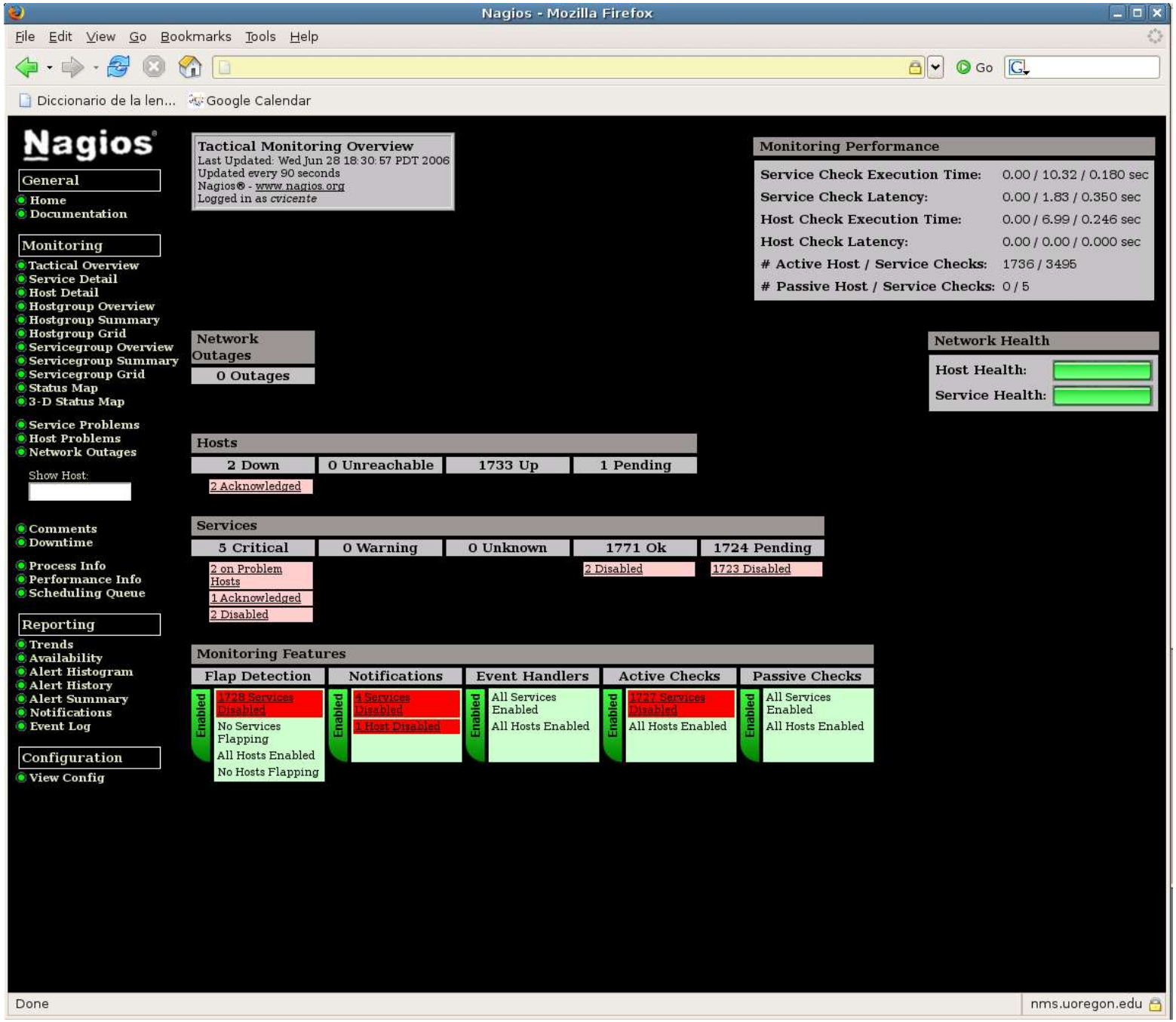
Nagios®

Baseline, Monitor, Detect, Analyze, Respond, & Recover

Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnauld 2009 Santiago, Chile

Introduction

- A key measurement tool for actively monitoring availability of devices and services.
- Possible the most used open source network monitoring software.
- Has a web interface.
  - Uses CGIs written in C for faster response and scalability.
- Can support up to thousands of devices and services.


Nagios - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Diccionario de la len...
Google Calendar
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Tactical Monitoring Overview
Last Updated: Wed Jun 28 18:30:57 PDT 2006
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as cvicente
Monitoring Performance
Service Check Execution Time: 0.00 / 10.32 / 0.180 sec
Service Check Latency: 0.00 / 1.83 / 0.350 sec
Host Check Execution Time: 0.00 / 6.99 / 0.246 sec
Host Check Latency: 0.00 / 0.00 / 0.000 sec
Active Host / Service Checks: 1736 / 3495
Passive Host / Service Checks: 0 / 5
Network Outages
0 Outages
Network Health
Host Health:
Service Health:
Hosts
2 Down
0 Unreachable
1733 Up
1 Pending
2 Acknowledged
Services
5 Critical
0 Warning
0 Unknown
1771 Ok
1724 Pending
2 on Problem Hosts
1 Acknowledged
2 Disabled
2 Disabled
1723 Disabled
Monitoring Features
Flap Detection
Notifications
Event Handlers
Active Checks
Passive Checks
Enabled
1728 Services Disabled
No Services Flapping
All Hosts Enabled
No Hosts Flapping
4 Services Disabled
1 Host Disabled
All Services Enabled
All Hosts Enabled
1727 Services Disabled
All Hosts Enabled
All Services Enabled
All Hosts Enabled
Done
nms.uoregon.edu

Features

- Verification of availability is delegated to plugins:
  - The product's architecture is simple enough that writing new plugins is fairly easy in the language of your choice.
  - There are many, many plugins available.
- *Nagios uses parallel checking and forking.*
  - *Version 3 of Nagios does this better.*

Features cont.

- Has intelligent checking capabilities. Attempts to distribute the server load of running Nagios (for larger sites) and the load placed on devices being checked.
- Configuration is done in simple, plain text files, but that can contain much detail and are based on templates.
- Nagios reads its configuration from an entire directory. You decide how to define individual files.

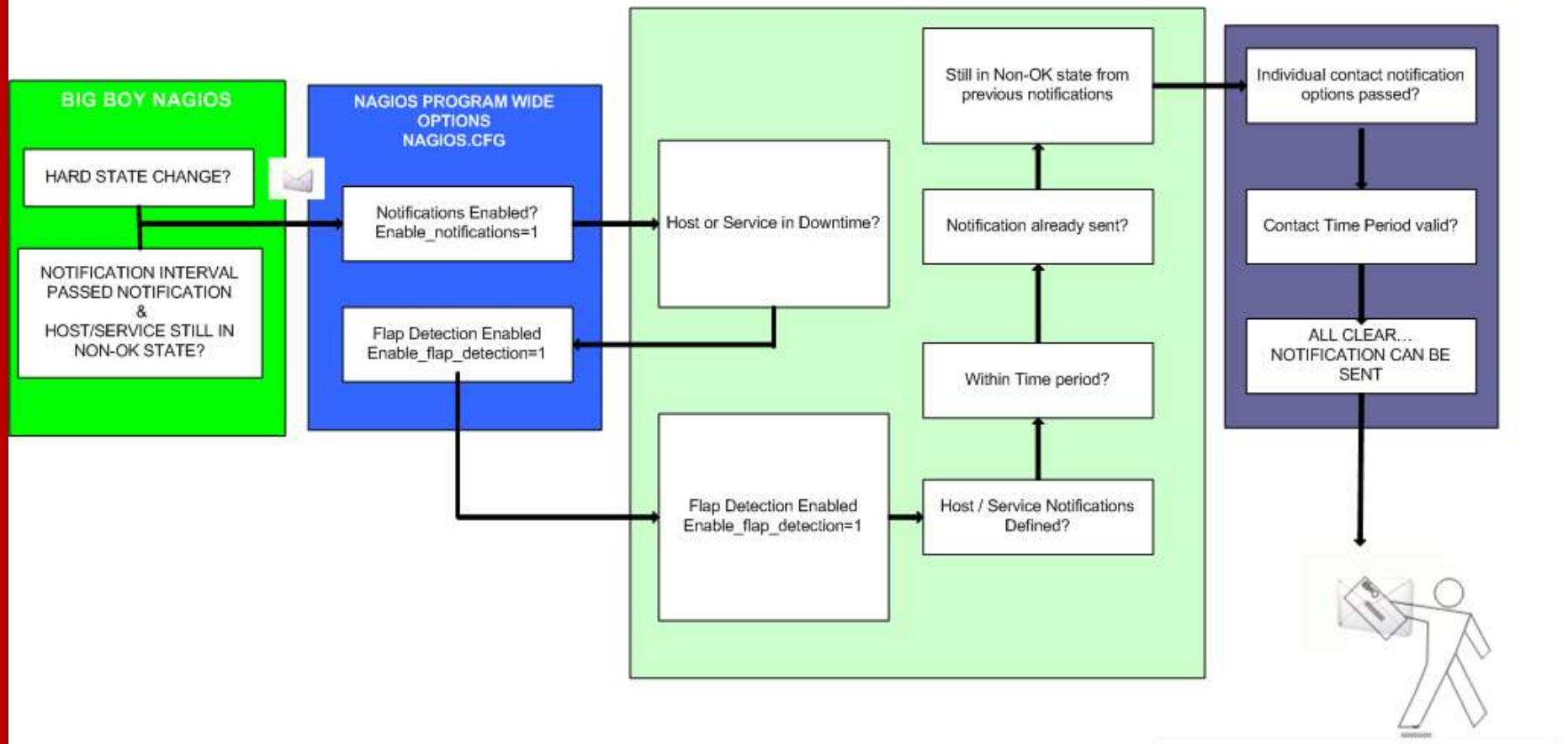
Yet More Features...

- Utilizes topology to determine dependencies.
  - *Nagios differentiates between what is down vs. what is not available. This way it avoids running unnecessary checks.*
- *Nagios allows you to define how you send notifications based on combinations of:*
  - *Contacts and lists of contacts*
  - *Devices and groups of devices*
  - *Services and groups of services*
  - *Defined hours by persons or groups.*
  - *The state of a service.*

And, even more...

- **Service state:**
- When configuration a service you have the following notification options:
  - **d:** DOWN: The service is down (not available)
  - **u:** UNREACHABLE: When the host is not visible
  - **r:** RECOVERY: (OK) Host is coming back up
  - **f:** FLAPPING: When a host first starts or stops or it's state is undetermined.
  - **n:** NONE: Don't send any notifications

NAGIOS - NOTIFICATION FLOW DIAGRAM



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

CONTACT GETS THE NOTIFICATION MESSAGE

Features, features, features

- Allows you to acknowledge an event.
  - A user can add comments via the GUI
- You can define maintenance periods
  - By device or a group of devices
- Maintains availability statistics.
- Can detect *flapping* and suppress additional notifications.
- Allows for multiple notification methods such as:
  - e-mail, pager, SMS, winpopup, audio, etc...
- *Allows you to define notification levels. Critical feature.*

How Checks Work

- A node/host/device consists of one or more service checks (PING, HTTP, MYSQL, SSH, etc)
- Periodically Nagios checks each service for each node and determines if state has changed. State changes are:
  - CRITICAL
  - WARNING
  - UNKNOWN
- For each state change you can assign:
  - Notification options (as mentioned before)
  - Event handlers

How Checks Work

- Parameters
  - Normal checking interval
  - Re-check interval
  - Maximum number of checks.
  - Period for each check
- Node checks only happen when no services respond (assuming you've configured this).
  - A node can be:
    - DOWN
    - UNREACHABLE

How Checks Work

- In this manner it can take some time before a host change's its state to “down” as Nagios first does a service check and then a node check.
- By default Nagios does a node check 3 times before it will change the nodes state to down.
- You can, of course, change all this.

Passive checks

- Nagios also supports “passive checks”.
- These are checks which are never actively scheduled. Instead, Nagios waits to receive notifications of the status of this service from an external program, to update the service status.
- The state doesn't change until a new update arrives.

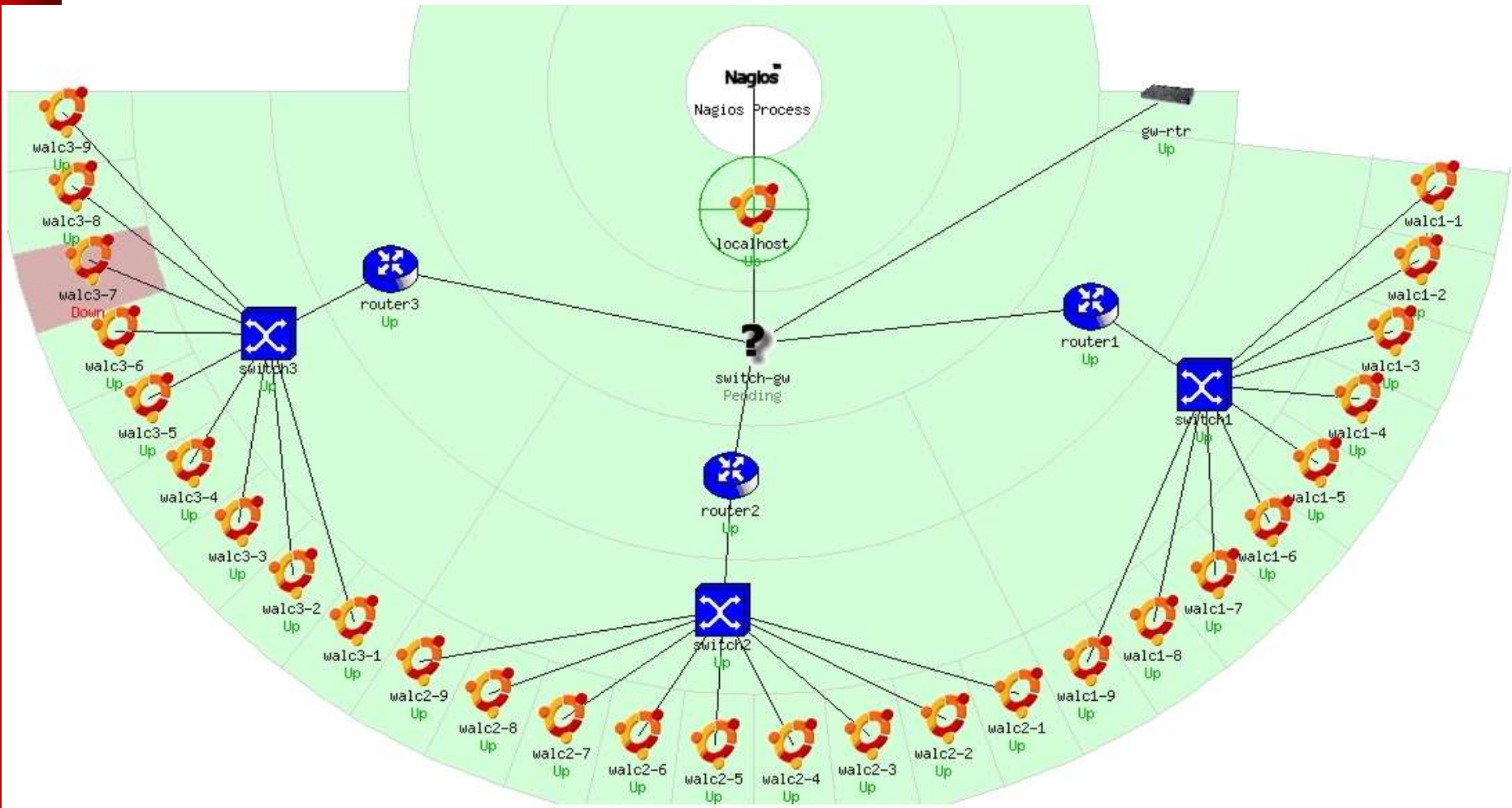
The Concept of “Parents”

- Nodes can have parents.
  - For example, the parent of a PC connected to a switch would be the switch.
  - This allows us to specify the network dependencies that exist between machines, switches, routers, etc.
  - This avoids having Nagios send alarms when a parent does not respond.
  - A node can have multiple parents.

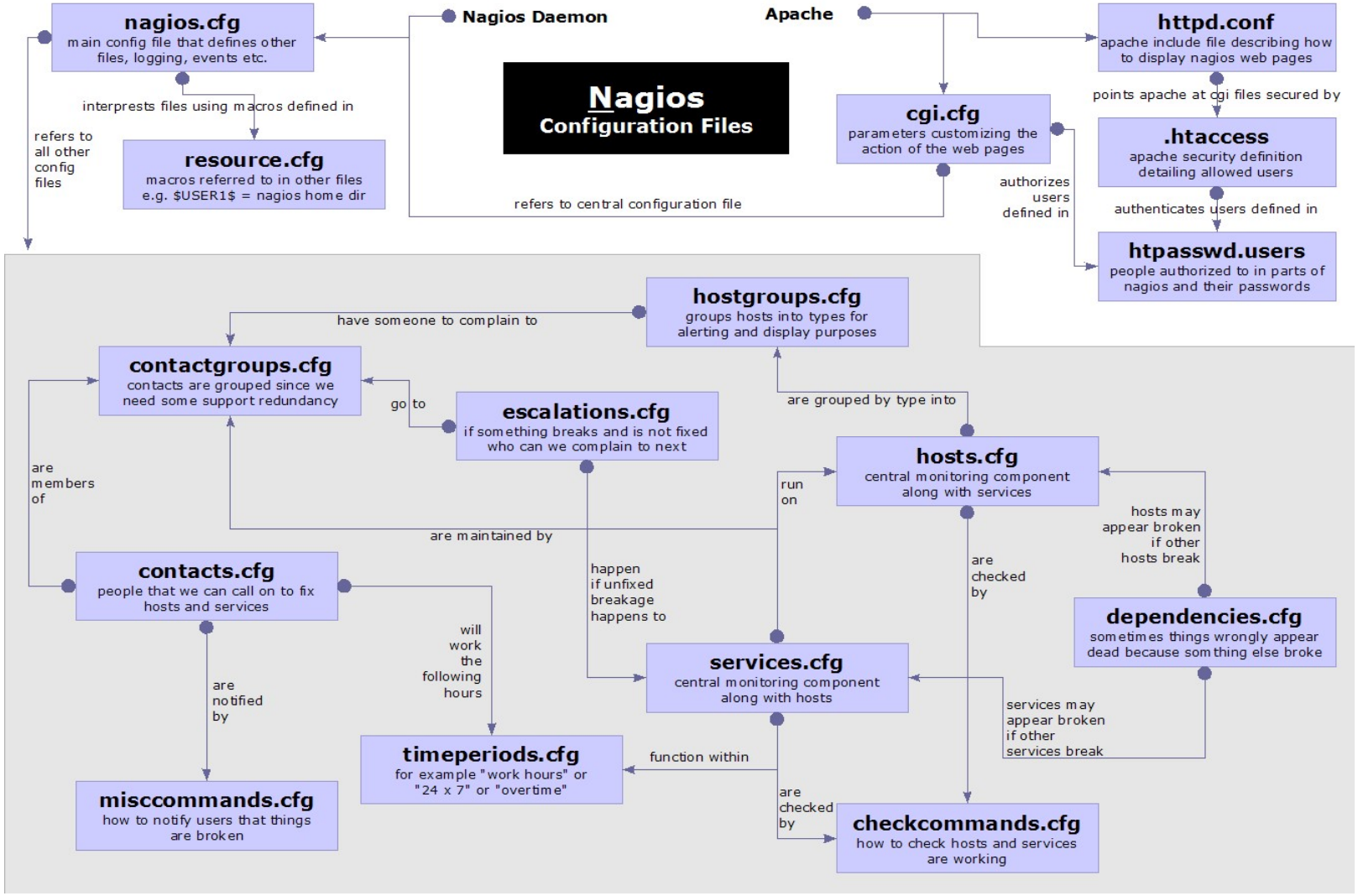
The Idea of Network Viewpoint

- Where you locate your Nagios server will determine your point of view of the network.
- Nagios allows for parallel Nagios boxes that run at other locations on a network.
- Often it makes sense to place your Nagios server nearer the border of your network vs. in the core.

Network Viewpoint



Nagios Configuration Files



Relations

- Hosts belong to host groups
- Contacts belong to contact groups
- Time periods are assigned to check periods and notification periods
- Services are assigned to hosts
- Service checks are assigned to services
- Host checks are assigned to hosts

All this allow for very flexible configuration

Configuration Files

- Located in /etc/nagios3/
- Important files include:
  - cgi.cfg — Controls the web interface and security options.
  - commands.cfg — The commands that Nagios uses for notifications.
  - nagios.cfg — Main configuration file.
  - conf.d/* — All other configuration goes here!

Configuration Files

- **Under conf.d/* (*sample only*)**

contacts_nagios3.cfg	users and groups
generic-host_nagios2.cfg	default host template
generic-service_nagios2.cfg	default service template
hostgroups_nagios2.cfg	groups of nodes
services_nagios2.cfg	what services to check
timeperiods_nagios2.cfg	when to check and who to notifiy

Configuration Files

- **Under conf.d some other possible config files:**
  - host-gateway.cfg — Default route definition
  - extinfo.cfg — Additional node information
  - servicegroups.cfig — Groups of nodes and services
  - localhost.cfg — Define the Nagios server itself
  - pcs.cfg — Sample definition of PCs (hosts)
  - switches.cfg — Definitions of switches (hosts)
  - routers.cfg — Definitions of routers (hosts)

Plugin Configuration

- The Nagios package in Ubuntu comes with a bunch of pre-installed plugins definitions:
- apt.cfg breeze.cfg dhcp.cfg disk-smb.cfg disk.cfg dns.cfg dummy.cfg flexlm.cfg fping.cfg ftp.cfg games.cfg hppjd.cfg http.cfg ifstatus.cfg ldap.cfg load.cfg mail.cfg mrtg.cfg mysql.cfg netware.cfg news.cfg nt.cfg ntp.cfg pgsql.cfg ping.cfg procs.cfg radius.cfg real.cfg rpc-nfs.cfg snmp.cfg ssh.cfg tcp_udp.cfg telnet.cfg users.cfg vsz.cfg

Main Configuration Details

- Global settings
- File: /etc/nagios3/nagios.cfg
  - Says where other configuration files are.
  - General Nagios behavior:
    - For large installations you should tune the installation via this file.
  - See: *Tuning Nagios for Maximum Performance* **http://nagios.sourceforge.net/docs/2_0/tuning.html**

CGI Configuration

- Archivo: /etc/nagios3/cgi.cfg
  - You can change the CGI directory if you wish
  - Authentication and authorization for Nagios use.
    - Activate authentication via Apache's .htpasswd mechanism, or using RADIUS or LDAP.
    - Users can be assigned rights via the following variables:
      - authorized_for_system_information
      - authorized_for_configuration_information
      - authorized_for_system_commands
      - authorized_for_all_services
      - authorized_for_all_hosts
      - authorized_for_all_service_commands
      - authorized_for_all_host_commands

Time Periods

- This defines the base periods that control checks, notifications, etc.
  - Defaults: 24 x 7
  - Could adjust as needed, such as work week only.
  - Could adjust a new time period for “outside of regular hours”, etc.

```
# '24x7'
define timeperiod{
        timeperiod_name 24x7
        alias           24 Hours A Day, 7 Days A Week
        sunday          00:00-24:00
        monday          00:00-24:00
        tuesday         00:00-24:00
        wednesday       00:00-24:00
        thursday        00:00-24:00
        friday          00:00-24:00
        saturday        00:00-24:00
        }
```

Configuring Service/Host Checks

- Define how you are going to test a service.

```
# 'check-host-alive' command definition
define command{
        command_name    check-host-alive
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c
5000.0,100% -p 1 -t 5
 }
```

Located in /etc/nagios-plugins/config, then adjust in /etc/nagios3/conf.d/services_nagios2.cfg

Notification Commands

- Allows you to utilize any command you wish.

```
# 'notify-by-email' command definition
define command{
        command_name    notify-by-email
        command_line    /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost:
$HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail -s
'$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
        }
```

From: nagios@nms.localdomain
To: switch-admins@localdomain
Subject: Host DOWN alert for switch1!
Date: Thu, 29 Jun 2006 15:13:30 -0700

Host: switch1
In: Core_Switches
State: DOWN
Address: 111.222.333.444
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds

Nodes and Services Configuration

- Based on templates
  - This saves lots of time avoiding repetition
  - *Similar to Object Oriented programming*
- Create default templates with default parameters for a:
  - generic node
  - generic service
  - generic contact

Generic Node Configuration

```
define host{
        name                            generic-host
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        check_command                   check-host-alive
        max_check_attempts              5
        notification_interval           60
        notification_period             24x7
        notification_options            d,r
        contact_groups                  nobody
        register                        0
        }
```

Individual Node Configuration

```
define host{
        use                     generic-host
        host_name               switch1
        alias                   Core_switches
        address                 192.168.1.2
        parents                 router1
        contact_groups          switch_group
}
```

Generic Service Configuration

```
define service{
        name                            generic-service
        active_checks_enabled           1
        passive_checks_enabled          1
        parallelize_check               1
        obsess_over_service             1
        check_freshness                 0
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              5
        normal_check_interval           5
        retry_check_interval            1
        notification_interval           60
        notification_period             24x7
        notification_options            c,r
        register                        0
        }
```

Individual Service Configuration

```
define service{
        host_name                       switch1
        use                             generic-service
        service_description             PING
        check_command                   check-host-alive
        max_check_attempts              5
        normal_check_interval           5
        notification_options            c,r,f
        contact_groups                  switch-group
}
```

Automation

- To maintain large configurations by hand becomes tiresome.
  - It's better to simplify and automate using scripts:

- **http://ns.uoregon.edu/~cvicente/download/nagios-config-scripts.tar.gz**
  - Or, export device (node) information from tools like Netdot, netdisco, OpenNMS, etc.

Beeper/SMS Messages

- It's important to integrate Nagios with something available outside of work
  - Problems occur after hours... (unfair, but true)
- A critical item to remember: an SMS or message system should be independent from your network.
  - You can utilize a modem and a telephone line
  - Packages like sendpage or qpage can help.

Some References

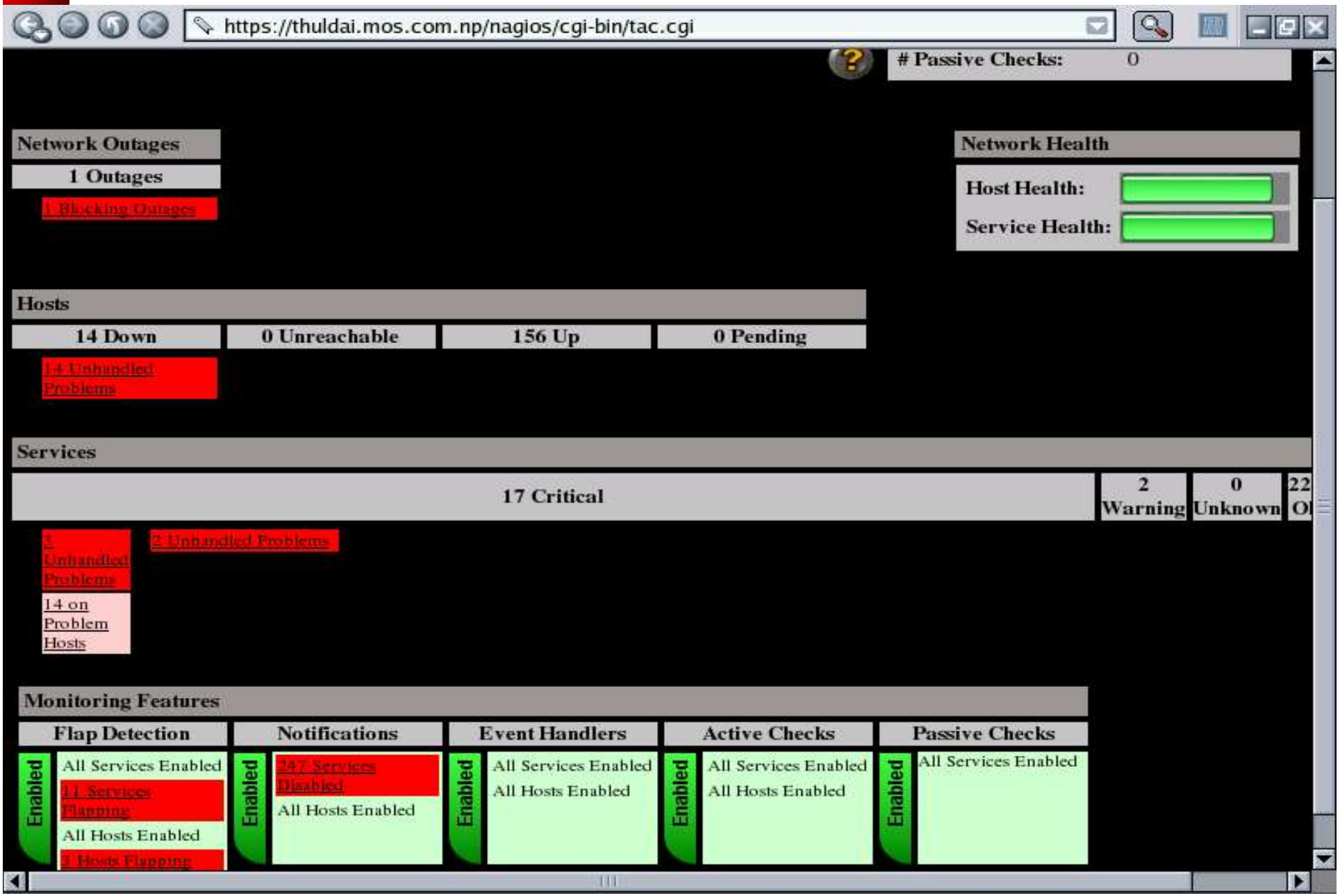
- **http://www.nagios.org**: Nagios web site
- **http://sourceforge.net/projects/nagiosplug**: Nagios plugins site
- *Nagios. System and Network Monitoring by* Wolfgang Barth. Good book onNagios
- **http://www.nagiosexchange.org**: Unofficial Nagios plugin site
- http://www.debianhelp.co.uk/nagios.htm: A Debian tutorial on Nagios
- http://www.nagios.com/: Commercial Nagios support

And, the O'Reilly book you received in class!

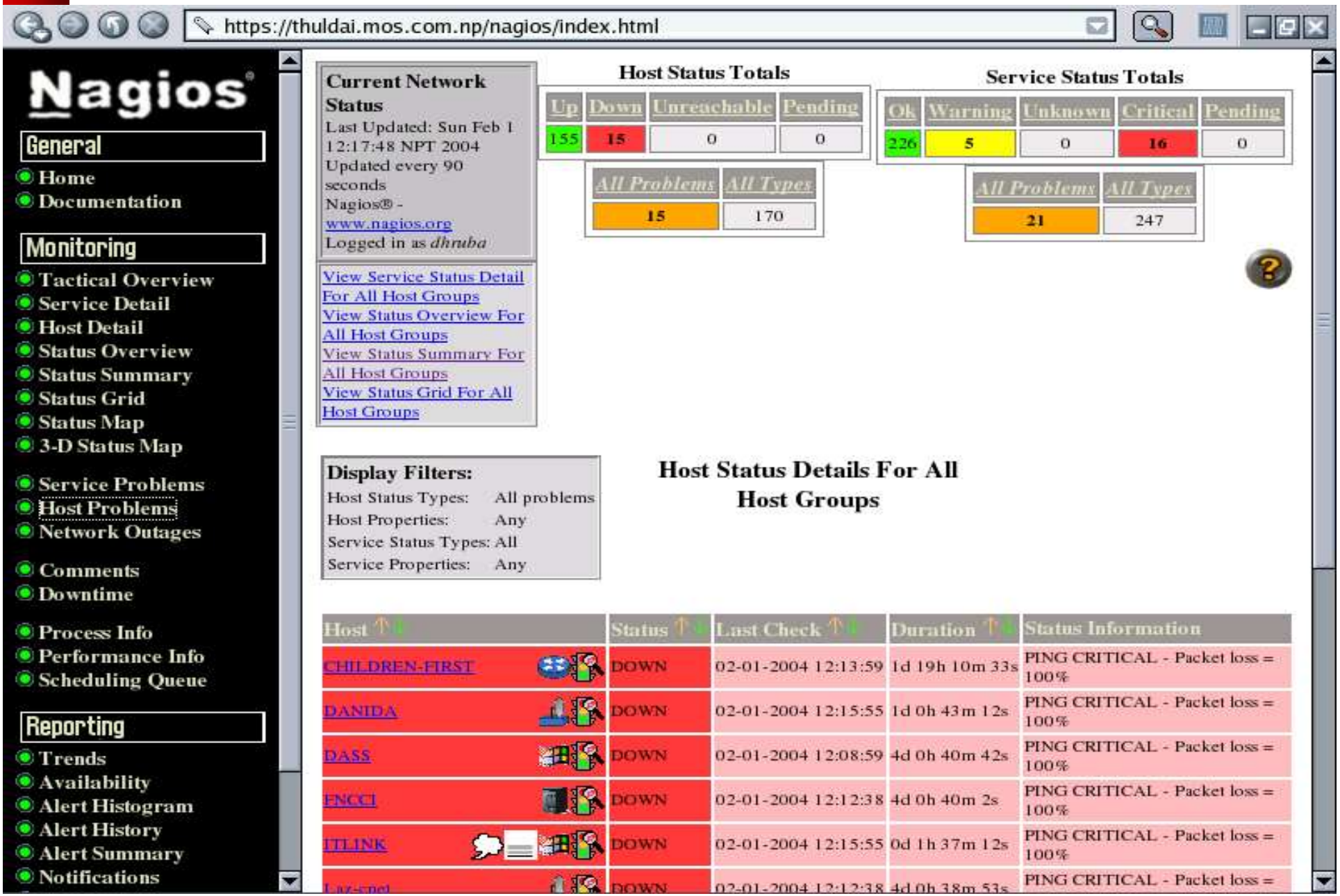
Nagios®

Reference Slides

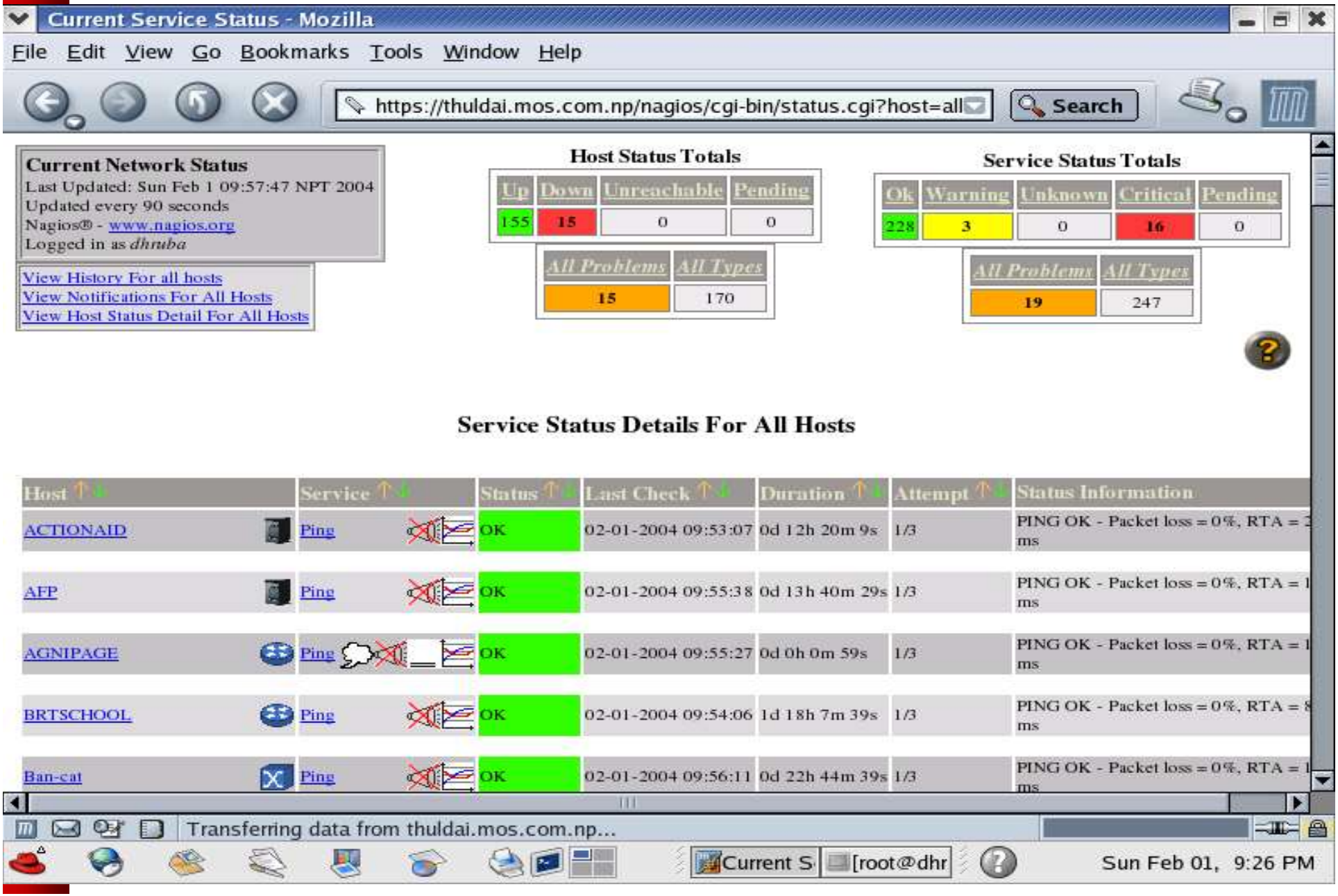
Nagios – (Tactical Overview)



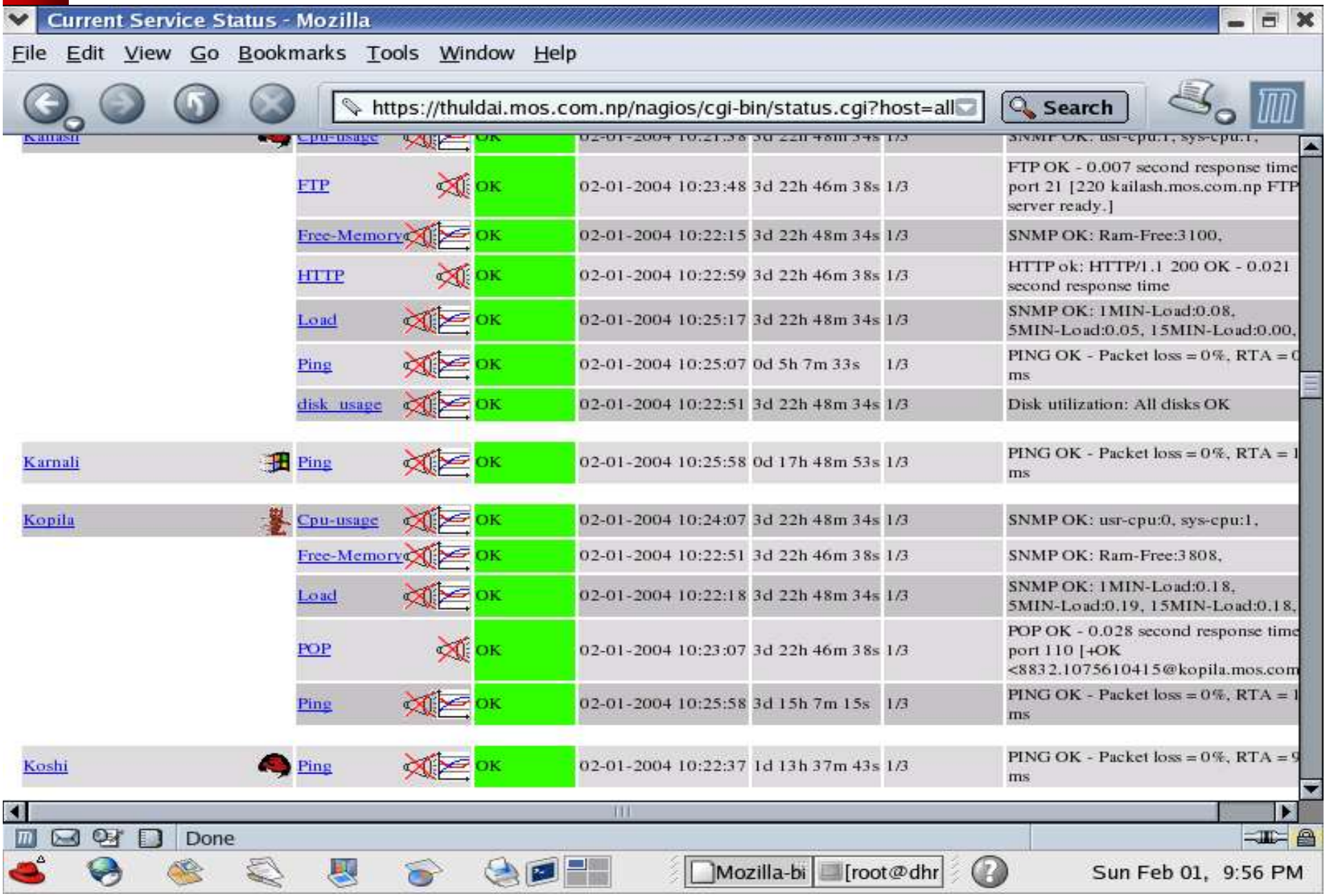
- **Status detail**



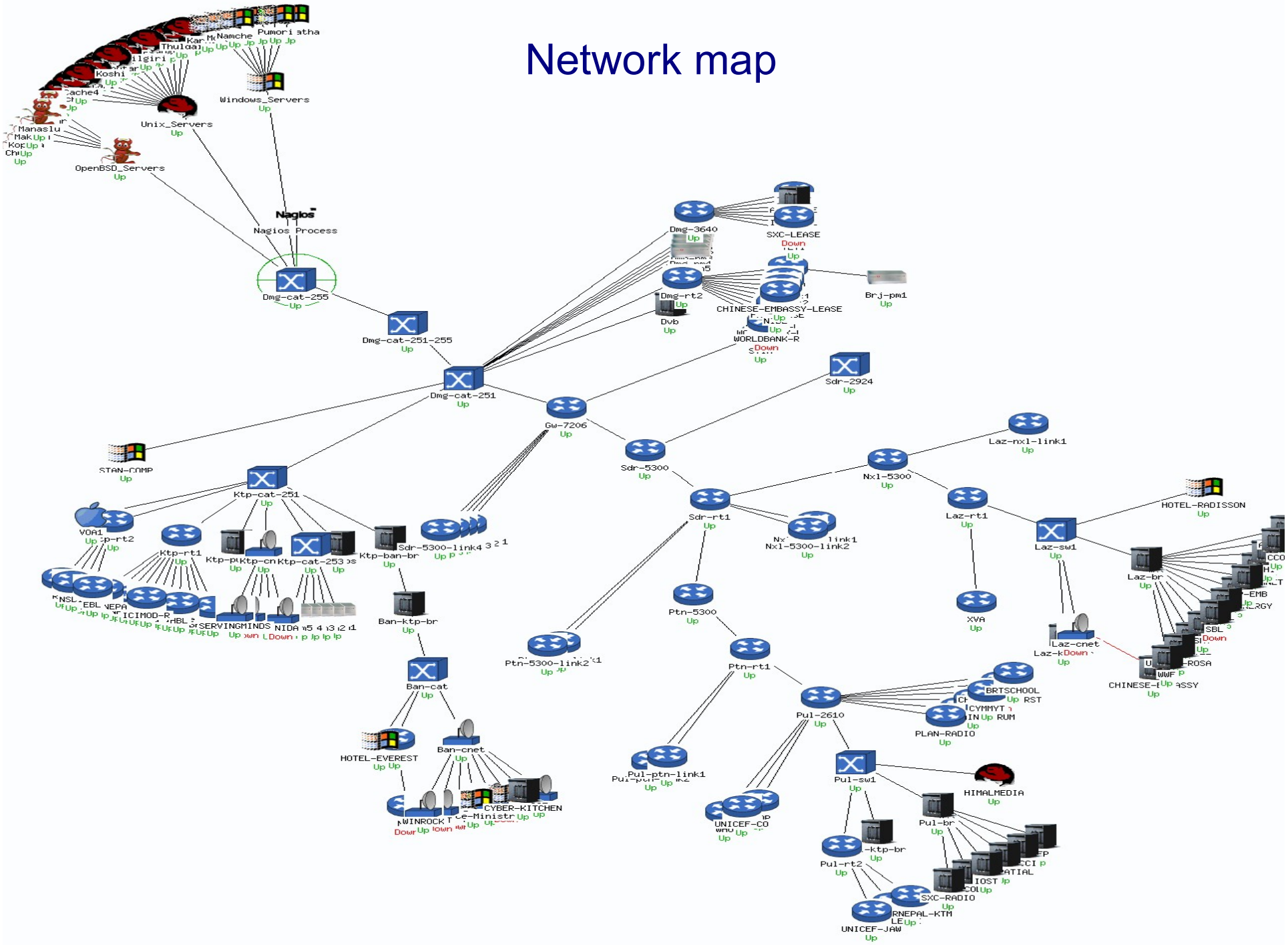
Status detail



Service overview

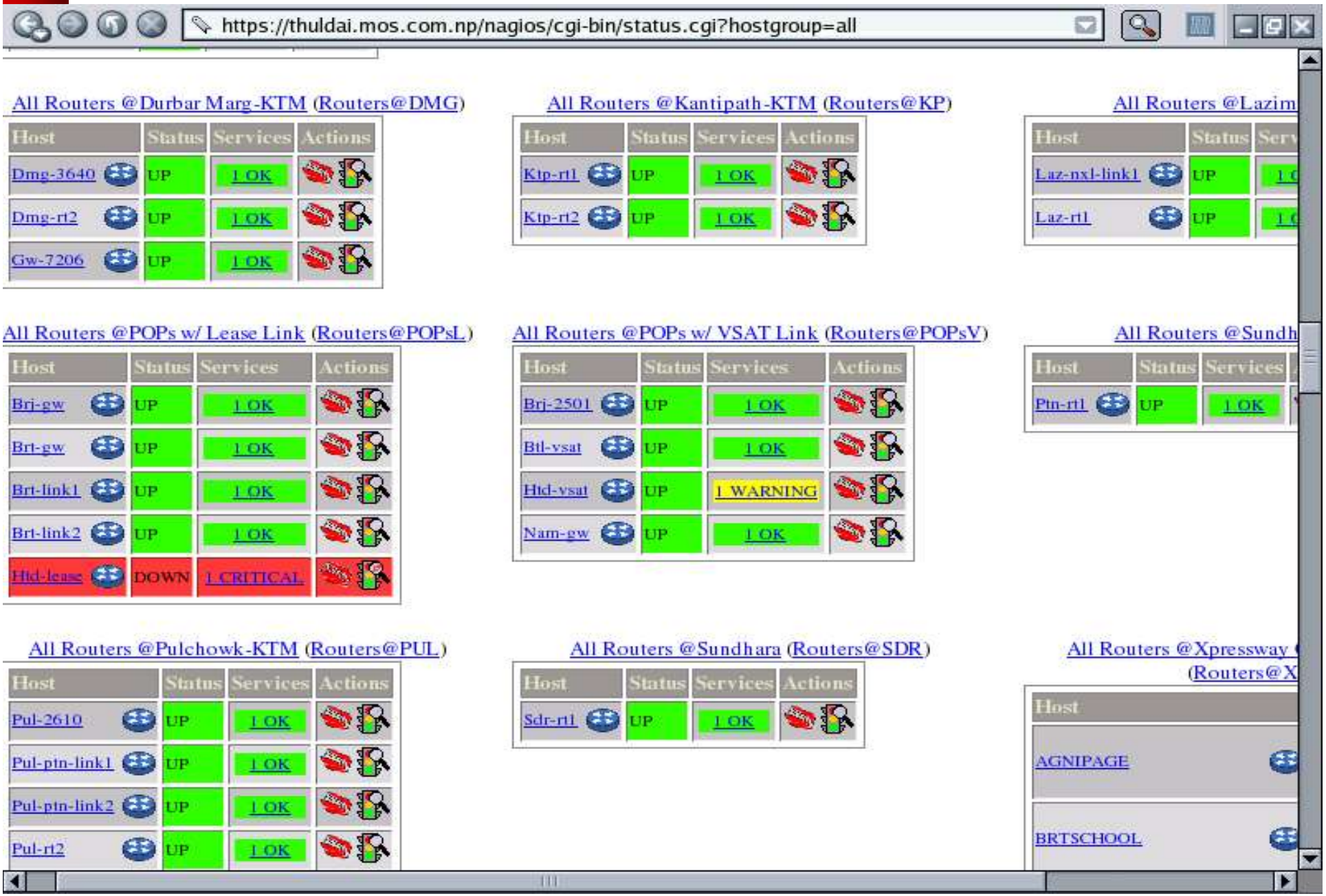


Network map

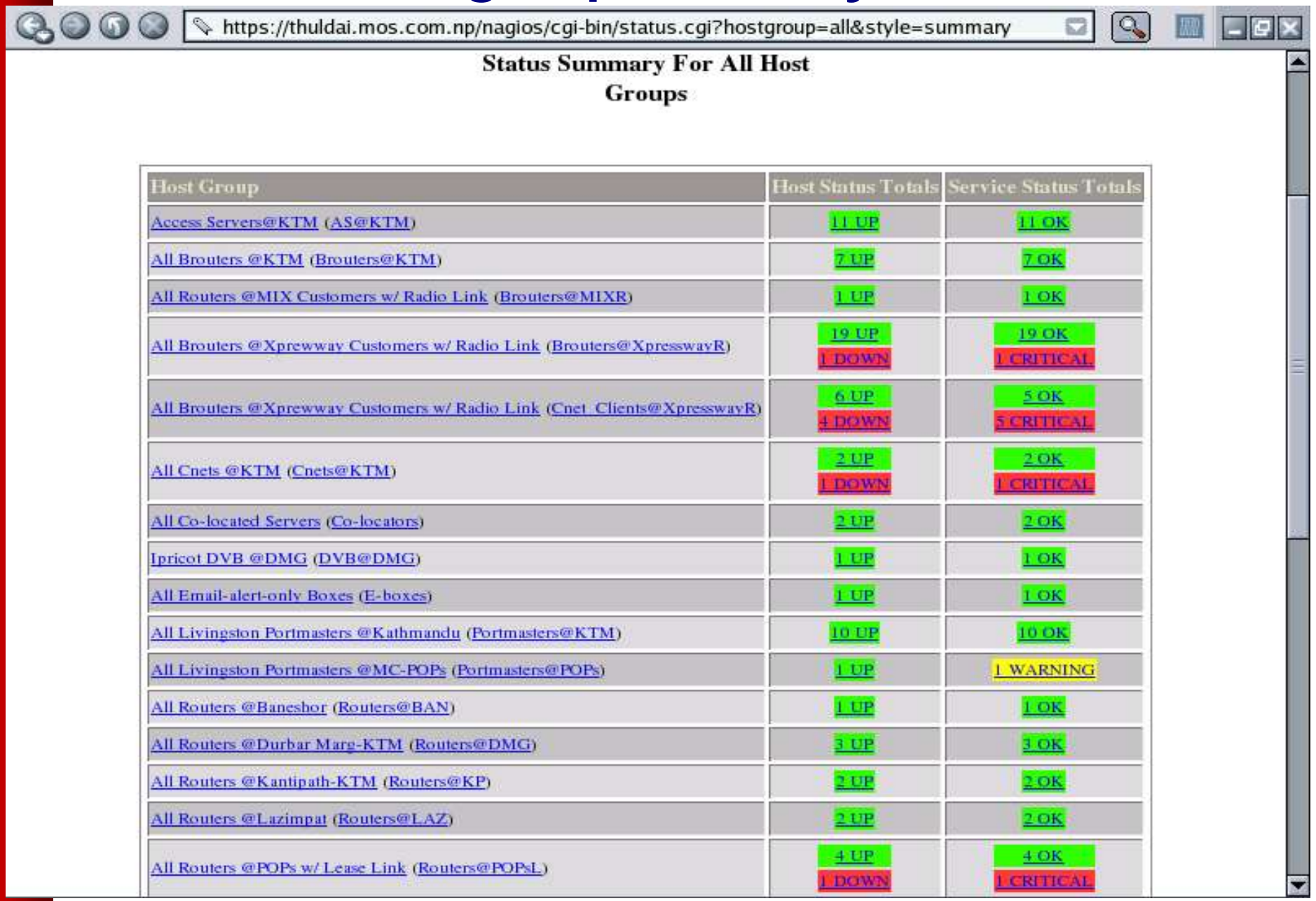


Windows_Servers
Unix_Servers
OpenBSD_Servers
Nagios Process
Dmg-cat-255
Dmg-cat-251-255
Dmg-cat-251
Dmg-3640
SXC-LEASE
Dmg-rt2
Dvb
CHINESE-EMBASSY-LEASE
Brj-pm1
WORLDBANK-R
Sdr-2924
Gw-7206
Sdr-5300
Laz-nxl-link1
Nxl-5300
Laz-rt1
HOTEL-RADISSON
Laz-sw1
Laz-br
Sdr-rt1
Nxl-5300-link2
Ktp-cat-251
Ktp-rt1
Ktp-ban-br
Sdr-5300-link4
Ban-ktp-br
Ban-cat
HOTEL-EVEREST
Ban-cnet
CYBER-KITCHEN
Ptn-5300
Ptn-5300-link2
Ptn-rt1
Pul-2610
PLAN-RADIO
Pul-ptn-link1
Pul-sw1
HIMALMEDIA
Pul-br
Pul-rt2
SXC-RADIO
UNICEF-JAW
Laz-cnet
XVA

Hostgroup status



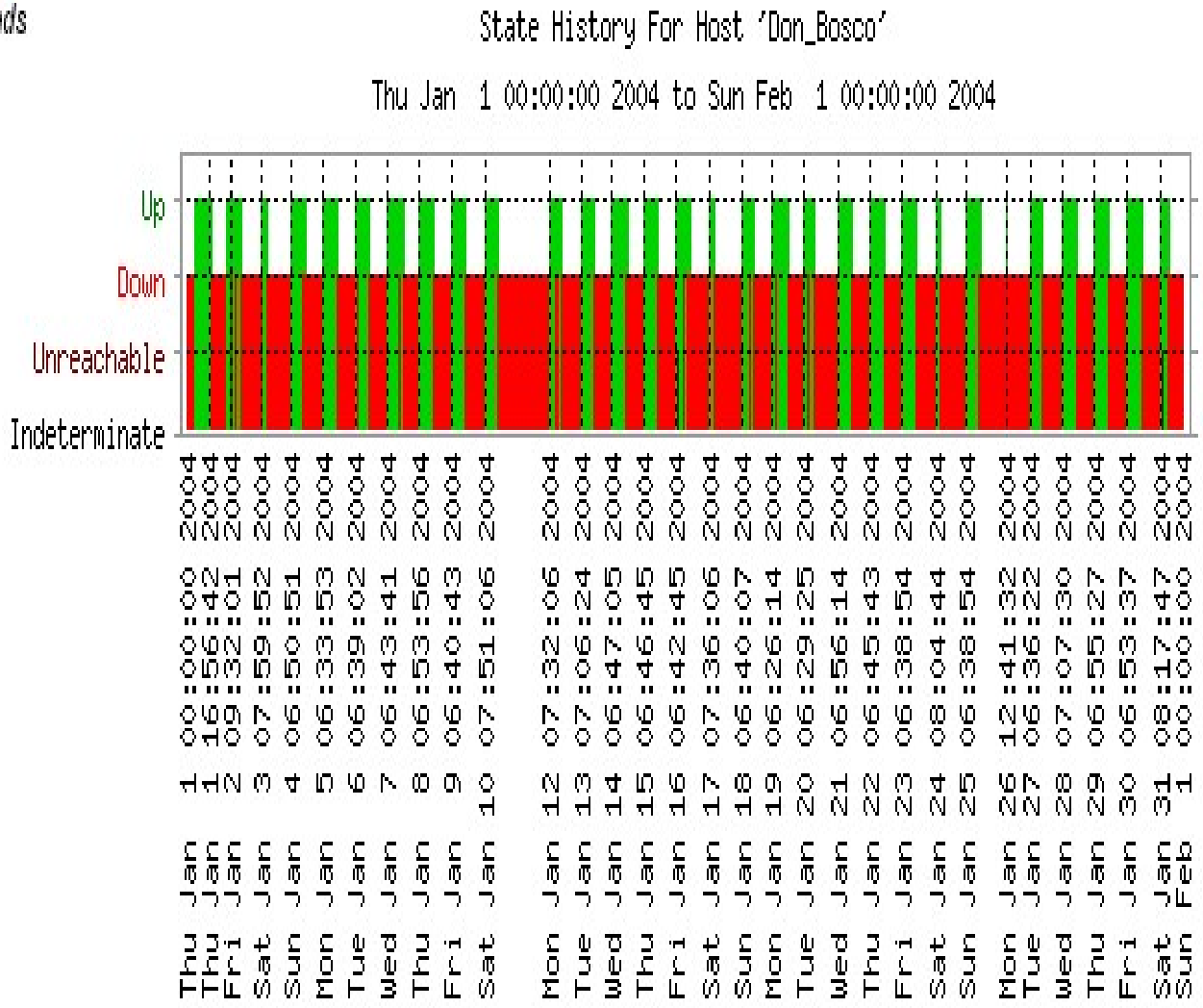
Hostgroup summary



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

Hisrotical trends

Trends



State Breakdowns:

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

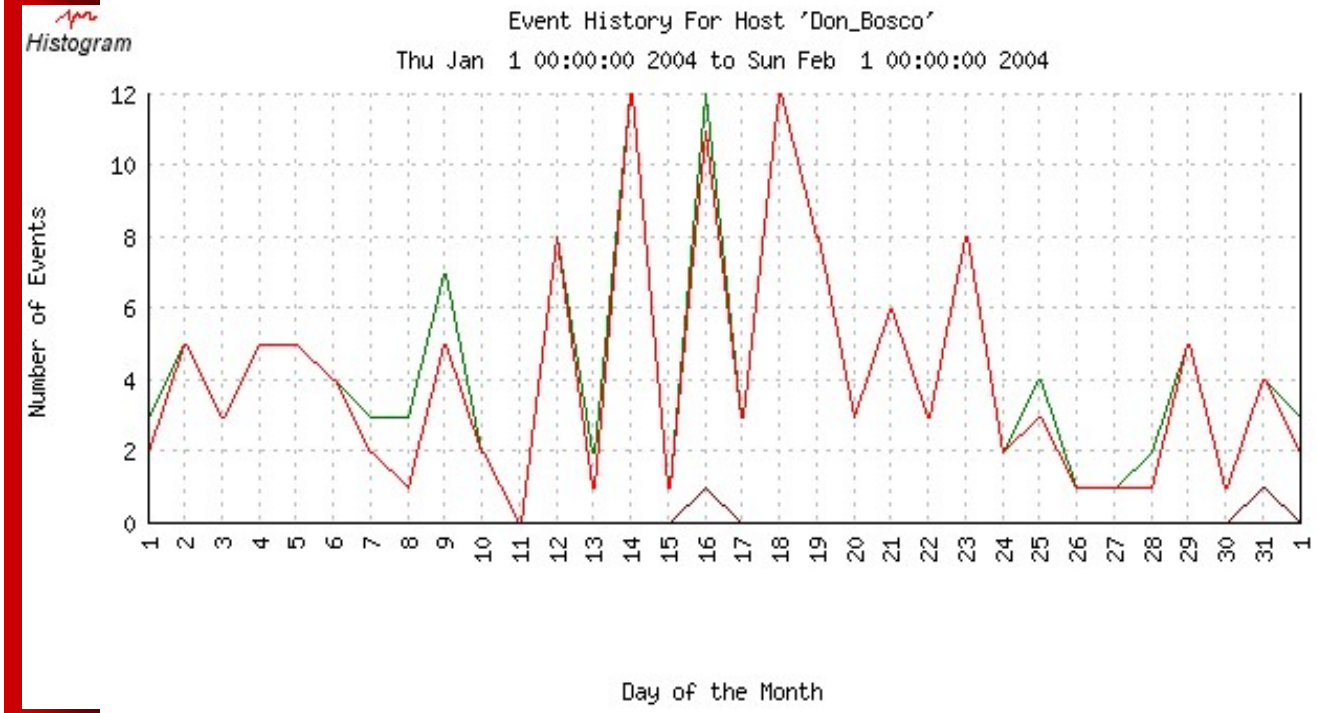
Down : (67.1%) 20d 19h 17m 27s

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

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

Alert histogram

Histogram



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..

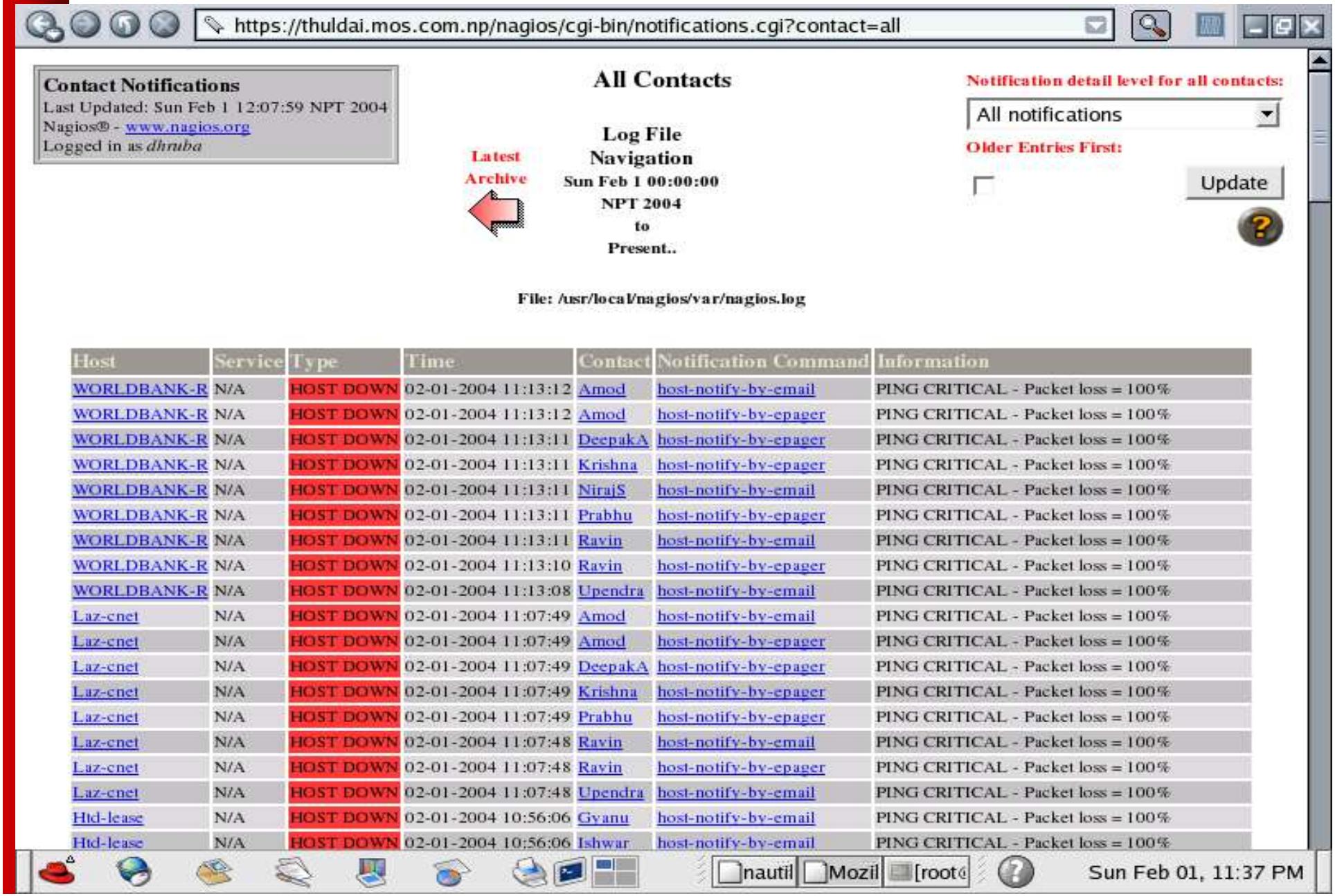
Older Entries First:
Update

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

Notification logs



Questions ?