Network Monitoring

Sebastian Büttrich, sebastian@less.dk
NSRC / IT University of Copenhagen
Last edit: February 2012, ICTP Trieste

http://creativecommons.org/licenses/by-nc-sa/3.0/
Agenda

- What is network monitoring?
- The "big three"
- Other useful tools and systems
- Questions and discussion
Remember the layer model

The TCP/IP and OSI Models

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical
Remember the layer model

The TCP/IP and OSI Models

- General Network monitoring
  mostly works on layer 3 and up, and often assumes TCP/IP networks

- Wireless network monitoring
  typically involves layer 2 - the specifically wireless aspects (spectrum, SSIDs, etc)
What are we monitoring?

- Connections, links, quality
- Bandwidth, usage
- Performance
- Systems & services
- Resources
- Configurations, changes
- Logfiles
- Users?
- Content of traffic?
Monitoring & Management

‣ Monitoring without response does not make much sense -

what good is seeing a problem if you don't react?

‣ Monitoring is part of management

‣ Management is closely related to expectations, contracts, SLAs
Different types of monitoring

- **human operated** vs **automatic**
- **active** vs **passive**

- Active human operated monitoring often gives good insight, but is not feasible 24/7
- Automatic monitoring can run 24/7, but needs to trigger notification/alerts and file service tickets in order to be useful
- Often the combination of both is needed.
The “big three”

- **Nagios**
  servers, switches, devices, services & anything that can talk IP and/or SNMP (this can include small wireless sensors!)

- **Smokeping**
  connections, quality, ping rtt, latency, jitter

- **Cacti**
  resources, traffic, interfaces, transactions, .. almost anything that is accessible via SNMP, e.g. temperature, power, ... sensor data
Nagios

- Nagios is an open source computer system monitor, network monitoring and infrastructure monitoring software application. Nagios offers monitoring and alerting for servers, switches, applications, and services. It watches hosts and services, alerting users when things go wrong and again when they get better.

(source: wikipedia)
Nagios
Nagios

Current Network Status

Last Updated: Tue Feb 14 22:30:00 CET 2012
Updated every 10 seconds
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as nagiosadmin

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>14</td>
</tr>
<tr>
<td>Down</td>
<td>4</td>
</tr>
<tr>
<td>Unreachable</td>
<td>2</td>
</tr>
<tr>
<td>Pending</td>
<td>0</td>
</tr>
</tbody>
</table>

All Problems: 6
All Types: 22

---

Host Status Details For All Host Groups

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Status</th>
<th>Last Check</th>
<th>Duration</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantis</td>
<td>UP</td>
<td>2012-02-14 22:47:41</td>
<td>30min 10s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.25 ms</td>
</tr>
<tr>
<td>Blinkx</td>
<td>UP</td>
<td>2012-02-14 22:49:01</td>
<td>69s 8s 22m 14s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.93 ms</td>
</tr>
<tr>
<td>Canary</td>
<td>UP</td>
<td>2012-02-14 22:49:11</td>
<td>69s 8s 22m 4s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.57 ms</td>
</tr>
<tr>
<td>BM2 gateway</td>
<td>UP</td>
<td>2012-02-14 22:49:31</td>
<td>69s 8s 22m 4s</td>
<td>PING OK - Packet loss = 0%, RTA = 1.40 ms</td>
</tr>
<tr>
<td>Capitola</td>
<td>UP</td>
<td>2012-02-14 22:48:31</td>
<td>144d 10h 15m 39s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.22 ms</td>
</tr>
<tr>
<td>Ferrari</td>
<td>UP</td>
<td>2012-02-14 22:49:31</td>
<td>71d 0h 4m 4s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.29 ms</td>
</tr>
<tr>
<td>IP2 sensor gateway</td>
<td>DOWN</td>
<td>2012-02-14 22:49:11</td>
<td>1d 14h 4m 26s</td>
<td>CRITICAL - Host Unreachable (130.220.142.106)</td>
</tr>
<tr>
<td>IP2 wireless</td>
<td>DOWN</td>
<td>2012-02-14 22:49:41</td>
<td>1d 14h 3m 5s</td>
<td>CRITICAL - Host Unreachable (130.220.142.109)</td>
</tr>
<tr>
<td>IP2, sensor gateway</td>
<td>DOWN</td>
<td>2012-02-14 22:47:41</td>
<td>23d 12h 31m 39s</td>
<td>CRITICAL - Host Unreachable (130.220.142.142)</td>
</tr>
<tr>
<td>Kinity</td>
<td>UP</td>
<td>2012-02-14 22:49:31</td>
<td>78d 12h 37m 34s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.58 ms</td>
</tr>
<tr>
<td>LAH2 gateway</td>
<td>UP</td>
<td>2012-02-14 22:49:51</td>
<td>144d 7h 41m 0s</td>
<td>PING OK - Packet loss = 0%, RTA = 1.42 ms</td>
</tr>
<tr>
<td>LAH1 gateway</td>
<td>UP</td>
<td>2012-02-14 22:49:01</td>
<td>31d 12h 53m 54s</td>
<td>PING OK - Packet loss = 0%, RTA = 1.48 ms</td>
</tr>
<tr>
<td>MONTANA parking</td>
<td>UP</td>
<td>2012-02-14 22:48:41</td>
<td>31d 13h 53m 54s</td>
<td>PING OK - Packet loss = 0%, RTA = 2.30 ms</td>
</tr>
<tr>
<td>Middletown</td>
<td>DOWN</td>
<td>2012-02-14 22:45:31</td>
<td>31d 13h 53m 44s</td>
<td>PING CRITICAL - Packet loss = 100%</td>
</tr>
<tr>
<td>Minerva</td>
<td>INREACHABLE</td>
<td>2012-03-14 22:46:41</td>
<td>1d 1h 6m 15s</td>
<td>CRITICAL - Host Unreachable (130.220.142.167)</td>
</tr>
<tr>
<td>Pfarmer</td>
<td>INREACHABLE</td>
<td>2012-02-14 22:45:51</td>
<td>30d 3h 40m 1s</td>
<td>CRITICAL - Host Unreachable (130.220.142.168)</td>
</tr>
<tr>
<td>Pikes, hill gateway</td>
<td>UP</td>
<td>2012-02-14 22:40:51</td>
<td>1d 14h 22m 14s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.20 ms</td>
</tr>
<tr>
<td>Pimliz</td>
<td>UP</td>
<td>2012-02-14 22:46:21</td>
<td>35d 10h 32m 21s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.03 ms</td>
</tr>
<tr>
<td>Pimliz</td>
<td>UP</td>
<td>2012-02-14 22:46:31</td>
<td>35d 10h 32m 4s</td>
<td>PING OK - Packet loss = 0%, RTA = 2.68 ms</td>
</tr>
<tr>
<td>Pimliz</td>
<td>UP</td>
<td>2012-02-14 22:46:41</td>
<td>50d 9h 30m 57s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.02 ms</td>
</tr>
<tr>
<td>Minster</td>
<td>UP</td>
<td>2012-02-14 22:48:11</td>
<td>33d 11h 32m 24s</td>
<td>PING OK - Packet loss = 0%, RTA = 0.24 ms</td>
</tr>
<tr>
<td>Pimliz</td>
<td>UP</td>
<td>2012-02-14 22:47:11</td>
<td>144d 0h 53m 30s</td>
<td>PING OK - Packet loss = 0%, RTA = 3.11 ms</td>
</tr>
</tbody>
</table>
Nagios – how to get started?

‣ For example by using the NSRC exercises:


http://nagios.org
Smokeping

- Smokeping is a network latency monitor. It measures network latency - rtt, jitter - to a configurable set of destinations on the network, and displays its findings in easy-to-read Web pages. SmokePing uses RRDtool as its logging and graphing back-end, making the system very efficient. The presentation of the data on the Web is done through a CGI with some AJAX capabilities for interactive graph exploration.

(source: freshmeat)
Smokeping

CN_Beijing_Daxing

KE_Nairobi_Strathmore

GH_Winneba_Univ_Winneba

US_Eugene_Univ_Oregon
Smokeping

Last 30 Hours

median rtt: 131.4 ms avg 213.0 ms max 116.1 ms min 146.9 ms now 17.8 ms sd 7.4 am/s
packet loss: 3.05 % avg 24.37 % max 0.00 % min 2.82 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s

end: Tue Feb 14 21:31:16 2012
Smokeping

Last 400 Days

median rtt: 429.1 ms avg 1.5 s max 116.4 ms min 125.0 ms now 333.3 ms sd 1.3 am/s
packet loss: 14.37 % avg 100.00 % max 0.00 % min 1.15 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s
end: Tue Feb 14 21:31:16 2012
Smokeping

GH_Winneba_Univ_Winneba

Navigator Graph

median rtt: 978.5 ms avg 1.9 s max 723.9 ms min 906.9 ms now 245.8 ms sd 4.0 am/s
packet loss: 31.10 % avg 100.00 % max 5.59 % min 27.43 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s end: Sun Apr 17 15:03:11 2011
Smokeping

IT_Trieste_ICTP

Navigator Graph

- Median RTT: 44.5 ms
- Average RTT: 52.4 ms
- Maximum RTT: 39.8 ms
- Minimum RTT: 41.0 ms
- Current RTT: 4.6 ms
- Standard Deviation: 9.6 ms

Packet Loss:
- Median Loss: 20.61%
- Average Loss: 100.00%
- Maximum Loss: 0.00%
- Minimum Loss: 0.00%
- Current Loss: 0.00%

Loss Color:
- Green: 0
- Blue: 1/20
- Black: 2/20
- Purple: 3/20
- Brown: 4/20
- Pink: 10/20
- Red: 19/20

Probe:
- 20 ICMP Echo Pings (56 Bytes) every 300s

End: Thursday, April 14, 2011 05:08:55
Smokeping – how to get started?

- For example by using the NSRC exercises:


  http://oss.oetiker.ch/smokeping/
Cacti

- Cacti is an open source, web-based graphing tool designed as a frontend to RRDtool's data storage and graphing functionality. Cacti allows a user to poll services at predetermined intervals and graph the resulting data. It is generally used to graph time-series data of metrics such as CPU load and network bandwidth utilization. A common usage is to monitor network traffic by polling a network switch or router interface via SNMP. (source: wikipedia)
Cacti

**WIFI login**

From 2012/01/13 21:42:00 To 2012/02/14 21:42:00

Average Login: 28.25  
Max Login: 194.85  
Min Login: 138.44

**Login pr SSID**

From 2012/01/13 21:42:00 To 2012/02/14 21:42:00

- **All**
- **Eduroam**
- **ITU**
- **Web-Auth**
Cacti

Mysql - MySQL Command Counters

*From 2012/01/13 21:42:00 To 2012/02/14 21:42:00*

- **Questions**: Cur: 3.8, Avg: 11.5, Max: 72.5
- **Com Select**: Cur: 2.7, Avg: 6.9, Max: 33.7
- **Com Delete**: Cur: 31.3m, Avg: 63.2m, Max: 395.4m
- **Com Insert**: Cur: 27.1m, Avg: 108.9m, Max: 596.2m
- **Com Update**: Cur: 45.6m, Avg: 304.4m, Max: 1.9
- **Com Replace**: Cur: 0.0, Avg: 18.1u, Max: 1.7m
- **Com Load**: Cur: 0.0, Avg: 723.4m, Max: 138.9u
- **Com Delete Multi**: Cur: 0.0, Avg: 1.1u, Max: 277.8u
- **Com Insert Select**: Cur: 0.0, Avg: 12.5m, Max: 98.0m
- **Com Update Multi**: Cur: 0.0, Avg: 0.0, Max: 0.0
- **Com Replace Select**: Cur: 0.0,Avg: 0.0, Max: 0.0
Cacti

- Traffic - (eth0)

From 2012/01/13 21:42:00 To 2012/02/14 21:42:00

- Inbound
  - Current: 110.36 k
  - Average: 85.14 k
  - Maximum: 549.89 k

- Outbound
  - Current: 72.95 k
  - Average: 96.91 k
  - Maximum: 732.76 k
Cacti

- Cacti is a good tool for monitoring power
  - e.g. solar installations
  - as it can monitor electrical and environmental data
Cacti – how to get started?

‣ By now you can guess :)


http://cacti.net
Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more."[1] It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. [2]

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.
(source: wikipedia)
Other useful tools

▶ Command line tools:

mtr – ping and traceroute
nmap – port scanning

▶ Iperf
command line client-server tests

```
# iperf -c 130.226.142.162

Client connecting to 130.226.142.162, TCP port 5001
TCP window size: 16.0 KByte (default)
[  3] local 140.105.20.155 port 50523 connected
with 130.226.142.162 port 5001
[ ID] Interval    Transfer  Bandwidth
[  3]  0.0-10.0 sec  24.3 MBytes  20.4 Mbits/sec
```
Other useful tools

- Wireshark: advanced packet dumper
Other useful tools

‣ Etherape: visualization toy, but a nice toy :)
Other useful tools

- Huge performance suite: perfSONAR
- Traffic, bandwidth: bandwidthhd
- Router config management: Rancid
- Network Documentation: Netdot
  https://netdot.uoregon.edu/
- Intrusion Detection: tripwire, snort
- Vulnerabilities: Nessus, OpenVAS
And ...

- There are dozens of others ...

... but I really have to go to bed now :) 

Questions?

- You tell me what you would like to monitor and we find the right tool for it!
Other useful tools

- Huge performance suite: perfSONAR
- Traffic, bandwidth: bandwidthd
- Router config management: Rancid
- Network Documentation: Netdot https://netdot.uoregon.edu/
- Intrusion Detection: tripwire, snort
- Vulnerabilities: Nessus, OpenVAS