ABCs of Network Monitoring
Automated Intelligence

GZ Kabir
BDCOM ONLINE LTD.
Network Monitoring
- Perspectives
- Components
- Tools
- Demonstration
Big picture – First View

How it all fits together

- Change control & monitoring
- Improvements
- Upgrades

- Monitoring
  - Data collection
  - Accounting

- NOC Tools
  - Ticket system

- Capacity planning
  - Availability (SLAs)
  - Trends
  - Detect problems

- User complaints
  - Requests

Fix problems

Notifications

Ticket

Ticket

Ticket

Ticket
- **Operation:**
  keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

- **Administration:**
  deals with keeping track of resources in the network and how they are assigned.

- **Maintenance:**
  concerned with performing repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run "better".

- **Provisioning:**
  is concerned with configuring resources in the network to support a given service.
Network Management is the use of a system that constantly monitors a computer network for slow or failing systems and that notifies the network administrator in case of outages via email, SMS or other alert Mechanisms.

subset of the functions involved in network management.
☐ System & Service monitoring
  ■ Reachability, availability
☐ Resource measurement/monitoring
  ■ Capacity planning, availability
☐ Performance monitoring (RTT, throughput)
☐ Stats & Accounting/Metering
☐ Fault Management
  ■ Fault detection, troubleshooting, and tracking
☐ Configuration/Change Management
☐ Coordination
☐ & So on ...
- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- Network Forensic
- Intrusion Detection ...
- ....
- ..... 
- Coordination
- **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools

- **Monitoring tools** – tools running in the background ("daemons" or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.

- **Performance tools** – tell us how our network is handling traffic flow.
Tools

- **Active tools**
  - Ping – test connectivity to a host
  - Traceroute – show path to a host
  - MTR – combination of ping + traceroute
  - SNMP collectors (polling)

- **Passive tools**
  - log monitoring, SNMP trap receivers

- **Automated tools**
  - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
  - MRTG – record and graph bandwidth usage on a switch port or network link, at regular intervals
  - So MANY More .....
Log, Log, Log ....
- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- Network Forensic
- Intrusion Detection ...
- ....
- ..... 
- Coordination
Tools ... Availability

- Nagios
  - server and service availability monitoring
  - Can monitor pretty much anything
  - HTTP, SMTP, DNS, Disk space, CPU usage, ...
  - BGP, OSPF, Switch Port, room temperature, ..
  - Easy to write new plugins (extensions)

- Zabbix, ZenOSS, Hyperic, ... Many more Open Source...

- Logging capability
- Notification mechanism
Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes.

- A key measurement tool for actively monitoring availability of devices and services.
- Possibly 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.
- Checks services
- If the service is down, checks the host
- If the host is down, checks its parent
- Find the highest-level thing that's down
- Retest it a few times (e.g. 5 or 10 times)
- If it stays down:
  - Figure out who to notify
  - Send them a message
  - Keep notifying them until it comes back up
- It nags us!
Advantages of Nagios

- Small, relatively easy to understand
- Lightweight and fast
- Easy to extend (write new plugins)
- Large library of agent-less monitoring plugins
- Agents for Windows and most Unixes
- Free and open source
Nagios Exchange

- Addons (537)
- Certified Compatible (3)
- Comparisons (8)
- Cool Stuff (6)
- Demos (3)
- Distributions (18)
- Documentation (123)
- Graphics and Logos (35)
- Media Coverage (5)
- Multimedia (104)
- Patches (20)
- Plugins (2593)
- Seedcamp (14)
- Translations (9)
- Tutorials (299)
- Uncategorized (0)
- Utilities (14)
<table>
<thead>
<tr>
<th>Tools .... Nagios</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nagios</strong></td>
</tr>
</tbody>
</table>

### Corporate Client (Corporate Client)

<table>
<thead>
<tr>
<th>Host</th>
<th>Status</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITDG</td>
<td>UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>berger</td>
<td>UP</td>
<td>1 OK</td>
</tr>
</tbody>
</table>

### Cisco-Mikrotik (Router)

<table>
<thead>
<tr>
<th>Host</th>
<th>Status</th>
<th>Services</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>b6ix</td>
<td>UP</td>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>bttb_main</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>coredrouter</td>
<td>UP</td>
<td>3 OK</td>
<td></td>
</tr>
<tr>
<td>coredrouter_smile</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>glaw</td>
<td>UP</td>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>glawg_router</td>
<td>UP</td>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>motihealgw_router</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>sylhet_router</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
</tbody>
</table>

### Linux Servers (linux-servers)

<table>
<thead>
<tr>
<th>Host</th>
<th>Status</th>
<th>Services</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>bbgw10</td>
<td>UP</td>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>bbgw20</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>bbgw30</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>bdoom_maxim_billing</td>
<td>DOWN</td>
<td>1 CRITICAL</td>
<td></td>
</tr>
<tr>
<td>cta_dist</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>cligum</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>dns1</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>dns2</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>dns3</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>delayed</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>delayed2</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>gis</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>hardy</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>jptalkG2</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>UP</td>
<td>8 OK</td>
<td></td>
</tr>
<tr>
<td>mail.com</td>
<td>UP</td>
<td>4 OK</td>
<td>1 WARNING</td>
</tr>
<tr>
<td>mail.net</td>
<td>UP</td>
<td>5 OK</td>
<td></td>
</tr>
<tr>
<td>motiheal_distribution</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>pantha_dist</td>
<td>UP</td>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>shout_share</td>
<td>UP</td>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>smtp</td>
<td>UP</td>
<td>2 OK</td>
<td>1 CRITICAL</td>
</tr>
<tr>
<td>Service</td>
<td>Type</td>
<td>Status</td>
<td>Time</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>corerouter</td>
<td>BGP_MOG</td>
<td>critical</td>
<td>3m 21s</td>
</tr>
<tr>
<td>bttb_main</td>
<td>-</td>
<td>down</td>
<td>6m 19s</td>
</tr>
<tr>
<td>pantha_dist</td>
<td>SSH</td>
<td>critical</td>
<td>9m 19s</td>
</tr>
<tr>
<td>pantha_dist</td>
<td>PING</td>
<td>critical</td>
<td>9m 21s</td>
</tr>
<tr>
<td>panthagw_router</td>
<td>PING</td>
<td>critical</td>
<td>9m 21s</td>
</tr>
<tr>
<td>sipix_bdix</td>
<td>PING</td>
<td>critical</td>
<td>9m 22s</td>
</tr>
<tr>
<td>sipix_bdix</td>
<td>-</td>
<td>unreachable</td>
<td>9m 54s</td>
</tr>
<tr>
<td>pantha_dist</td>
<td>-</td>
<td>unreachable</td>
<td>9m 57s</td>
</tr>
<tr>
<td>panthagw_router</td>
<td>-</td>
<td>down</td>
<td>13m 48s</td>
</tr>
</tbody>
</table>
Text message

1:37 pm 02/09/10

From NMS Gateway

*BDCOM NMSGW *
Host: berger
State: DOWN
Address: 210.4.74.82
Date/Time: Thu Sept 213:36:53
BDT 2010
☐ Availability
☐ Reliability
☐ Performance
☐ Configuration Mgmt & Monitoring
☐ Network Forensic
☐ Intrusion Detection ...
☐ ....
☐ ..... 
☐ Coordination
Tools ... Reliability

SmokePing

- Keeps track of your network latency.
- Best of breed latency visualisation.
- Interactive graph explorer.
- Wide range of latency measurement plugins.
- Master/Slave System for distributed measurement.
- Highly configurable alerting system.
- Live Latency Charts with the most interesting graphs.

Free and OpenSource Software written in Perl.
### SmokeTrace:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Host</th>
<th>Ip</th>
<th>Loss [%]</th>
<th>Sent</th>
<th>Last [ms]</th>
<th>Avg [ms]</th>
<th>Best [ms]</th>
<th>Worst [ms]</th>
<th>StDev [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>r4.core init7.net</td>
<td>213.144.138.193</td>
<td>0</td>
<td>20</td>
<td>122.8</td>
<td>7.6</td>
<td>0.3</td>
<td>122.8</td>
<td>27.4</td>
</tr>
<tr>
<td>2.0</td>
<td>r12ur1.core init7.net</td>
<td>77.109.128.49</td>
<td>0</td>
<td>20</td>
<td>7.9</td>
<td>3.0</td>
<td>0.5</td>
<td>9.6</td>
<td>2.9</td>
</tr>
<tr>
<td>3.0</td>
<td>swiX1-10GE-1-2.switch.ch</td>
<td>194.242.34.53</td>
<td>0</td>
<td>20</td>
<td>1.7</td>
<td>1.2</td>
<td>0.7</td>
<td>1.8</td>
<td>0.3</td>
</tr>
<tr>
<td>4.0</td>
<td>swiZH2-10GE-1-3.switch.ch</td>
<td>130.59.36.130</td>
<td>0</td>
<td>20</td>
<td>1.1</td>
<td>1.2</td>
<td>0.9</td>
<td>1.6</td>
<td>0.2</td>
</tr>
<tr>
<td>5.0</td>
<td>swiEL2-G2-3.switch.ch</td>
<td>130.59.36.78</td>
<td>0</td>
<td>20</td>
<td>4.1</td>
<td>4.5</td>
<td>3.7</td>
<td>10.5</td>
<td>1.4</td>
</tr>
<tr>
<td>6.0</td>
<td>swiAM2-10GE-1-4.switch.ch</td>
<td>130.59.36.10</td>
<td>0</td>
<td>20</td>
<td>3.9</td>
<td>4.0</td>
<td>3.6</td>
<td>4.5</td>
<td>0.2</td>
</tr>
<tr>
<td>7.0</td>
<td>oreus.switch.ch</td>
<td>130.59.138.34</td>
<td>0</td>
<td>20</td>
<td>3.6</td>
<td>3.8</td>
<td>3.4</td>
<td>4.3</td>
<td>0.2</td>
</tr>
</tbody>
</table>

SmokeTrace is part of the SmokePing suite created by Tobi Oetiker, Copyright 2008.
Components

- Availability
- Reliability
- **Performance**
- Configuration Mgmt & Monitoring
- Network Forensic
- Intrusion Detection ...
- ....
- .....  
- Coordination
Cacti/MRTG

- A tool to monitor, store and present network and system/server statistics
- Designed around RRDTool with a special emphasis on the graphical interface
- Almost all of Cacti’s functionality can be configured via the Web.
- Uses RRDtool, PHP and stores data in MySQL
- Supports the use of SNMP and graphics with MRTG
- Authentication Scheme
- Large Network Deployment
WeatherMap

Weathermap is a network visualization tool to take data you already have and show you an overview of your network in your own customized map form/shape.
**KEY FEATURES:**

**Cacti integration:** Weathermap comes with a Cacti plugin, allowing you to integrate network maps into the Cacti web UI, and provide a view of those maps to your users using Cacti's access control system. You don't need Cacti to use it though.

**Editor:** Weathermap includes a web-based editor to allow you to quickly 'sketch out' your map. It doesn't support all the features of Weathermap, but it doesn't get in their way either. You can use the web editor and a text editor together on the same map.

**Maintained and updated:** Weathermap is still being developed! I use this software myself, and as a result, find new ways I'd like to be able to do things. That means that bugs do get fixed, and features do get added.
- Availability
- Reliability
- Performance
- **Configuration Mgmt & Monitoring**
- Network Forensic
- Intrusion Detection ...
- ....
- ..... 
- Coordination
The "Really Awesome New Cisco config Differ"

- **Rancid**

  Rancid is a configuration management tool that keeps track of changes in the configurations of any size network equipment (Cisco, HP, Juniper, Foundry, etc.). Works on routers and switches. Automates retrieval of the configurations and archives them as backup tool, audit tool, blame allocation.
The "Really Awesome New Cisco config Differ"

- Rancid

The data is stored in a VCS (Version Control System) which keeps

- Track changes in the equipment configuration
- Track changes in the hardware (S/N, modules)
- Track version changes in the OS (IOS, CatOS versions)
- Find out what your colleagues have done without telling you!
- Recover from accidental configuration errors.
Tools ... Rancid

```
from rancid@nmsgw.bdcom.com
subject all router config diffs
to rancid-all@nmsgw.bdcom.com

210.4.77.136 | 5 +++--
1 file changed, 3 insertions(+), 2 deletions(-)
Index: configs/210.4.77.136

retrieving revision 1.34
diff -U 4 -r1.34 210.4.77.136
@@ -19,13 +19,13 @@
 !BootFlash: BOOTLDR variable does not exist
 !BootFlash: Configuration register is 0x2101

 !Flash: nvram: Directory of nvram:/
- !Flash: nvram: 397 -rw- 7057 <no date> startup-config
+ !Flash: nvram: 397 -rw- 7048 <no date> startup-config
 !Flash: nvram: 398 ---- 27 <no date> private-config
 !Flash: nvram: 1 ---- 4 <no date> rf_cold_starts
 !Flash: nvram: 2 ---- 12 <no date> persistent-data

- !Flash: nvram: 413678 bytes total (404492 bytes free)
+ !Flash: nvram: 413070 bytes total (405401 bytes free)

 !Flash: bootflash: Directory of bootflash:/
 !Flash: bootflash: 61341696 bytes total (50709288 bytes free)
@@ -505,8 +505,8 @@
```
- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- **Network Forensic**
- Intrusion Detection ...
- ....
- .....
Network Flow Analysis Tool

- NetFlow (C),
- cflowd (F),
- FlowScan (F),
- Sniffer Pro (C),
- argus (F),
- i-Flow (C)
- NFSen (F)
**Network Flow Analysis Tool**

- **NFSen**
  - Display netflow data: Flows, Packets and Bytes using RRD (Round Robin Database).
  - Easily navigate through the netflow data.
  - Process the netflow data within the specified time span.
  - Create history as well as continuous profiles.
  - Set alerts, based on various conditions.
Tools for Network Traffic Monitoring

NFSen: Network Flow Sensor

Graphs showing traffic flow and packet rates over time for different protocols such as TCP, UDP, ICMP, and other.

Profile information:
- Type: live
- Max: unlimited
- Exp: never
- Start: Aug 26 2010 - 13:05 BDT
- End: Sep 02 2010 - 12:50 BDT
- start 2010-09-01-22-35
- end 2010-09-02-01-55

Traffic statistics for BTCL channel:
- Flows: 1.8 k/s, 712.1 k/s, 31.9 k/s, 1.4 k/s, 23.0 k/s, 9.1 k/s, 134.9 k/s, 142.7 k/s, 120.4 Mb/s, 74.0 Mb/s, 46.0 Mb/s, 88.7 kb/s, 255.1 kb/s
Profile: Bots

TCP

UDP

ICMP

other

Profileinfo:
Type: continuous
Max: 10.0 GB
Exp: never
Start: Nov 13 2011 - 21:45 UTC
End: Feb 22 2012 - 08:30 UTC

t_{start} 2012-02-21-08-30
t_{end} 2012-02-21-20-30

Packets

Flows

Select Time Window ▼
Display: 1 day ▼
## Netflow Processing

**Source:**  
FSD-Edge  
MUL-Edge  
LHR-Edge  
ISB-Edge  
edge1  
edge2  
All Sources

**Filter:**  
*ip 124.29.233.134 and port in [25 587]*

**Options:**

- **List Flows**  
- **Stat TopN**

- **Limit to:**
  - Flows
  - 100 Flows

- **Aggregate**
  - bi-directional
  - proto
  - srcPort
  - dstPort

- **Sort:**
  - start time of flows

- **Output:**
  - auto
  - /IPv6 long

---


**nfdump filter:**  
*ip 124.29.233.134 and port in [25 587]*

<table>
<thead>
<tr>
<th>Date</th>
<th>flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dest IP Addr:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-05-25 08:15:15.764</td>
<td>0.448 TCP</td>
<td>72.30.235.6:25</td>
<td>124.29.233.134:64185</td>
<td>4</td>
<td>336</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:15:20.051</td>
<td>1.792 TCP</td>
<td>65.54.188.72:25</td>
<td>124.29.233.134:41370</td>
<td>6</td>
<td>846</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:15:42.772</td>
<td>0.576 TCP</td>
<td>98.137.54.238:25</td>
<td>124.29.233.134:2612</td>
<td>4</td>
<td>336</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:09.582</td>
<td>0.512 TCP</td>
<td>98.139.175.225:25</td>
<td>124.29.233.134:3259</td>
<td>4</td>
<td>336</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:34.484</td>
<td>0.512 TCP</td>
<td>72.30.235.196:25</td>
<td>124.29.233.134:64618</td>
<td>5</td>
<td>382</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:34.770</td>
<td>0.704 TCP</td>
<td>67.195.103.233:25</td>
<td>124.29.233.134:53453</td>
<td>4</td>
<td>336</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:34.036</td>
<td>0.704 TCP</td>
<td>67.195.103.232:25</td>
<td>124.29.233.134:52872</td>
<td>4</td>
<td>336</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:43.251</td>
<td>1.728 TCP</td>
<td>65.54.188.110:25</td>
<td>124.29.233.134:1205</td>
<td>6</td>
<td>846</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-05-25 08:16:49.711</td>
<td>4.032 TCP</td>
<td>65.54.188.110:25</td>
<td>124.29.233.134:60700</td>
<td>6</td>
<td>846</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Netflow Processing

### Source: dst ip 124.29.233.134 and not port in [25 587]

<table>
<thead>
<tr>
<th>Filter:</th>
<th>Options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSD-Edge</td>
<td>List Flows</td>
</tr>
<tr>
<td>MUL-Edge</td>
<td>Stat TopN</td>
</tr>
<tr>
<td>LHR-Edge</td>
<td>Top: 100</td>
</tr>
<tr>
<td>ISB-Edge</td>
<td>Stat: SRC IP Address order by packets</td>
</tr>
<tr>
<td>edge1</td>
<td>Limit: 0 Packets</td>
</tr>
<tr>
<td>bx2</td>
<td>Output: / IPv6 long</td>
</tr>
</tbody>
</table>


dst ip 124.29.233.134 and not port in [25 587]

Top 100 Src IP Addr ordered by packets:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Src IP Addr</th>
<th>Flows(%)</th>
<th>Packets(%)</th>
<th>Bytes(%)</th>
<th>pps</th>
<th>bps</th>
<th>bpp</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-04-06 08:46:04.832</td>
<td>4306718.743</td>
<td>111( 0.0)</td>
<td>2.0 M(10.1)</td>
<td>206.6 M(1.5)</td>
<td>0</td>
<td>383</td>
<td>101</td>
</tr>
<tr>
<td>2012-04-05 15:23:38.154</td>
<td>4347402.570</td>
<td>173( 0.4)</td>
<td>1.1 M(5.6)</td>
<td>183.8 M(1.4)</td>
<td>0</td>
<td>338</td>
<td>163</td>
</tr>
<tr>
<td>2012-05-25 14:44:44.065</td>
<td>2104.026</td>
<td>152( 0.0)</td>
<td>80300( 4.0)</td>
<td>584.9 M(4.4)</td>
<td>381</td>
<td>2.2 M</td>
<td>728</td>
</tr>
<tr>
<td>2012-05-25 21:33:27.367</td>
<td>21471.432</td>
<td>125( 0.0)</td>
<td>768000( 3.8)</td>
<td>558.6 M(4.2)</td>
<td>35</td>
<td>208111</td>
<td>727</td>
</tr>
<tr>
<td>2012-05-25 08:49:08.975</td>
<td>51661.144</td>
<td>616( 0.2)</td>
<td>700000(3.5)</td>
<td>119.9 M(0.9)</td>
<td>13</td>
<td>18564</td>
<td>171</td>
</tr>
<tr>
<td>2012-02-06 01:03:29.837</td>
<td>4462283.850</td>
<td>204152.184</td>
<td>132956(31.2)</td>
<td>495230(2.4)</td>
<td>35.8 M(0.3)</td>
<td>0</td>
<td>64</td>
</tr>
<tr>
<td>2012-05-25 08:15:24.673</td>
<td>202058.079</td>
<td>314( 0.1)</td>
<td>427000( 2.1)</td>
<td>405.1 M(3.0)</td>
<td>2</td>
<td>16040</td>
<td>948</td>
</tr>
<tr>
<td>2012-04-07 21:32:03.616</td>
<td>4302129.401</td>
<td>65.49(2.1)</td>
<td>405922(2.0)</td>
<td>556.3 M(4.1)</td>
<td>0</td>
<td>1034</td>
<td>1370</td>
</tr>
<tr>
<td>2012-05-25 08:21:39.910</td>
<td>197910.247</td>
<td>287( 0.1)</td>
<td>383000(1.9)</td>
<td>358.5 M(2.7)</td>
<td>1</td>
<td>14490</td>
<td>935</td>
</tr>
<tr>
<td>2012-05-25 19:06:43.841</td>
<td>3311.300</td>
<td>50( 0.0)</td>
<td>357000(1.8)</td>
<td>266.4 M(2.0)</td>
<td>107</td>
<td>643633</td>
<td>746</td>
</tr>
<tr>
<td>2012-04-06 22:52:33.084</td>
<td>4298546.576</td>
<td>173176.251</td>
<td>35( 0.0)</td>
<td>343002(1.7)</td>
<td>58.2 M(0.4)</td>
<td>0</td>
<td>108</td>
</tr>
<tr>
<td>2012-05-25 16:09:56.934</td>
<td>56199.733</td>
<td>74125.127</td>
<td>97( 0.0)</td>
<td>302000(1.5)</td>
<td>88.4 M(0.7)</td>
<td>5</td>
<td>12580</td>
</tr>
<tr>
<td>2012-04-05 20:05:07.638</td>
<td>4480185.409</td>
<td>74125.236</td>
<td>23881( 6.0)</td>
<td>300381(1.5)</td>
<td>234.2 M(1.7)</td>
<td>0</td>
<td>418</td>
</tr>
<tr>
<td>2012-04-06 04:14:27.276</td>
<td>4550825.770</td>
<td>74125.236</td>
<td>23607( 5.9)</td>
<td>250647(1.2)</td>
<td>164.6 M(1.2)</td>
<td>0</td>
<td>295</td>
</tr>
<tr>
<td>2012-04-06 09:11:20.075</td>
<td>4297422.238</td>
<td>78138.127</td>
<td>27( 0.0)</td>
<td>242260(1.2)</td>
<td>363.3 M(2.7)</td>
<td>0</td>
<td>676</td>
</tr>
<tr>
<td>2012-05-25 08:15:10.449</td>
<td>202737.626</td>
<td>77120.104</td>
<td>227( 0.1)</td>
<td>227000( 1.1)</td>
<td>23.6 M(0.2)</td>
<td>1</td>
<td>932</td>
</tr>
<tr>
<td>2012-04-06 03:54:28.955</td>
<td>4302710.803</td>
<td>3896148.98</td>
<td>55( 0.0)</td>
<td>225780(1.1)</td>
<td>243.6 M(1.8)</td>
<td>0</td>
<td>452</td>
</tr>
<tr>
<td>2012-04-05 20:07:05.648</td>
<td>4298665.103</td>
<td>686418.29</td>
<td>32( 0.0)</td>
<td>223989(1.1)</td>
<td>75.6 M(0.6)</td>
<td>0</td>
<td>140</td>
</tr>
<tr>
<td>2012-05-25 08:39:57.211</td>
<td>199856.286</td>
<td>193169.178</td>
<td>223( 0.1)</td>
<td>223000( 1.1)</td>
<td>22.5 M(0.2)</td>
<td>1</td>
<td>901</td>
</tr>
</tbody>
</table>
Tools... NFSen (Port Tracker)
<table>
<thead>
<tr>
<th>Rank</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
<th>Port</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>80</td>
<td>39029</td>
<td>80</td>
<td>570630</td>
<td>80</td>
<td>111021671</td>
<td>53</td>
<td>116671</td>
<td>53</td>
<td>150335</td>
<td>12610</td>
<td>142186426</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>445</td>
<td>27833</td>
<td>25</td>
<td>83140</td>
<td>40936</td>
<td>88004359</td>
<td>6881</td>
<td>2388</td>
<td>12610</td>
<td>99433</td>
<td>28712</td>
<td>101344390</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>135</td>
<td>24572</td>
<td>40936</td>
<td>66203</td>
<td>25</td>
<td>52612168</td>
<td>39792</td>
<td>2276</td>
<td>28712</td>
<td>70901</td>
<td>40493</td>
<td>93146942</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>25</td>
<td>7881</td>
<td>445</td>
<td>53175</td>
<td>55893</td>
<td>43525223</td>
<td>15507</td>
<td>1904</td>
<td>40493</td>
<td>65155</td>
<td>46886</td>
<td>27824516</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>23</td>
<td>6761</td>
<td>135</td>
<td>49066</td>
<td>46395</td>
<td>39079355</td>
<td>43040</td>
<td>1611</td>
<td>15699</td>
<td>46682</td>
<td>57563</td>
<td>26436088</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3128</td>
<td>4786</td>
<td>55893</td>
<td>37615</td>
<td>2889</td>
<td>30261886</td>
<td>60928</td>
<td>1588</td>
<td>1416</td>
<td>40540</td>
<td>62390</td>
<td>25767022</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>443</td>
<td>2999</td>
<td>46395</td>
<td>35068</td>
<td>1317</td>
<td>24692504</td>
<td>51012</td>
<td>1573</td>
<td>57563</td>
<td>37794</td>
<td>54505</td>
<td>25550351</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>2517</td>
<td>22</td>
<td>27489</td>
<td>49674</td>
<td>23472247</td>
<td>61295</td>
<td>1447</td>
<td>34018</td>
<td>37747</td>
<td>55893</td>
<td>23548341</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9415</td>
<td>1275</td>
<td>443</td>
<td>26468</td>
<td>54311</td>
<td>23342821</td>
<td>5060</td>
<td>1309</td>
<td>21694</td>
<td>24942</td>
<td>40633</td>
<td>22940400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>8080</td>
<td>1081</td>
<td>21651</td>
<td>25614</td>
<td>44879</td>
<td>23306526</td>
<td>49665</td>
<td>1225</td>
<td>46886</td>
<td>19468</td>
<td>40403</td>
<td>19544859</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- Network Forensic
- **Intrusion Detection** ...
- ....
- ..... 
- Coordination
Computer Security is not something that you can just add on when you need it.

Proper planning, installation, monitoring and maintenance all become part of a successful IDS/IPS implementation.

- Tri-Sentry (Host Sentry, NetSentry, Service Sentry)
- Nessus, Snort, nmap, Nikto, Tripwire, Samhain, Fcheck
- Checkpoint, Cisco IPS, VCC/Tripwire, F5, Big Iron, Juniper
- UTM (Cyberoam, Barracuda)

**BIG BOYS WILL DISCUSS ....**
- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- Network Forensic
- Intrusion Detection ...
- ....
- .....  
- **Coordination**
So, we have many Open Source/Commercial deployments already to monitor our network.

All the programs can generate alert/alarm on fault detection.

Need to centralize all the information.

We need to collaborate these programs

Need NOC

It's not a big Room/House – it’s a software

It's –RT (the ticketing system)
Request Tracker

- **RT** is a battle-tested issue tracking system which thousands of organizations use for
  - bug tracking,
  - help desk ticketing,
  - customer service,
  - workflow processes,
  - change management,
  - network operations,
  - And so on..
Fault documentation

RT

Trouble ticket system

NOC
User help desk

Information assistance
Trouble tickets

USER

Network

Correction

Diagnosis

Monitoring

Management action

Alarms
Request Tracker

Whenever, wherever and however there is a problem in the network the relevant monitoring software will send a ticket directly to RT system and system admins will know immediately via email or SMS. This automation will keep track of the SLA. RT has its own Help Desk system and escalation procedure.
- **Why are they important?**
  - Track all events, failures and issues

- **Focal point for help desk communication**

- **Use it to track all communications**
  - Both internal and external

- **Events originating from the outside:**
  - Customer complaints

- **Events originating from the inside:**
  - System outages (direct or indirect)
  - Planned maintenance, upgrades, etc.
- Monitoring
  - Data collection
  - Accounting

- Change control & monitoring

- Improvements
  - Upgrades

- NOC Tools
  - Ticket system

- Capacity planning
  - Availability (SLAs)
  - Trends
  - Detect problems

- User complaints
  - Requests

- Fix problems

Notifications

Ticket
• We learned some of the advantages of having a well-managed network
• We learned the features of some Open Source Network Monitoring tools
  o Nagios for monitoring network elements and servers
  o Smokeping for measuring latency in your network reliability measurement
  o Cacti/MRTG & Weathermap for graphing traffic and other statistics
  o RANCID for the backup of configs with version control
  o NFSen for network forensic
• We tied them all in a simple working Environment - RT
• So much more...

• All this software has many more features and is extensible
  o Read docs, forums, examples
  o Read the source code if you can
  o Ask questions, try it out

• There's commercial alternatives, and alternatives by hardware vendors
  o Compare the features, ask for a test version
  o Only because it costs money, it's not necessarily better/easier to manage (but maybe it is)
  o It all depends on YOUR needs
  o Support is also available for open-source tools
There's more network management/monitoring than the tools we covered, you can try the following tools (in no particular order)

- Visualize network designs with tools like Dia or Microsoft Visio or discover it automatically with Network Weathermap via Cacti
- Manage/secure who has router access with RADIUS or TACACS servers like Shrubbery's TACACS+ daemon or Freeradius
- Sniff and analyze Network traffic using Wireshark
- Install intrusion detection systems like SNORT
- Use a portscanner like nmap to find open ports or a scanner like Nessus to find potential vulnerabilities in your network
• Use a Wiki or Content Management system for your documentation like **trac** or **TWiki**

• Use **Netdot** and **Netdisco** to manage your addressing equipment

• Manage code for your tools or other data which changes using a versioning system like **CVS** or **Subversion** (we mentioned it in RANCID)
<table>
<thead>
<tr>
<th>Performance</th>
<th>Change Mgmt</th>
<th>Net Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cricket</td>
<td>Mercurial</td>
<td>Big Brother</td>
</tr>
<tr>
<td>IFPFM</td>
<td>Rancid (routers)</td>
<td>Big Sister</td>
</tr>
<tr>
<td>flowc</td>
<td>RCS</td>
<td>Cacti</td>
</tr>
<tr>
<td>mrtg</td>
<td>Subversion</td>
<td>Hyperic</td>
</tr>
<tr>
<td>netflow</td>
<td></td>
<td>Munin</td>
</tr>
<tr>
<td>NfSen</td>
<td></td>
<td>Nagios*</td>
</tr>
<tr>
<td>ntop</td>
<td></td>
<td>Netdisco</td>
</tr>
<tr>
<td>pmacct</td>
<td>Nessus</td>
<td>Netdot</td>
</tr>
<tr>
<td>rrdtool</td>
<td>OSSEC</td>
<td>OpenNMS</td>
</tr>
<tr>
<td>SmokePing</td>
<td>Prelude</td>
<td>Sysmon</td>
</tr>
<tr>
<td>Ticketing</td>
<td>Samhain</td>
<td>Untangle</td>
</tr>
<tr>
<td>RT, Trac, Redmine</td>
<td>SNORT</td>
<td>Zabbix</td>
</tr>
</tbody>
</table>

Security/NIDS

And that's not all!!!