Availability Management
Nagios overview

Agenda

Nagios®

- **Introduction**
  - Objectives
  - Functionalities
  - Requirement.

- **Architecture & Operation**
  - Operation Description
  - WEB portal

- **Plugins and extensions**
  - Plugins description
  - Useful extensions
  - Extension example

INTRODUCTION

Objectives: Availability Management

Nagios®

- Availability Management is a process of the Service Delivery (ITIL specifications). Its goal is to ensure that the required level of Availability is provided. The measurement and monitoring of IT Availability is a key activity to ensure Availability levels are being met consistently. Availability Management should look continuously to optimise the Availability of the IT Infrastructure, services and supporting organisation.

- In a Network Management environment, monitoring services needed are for example:
  - Routers status
  - Routers environment (CPU, Memory, Temperature…)
  - Links status (interconnexion, access)
  - Links health (traffic evolution, errors level, instability…)
  - Routing protocol status (BGP, MPLS…)
  - …

- The functionalities needed are:
  - Extended monitoring capabilities, including custom programs for non-standard elements
  - Powerful analysis and notification when an incident is detected
  - Easy to use configuration interface
  - Friendly GUI for service status display

CS
COMMUNICATION
& SYSTEMES

Nagios functionalities

- Nagios® is an open source tool specially developed to monitor host and service and designed to inform you of network incidents before your clients, end-users or managers do. It has been designed to run under the Linux operating system, but works fine under most *NIX variants as well

- Initially developed for servers and application monitoring, it is now widely used to monitor networks availability. It is possible with the development of specific plugins around Nagios process.

- Nagios works with a set of "plugins" to provide local and remote service status. The monitoring daemon runs intermittent checks on hosts and services you specify using external "plugins" which return status information to Nagios.

- When incidents are detected, the daemon 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.

- Custom "plugins" are relatively easy to develop

- Different methods are provided for remote resource discovery

- Nagios is freely available from http://www.nagios.org

Nagios functionalities

Nagios

- Nagios tool provide monitoring facilities (polling elements at regular intervals and generating events depending on polling return status. Nagios can be considered as a scheduler, which execute plugins, analyse results and obtain a status about each element concerned.

- Nagios can be configured to monitor anything that you can write a script for (Perl scripts, Shell, C programs, …).

- Nagios comes with loads of plugins for just about every normal known service such as SNMP, DNS, SSH, HTTP, NFS, FTP, etc, etc.

- The advantages of Nagios against other manufacturer products are:
  - It is a free product, running on Linux OS
  - It is an easy to use product, including all functions needed to perform availability monitoring
  - Extensions (plugins) are simple to develop, using well known languages
  - It is scalable, and it is possible to deploy a hierarchy of Nagios servers to provide consolidated views of network and / or system availability (Hypervisor)

- The platform shall nevertheless be integrated in an operational environment with all its constraints:
  - Automatic or semi-automatic configuration of multiple services and instances
  - Attractive GUI for incidents identification, reporting, and relation with Incident Management process
  - Operators alarm (visual, audio or through pager for on-call FTE)

COMMUNICATION & SYSTEMES

Requirements

- **Other things you will need to get Nagios working are:**
  - Nagios Plugins (from Nagios download URL)
  - GD – Graphics Libraries
  - JPEG Lib Sources
  - PNG Lib Sources
  - FPing (Fast Ping), this is optional but useful.
  - For SNMP monitoring you will need:
    - net-snmp-tools, and
    - net-snmp-utils

- **MySQL database for storing:**
  - Elements status logs

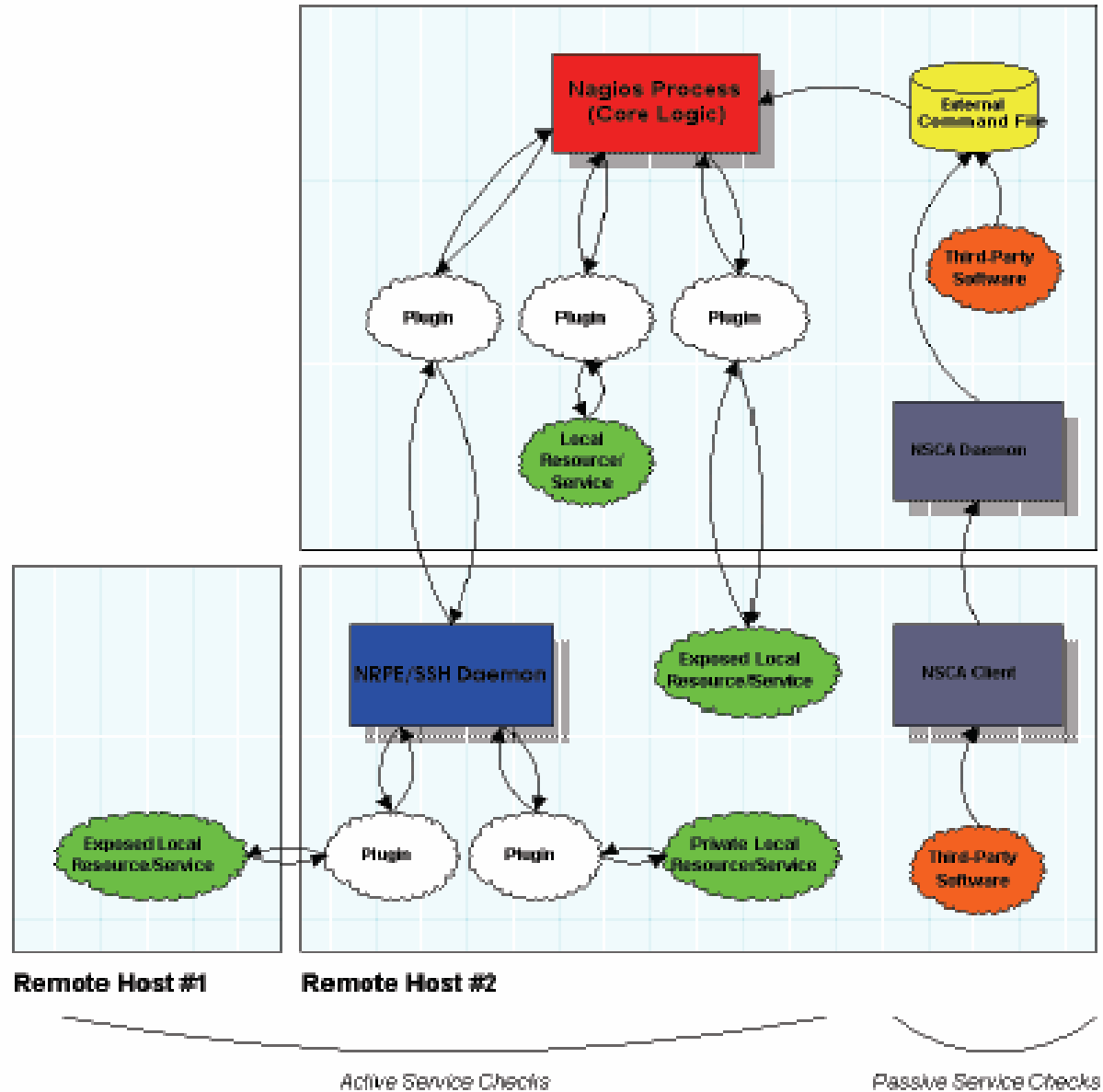# ARCHITECTURE
&
OPERATION

Architecture

- Nagios is built on a server/agents architecture.
  Usually, on a network, a Nagios server is running on a host, and plugins are running on all the remote hosts that need to be monitored. These plugins send information to the server, which displays them in a GUI.

- Nagios is composed of three parts:

  - A scheduler: this is the server part of Nagios.
    At regular interval, the scheduler checks the plugins, and according to their results do some actions.

  - A GUI: the interface of Nagios (with the configuration, the alerts, ...). It is displayed in web pages generated by CGI.
    It can be state buttons (green,OK/red,Error), sounds, MRTG graphs, ...

  - The plugins. They are configurable by the user. They check a service and return a result to the Nagios server.

- A soft alert is raised when a plugin returns a warning or an error.
  Then on the GUI, a green button turns to red, and a sound is emitted.
  When this soft alert is raised many times (the number is configurable), a hard alert is raised, and the Nagios server sends notifications: email, SMS, ...

Nagios Architecture (internal)
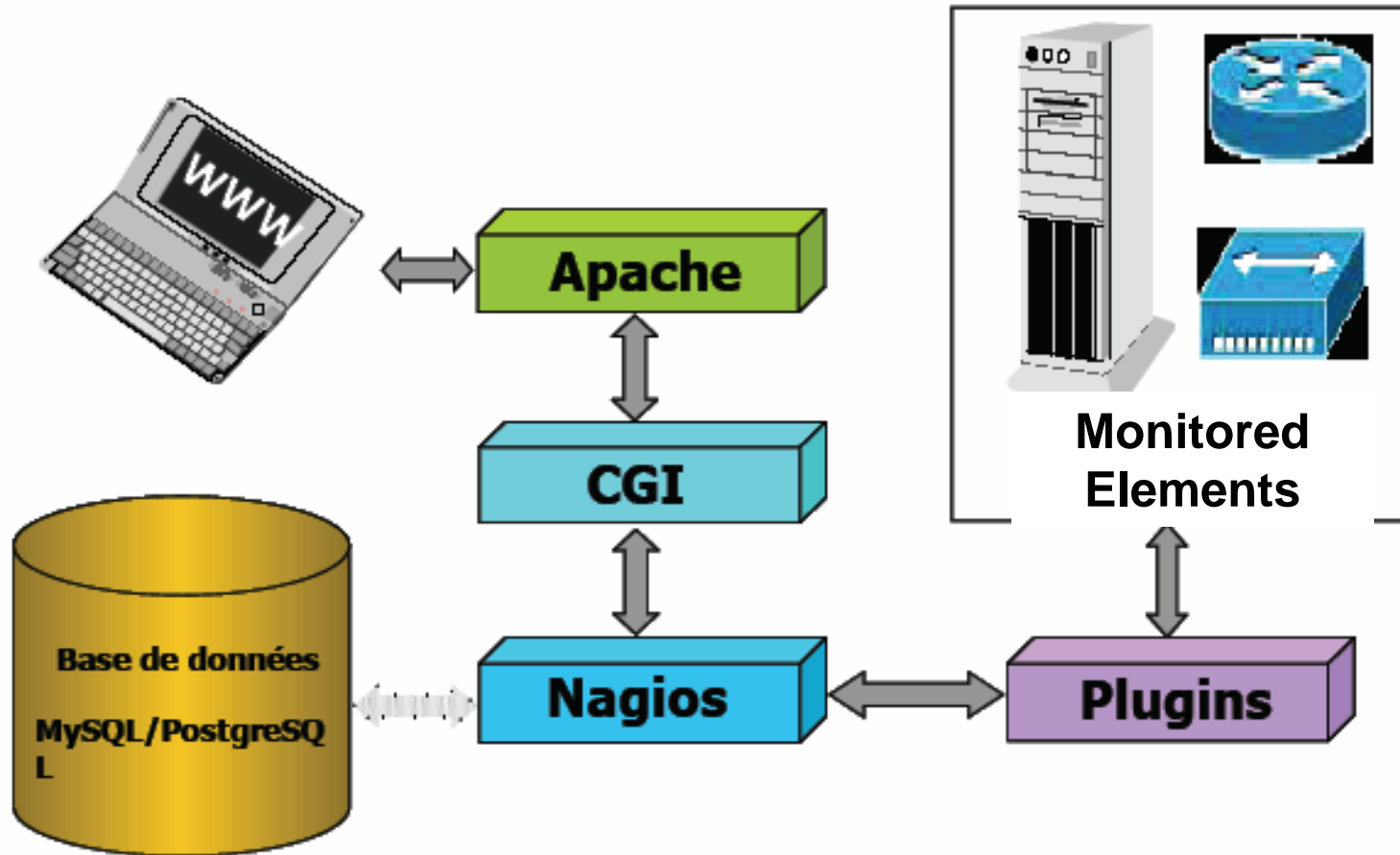
Nagios

Nagios architecture (external)

- **Local host**
  - Nagios process
  - Plugins
  - NCSA daemon

- **Remote host**
  - NCSA client
  - NRPE/SSH daemon
  - Plugins

Web Interface: tactical overview

Web Interface: services overview

Web Interface: services status detail

Web Interface: services status detail

Web Interface: services status detail

NAGIOS

Web Interface: services status detail

Web Interface: 3D status map
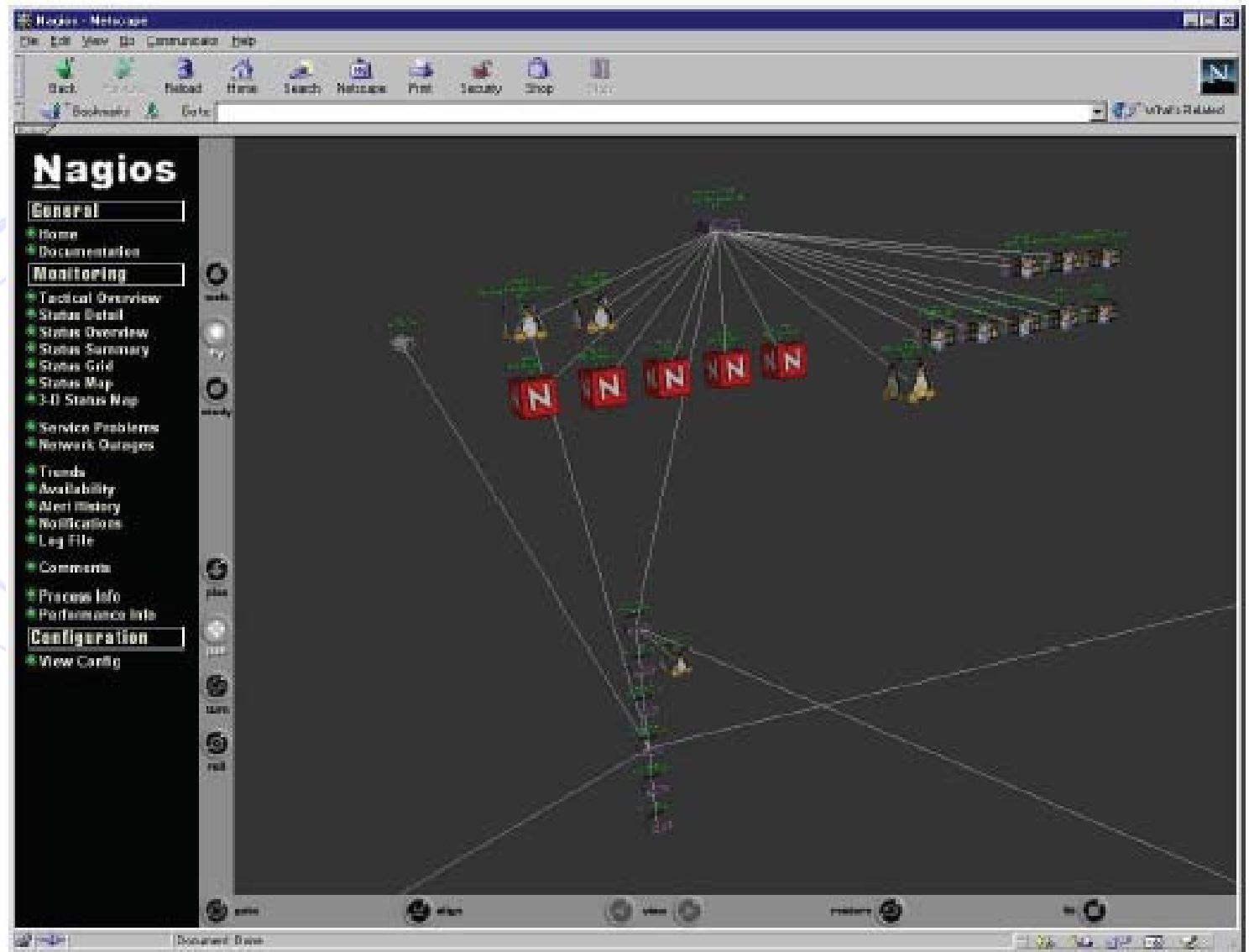
Configuration Files

Nagios®

- **nagios.cfg**
  - Main configuration file
  - Monitored elements configuration

- **resource.cfg**
  - User defined elements configuration file

- **cgi.cfg**
  - Display options for CGI

- **host, hostgroup and hostextinfo**
  - Information concerning monitored equipments

- **service, servicextinfo**
  - Information concerning monitored services

- **host and service dependency**
  - Dependencies between hosts and between services

- **host escalation, host group escalation, service escalation**
  - Escalation notification

Configuration Files

- **contact**
  - Nagios users. To access Nagios interface, it is necessary to be registered in this contact file

- **contactgroup**
  - User Groups. Notifications and display rights are settled in this file

- **timeperiod**
  - Use to configure period of time for elements monitoring and users notifications.

- **command**
  - Set of commands used to control services, equipments, events management and notifications

Sample configuration files

```
Hosts.cfg :
=========
define host{

        notifications_enabled          1 ; Host notifications are enabled
        event_handler_enabled          1 ; Host event handler is enabled
        flap_detection_enabled         1 ; Flap detection is enabled
        process_perf_data              1 ; Process performance data
        retain_status_information      1 ; Retain status information
across
program restarts
        retain_nonstatus_information   1 ; Retain non-status information
across program restarts
```
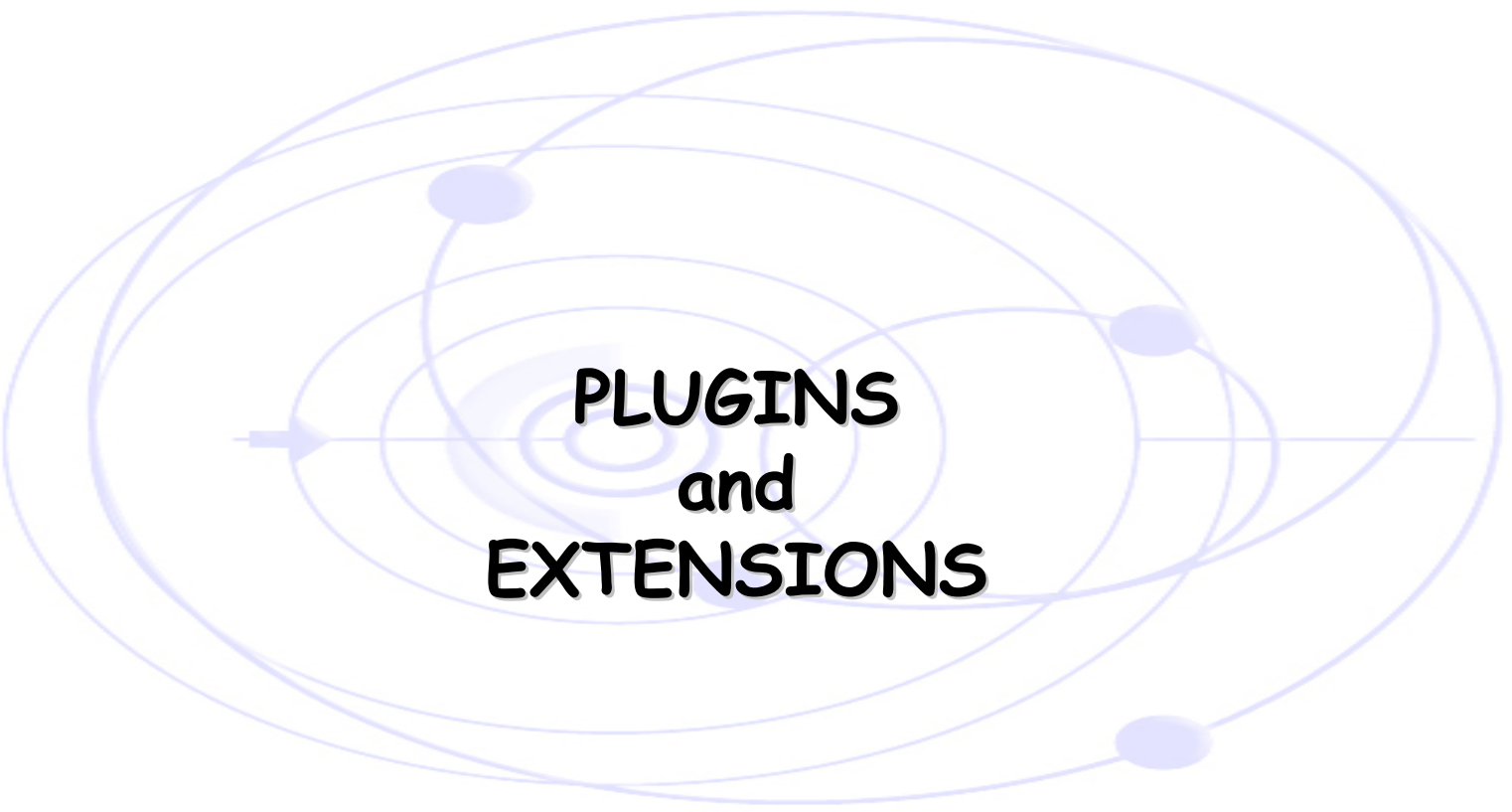
```
                        # 'novell1' host definition
                        define host{
                                use                 generic-host  ; Name of host template to
                        use

                                host_name           novell1
                                alias               Novell Server #1
                                address             192.168.1.2
                                check_command       check-host-alive
                                max_check_attempts  10
                                notification_interval  120
                                notification_period  24x7
                                notification_options  d,u,r
                                }
```

PLUGINS
and
EXTENSIONS

Plugins and Extensions

- Developments on Nagios can be found at http://www.nagiosexchange.org/

- AddOn projects are freely available. They cover subjects on:
  - Charts,
  - Communications,
  - Configuration,
  - Development,
  - DownTimes,
  - FrontEnds,
  - Notificatons,
  - Misc

- Plugins have been developed on:
  - Networking,
  - SNMP,
  - Hardware,
  - Linux,
  - Solaris,
  - Windows, …

PLUGINS

Nagios®

- A plugin is a small program (in Perl, C, java, python, ...) that checks a service (a daemon, some free space on a disk, ...). It must return a value and a small line of text (Nagios will only grab the first line of text).

  Output should be in the format: *METRIC STATUS: information text/performance data*
  The allowed METRIC STATUS are 0 (OK), 1 (WARNING), 2 (CRITICAL) or 3 (UNKNOWN)

- The warning and critical **thresholds** are parameters, set by the user, passed as arguments to the plugin.

- A plugin can also return **performance data** in the format: "label1=value1 label2=value2 ..." These data are stored by Nagios and may be later displayed with **MRTG** (**http://people.ee.ethz.ch/~oetiker/webtools/mrtg/**)

- The plugins can be run:
  - **Locally**, on the Nagios server.
    But such a plugin can check remote hosts, for example *check_ping* which pings remote hosts to check if they are running.
  - **Remotely**, through a remote Nagios server, with ssh, with snmp, with NRPE (Nagios Remote Plugin Executor), or with NSCA (Nagios Service Check Acceptor).
    It means that the plugin either waits for a verification request from the Nagios server before sending its result, or executes itself and sends the result to the Nagios server.

CS
COMMUNICATION
& SYSTEMES

Sample Plugin: Check_Cisco-Ping (beginning)

Nagios

```perl
#!/usr/bin/perl

# check_cisco_command - telnet's to a Cisco router to run a command

# License Information:
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#




use strict;

use Getopt::Long;

use vars qw($opt_d $opt_u $opt_p $opt_P $opt_h $opt_H $opt_V $opt_v
        $debug $username $password $hostname $state $error $PROGNAME
        @command_output $session $command $opt_r $tmp_var_loss
$tmp_var_latency
        $opt_c $opt_w $info $answer $opt_m $metric $warning_rta $warning_pl
        $timeout $router $critical_rta $critical_pl $opt_t $vrf $stats);
use lib  "utils.pm";
use utils qw(%ERRORS &print_revision &support &usage );

use Net::Telnet::Cisco;

sub print_help ();
sub print_usage ();

$ENV{'PATH'}='';
$ENV{'BASH_ENV'}='';
$ENV{'ENV'}='';
```

CS
COMMUNICATION
& SYSTEMES

Other useful developments

- **Alarm resiliency**
    - Nagios gives an immediate status of the monitored elements, it has no memory (except in log). It is useful to keep trace of an incident until it has been checked and acknowledged by an operator.

- **Network Interfaces discovery**
    - Within big networks, it is useful to « compare » real configuration with database configuration. An external program can check every day (auto-discovery) the real network configuration versus Nagios database.
    - If differences appears, notify network administrator of the change.

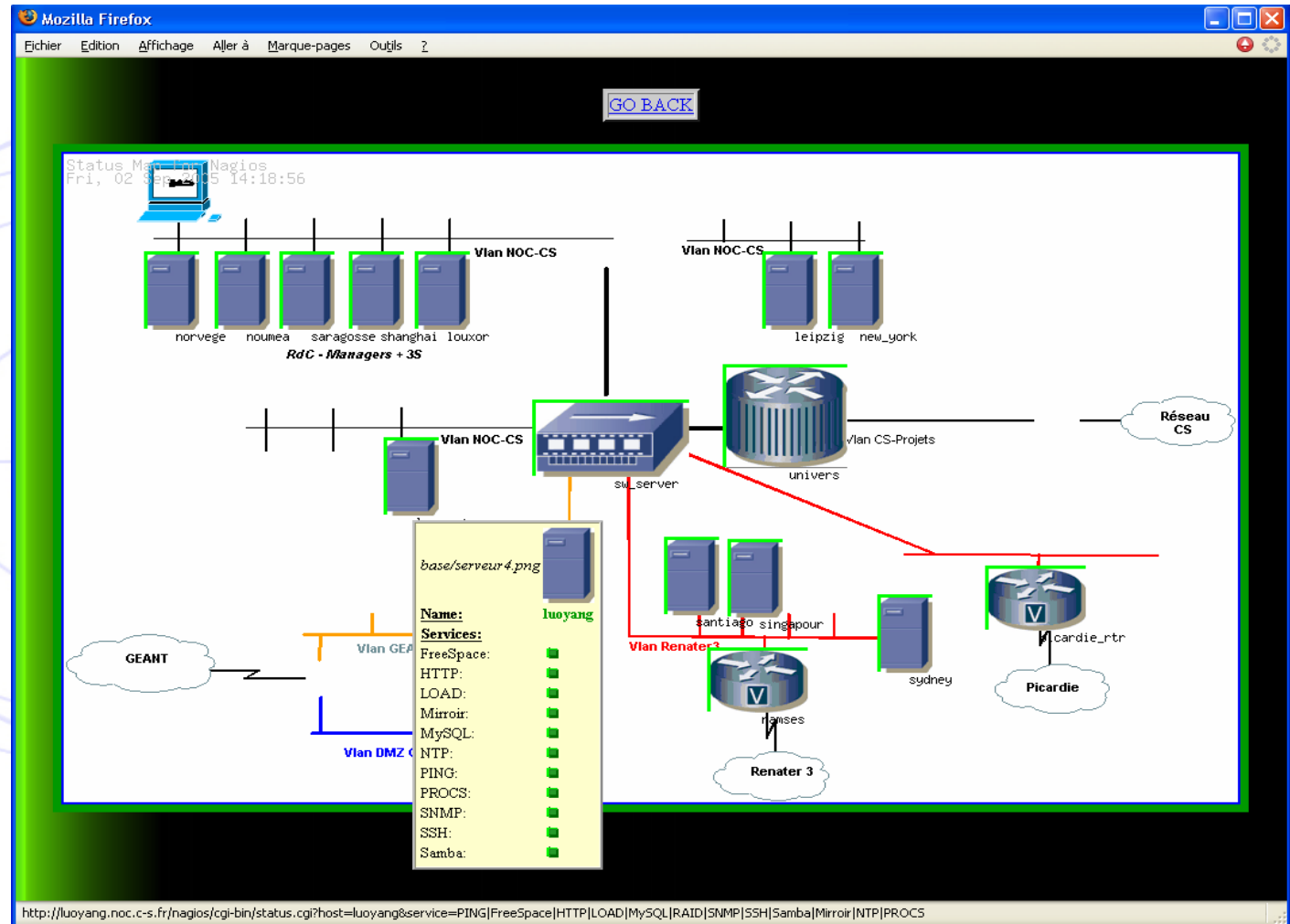- **Semi-automatic configuration**
    - For each new element, multiple identified checking have to be configured and started
    - Semi-automatic configuration tool will write Nagios configuration files based on higher level network description files

Networks and Equipments

Nagios

Extension Example

SNMP Traps (UDP Port 162)

SNMP Poll (UDP Port 161)

SNMP Poll (UDP Port 161) SSH Access (TCP Port 22)

./bin/traps-dispatch.pl

./bin/net-getif.pl

./var/history

Text file interfaces history interface_DATE

./libexec/check_****
./libexec_noc/check_****.pl

Email notification (not used)

./var/spool/

Text file logfile.odd logfile.even

./var/

Text file interfaces.dat interfaces.monitor

./bin/traps-rotate.pl

On-call FTE

MySQL events base

./bin/nagios

nagios process

Interfaces-form.cgi

./bin/nagios-oncall.pl

alarms-form.cgi

./bin/traps-compute.pl

./var/

Text file avail_cache.htm current_alarm.gen

./etc/

Text file Nagios configuration process nagios.cfg

compute-form.cgi

Monthly report: Circuits availability

./bin/nagios-configmaker.pl

./nagios/

Text file Nagios format nagios.gen

log-form.cgi

./config/

Text file Extensions configuration netadmin.cfg

./logs/

Log files netadmin.log netadmin.log.1.gz

./config/

Services file configuration Full_network Workstations

COMMUNICATION & SYSTEMES

> Consult

> Configure

> Use

> Produce

Program   **Daemon**   **Crontab Job**   > **Execute**

Extensions

BBMAP interfacing Nagios

NAGIOS

- **BBMAP
  (Big Brother MAP)**

  - BBMAP gives a graphical view of Nagios elements.

  - Elements on the map are "clickable" and give access to underlying status details

  - It is easier to modify than Nagios maps (2D and 3)

  - It is logically separated from Nagios (security enhancement):
    -Nagios is for administrator
    -BBMAP is for users

BBMAP interfacing Nagios and WheatherMap

Cacti and BBMAP consolidation

Cacti / BBMAP

NOC

User in its office

Cacti / Nagios / MySQL server

ISP ADSL

User at home
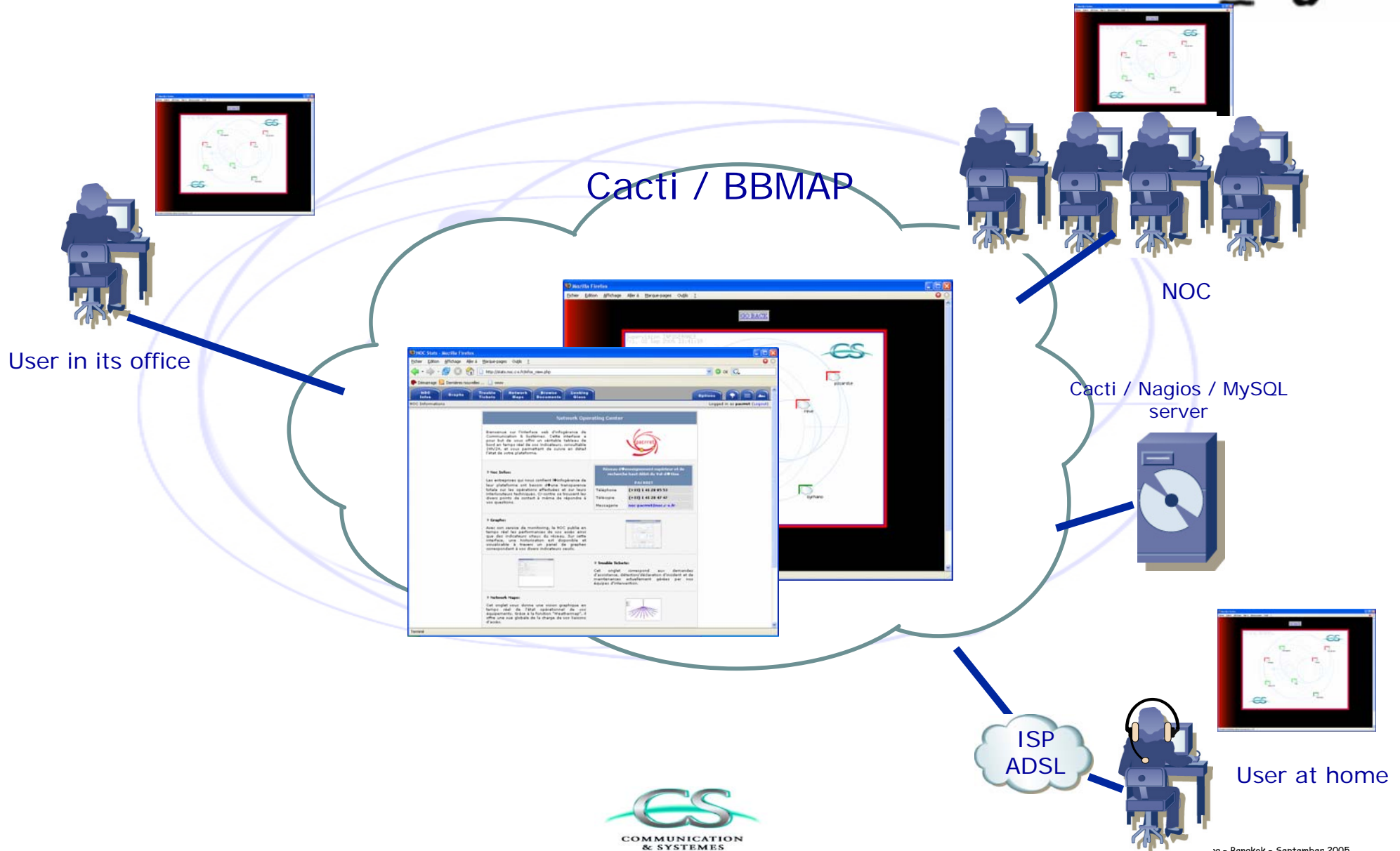
References

- **Nagios source program**
  - http://www.nagios.org/download/

- **Nagios Extra developments**
  - http://www.nagiosexchange.org/

- **Official plugins**
  - http://nagiosplug.sourceforge.net/

- **Conferences**
  - http://www.nagios.org/propaganda/conferences/

THE END

Thank you for your attention