
Packets/sec
6.0 k
5.0 k
4.0 k
3.0 k
2.0 k
12:00
18:00
00:00
06:00
ethernet
broadcast
Packets/sec
4.0 k
2.0 k
12:00
18:00
00:00
06:00
upTo1024
upTo256
upTo64
1.5 M

CONT…

- PRTG
  - PRTG Traffic Grapher is an easy to use Windows software that monitors bandwidth usage and other network parameters via SNMP.
  - PRTG Traffic Grapher monitors network and bandwidth usage as well as various other network parameters like memory and CPU usages, providing system administrators with live readings and periodical usage trends to optimize the efficiency, layout and setup of leased lines, routers, firewalls, servers and other Simple Network Management Protocol (SNMP) enabled network components.

PRTG Example



CONT…

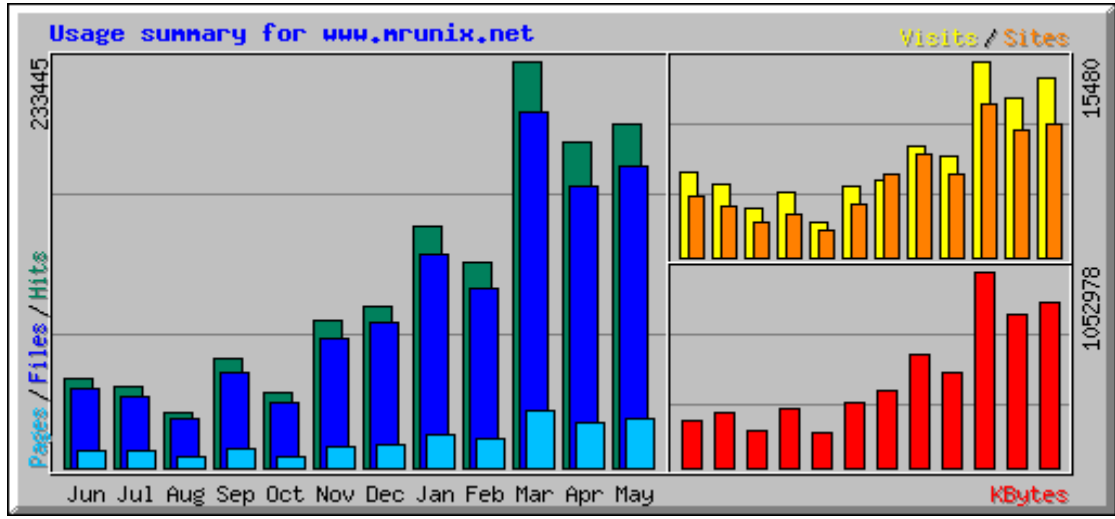
- Webalizer
  - ***The Webalizer*** is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

Usage Statistics for global netmon.oauife.edu.ng

Summary Period: May 2003
Generated 01-Jun-2003 04:14 WAT

[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

Monthly Statistics for May 2003		
Total Hits		131872976
Total Files		131872976
Total Pages		25
Total Visits		25
Total KBytes		240676917
Total Unique Sites		231504
Total Unique URLs		633168
Total Unique Referrers		1
Total Unique User Agents		1
	Avg	Max
Hits per Hour	177248	1003392
Hits per Day	4253966	9477854
Files per Day	4253966	9477854
Pages per Day	0	3
Visits per Day	0	3
KBytes per Day	7763772	21992252
Hits by Response Code		
Code 200 - OK		131872976



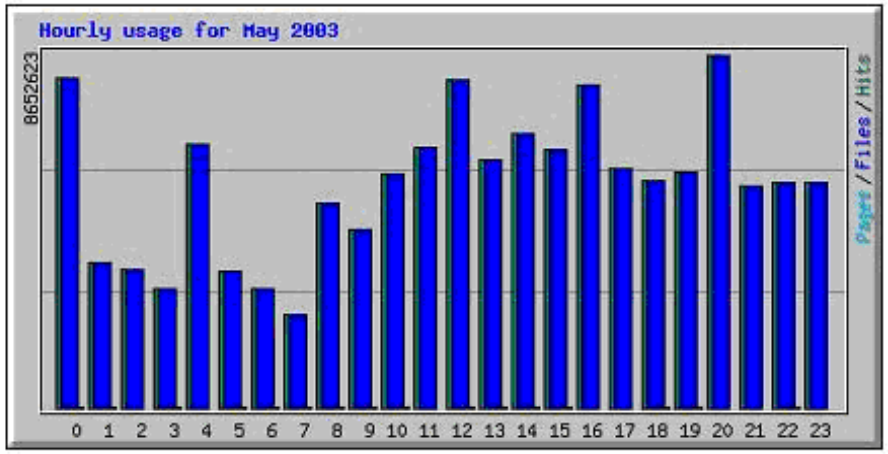


FIG. 7: Webalizer Global hourly usage

CONT…

- WebTrafMon
  - Web-based network traffic monitoring and analysis system.
  - Displays a list of hosts that are currently using the network and reports information concerning the IP(Internet Protocol) traffic generated and exchanged by each host.
  - Limitations….
- Can not Monitor and analyze the Fast Ethernet and Gigabit Ethernet
- Can not Analyze large log files

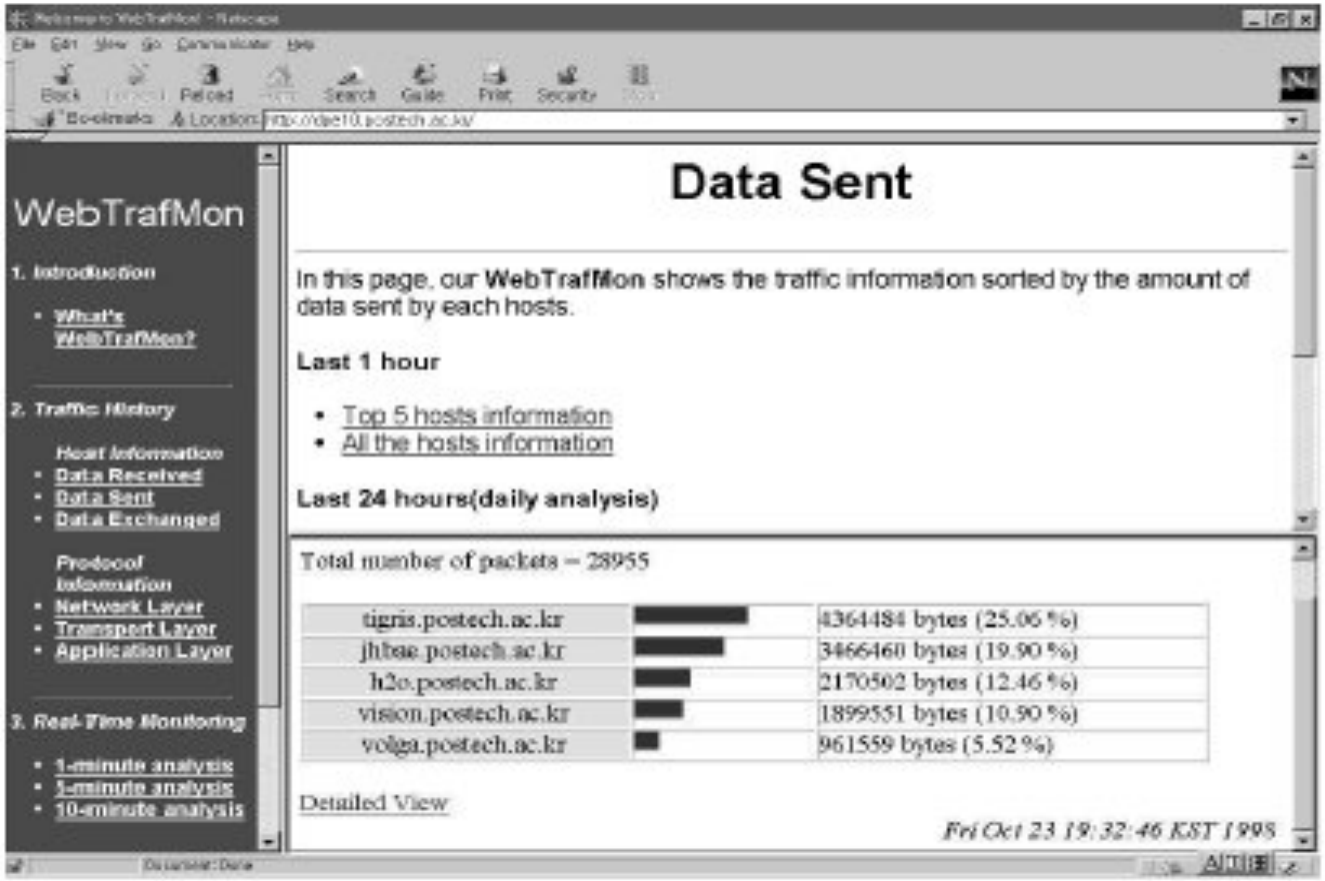


Fig. 6. Source host traffic analysis view.

Bandwidth measurement services

- http://www.2wire.com/?p=154
- http://www.speakeasy.net/speedtest/http://www.ookla.com/speedtest/
- http://reviews.cnet.com/7004-7254_70.html?tag=txt
- http://us.mcafee.com/root/speedometer/default.asp
- http://www.zapp.ro/buy/speedmeter/
- http://www.bandwidthplace.com/speedtest/
- http://reviews-zdnet.com.com/Bandwidth_meter/7004-7254_16-0.html
- http://bluefield.speedtest.frontiernet.net/ Bluefield WV http://bos.speakeasy.net Boston, speakeasy bandwidth speed test http://box54.org/SpeedTest.html Box 54 Server http://bugclub.org/BUGSpeed.html Brevard Users Group server Speed Test http://chi.speakeasy.net Chicago, speakeasy networked server speed test http://cookeville.speedtest.frontiernet.net/ Cookeville TN http://den.speakeasy.net Denver, speakeasy bandwidth speeds http://dfw.speakeasy.net Dallas, speakeasy bandwidth speeds http://download.enitel.no/speedtest/ Speed test - text download, Norway
- http://elkgrove.speedtest.frontiernet.net/ Elk Grove CA (Nice test site)
- http://gemal.dk/browserspy/bandwidth.html BrowserSpy, How fast is your connection...
- http://home.austin.rr.com/bc/bandwidth.htm RoadRunner of Austin, Texas http://home.broadpark.no/~tbjorgen-1/speedometer.html Lars-Magnus Lier http://home.cfl.rr.com/bjp/test.htm Brad's RoadRunner networked server speeds http://home.cfl.rr.com/cm3/speedtest7.htm Corley's RoadRunner Test page http://home.cfl.rr.com/eaa/SpeedTest.htm Eric's own RoadRunner Bandwidth Test http://homepage.tinet.ie/~leslie/testpage.htm 2 tests available.
- http://support.sbcglobal.net/dsl/speedtest/ http://us.mcafee.com/root/speedometer.asp Mcafee's SpeedOmeter (resurrected) http://w1.970.telia.com/~u97007522/ Speed test, Located in northern Sweden http://web.bitnet.net/dimension/ (Sweden - Borlange) http://web.bitnet.net/dimension/speedtest.htm Sweden, bandwidth speedtest http://web.tampabay.rr.com/giis/50.htm RoadRunner of Tampa Bay, FL http://webservices.cnet.com/Bandwidth/?tag=tm CNET's test. http://www.2wire.com/meter/bm.html 2Wire Bandwidth Meter. http://www.2wire.com/meter/bmresult.html?kbps=1863 2Wire Bandwidth Meter. http://www.aitsoft.com/Services/speedtest.asp AIT -- Services -- Speed Test http://www.alken.nl/ Online Speedtest etc. http://www.aroundcinci.com/speedtest/ speedtest home of Cincinati, Ohio http://www.austin.rr.com/speedtest/speed.asp RoadRunner home of Austin, Texas http://www.bandwidthplace.com/speedtest/ Bandwidth Place Welcome! http://www.beelinebandwidthtest.com/ Beeline Bandwidth Test, Amsterdam http://www.cable-modem.net/features/oct99/speed.html bandwidth speedtest http://www.computers4sure.com/speed.asp?iid=154 By mhmd, 4SURE.com bandwidth http://www.dagbladet.no/dinside/baandbredde/start.html Norway http://www.donspage.com/dsltest/speedtest.html online services bandwidth speed test http://www.dslreports.com/stest?loc=1 DSL Reports in Megapath, CA

Cont…

- http://www.eaglepro.net/bandwith/ Sweden bandwidth speed test http://www.ececs.uc.edu/~annexste/speed.html internet performance speedtest http://www.ececs.uc.edu/~annexste/speed100.html University of Cincinnati http://www.elkindustries.com/SpeedTest.htm Elk Industries Server Test http://www.info-techs.com/speedtest.html Information Technologies http://www.info-techs.com/speedtest50.html Lakeview Terrace, CA http://www.info-techs.com/speedtest500.html Lakeview Terrace, CA http://www.intercom.net/xpeedometer/xpeedometer.htm http://www.itcom.itd.umich.edu/adsl/speedtest.html broadband connection test http://www.midsouth.rr.com/speed.asp RoadRunner of the Mid-South Speed Test http://www.mordax.nl/ Netherlands internet speedtest http://www.numion.com/YourSpeed/Checkup.php?L=br connection performance http://www.numion.com/YourSpeed/Checkup.php?L=tw United Kingdom http://www.pcpitstop.com/internet/Bandwidth.asp speed test page for Fort Wayne,IN http://www.pcpitstop.com/internet/default.asp PC Pitstop's Internet Connection Center http://www.satx.rr.com/support/speedtest/ RoadRunner Speed Tests http://www.speedsuite.net/speedsuite/ Networked Speed test, Amsterdam http://www.speedtest.nl/ Netherlands http://www.squigly.com/performance/ cable speeds near Toronto, Canada http://www.summitcomputer.net/speedtest/unlisted/speedtest500.asp http://www.testmy.net/ Bandwidth Speed Test & Broadband Forum-Chat http://www.zensupport.co.uk/speedtest/ Zen's Web test http://speed.kify.com/
- http://speedtest.csloxinfo.com/
- www.adslthailand.com/bandwidthmeter/initialmeter.php
- http://wow.asianet.co.th/speedtest.php
- http://203.147.12.250/bwtest/initialmeter.php
- http://bandwidth.west.cat.net.th/meter.php
- http://media.thai2learn.com/meter/initialmeter.php
- http://www.ine.co.th/support/speed/meter.php
- http://wow.trueinternet.co.th/speedtest.php

Setting up Ntop

- Download Ntop
- Using a tar ball

```
tar xpfz ntop-3.0-4.tar.gz
./configure
make
make install
```

- http://rpm.pbone.net

- Installing with RPM is also easy. The package name may vary, but you simply use the command:

```
rpm –uvh ntop-3.0-4mdk.i586.rpm
```

- Run ntop (service ntop start)
- Go to a web browser type http://localhost:3000

Setting up MRTG

- Net-snmp
- Mrtg
- Snmpd.conf

```
# define RO community
      rocommunity     bow
      rwcommunity     bow


#First Map the community name “bow" into a "security name“
#               sec.name   source                              community
                com2sec    oaunet          default             bow

# Second, map the security name into a group name:

#               groupName      securityModel       securityName
      group                    oaugroup        v1                  oaunet
      group                    oaugroup        v2c                 oaunet
```

Snmpd.conf cont…

```
# Third, create a view for us to let the group have rights to:
#        name            incl/excl     subtree         mask(optional)
#view    systemview      included      system

view        all included            .1          80
# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write  notif
access  notConfigGroup ""      any       noauth    exact  systemview none none
```

Sample snmpd.conf file

```
rocommunity      bow
com2sec local          localhost              bow
com2sec mynetwork  10.105.1.0/24         bow

group  myRwgroup  any       local
group  myRogroup  any       mynetwork
view all    included  .1                    80
access myRogroup ""      any      noauth    all    none    none
access myRwgroup ""      any      noauth    all    all    all
```

Start your Snmp server and test it

- # chkconfig snmpd on
- Start the service snmpd (#service snmpd start)
- Run snmpwalk utility to request for a tree of info about network entity (query snmp server for your IP address assigned to etho, eth1, lo)
- #snmpwalk -c bow -v 1 localhost

Install mrtg

- Installing with RPM is also easy. The package name may vary, but you simply use the command:

  rpm –Uvh mrtg-2.10.5-3mdk

  Create a work directory

  mkdir /var/www/mrtg

  chmod 755 /var/www/mrtg

  Create the mrtg configuration file

  # cfgmaker --global "WorkDir: /var/www/mrtg" \
  --global "Options[_]: growright,bits" \
  --ifref=ip \
  bow@localhost > mrtg.cfg

Run mrtg using the Configuration file

- #mrtg /var/www/mrtg/mrtg.cfg
- Note: You may get few warning message for first time; ignore them. Run mrtg about 3 times
- View the graph using a browser
  - file//mrtg

THANK YOU