An Introduction

Nagios®

intERLab at AIT

Network Management Workshop

March 11-15 – Bangkok, Thailand

Hervey Allen & Phil Regnauld

Where Does Nagios Fit?

Nagios, in some ways, ties it all together. We've seen things like:

- SNMP
- MRTG
- RRDTool
- Rancid
- Cacti
- Smokeping

You can and will use all this functionality in Nagios.

It is a monolithic tool:

- Big
- Complex
- Powerful

Why Nagios

- Open source
- Relatively scalable, Manageable, Secure and more
- Best documentation available
- Good log and database system
- Nice, informative and attractive web interface
- Very flexible
- Alerts automatically sent if condition changes
- Various notification options (Email, pager, mobile phone)

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 avoids unnecessary checks
  - e.g. HTTP responds, therefore no need to ping
  - e.g. power outage, no ping response, so don't bother trying anything else
  - Services are running fine no need to do check if the host itself is alive

What Can it Do?

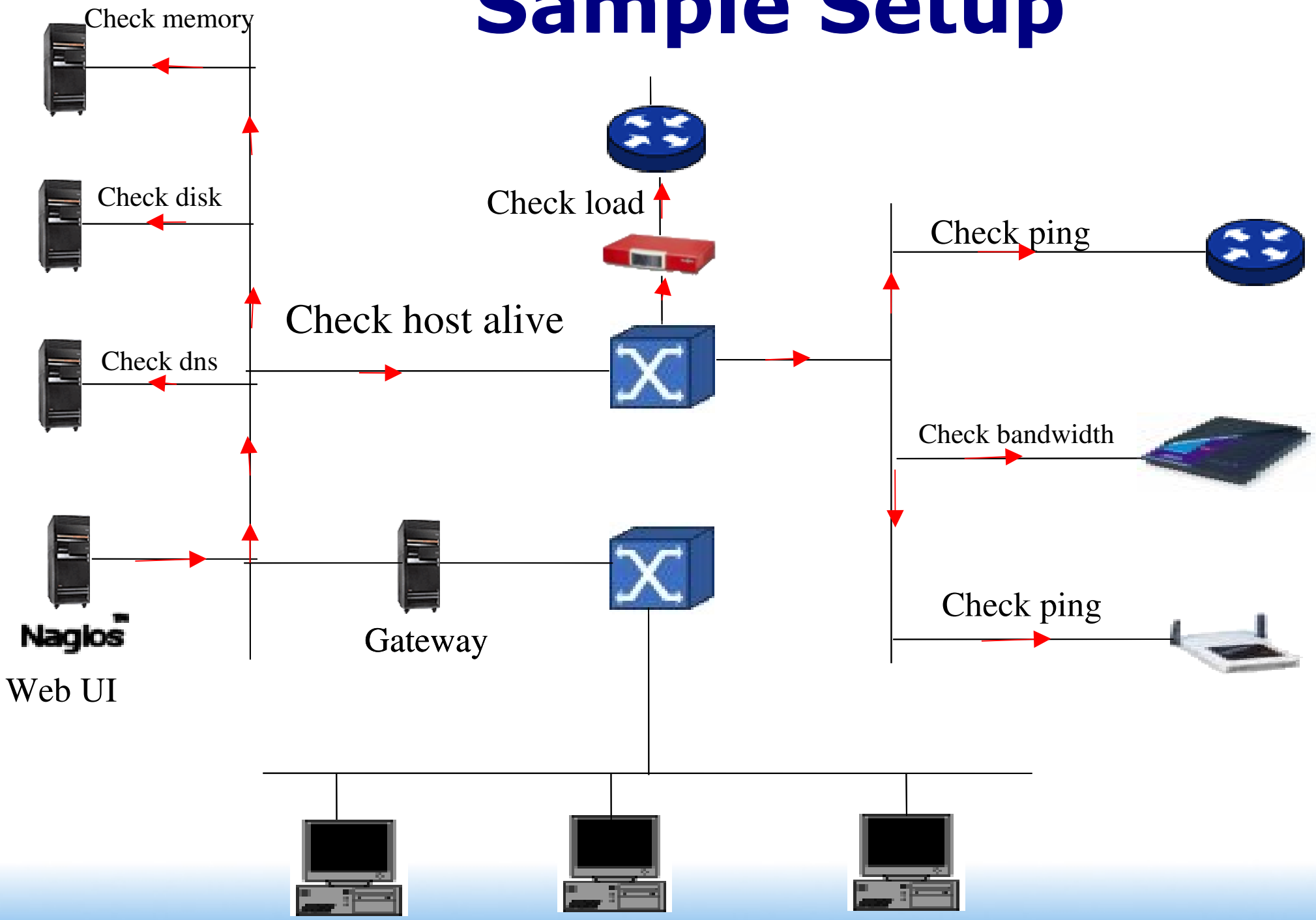
- Individual node status
  - Is it up?
  - What is its load?
  - What is the memory and swap usage?
  - NFS and network load?
  - Are the partitions full?
  - Are applications and services running properly?
  - How about ping latency?
- Aggregated node status
  - Same info, but across groups of nodes

What Can it Do?

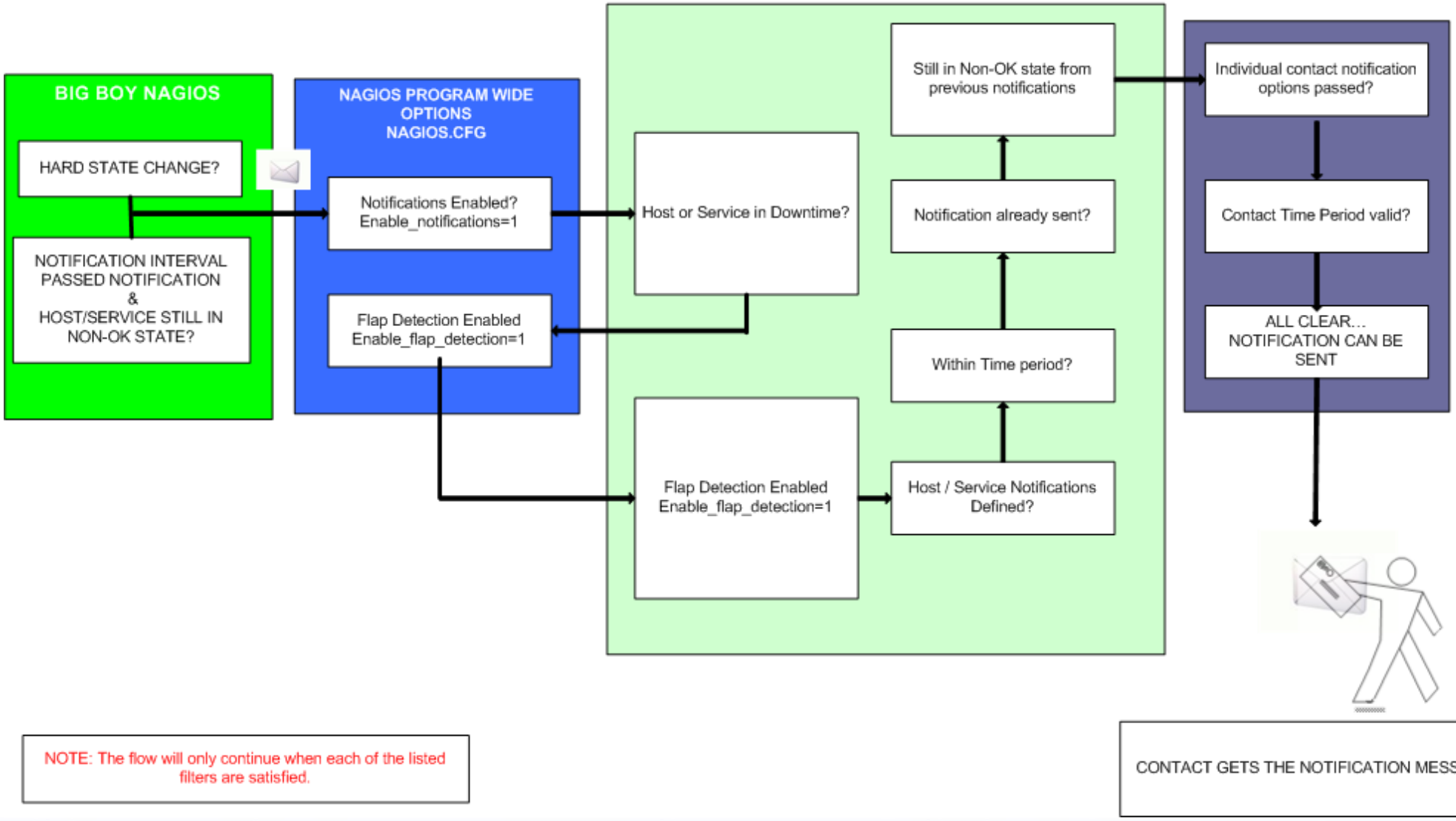
A lot, including:

- Service monitoring
- Alerts from SNMP traps
- Monitoring redundancy
- Detection of primary failure to avoid multiple like alerts.
- Notifications via email, pager, etc.
- Notifications to individuals or defined groups
- Log information
- Use databases to store history
- Graph generation from MRTG
- Very extensible via plug-ins, add-ons and local scripts.
- Can scale to large installations
- Allows for redundant monitoring
- Aggregation of like-data across multiple nodes.
- Ability to escalate alerts
- Runs on multiple Unices
- Licensed under GPL v2

Sample Setup

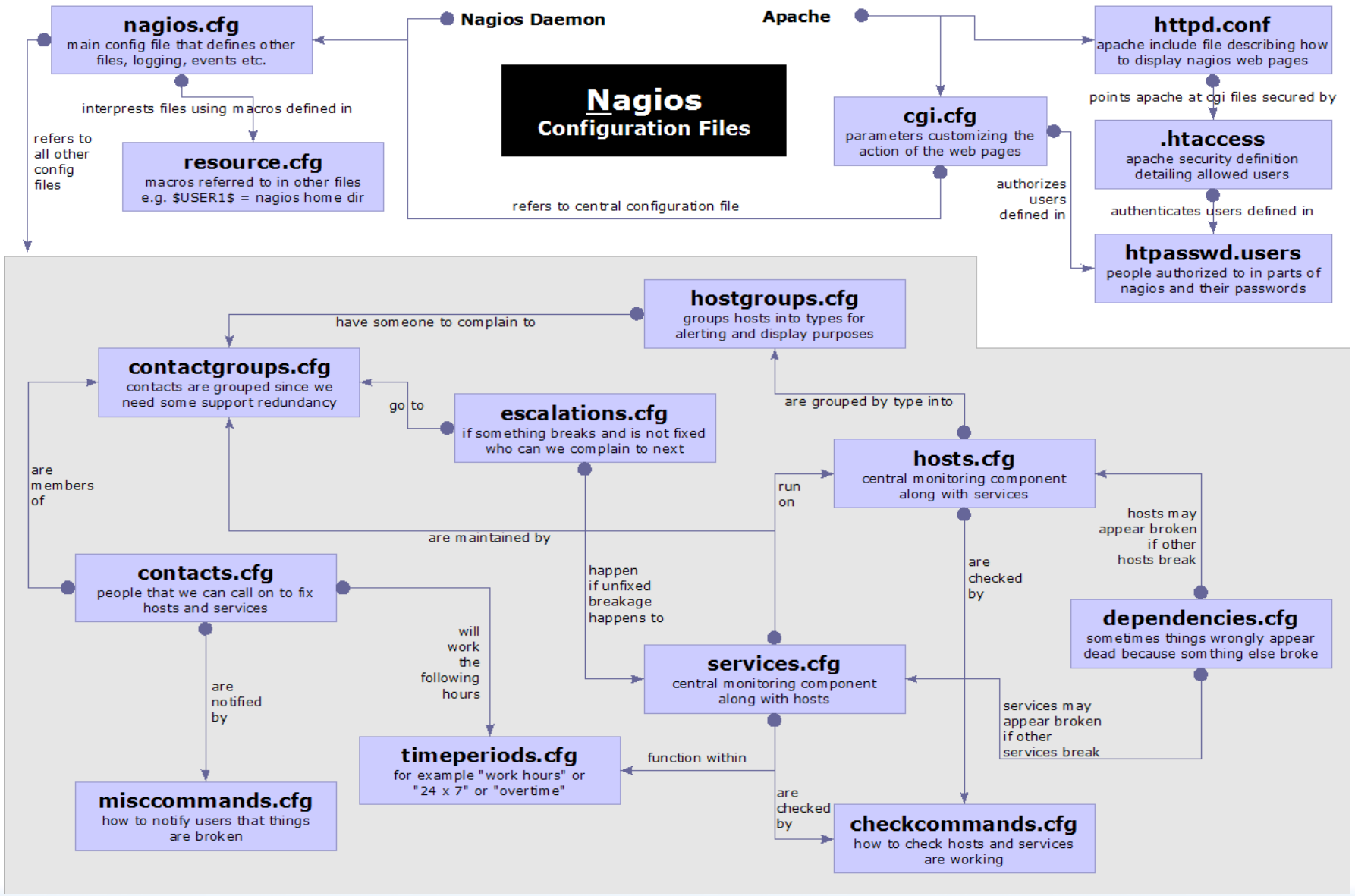


NAGIOS - NOTIFICATION FLOW DIAGRAM



NOTE: The flow will only continue when each of the listed filters are satisfied.

Nagios Configuration

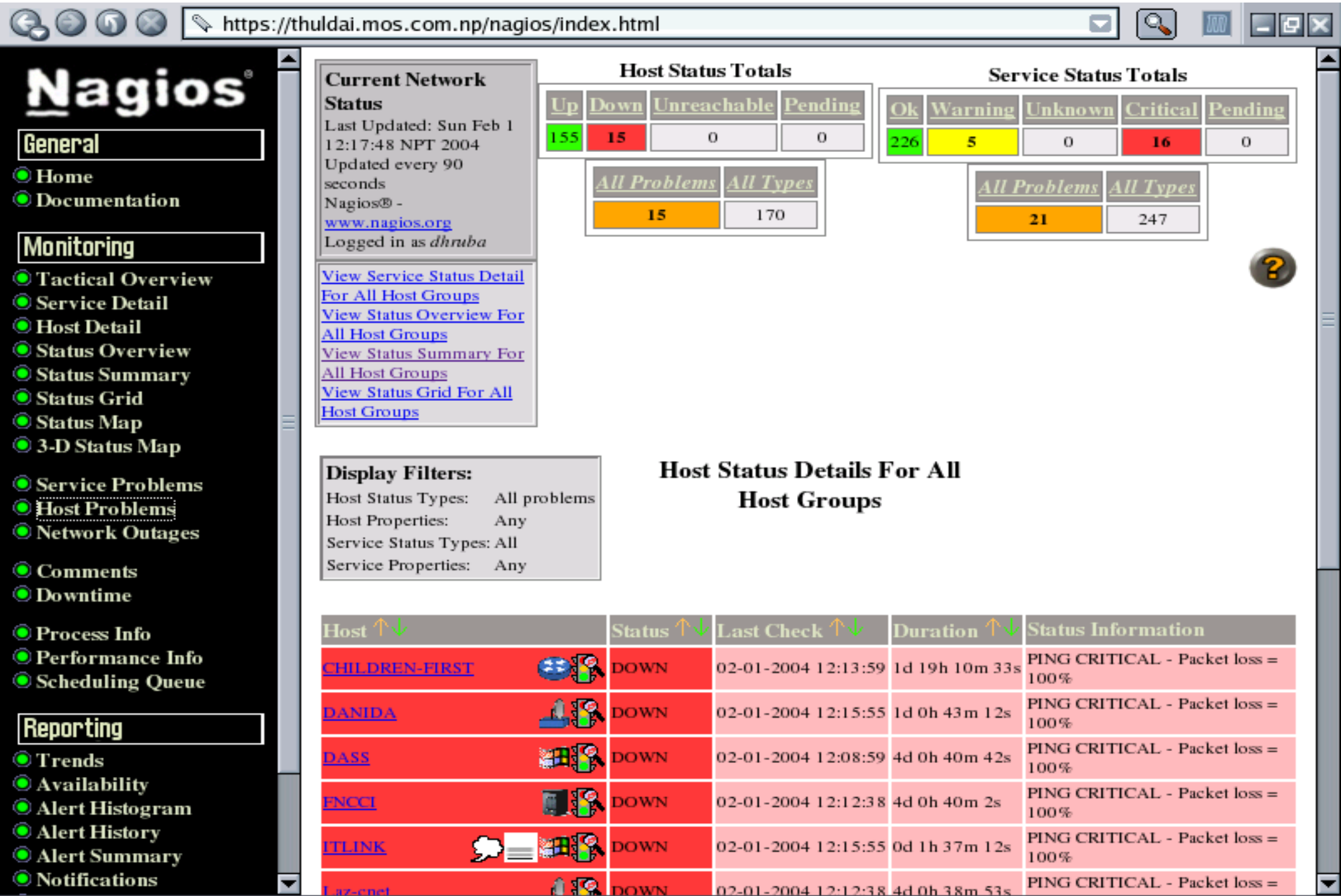


Remaining Slides

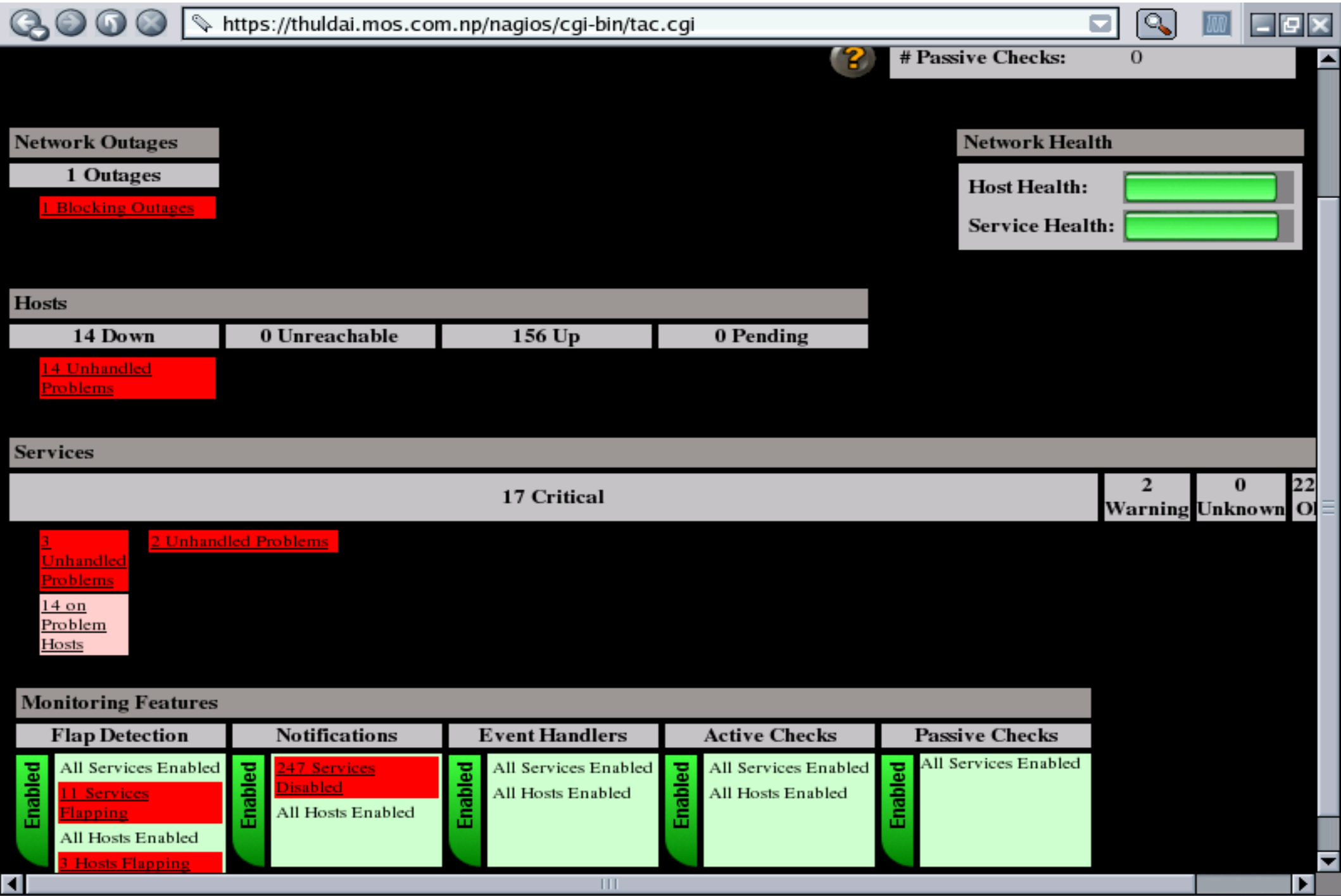
Dhruba Raj Bhandari
(CCNA)

Additions by Phil Regnauld
bhandari.dhruba@scp.com.np

- Nagios Status Detail screen

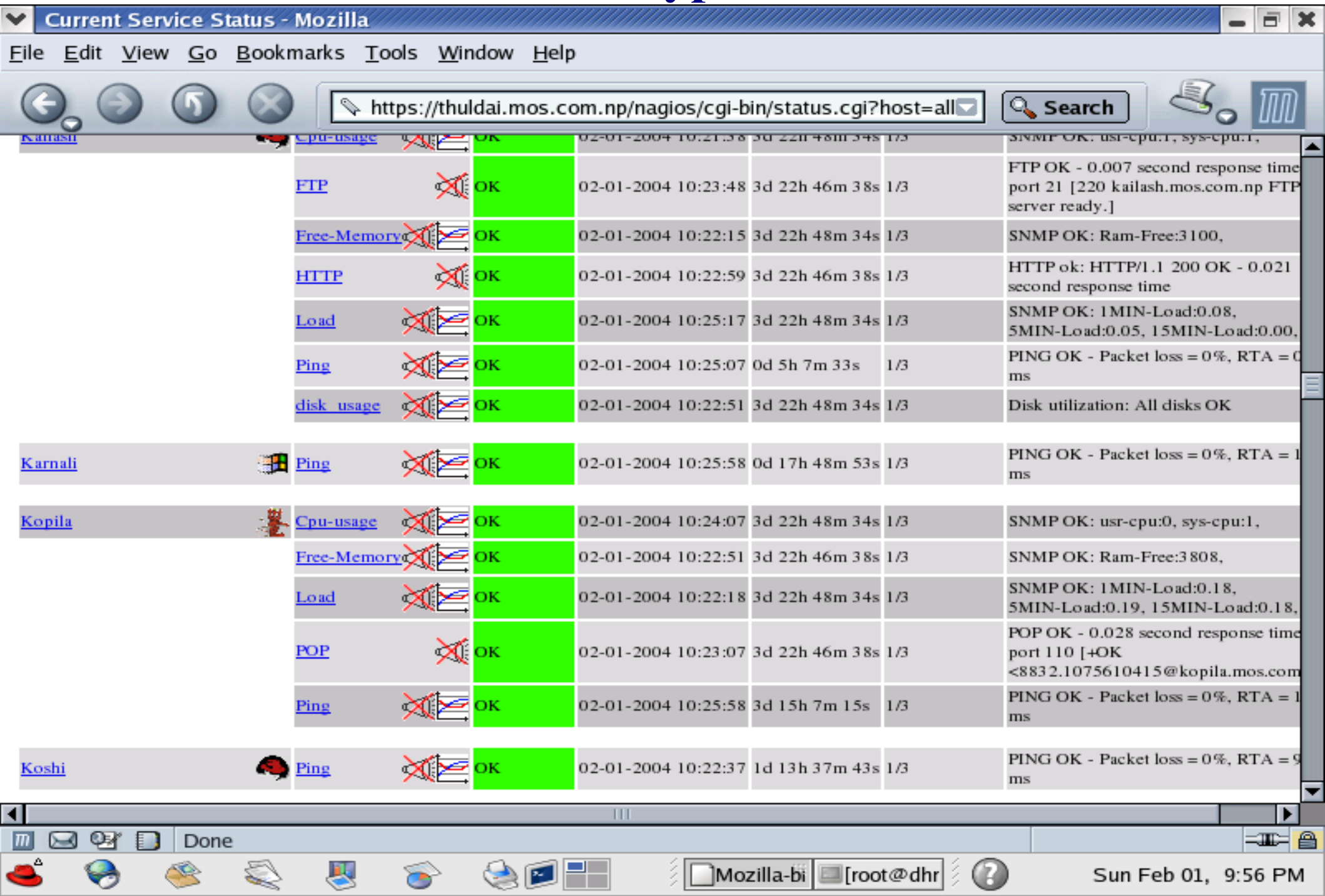


Tactical Overview Of Nagios

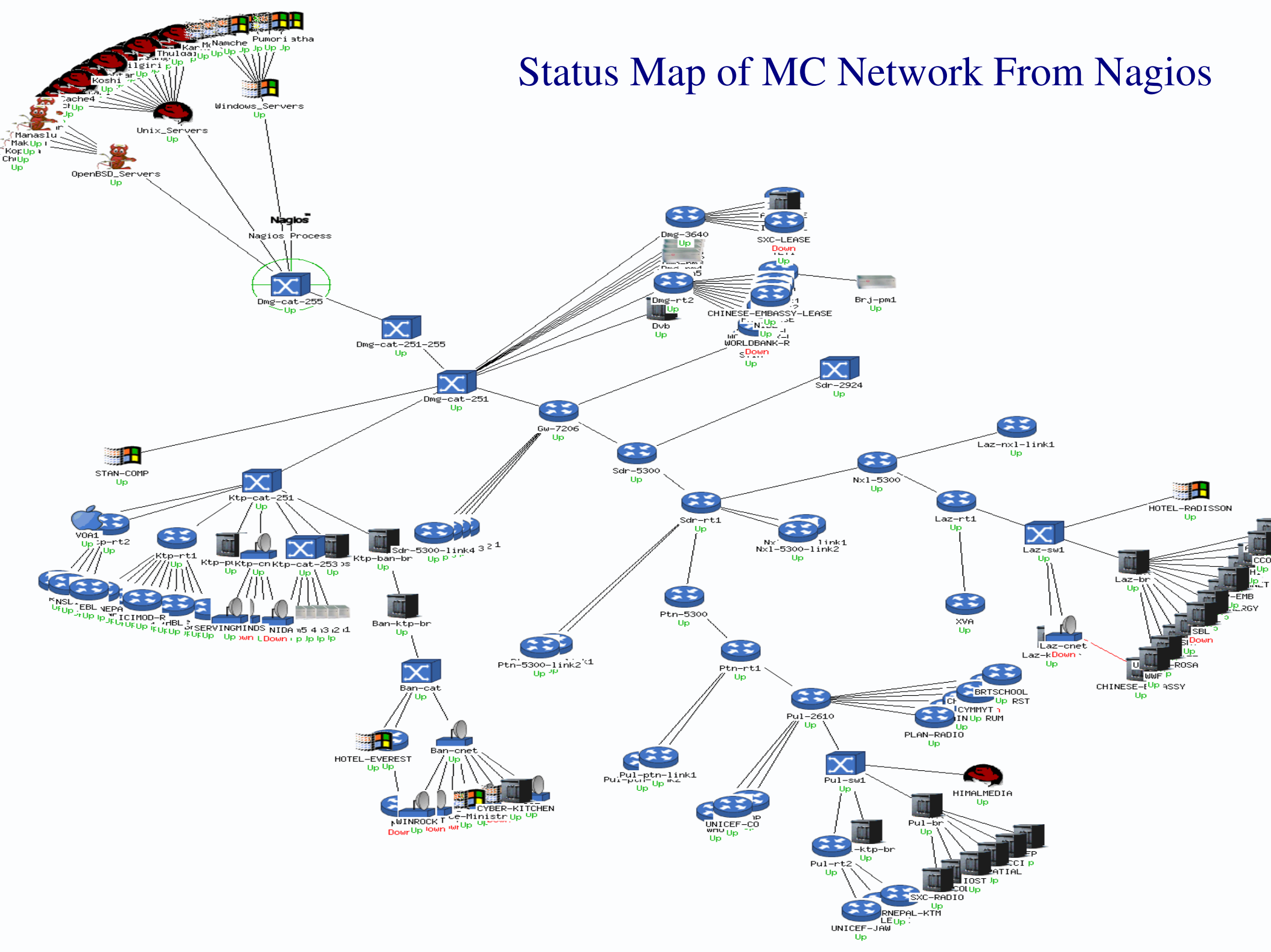


Service Detail of Nagios

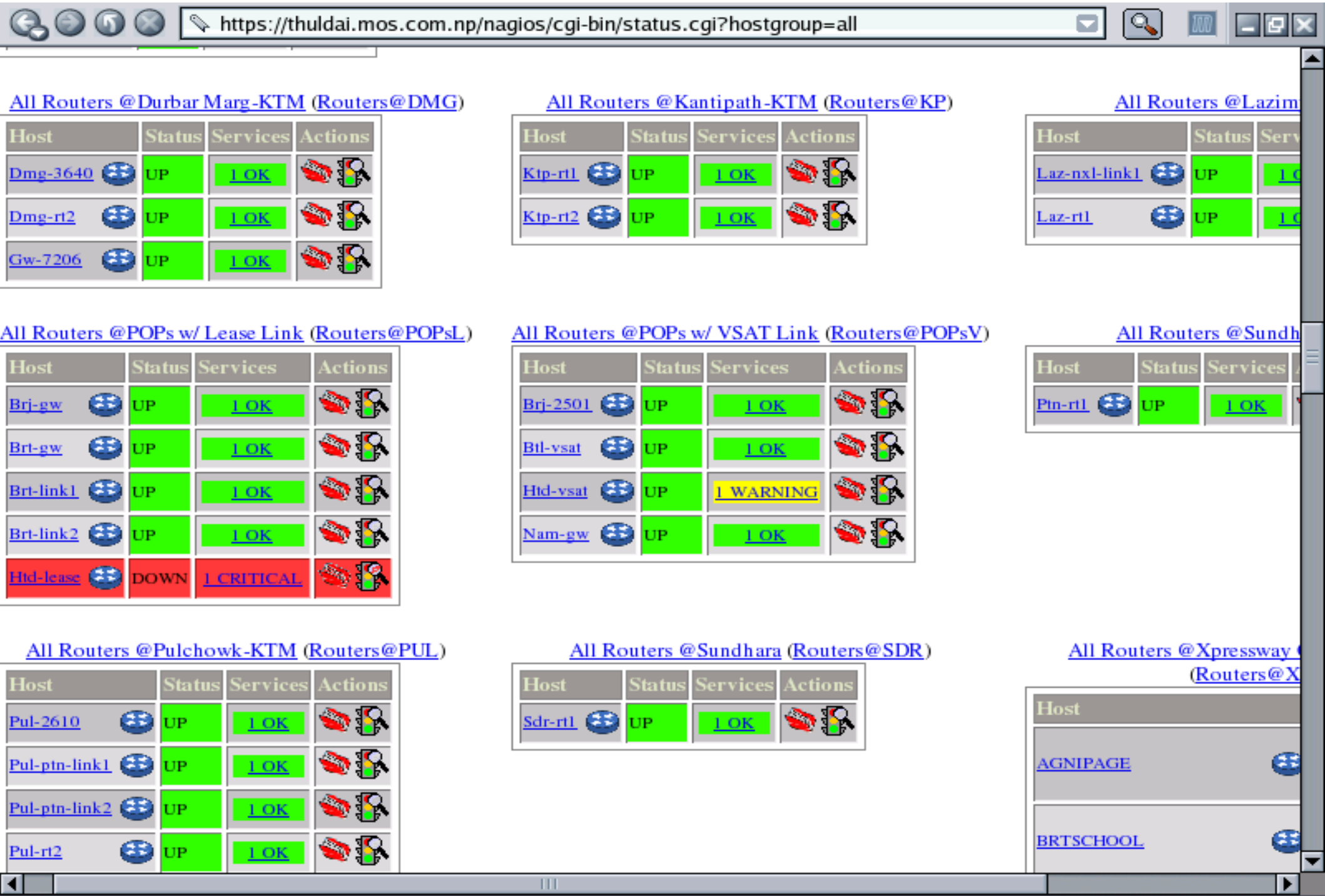
Service Types



Status Map of MC Network From Nagios



Status Overview from nagios



Status Summary Based On Hostgroup

Status Summary For All Host Groups

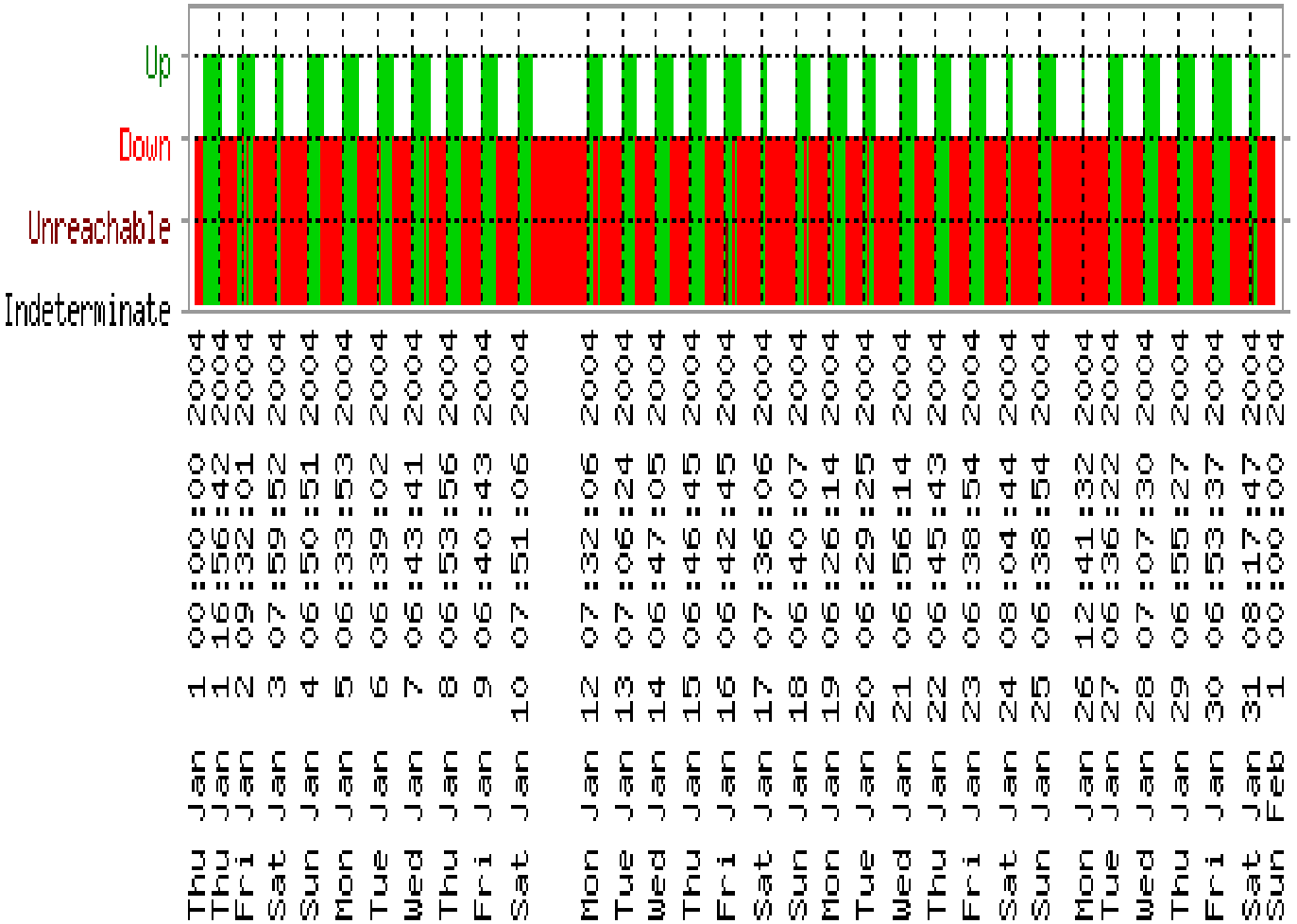
Host Group	Host Status Totals	Service Status Totals
Access Servers@KTM (AS@KTM)	11 UP	11 OK
All Brouters @KTM (Brouters@KTM)	7 UP	7 OK
All Routers @MIX Customers w/ Radio Link (Brouters@MIXR)	1 UP	1 OK
All Brouters @Xprewway Customers w/ Radio Link (Brouters@XpresswayR)	19 UP 1 DOWN	19 OK 1 CRITICAL
All Brouters @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@POPsL)	4 UP 1 DOWN	4 OK 1 CRITICAL

Host Trends or Status History

Trends

State History For Host 'Don_Bosco'

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

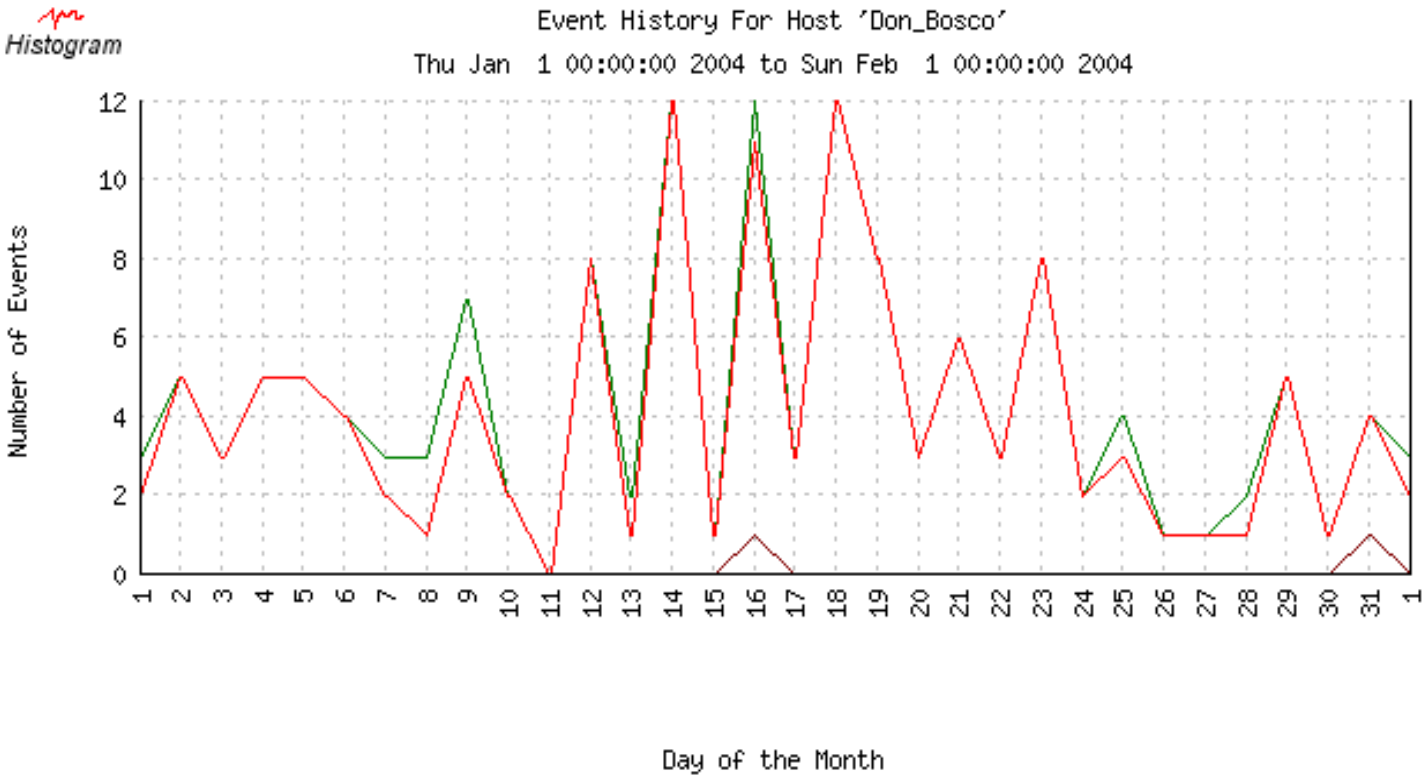


State Breakdowns:

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

Report Produced By:
Nagios®
http://www.nagios.org

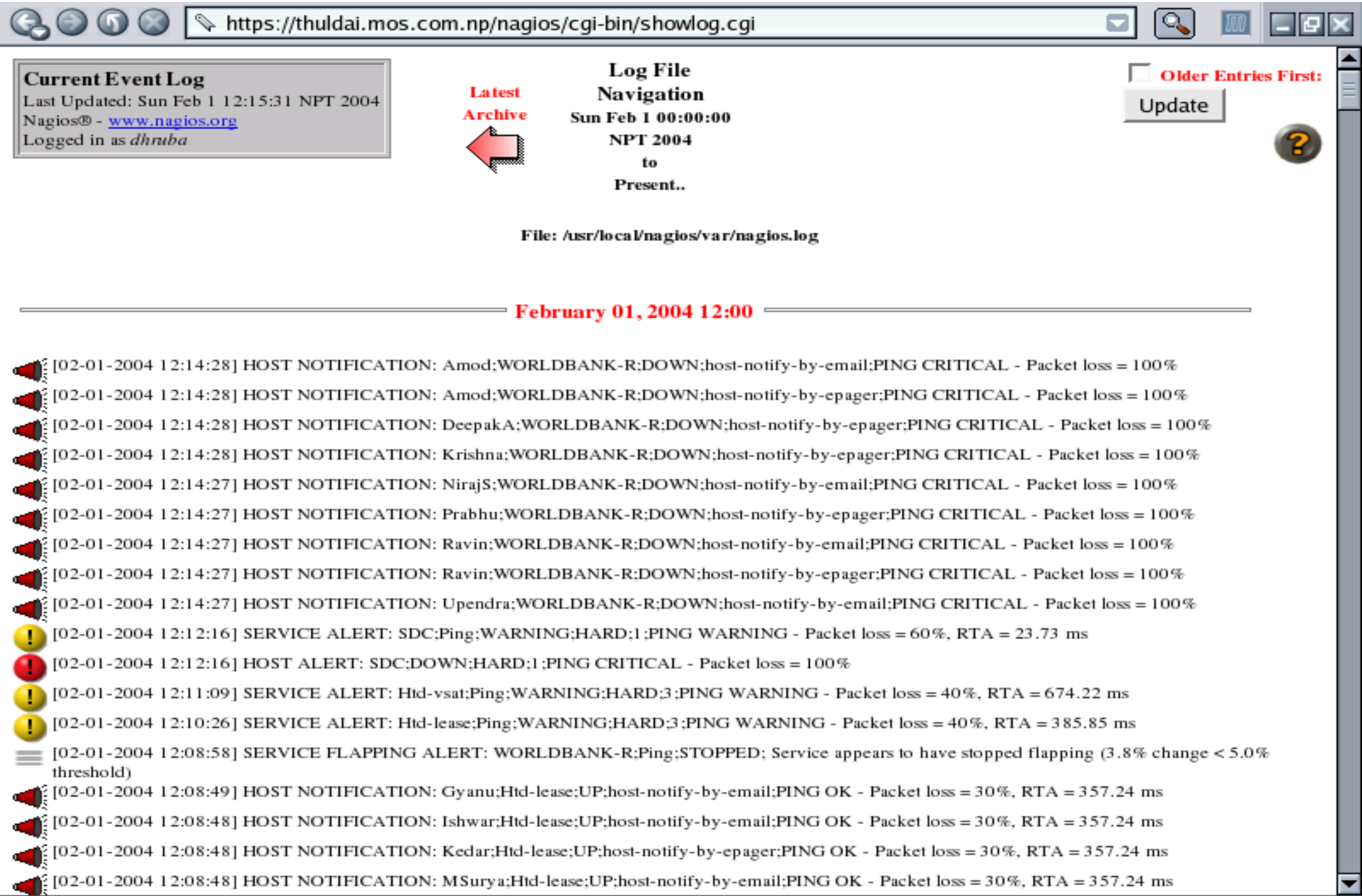
Histogram Of Host



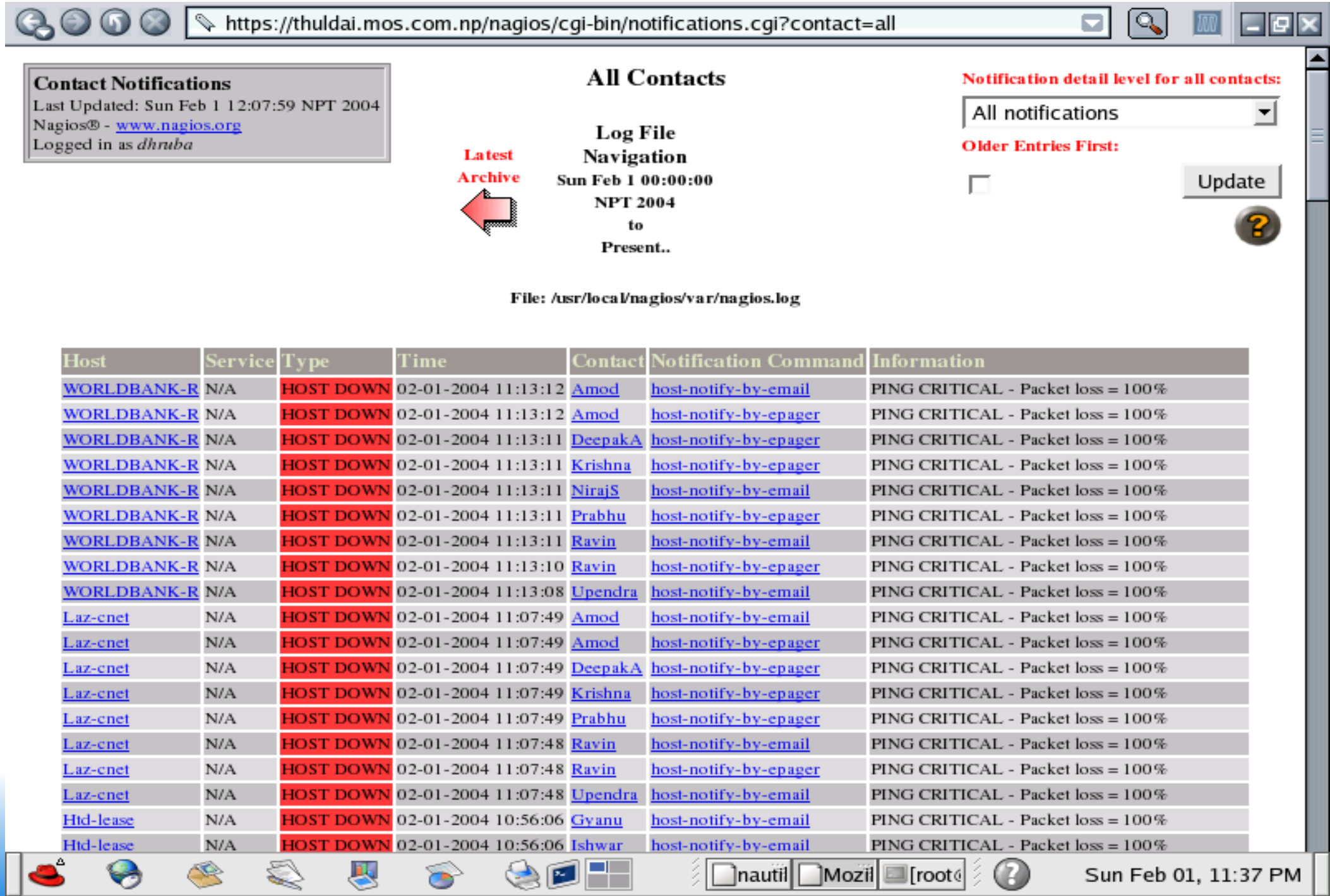
EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06

Report Produced By:
Nagios®
http://www.nagios.org

Event Logs


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
Latest Archive
Log File Navigation
Sun Feb 1 00:00:00 NPT 2004 to Present..
Older Entries First:
Update
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-vsat;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 is Notified?



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
```

Nagios configuration files

- Located in /etc/nagios2/
- Important files:
  - cgi.cfg controls the Web Interface options security
  - commands.cfg commands that Nagios uses to notify
  - nagios.cfg main Nagios configuration file
  - conf.d/* the core of the config files

Nagios configuration files

- Under conf.d/*, files “xxxx_nagios2.cfg”:
- contacts users and groups
- generic-host “template” host (default)
- generic-service “template” service
- hostgroups host group definitions
- services which services to check
- timeperiods when to check and notify

Nagios plugin configuration

- /etc/nagios-plugins/config/

apt.cfg ntp.cfg dhcp.cfg ping.cfg

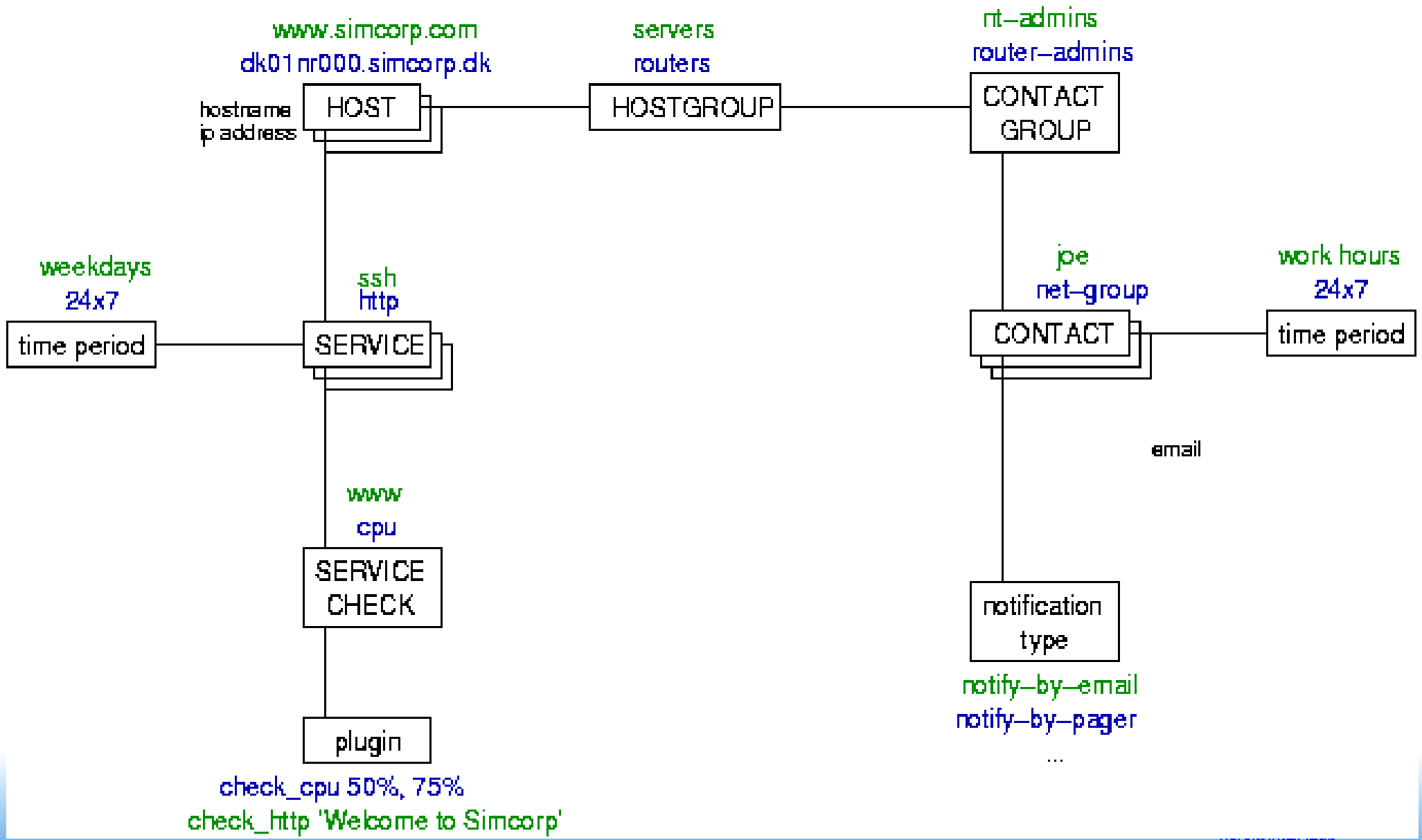
disk.cfg procs.cfg dummy.cfg real.cfg

ftp.cfg ssh.cfg http.cfg tcp_udp.cfg

load.cfg telnet.cfg mail.cfg users.cfg

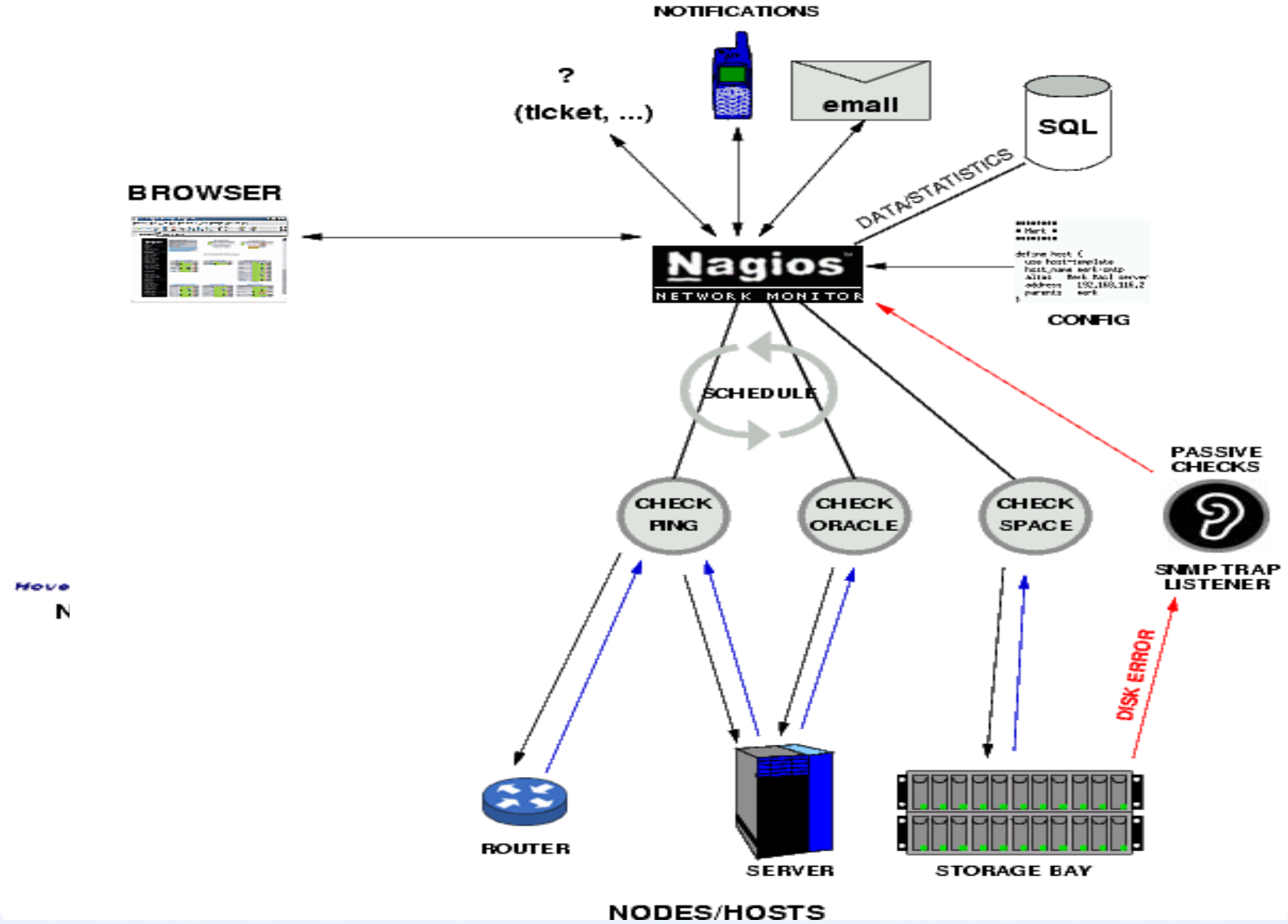
news.cfg

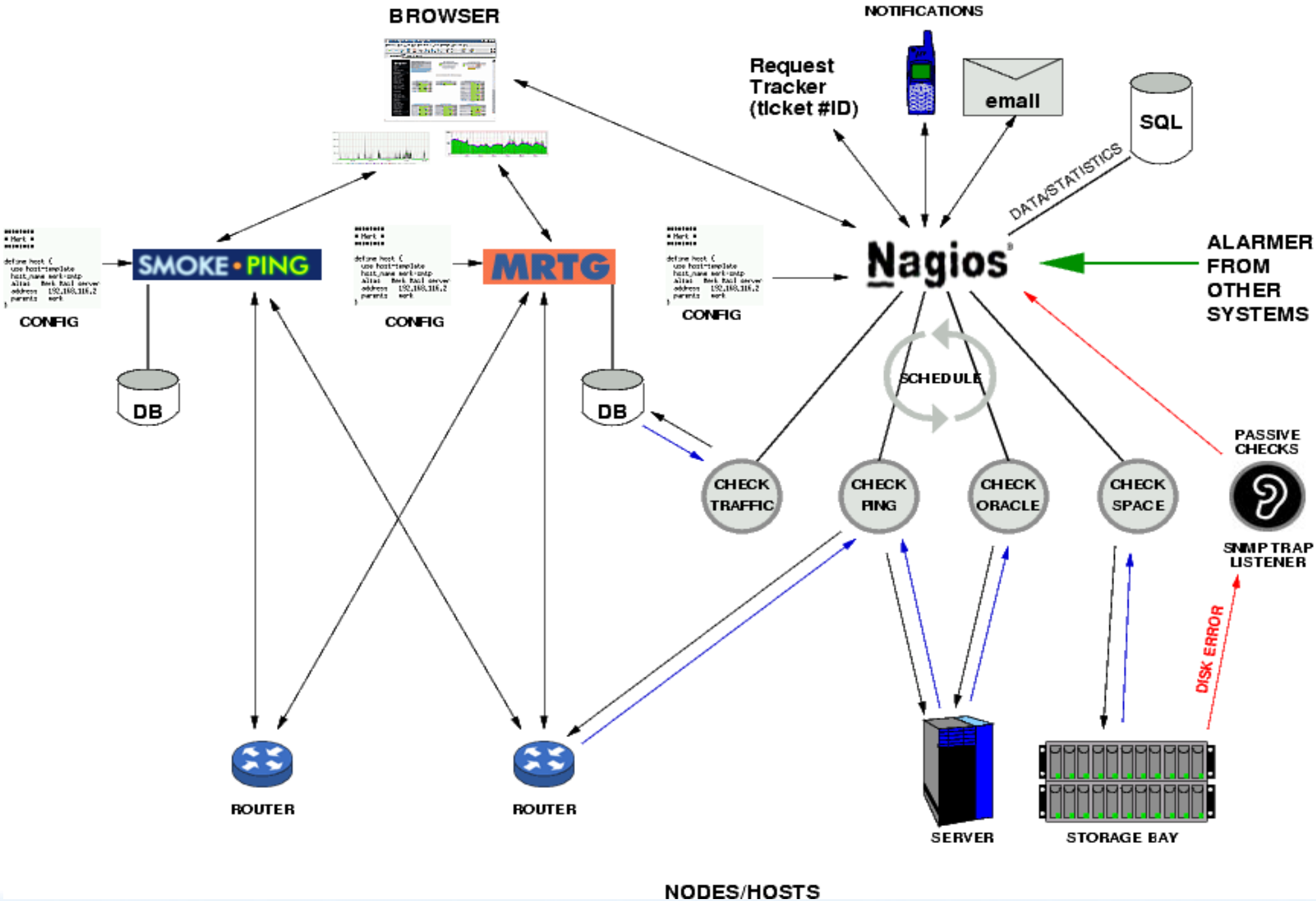
NAGIOS schema



Concepts: parents

- Hosts can have parents
  - Allows one to specify which dependencies there are in the network
  - Avoid sending alarms if we cannot know the state of a host...


NOTIFICATIONS
?
(ticket, ...)
email
SQL
DATA/STATISTICS
BROWSER
Nagios
NETWORK MONITOR
CONFIG
SCHEDULE
PASSIVE CHECKS
CHECK PING
CHECK ORACLE
CHECK SPACE
SNMP TRAP LISTENER
DISK ERROR
ROUTER
SERVER
STORAGE BAY
NODES/HOSTS


BROWSER
NOTIFICATIONS
Request
Tracker
(ticket #ID)
email
SQL
DATA/STATISTICS
SMOKE • PING
MRTG
Nagios
ALARMER
FROM
OTHER
SYSTEMS
CONFIG
CONFIG
CONFIG
DB
DB
SCHEDULE
CHECK
TRAFFIC
CHECK
PING
CHECK
ORACLE
CHECK
SPACE
PASSIVE
CHECKS
SNMP TRAP
LISTENER
DISK ERROR
ROUTER
ROUTER
SERVER
STORAGE BAY
NODES/HOSTS

Nagios Resources

Nagios Home

http://www.nagios.org/

Nagios Plugins and Add Ons Exchange

http://www.nagiosexchange.com/

Nagios Tutorial for Debian

http://www.debianhelp.co.uk/nagios.htm

Nagios Commercial Support

http://www.nagios.com/

Questions?