

Nagios®



RRD TOOL

Network Monitoring Workshop

Dhruba Raj Bhandari

(CCNA)

Network/System Administrator

Mercantile Communication Pvt. Ltd.

NEPAL

dhruba@mos.com.np

Welcome!

Network Monitoring Workshop

Network Monitoring Concepts, Tools And
Deployment Procedures

18-27 February 2004, Kuala Lumpur, Malaysia

Assumptions & Objectives

Assumptions

- ? Know basic networking concept and fundamentals.
- ? Linux literate, knowledge of basic linux commands.
- ? Interest to learn.

Objectives

- ? Understand general concepts of Network Monitoring.
- ? Ability to configure Nagios, Apan, RRDtool, Nagios-statd, Snmp.
- ? Daily administration and maintenance.

Agenda

- ? Why Network Monitoring
- ? Various Network Monitoring Tools
- ? Why Nagios
- ? Live presentation of network monitoring application
Nagios with apan and rrdtool on pre-configured Nagios server
- ? Nagios, Apan, rrdtool installation procedure
- ? Step by step procedure to configure Nagios with apan, rrdtool, snmp, nagios-statd
- ? All students are requested to act together with presentation

Why Monitoring

- ? With large numbers of machines it is hard to keep track of what's going on without good monitoring tool
- ? To know the problems before manager ask you to do and before customer calls
- ? To keep network always sound and healthy
- ? Fault detection for networks, gateways and critical servers
- ? To notify an administrator of problems on time
- ? Documentation and visualization of the network
- ? Benefits of centralized administration
- ? Is must on networking environment

Ok Monitoring But How?

- ? With the help of system builtin commands i.e ping, traceroute, tcpdump, nmap, netstat etc.
- ? With some other commercial tools i.e network inspector
- ? With the help of open source or community contributed application i.e nagios, apan, mrtg, which we always prefer

What open source application available

- ? Nagios
- ? Angel Network Monitor
- ? Auto Status
- ? HiWAyS
- ? MARS
- ? Node Watch
- ? More on freshmeat.net

Why Nagios?

- ? Open source
- ? Very scaleable, Manageable, Secure and more
- ? Best documentation available
- ? Good log and database system
- ? Nice and attractive web interface
- ? Very flexiable
- ? Emails automatically sent if condition changes
- ? Verious notification options (Email, epager, mobilephone)

Why Nagios

- ? Avoidance of “Too many red flashing lights”
 - “Just the facts” – only want root cause failures to be reported, not cascade of every downstream failure.
 - also includes avoiding unnecessary checks
 - e.g. HTTP responding, therefore no need to ping
 - e.g. power outage, doesn't ping, so don't bother trying anything else
 - Services are running fine no need to do host-check-alive

- Individual node status
 - ? Is it up?
 - ? What is its load?
 - ? What is the memory and swap usage?
 - ? NFS and network load?
 - ? Are the partitions full?
 - ? Are applications and services running properly?
 - ? How about ping latency?
- Amalgamated node status
 - Same info but across groups of nodes

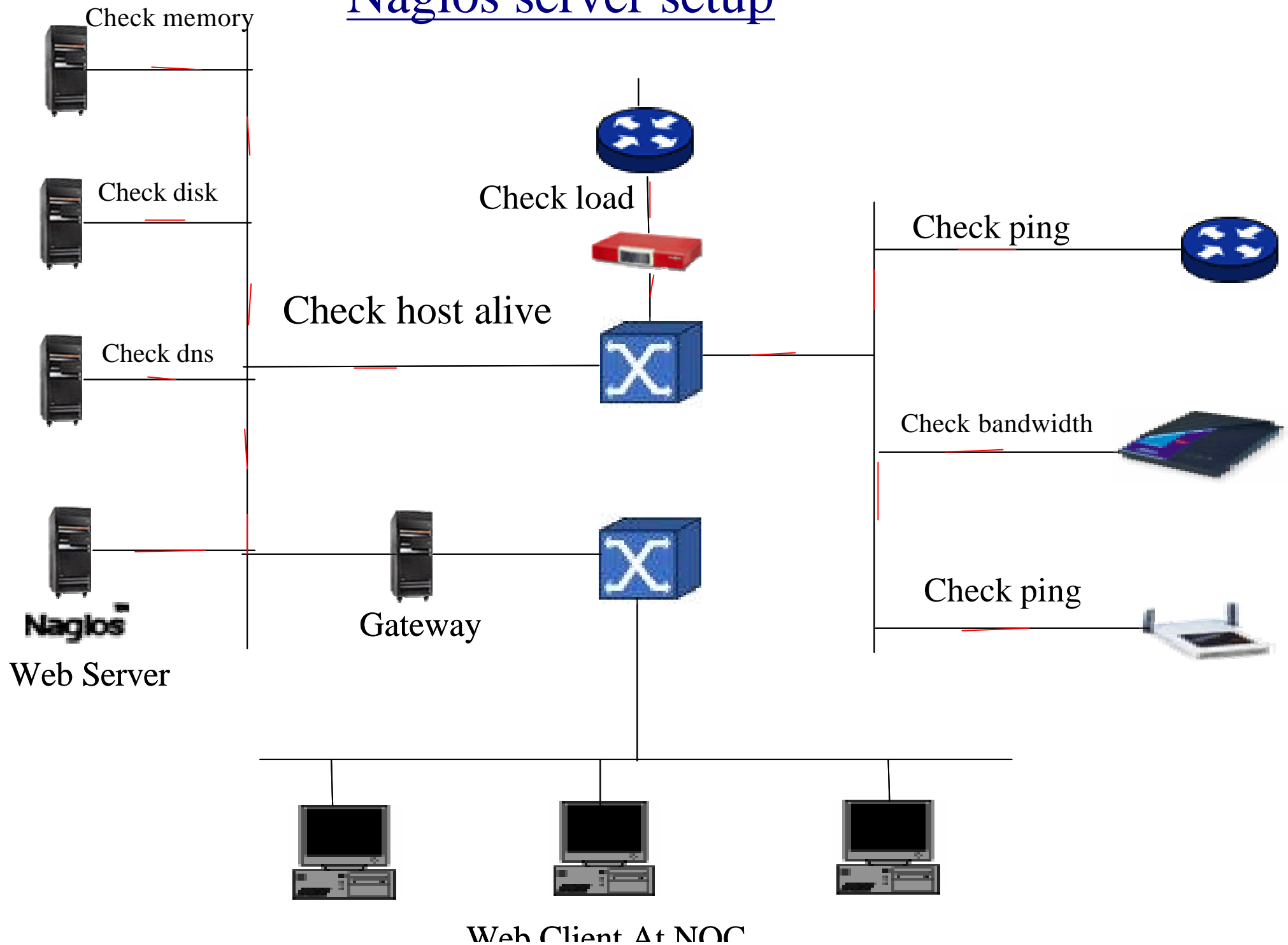
Nagios Feature

- Nagios (formerly Netsaint)
 - host and service monitor designed to inform you of network problems before your clients, end-users or managers do
 - Designed to run under the Linux operating system, but works fine under most *NIX variants
 - Monitoring daemon runs intermittent checks on hosts and services
 - uses external "plugins" which return status information to Nagios
 - when problems are encountered, the daemon can send notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.)
 - current status information, historical logs, and reports can all be accessed via a web browser
 - Nagios® is licensed under the terms of the GNU General Public License, Version 2, or any later version. For a complete text of the license, see the file COPYING.

Feature contd.

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoring of host resources (CPU load, disk and mem usage, etc.)
- Monitoring of environment / temperature
- Simple plugin design that allows users to easily develop their own host and service checks
- Ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved (via email, pager, or other user-defined method)
- Optional escalation of host and service notifications to different contact groups
- Support for implementing redundant and distributed monitoring servers
- Retention of host and service status across program restarts
- Ability to acknowledge problems via the web interface
- Web interface for viewing current network status, notification and problem history, log file, etc
- Simple authorization scheme that allows you restrict what users can see and do from the web interface

Nagios server setup



– Nagios Status Detail screen

https://thuldai.mos.com.np/nagios/index.html

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems**
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications

Current Network Status

Last Updated: Sun Feb 1 12:17:48 NPT 2004
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as *dhruba*

[View Service Status Detail For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
226	5	0	16	0

All Problems	All Types
21	247

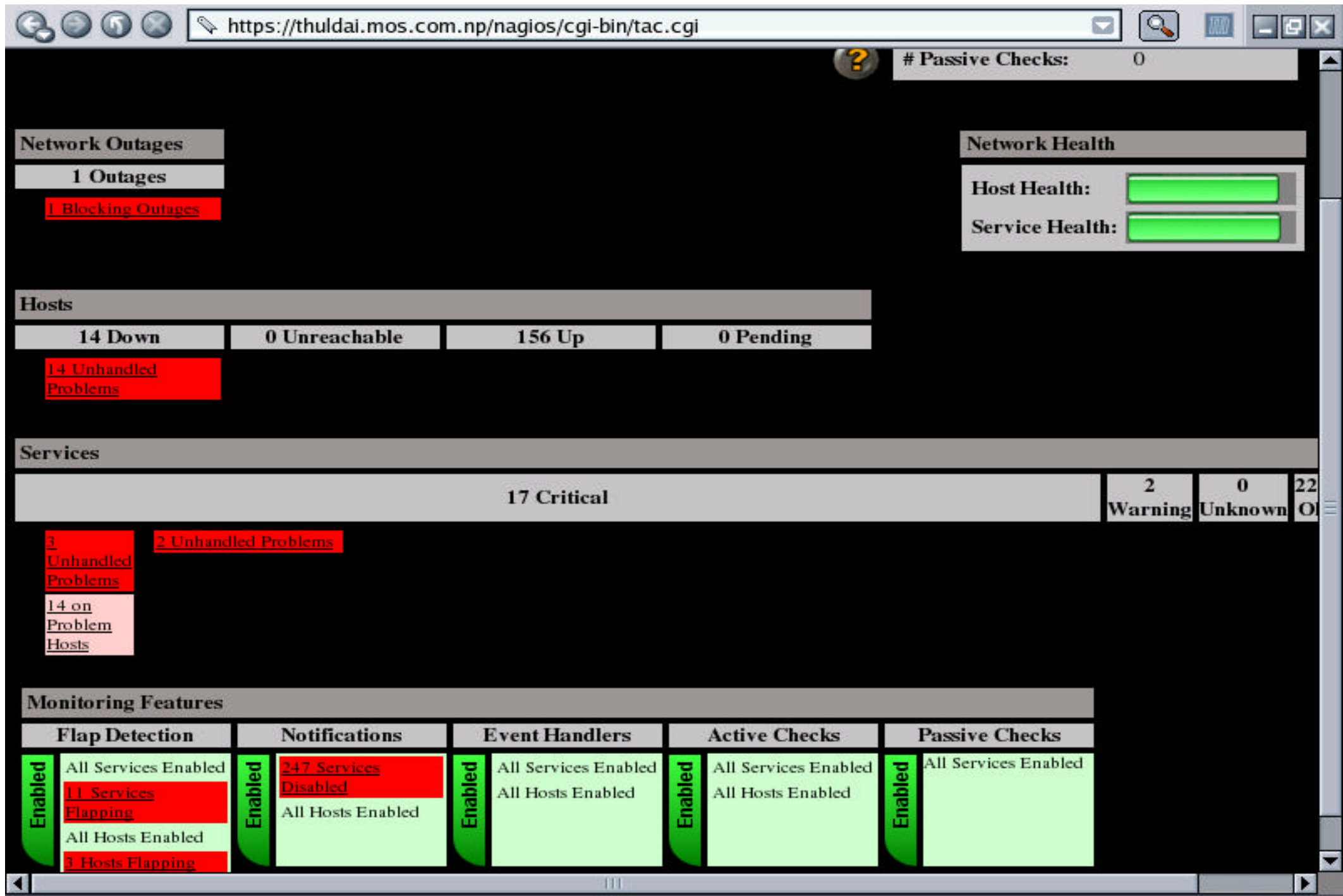
Display Filters:

Host Status Types: All problems
Host Properties: Any
Service Status Types: All
Service Properties: Any

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
CHILDREN-FIRST	DOWN	02-01-2004 12:13:59	1d 19h 10m 33s	PING CRITICAL - Packet loss = 100%
DANIDA	DOWN	02-01-2004 12:15:55	1d 0h 43m 12s	PING CRITICAL - Packet loss = 100%
DASS	DOWN	02-01-2004 12:08:59	4d 0h 40m 42s	PING CRITICAL - Packet loss = 100%
FNCCI	DOWN	02-01-2004 12:12:38	4d 0h 40m 2s	PING CRITICAL - Packet loss = 100%
ITLINK	DOWN	02-01-2004 12:15:55	0d 1h 37m 12s	PING CRITICAL - Packet loss = 100%
Laz-cnet	DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss = 100%

Tactical Overview Of Nagios



Service Detail of Nagios

Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

←

→

↶

✕

<https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all>

Search

Current Network Status
 Last Updated: Sun Feb 1 09:57:47 NPT 2004
 Updated every 90 seconds
 Nagios® - www.nagios.org
 Logged in as *dhruba*

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
228	3	0	16	0

All Problems	All Types
19	247

?

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
ACTIONAID	Ping	OK	02-01-2004 09:53:07	0d 12h 20m 9s	1/3	PING OK - Packet loss = 0%, RTA = 2 ms
AFP	Ping	OK	02-01-2004 09:55:38	0d 13h 40m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
AGNIPAGE	Ping	OK	02-01-2004 09:55:27	0d 0h 0m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
BRTSCHOOL	Ping	OK	02-01-2004 09:54:06	1d 18h 7m 39s	1/3	PING OK - Packet loss = 0%, RTA = 8 ms
Ban-cat	Ping	OK	02-01-2004 09:56:11	0d 22h 44m 39s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms

Transferring data from thuldai.mos.com.np...

Current S

[root@dhr

?

Sun Feb 01, 9:26 PM

Service Types

Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

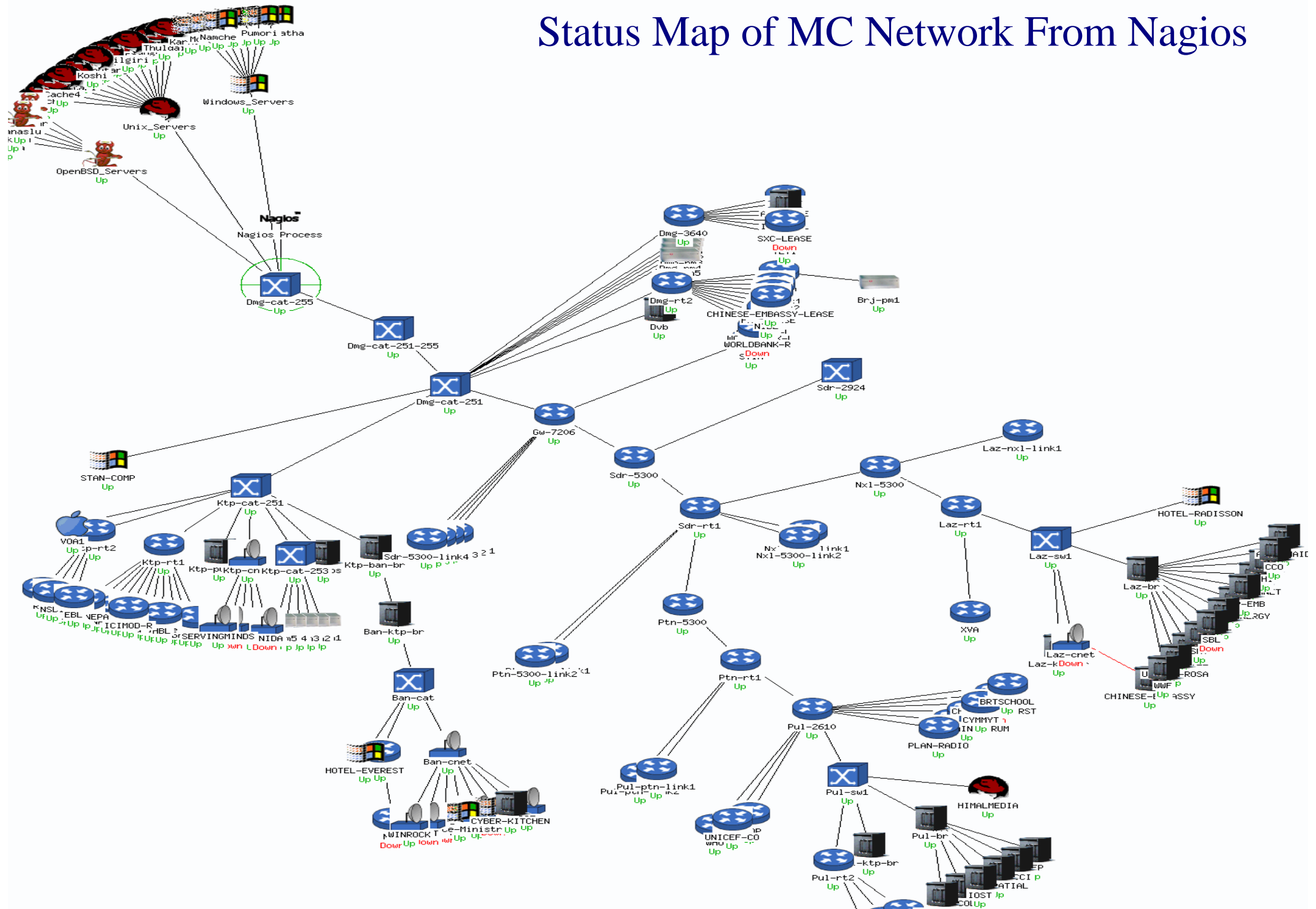
https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all Search

Host	Service	Status	Output
Kailash	Cpu-usage	OK	SNMP OK: usr-cpu:1, sys-cpu:1,
	FTP	OK	FTP OK - 0.007 second response time port 21 [220 kailash.mos.com.np FTP server ready.]
	Free-Memory	OK	SNMP OK: Ram-Free:3100,
	HTTP	OK	HTTP ok: HTTP/1.1 200 OK - 0.021 second response time
	Load	OK	SNMP OK: 1MIN-Load:0.08, 5MIN-Load:0.05, 15MIN-Load:0.00,
	Ping	OK	PING OK - Packet loss = 0%, RTA = 0 ms
	disk_usage	OK	Disk utilization: All disks OK
Karnali	Ping	OK	PING OK - Packet loss = 0%, RTA = 1 ms
Kopila	Cpu-usage	OK	SNMP OK: usr-cpu:0, sys-cpu:1,
	Free-Memory	OK	SNMP OK: Ram-Free:3808,
	Load	OK	SNMP OK: 1MIN-Load:0.18, 5MIN-Load:0.19, 15MIN-Load:0.18,
	POP	OK	POP OK - 0.028 second response time port 110 [+OK <8832.1075610415@kopila.mos.com
	Ping	OK	PING OK - Packet loss = 0%, RTA = 1 ms
Koshi	Ping	OK	PING OK - Packet loss = 0%, RTA = 9 ms

Done

Mozilla-bi [root@dhr ? Sun Feb 01, 9:56 PM













Status Map of MC Network From Nagios











Status Overview from nagios

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all

All Routers @Durbar Marg-KTM (Routers@DMG)

Host	Status	Services	Actions
Dmg-3640	UP	1 OK	   
Dmg-rt2	UP	1 OK	   
Gw-7206	UP	1 OK	   





















All Routers @Kantipath-KTM (Routers@KP)

Host	Status	Services	Actions
Ktp-rt1	UP	1 OK	   
Ktp-rt2	UP	1 OK	   

















All Routers @Lazim

Host	Status	Services
Laz-nx1-link1	UP	1 OK
Laz-rt1	UP	1 OK

All Routers @POPs w/ Lease Link (Routers@POPsL)

Host	Status	Services	Actions
Bri-gw	UP	1 OK	   
Bri-gw	UP	1 OK	   
Bri-link1	UP	1 OK	   
Bri-link2	UP	1 OK	   
Htd-lease	DOWN	1 CRITICAL	   

















All Routers @POPs w/ VSAT Link (Routers@POPsV)

Host	Status	Services	Actions
Bri-2501	UP	1 OK	   
Btl-vsai	UP	1 OK	   
Htd-vsai	UP	1 WARNING	   
Nam-gw	UP	1 OK	   





All Routers @Sundhara

Host	Status	Services
Ptn-rt1	UP	1 OK

All Routers @Pulchowk-KTM (Routers@PUL)

Host	Status	Services	Actions
Pul-2610	UP	1 OK	   
Pul-ptn-link1	UP	1 OK	   
Pul-ptn-link2	UP	1 OK	   
Pul-rt2	UP	1 OK	   

All Routers @Sundhara (Routers@SDR)

Host	Status	Services	Actions
Sdr-rt1	UP	1 OK	   

All Routers @Xpressway (Routers@X)

Host
AGNIPAGE
BRTSCHOOL

Status Summery Based On Hostgroup

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all&style=summary

Status Summary For All Host Groups

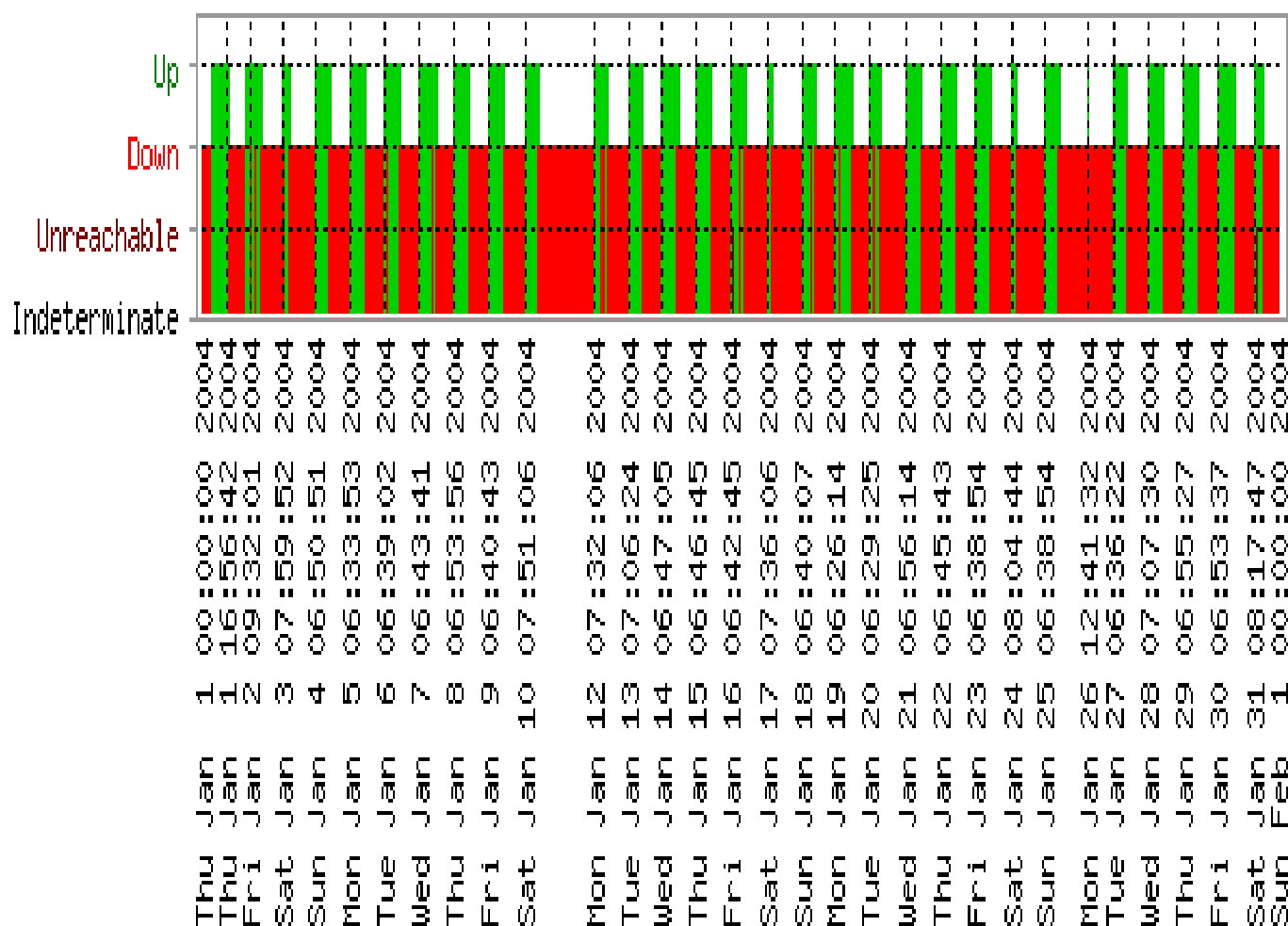
Host Group	Host Status Totals	Service Status Totals
Access Servers@KTM (AS@KTM)	11 UP	11 OK
All Routers @KTM (Routers@KTM)	7 UP	7 OK
All Routers @MIX Customers w/ Radio Link (Routers@MIXR)	1 UP	1 OK
All Routers @Xprewway Customers w/ Radio Link (Routers@XpresswayR)	19 UP 1 DOWN	19 OK 1 CRITICAL
All Routers @Xprewway Customers w/ Radio Link (Cnet_Clients@XpresswayR)	6 UP 4 DOWN	5 OK 5 CRITICAL
All Cnets @KTM (Cnets@KTM)	2 UP 1 DOWN	2 OK 1 CRITICAL
All Co-located Servers (Co-locators)	2 UP	2 OK
Ipricot DVB @DMG (DVB@DMG)	1 UP	1 OK
All Email-alert-only Boxes (E-boxes)	1 UP	1 OK
All Livingston Portmasters @Kathmandu (Portmasters@KTM)	10 UP	10 OK
All Livingston Portmasters @MC-POPs (Portmasters@POPs)	1 UP	1 WARNING
All Routers @Baneshor (Routers@BAN)	1 UP	1 OK
All Routers @Durbar Marg-KTM (Routers@DMG)	3 UP	3 OK
All Routers @Kantipath-KTM (Routers@KP)	2 UP	2 OK
All Routers @Lazimpat (Routers@LAZ)	2 UP	2 OK
All Routers @POPs w/ Lease Link (Routers@POPxL)	4 UP 1 DOWN	4 OK 1 CRITICAL

Host Trends or Status History

Apex
Trends

State History For Host 'Don_Bosco'

Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004



State Breakdowns:

Up : (32.6%) 10d 2h 21m 41s

Down : (67.1%) 20d 19h 17m 27s

Unreachable : (0.3%) 0d 2h 5m 12s

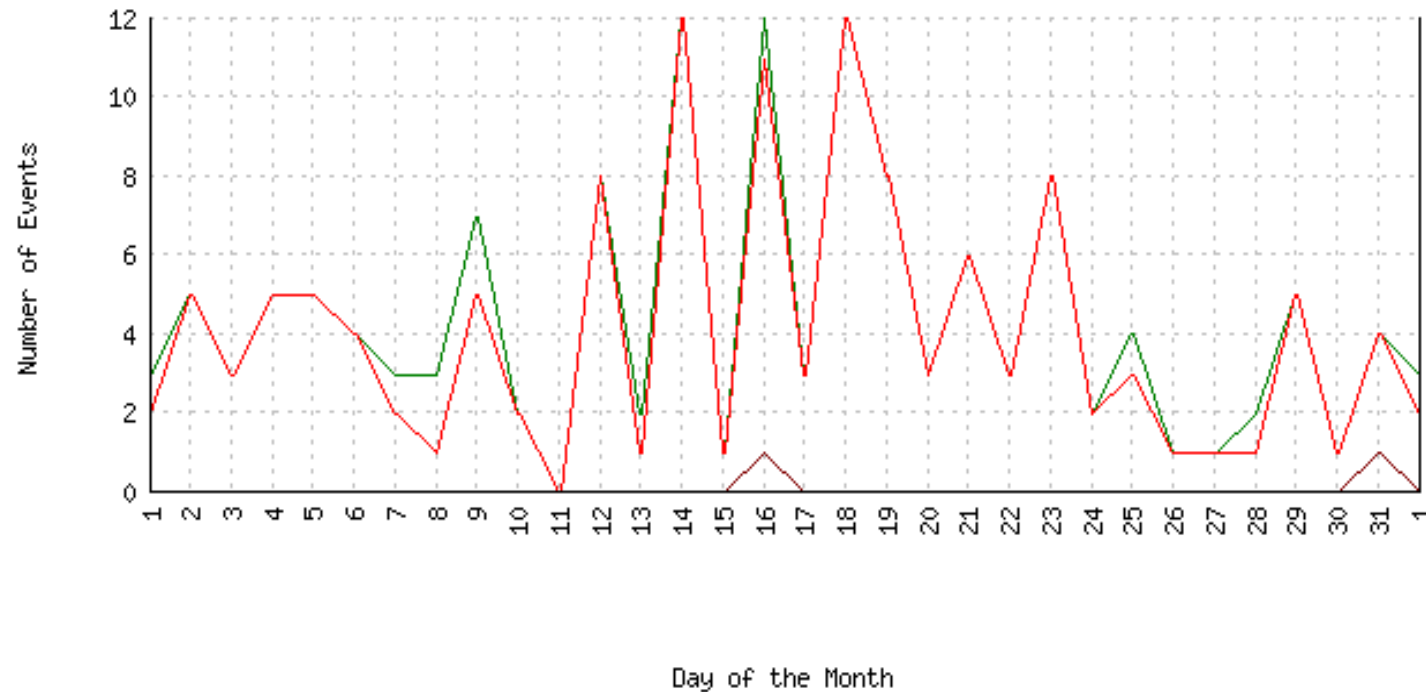
Indeterminate: (0.0%) 0d 0h 15m 40s



Histogram Of Host

 Histogram

Event History For Host 'Don_Bosco'
Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06




Event Logs

Browser address bar: <https://thuldai.mos.com.np/nagios/cgi-bin/showlog.cgi>

Current Event Log
Last Updated: Sun Feb 1 12:15:31 NPT 2004
Nagios® - www.nagios.org
Logged in as *dhruba*

Log File Navigation
Sun Feb 1 00:00:00 NPT 2004
to
Present..

☐ **Older Entries First:**

 **Latest Archive**

File: /usr/local/nagios/var/nagios.log

February 01, 2004 12:00

- [02-01-2004 12:14:28] HOST NOTIFICATION: Amod;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:28] HOST NOTIFICATION: Amod;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:28] HOST NOTIFICATION: DeepakA;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:28] HOST NOTIFICATION: Krishna;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:27] HOST NOTIFICATION: NirajS;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:27] HOST NOTIFICATION: Prabhu;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:27] HOST NOTIFICATION: Ravin;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:27] HOST NOTIFICATION: Ravin;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:14:27] HOST NOTIFICATION: Upendra;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:12:16] SERVICE ALERT: SDC;Ping;WARNING;HARD;1;PING WARNING - Packet loss = 60%, RTA = 23.73 ms
- [02-01-2004 12:12:16] HOST ALERT: SDC;DOWN;HARD;1;PING CRITICAL - Packet loss = 100%
- [02-01-2004 12:11:09] SERVICE ALERT: Htd-vsai;Ping;WARNING;HARD;3;PING WARNING - Packet loss = 40%, RTA = 674.22 ms
- [02-01-2004 12:10:26] SERVICE ALERT: Htd-lease;Ping;WARNING;HARD;3;PING WARNING - Packet loss = 40%, RTA = 385.85 ms
- [02-01-2004 12:08:58] SERVICE FLAPPING ALERT: WORLDBANK-R;Ping;STOPPED; Service appears to have stopped flapping (3.8% change < 5.0% threshold)
- [02-01-2004 12:08:49] HOST NOTIFICATION: Gyanu;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms
- [02-01-2004 12:08:48] HOST NOTIFICATION: Ishwar;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms
- [02-01-2004 12:08:48] HOST NOTIFICATION: Kedar;Htd-lease;UP;host-notify-by-epager;PING OK - Packet loss = 30%, RTA = 357.24 ms
- [02-01-2004 12:08:48] HOST NOTIFICATION: MSurya;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms

Who are Notified?



Contact Notifications

Last Updated: Sun Feb 1 12:07:59 NPT 2004
Nagios® - www.nagios.org
Logged in as *dhruba*

All Contacts

Log File Navigation

Sun Feb 1 00:00:00
NPT 2004
to
Present..

Latest
Archive



Notification detail level for all contacts:

All notifications

Older Entries First:



Update



File: /usr/local/nagios/var/nagios.log

Host	Service	Type	Time	Contact	Notification Command	Information
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	NirajS	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:10	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:08	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Gyanu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Ishwar	host-notify-by-email	PING CRITICAL - Packet loss = 100%



nautil Mozil [root@



Sun Feb 01, 11:37 PM

Notification Email Sample

From: nagios@thuldai.mos.com.np

To: "ishwars@mos.com.np" <ishwars@mos.com.np>

Subject: Host DOWN alert for WORLDBANK-L!

Date: 05/02/04 11:09

***** Nagios *****

Notification Type: PROBLEM

Host: WORLDBANK-L

State: DOWN

Address: 202.52.239.70

Info: PING CRITICAL - Packet loss = 100%

Date/Time: Thu Feb 5 11:06:38 NPT 2004

APAN



Apan.sourceforge.net

- ? Is used to collect result from Nagios plugins and stores it in RRD-files
- ? APAN-Advance Performance Addon for Nagios
- ? Can be used to view graphs of data in Nagios web-interface
- ? It creates graphs on the fly
- ? A wonderful stuff

Oh! What is RRD-tool Again

- ? Is a tool to create round robin database file
- ? Is not a linear database which keep appending to the table when new data is arrived
- ? Size of an rrdtool database is determined at the time of creation
- ? RRDtool database is a kind of perimeter of a circle, when new data reaches the starting point it overwrite the existing data.
- ? It is both frontend and backend tool
- ? But we use it as a backend tool, our front end is APAN

RRDtool



www.rrdtool.com

- Round Robin Database for time series data storage
- Command line based
- From the author of MRTG
- Made to be faster and more flexible
- Includes CGI and Graphing tools, plus APIs
- Solves the Historical Trends and Simple Interface problems

Define Data Sources (Inputs)

? DS : speed : COUNTER : 600 : U : U

? DS : fuel : GAUGE : 600 : U : U

- DS = Data Source
- speed, fuel = “variable” names
- COUNTER, GAUGE = variable type
- 600 = heart beat – UNKNOWN returned for interval if nothing received after this amount of time
- U:U = limits on minimum and maximum variable values (U means unknown and any value is permitted)

Define Archives (Outputs)

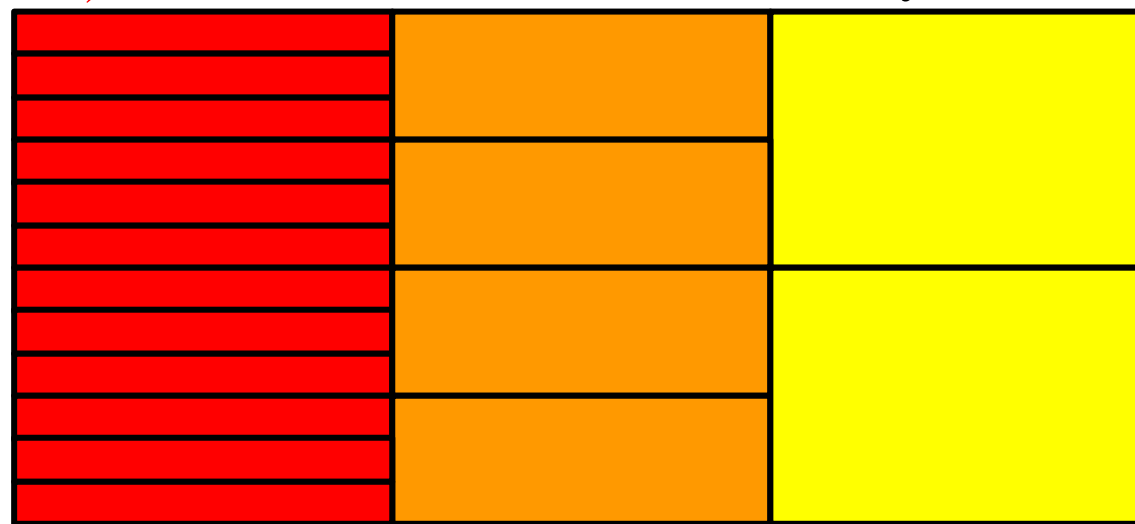
- ? RRA:AVERAGE:0.5:1:24
- ? RRA:AVERAGE:0.5:6:10
 - RRA = Round Robin Archive
 - AVERAGE = consolidation function
 - 0.5 = up to 50% of consolidated points may be UNKNOWN
 - 1:24 = this RRA keeps each sample (average over one 5 minute primary sample), 24 times (which is 2 hours worth)
 - 6:10 = one RRA keeps an average over every six 5 minute primary samples (30 minutes), 10 times (which is 5 hours worth)
- **Clear as mud!**
 - all depends on original step size which defaults to 5 minutes

RRDtool Database Format

Recent data stored once every
5 minutes for the past 2 hours
(1:24)

Old data averaged to one
entry per day for the last 365
days (288:365)

--step
300
(5 minute
input step
size)



RRA
1 : 24

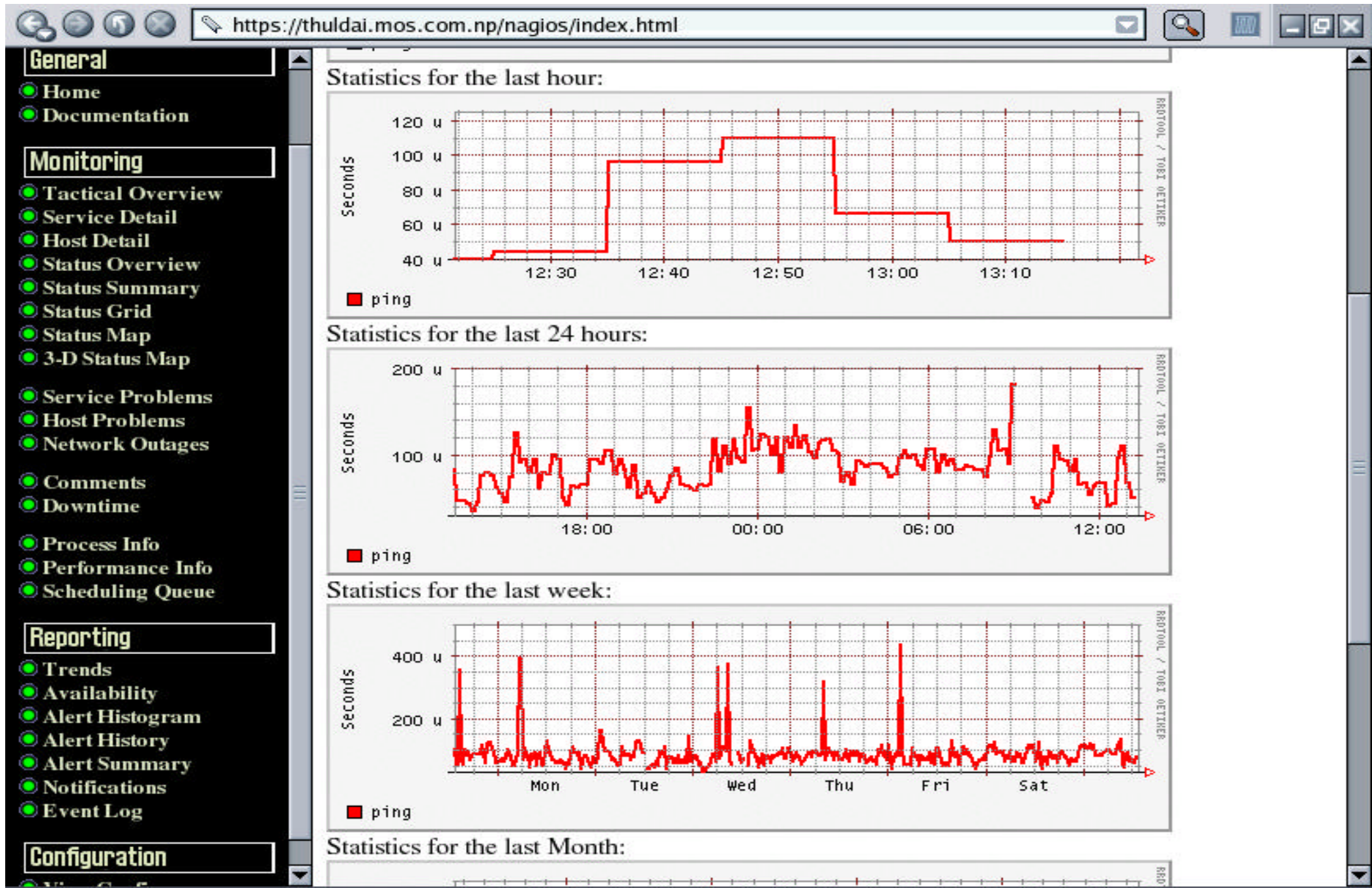
RRA
6 : 10

RRA
288 : 365

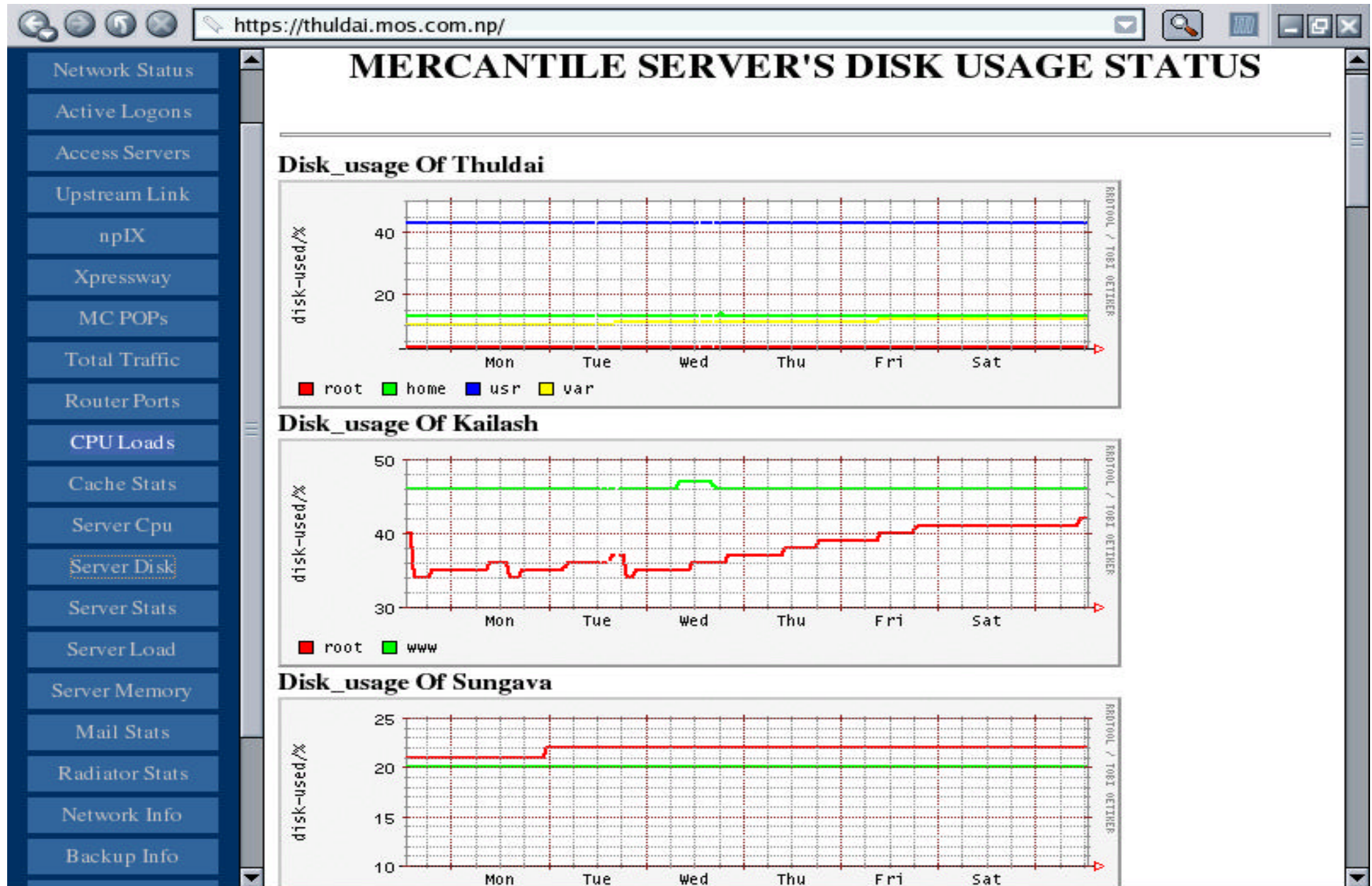
RRD
File

Medium length data averaged to one
entry per half hour for the last 5 hours
(6:10)

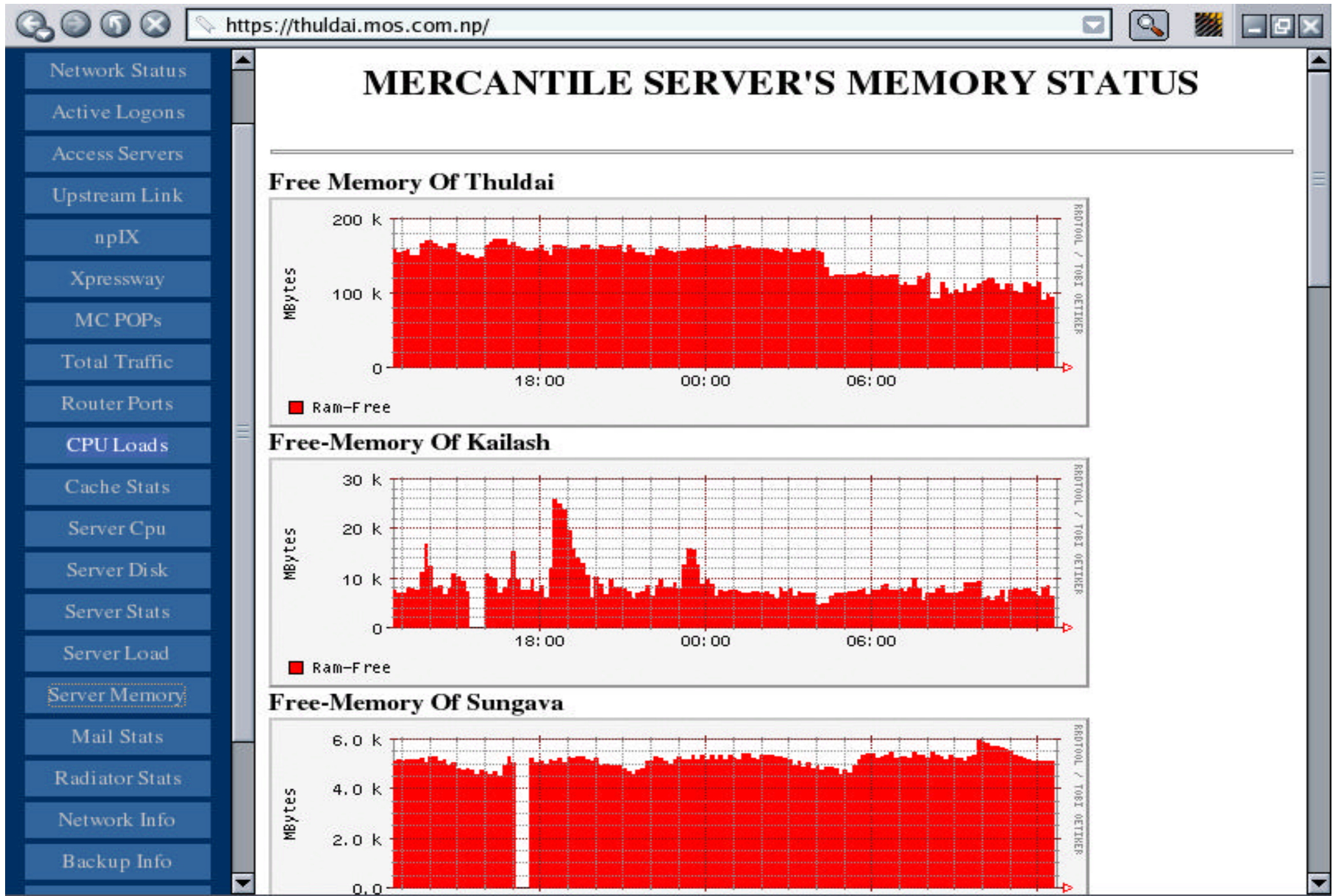
Ping Latency Graph Created by Apan form rrd Database



Disk Usage



Free Memory



Network Status

Active Logons

Access Servers

Upstream Link

npIX

Xpressway

MC POPs

Total Traffic

Router Ports

CPU Loads

Cache Stats

Server Cpu

Server Disk

Server Stats

Server Load

Server Memory

Mail Stats

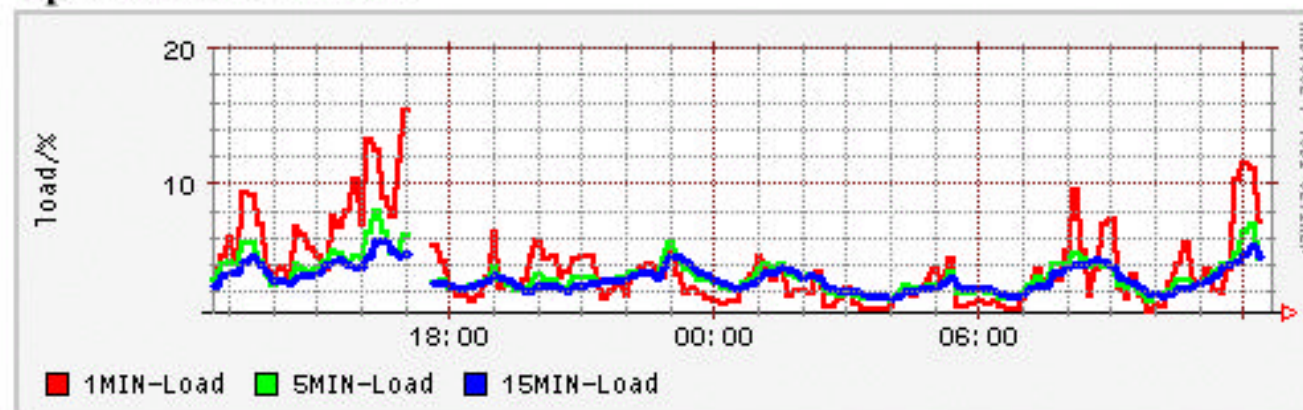
Radiator Stats

Network Info

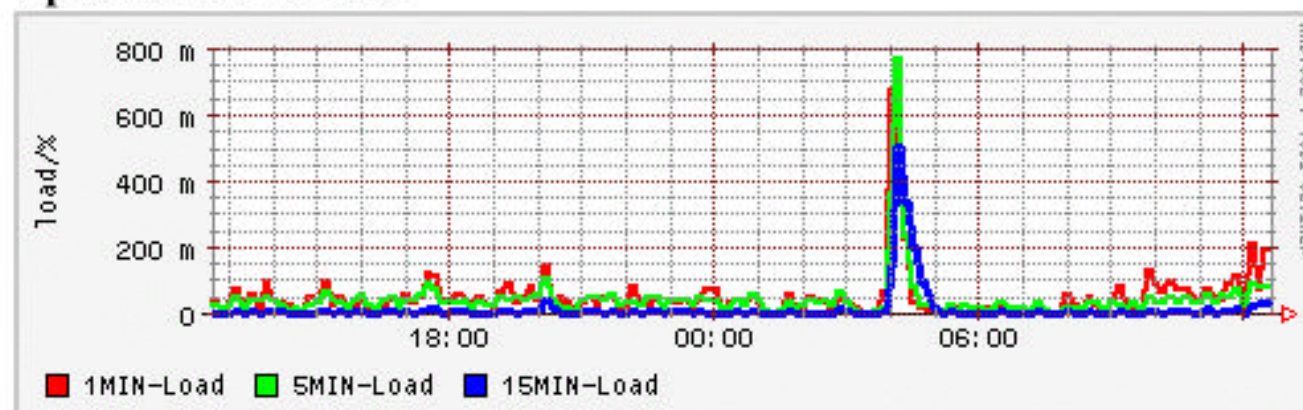
Backup Info

MERCANTILE SERVER'S LOAD STATUS

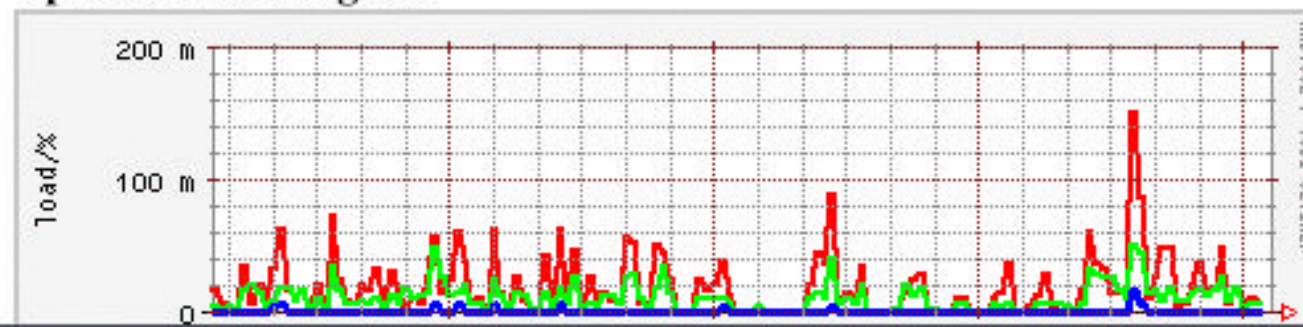
Cpu Load Of Thuldai



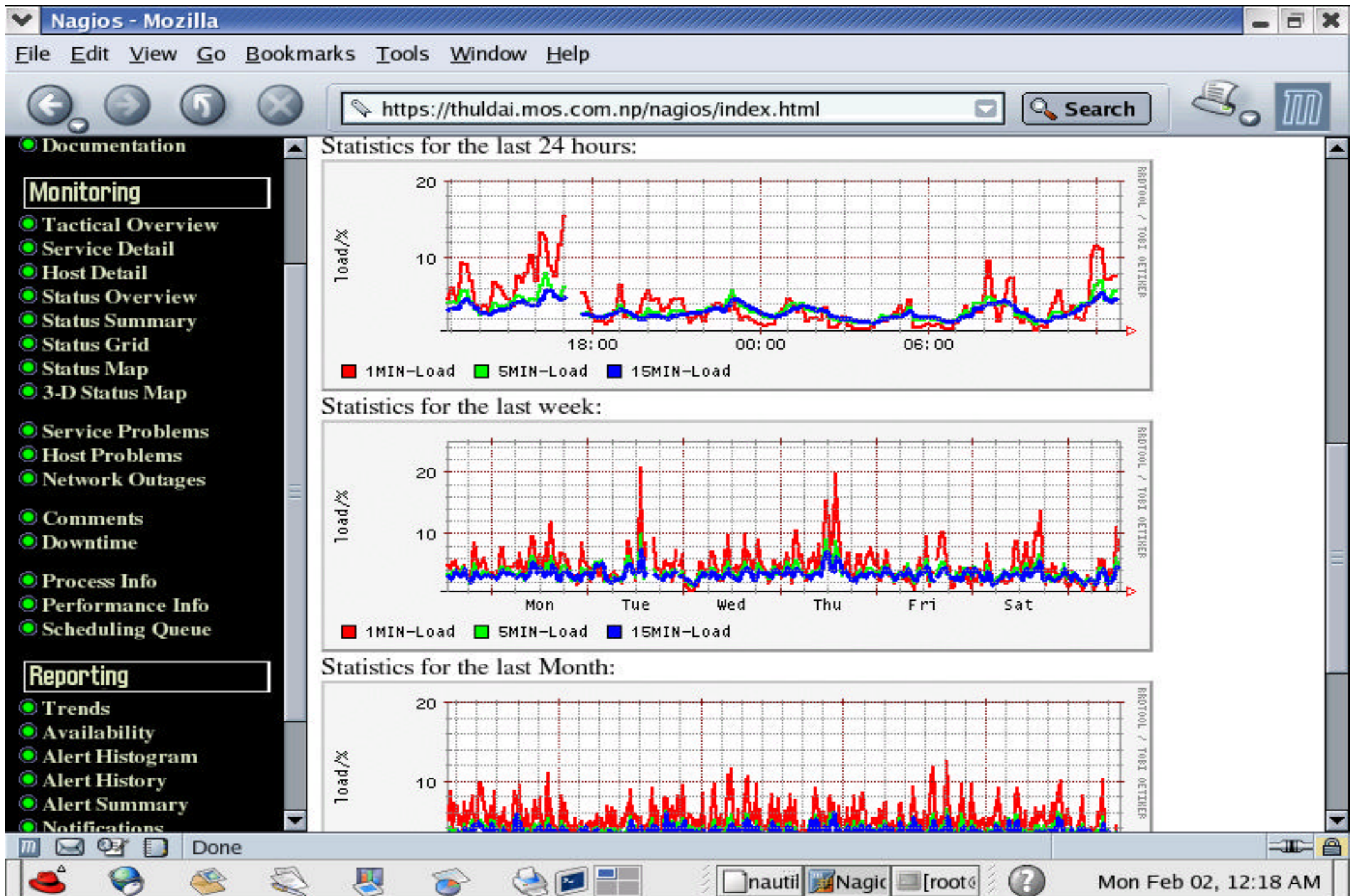
Cpu Load Of Kailash



Cpu Load Of Sungava



Server load detail of particular host



Nagios-statd

- ? Nagios-statd is the daemon program that listens for connection from clients
- ? It forks off a new daemon for each incoming connection.
- ? The forked daemon executes a series of typical UNIX command and return output to the client
- ? It is installed on the host to be monitored
- ? It is designed to be integrated with the nagios monitoring tool

Nagios-stat

- ? Nagios-stat is the client that connects to the nagios-statd server
- ? It then sends the daemon which check it want to run, parse the data, prints a result and then exits appropriately
- ? It is installed on nagios server at /usr/local/nagios/libexec/nagios-stat as plugin
- ? Both nagios-statd and nagios-stat programs together comprise a systems monitoring tool for various platform

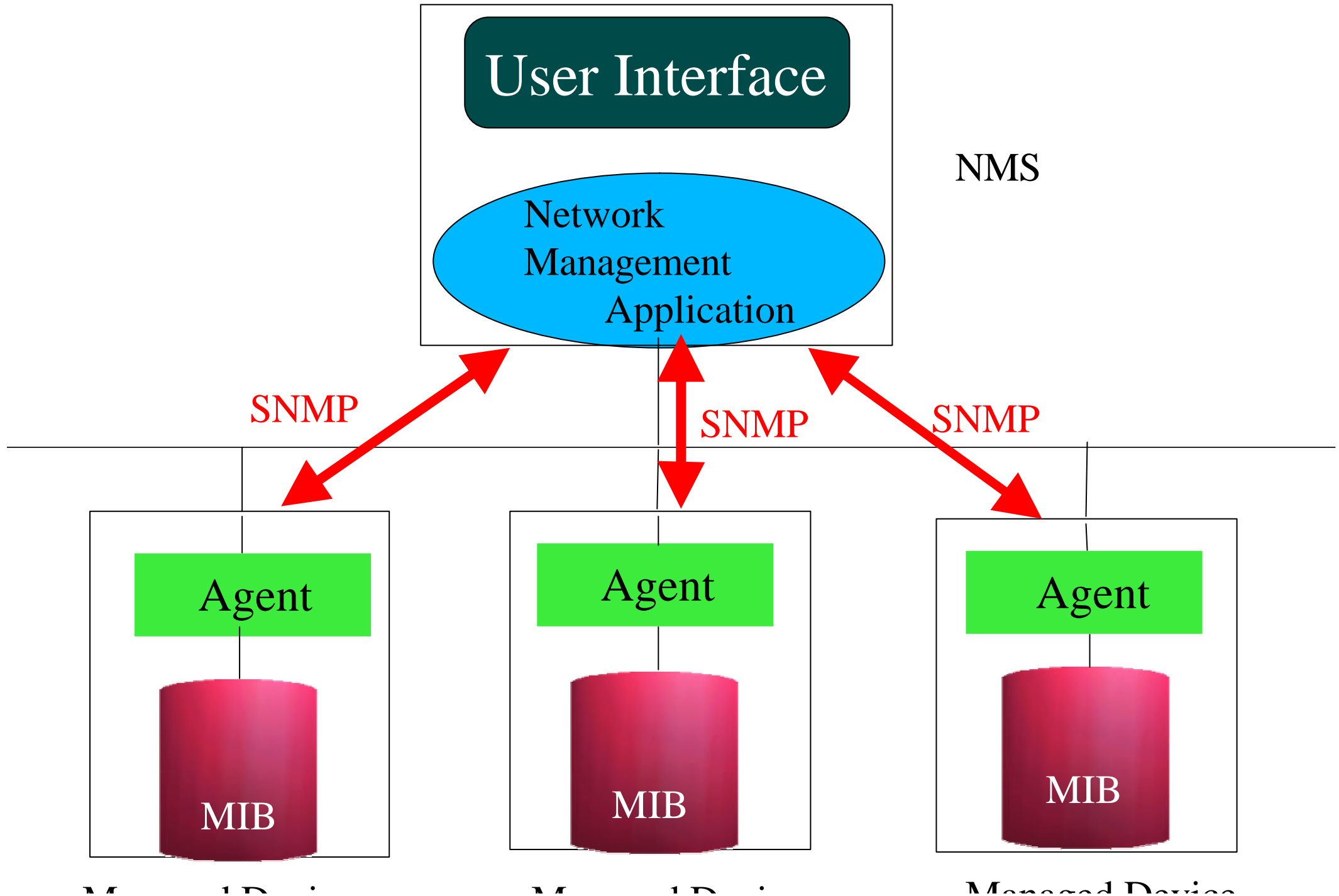
Snmp

- ? A request-reply protocol run on udp port 161
- ? Operate between management-station and an agent
- ? Nagios server is mainly a management-station and monitored nodes are agent
- ? Snmp agent need to be installed and running on to monitor snmp based services through nagios.
- ? Required packages are: net-snmp and net-snmp-utils

Snmp How?

- ? Management Information base (MIB) is a database which contain various information about system i.e. Memory, cpu-usage, routing table information, inerfaces statistics etc.
- ? Or it is a set of managed object
- ? We need access to managed objects, but how?
- ? With the help of “OID” object identifier
- ? OID is a series of integer that represent the hierarchical value of mib managed strings

Internet Management Model



Snmp manager utilities

- ? Net-snmp-utils rpm contains required utilities i.e. Snmpwalk, snmpget etc
- ? .1.3.6.1.4.1.2021.10.1.3.1 is a oid to get 1 munit
- ? average load of linux box
- ? Snmpget -c <community name> <ip or hostname> oid
- ? Snmpget -c public 192.168.10.1 .1.3.6.1.4.1.2021.10.1.3.1
- ? Snmpwalk -v1 192.168.10.1 -c public (to test weather snmp agent is running or not on remote node)
- ? Some important oids are available at our server name is “Imp linux oids”

How to enable snmp agent on cisco router

my-router# configure terminal

? Create access-list so that only specific host can query

my-router(config)# access-list 99 permit 202.52.255.25

my-router(config)# snmp-server community IacH25 RO 99

my-router(config)# end

? RO is for read Only

? 99 is access-list applied

How to run snmp agent on linux

```
# rpm -qa | grep snmp
```

`net-snmp` and `net-snmp-utils` need to be installed

```
#cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bkup
```

```
# vi /etc/snmp/snmpd.conf
```

d shift+G

```
rocommunity public 202.52.255.225
```

? For more options check `/etc/snmp/snmpd.conf.bkup`

? For interactive configuration run following command

```
# snmpconf -g basic_setup
```

```
#!/sbin/chkconfig --level 235 snmpd on
```

```
#!/sbin/service snmnd start
```

Some Imp OIDs

? To get cpu stuff:

a) Load:

1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1

5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2

15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3

b) CPU:

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0

raw user cpu time: .1.3.6.1.4.1.2021.11.50.0

percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0

raw system cpu time: .1.3.6.1.4.1.2021.11.52.0

percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0

raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0

raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

Some Imp OIDs

? To get memory stuff:

Total Swap Size:	.1.3.6.1.4.1.2021.4.3.0
Available Swap Space:	.1.3.6.1.4.1.2021.4.4.0
Total RAM in machine:	.1.3.6.1.4.1.2021.4.5.0
Total RAM used:	.1.3.6.1.4.1.2021.4.6.0
Total RAM Free:	.1.3.6.1.4.1.2021.4.11.0
Total RAM Shared:	.1.3.6.1.4.1.2021.4.13.0
Total RAM Buffered:	.1.3.6.1.4.1.2021.4.14.0
Total Cached Memory:	.1.3.6.1.4.1.2021.4.15.0

? To get incoming and outgoing octets on interface

interfaces.ifTable.ifEntry.ifInOctets.2	.1.3.6.1.2.1.2.2.1.10.2
interfaces.ifTable.ifEntry.ifOutOctets.2	.1.3.6.1.2.1.2.2.1.16.2

Questions?

Installation steps

- ? Nagios
- ? Nagios Plugins
- ? Web Interface
- ? RRDtool
- ? Apan
- ? Logos and images
- ? Nagios- statd
- ? Configuration

Nagios Installation

- ? Login as a root user
- ? `#useradd nagios`
- ? `#passwd nagios` (enter password “nagios”)
- ? `#cd /home/nagios`
- ? `#scp -r nagios@<server_ip>:/home/nagios/ .`
- ? `#ll /home/nagios` (you should see all tars other directories copied on there)
- ? `#mkdir /usr/local/nagios`
- ? `#chown nagios: /usr/local/nagios`

Nagios Installation

- ? `#cd /home/nagios`
- ? `#gunzip nagios-1.1.tar.gz`
- ? `#tar -xvf nagios-1.1.tar`
- ? `#cd nagios-1.1`
- ? `#./configure`
- ? `#make all`
- ? `#make install`
- ? `#make install-init`
- ? `#make install-commandmode`
- ? `#make install-config`
- ? `#chmod 755 /etc/rc.d/init.d/nagios`

Plugin Installation

- ? `#cd /home/nagios`
- ? `#gunzip nagios-plugins-1.3.1.tar.gz`
- ? `#tar -xvf nagios-plugins-1.3.1.tar`
- ? `#cd nagios-plugins-1.3.1`
- ? `#./configure`
- ? `#make all`
- ? `#make install`
- ? `#chown -R nagios: /usr/local/nagios/libexec`
- ? Verify that all plugins are installed at
/usr/local/nagios/libexec and are owned by nagios

Secured Web Interface Installation

? #vi /etc/httpd/conf/httpd.conf (locate the place where alias are defined)

ScriptAlias /nagios/cgi-bin/ /usr/local/nagios/sbin/

<Directory "/usr/local/nagios/sbin/">

AllowOverride AuthConfig

Options ExecCGI

Order allow,deny

Allow from all

</Directory>

Alias /nagios/ /usr/local/nagios/share/

<Directory "/usr/local/nagios/share">

AllowOverride AuthConfig

Order allow,deny

Allow from all

</Directory>

Web Authentication

? #su nagios

? \$ cd /usr/local/nagios/sbin

? \$ vi .htaccess

AuthName "Nagios Access"

AuthType Basic

AuthUserFile /usr/local/nagios/etc/htpasswd.users

require valid-user

? Save & exit

? \$htpasswd -c /usr/local/nagios/etc/htpasswd.users nagios

? Enter password nagios

? \$chmod 644 /usr/local/nagios/etc/htpasswd.users

? \$ cp /usr/local/nagios/sbin/.htaccess /usr/local/nagios/share/.

? Verify that cgi.cfg has line **use_authentication=1**

Logos and Images

- ? Logos and images make user to easily identify the devices on network
- ? Make look of nagios more professional
- ? Status map looks pretty
- ? Logos are to be copied at
/usr/local/nagios/share/images/logos
- ? `$ cp /home/nagios/logos/*
/usr/local/nagios/share/images/logos/.`

RRDtool Installation

- ? \$ cd /home/nagios
- ? \$ gunzip rrdtool.tar.gz
- ? \$ tar -xvf rrdtool.tar
- ? \$ cd rrdtool-1.0.45/
- ? \$./configure
- ? \$ make

RRDtool Installation

```
? $ su
? # make install
? # cd /usr/local/rrdtool-1.0.45/bin/
? # cp * /usr/local/bin/
? # su nagios
? $ mkdir /usr/local/nagios/rrd
? $ chmod 777 /usr/local/nagios/rrd/
```

Apan Installation

- ? `$ cd /home/nagios`
- ? `$ gunzip apan-0.2.1.tar.gz`
- ? `$ tar -xvf apan-0.2.1.tar -C /usr/local/nagios/`
- ? `$ cd /usr/local/nagios/apan`
- ? Fix the bug on apan.sh
- ? `$ vi apan.sh`

Change `CONF = `grep "${HOST}; ${SVCNAME}`

to

`CONF = `grep “^${HOST}; ${SVCNAME}`

Apan Installation

- ? `$ chmod -R 755 plugs/`
- ? `$ cp apan.cgi generate.cgi /usr/local/nagios/sbin/`
- ? `$ chmod 775 /usr/local/nagios/sbin/apan.cgi`
- ? `$ chmod 775 /usr/local/nagios/sbin/generate.cgi`
- ? `$ cp graph.png
/usr/local/nagios/share/images/logos/`
- ? `$ cp -a libexec/* /usr/local/nagios/libexec/.`

Nagios-statd Installation

- ? `$ cd /home/nagios`
- ? `$ gunzip nagios-statd-3.08.tar.gz`
- ? `$ tar -xvf nagios-statd-3.08.tar`
- ? `$ cd nagios-statd-3.08`
- ? `$ cp bin/nagios-stat /usr/local/nagios/libexec/`
- ? `$ vi sbin/nagios-statd`

Change `#!/usr/bin/python`

To `#!/usr/bin/python2.2`

- ? Because nagios-statd requires python version 2 or higher

Nagios-statd Installation

? \$ su

? # cp sbin/nagios-statd /usr/local/bin

? # vi /etc/rc.local

/usr/local/bin/nagios-statd daemon

? Nagios-stat is nagios serverside plugin

? Is used to retrieve information from nagios-statd daemon

Nagios-stat Command Line Option

- ? `$ /usr/local/nagios/libexec/nagios-stat -w 2.5 -c 10 load <ip>`
- ? `$ /usr/local/nagios/libexec/nagios-stat -w 5 -c 10 -s Z proc <ip>`
- ? `$ /usr/local/nagios/libexec/nagios-stat -w 10000 -c 20 -s NWZ
proc <ip>`
- ? `$ /usr/local/nagios/libexec/nagios-stat -w 50 -c 75 swap <ip>`
- ? `$ /usr/local/nagios/libexec/nagios-stat -w 2 -c 5 user <ip>`
- ? `$ /usr/local/nagios/libexec/nagios-stat -w 60 -c 80 disk <ip>`
- ? More are available on online documentation

Nagios Configuration

1. nagios.cfg (main configuration file)
2. cgi.cfg
3. hosts.cfg
4. hostgroup.cfg
5. service.cfg
6. contacts.cfg
7. contactgroups.cfg
8. hostextinfo.cfg
9. serviceextinfo.cfg
10. checkcommands.cfg
11. others found in
/usr/local/nagios/etc

nagios.cfg

cfg_file=/usr/local/nagios/etc/contactgroups.cfg

cfg_file=/usr/local/nagios/etc/contacts.cfg

? Need to hash folloing two files

#cfg_file=/usr/local/nagios/etc/dependencies.cfg

#cfg_file=/usr/local/nagios/etc/escalations.cfg

cfg_file=/usr/local/nagios/etc/hostgroups.cfg

cfg_file=/usr/local/nagios/etc/hosts.cfg

cfg_file=/usr/local/nagios/etc/services.cfg

cfg_file=/usr/local/nagios/etc/timeperiods.cfg

cgi.cfg

Change

`nagios_check_command=/usr/local/nagios/libexec/check_nagios`

to

`nagios_check_command= /usr/local/nagios/libexec/check_nagios`

? Add following 2 lines to proper place

At bottom of EXTENDED HOST INFORMATION Section

`xedtemplate_config_file=/usr/local/nagios/etc/hostextinfo.cfg`

At bottom of EXTENDED SERVICE INFORMATION Section

`xedtemplate_config_file=/usr/local/nagios/etc/serviceextinfo.cfg`

cgi.cfg

? Change some option as following

```
default_user_name=guest
```

```
authorized_for_system_information=*
```

```
authorized_for_configuration_information=*
```

```
authorized_for_system_commands=nagios
```

```
authorized_for_all_services=*
```

```
authorized_for_all_hosts=*
```

```
authorized_for_all_service_commands=nagios
```

```
authorized_for_all_host_commands=nagios
```

Sample of nagios.cfg, cgi.cfg, checkcommands.cfg and rrdtool create
are also available at [/home/nagios](#)

Contacts.cfg

```
# 'dhruba' contact definition
```

```
define contact{
```

```
    contact_name                dhruba
```

```
    alias                       Sys Admin
```

```
    service_notification_period 24x7
```

```
    host_notification_period    24x7
```

```
    service_notification_options c,u,r
```

```
    host_notification_options   d,u,r
```

```
    service_notification_commands notify-by-email
```

```
    host_notification_commands  host-notify-by-email
```

```
    email                       dhruba@mos.com.np
```

```
}
```

Contactgroups.cfg

```
? # 'Sys-Adms' contact group definition
define contactgroup{
    contactgroup_name      Sys-Adms
    alias                  System Administrator
    members                dhruba
}
```

Host.clg

```
? # 'FNCCI' host definition
```

```
define host{
```

```
    use
```

```
    generic-host
```

```
    ; Name of host template
```

```
to use
```

```
    host_name
```

```
FNCCI
```

```
    alias
```

```
Brouter @FNCCI
```

```
    address
```

```
202.52.238.170
```

```
    parents
```

```
Pul-br
```

```
    check_command
```

```
check-host-alive
```

```
    max_check_attempts
```

```
1
```

```
    notification_interval
```

```
0
```

```
    notification_period
```

```
workhours
```

```
    notification_options
```

```
d,r
```

```
,
```


Hostgroup.cfg

```
# 'Routers@Xpressway R' host group definition
define hostgroup{
    hostgroup_name          Routers@XpresswayR
    alias                    All Routers
                           @Xpressway Customers w/ Radio Link
    contact_groups          Sys-Adms
    members
    ICIMODR,PLAN,UNICEFJAW,NRB,RBB,CYMMYT,WHO,RBA,NSBI,SE
    RVINGMINDS,DANIDA,WORLDBANK-R,EBL,DABURNEPAL-
    KTM,AFP,FNCCI
}
```

Service.ctg

```
# Service definition
```

```
define service{
```

```
    use                                generic-service                ; Name of
service template to use
```

```
    hostgroup_name                     Routers@XpresswayR,Brouters@KTM
```

```
    service_description                Ping
```

```
    is_volatile                        0
```

```
    check_period                       24x7
```

```
    max_check_attempts                 3
```

```
    normal_check_interval               5
```

```
    retry_check_interval                1
```

```
    contact_groups                     Sys-Adms
```

```
    notification_interval               0
```

```
    notification_period                 24x7
```

```
    notification_options                u,c,r
```

```
    check_command                       apan!ping!600.0,40%!1000.0,80%
```

Hostextinfo.cfg

```
? # 'FNCCI' hostextinfo definition
define hostextinfo{
    host_name                FNCCI
    ; The name of the host this data is
    associated with
    icon_image                router40.gif
    gd2_image                 router40.gd2
    icon_image_alt
}
}
```

serviceextinfo.cfg

```
define serviceextinfo{
host_name                FNCCI
service_description      Ping
notes_url                /nagios/cgi-
    bin/apan.cgi?host=FNCCI&service=Ping
icon_image               graph.png
icon_image_alt           View graphs
}
```

checkcommands.cfg

```
define command {  
    command_name                apan  
    command_line                /usr/local/nagios/apan/apan.sh $ARG1$ $HOSTNAME$  
    "$SERVICEDESC$" $TIMET$ $ARG2$ $ARG3$  
}  
  
define command {  
    command_name                check-host-alive  
    command_line                $USER1$/check_ping -H  
    $HOSTADDRESS$ -w 10000.0,100% -c 10000.0,100% -p 10  
}
```

How to create RRDtool database file

- ? `rrdtool create /usr/local/nagios/rrd/Mustang_Ram-usage.rrd -s 600 DS:Ram-Free:GAUGE:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- ? `rrdtool create /usr/local/nagios/rrd/Mustang_Cpu-usage.rrd -s 600 DS:usr-cpu:GAUGE:1200:0:U DS:sys-cpu:GAUGE:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- ? `rrdtool create /usr/local/nagios/rrd/Mustang_load.rrd -s 600 DS:1MIN-Load:GAUGE:1200:0:100 DS:5MIN-Load:GAUGE:1200:0:100 DS:15MIN-Load:GAUGE:1200:0:100 RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- ? `rrdtool create /usr/local/nagios/rrd/Sungava_disk_usage.rrd -s 600 DS:root:GAUGE:1200:0:U DS:home:GAUGE:1200:0:U DS:usr:GAUGE:1200:0:U DS:var:GAUGE:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`

For Ping and Bandwidth

- ? `rrdtool create /usr/local/nagios/rrd/RELIANCE-INTL_Ping.rrd -s 600 DS:ping:GAUGE:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- ? `rrdtool create /usr/local/nagios/rrd/Mc-gw_total.rrd -s 600 DS:IN:COUNTER:1200:0:U DS:OUT:COUNTER:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- ? **Oid for incoming and outgoing traffic**
 - .1.3.6.1.2.1.2.2.1.10.2 #incoming traffic on first ethernet**
 - .1.3.6.1.2.1.2.2.1.16.2 #outgoing traffic on first ethernet**
- ? **Oid for Cisco router is same**
- ? **The last number is changed for Various interface**
- ? **i.e .1=Ethernet0, .2=FastEthernet, .3=Serial0, .4= Serial1 etc**

Nagios service Defination for bandwidth

```
define service{
    use                               generic-service           ; Name
    of service template to use
    host_name                         Mc-gw
    service_description               bandwidth_total
    is_volatile                       0
    check_period                      24x7
    max_check_attempts                3
    normal_check_interval              5
    retry_check_interval               1
    contact_groups                     Sys-Adms
    notification_interval              0
    notification_period                24x7
    notification_options               u,c,r
    check_command                      apan!snmpget!10!20
}
```

Serviceextinfo.cfg

? Define serviceextinfo{

host_name Mc-gw

service_description **bandwidth_total**

notes_url /nagios/cgi-bin/apan.cgi?host=Mc-gw&service=**bandwidth_total**

icon_image graph.png

icon_image_alt View graphs

}

This most match with nagios service



apan.cfg

? `Mc-gw;bandwidth_total;/usr/local/nagios/rrd/Mc-gw_total.rrd;criFOOT:.1.3.6.1.2.1.2.2.1.10.1|criFOOT:.1.3.6.1.2.1.2.2.1.16.1;IN:LINE2 OUT:LINE2;Network throughput;Bytes/sek;`

? All host name resolution need to be done on /etc/hosts i.e

`station1 192.168.10.1`

`station2 192.168.10.2`

? Nagios need to be reloaded or restarted after changes are done

Point to remember

? After making any changes on cfg file always run following command

```
$ /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

? To run nagios on daemon mode

```
$ /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

? To run nagios as foreground

```
$ /usr/local/nagios/bin/nagios /usr/local/nagios/etc/nagios.cfg
```

? To run nagios as background process

```
$ /usr/local/nagios/bin/nagios /usr/local/nagios/etc/nagios.cfg &
```

? To reload configuration file after making some changes

```
$ kill -HUP <nagios process id>    or
```

```
$/etc/rc.d/init.d/nagios reload
```

Daily Administration

- ? Add host and services
- ? Check nagios performance
- ? Check log files
- ? Close apan graph window after checking
- ? Check nagios server's load
- ? Cgi security
- ? Web security and authentication
- ? Nagios server security

Web Sites

- ? <http://nagios.org>
- ? <http://apan.sourceforge.net>
- ? <http://www.rrdtool.com>
- ? <http://www.snmp.com>
- ? <http://net-snmp.sourceforge.net>

Questions?