Nagios®

Nagios - introduction

Dhruba Raj Bhandari
(CCNA)

Additions by Phil Regnauld

bhandari.dhruba@scp.com.np

Why Nagios?

- Open source
- Relatively scaleable, 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 downstram 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

What one can check

- 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

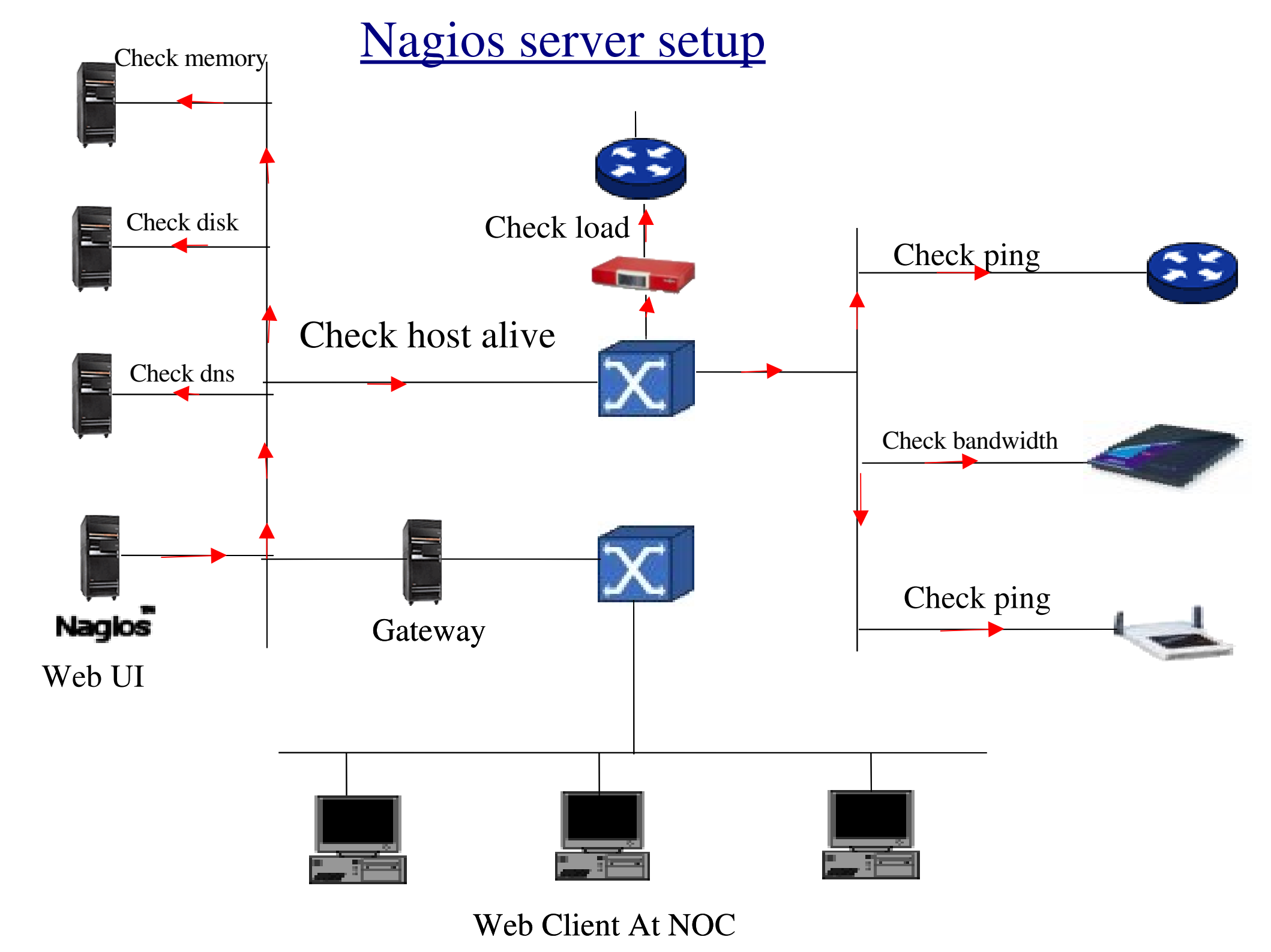
Nagios Features

- Nagios
  - host and service monitor designed to inform you of network problems before your clients, end-users or managers do ;
  - Designed to run under the UNIX (Linux, *BSD, Solaris, ...)
  - 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

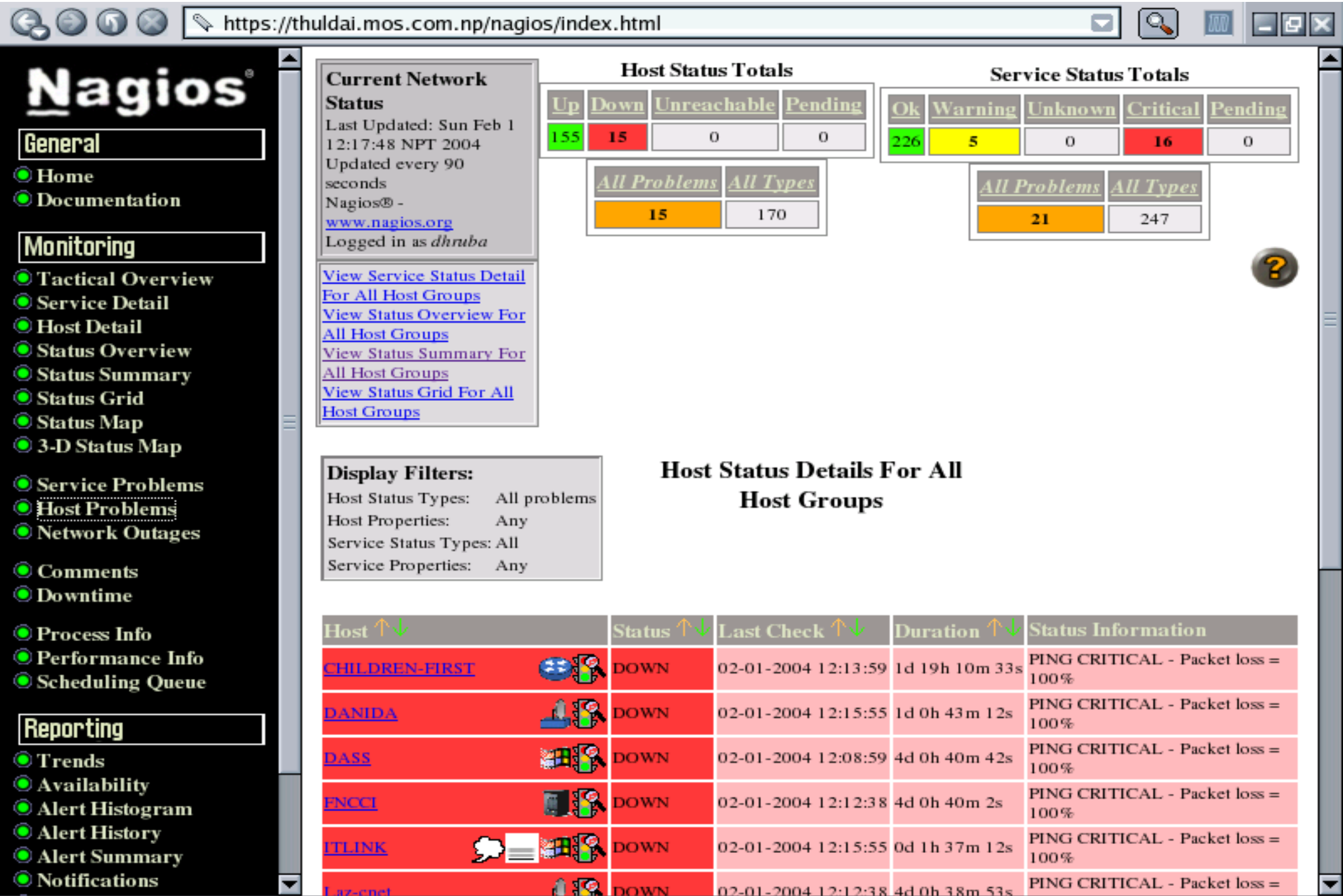
Features contd.

- 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

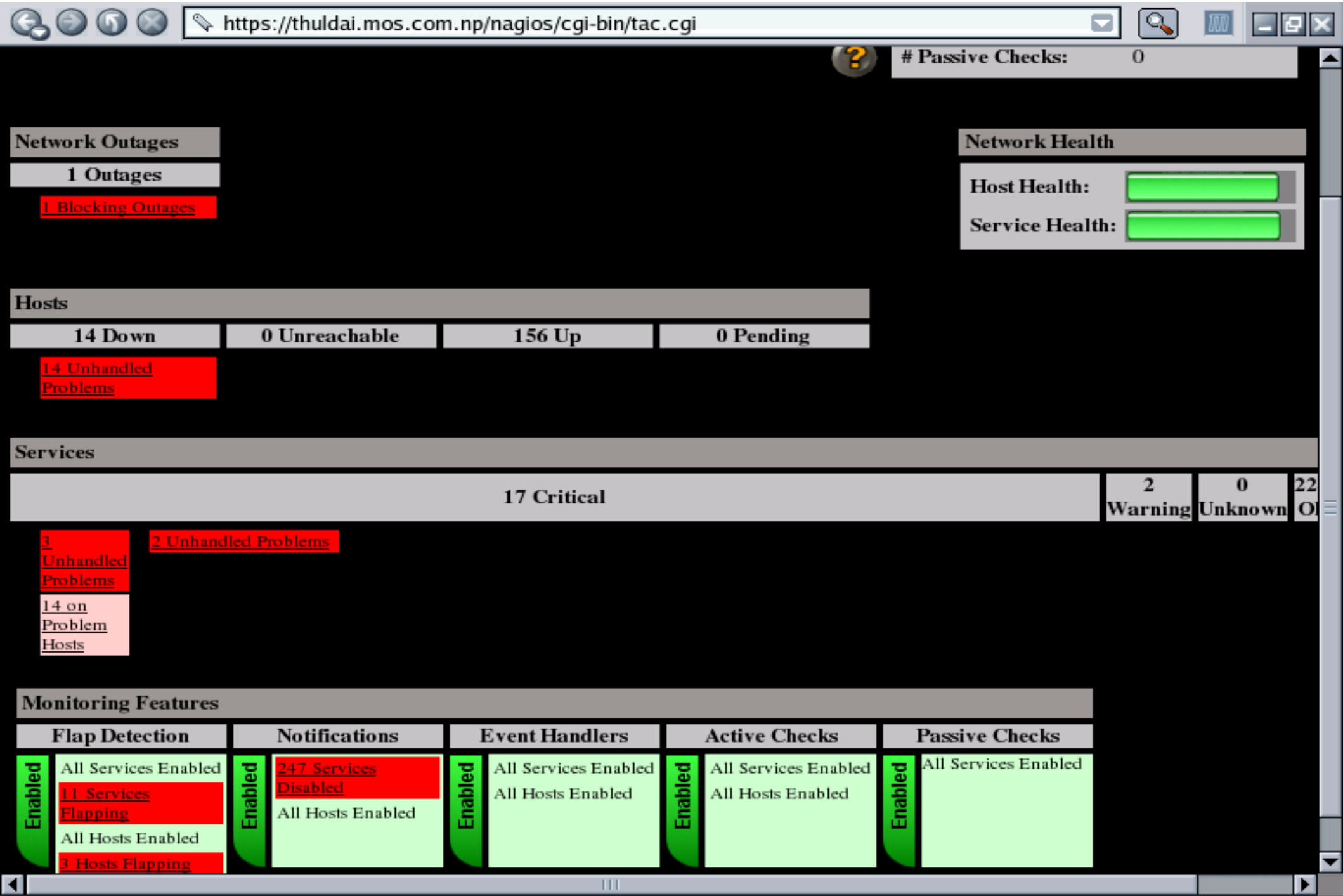
Nagios server setup



– Nagios Status Detail screen

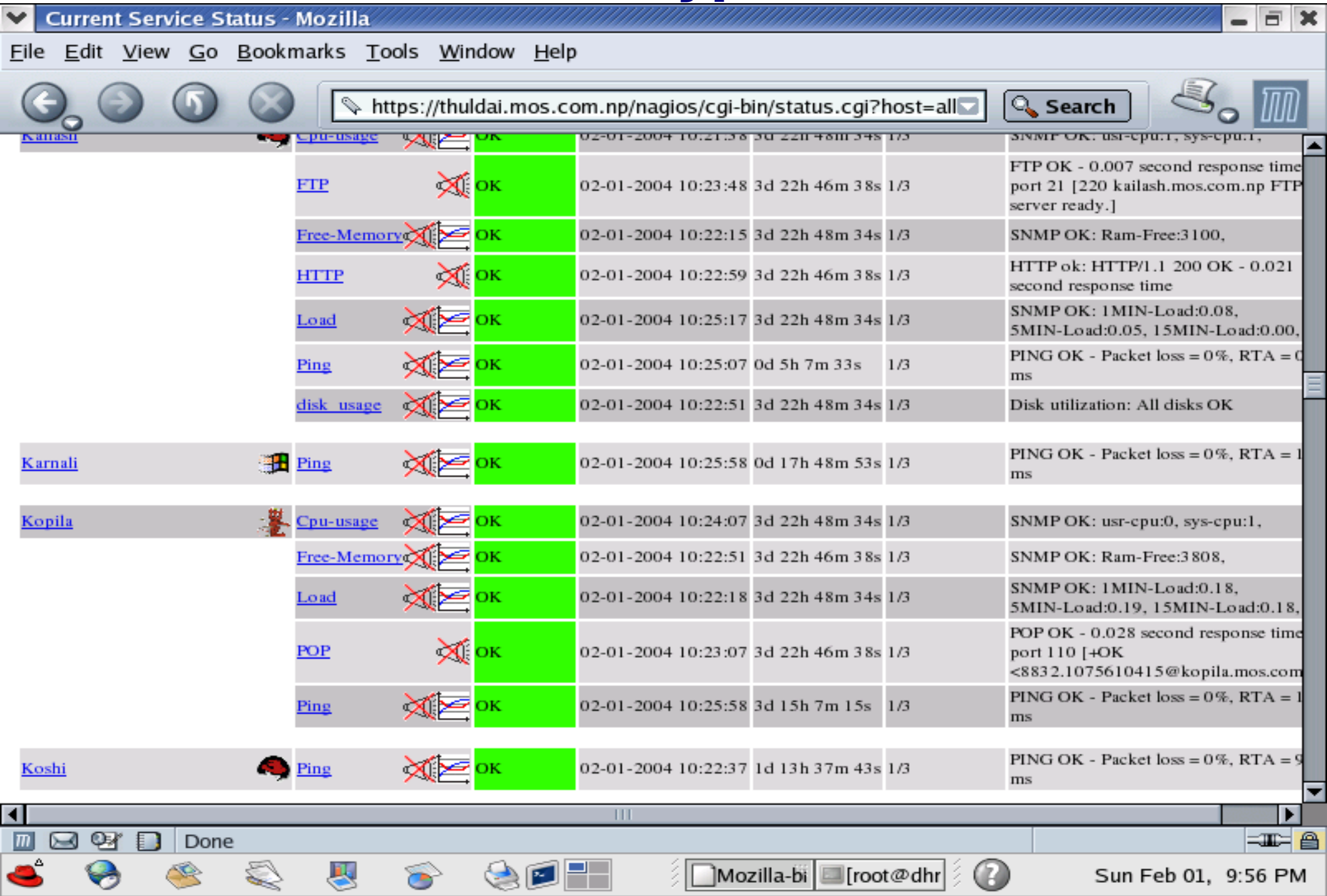


Tactical Overview Of Nagios

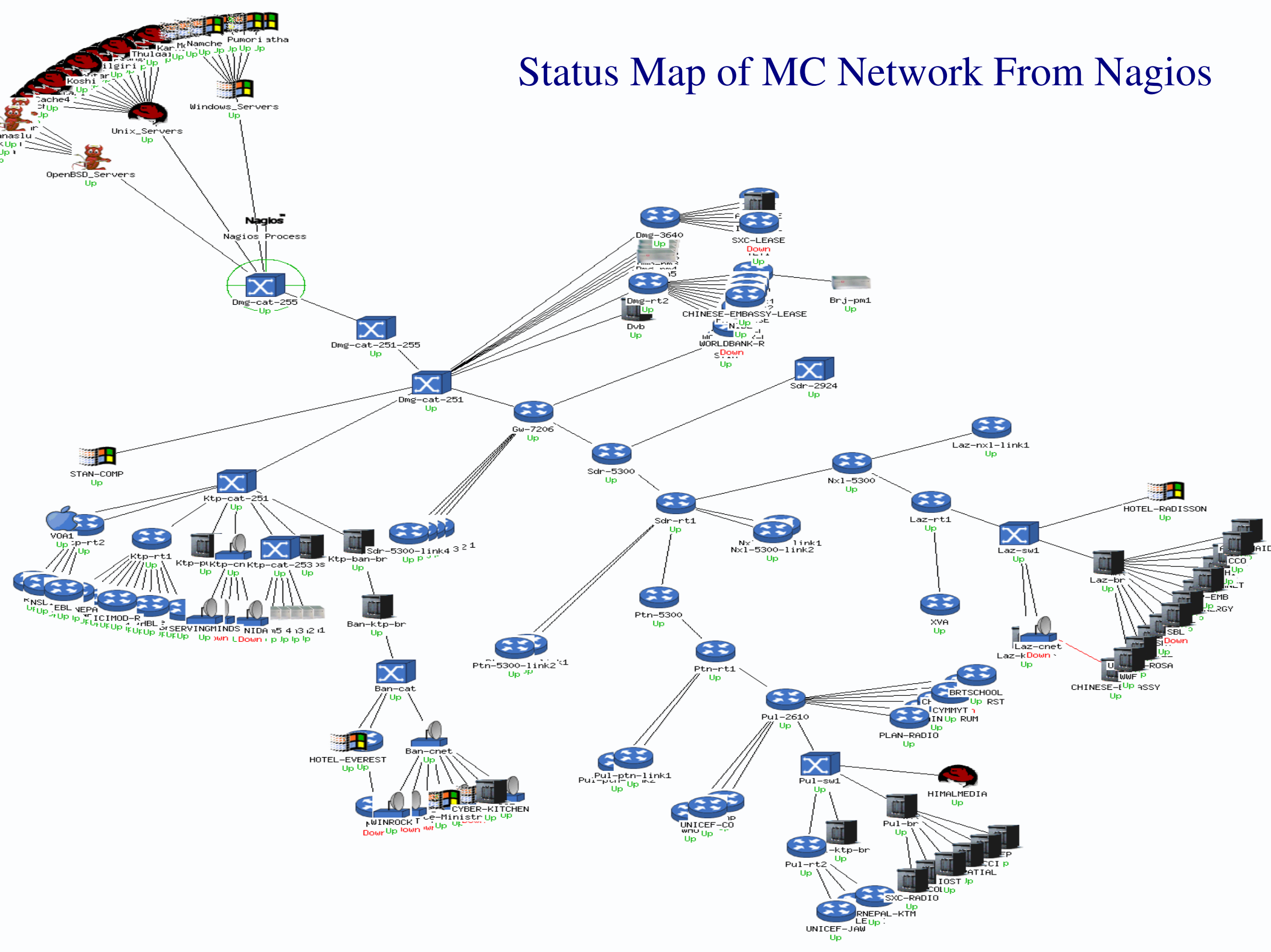


Service Detail of Nagios

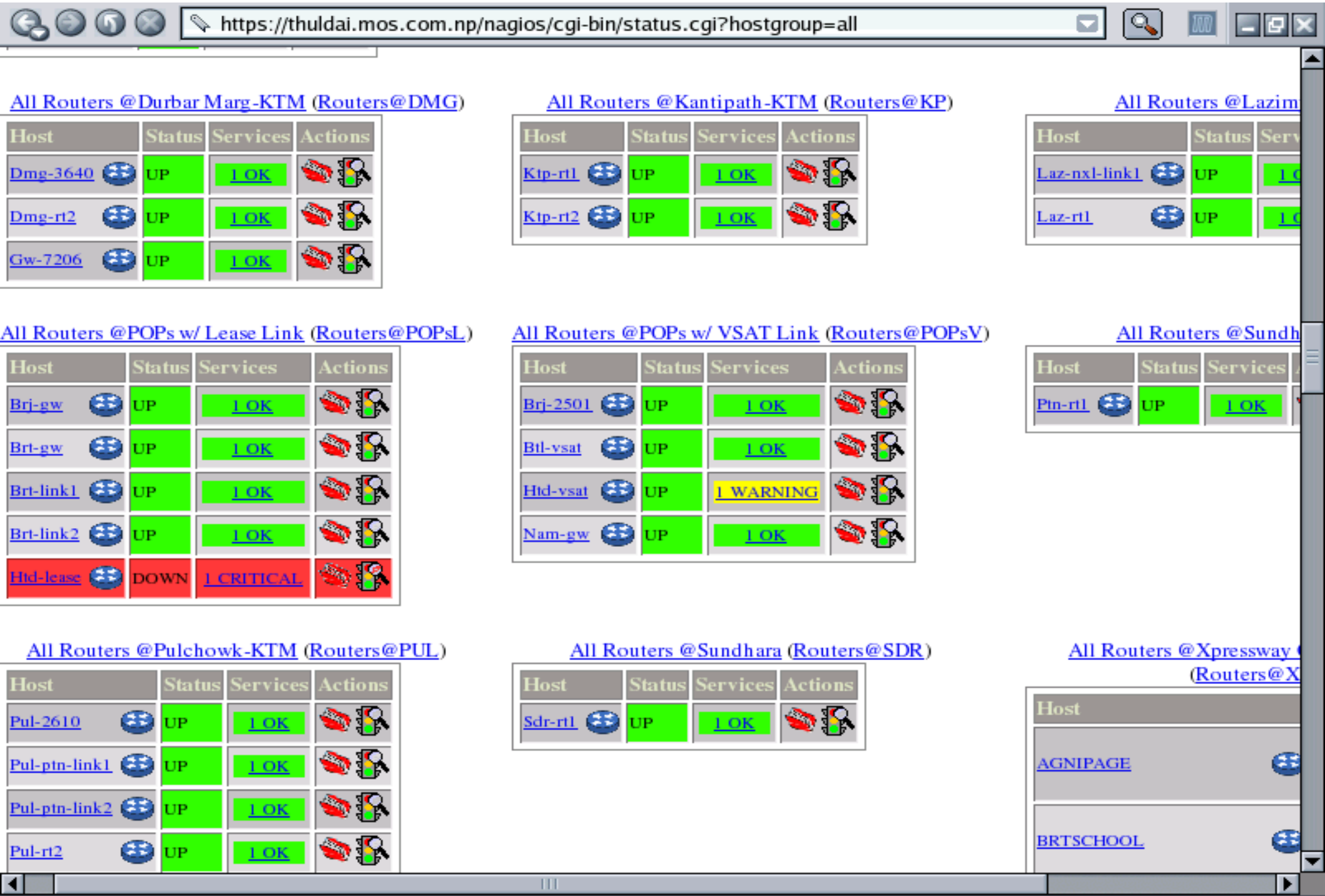
Service Types



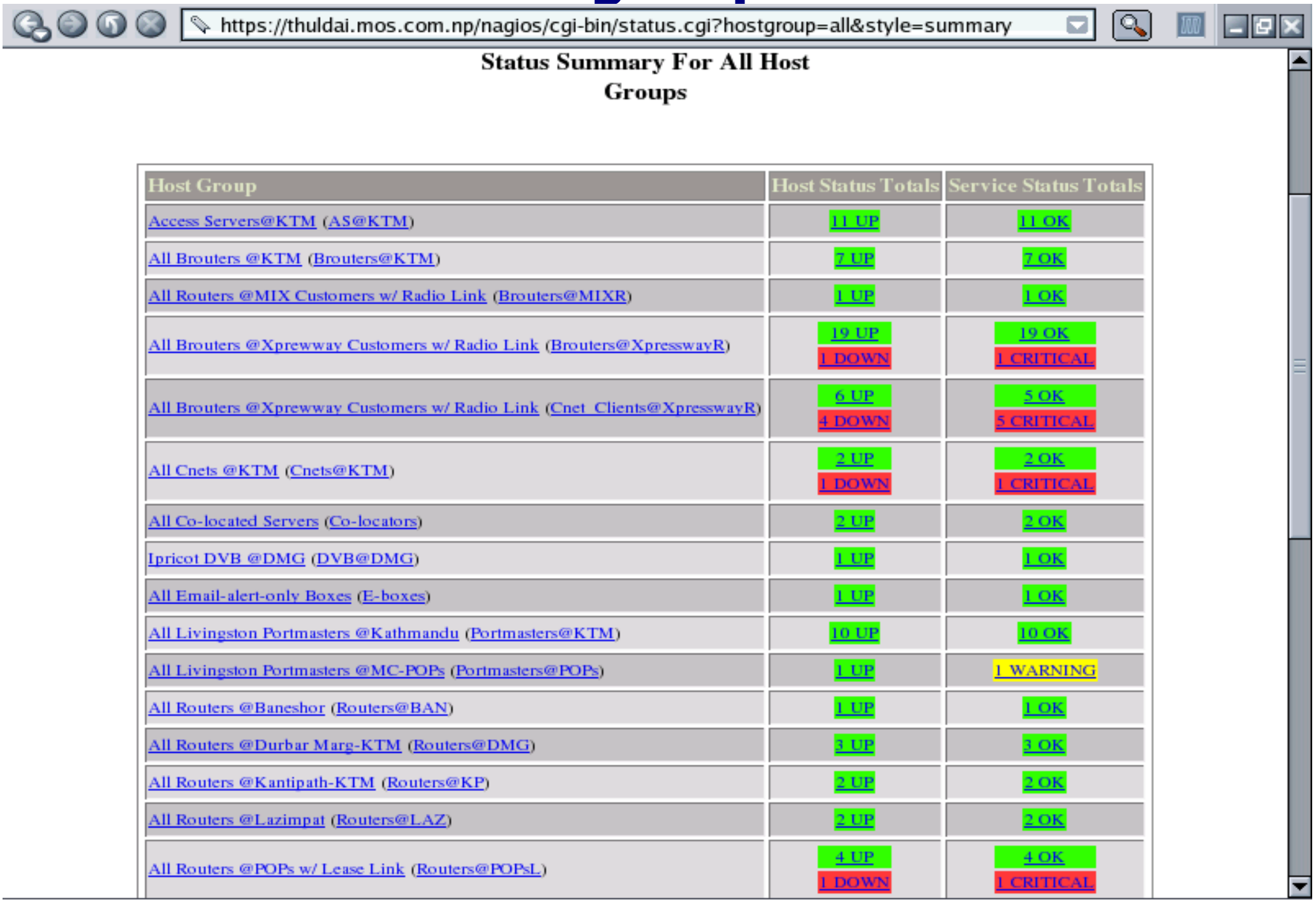
Status Map of MC Network From Nagios



Status Overview from nagios



Status Summary Based On Hostgroup

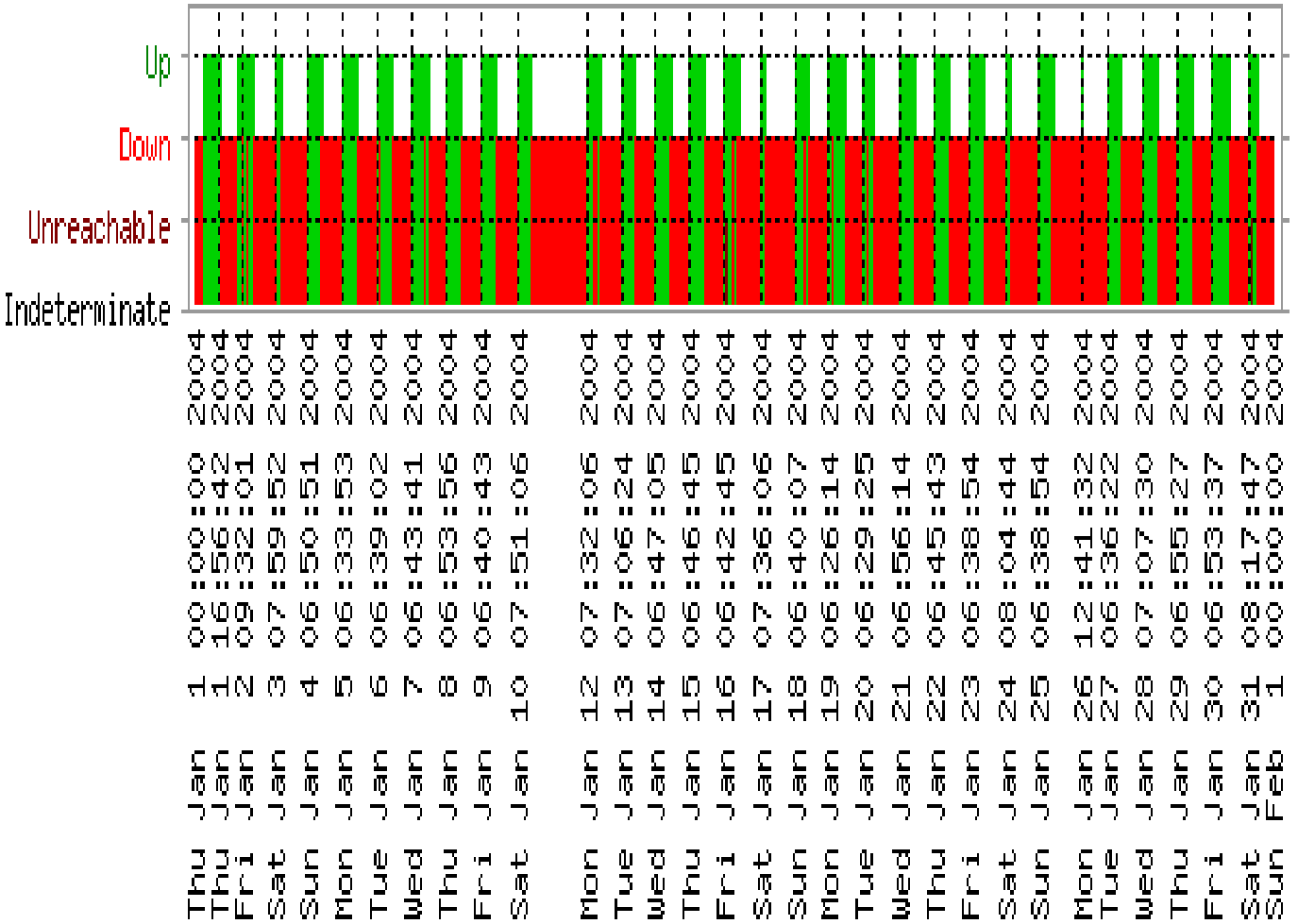


Host Trends or Status History

Trends

State History For Host 'Don_Bosco'

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

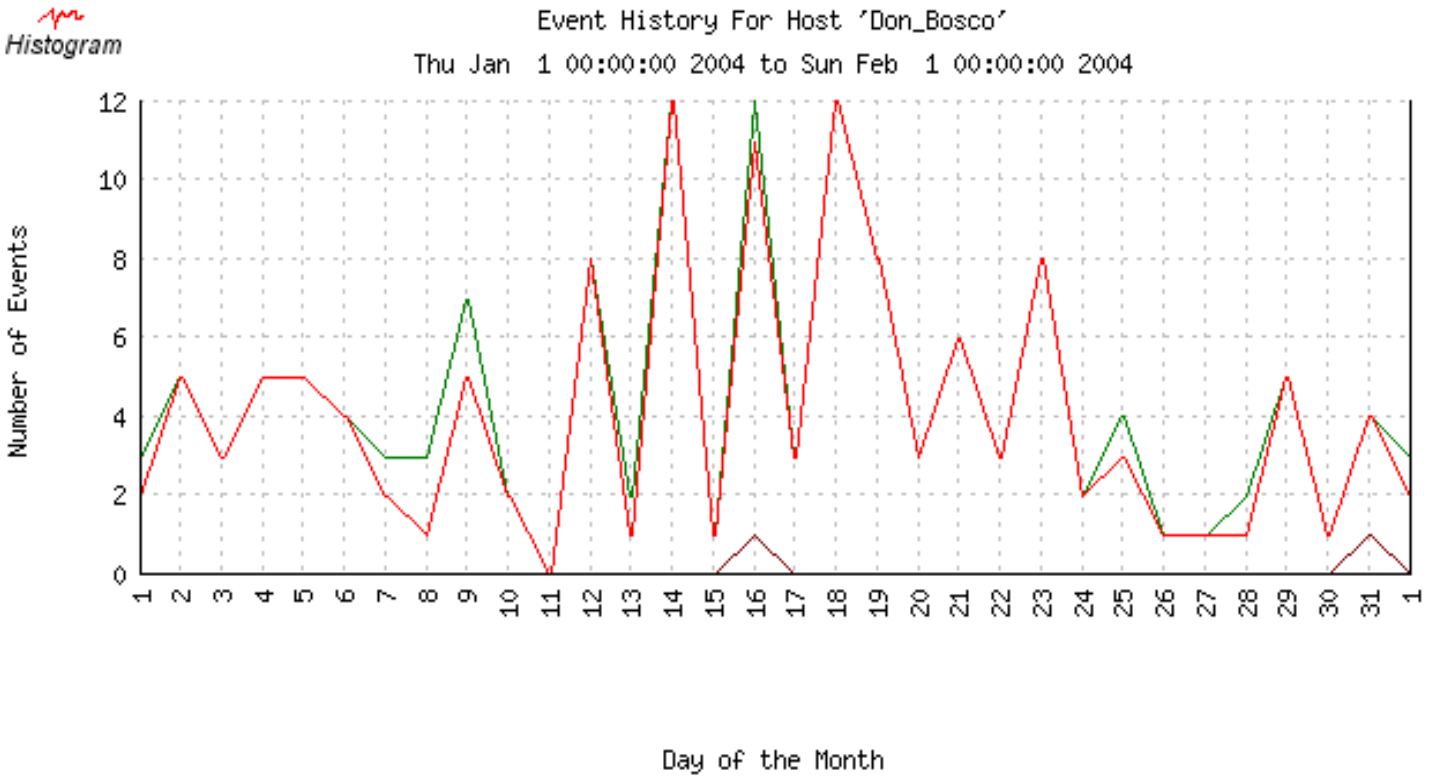


State Breakdowns:

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

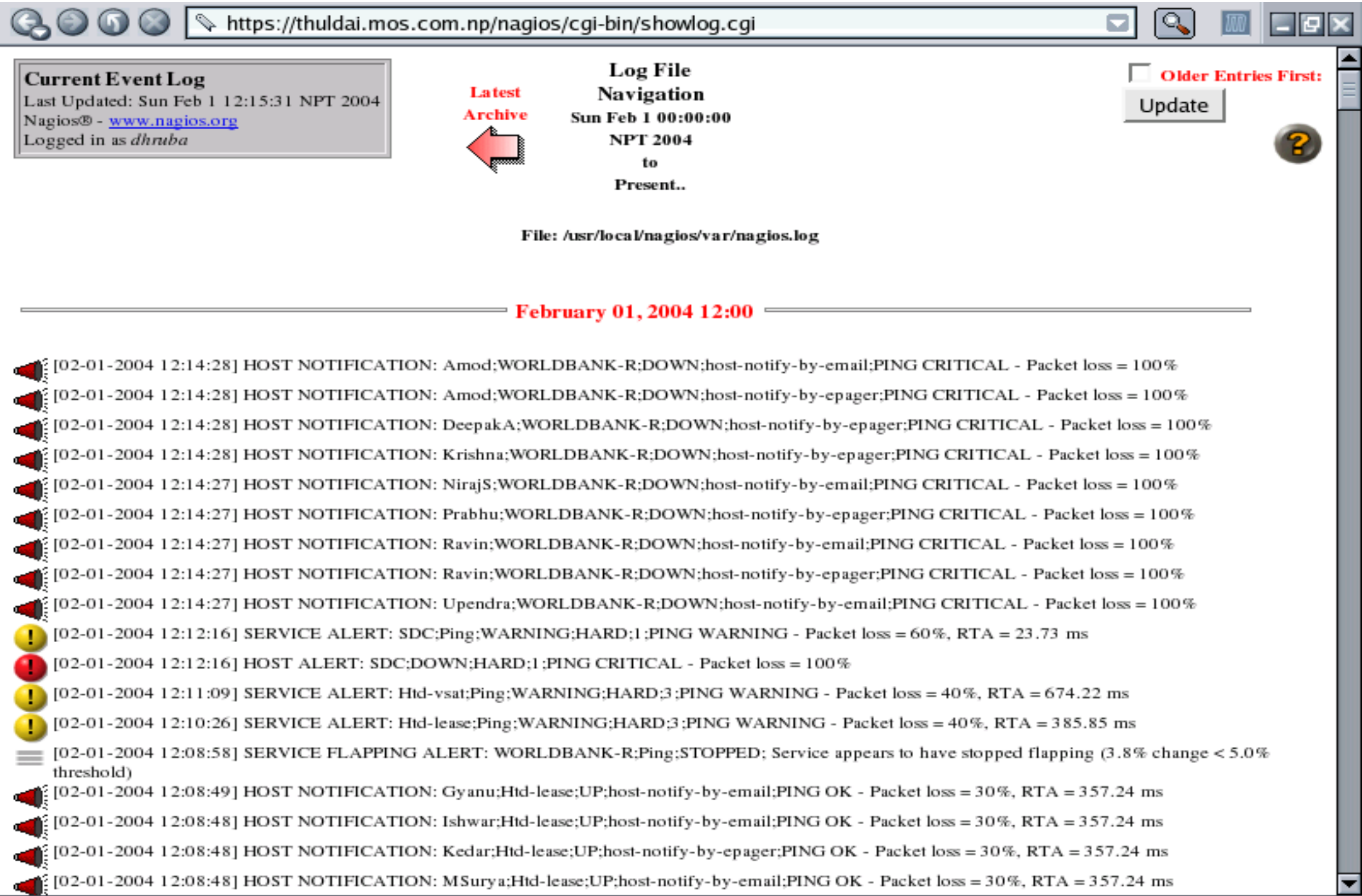
Histogram Of Host



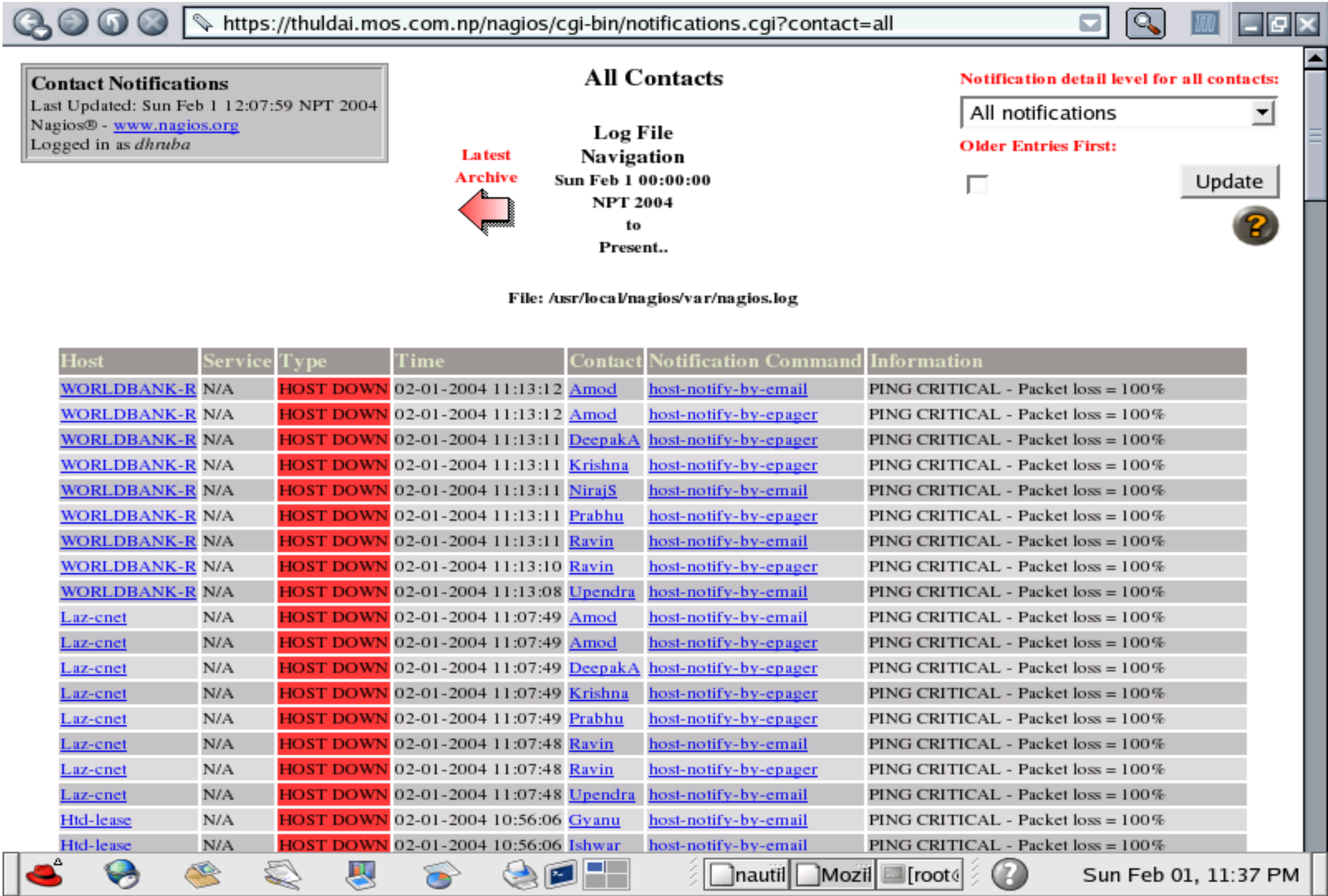
EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06

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

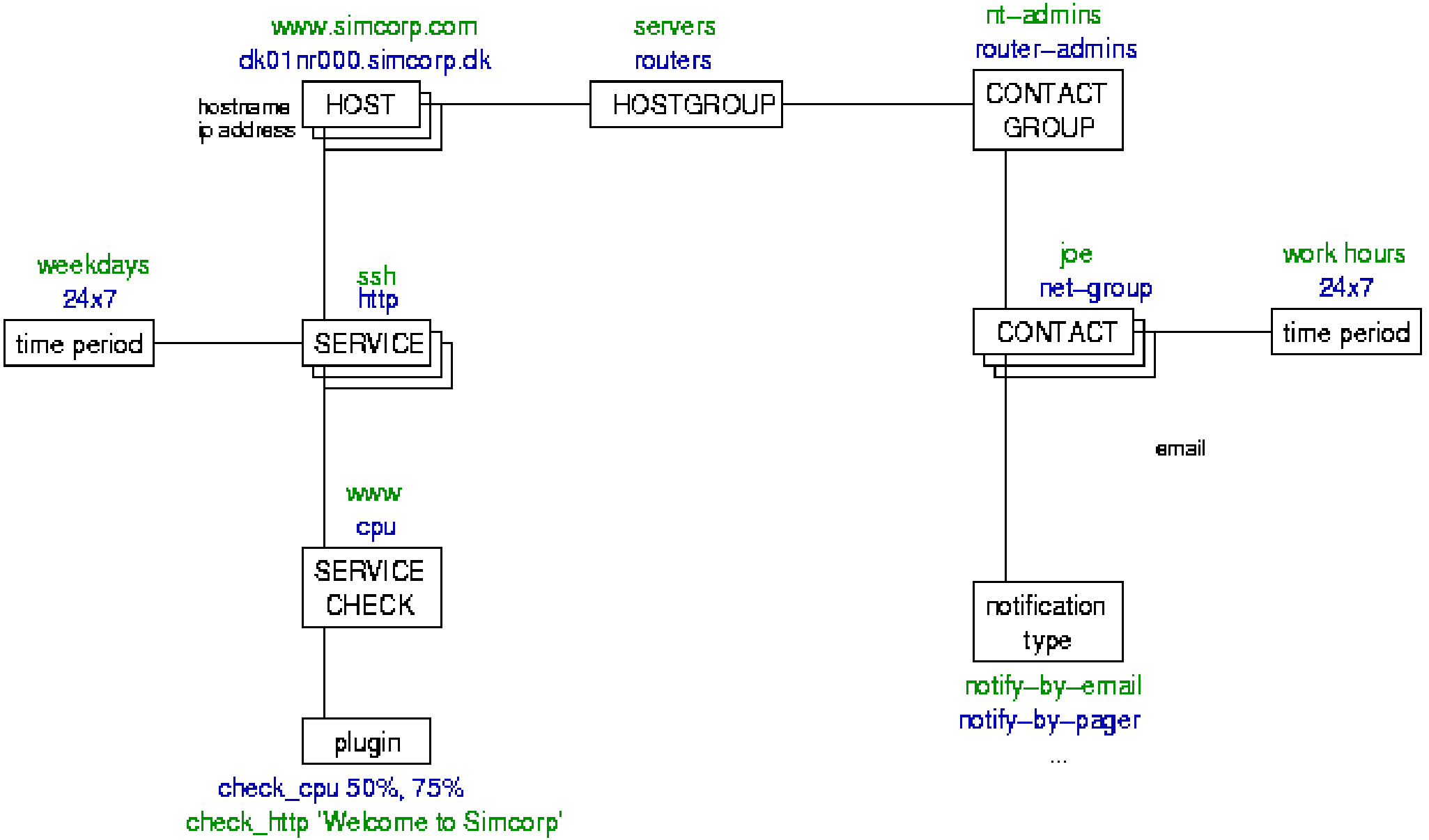
Nagios plugin configuration

- /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 configuration walkthrough

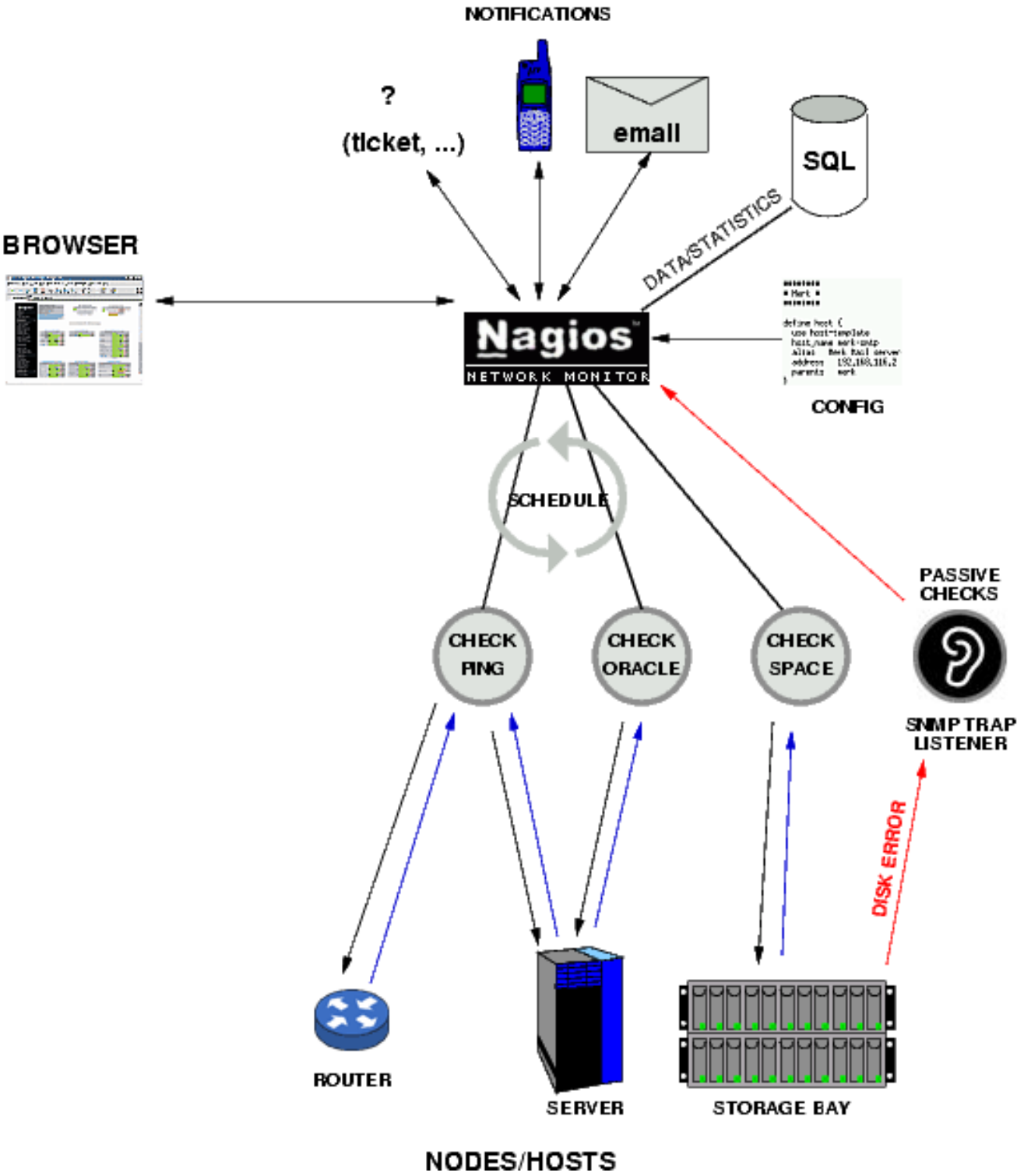
- Let's review the configuration files...

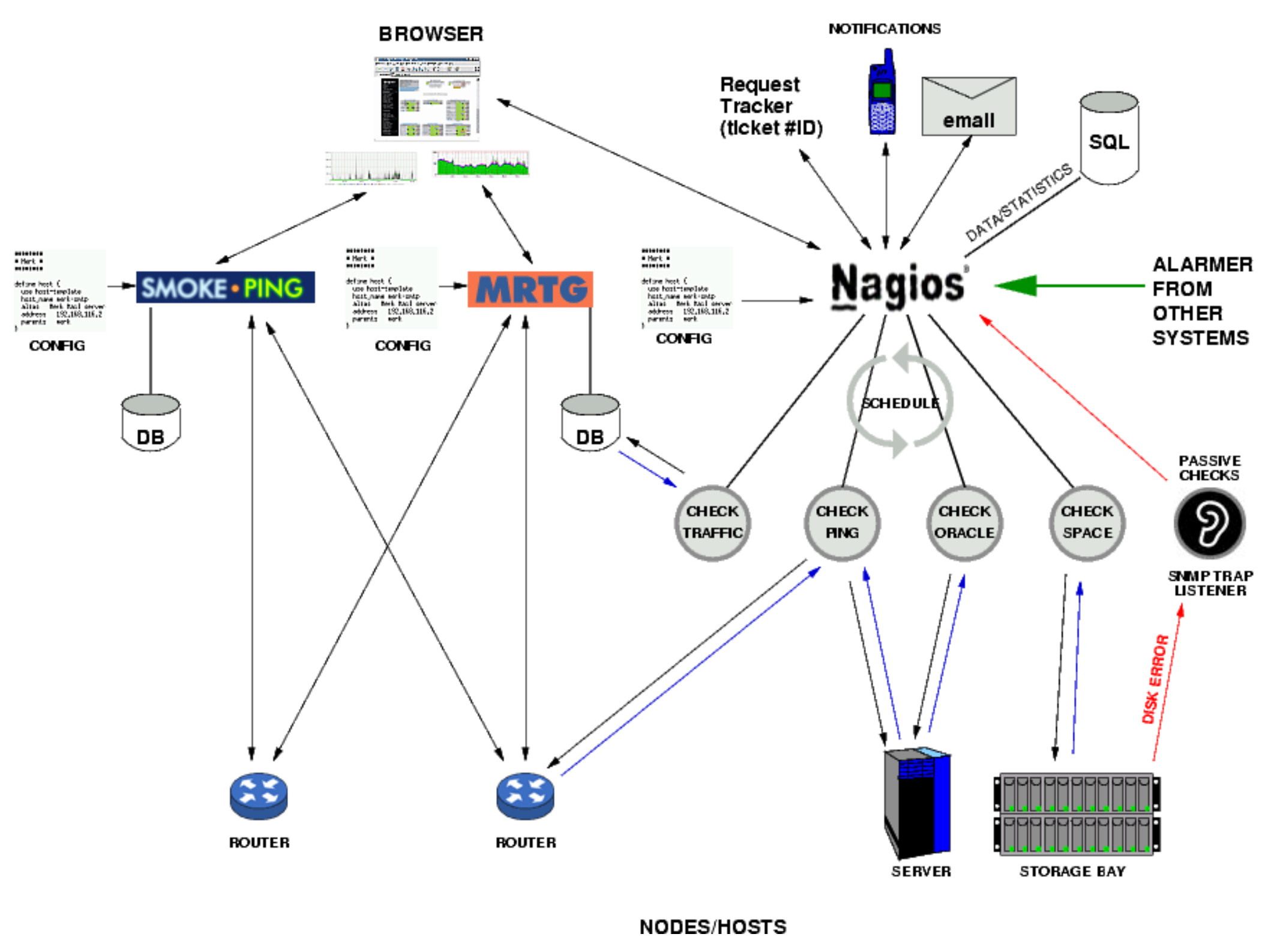
NAGIOS schema



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

Questions?