NOC Tools Tutorial

Luke Fowler
<luke@grnoc.iu.edu>

Internet2/ESCC Joint Techs Workshop, Albuquerque, NM
February, 2006

http://tools.globalnoc.iu.edu/
# Tools Overview

<table>
<thead>
<tr>
<th>Open Source</th>
<th>Home Grown</th>
</tr>
</thead>
<tbody>
<tr>
<td>RANCID</td>
<td>Syslog Analysis Tool</td>
</tr>
<tr>
<td>MRTG</td>
<td>SNAPP</td>
</tr>
<tr>
<td>RRDtool</td>
<td>Router Proxy</td>
</tr>
<tr>
<td>Syslog-ng</td>
<td>Weather Map</td>
</tr>
<tr>
<td>Nagios</td>
<td>Nagios Plugins / Config Generator</td>
</tr>
<tr>
<td></td>
<td>Alert Mon</td>
</tr>
<tr>
<td></td>
<td>Visible Backbone</td>
</tr>
<tr>
<td></td>
<td>Firewall Filter Viz.</td>
</tr>
<tr>
<td></td>
<td>Network Information Database</td>
</tr>
</tbody>
</table>
RANCID

- “Really Awesome New Cisco Differ”
- Puts router/switch configs into a CVS repository.
- Sends e-mail messages showing router config diffs.
- Works on more than just Cisco devices!
RANCID
“Multi Router Traffic Grapher”

Collects time-series statistics via SNMP, graphs these data.

Collector process invoked by ‘cron’

Can store data in ‘.log’ or RRD format

Released under the GNU General Public License (GPL)

Very popular!

http://www.mrtg.org/
RRDtool

http://rrdtool.eu.org/

• “Round Robin Database”

• Written by Tobi Oetiker, author of MRTG.

• Stores time-series data in a fixed-sized file. When the file gets ‘full’ the oldest samples are discarded to make room for new data.

• Does not do data collection -- you supply the collector (MRTG or SNAPP might do the trick)
RRDtool (cont’d)

• Several data types: gauge, derive, counter, absolute

• set the “step” of your RRD file to your collection interval

• RRA definitions dictate data retention options. You choose the granularity of data retention. Very flexible (e.g. store 30-second ‘maximum’ data for 6 months, store 5 minute averages for 4 years)
RRDtool (cont’d)

- RRDtool includes a tool to create graph images of data stored in .rrd files.
- Can consolidate data sources, apply RPN (reverse polish notation) expressions to items being graphed.
- Graphs “lines”, (solid) “areas”, and “stack”ed areas.
- Outputs .gif and .png.
- All RRDtool operations available through Perl library ‘RRDs’, and C library.
syslog-ng

- Sink for your syslogs
- Stores syslogs in a user-defined format
- Filter logs on regular expressions, and additional functions like “host”, program field, facility code, etc.
- Can forward syslogs on to another syslog server.
- Can be used to store syslogs in a relational database.
- We use syslog-ng along with our syslog analysis scripts at the Global NOC.

http://www.balabit.com/products/syslog_ng/
Nagios

- Open source network monitoring system. Formerly “Netsaint”.
- Web-based user interface
- Flexible plugin based host/service check execution. Nagios spawns small “plugin” executables for each check.
- Plugins are very easy to write.
- Licensed under the GNU GPL
## Service Status Details For Host Group 'nlr-layer-3'

<table>
<thead>
<tr>
<th>Host</th>
<th>Service</th>
<th>Status</th>
<th>Last Check</th>
<th>Duration</th>
<th>Attempt</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATLAcrs</td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:45:59</td>
<td>3d 1h 11m 39s</td>
<td>1/1</td>
<td>Link to BB to WASH tel/0/0 - NLR-ATLA-WASH-10GE-04 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/1</td>
<td>OK</td>
<td>02-05-2006 11:46:04</td>
<td>1d 20h 2m 21s</td>
<td>1/1</td>
<td>Link to BB to ATLA 6509 tel/1/2 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:46:01</td>
<td>1d 20h 41m 6s</td>
<td>1/1</td>
<td>Link to BB to HOUS tel/0/2/0 - NLR-ATLA-HOUS-10GE-70 is Up</td>
</tr>
<tr>
<td>CHCCrs</td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:45:53</td>
<td>3d 1h 8m 41s</td>
<td>1/1</td>
<td>Link to BB to WASH tel/0/2/04 - NLR-CHC-WASH-10GE-59 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/4</td>
<td>OK</td>
<td>02-05-2006 11:46:01</td>
<td>3d 1h 11m 37s</td>
<td>1/1</td>
<td>Link to BB to DENV tel/0/2/01 - NLR-CHC-DENV-10GE-126 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/6</td>
<td>OK</td>
<td>02-05-2006 11:46:01</td>
<td>3d 1h 11m 37s</td>
<td>1/1</td>
<td>Link to BB to DENV tel/0/2/0 - NLR-CHC-DENV-10GE-36 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:46:01</td>
<td>2d 14h 26m 21s</td>
<td>1/1</td>
<td>Link to BB to CHC 6509 tel/1/4 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceStarlight110</td>
<td>OK</td>
<td>02-05-2006 11:46:14</td>
<td>0d 3h 31m 1s</td>
<td>1/6</td>
<td>Link to StarLight Force10 is Up</td>
</tr>
<tr>
<td></td>
<td>interface-ultrash-10GigE-1</td>
<td>OK</td>
<td>02-05-2006 11:42:17</td>
<td>3d 7h 47m 33s</td>
<td>1/6</td>
<td>Link to UltraLight 10GigE 1/2 is Up</td>
</tr>
<tr>
<td></td>
<td>interface-ultrash-10GigE-2</td>
<td>OK</td>
<td>02-05-2006 11:40:53</td>
<td>3d 20h 48m 52s</td>
<td>1/6</td>
<td>Link to UltraLight 10GigE 2/2 is Up</td>
</tr>
<tr>
<td>DENVCrs</td>
<td>NCAR Interface</td>
<td>CRITICAL</td>
<td>02-05-2006 11:42:53</td>
<td>1d 21h 20m 54s</td>
<td>0/6</td>
<td>Link to UOAR (A3 14041) M20 peering via 605 is down</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:45:54</td>
<td>3d 1h 8m 41s</td>
<td>1/1</td>
<td>Link to BB to CHC tel/0/5/0 - NLR-CHC-CHC-10GE-36 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/1</td>
<td>OK</td>
<td>02-05-2006 11:46:06</td>
<td>3d 1h 11m 33s</td>
<td>1/1</td>
<td>Link to BB to CHC tel/0/2/0/4 - NLR-CHC-DENV-10GE-126 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/2</td>
<td>OK</td>
<td>02-05-2006 11:46:06</td>
<td>3d 1h 8m 41s</td>
<td>1/1</td>
<td>Link to BB to CHC tel/0/5/0/2 - NLR-CHC-DENV-10GE-92 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/4</td>
<td>OK</td>
<td>02-05-2006 11:46:06</td>
<td>2d 14h 26m 55s</td>
<td>1/1</td>
<td>Link to BB to CHC tel/0/2/0 - NLR-CHC-DENV-10GE-36 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:46:05</td>
<td>3d 1h 11m 31s</td>
<td>1/1</td>
<td>Link to BB to CHC tel/0/5/0/6 - NLR-CHC-DENV-10GE-70 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/5</td>
<td>OK</td>
<td>02-05-2006 11:46:01</td>
<td>2d 20h 12m 16s</td>
<td>1/1</td>
<td>Link to BB to HOUS tel/0/5/0 - NLR-CHC-DENV-10GE-82 is Up</td>
</tr>
<tr>
<td>HOUS-crs</td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:45:55</td>
<td>0d 2h 38m 10s</td>
<td>1/1</td>
<td>Link to BB to HOUS 6509 Tel/1/1 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/1</td>
<td>OK</td>
<td>02-05-2006 11:46:54</td>
<td>1d 23h 5m 3s</td>
<td>1/1</td>
<td>Link to BB to ATLA tel/0/5/0 - NLR-ATLA-HOUS-10GE-70 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/2</td>
<td>OK</td>
<td>02-05-2006 11:46:54</td>
<td>0d 4h 5m 2s</td>
<td>1/1</td>
<td>Link to BB to ATLA tel/0/5/0/4 - NLR-ATLA-HOUS-10GE-82 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/4</td>
<td>OK</td>
<td>02-05-2006 11:46:56</td>
<td>0d 4h 50m 32s</td>
<td>1/1</td>
<td>Link to BB to ATLA tel/0/5/0/6 - NLR-ATLA-HOUS-10GE-82 is Up</td>
</tr>
<tr>
<td></td>
<td>ping</td>
<td>OK</td>
<td>02-05-2006 11:46:53</td>
<td>2d 12h 20m 16s</td>
<td>1/6</td>
<td>Ping OK - Packet loss = 0%, RTA = 49.69 ms</td>
</tr>
<tr>
<td>LOSACrs</td>
<td>interfaceTenGigE/2/0/0</td>
<td>OK</td>
<td>02-05-2006 11:46:26</td>
<td>1d 1h 3m 29s</td>
<td>1/1</td>
<td>Link to BB to LOSA tel/0/5/0/2 - NLR-LOS-LOS-10GE-87 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/1</td>
<td>OK</td>
<td>02-05-2006 11:46:29</td>
<td>3d 1h 11m 39s</td>
<td>1/1</td>
<td>Link to BB to LOSA tel/0/5/0/4 - NLR-LOS-LOS-10GE-90 is Up</td>
</tr>
<tr>
<td></td>
<td>interfaceTenGigE/2/0/2</td>
<td>OK</td>
<td>02-05-2006 11:46:29</td>
<td>3d 1h 11m 39s</td>
<td>1/1</td>
<td>Link to BB to LOSA tel/0/5/0/6 - NLR-LOS-LOS-10GE-90 is Up</td>
</tr>
</tbody>
</table>

**Current Network Status**

Last Updated: Jun 26 11:14:55 EST 2005
Updated every 00 seconds
Nagios - [web.nagios.org](http://web.nagios.org)
Logged in as Luke

[View Service Status Details For All Host Groups](https://nlrmon.grnoc.iu.edu/nagios/cgi-bin/status.cgi?hostgroup=nlr-layer-3&style=)
[View Host Status Detail For This Host Group](https://nlrmon.grnoc.iu.edu/nagios/cgi-bin/status.cgi?hostgroup=nlr-layer-3&style=)
[View Status Overview For This Host Group](https://nlrmon.grnoc.iu.edu/nagios/cgi-bin/status.cgi?hostgroup=nlr-layer-3&style=)
[View Status Summary For This Host Group](https://nlrmon.grnoc.iu.edu/nagios/cgi-bin/status.cgi?hostgroup=nlr-layer-3&style=)
[View Status Grid For This Host Group](https://nlrmon.grnoc.iu.edu/nagios/cgi-bin/status.cgi?hostgroup=nlr-layer-3&style=)
## Status Summary

### Current Network Status
- **Last Updated:** Sun Feb 5 11:48:57 EST 2006
- **Updated every 90 seconds**
- **Nagios® - www.nagios.org**
- **Logged in as Luke**

### Current Service Status

### Host Status Totals
- **Up**: 248
- **Down**: 15
- **Thresholds**: 0
- **Pending**: 0

### Service Status Totals
- **OK**: 411
- **Warning**: 0
- **Unknown**: 0
- **Critical**: 34
- **Pending**: 0

### Status Summary For All Host Groups

<table>
<thead>
<tr>
<th>Host Group</th>
<th>Host Status Totals</th>
<th>Service Status Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 3 BGP Sessions (L3-BGP)</td>
<td>7 UP</td>
<td>9 OK</td>
</tr>
<tr>
<td>NLR/CENIC_15454 Los Angeles, CA &lt;-&gt; San Diego, CA (nir-CENIC-los-san-don)</td>
<td>1 UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>NLR/CENIC_15454 Los Angeles, CA &lt;-&gt; Sunnyvale, CA (nir-CENIC-los-sunny)</td>
<td>2 UP</td>
<td>2 OK</td>
</tr>
<tr>
<td>NLR OOB Reuters (nir-OOB)</td>
<td>1 UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>NLR Chicago &lt;-&gt; STARLIGHT_15454s (nir-STAR-CHI-15454s)</td>
<td>1 UP</td>
<td>1 OK</td>
</tr>
<tr>
<td>NLR 15454s Albuquerque &lt;-&gt; El Paso (nir-abc-elp)</td>
<td>8 UP</td>
<td>8 OK</td>
</tr>
<tr>
<td>NLR 15454s Atlanta &lt;-&gt; Jacksonville (nir-atl-jack)</td>
<td>7 UP</td>
<td>7 OK</td>
</tr>
<tr>
<td>NLR Chicago &lt;-&gt; Pittsburgh 15454s (nir-chic-pitt-006)</td>
<td>12 UP</td>
<td>12 OK</td>
</tr>
<tr>
<td>NLR Dallas &lt;-&gt; Houston (nir-dal-hosp)</td>
<td>10 UP</td>
<td>10 OK</td>
</tr>
<tr>
<td>NLR Denver, CO &lt;-&gt; Chicago, IL 15454s (nir-den-chic-006)</td>
<td>24 UP</td>
<td>24 OK</td>
</tr>
<tr>
<td>NLR Denver &lt;-&gt; Reton (nic-den-ret)</td>
<td>8 UP</td>
<td>8 OK</td>
</tr>
<tr>
<td>NLR El Paso &lt;-&gt; San Antonio (nic-elp-san)</td>
<td>11 UP</td>
<td>11 OK</td>
</tr>
<tr>
<td>NLR Front End Cheaslea (nic-front-ends)</td>
<td>26 UP</td>
<td>26 OK</td>
</tr>
<tr>
<td>NLR Houston &lt;-&gt; Reton Route (nic-hous-ret)</td>
<td>8 UP</td>
<td>8 OK</td>
</tr>
<tr>
<td>NLR Jacksonville &lt;-&gt; Pensacola (nic-jackson-pena)</td>
<td>11 UP</td>
<td>12 OK</td>
</tr>
<tr>
<td>NLR Kansas City &lt;-&gt; Tulsa (nic-kans-tul)</td>
<td>8 UP</td>
<td>8 OK</td>
</tr>
<tr>
<td>NLR Layer 2 (6509) Network (nic-layer-2)</td>
<td>17 UP</td>
<td>17 OK</td>
</tr>
<tr>
<td>NLR Layer 3 (6509) Network (nic-layer-3)</td>
<td>3 UP</td>
<td>3 OK</td>
</tr>
</tbody>
</table>

### View Service Status Detail For All Host Groups
- **View Status Overview For All Host Groups**
- **View Status Grid For All Host Groups**

---

[Image: screenshot of the status summary page with a table showing various host groups and their status counts, along with critical and OK counts for services.]
Alert History

All Hosts and Services

July 17, 2004 11:00

[07-17-2004 11:01:46] HOST ALERT: is-CENIC-SUNVL03.UP:SOFT;2,PING OK - Packet loss = 0%, RTA = 74.36 ms
[07-17-2004 11:01:46] HOST ALERT: is-CENIC-SUNVL03.DOWN:SOFT;1,Critical - Plugin timed out after 10 seconds

July 17, 2004 00:00

[07-17-2004 00:45:39] HOST ALERT: is-CENIC-SUNVL03.UP:SOFT;2,PING OK - Packet loss = 0%, RTA = 74.82 ms
[07-17-2004 00:45:39] HOST ALERT: is-CENIC-SUNVL03.DOWN:SOFT;1,Critical - Plugin timed out after 10 seconds
IU Nagios Plugins

• Plugins written at IU, used to monitor a variety of network services. Released under the IU Open Source License.

• Mostly written in Perl, BGP plugin written in C

<table>
<thead>
<tr>
<th></th>
<th>IS-IS</th>
<th>OSPF</th>
<th>MSDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td></td>
<td></td>
<td>Interface up/down</td>
</tr>
<tr>
<td>Cisco/Juniper CPU Load</td>
<td></td>
<td>TL1 alarm monitoring</td>
<td></td>
</tr>
</tbody>
</table>
IU Nagios Plugins

• Get plugin usage by invoking the plugin with no arguments

• BGP plugin requires NET-SNMP libraries, other plugins require Getopt::Std, Net::SNMP.
Configuring a new plugin in Nagios

Define a ‘command’ statement for each plugin

```bash
define command {
    command_name  check_cpu
    command_line  $USER1$/check_cpu -r $HOSTADDRESS$ -c $ARG1$ -v $ARG2$
}

define command {
    command_name  check_isis
    command_line  $USER1$/check_isis -r $HOSTADDRESS$ -c $ARG1$ -n $ARG2$
}

define command {
    command_name  check_intf
    command_line  $USER1$/check_intf -r $HOSTADDRESS$ -c $ARG1$ -i $ARG2$
}

define command {
    command_name  check_msdp
    command_line  $USER1$/check_msdp -r $ARG1$ -c $ARG2$ -p $ARG3$
}
```
Configuring a Service Check

Add a service check definition for each instance of a service you wish to monitor.
Optical Network Element Monitoring

- As we began supporting networks with a layer-1 component, we had a need to integrate monitoring of these devices into our monitoring environment.

- Goal: Monitor optical NE alarms in the current Nagios-based system

- Problem: There were no Nagios plugins in existence for optical device monitoring
Optical Monitoring

- Most optical devices provide a TLI ("Transaction Language 1") interface for management
- text-based request/response system for retrieving operational information and for provisioning optical devices
- Very little open-source / free software to work with TLI
- Recently Net::TLI Perl module has been released, but it does not yet work with many devices.
Optical Monitoring

• We chose to develop our optical monitoring solution using the Monfox DynamicTL1 Manager SDK

• Commercial package

• This SDK provides a Java interface to TL1 interaction with optical devices

• We used this SDK to write a set of Nagios plugins, and a Nagios “Optical Passive Checker” daemon
Optical Monitoring

- Our Optical Passive Checker daemon currently supports Cisco 15454, 15808 and Nortel HDXc, OME 6500.
- Only small changes are necessary to support most other optical platforms.
- We currently alert on any MAJOR or CRITICAL level alarm being emitted by the optical device.
- Alerts for specified alarm codes can be suppressed on an individual basis.
Nagios at the Global NOC

• We auto-generate much of our Nagios config based on router/switch configs.

• Network devices are polled via JUNOScript or IOS-XR XML, and configs stored by RANCID are analyzed to construct Nagios config.

• NOC Operators watch an “Alert Mon” display, which shows information about all pending alerts.
Monitored Services

- Ping
- ISIS and BGP Peering
- Layer 1 Alarms
- Interface up/down status
- Systems monitoring (CPU and Disk Thresholds, ssh reach-ability, etc.)
- Process / Application Specific Monitoring
- TCP Performance
AlertMon

• Centralized Alert Monitor

• Provides one location to see current alarms

• Allows the GlobalNOC to easily correlate alarms and the status of the progress resolution

• Documentation and Procedure “Hub”

• NOC ”Big Board”
AlertMon Features

- Visually and audibly flagging new alerts
- Collapses alerts when parent is down
- Tickets, documentation, and procedures are linked to each alert
- Alert Filters (by administrative grouping, alert type, priority)
AlertMon

Current Network Status
Last Updated: Thu Jul 15 08:21:45 2004
Refreshed every 30 seconds

<table>
<thead>
<tr>
<th>Host</th>
<th>Service Type</th>
<th>Duration</th>
<th>Status Information</th>
<th>Claim</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHINng:9264:140.109.251.150</td>
<td>PING</td>
<td>23d 23h 18m 31s</td>
<td>ASNet (Taiwan) is ICMP Unreachable</td>
<td>5234:2</td>
<td></td>
</tr>
<tr>
<td>rls</td>
<td>PING</td>
<td>34d 23h 12m 33s</td>
<td>rls.uits.indiana.edu is ICMP Unreachable</td>
<td>331:7</td>
<td></td>
</tr>
<tr>
<td>HSTNng:18592:200.23.60.21</td>
<td>PING</td>
<td>58d 15h 8m 11s</td>
<td>CUDI-multihop via UTEP is ICMP Unreachable</td>
<td></td>
<td>EDIT</td>
</tr>
</tbody>
</table>

AlertMon Service Troubleshooting Link

Documentation

Escalation Info

DB Link to Host/Interface Info

DB Link to Contacts

Link to Ticket
AlertMon Workflow

- New Alert on AlertMon
- NOC uses documentation presented in each alert to troubleshoot the problem
- If problem is real and persistent the NOC claims the message and opens a ticket
- The NOC follows the escalation procedures linked from the alert
AlertMon Design

- SOAP is used to pass message from monitoring server (Nagios) to data collectors
- XML and RSS Files are generated
- CGI Front-End reads the XML file and generates a HTML version
- Distributed Architecture
AlertMon
System
Architecture
Weathermap

- uses MRTG .log or RRDtool .rrd files as input
- You configure a background image, locations of arrows, and nodes, etc.
- A perl script that is run via Cron will update your template image, producing an updated weathermap graphic
- Available for free to educational and non-profit organizations.
- SVG version of the Weathermap software is completed and about to be deployed

Available at: http://tools.globalnoc.iu.edu/
Weathermap Configuration

- Set up file paths, legend and clock parameters, and scale parameters.
Weathermap Configuration

- “link” settings tell the weathermap where to draw “arrows” between nodes.

- “area” settings indicate where to place links to detailed graphs for nodes/arrows.
Weathermap Configuration

- “label” settings tell the weathermap where to place “nodes”, and what captions to place next to them.
Router Proxy

Abilene Core Node Router Proxy

A service of the Abilene NOC

This tool allows you to submit show commands to an Abilene core node router. Select a core node, select and complete the command of your choice, and submit the form; the output of the command will be returned in the lower frame.

Router: [IPLSg [Indianapolis, Indiana – Juniper T640]]
Command: [show ip routing]

For questions, concerns, or problems, please contact webmaster@abilene.iu.edu.

Response from Router:

inet.0: 8926 destinations, 14203 routes (867 active, 1 holddown, 288 hidden)
+ = Active Route, - = Last Active, * = Both

129.79.0.0/16  *(BGP/170) v4/ID 14:58:19, MED 0, localpref 200
AS path: 19782 87 1
> to 192.12.296.250 via ge-2/3/0.0

129.79.0.0/16  *(BGP/170) v4/ID 14:58:09, MED 0, localpref 200
AS path: 19782 87 1
> to 192.12.296.250 via ge-2/3/0.0
Router Proxy

- A web interface to router/switch ‘show’ commands.
- Connects to devices using Telnet or SSH
- Users enter their command on a HTML form, submit, and results are returned in the lower HTML frame.
- Router Proxy for Abilene at http://loadrunner.uits.iu.edu/~routerproxy/abilene/
Router Proxy: Commands

• On our router proxy implementations, we allow:
  show ip, show ipv6, show interface, show controller, show route-map, traceroute, ping, show version, show environment, show atm, show proc, show bgp, mtrace, show msdp, show pim, show multicast, show route, show chassis, show policy, show isis

• You set up your router proxy instance to allow or deny any commands you choose.

• We disallow certain expressions that could take a lot of processor time on the router (e.g. the “|” operator, so a user cannot do something such as piping output to a complicated ‘match’ expression)
Router Proxy Config

• We set up a ‘routerproxy’ user, which owns all Router Proxy files, and which the Router Proxy CGI scripts run as.

• Requires Perl with CGI.pm, Net::Telnet, Net::SSH::Perl, and Config:INIFiles

• Logs of proxy usage are stored in ‘proxy.log’ for debugging and accounting purposes.
Router Proxy Config

- Global configuration parameters, such as the username/password the router proxy will use to login to devices, paths to support files, ‘header’ output for the web form are set first.

- The “router” section specifies parameters for each router proxy device.
Router Proxy Config

- "command" parameters specify attributes for router proxy commands.
- "rule" parameters define regular expressions to allow or disallow in user commands.
SNAPP

• “SNMP Network Analysis and Presentation Package”
• Short-interval data collection for SNMP variables.
• Stores data in RRDtool .rrd files
• Web front-end for viewing data
• XML based configuration
• Custom view groupings / custom graphing
• Basic threshold reporting
• Licensed under the GNU GPL
SNAPP Data Collector

- Multi-threaded, persistent data collector
- Written in C
- Talks to SNMP devices using the UCD-SNMP library, writes data to RRD files using librrd.
- Configuration information stored as XML
- Changes made to collections via the front-end generate a HUP signal to the collector, causing it to re-load configuration data.
SNAPP Front-End

- Web based CGIs, written in Perl
- Session support, logins can persist between browser sessions, for up to 1 month.
- Restrict administrative access by group membership
- Collections and users may be members of several groups
- Flexible visualization options
SNAPP Collection Classes

- Each collection is associated with a “collection class”
- Specifies SNMP OIDs to collect, data retention parameters, default graphing behavior, data collection interval, etc.
- Supports “graph math” via RRD RPN expressions
SNAPP: Adding Collections

- Select a collection class
- Select collection-specific parameters (SNMP host, community string, group access, threshold override, etc.)
- Click “Add Link” -- a new RRD file will be created, the SNAPP config will be updated, and the collector will reload its’ configuration.
SNAPP: Custom Views

- Allows users to group a set of graphs together (e.g. all collections on a single router)
- Default graphs for custom view members are shown together on a single page
- View can be created based on groups, or individual collections
- Anyone can see and create custom views, admins can edit/remove.
SNAPP: Custom Graphs

- Allows custom graphs to be generated based on start and end date/time
- Allows a user to select which SNMP variables to show / hide
Syslog Scripts

- Gather syslogs using the syslog-ng tool
- We separate out logs into one file per network (filter by facility code)
- Each log file gets processed by the syslog scripts, generating an e-mail containing all interesting log entries for the past 24 hours
- Requires Perl with Config::INIfiles
Syslog Scripts

Subject: Abilene Syslog Errors (2004-05-11): 100 total messages

Syslog errors for 2004-05-11:

Filters:
- Priority 0 - 3
  - Include regexp: "Configured maximum prefix-limit" "Sensor Fail"
  - Include regexp: "loopback" "loopback suspected" "xmtpd"
  - "tcp_send" "SHMID_SEND_FAILURE" "ssh_correct" "ssh DCP" "BGP" "ISDN ROUTE-3-ROUTE3UNI_EX" "DMP-3-AUTHFAIL" "LINK-3-UPDOWN" "GRACEFUL-3-THREUT"

Summary of Log Messages:
  - CPIN: 1,939
  - NFAS: 10
  - total: 1

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Cnt</th>
<th>Prior</th>
<th>Host</th>
<th>Process</th>
</tr>
</thead>
</table>

Note: Fri, 9 Jul 2004 23:50:05 -0400 (EDT)
From: Syslog Admin <syslog@abilene.abilene.edu>
To: routing@abilene.edu
Subject: Gigasys Syslog Errors (2004-07-09): 33 total messages

Syslog errors for 2004-07-09:

Filters:
- Priority 0 - 3
  - Include regexp: "Configured maximum prefix-limit" "Sensor Fail"
  - Exclude regexp: "loopback" "loopback suspected" "xmtpd"

Summary of Log Messages:
  - unknown: 28
  - sshd: 5

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Cnt</th>
<th>Prior</th>
<th>Host</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-07-09 23:44:00</td>
<td>23:44:05</td>
<td>27</td>
<td>3</td>
<td>ui</td>
<td>rpd</td>
</tr>
<tr>
<td>2004-07-09 23:44:00</td>
<td>23:44:05</td>
<td>27</td>
<td>3</td>
<td>ui</td>
<td>rpd</td>
</tr>
<tr>
<td>2004-07-09 23:44:00</td>
<td>23:44:05</td>
<td>27</td>
<td>3</td>
<td>ui</td>
<td>rpd</td>
</tr>
</tbody>
</table>

Help ❯ MsgIndex P PrevLog - F NextPage D Delete R Reply
Help ❯ MsgIndex P PrevLog - F NextPage D Delete R Reply
Syslog Scripts Config

- The syslog-ng.template file is used to generate a syslog-ng.conf file
- ‘active’ elements are enclosed in < > tags
- Configure log file paths, ownership, and filtering (e.g. by facility)
Syslog Scripts Config

- The ‘config’ section contains group and facility names for the syslog group.
- The ‘email’ section contains recipients of syslog reports.
- The ‘hosts’ section contains parameters for each device we are receiving syslogs from.
Syslog Scripts Config

- The ‘filters’ section is used to describe which log entries to report.
  - Any entry that matches an item listed in ‘exclude’ will not get reported.
  - Any entry that matches an item listed in ‘include’ will get reported.
  - An entry with a priority level listed in ‘priority’ will get included (if not in ‘exclude’ list).
Visible Backbone

- Visible Backbone collects information from Juniper routers using JUNOScript, Juniper’s XML/RPC interface
- Presents a set of web pages with various views of data collected
- Access to archived data is available through a SOAP interface
- Requires Perl, the JUNOScript API, XML::DOM, XML::Simple, and File::Copy
- Consists of an XML collector, and a set of scripts to process each type of XML data
Visible Backbone

Abilene - Visible Backbone

Most Elements are now linked to RRD graphs, where appropriate.

Every hour a wide variety of data is gathered from all of the Abilene backbone Juniper routers via XML. Shortly after the data is gathered it is processed by a large member of Perl programs. These programs generate the data available on this page, The Abilene Visible Backbone.

We should be adding more processed data on a regular basis. Send us some e-mail if there's something you're particularly interested in.

Abilene - Gigapop Technology Support

"Internet2 Working Groups"

Gigapops are encouraged to take advantage of several areas of advanced networking. This includes large MTUs (>9000), as well as support for IPv6 and Multicast. We track the individual gigapops support of these three areas of advanced technology. We track the gigapops speed & MTU from their interface. IPv6 support is determined by the existence of a valid 2001 or 3FFE IPv6 address on a gigapop's interface. Multicast support is gauged by the existence of a PIM neighbor relation on the gigapop's interface.

<table>
<thead>
<tr>
<th>Technology Support by Gigapop</th>
<th>Description</th>
<th>Router</th>
<th>Speed</th>
<th>MTU</th>
<th>IPv6?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arizona State University</td>
<td>drvmg</td>
<td>OC3</td>
<td>9180</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CERN (LHCb, primary v4 link)</td>
<td>ching</td>
<td>10GigE</td>
<td>9174</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CERN DataTAG (v4)</td>
<td>ching</td>
<td>10GigE</td>
<td>9000</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CHECNS-MET (New Mexico aggregate)</td>
<td>drvmg</td>
<td>OC3</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CalREN North</td>
<td>suwarg</td>
<td>OC12</td>
<td>9120</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CalREN South</td>
<td>losang</td>
<td>10GigE</td>
<td>9178</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Drexel</td>
<td>washing</td>
<td>OC3</td>
<td>3470</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Florida AM University</td>
<td>hstng</td>
<td>OC12</td>
<td>9120</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Front Range Gigapop</td>
<td>drvmg</td>
<td>OC12</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Great Plains Network</td>
<td>kscynq</td>
<td>OC12</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Indiana Gigapop GigabitEthernet</td>
<td>ipbsg</td>
<td>GigE</td>
<td>1500</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interuniversity Gigapop</td>
<td>drvmg</td>
<td>OC3</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Iowa State</td>
<td>kscynq</td>
<td>OC3</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jackson State via BellSouth ATM</td>
<td>atl-mfls</td>
<td>OC3</td>
<td>9120</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LaNet</td>
<td>hstng</td>
<td>OC3</td>
<td>3470</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MAGPI</td>
<td>washing</td>
<td>OC12</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MREN via StarLight</td>
<td>ching</td>
<td>10GigE</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Merit net2</td>
<td>ipbsg</td>
<td>OC12</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mid-Atlantic Crossroads</td>
<td>washing</td>
<td>OC48</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mississippi State via BellSouth ATM</td>
<td>atl-mfls</td>
<td>OC3</td>
<td>9120</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NCSN/AMCNC</td>
<td>washing</td>
<td>OC48</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NYSERNET GigE</td>
<td>nycang</td>
<td>GigE</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NYSERNET - Chicago</td>
<td>ching</td>
<td>OC12</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>North Texas Gigapop</td>
<td>hstng</td>
<td>OC3</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Northern Crossroads</td>
<td>nycang</td>
<td>OC48</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Northern Lights OC12</td>
<td>ipbsg</td>
<td>OC12</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OARNET CO-45</td>
<td>ipbsg</td>
<td>OC48</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OneNet</td>
<td>kscynq</td>
<td>OC12</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oregon Gigapop - Denver</td>
<td>drvmg</td>
<td>OC3</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oregon Gigapop - Sunnyvale</td>
<td>suwarg</td>
<td>OC3</td>
<td>9180</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pacific Northwest Gigapop</td>
<td>digital</td>
<td>10GigE</td>
<td>9000</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Visible Backbone Config

- There are two configuration files: `<your-net>.rtr` and `<your-net>.cmd`
- The .rtr file contains a list of routers to collect data from, the .cmd file a list of commands to execute.
Visible Backbone Config

- Finally, you supply the XML collector with a username and password to login to your router(s) with. Search for ‘login’ in xml-collector.pl and replace the ‘login’ and ‘password’ values.
Firewall Filter Visualization

- Collect, store, and graph time series data of counters from Juniper firewall filters
- Data collector, invoked via Cron, uses JUNOScript to collect firewall filter counters from a set of Juniper routers
- Aggregates per-interface counters on a per-router and per-network basis
- Displays sets of graphs on a series of web pages
Firewall Filter Visualization

Change View Options: Set common Y-Axis

Filter: connector-in → Counter: tcp-80

STTLng - Seattle, WA

WASHng - Washington, DC

CHINng - Chicago, IL

KSCYng - Kansas City, KS

IPLStg - Indianapolis, IN

ATLAng - Atlanta, GA

Device: iplng.abilene.uncid.edu Filter: connector-in Counter: tcp-80

gc-2/3/0.0 (input)

so-1/0/0.0 (input)

so-1/2/0.0 (input)

so-2/1/0.0 (input)

so-2/1/2.512 (input)

GigabitEthernet

OARNET oc48

University of Louisville oc3

Northern Lights OC12

Ment oc12

Ment
Firewall Filter Visualization

- All data stored in RRD files, RRDtool used to produce graphs
- In use on Abilene core nodes
- We have a filter applied inbound on connector interfaces, counting bits and packets matching a variety of protocols/ports
- We are also using firewall filters to collect IPv6 statistics
Network Information Database

• Repository for contact, equipment, circuit, monitoring, IP addressing, and topology data

• Relational database with a web based front-end

• Drives configuration of monitoring / measurement / management systems

• Various auto-population scripts talk to network devices, collecting data to affect database state

• Consolidates monitoring/measurement system configurations in one central repository
Organizational Entities

- Record details pertaining to an organizational entity as a whole
- Vendors, customers, internal contacts
- Each entity has one or more contacts associated with it.
- Entities also are associated with “agreements” (eg. membership agreement)
Contact Management:

- Contacts have an arbitrary number of “contact methods” such as ‘Office phone’, ‘email’, ‘cell phone’, etc.

- Contact methods are “time sensitive”

- Contacts may be associated with more than one entity
Nodes

- Node Management:
- Records “node” data, such as IP address, links to monitoring configuration, rack elevation, links to “devices” section containing physical hardware data, etc.
Devices

• “Devices” Management:

• Records attributes of physical devices such as serial number, slot number, hardware and software versions, device type, etc.

• Represented as a N-ary tree of arbitrary depth (e.g. Juniper T640 chassis is a “root” device with child “FPC2”, which in turn has children “OC192 PIC in slot 2/3/0” and “OC48 PIC in slot 2/3/1” )
Interface Data

- Manages data about physical and logical interfaces on a device.
- Records attributes such as IP addressing, interface identifier, speed, etc.
- Ties interfaces to entities
POPs

- Records POP facility owner, address, longitude/latitude, CLLI code, manned/unmanned status, etc.
- Linked to “node” section, showing nodes which reside in this POP location
- Linked to “rack” section, showing locations of bays inside the POP.
“POP Visits”

- Tracks who went to a site, when, and for what purpose
- Container for photographs taken during site visit
“Rack Data”

- Tracks physical rack attributes (width, # of rack units, etc.)
- Tracks position of equipment in racks / available empty space
- Uses SVG to draw a “rack diagram”
WDM Route Management

- Stores data about an optical system
- Path data
- Channel Allocation
- Channel Status
IP Address Management

- Represent IP allocation structure in the database
- Attach comments / “owners” to IP subnets
- Automatically make new allocations based on available space
IU Open Source License

• Many of our tools are licensed under the IU Open Source License.

• Very similar to the BSD license.

• You are free to use, modify, and distribute our code, subject to a few conditions.

• You must credit Indiana University when distributing our code, or derivative code.

• A full copy of the license is included with each tool.
SourceForge Projects

- Software Releases
- Discussion Forums
- Bug Reporting
- CVS Repositories

SourceForge links at http://tools.globalnoc.iu.edu/
That’s All Folks.....

Thanks!

http://tools.globalnoc.iu.edu/