Network Monitoring & Performance

Network Performance Analysis

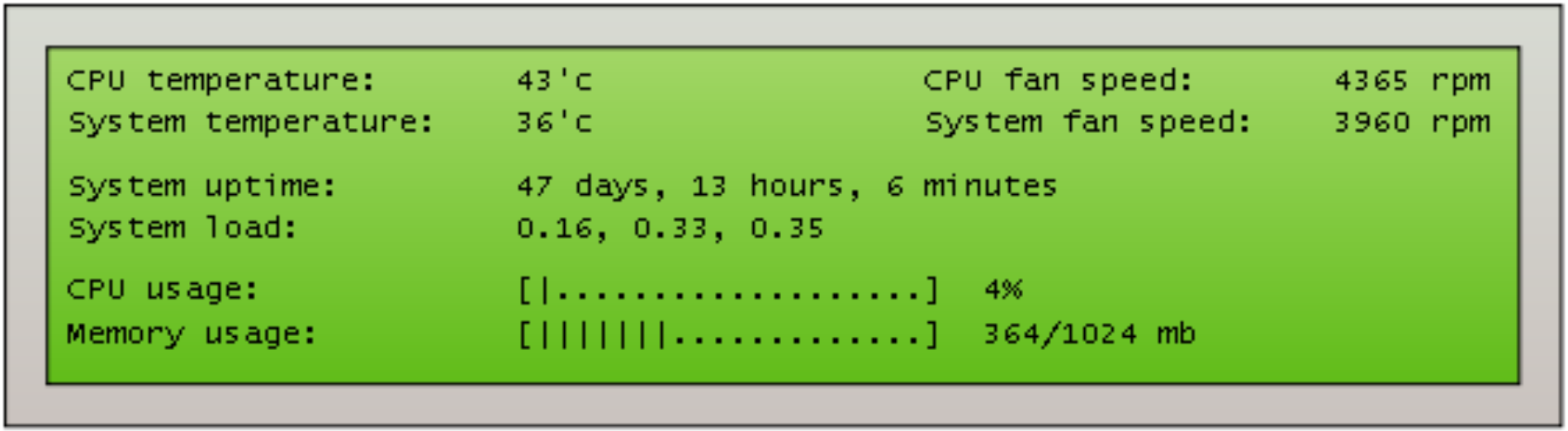
#3 Network Management System

Susmini I. Lestariningati, M.T

Definition

- **Network Monitoring** : the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS, or other alarm) in case of outages.
- **Network traffic measurement** is the process of measuring the amount and type of traffic on a particular network. This is especially important with regard to effective bandwidth management.

- While an intrusion detection system monitors a network for threats from the outside, a network monitoring system monitors the network for problems caused by overload and/or crashed servers, network connections or other devices.
    - for example, to determine the status of a web servers, monitoring software may periodically send and HTTP request to fetch page
    - for email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3
- Commonly measured metrics are *response time, availability and uptime*, although both consistency and reliability metrics are starting to gain popularity.


CPU temperature: 43'c
CPU fan speed: 4365 rpm
System temperature: 36'c
System fan speed: 3960 rpm
System uptime: 47 days, 13 hours, 6 minutes
System load: 0.16, 0.33, 0.35
CPU usage: [|.....] 4%
Memory usage: [|||||||.....] 364/1024 mb

- **Status request failures -** such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved - usually produce an action from the monitoring system.
- These actions vary -- an alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.
- Monitoring the performance of a network uplink is also known as network traffic measurement, and more software is listed there.

Motivation

- **Needs of service providers:**
  - Understand the behavior of their networks
  - Provide fast, high-quality, reliable service to satisfy customers and thus reduce churn rate
  - Plan for network deployment and expansion
  - SLA monitoring, Network security
  - Usage-based billing for network users (like telephone calls)
  - Marketing using CRM data
- **Needs of Customers:**
  - Want to get their money's worth
  - Fast, reliable, high-quality, secure, virus-free Internet access

Network Tomography

- Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/ Internet.

Route Analytics

- Route analytics is another important area of network measurement. It includes the methods, systems, algorithms and tools to monitor the routing posture of networks.
- Incorrect routing or routing issues cause undesirable performance degradation or downtime.

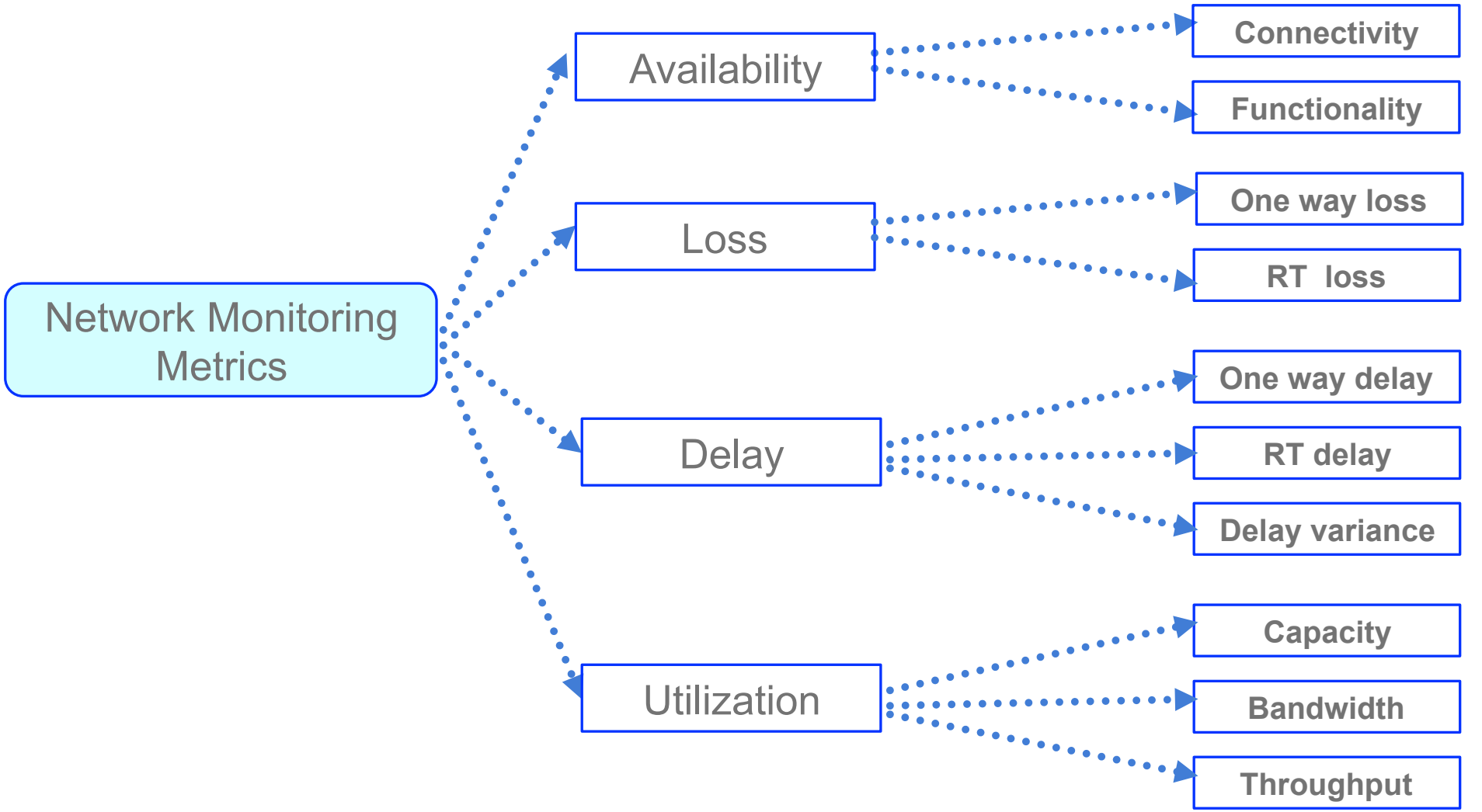
- Website monitoring service can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ICMP, SIP, UDP, Media Streaming and a range of other ports with a variety of check intervals ranging from every four hours to every one minute.
- Typically, most network monitoring services test your server anywhere between once-per-hour to once-per-minute.

Monitoring Server

- Monitoring an internet server means that the server owner always knows if one or all of his services go down.
- Server monitoring may be internal, i.e. web server software checks its status and notifies the owner if some services go down, and external, i.e. some web server monitoring companies check the services status with a certain frequency.
- Server monitoring can encompass a check of system metrics, such as CPU usage, memory usage, network performance and disk space. It can also include application monitoring, such as checking the processes of programs such as Apache, MySQL, Nginx, Postgres and others.

- External monitoring is more reliable, as it keeps on working when the server completely goes down. Good server monitoring tools also have performance benchmarking, alerting capabilities and the ability to link certain thresholds with automated server jobs such as provisioning more memory or performing a backup.

Network Monitoring Metrics



Network Monitoring Metrics

- Availability: The percentage of a specified time interval during which the system was available for normal use.
  - Connectivity: the physical connectivity of network elements.
  - Functionality: whether the associated system works well or not.
- Latency: The time taken for a packet to travel from a host to another.
  - Round Trip Delay = Forward transport delay + server delay + backward transport delay
  - Ping is still the most commonly used to measure latency.
- Link Utilization over a specified interval is simply the throughput for the link expressed as a percentage of the access rate.

Network Monitoring Metrics

- CAIDA Metrics Working Group (www.caida.org)
  - Latency
  - Packet Loss
  - Throughput
  - Link Utilization
  - Availability
- IETF's IP Performance Metrics (IPPM) Working Group
  - Connectivity (RFC 2687)
  - One-Way Delay (RFC 2679)
  - One-Way Packet Loss (RFC 2680)
  - Round Trip Delay (RFC 2681)
  - Delay Variation
  - Bulk transfer capacity

Monitoring Method

- Active Monitoring
- Passive Monitoring

Active Monitoring

- Performed by sending test traffic into network
  - Generate test packets periodically or on-demand
  - Measure performance of test packets or responses
  - Take the statistics
- Impose extra traffic on network and distort its behavior in the process
- Test packet can be blocked by firewall or processed at low priority by routers
- Mainly used to monitor network performance
- Active techniques (e.g. Iperf) are more intrusive but are arguably more accurate

Passive Monitoring

- Carried out by observing network traffic
  - Collect packets from a link or network flow from a router
  - Perform analysis on captured packets for various purposes
  - Network device performance degrades by mirroring or flow export
- Used to perform various traffic usage/characterization analysis/intrusion detection
- Passive techniques are of less network overhead and hence can run in the background to be used to trigger network management actions.

Comparison of Monitoring Approaches

	Active Monitoring	Passive Monitoring
Configuration	Multi-point	Single or multi-point
Data size	Small	Large
Network overhead	Additional traffic	- Device overhead - No overhead if splitter is used
Purpose	Delay, packet loss, availability	Throughput, traffic pattern, trend, & detection
CPU Requirement	Low to Moderate	High

Softwares

- Various software tools are available to measure network traffic. Some tools measure traffic by sniffing and others use SNMP, WMI or other local agents to measure bandwidth use on individual machines and routers.
- However, the latter generally do not detect the type of traffic, nor do they work for machines which are not running the necessary agent software, such as rogue machines on the network, or machines for which no compatible agent is available.

- In the latter case, inline appliances are preferred. These would generally 'sit' between the LAN and the LAN's exit point, generally the WAN or Internet router, and all packets leaving and entering the network would go through them. In most cases the appliance would operate as a bridge on the network so that it is undetectable by users.

Measurement tools generally have these functions and features:

- User interface (web, graphical, console)
- Real-time traffic graphs
- Network activity is often reported against pre-configured traffic matching rules to show:
  - Local IP address
  - Remote IP address
  - Port number or protocol
  - Logged in user name
- Bandwidth quotas
- Support for traffic shaping or rate limiting (overlapping with the network traffic control page)
- Support website blocking and content filtering
- Alarms to notify the administrator of excessive usage (by IP address or in total)

Some available tools

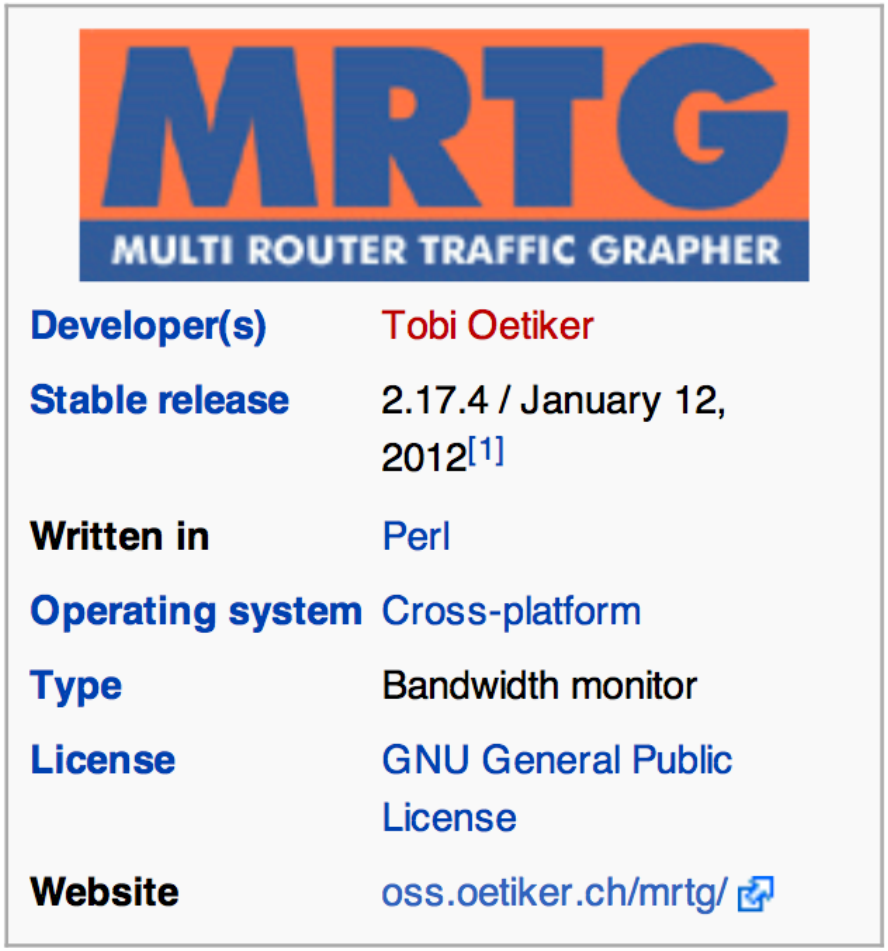
- **Argus** processes packets into detailed network flow audit data for operations, performance and security management.
- **Cacti** allows a user to poll services at predetermined intervals and graph the resulting data.
- **cFosSpeed** performs traffic classification and lets the user display, shape, tag or rate-limit protocols or programs under Windows.
- **FlowMon** is a complete solution for NetFlow monitoring and analysis including probes up to 10 Gbit/s, collectors and other supervision systems.
- **InterMapper** Originally developed for the Macintosh Classic in 1994 by the network manger of Dartmouth College this application uses SNMP, Ping and Netflow to build a graphical network map similar to HP Openview which shows bandwidth usage by port information and protocol. VLAN aware. Supported platforms: MacOS X, Linux and Windows.

- **LiveAction** provides real-time routing layer visualizations that allow the user to see and troubleshoot routes and implement policy-based routing.
- **MRTG**.
- **NetLimiter** is a traffic monitoring and shaping software for Windows.
- **OmniPeek** is an end-to-end network monitoring solution, offering support for many packet adapters and remote collectors.
- **Observium** is an autodiscovering network monitoring application focusing on extensive data collection and graphing of network infrastructure.
- **PRTG** runs on Windows, with graphical and web interfaces. It captures packets using Cisco Netflow or packet sniffing or uses SNMP to monitor bandwidth usages.

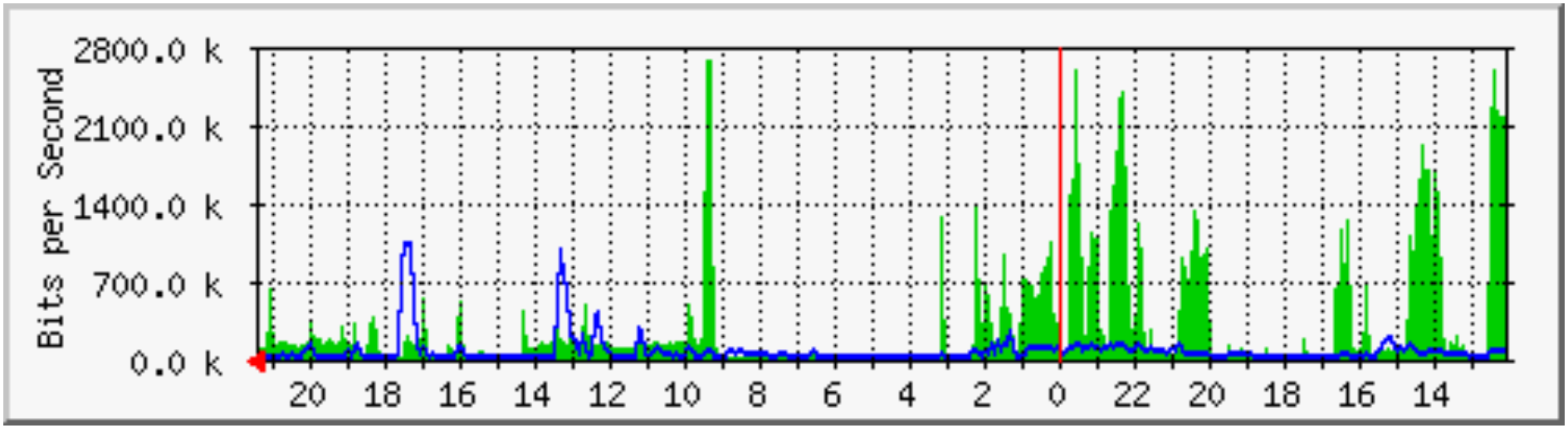
- **Wireshark** network packet logger, visualizer, inspector, some analyses.
- **PacketTrap** Networks - Traffic and Traffic Flow Analyzer
- **Scrutinizer** NetFlow and sFlow Analyzer provides deep visibility into network traffic behavior and trends. Leveraging NetFlow, J-Flow, and sFlow data, NetFlow Traffic Analyzer identifies which users and applications are consuming the most bandwidth.
- **Sparrowiq** Packet-based network traffic monitoring and analytics.
- **Sandvine** Intelligent Network Solutions measure and manage network traffic using Policy Traffic Switches
- **SevOne** Network Performance Monitoring System.

MRTG
(Multi Router Traffic Grapher)

- The Multi Router Traffic Grapher, or just simply MRTG, is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.
- It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.
- MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare.



Sample MRTG Bandwidth Graph

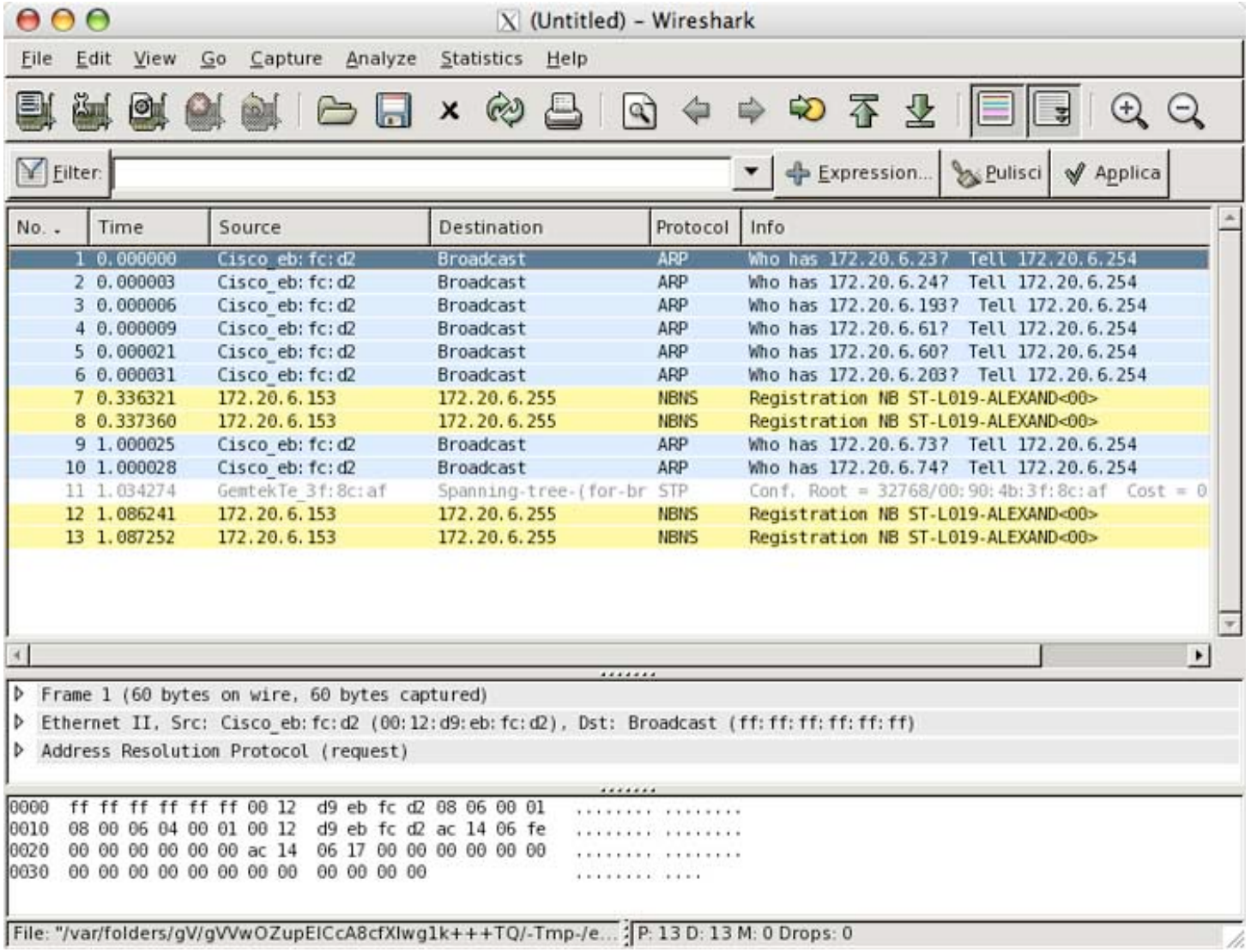


How It Works

- MRTG uses the Simple Network Management Protocol (SNMP) to send requests with two object identifiers (OIDs) to a device.
- The device, which must be SNMP-enabled, will have a management information base (MIB) to look up the OIDs specified.
- After collecting the information it will send back the raw data encapsulated in an SNMP protocol.
- MRTG records this data in a log on the client along with previously recorded data for the device. The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected devices in the server.

Wireshark

- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues


(Untitled) – Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Pulisci Applica
No. Time Source Destination Protocol Info
1 0.000000 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.23? Tell 172.20.6.254
2 0.000003 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.24? Tell 172.20.6.254
3 0.000006 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.193? Tell 172.20.6.254
4 0.000009 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.61? Tell 172.20.6.254
5 0.000021 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.60? Tell 172.20.6.254
6 0.000031 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.203? Tell 172.20.6.254
7 0.336321 172.20.6.153 172.20.6.255 NBNS Registration NB ST-L019-ALEXAND<00>
8 0.337360 172.20.6.153 172.20.6.255 NBNS Registration NB ST-L019-ALEXAND<00>
9 1.000025 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.73? Tell 172.20.6.254
10 1.000028 Cisco_eb:fc:d2 Broadcast ARP Who has 172.20.6.74? Tell 172.20.6.254
11 1.034274 GemtekTe_3f:8c:af Spanning-tree-(for-br STP Conf. Root = 32768/00:90:4b:3f:8c:af Cost = 0
12 1.086241 172.20.6.153 172.20.6.255 NBNS Registration NB ST-L019-ALEXAND<00>
13 1.087252 172.20.6.153 172.20.6.255 NBNS Registration NB ST-L019-ALEXAND<00>
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_eb:fc:d2 (00:12:d9:eb:fc:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 12 d9 eb fc d2 08 06 00 01 ....
0010 08 00 06 04 00 01 00 12 d9 eb fc d2 ac 14 06 fe ....
0020 00 00 00 00 00 00 ac 14 06 17 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
File: "/var/folders/gV/gVVwOZupEICcA8cfXIwg1k+++TQ/-Tmp-/e...
P: 13 D: 13 M: 0 Drops: 0

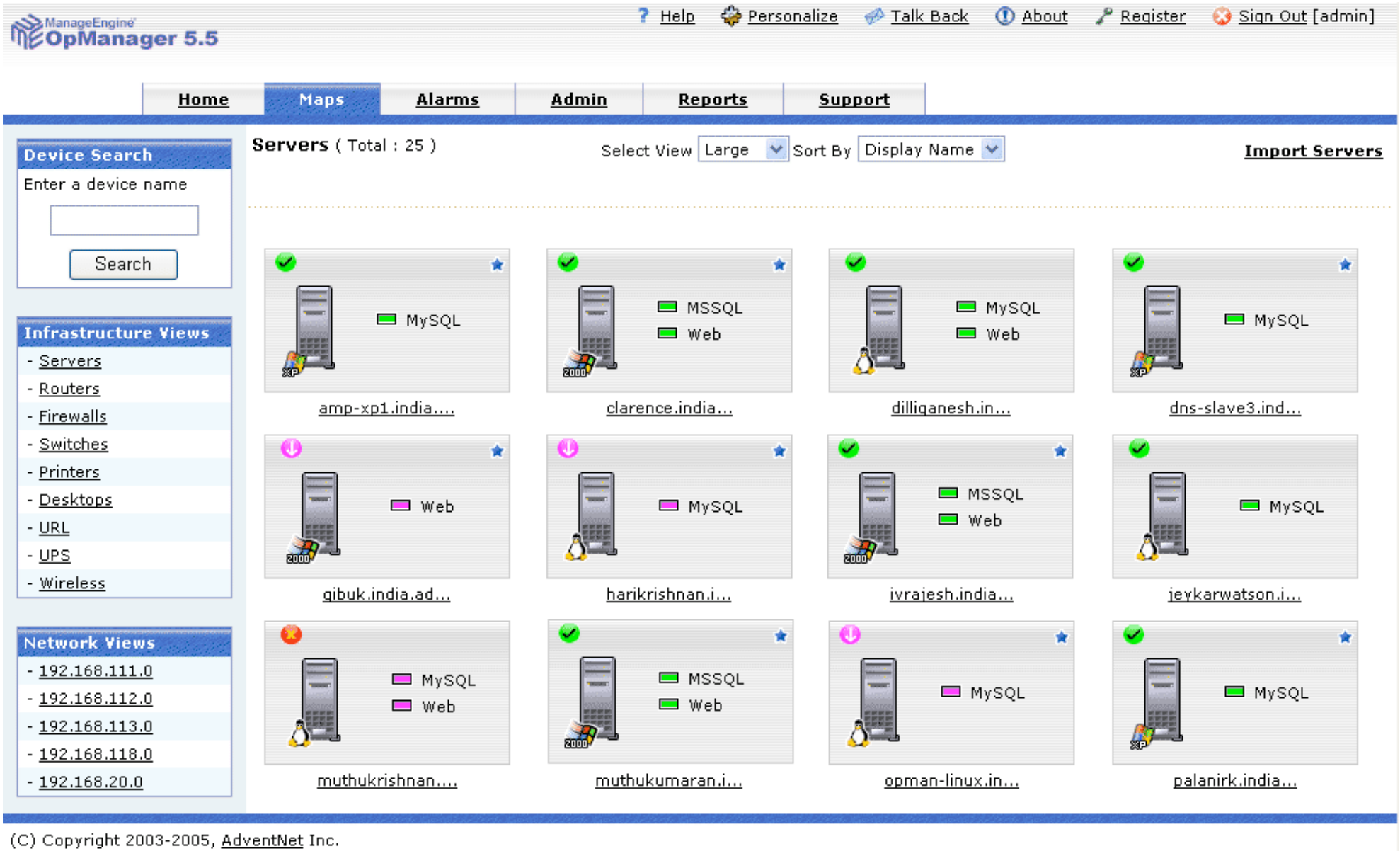
Features

- Data can be captured "from the wire" from a live network connection or read from a file that recorded already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.[16]
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.

OpManager


ManageEngine
OpManager
Buy Now!
Personalize
Help
About
Register
Sign Out [admin]
Trial period will expire in 19 days...
Home
Maps
Alarms
Admin
Reports
Support
Jump To
...Device Search...
Go
Overview
Network
Servers
Last 24 hours
Dashboard
Infrastructure Snapshot
Servers
Routers
Switches
Desktops
Firewalls
DomainControllers
Wireless
Printers
UPS
VOIP
Add | More
Business Snapshot
view1
VOIP
Caps
algeria
CRM
Global View
Add
Availability Distribution
16 18 20 22 00 02 04 06 08 10 12 14
100
75
50
25
0
Distribution(%)
99.99 - 100
99 - 99.99
90 - 99
50 - 90
10 - 50
0 - 10
Not Monitored
Recent Alarms
Source
Alarm Message
Shiva
Device not responding: Probably down or...
Suguna
Device not responding: Probably down or...
Prakasaraman
Probable device failure: No response fr...
Agni
Internal Problem - Paper Jam
Araman
Device Down: No response from device fo...
Appsec4
Web Service is Down
Advent-dual2
Device Down: No response from device fo...
Jaikrishnang
Device Down: No response from device fo...
Details
Alarms Graph
Server
Router
Switch
Desktop
Firewall
DomainController
Wireless
Printer
UPS
VOIP
60
50
40
30
20
10
0
Number of Alarms
Critical
Trouble
Attention
Service Down
© Copyright 2003-2007, AdventNet Inc.

OpManager


ManageEngine
OpManager 5.5
Help
Personalize
Talk Back
About
Register
Sign Out [admin]
Home
Maps
Alarms
Admin
Reports
Support
Device Search
Enter a device name
Search
Infrastructure Views
- Servers
- Routers
- Firewalls
- Switches
- Printers
- Desktops
- URL
- UPS
- Wireless
Network Views
- 192.168.111.0
- 192.168.112.0
- 192.168.113.0
- 192.168.118.0
- 192.168.20.0
Servers (Total : 25)
Select View Large
Sort By Display Name
Import Servers
MySQL
amp-xp1.india....
MSSQL
Web
clarence.india...
MySQL
Web
dilliganesh.in...
MySQL
dns-slave3.ind...
Web
qibuk.india.ad...
MySQL
harikrishnan.i...
MSSQL
Web
ivrajesh.india...
MySQL
jeykarwatson.i...
MySQL
Web
muthukrishnan....
MSSQL
Web
muthukumaran.i...
MySQL
opman-linux.in...
MySQL
palanirk.india...
(C) Copyright 2003-2005, AdventNet Inc.

Software in Network Monitoring and Management

- EPM
- The ping program
- SNMP servers
- IBM AURORA Network Performance Profiling System
- Intellipool Network Monitor
- Jumpnode
- Microsoft Network Monitor 3
- MRTG
- Nagios (formerly Netsaint)
- Netdisco
- NetQoS
- NetXMS Scalable network and application monitoring system

Software in Network Monitoring and Management

- Opennms
- PRTG
- Pandora (Free Monitoring System) - Network and Application Monitoring System
- PIKT
- RANCID - monitors router/switch configuration changes
- RRDtool
- siNMs by Siemens
- SysOrb Server & Network Monitoring System
- Sentinet3 - Network and Systems Monitoring Appliance
- ServersCheck Monitoring Software
- Cacti network graphing solution
- Zabbix - Network and Application Monitoring System
- Zenoss - Network and Systems Monitoring Platform
- Level Platforms - Software support for network monitoring

See You Next Week