NMIS8 User Training

January 2013
Keith Sinclair, keiths@opmantek.com

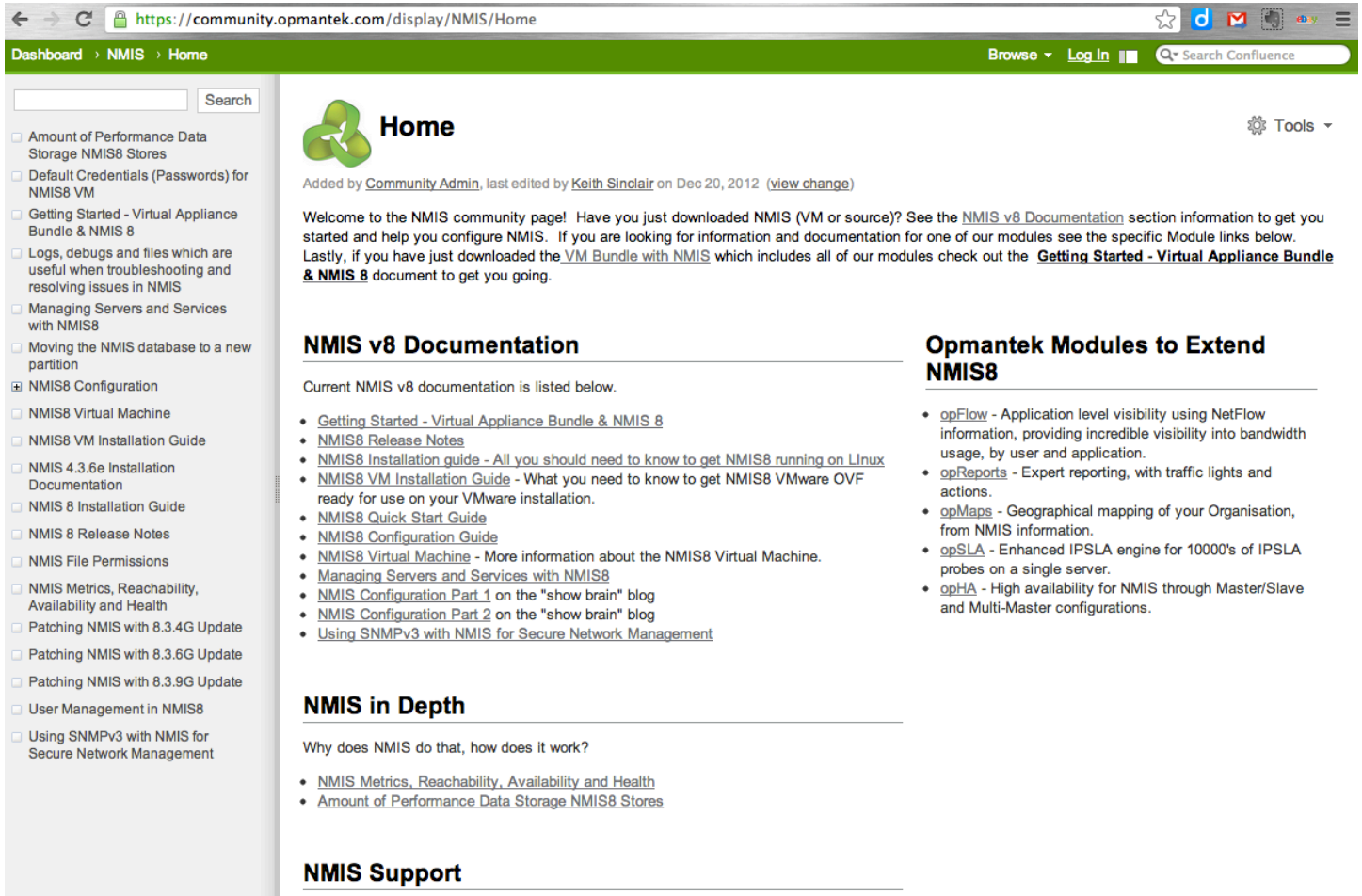
User Training Agenda

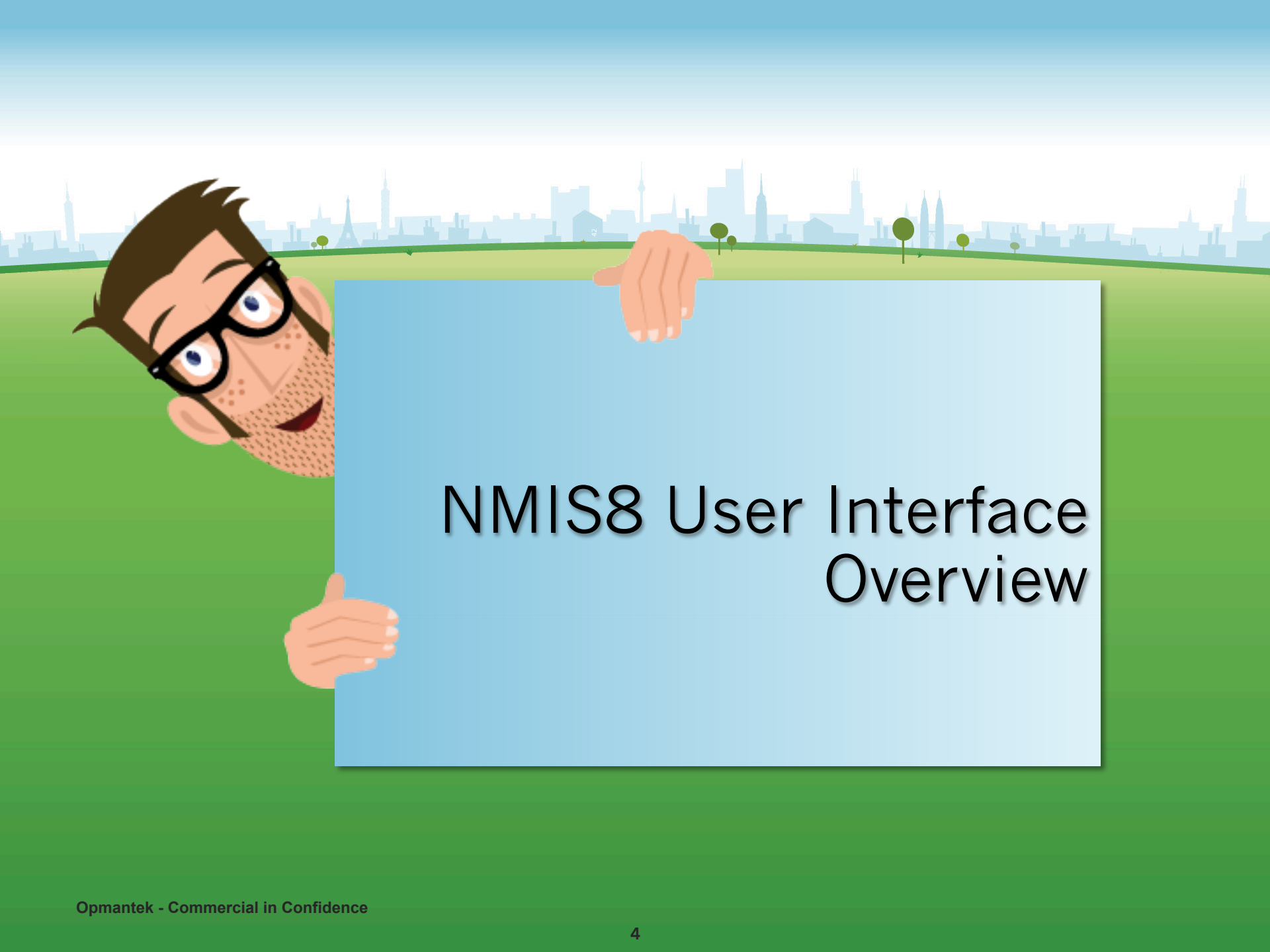
Time	Session
1 hour	NMIS User Interface Overview
1 hour	Managing Nodes (devices) in NMIS. Adding and deleting devices and groups in NMIS8
1 hour	Incident Scenarios and NMIS Visibility (what happens when things break and how will it look in NMIS8)

Opmantek Community Wiki

- Access all available documentation at the Opmantek Community Wiki. https://community.opmantek.com

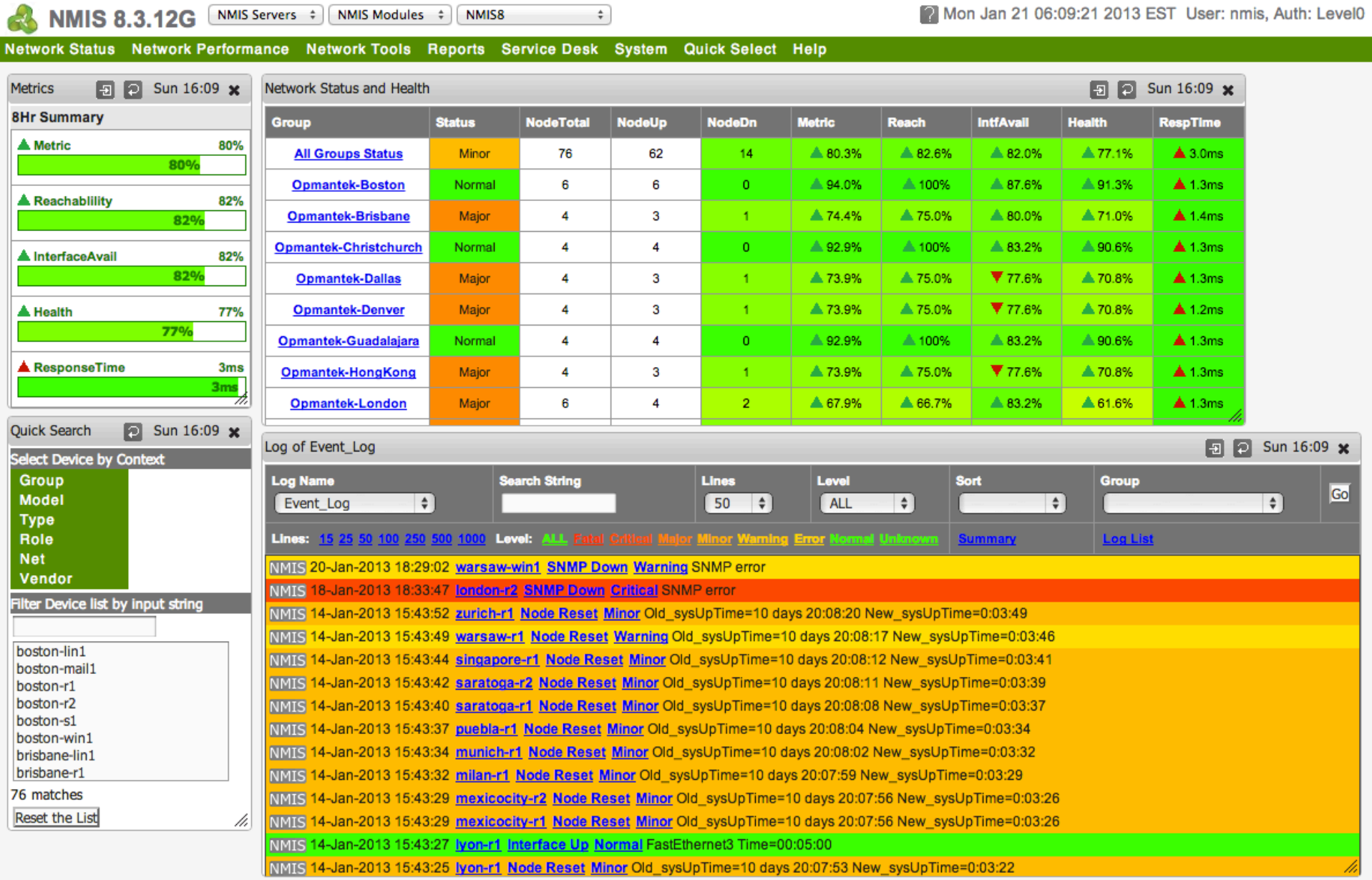
- Register @ https://opmantek.com "Join Community" top right.



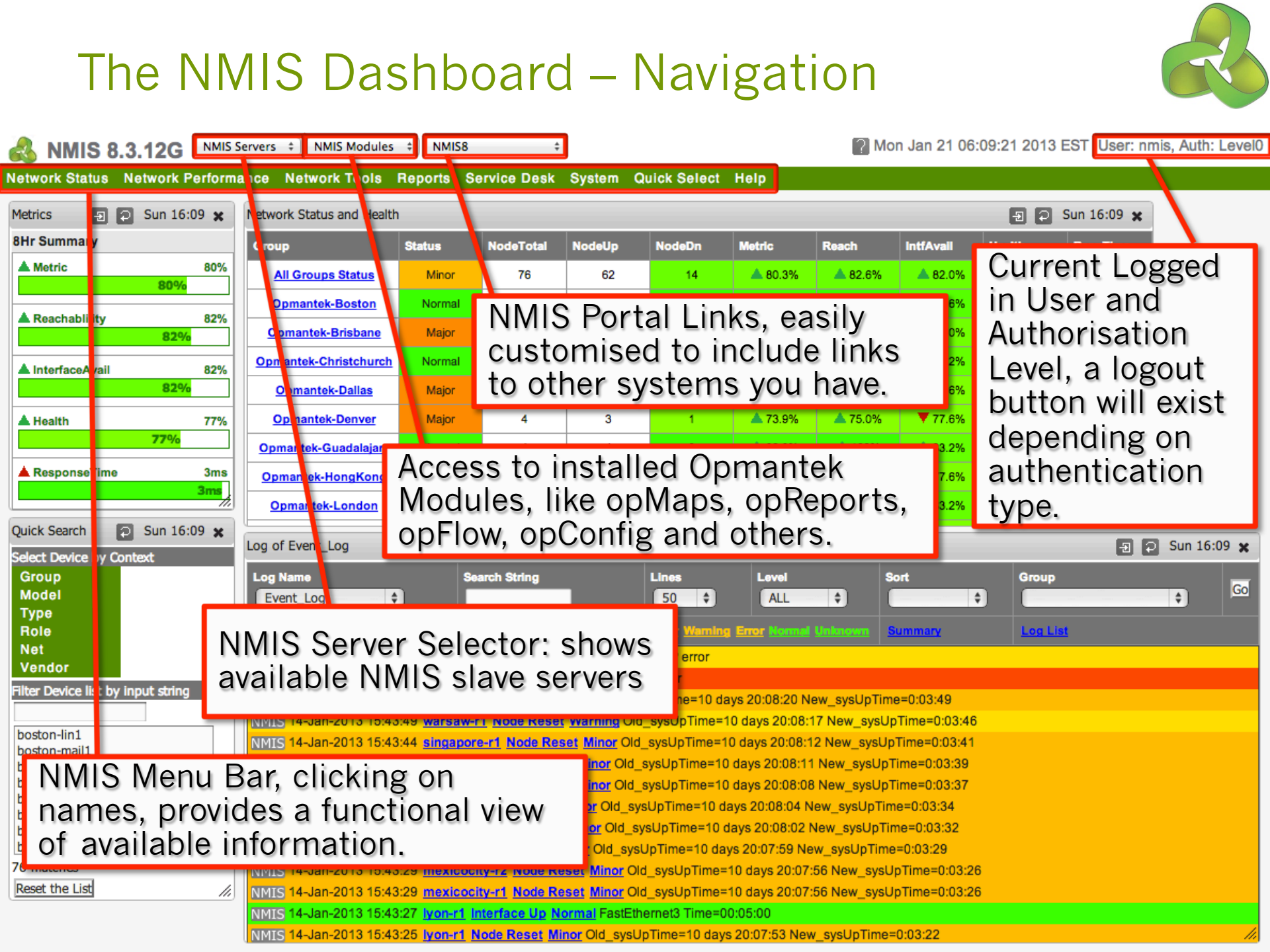

NMIS8 User Interface
Overview

The NMIS Dashboard

http://server_name_or_ip/cgi-nmis8/nmiscgi.pl



The NMIS Dashboard – Navigation



NMIS Portal Links, easily customised to include links to other systems you have.

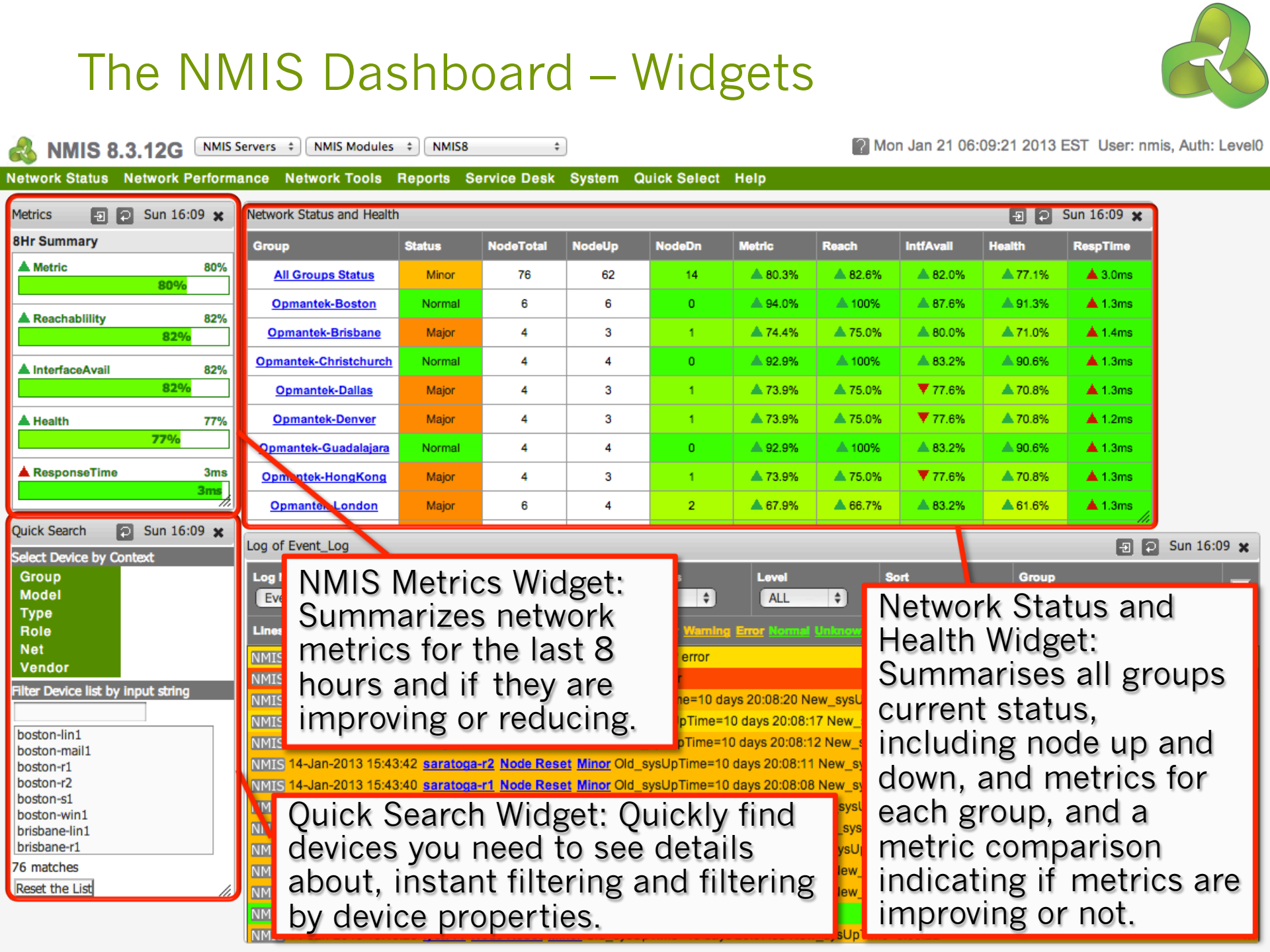
Current Logged in User and Authorisation Level, a logout button will exist depending on authentication type.

Access to installed Opmantek Modules, like opMaps, opReports, opFlow, opConfig and others.

NMIS Server Selector: shows available NMIS slave servers

NMIS Menu Bar, clicking on names, provides a functional view of available information.

The NMIS Dashboard – Widgets

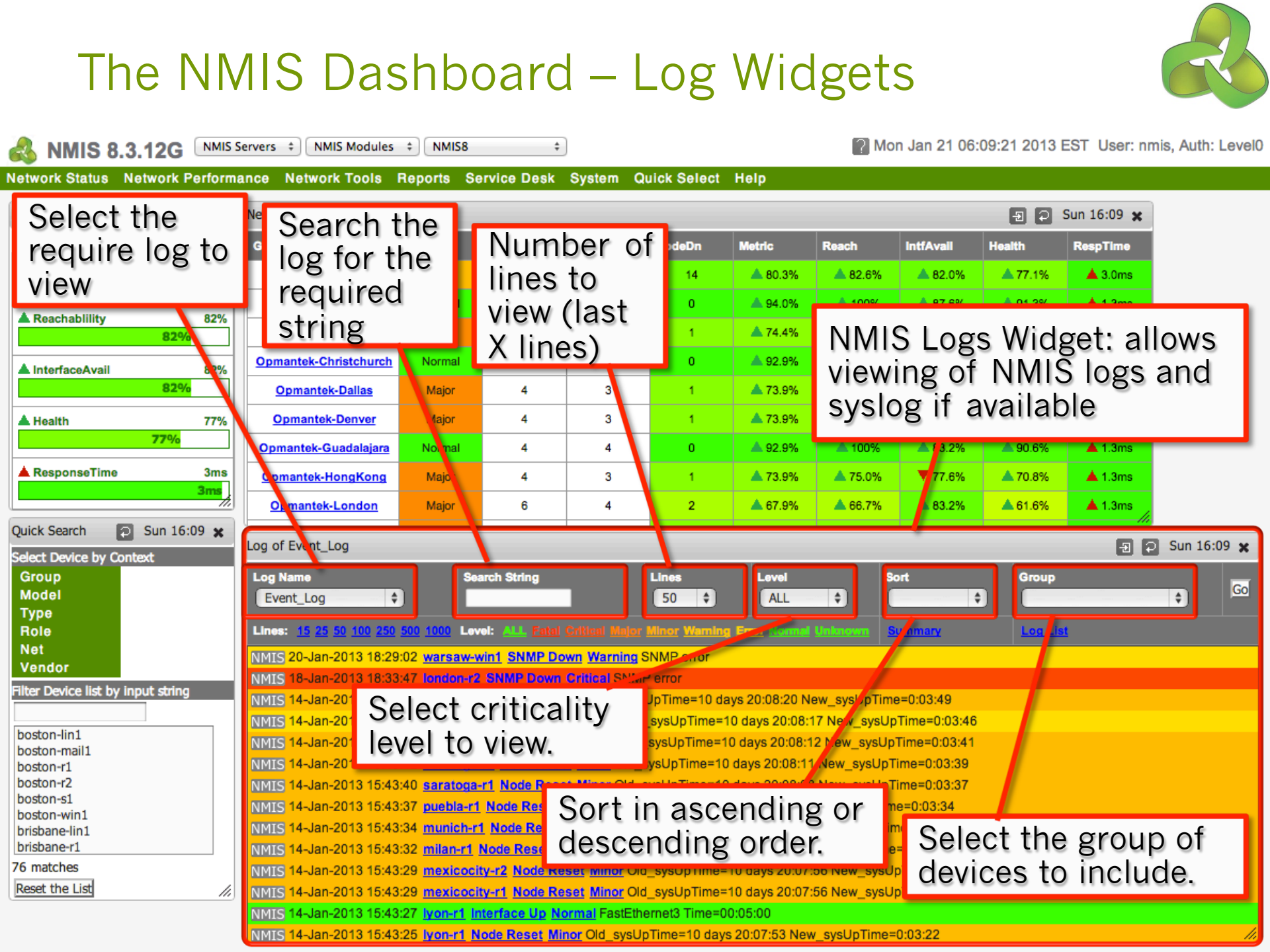


NMIS Metrics Widget: Summarizes network metrics for the last 8 hours and if they are improving or reducing.

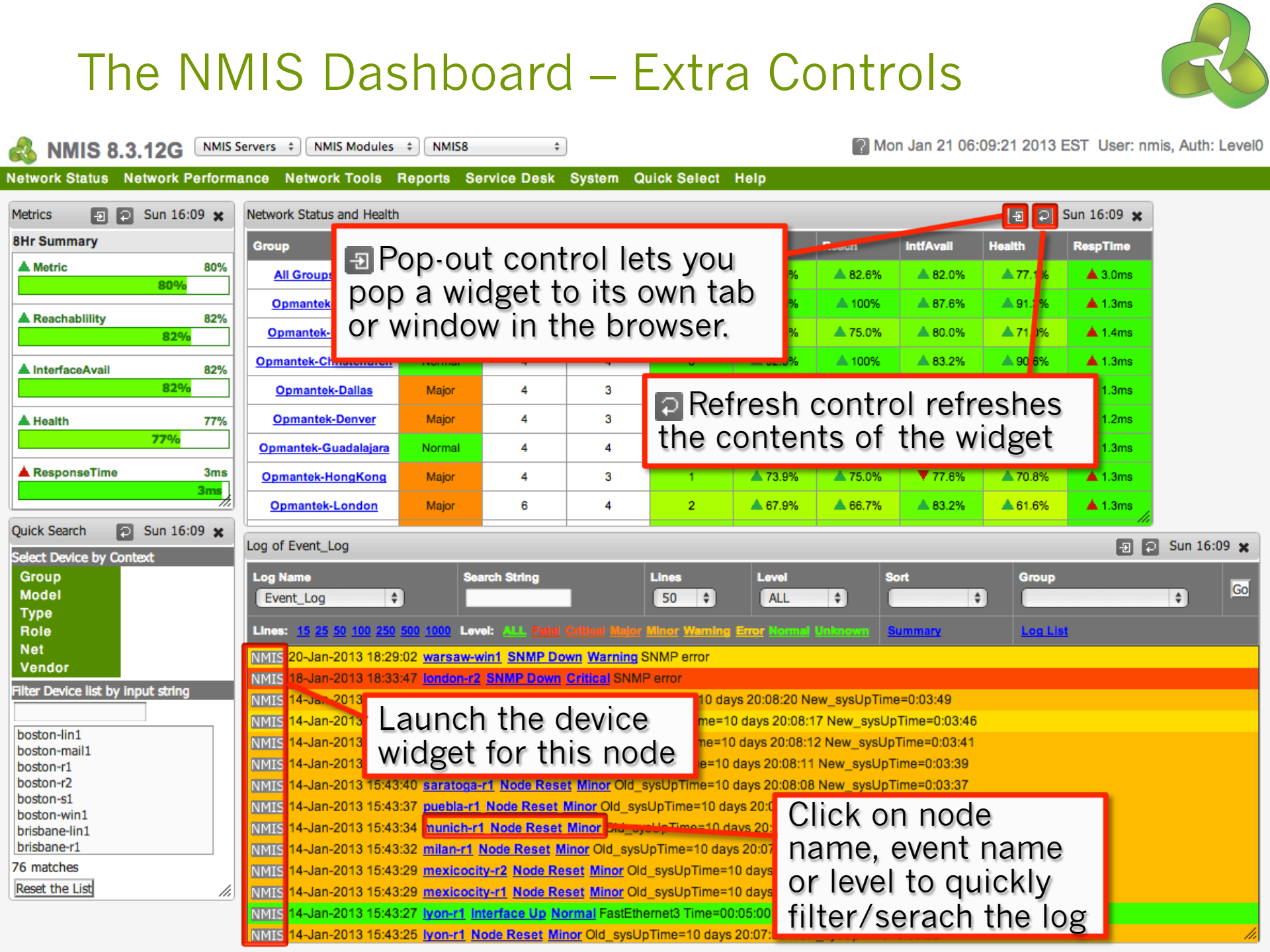
Quick Search Widget: Quickly find devices you need to see details about, instant filtering and filtering by device properties.

Network Status and Health Widget: Summarises all groups current status, including node up and down, and metrics for each group, and a metric comparison indicating if metrics are improving or not.

The NMIS Dashboard – Log Widgets

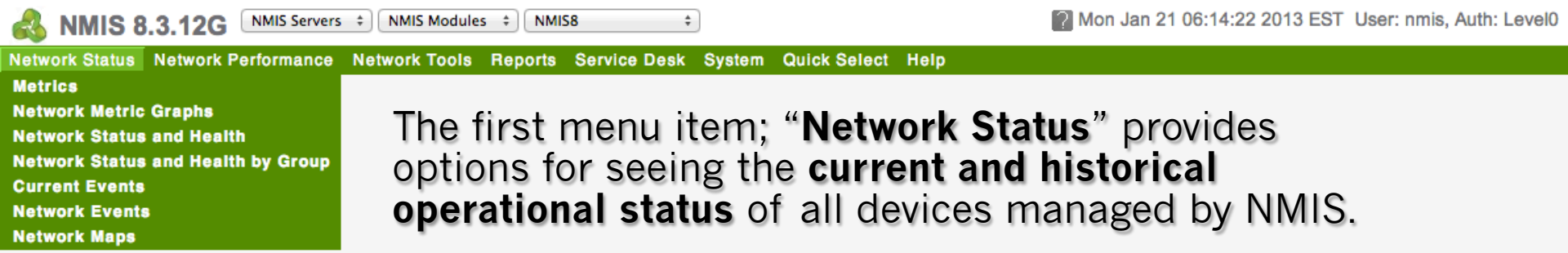


The NMIS Dashboard – Extra Controls

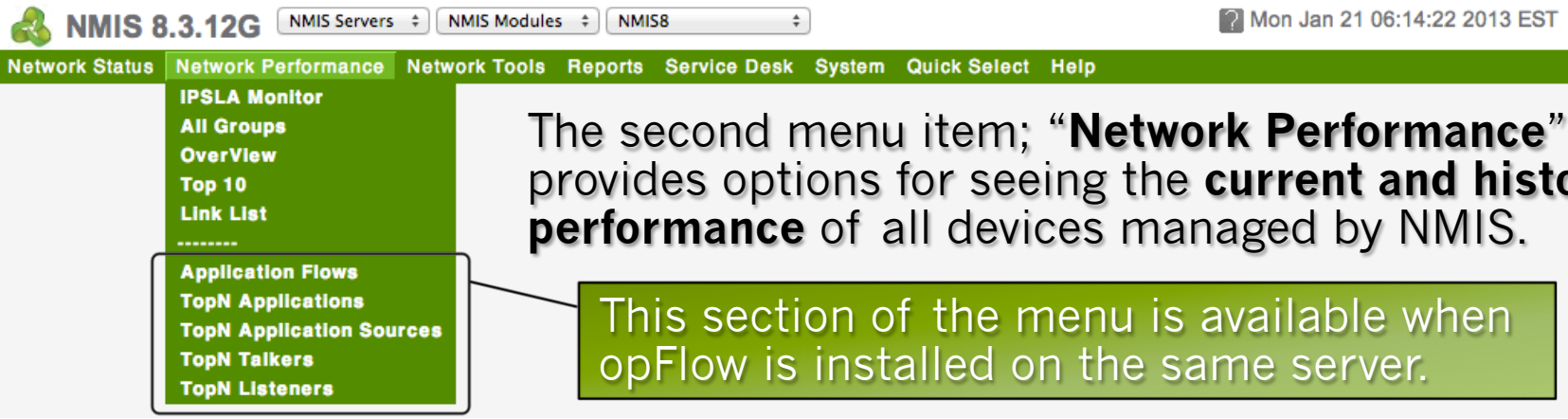


NMIS Menu Summary

NMIS Primary Menu Options

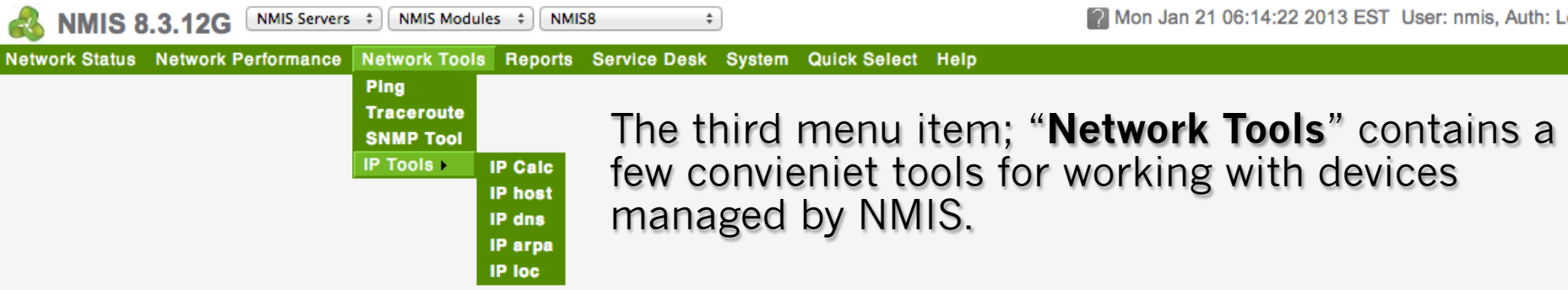


The first menu item; "**Network Status**" provides options for seeing the **current and historical operational status** of all devices managed by NMIS.



The second menu item; "**Network Performance**" provides options for seeing the **current and historical performance** of all devices managed by NMIS.

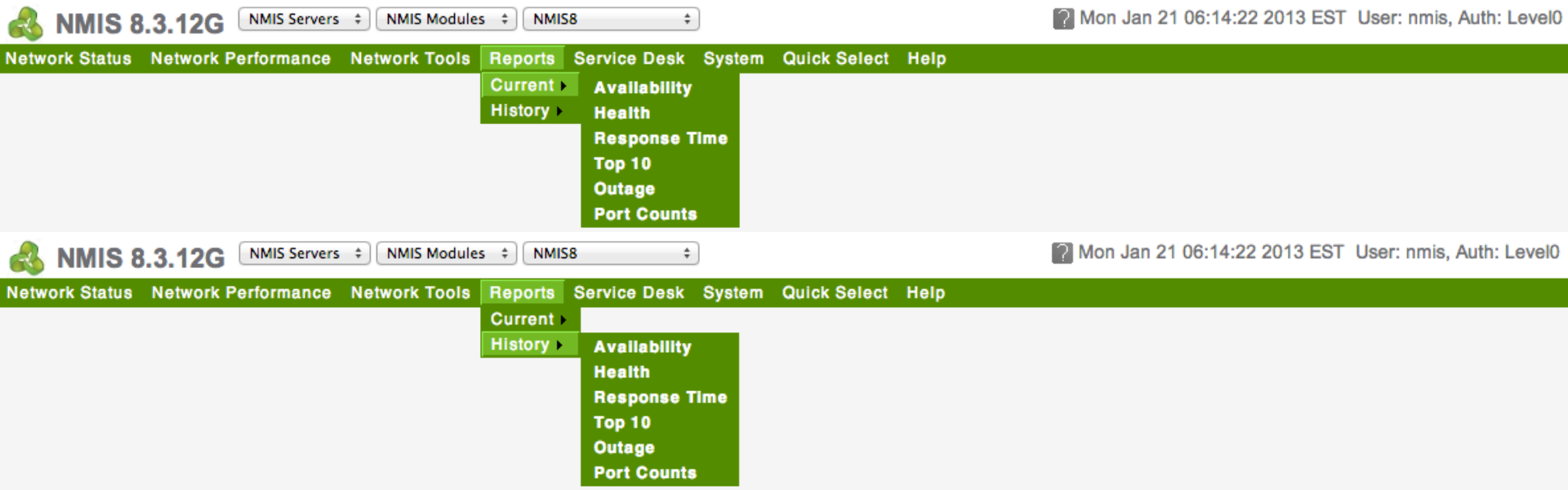
This section of the menu is available when opFlow is installed on the same server.



The third menu item; "**Network Tools**" contains a few convieniet tools for working with devices managed by NMIS.

NMIS Report Menu

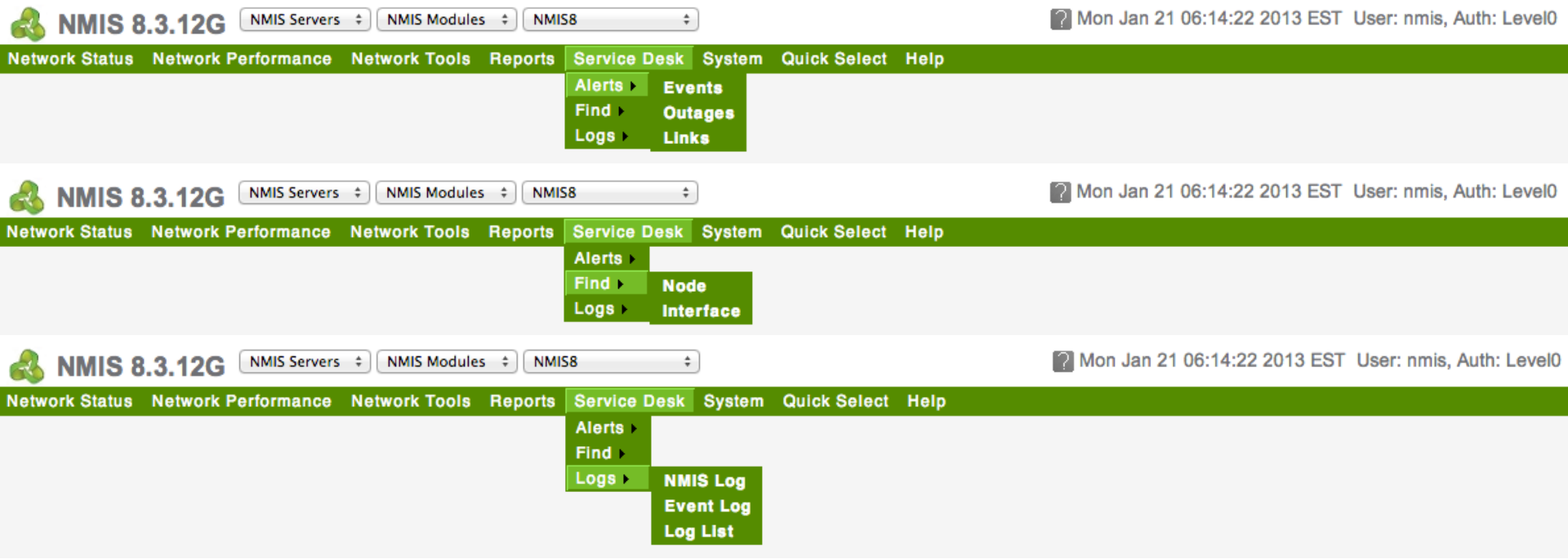
The forth menu item; "**Reports**" provides access to generate reports now and historically, these are through the options "**Current**" and "**History**".



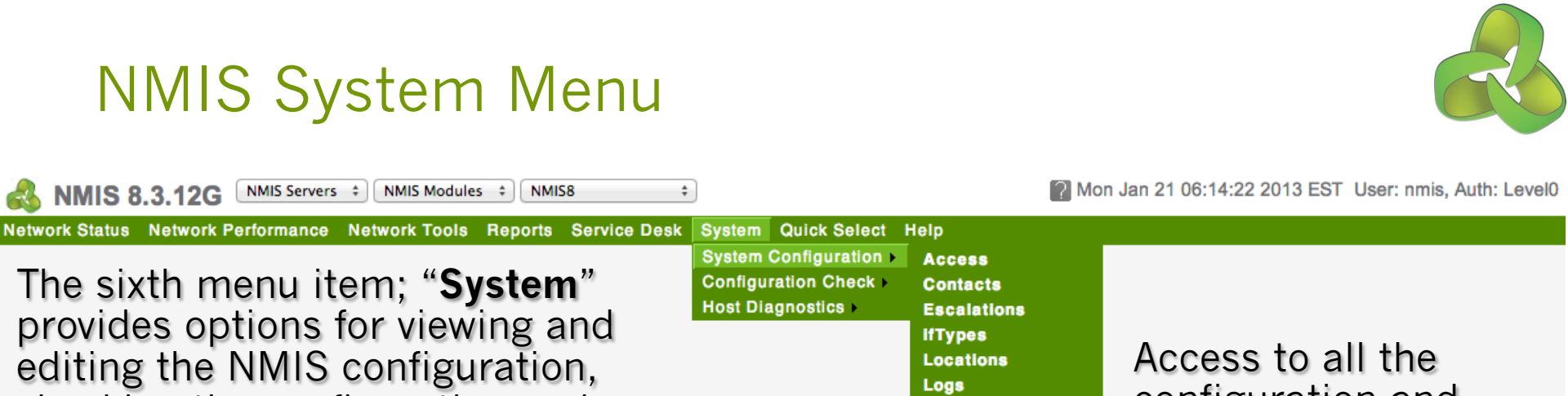
Report Name	Description
Availability	Summarises the availability of all devices for the reporting period
Health	Summarises the health of all devices
Response Time	Summarises the response of all devices
Top 10	Finds the Top10 devices in several categories, the busy devices.
Outage	Shows all the outages for node or interface in the reporting period
Port Counts	Summarises available ports (interfaces), available physical capacity

NMIS Service Desk Menu

The fifth menu item; "**Service Desk**" includes options for seeing alerting, finding elements and viewing logs.

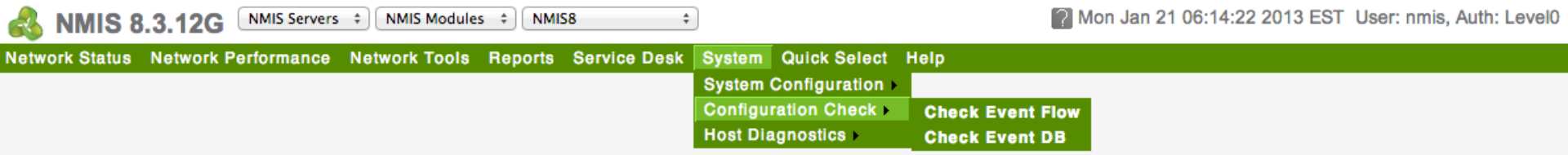


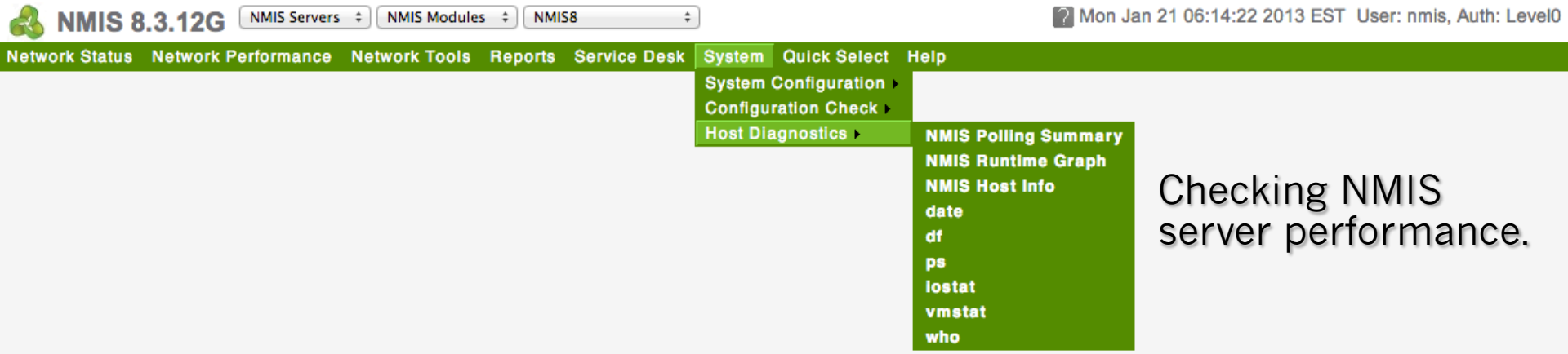
NMIS System Menu



The sixth menu item; "**System**" provides options for viewing and editing the NMIS configuration, checking the configuration and checking NMIS server performance.

Access to all the configuration and policy files.



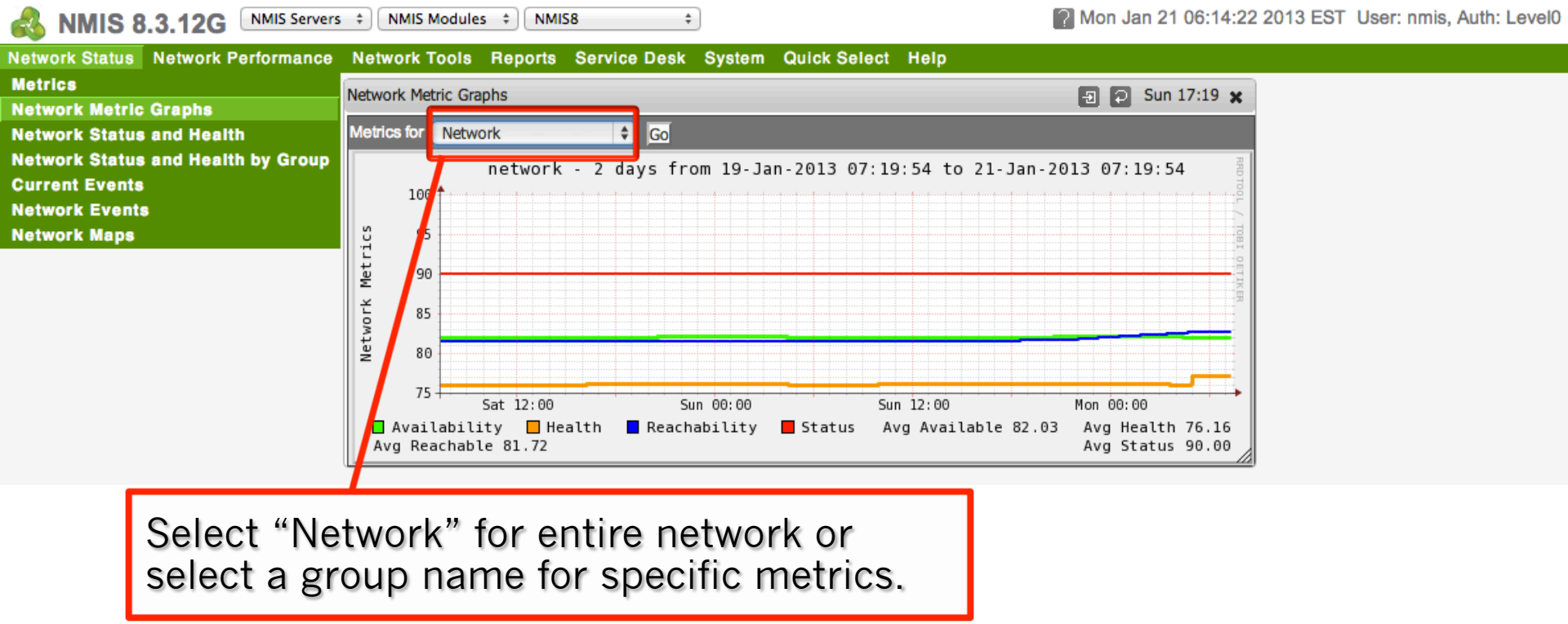


Checking NMIS server performance.

NMIS Menu Drill Down

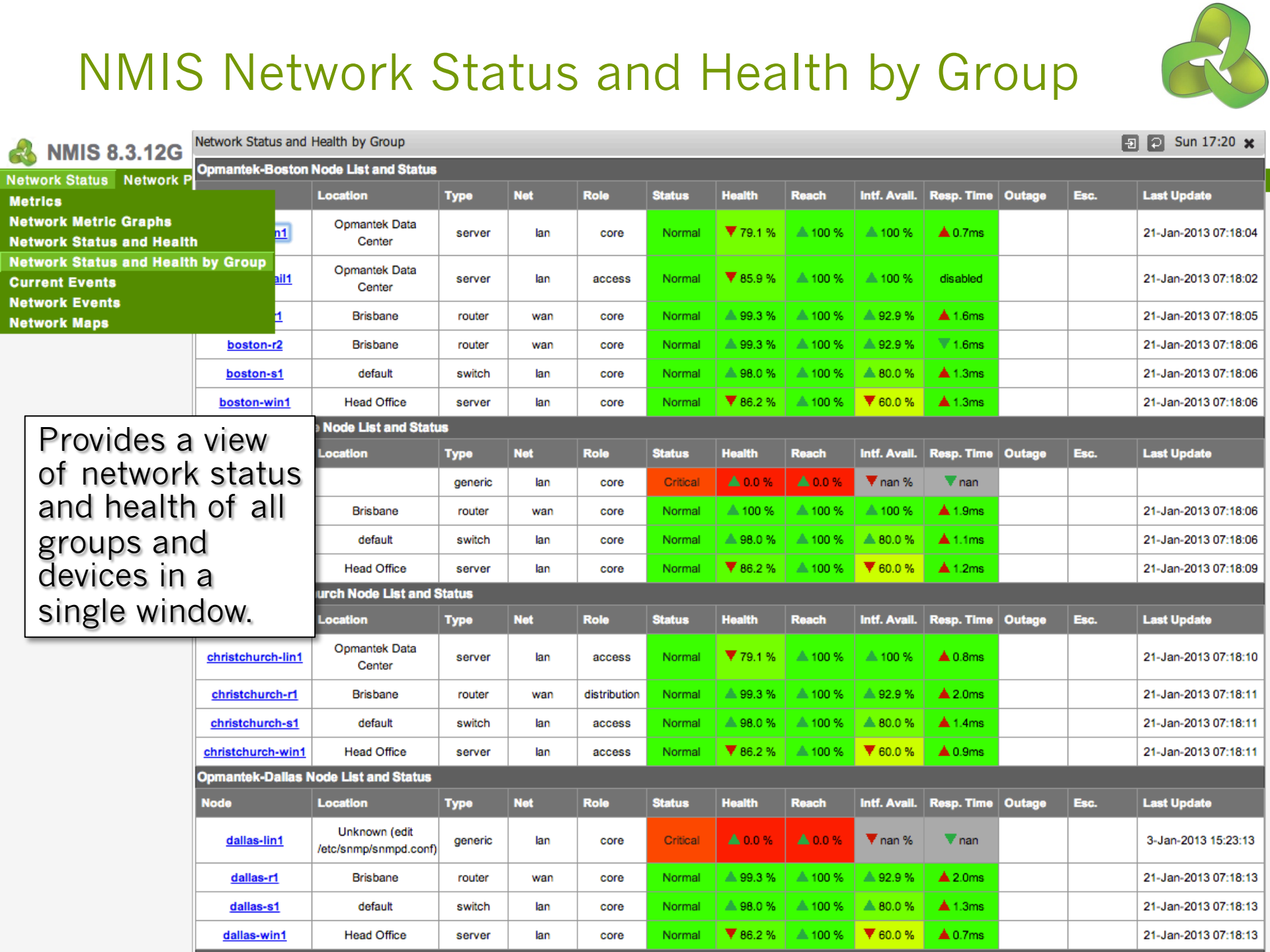
NMIS Network Metric Graphs

The menu item “Network Status -> Network Metric Graphs” provides access to seeing the NMIS metrics, availability, health, reachability and status over time.



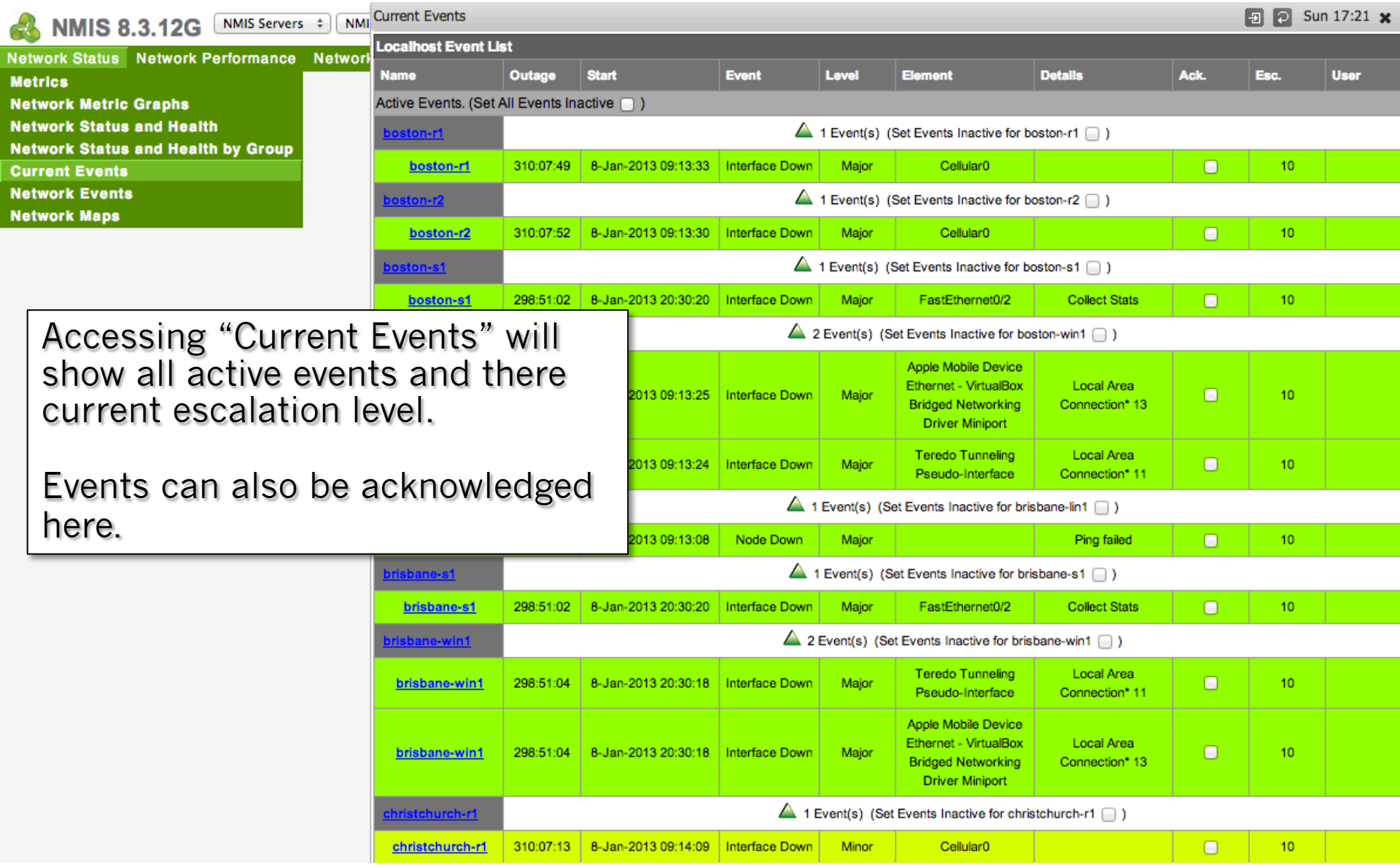
Select “Network” for entire network or select a group name for specific metrics.

NMIS Network Status and Health by Group



Provides a view of network status and health of all groups and devices in a single window.

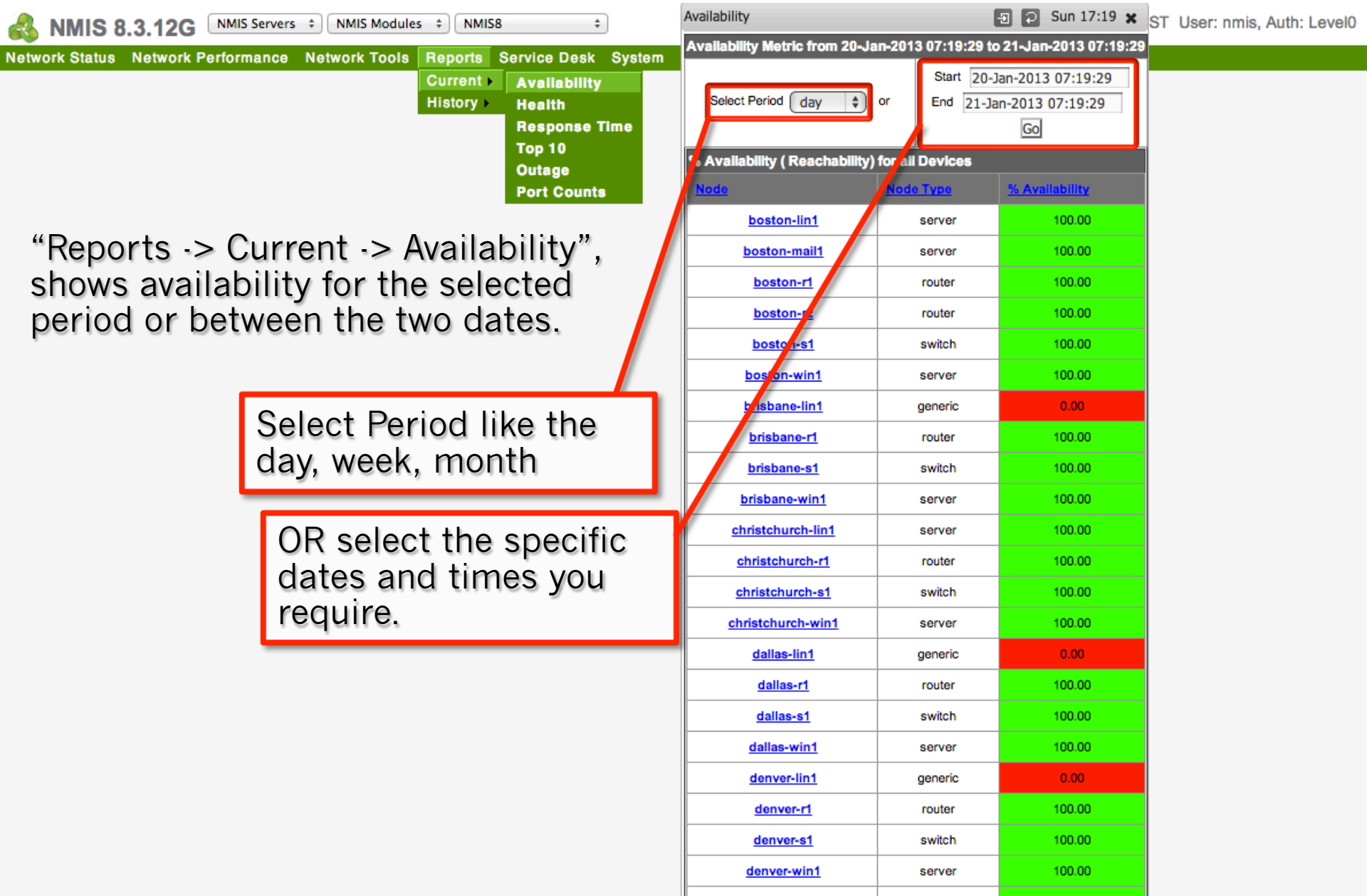
NMIS Current Events



Accessing “Current Events” will show all active events and there current escalation level.

Events can also be acknowledged here.

NMIS Reports – Availability

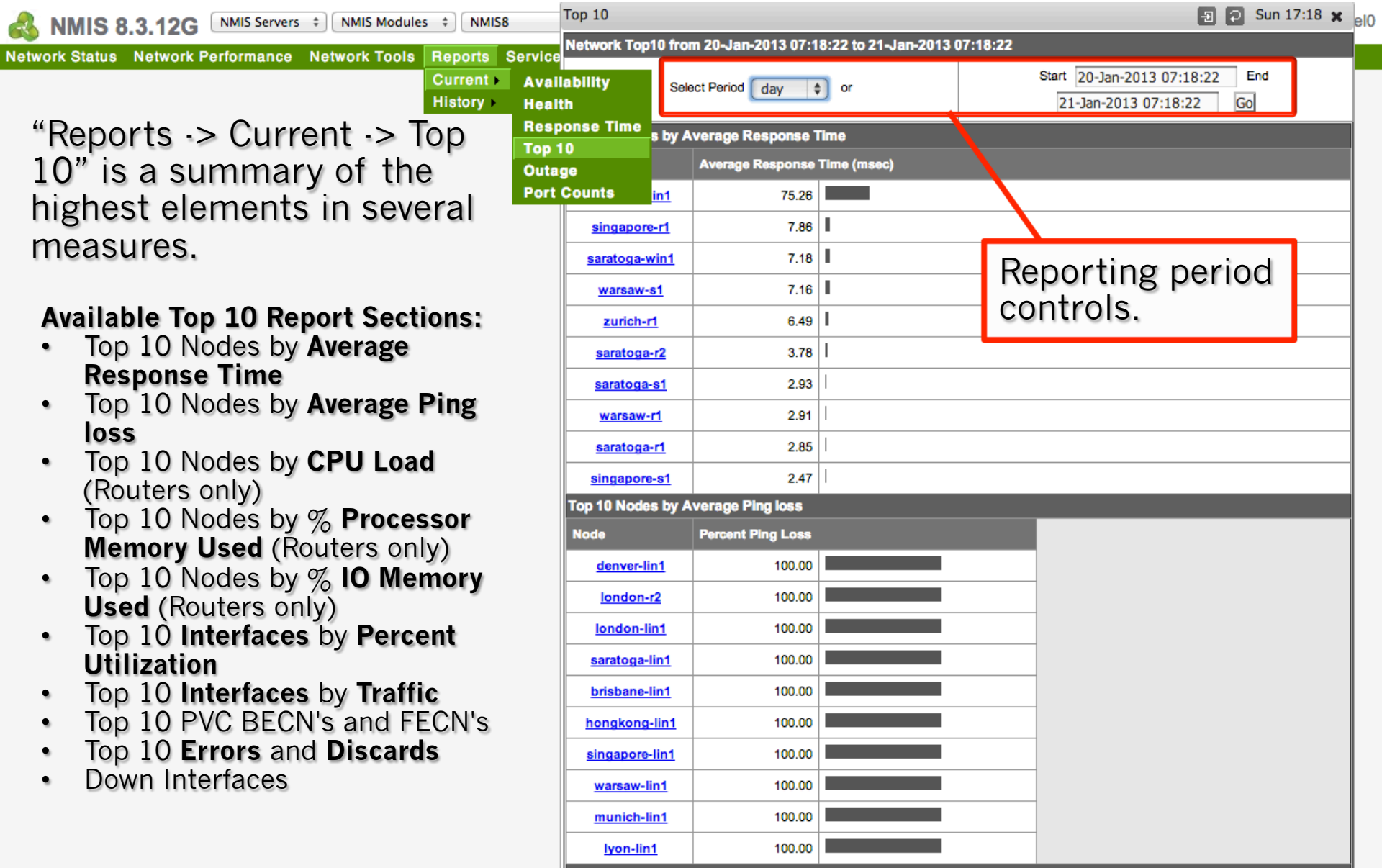


"Reports -> Current -> Availability", shows availability for the selected period or between the two dates.

Select Period like the day, week, month

OR select the specific dates and times you require.

NMIS Reports – Top 10

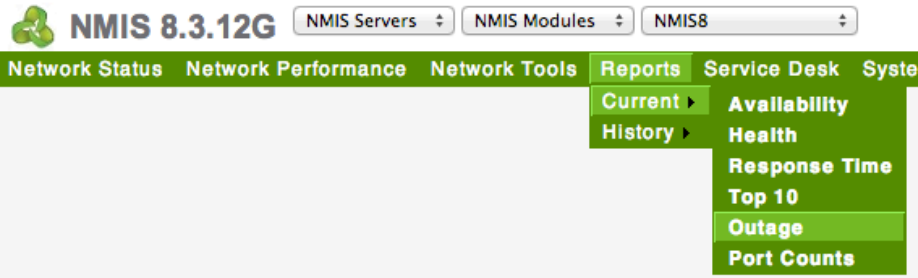


"Reports -> Current -> Top 10" is a summary of the highest elements in several measures.

Available Top 10 Report Sections:

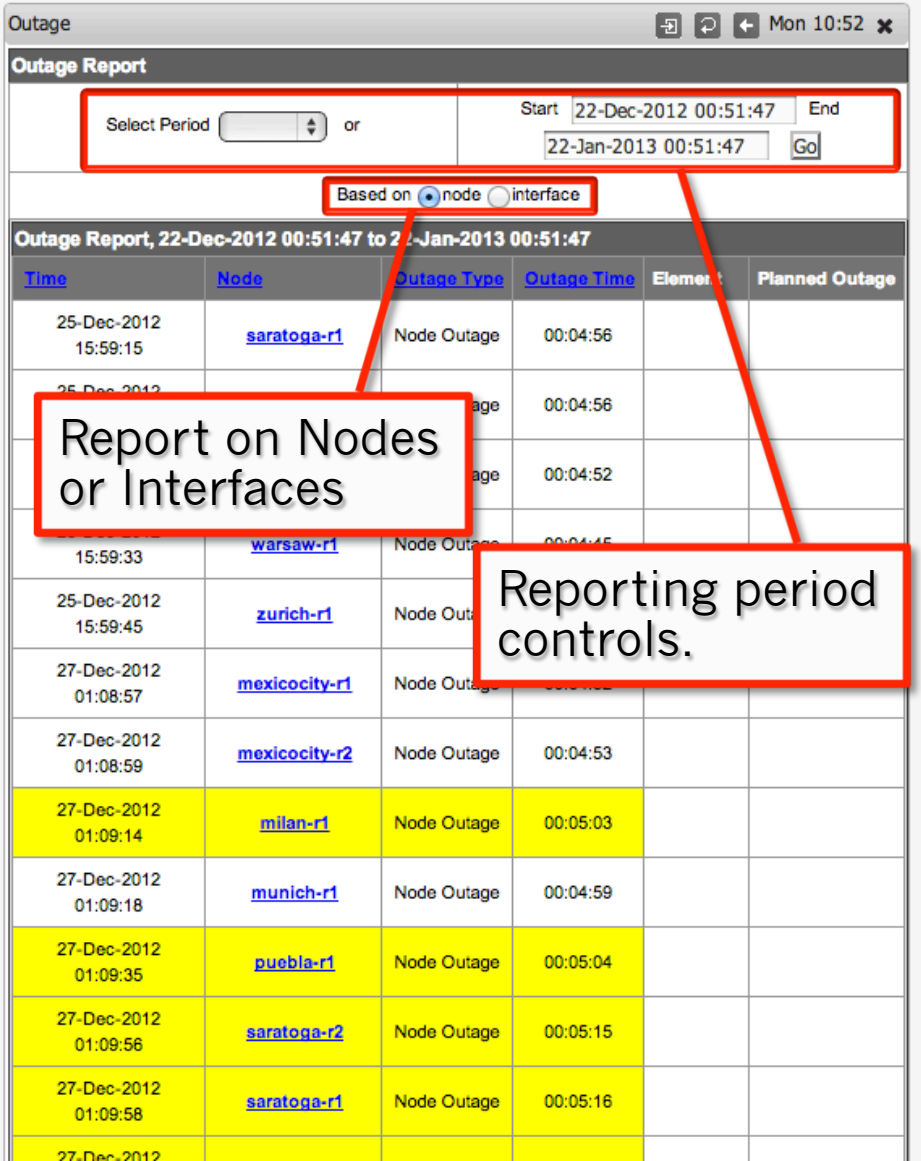
- Top 10 Nodes by **Average Response Time**
- Top 10 Nodes by **Average Ping loss**
- Top 10 Nodes by **CPU Load** (Routers only)
- Top 10 Nodes by % **Processor Memory Used** (Routers only)
- Top 10 Nodes by % **IO Memory Used** (Routers only)
- Top 10 **Interfaces** by **Percent Utilization**
- Top 10 **Interfaces** by **Traffic**
- Top 10 PVC BECN's and FECN's
- Top 10 **Errors** and **Discards**
- Down Interfaces

NMIS Reports – Outage

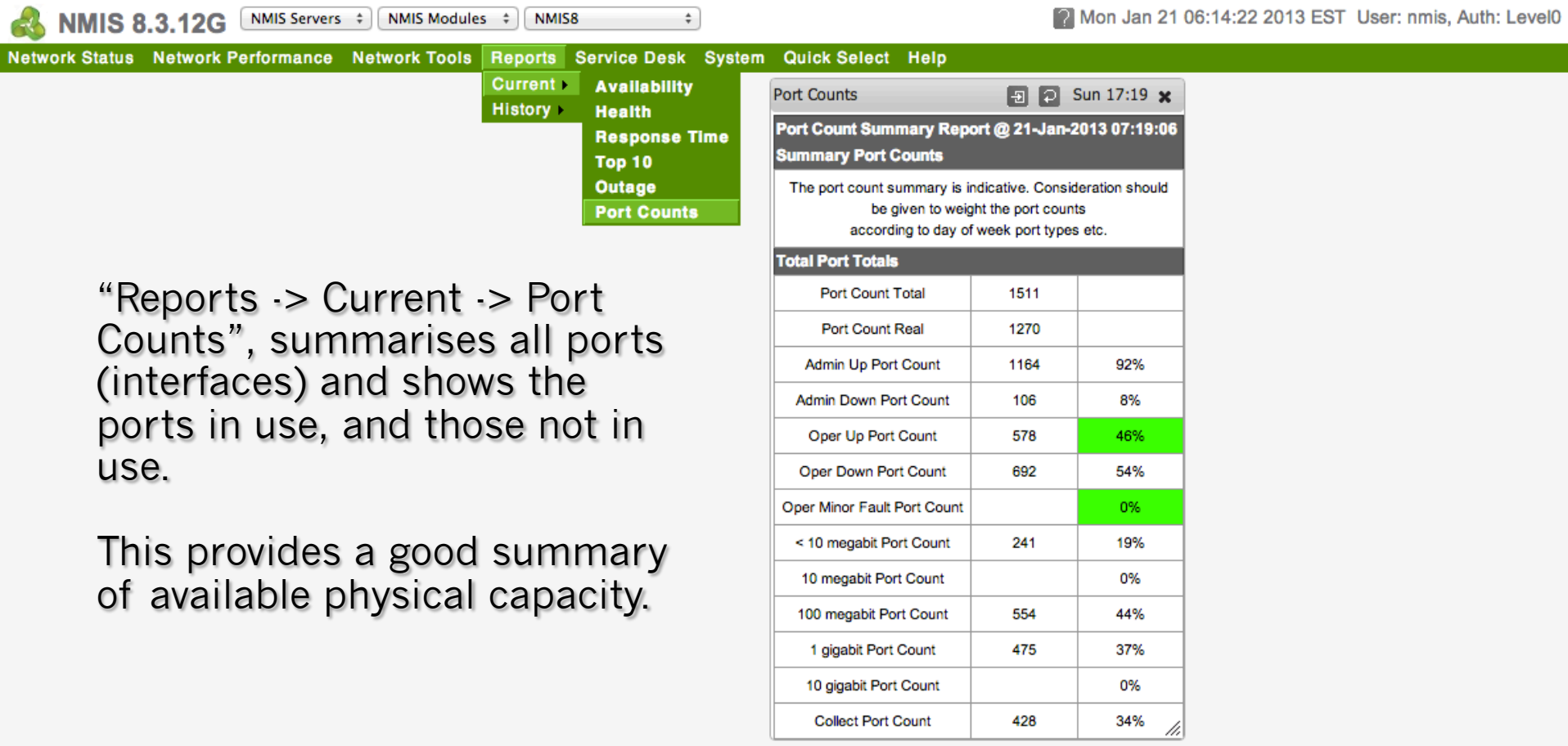


"Reports -> Current -> Outage" Provides a summary of all the elements which were down during the selected period.

Report can be for nodes or interfaces.



NMIS Reports – Port Counts



"Reports -> Current -> Port Counts", summarises all ports (interfaces) and shows the ports in use, and those not in use.

This provides a good summary of available physical capacity.

NMIS Device Screens

NMIS Node Widget

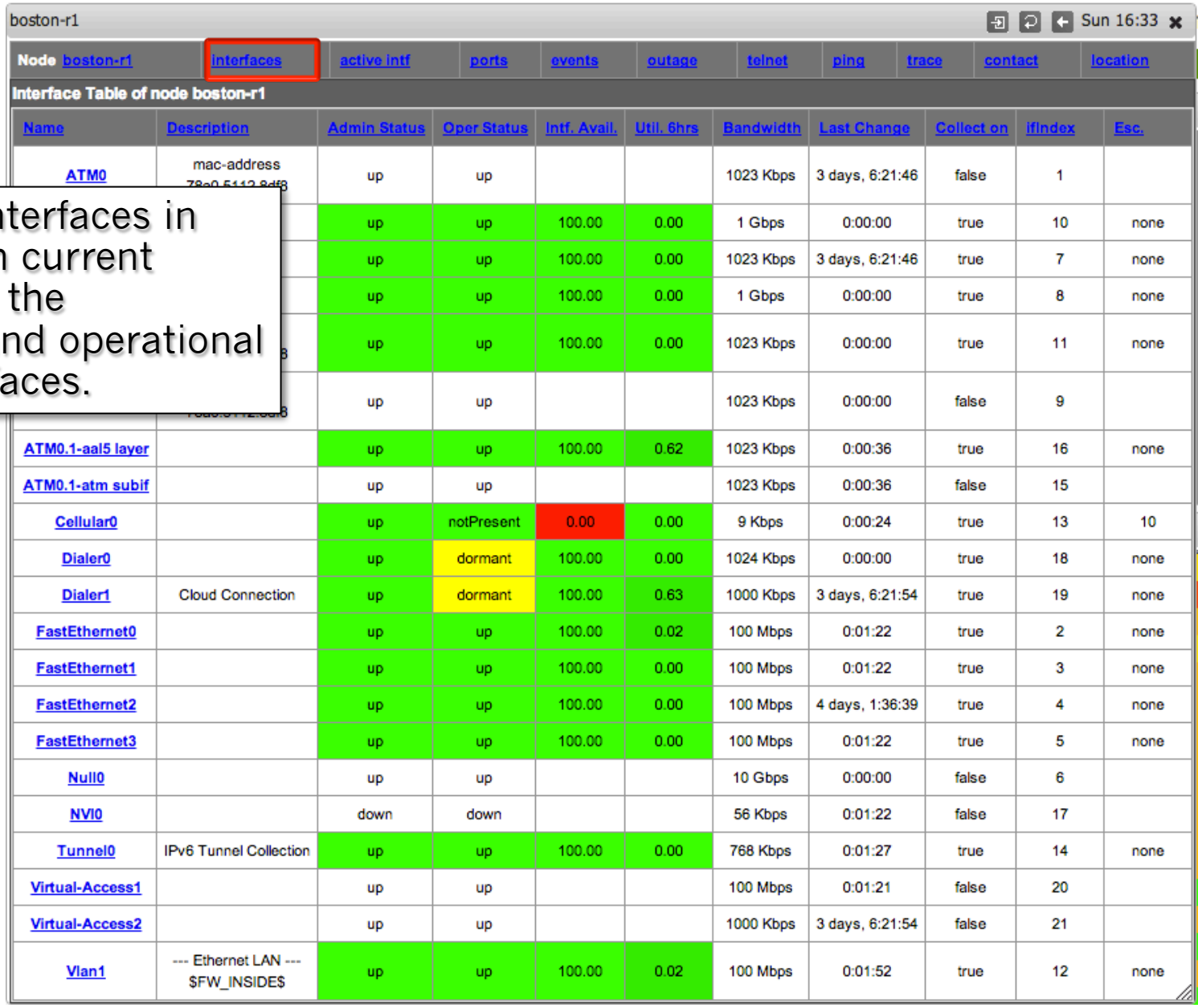
Node menu with available node/ device views

Summary of node node information.

Available node level graphs

Node Widget: Interfaces

A table of all interfaces in the device, with current information on the configuration and operational status of interfaces.



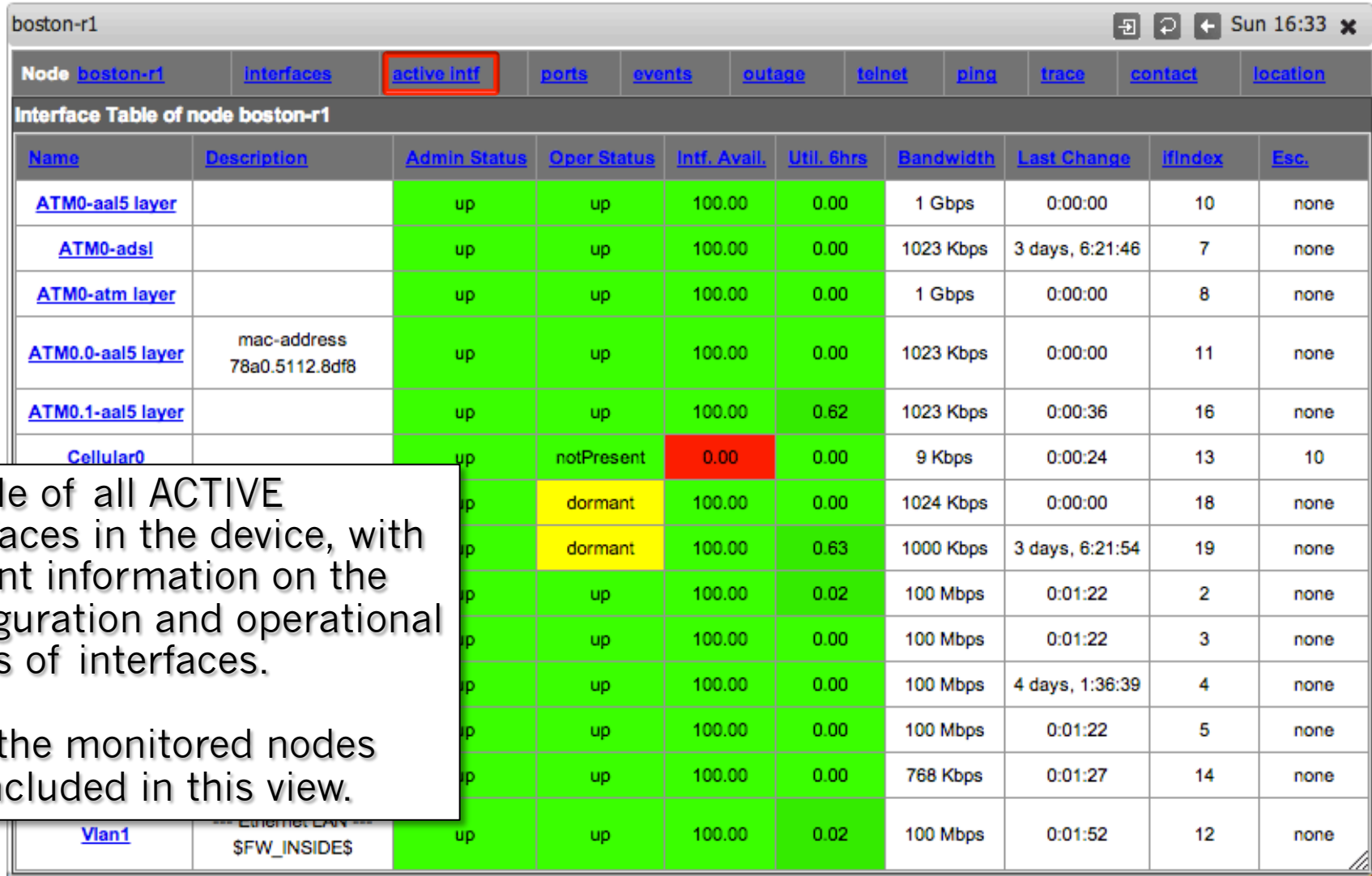
boston-r1 — Sun 16:33

Node boston-r1 | interfaces | active intf | ports | events | outage | telnet | ping | trace | contact | location

Interface Table of node boston-r1

Name	Description	Admin Status	Oper Status	Intf. Avail.	Util. 6hrs	Bandwidth	Last Change	Collect on	ifIndex	Esc.
ATM0	mac-address	up	up			1023 Kbps	3 days, 6:21:46	false	1	
		up	up	100.00	0.00	1 Gbps	0:00:00	true	10	none
		up	up	100.00	0.00	1023 Kbps	3 days, 6:21:46	true	7	none
		up	up	100.00	0.00	1 Gbps	0:00:00	true	8	none
		up	up	100.00	0.00	1023 Kbps	0:00:00	true	11	none
		up	up			1023 Kbps	0:00:00	false	9	
ATM0.1-aal5 layer		up	up	100.00	0.62	1023 Kbps	0:00:36	true	16	none
ATM0.1-atm subif		up	up			1023 Kbps	0:00:36	false	15	
Cellular0		up	notPresent	0.00	0.00	9 Kbps	0:00:24	true	13	10
Dialer0		up	dormant	100.00	0.00	1024 Kbps	0:00:00	true	18	none
Dialer1	Cloud Connection	up	dormant	100.00	0.63	1000 Kbps	3 days, 6:21:54	true	19	none
FastEthernet0		up	up	100.00	0.02	100 Mbps	0:01:22	true	2	none
FastEthernet1		up	up	100.00	0.00	100 Mbps	0:01:22	true	3	none
FastEthernet2		up	up	100.00	0.00	100 Mbps	4 days, 1:36:39	true	4	none
FastEthernet3		up	up	100.00	0.00	100 Mbps	0:01:22	true	5	none
Null0		up	up			10 Gbps	0:00:00	false	6	
NVI0		down	down			56 Kbps	0:01:22	false	17	
Tunnel0	IPv6 Tunnel Collection	up	up	100.00	0.00	768 Kbps	0:01:27	true	14	none
Virtual-Access1		up	up			100 Mbps	0:01:21	false	20	
Virtual-Access2		up	up			1000 Kbps	3 days, 6:21:54	false	21	
Vlan1	--- Ethernet LAN --- FW_INSIDE	up	up	100.00	0.02	100 Mbps	0:01:52	true	12	none

Node Widget: Active Interfaces



A table of all ACTIVE interfaces in the device, with current information on the configuration and operational status of interfaces.

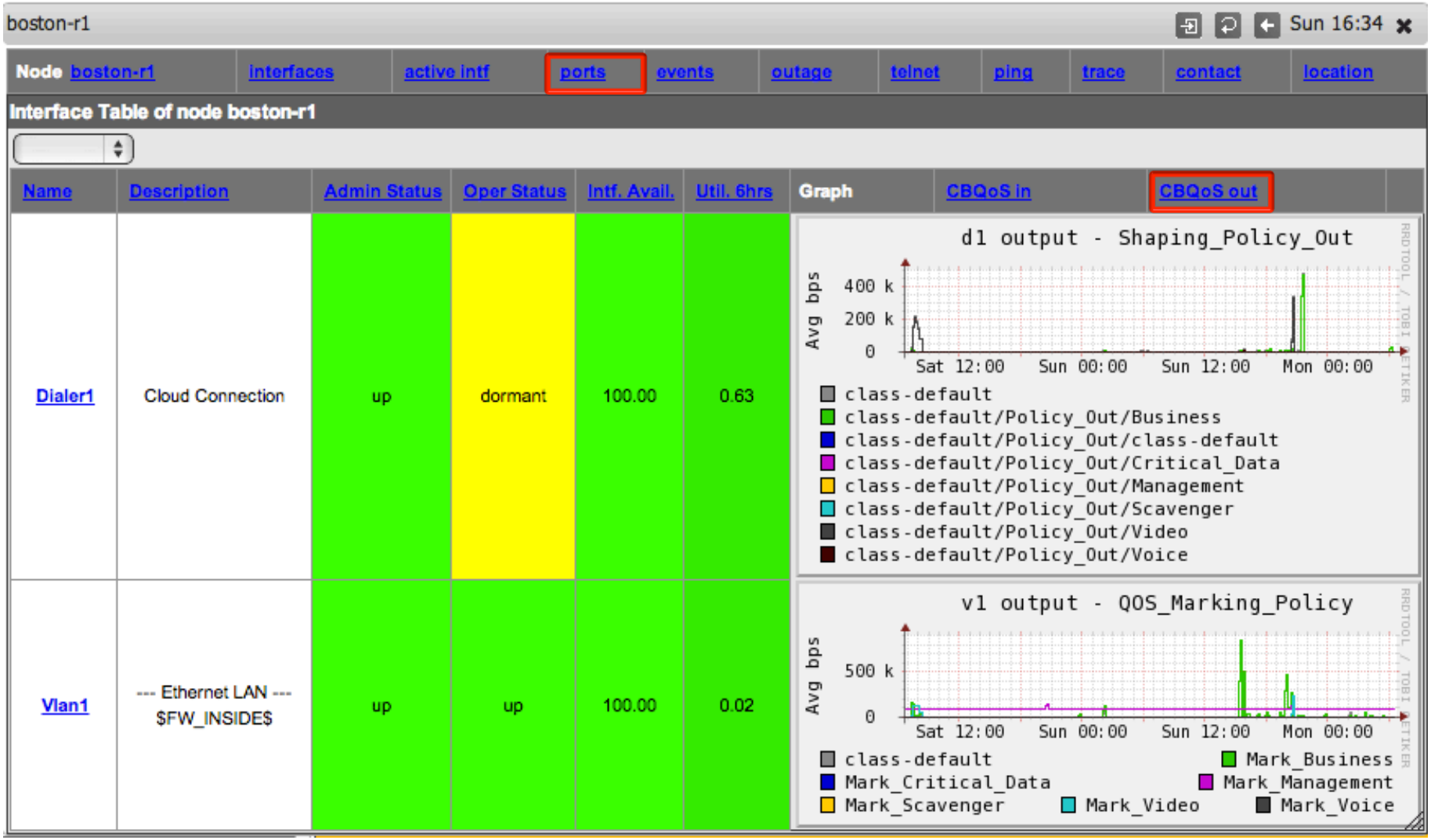
Only the monitored nodes are included in this view.

Node Widget: Ports

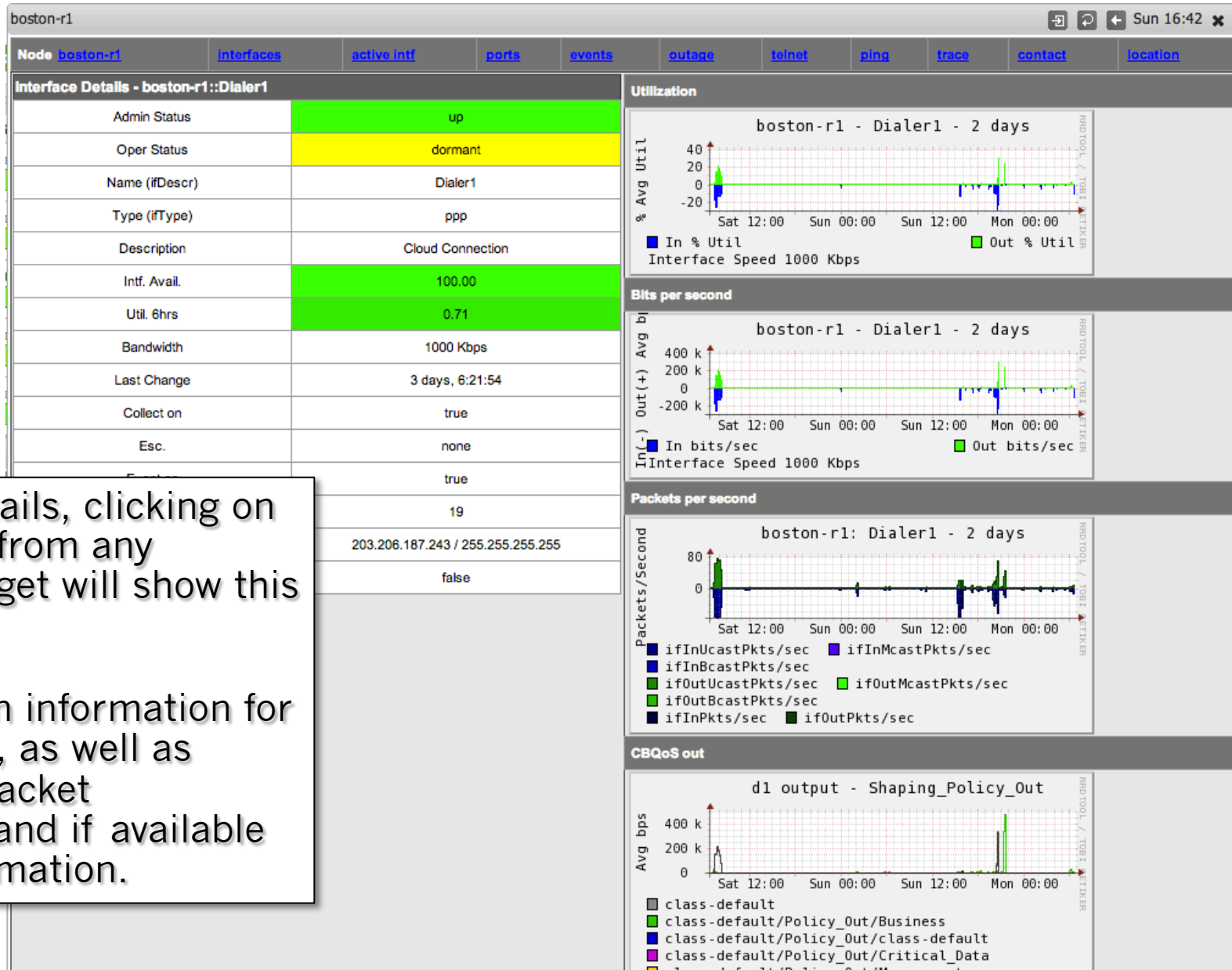
The port view shows a small graph for each interface being collected, very handy for comparing where traffic is coming from and going to.

Controls included to view different graphs and CBQoS if required.

Node Widget: Ports -> CBQoS



Node Widget: Interface Details

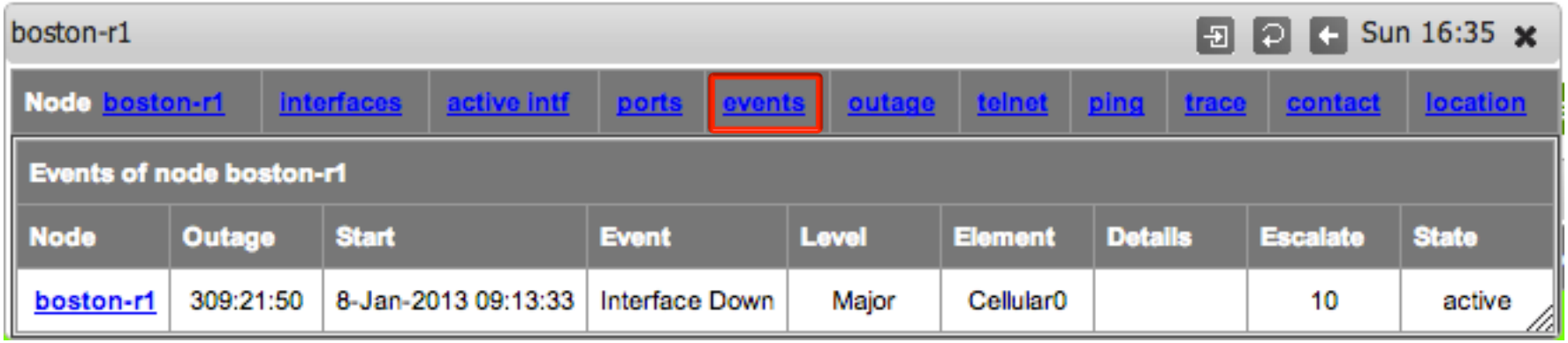


Interface details, clicking on an interface from any previous widget will show this information.

Configuration information for the interface, as well as utilisation, packet information and if available CBQoS information.

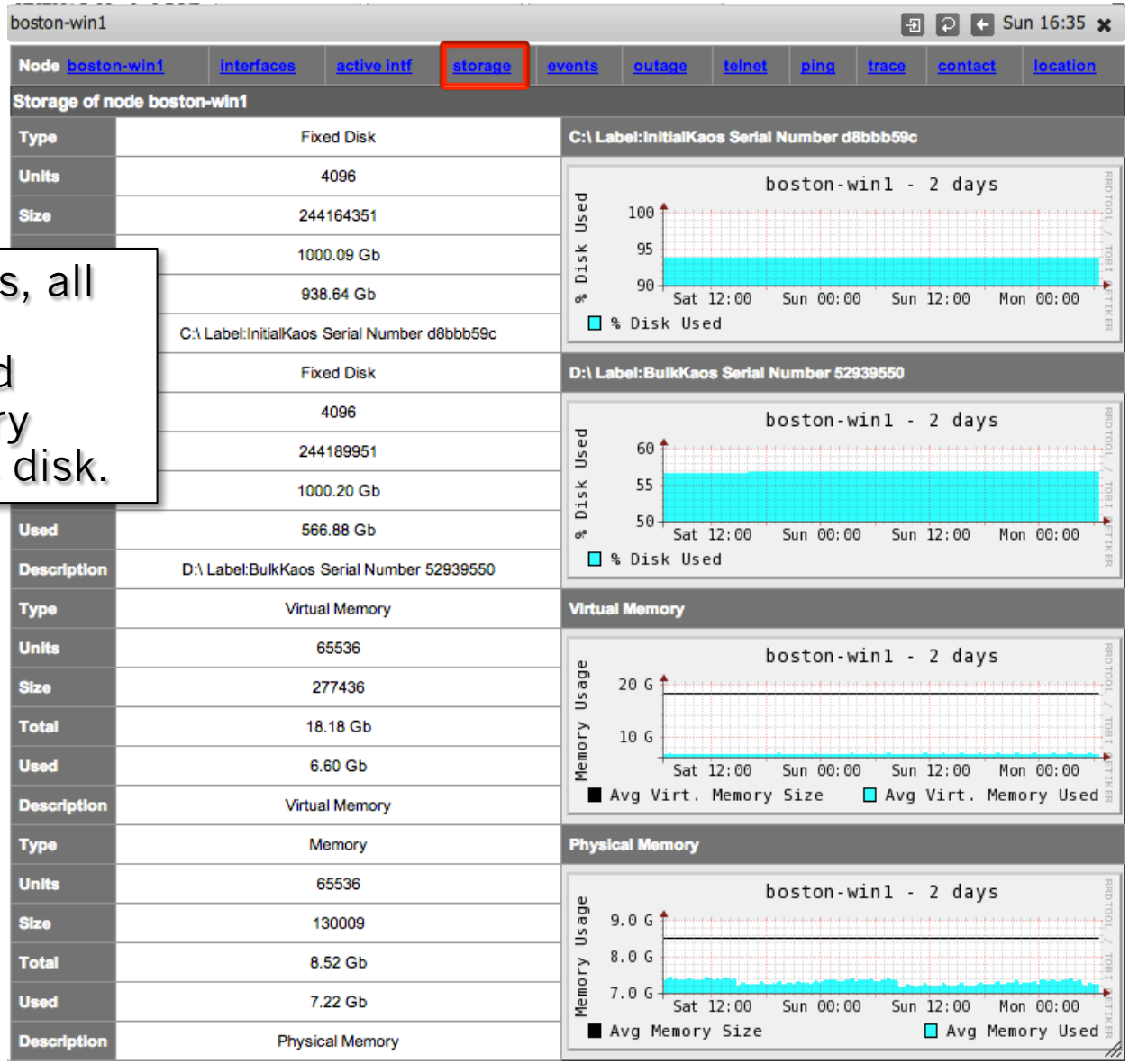
Node Widget: Outage

Current events for this device, that is stateful events which are active and the escalation level.



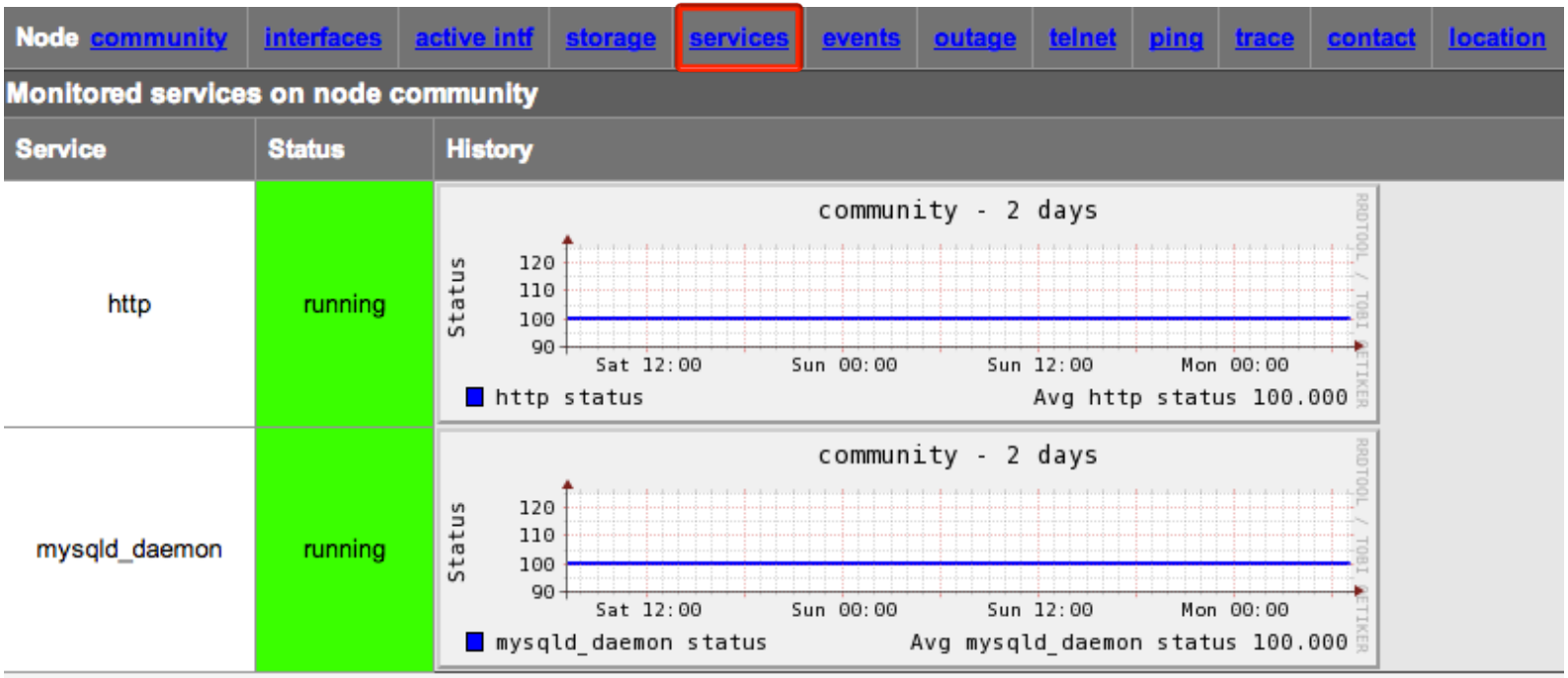
Node Widget: Storage

For devices like servers, all the available storage information, this could include Virtual memory information as well as disk.



Node Widget: Services

For devices like servers, all the available services being monitored.

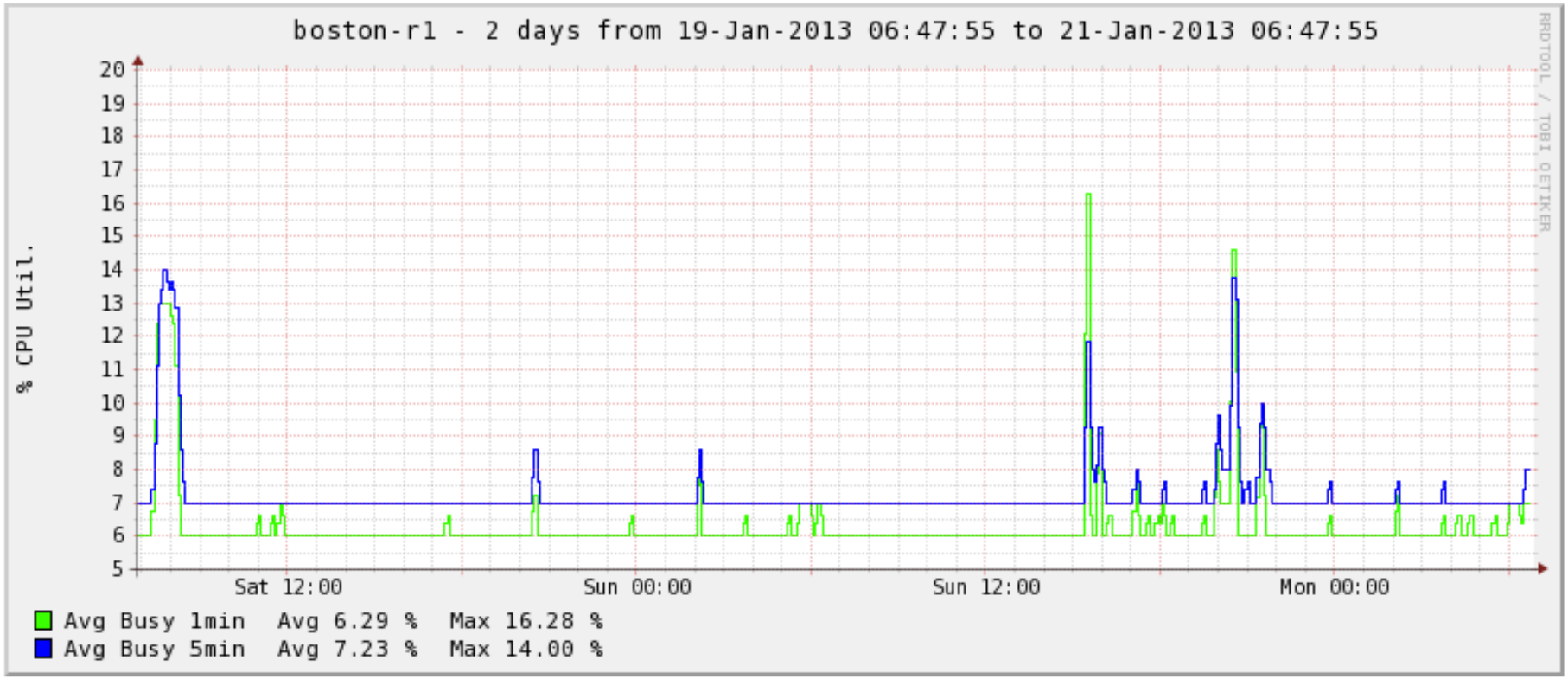


Graph Drill-in: CPU Utilisation

Clicking on any graph, brings up a BIG graph, you can select the time period and zoom in and out of the graph by clicking on different parts of it.

CPU Utilisation

Start 19-Jan-2013 06:47:55	Node boston-r1	Type cpu	Submit
End 21-Jan-2013 06:47:55	Interface Dialer1	CPU IP Response Health Memory Export Stats NMIS	



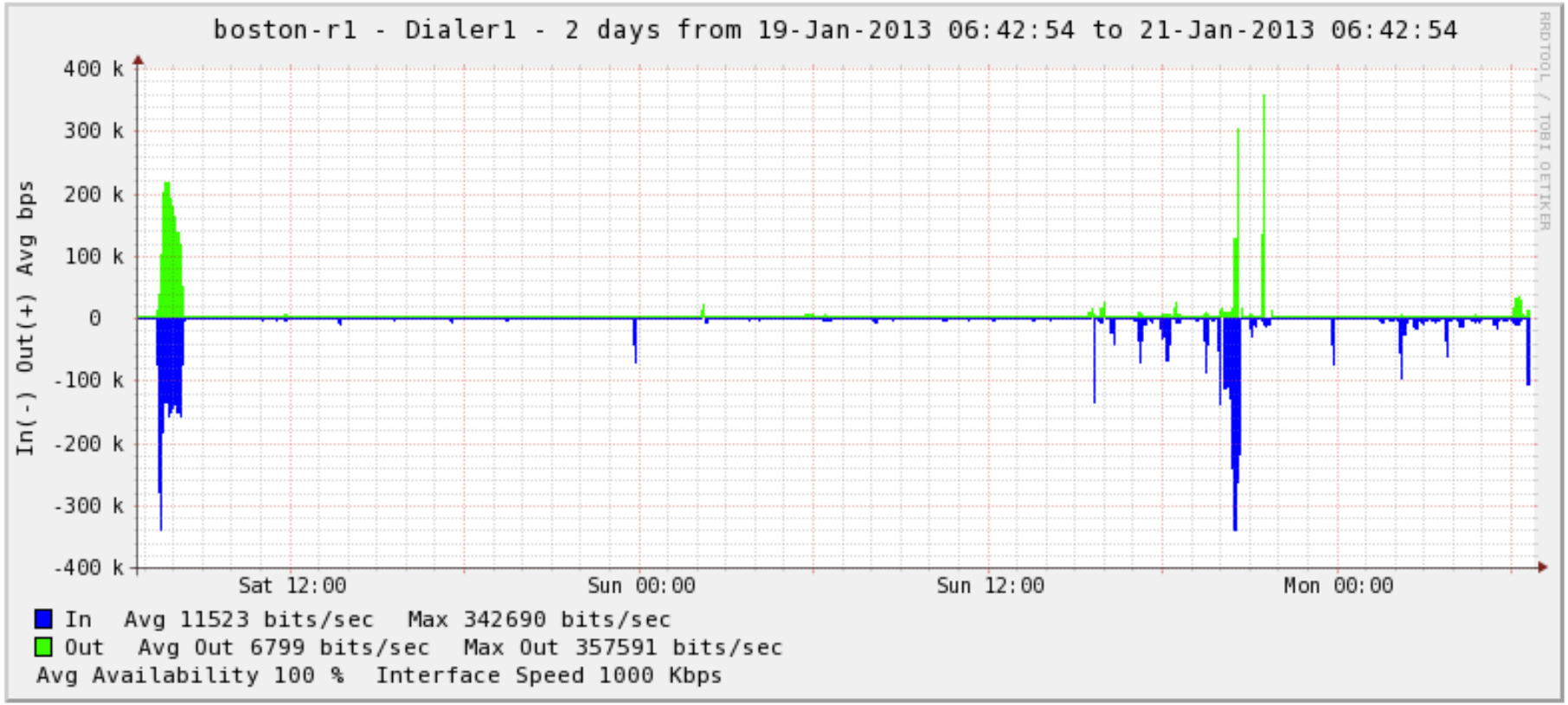
Clickable graphs: Left -> Back; Right -> Forward; Top Middle -> Zoom In; Bottom Middle-> Zoom Out, in time

Graph Drill-in: Interface Utilsation

Interface dialer1 Bits/Second Utilisation

Start	19-Jan-2013 06:42:54	**Node**	boston-r1	**Type**	abits	Submit
End	21-Jan-2013 06:42:54	**Interface**	Dialer1	CPU IP Response Health Memory Export Stats NMIS		

Type	ppp	**Speed**	1000 Kbps
Last Updated	21-Jan-2013 06:38:09	**Description**	Cloud Connection



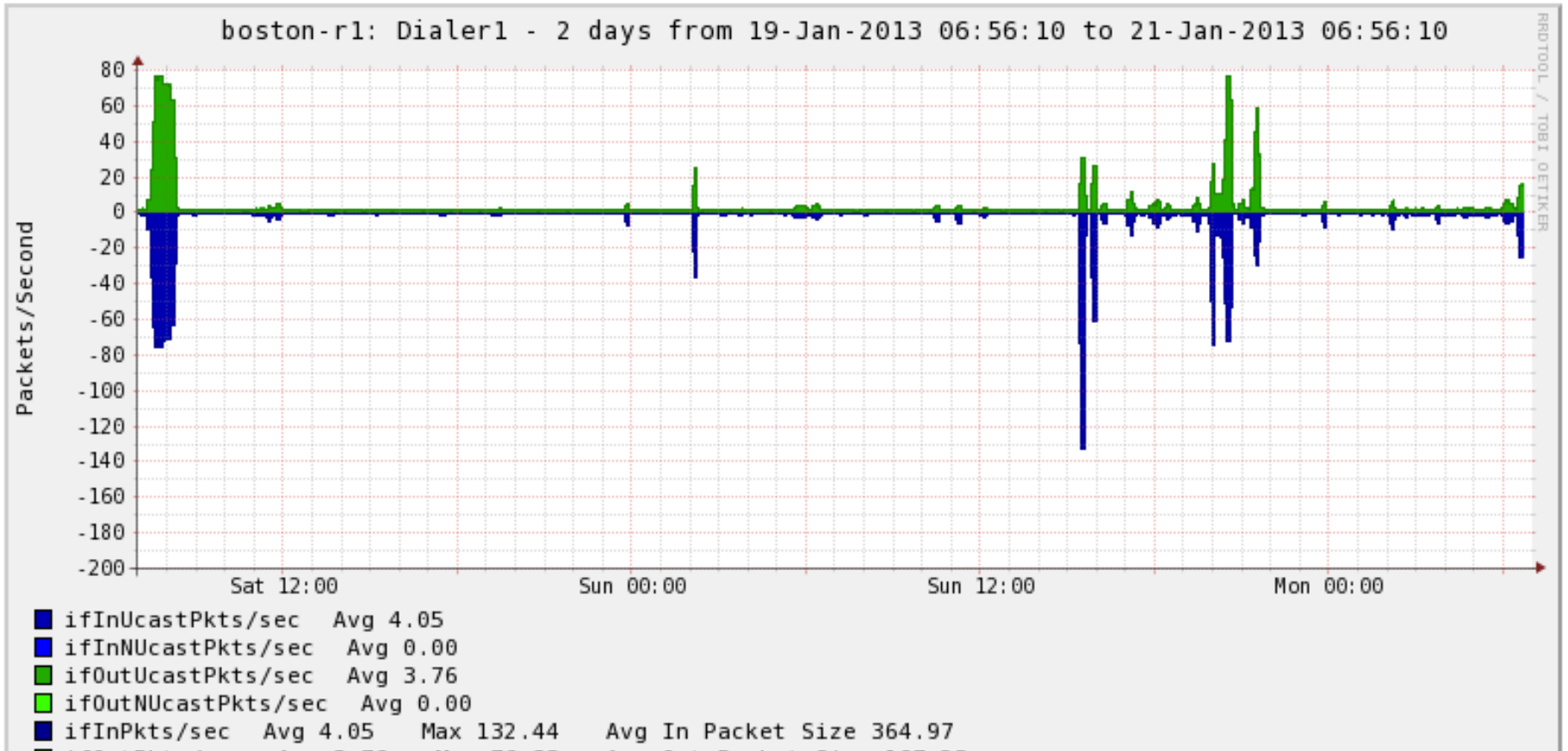
Clickable graphs: Left -> Back; Right -> Forward; Top Middle -> Zoom In; Bottom Middle-> Zoom Out, in time

Graph Drill-in: Packet Utilisation

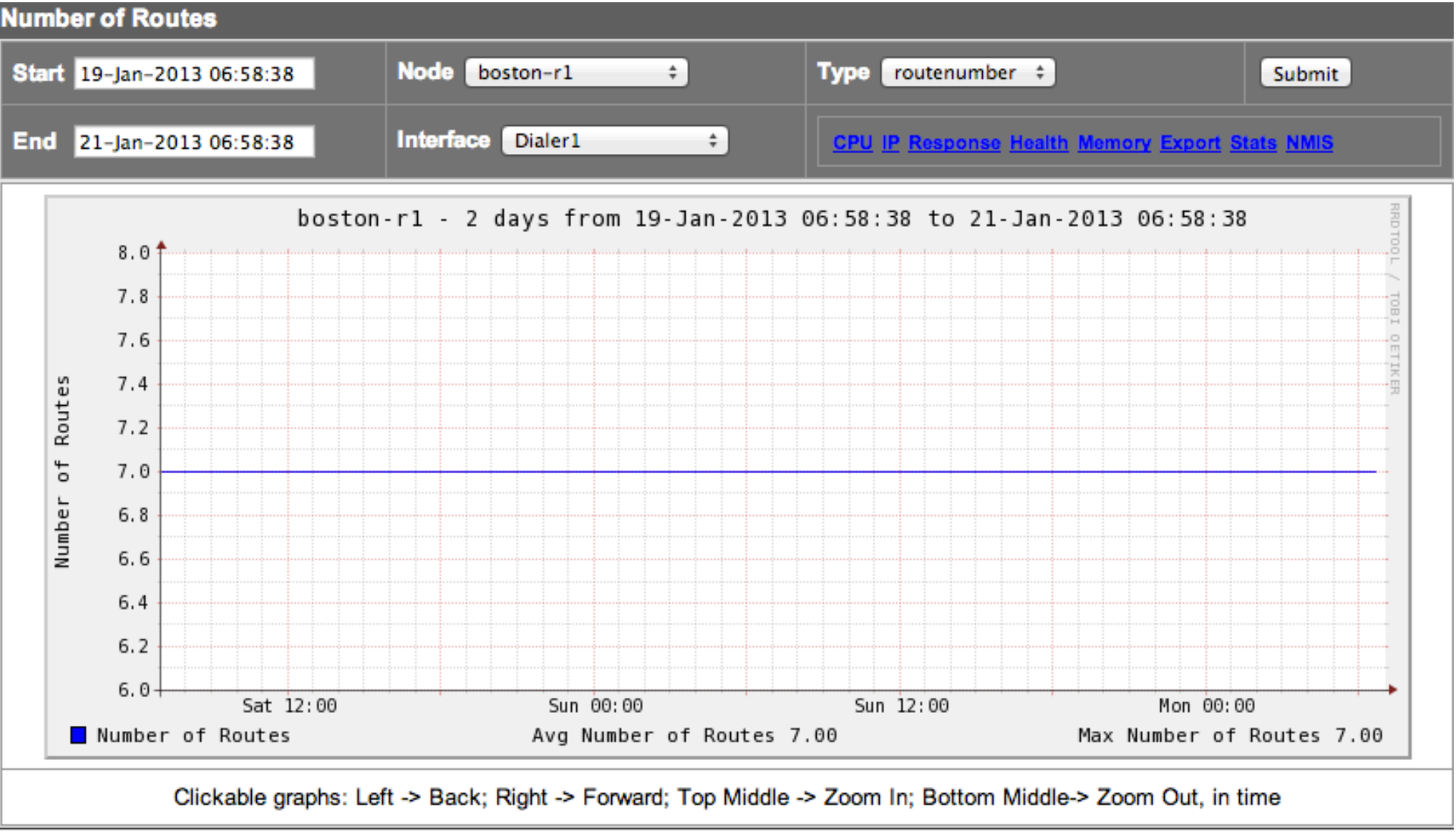
Interface Packets/Second Utilisation

Start	19-Jan-2013 06:56:10	**Node**	boston-r1	**Type**	pkts	Submit
End	21-Jan-2013 06:56:10	**Interface**	Dialer1	CPU IP Response Health Memory Export Stats NMIS		

Type	ppp	**Speed**	1000 Kbps
Last Updated	21-Jan-2013 06:43:09	**Description**	Cloud Connection



Graph Drill-in: Number of Routes




Managing Devices in NMIS8

Information required to add devices.

Determine your groups before you add devices.

Decide on Group Names

- How does the network look?
- What are the major locations or buildings.
- How does the business operate?
- Are there multiple countries?
- Are their data centres?
- Will branches or offices be represented by region
- Each of these things will likely be a group.

Minimum device information

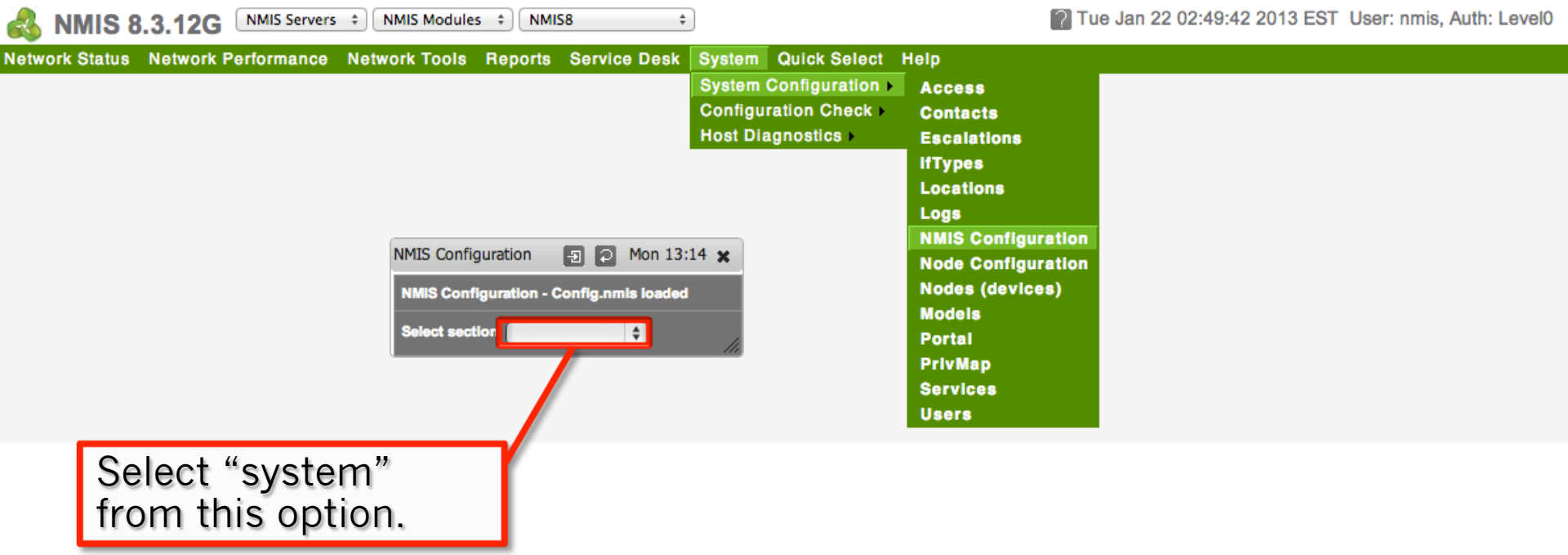
- The absolute minimum you can add a device with is:
  - IP address
  - SNMP community string
- Good to include the following:
  - name
  - group
  - role
  - CBQoS required or not
  - business_services
  - status
  - services (if a server)

Manage Groups

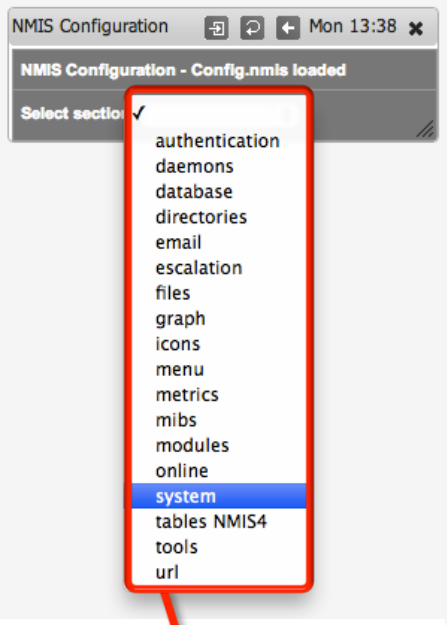
Managing Groups in NMIS8

To manage groups in NMIS access the menu option “System -> System Configuration -> NMIS Configuration”.

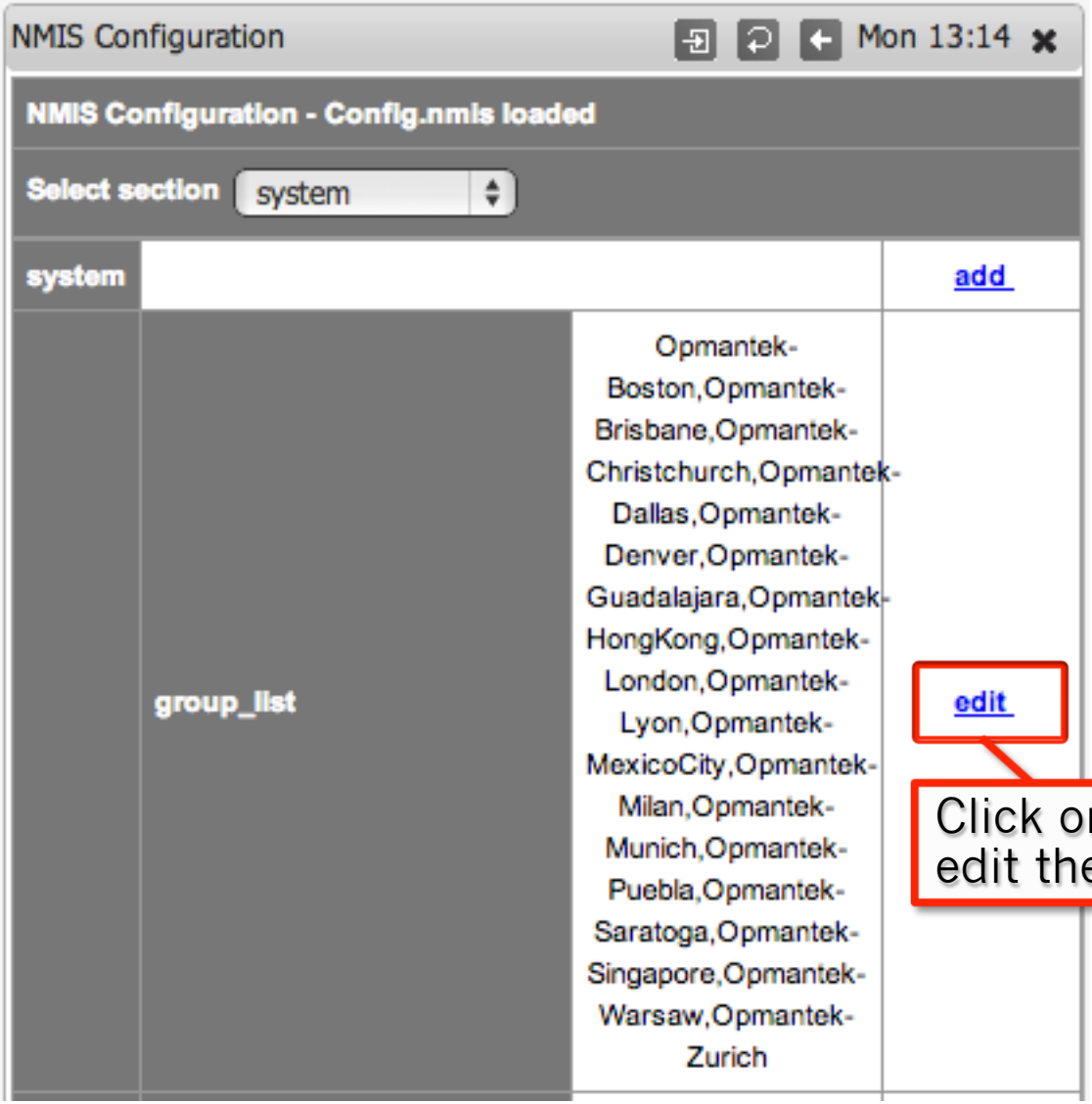
This will launch a small widget, which hides many settings.



Access the Group Settings

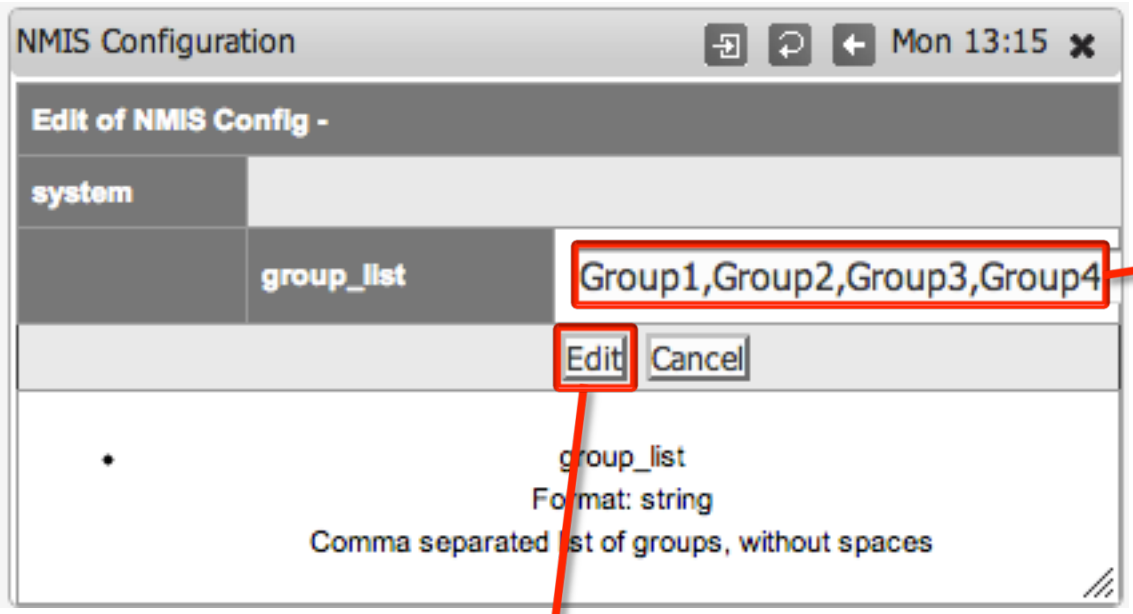


After selecting system from this list the panel on the left will be displayed.



Click on “edit” to edit the “group_list”.

Editing the Group List



Edit the group_list adding or removing the required groups.

This is a string of group names, which can not contain spaces, and there is a "," (comma) between each group name.

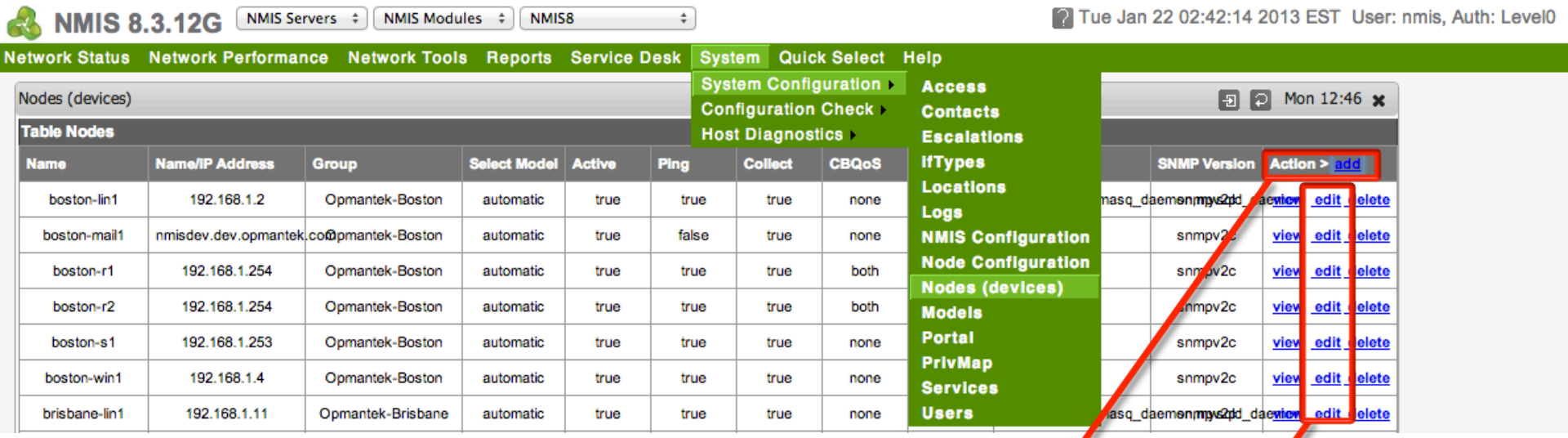
Click "Edit" when done to save the changes.

Manage Nodes

Managing Nodes (Devices) in NMIS8

To manage devices in NMIS access the menu option “System -> System Configuration -> Nodes (devices)”.

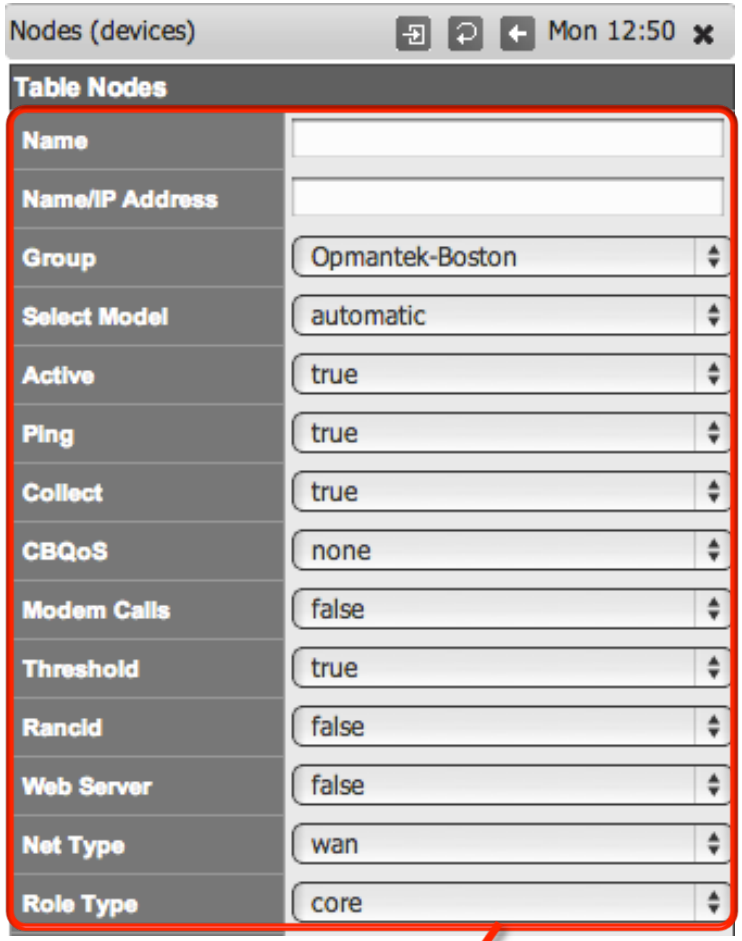
This will display a list of devices already being managed by NMIS. You can view, add, edit, delete devices from this menu.



Select “add” to add a device. This will only be visible if you are authorised.

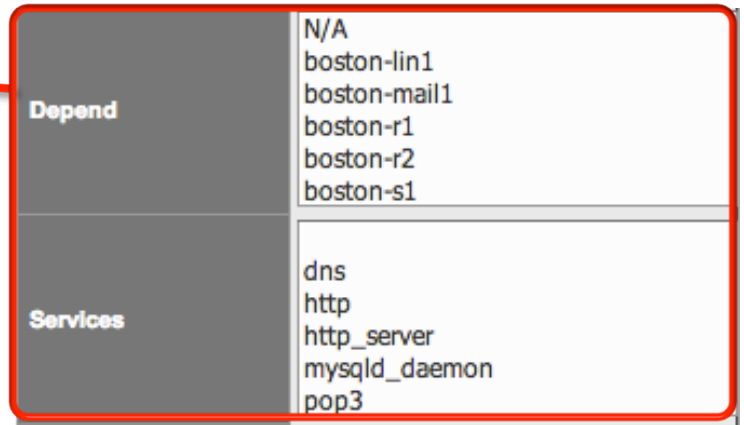
Selecting “edit” will bring the same screen as “add” but all existing properties available.

Add or Edit a Node (Device) in NMIS8

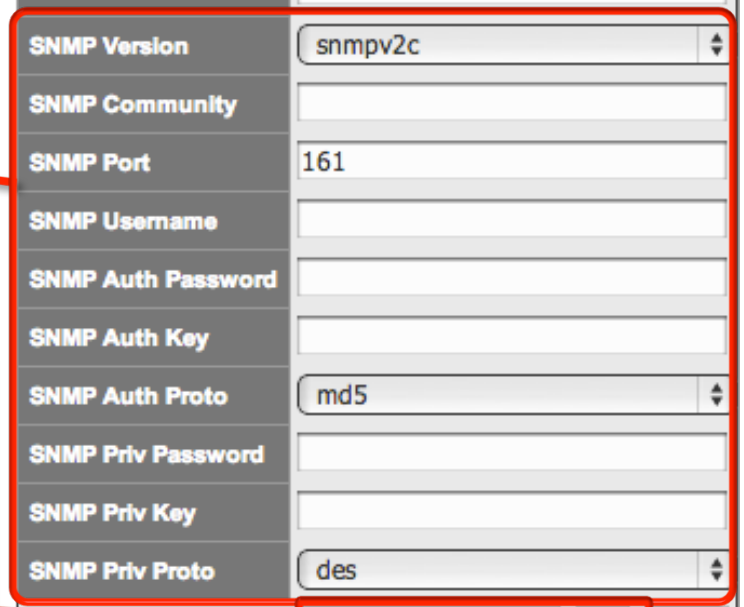


1. Complete the node properties, selecting or entering the required information.

2. Optionally complete the Depend and Services properties.



3. Select the SNMP Version, if using snmpv1 or snmpv2c only a community string is required. For snmpv3 many properties are required.



4. If changing the node, select "Add/Edit and Update Node" to finish. Select add if you will update later.

Node Properties

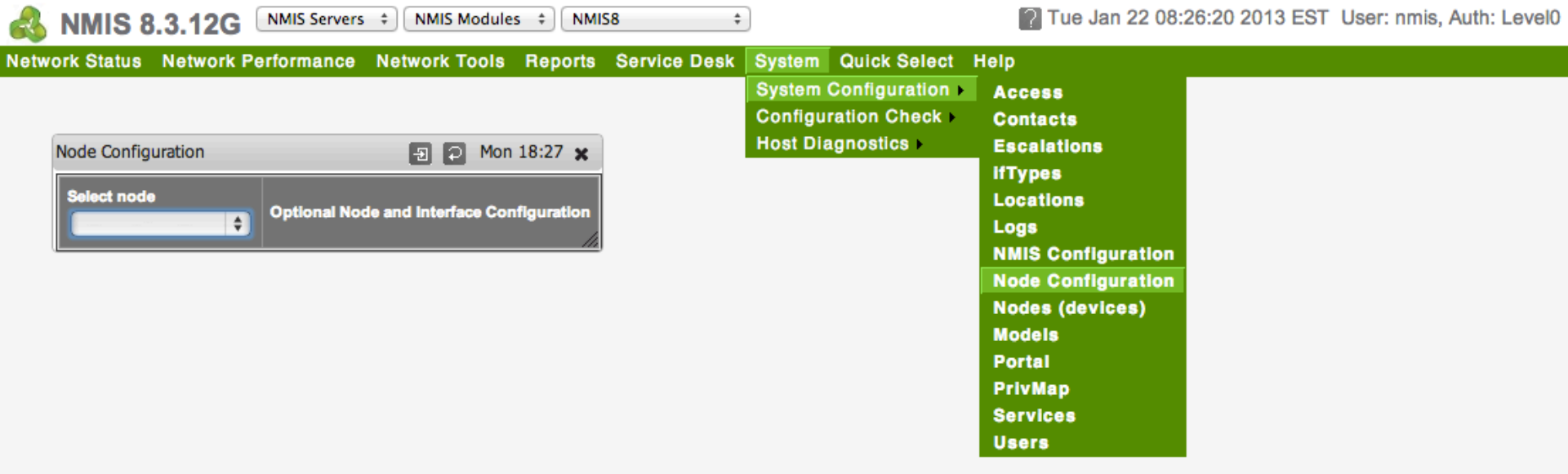
Heading	Default	Description	Values
name		The name of the device to be used, this should be the CI ID as used in other systems	
host		Hostname or IP address of the device, this may need to be the FQDN of the device	
community	public	The SNMP Community which has been configured to use on this device	
group		The group to which this device belongs	A valid group name from group_names in Config.nmis
roleType		The role of the device in the network	core, distribution, access
services		The services on this device to monitor	A valid service name from Services.nmis
businessService		A list of the business services for this device	A valid business sevice name from Business_Services.nmis
serviceStatus	Production	The status of the device for service management	Planning, Deployment, Pre-production, Production, Pilot, Suspended, Decommissioned, Test Lab, Other
location		The location of the device, not the SNMP sysLocation	
version	snmpv2c	The version of SNMP to use	snmpv1, snmpv2c, snmpv3
port	161	The SNMP Daemon UDP port to use for connection	Any valid UDP port
model	automatic	The name of the Model to use for this device, default is automatic	A valid model name from the NMIS8 models directory
active	true	Is this device active in NMIS8, should it be actively polled	true, false
collect	true	Should SNMP be collected on this device	true, false
ping	true	Should this device be polled with ICMP Pings	true, false
netType	lan	The network this device connects to.	lan, wan
threshold	true	Should thresholding be done on this device	true, false
cbqos	none	Should Cisco CBQoS MIB data be polled on this device	none, in, out, both
depend		What other nodes is this node dependant on.	
webserver	false	Does this node run a webserver for management	true, false
timezone	0	What is the timezone offset for this device	
calls	false	Collect Call SNMP information	
username		SNMP V3 Security Settings	
authkey		SNMP V3 Security Settings	
authpassword		SNMP V3 Security Settings	
authprotocol	md5	SNMP V3 Security Settings	
privkey		SNMP V3 Security Settings	
privpassword		SNMP V3 Security Settings	
privprotocol	des	SNMP V3 Security Settings	

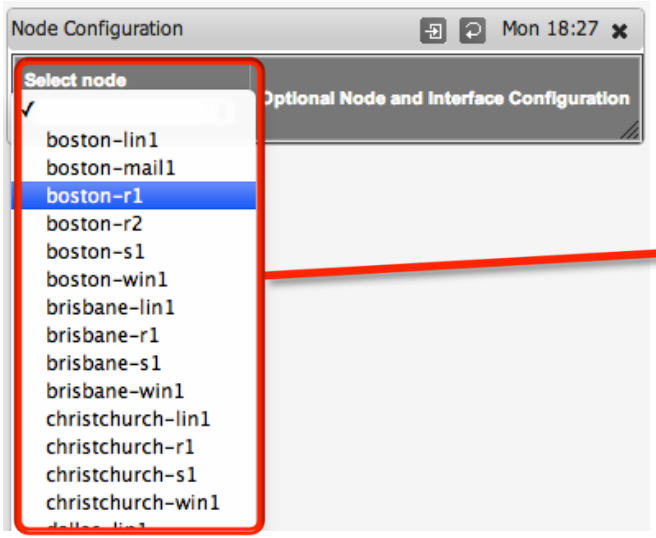
Customise Node Configuration

By default NMIS will use policy and models to configure nodes, but you can always override those settings by using Node Configuration.

Modify the Node Configuration for a Node

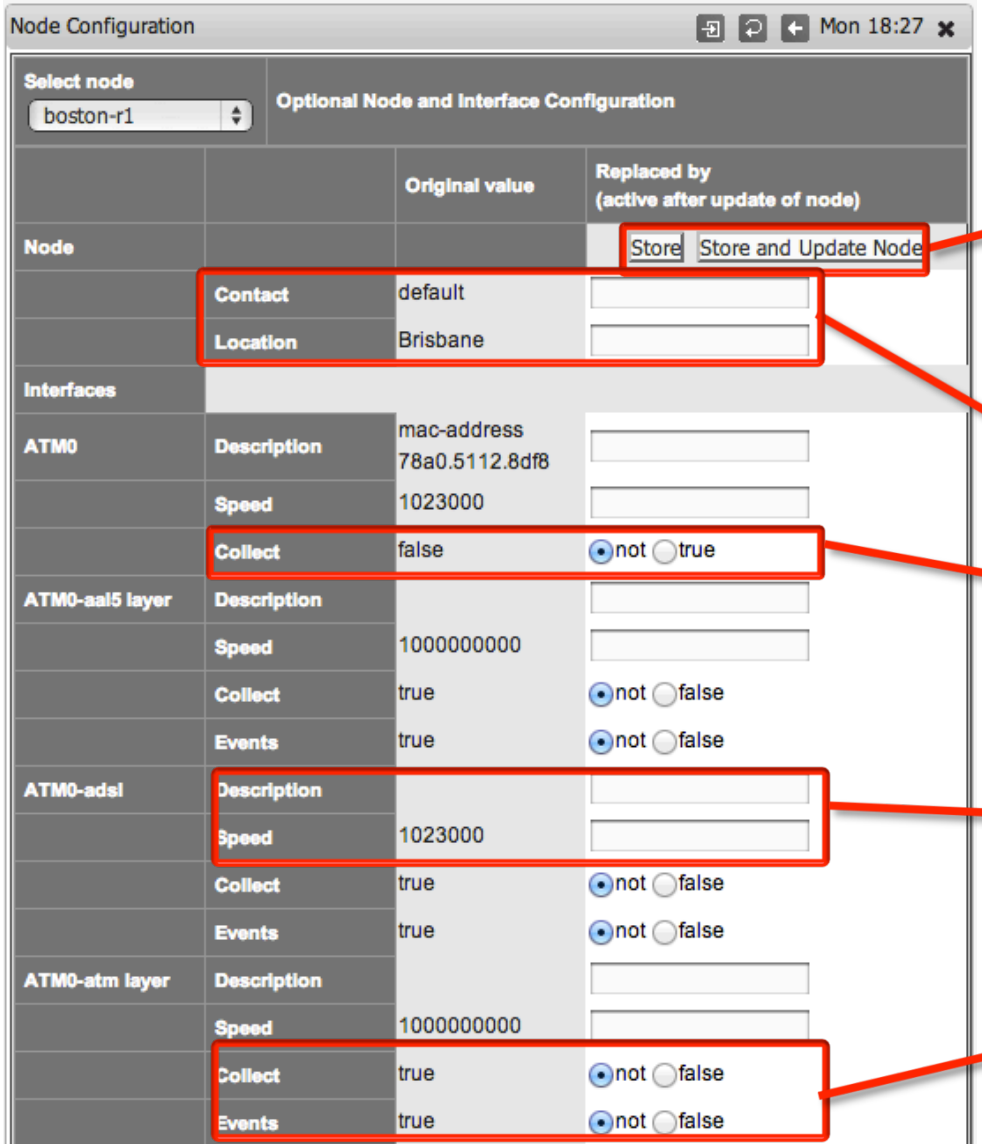
To access Node Configuration access the menu option “System -> System Configuration -> Node Configuration”. This will launch a small widget.





Select a node to modify the configuration for.

Modify the Node Configuration (overide)



When changes are complete, select “Store and Update Node” to finish. Select “Store” if you will update later.

Modify/override node contact and location (SNMP sysContact and sysLocation)

Enable collection when an interface is not being collected.

Modify/override interface descriptions or speed.

Disable collection or events when an interface is being collected.

Incident Scenarios and NMIS Visibility

This section is to work through how incidents will appear in NMIS and how you can use NMIS to troubleshoot what is happening in the network.

What causes an incident (event/alert/outage)?

Hard failures, soft failures, and people/process issues

Hard Failures

- Equipment failure
  - Processor boards
  - Power supply
- Power failure
  - Branch
  - Data center
- Cable cuts and failure
  - WAN cables
  - LAN cables
  - Fibre optic cables
  - Data center, LAN or branch

Soft Failures

- Resource usage
  - CPU load
  - Disk usage
  - Memory usage
  - Network interface capacity
- Application scalability
  - Concurrency/scalability

People/Process

- Changes
  - Configuration change
  - Equipment upgrades
  - Operating system upgrades

Incident Scenarios and NMIS Visibility

The following scenarios describe what happens before an incident.

- Scenario 1: High Router CPU
- Scenario 2: High Server CPU
- Scenario 3: WAN Packet Loss
- Scenario 4: Network interface congestion
- Scenario 5: Switch hardware failure
- Scenario 6: Router hardware failure
- Scenario 7: WAN connectivity failure
- Scenario 8: Service running service fails
- Scenario 9: Routing Problem

Scenario 1: Router High CPU

Business/Customer Impact:

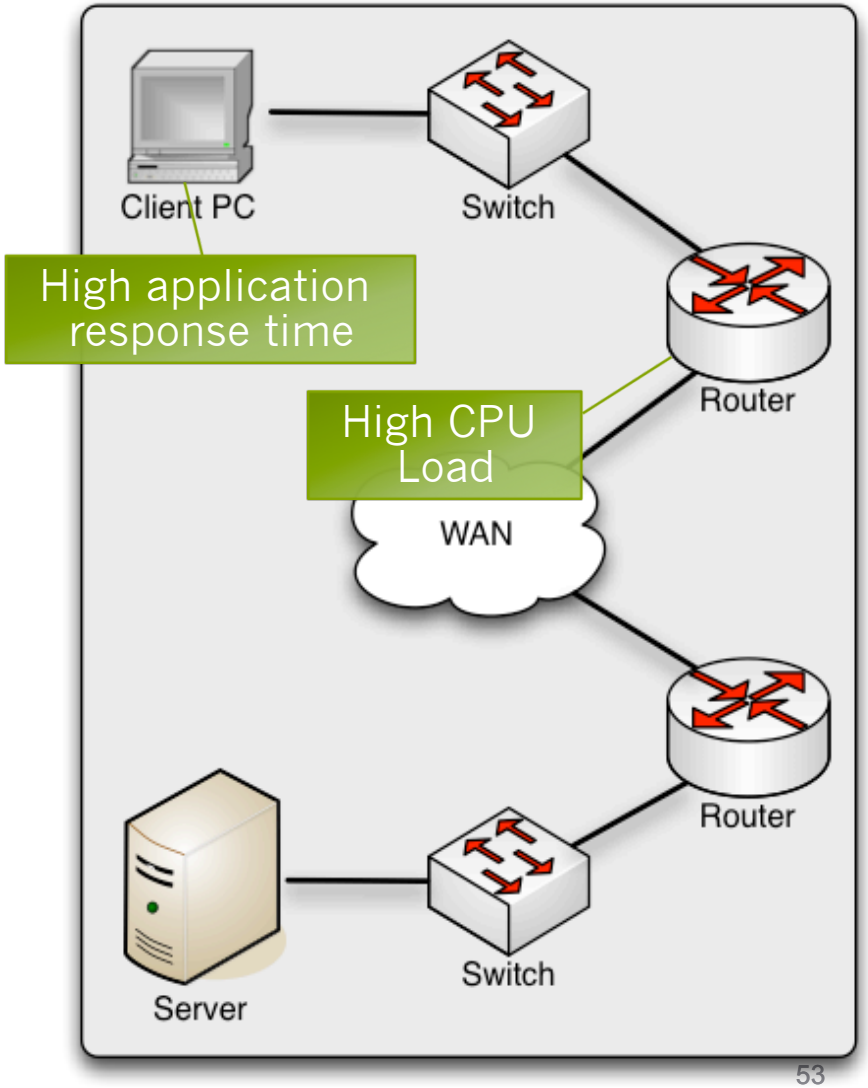
- User experiencing high application reponse time and having productivity problems.

Technical Symptoms:

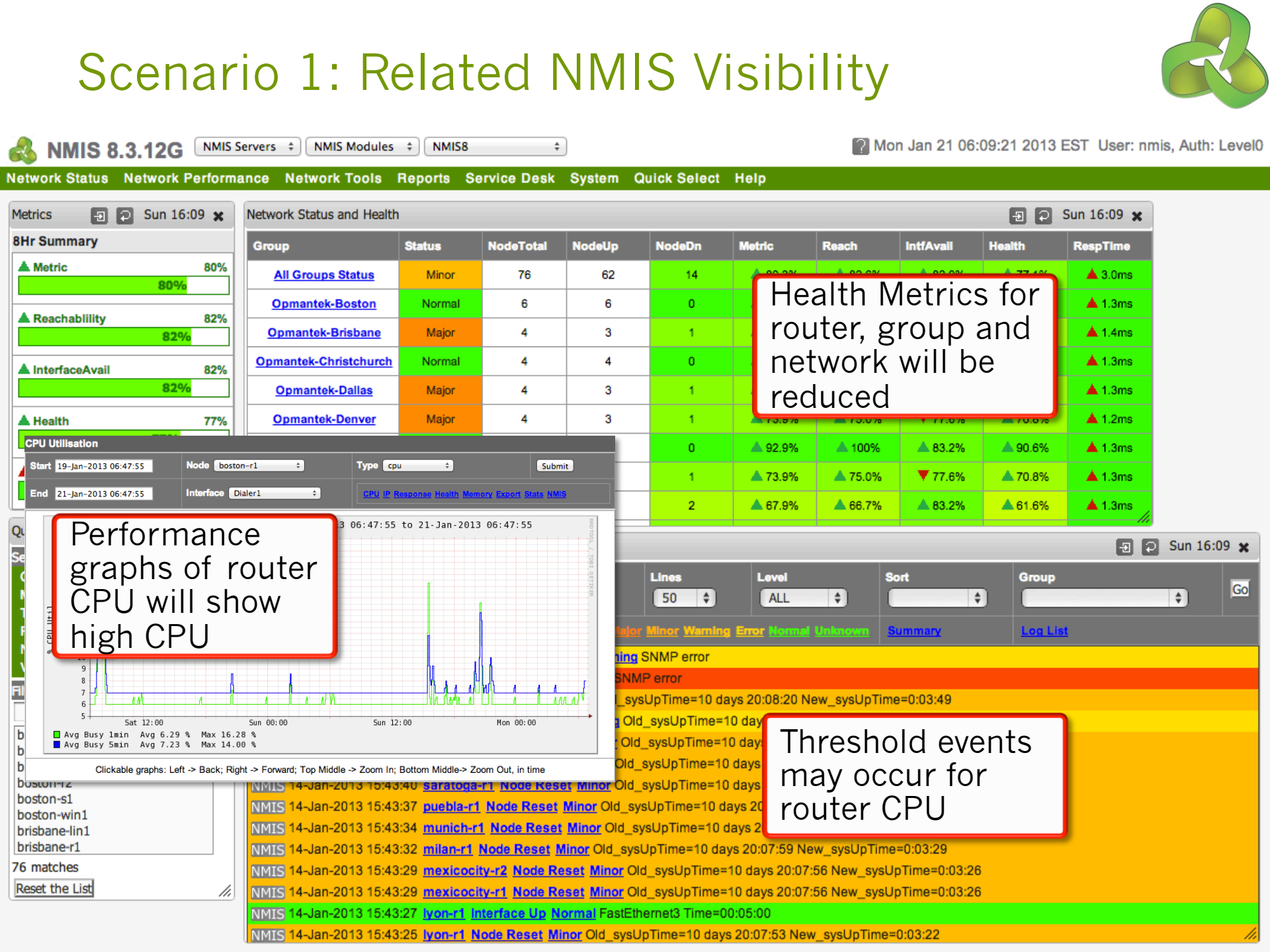
- Client experiencing high application response time
- Branch router has high CPU load
- Servers are OK

NMIS8 Visibility:

- Health Metrics for router, group and network will be reduced
- Performance graphs of router CPU will show high CPU
- Threshold events may occur for router CPU
- Response time will increase for router and switch.
- Synthetic transactions will show increased response time.



Scenario 1: Related NMIS Visibility



Scenario 2: Server High CPU

Business/Customer Impact:

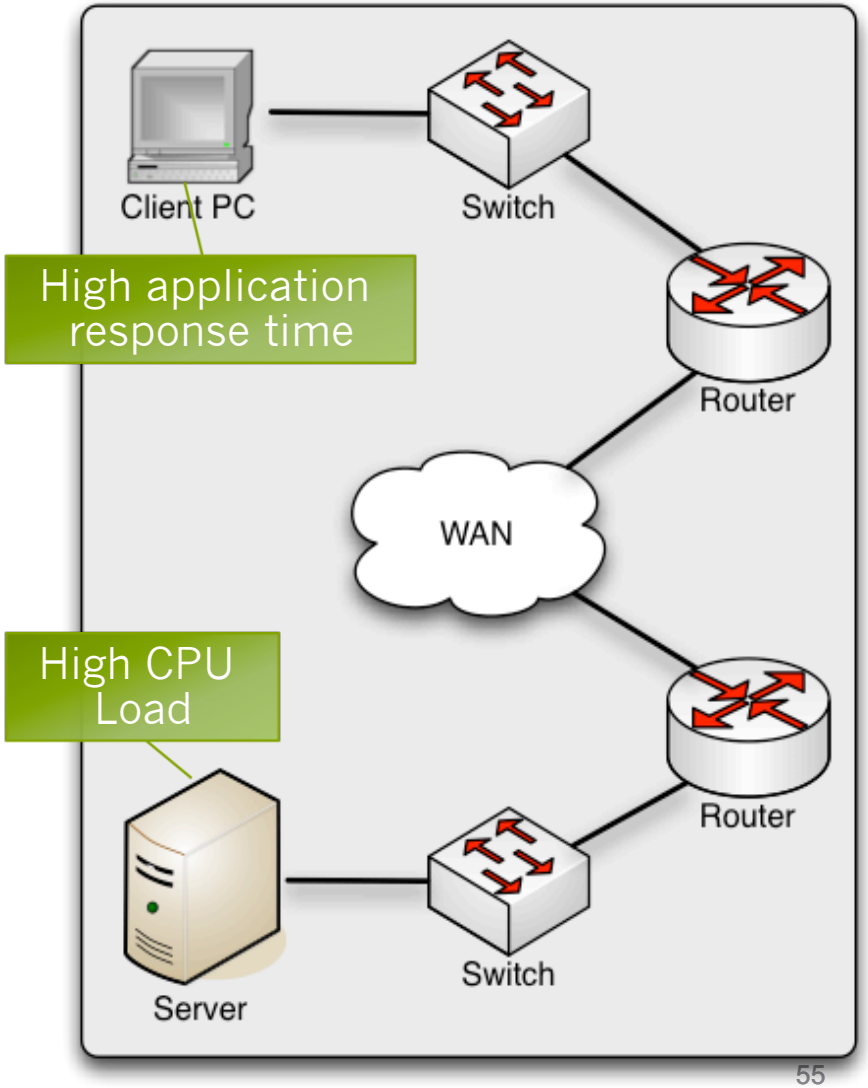
- User experiencing high application reponse time and having productivity problems.

Technical Symptoms:

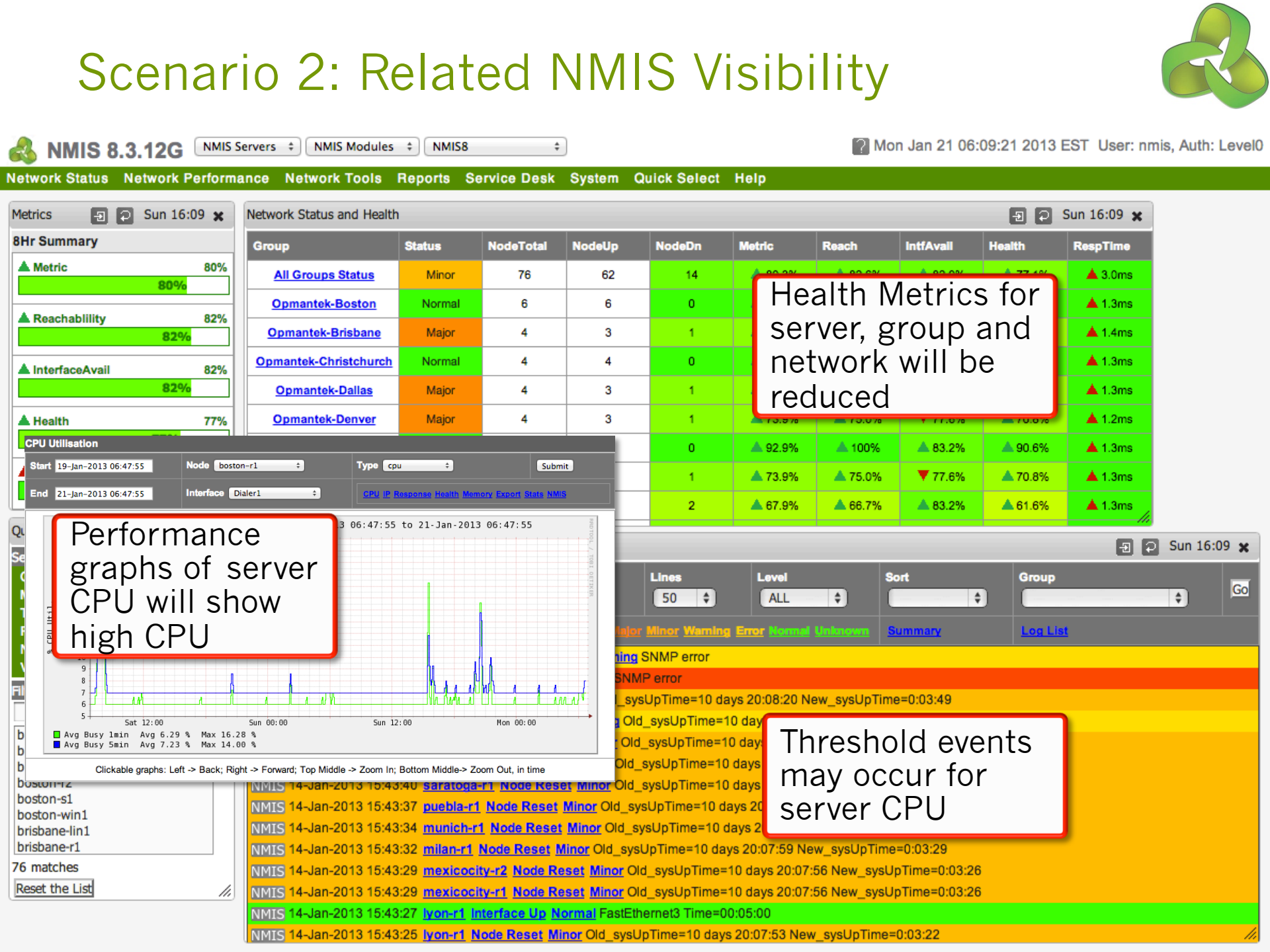
- Client experiencing high application response time
- Server has high CPU load
- Network is OK

NMIS8 Visibility:

- Health Metrics for server, group and network will be reduced
- Performance graphs of server CPU will show high CPU
- Threshold events may occur for Server CPU
- Synthetic transactions will show increased response time.
- Response time for server will increase



Scenario 2: Related NMIS Visibility



Scenario 3: WAN Packet Loss

Business/Customer Impact:

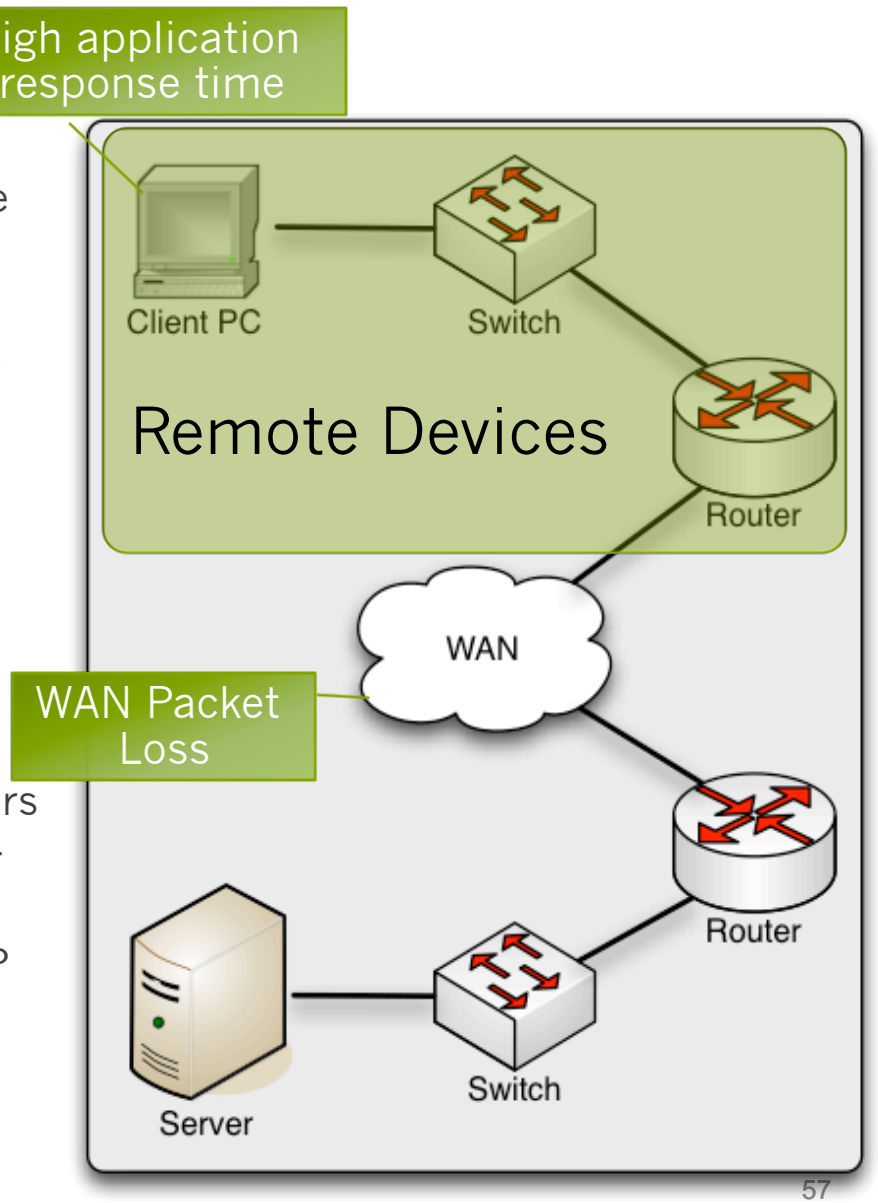
- User(s) experiencing high application reponse time and having productivity problems.

Technical Symptoms:

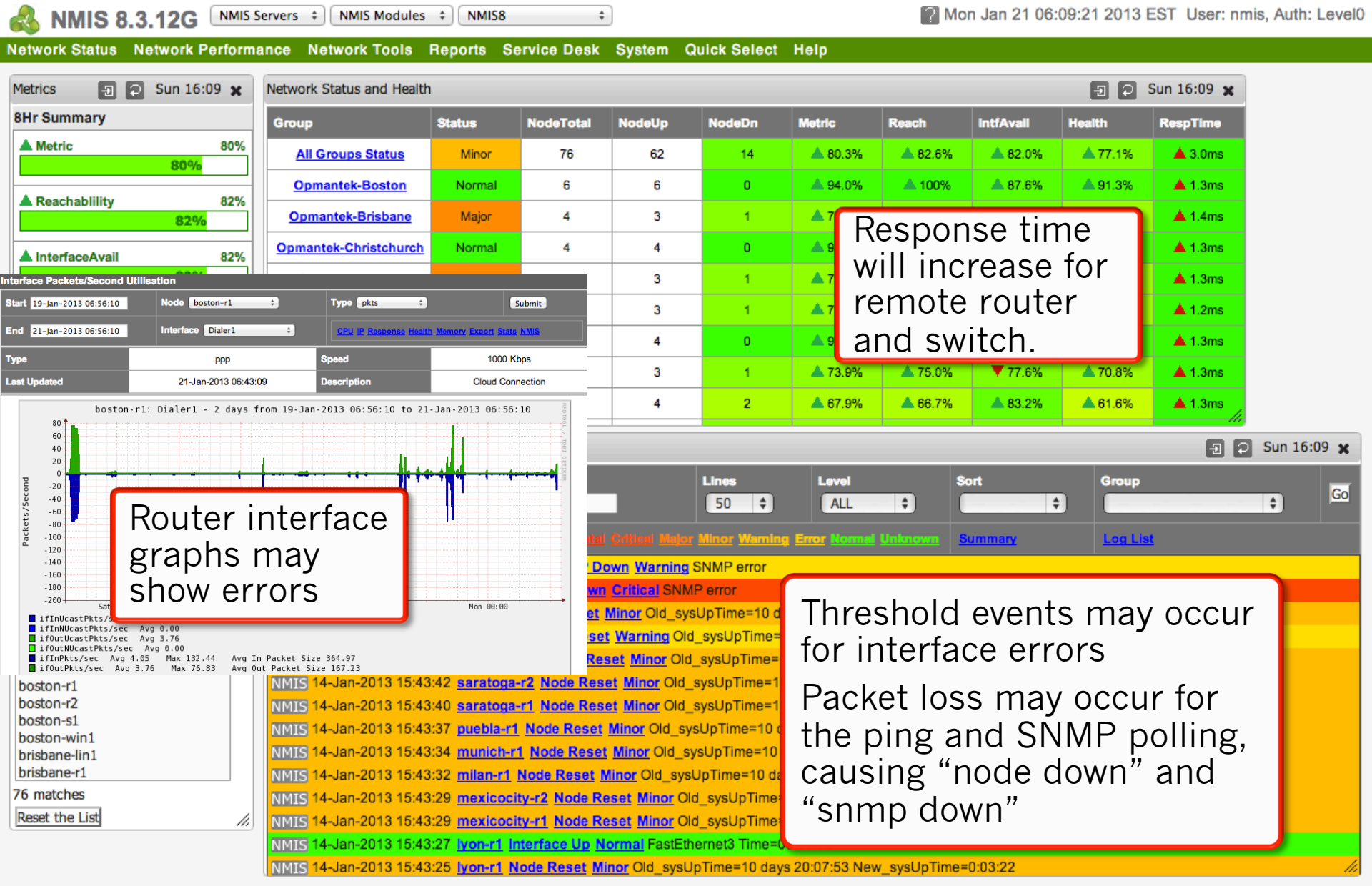
- Client experiencing high application response time
- Network devices are OK
- Servers are OK

NMIS8 Visibility:

- Packet loss will result in TCP retransmissions between the server and the client.
- Router interface graphs may show errors.
- Threshold events may occur for interface errors
- Response time will increase for remote router and switch.
- Packet loss may occur for the ping and SNMP polling, causing “node down” and “snmp down”.
- Synthetic transactions will show increased response time and packet loss.



Scenario 3: Related NMIS Visibility



Scenario 4: Network interface congestion

Business/Customer Impact:

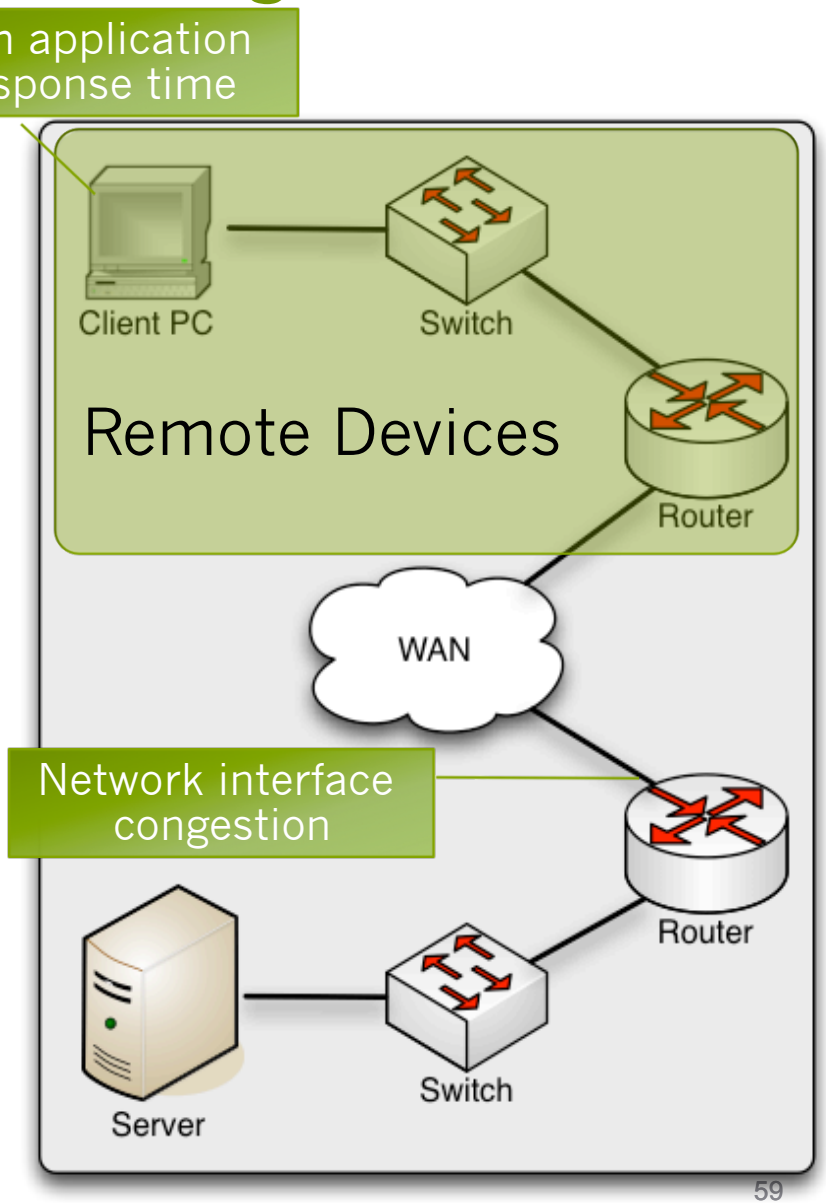
- User experiencing high application reponse time and having productivity problems.

Technical Symptoms:

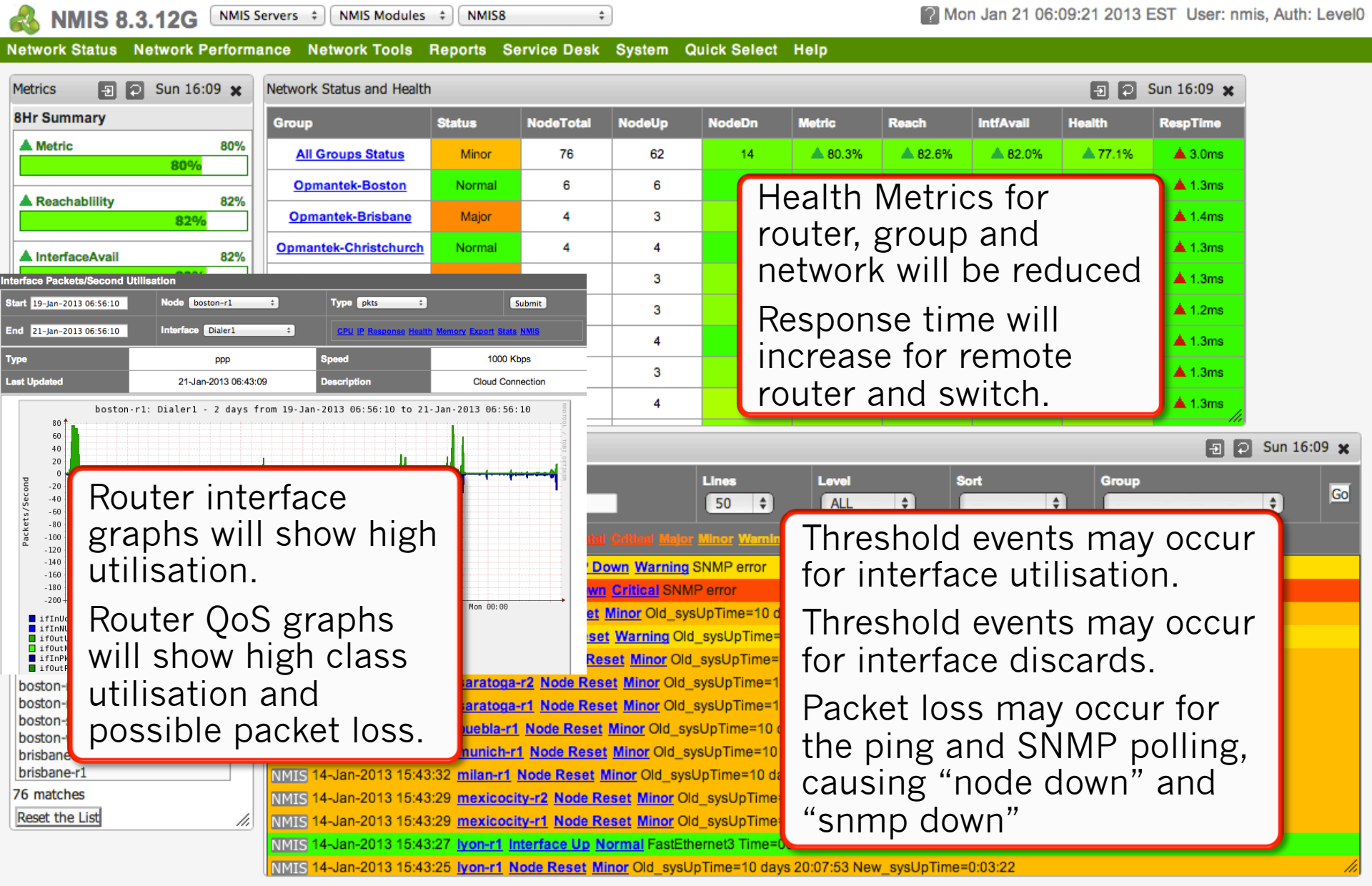
- Client experiencing high application response time
- Servers are OK

NMIS8 Visibility:

- Health Metrics for router, group and network will be reduced
- Congestion will likely result in packet loss and TCP retransmissions between the server and the client.
- Router interface graphs will show high utilisation.
- Router QoS graphs will show high class utilisation and possible packet loss.
- Threshold events may occur for interface utilisation.
- Threshold events may occur for interface discards.
- Response time will increase for remote router and switch.
- Packet loss may occur for the ping and SNMP polling, causing “node down” and “snmp down”.
- Synthetic transactions will show increased response time and packet loss.



Scenario 4: Related NMIS Visibility



Scenario 5: Switch hardware failure

Business/Customer Impact:

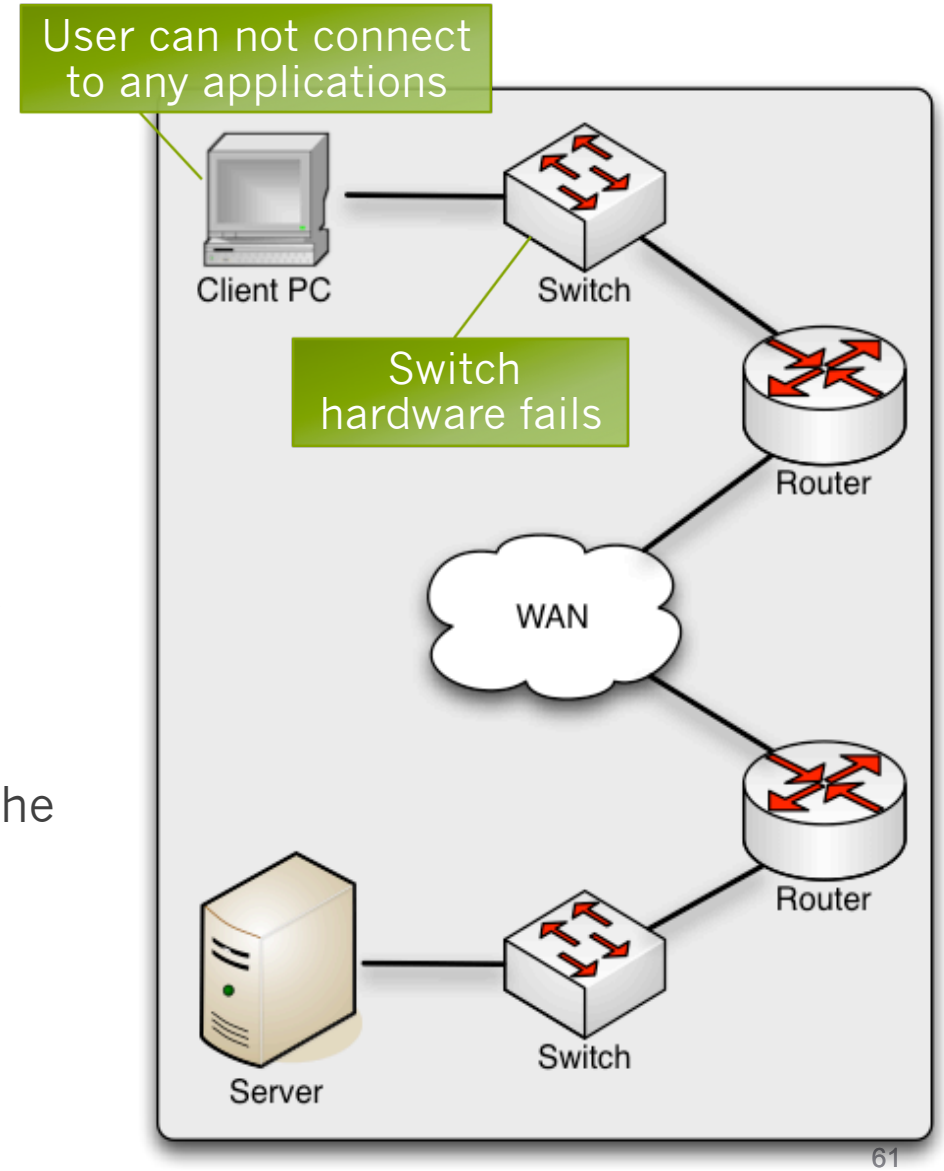
- User is unable to connect to any applications.

Technical Symptoms:

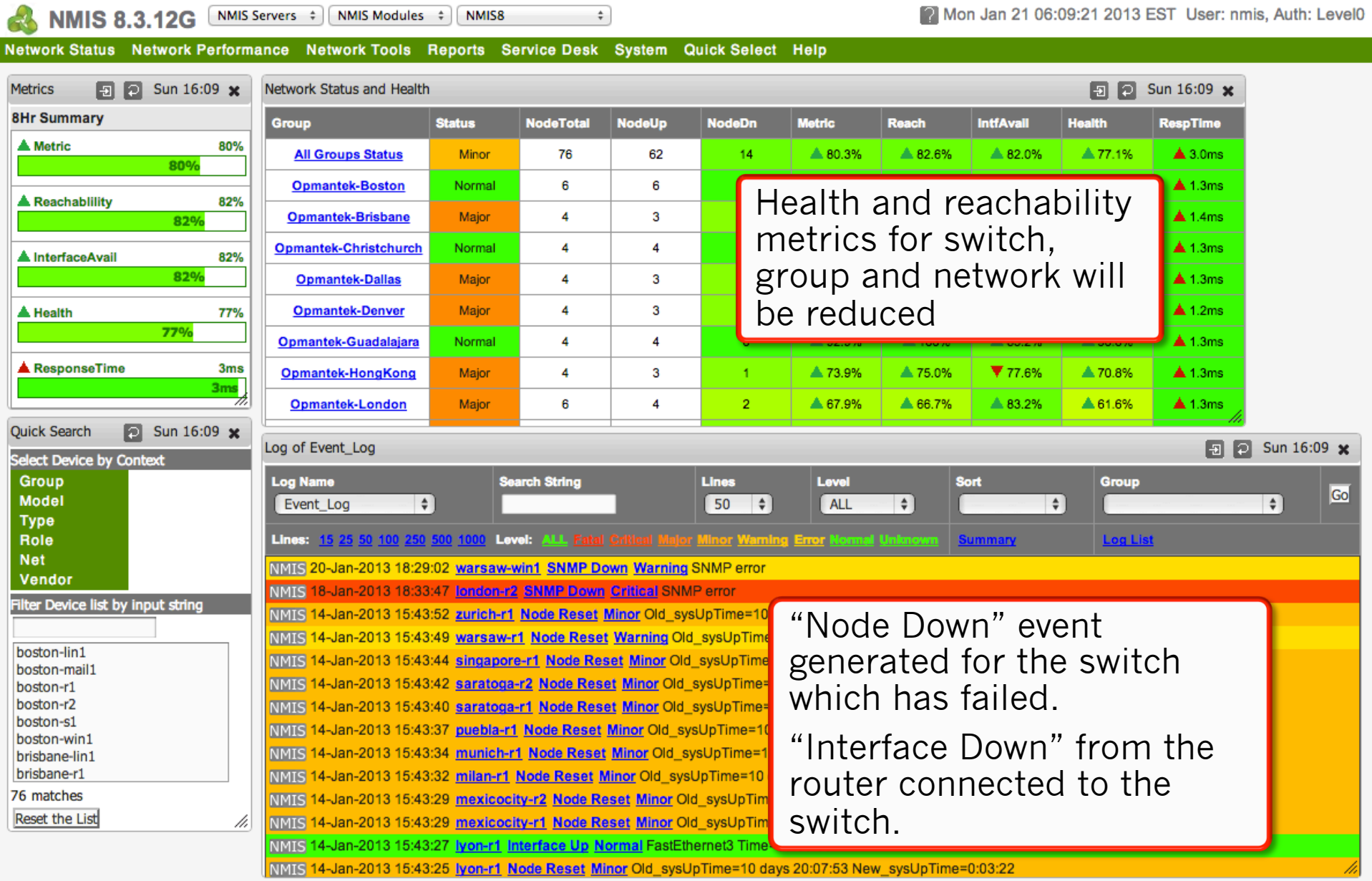
- User has no network connectivity
- Servers are OK

NMIS8 Visibility:

- Health and reachability metrics for switch, group and network will be reduced
- “Node Down” event generated for the switch which has failed.
- “Interface Down” from the router connected to the switch.



Scenario 5: Related NMIS Visibility



Scenario 6: Router hardware failure

Business/Customer Impact:

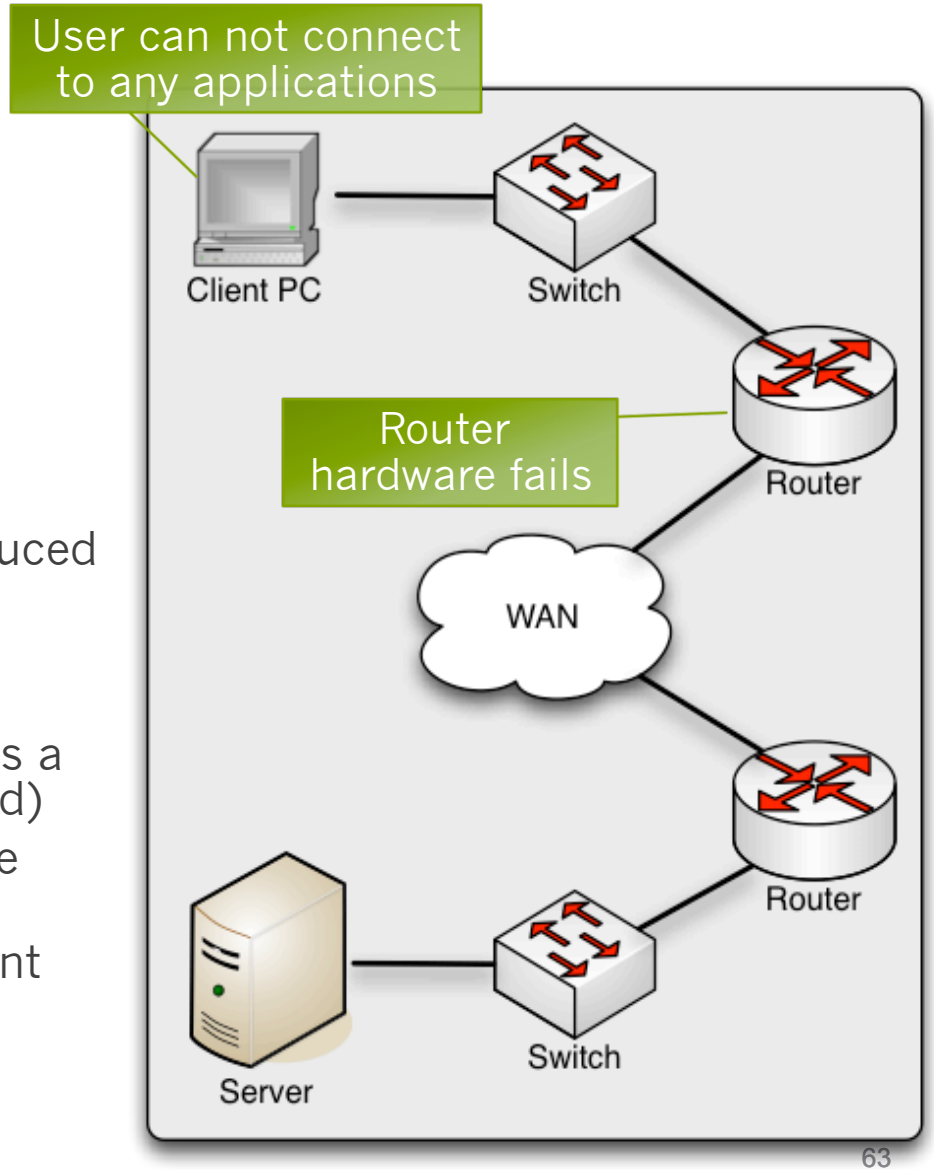
- User unable to connect to any applications.

Technical Symptoms:

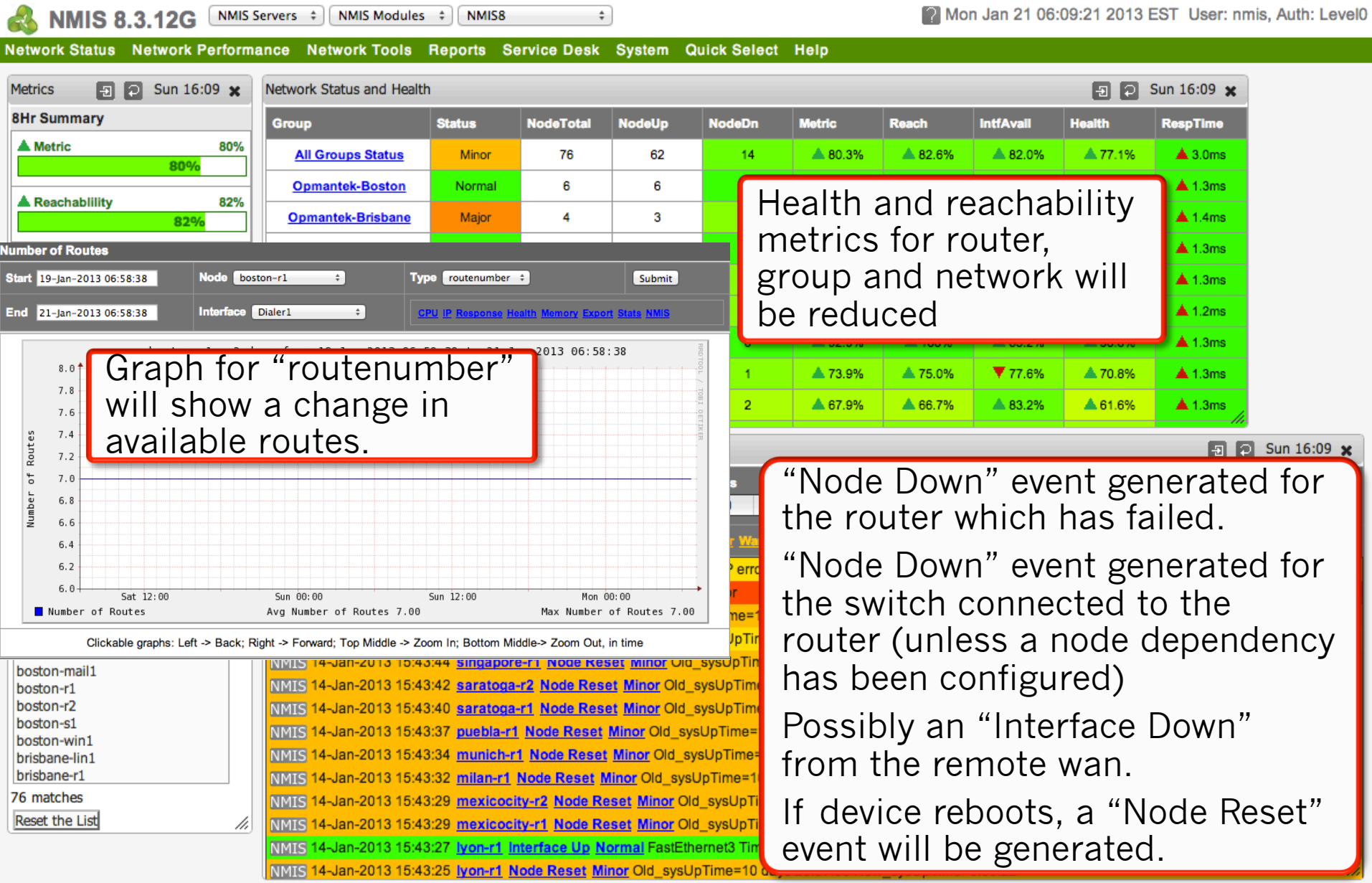
- User has connectivity to switch only
- Servers are OK

NMIS8 Visibility:

- Health and reachability metrics for router, group and network will be reduced
- “Node Down” event generated for the router which has failed.
- “Node Down” event generated for the switch connected to the router (unless a node dependency has been configured)
- Possibly an “Interface Down” from the remote wan.
- If device reboots, a “Node Reset” event will be generated.
- Graph for “routenumber” will show a change in available routes.



Scenario 6: Related NMIS Visibility



Scenario 7: WAN connectivity failure

Business/Customer Impact:

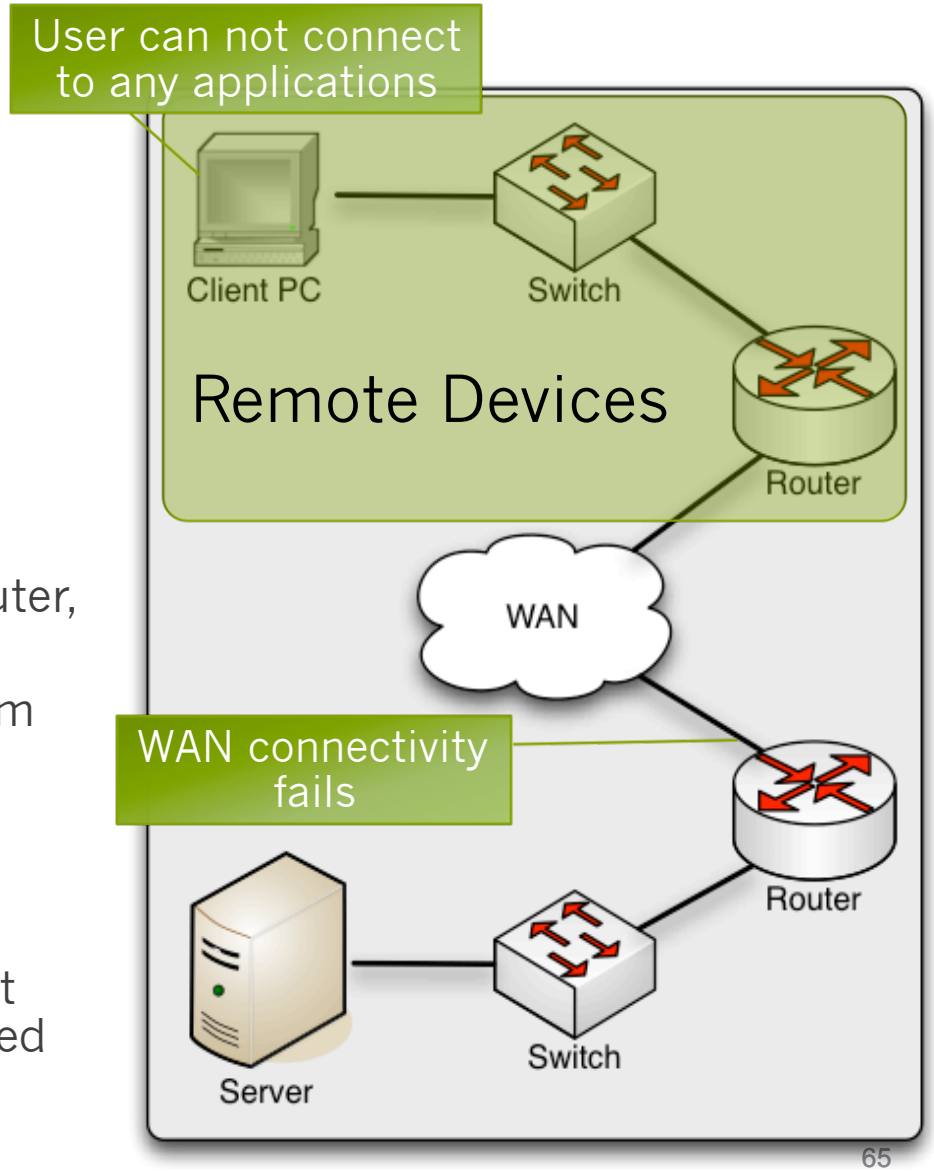
- User(s) unable to connect to any applications.

Technical Symptoms:

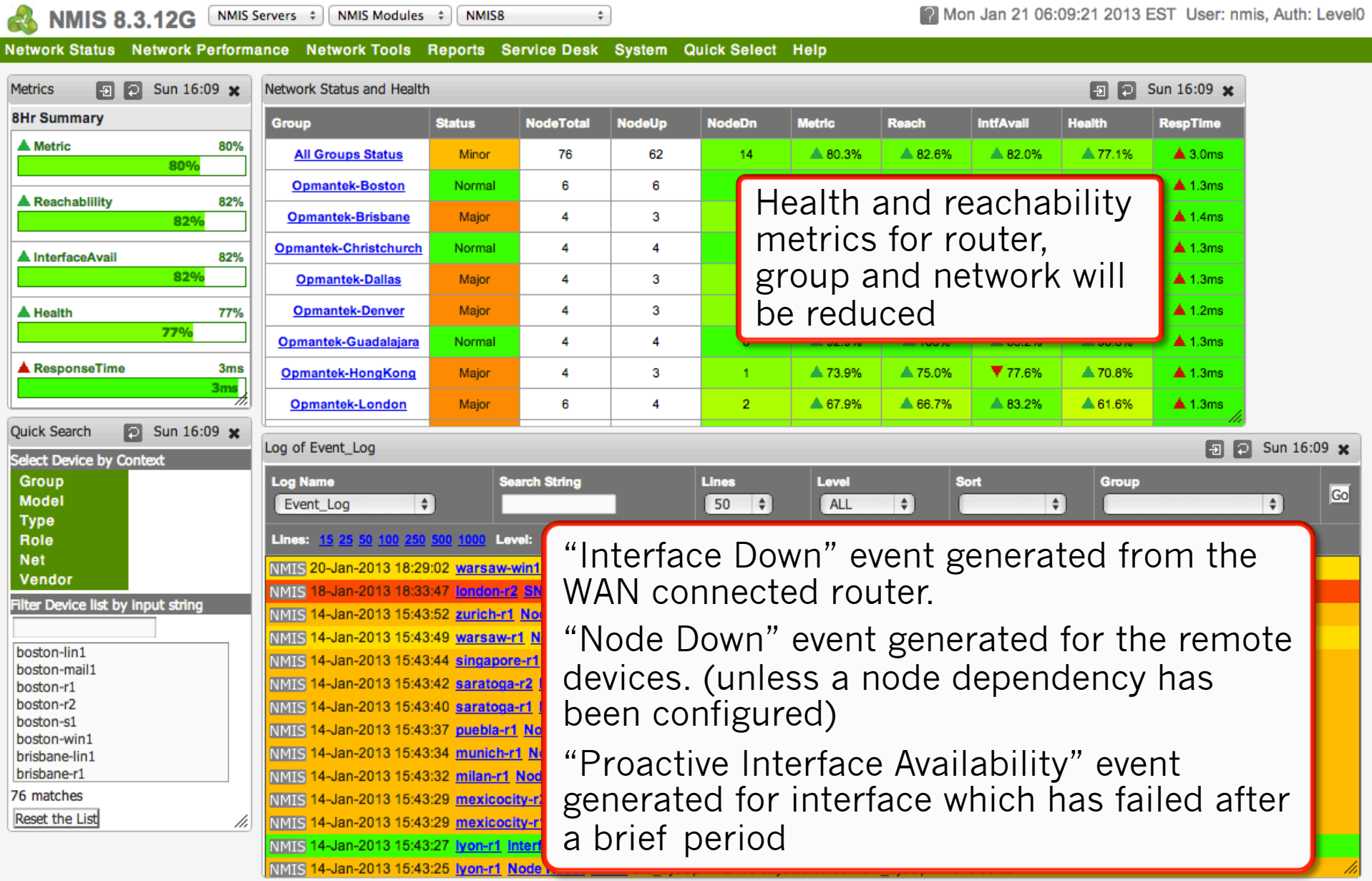
- User has connectivity to switch and router.
- Servers are OK

NMIS8 Visibility:

- Health and availability metrics for router, group and network will be reduced
- "Interface Down" event generated from the WAN connected router.
- "Node Down" event generated for the remote devices. (unless a node dependency has been configured)
- "Proactive Interface Availability" event generated for interface which has failed after a brief period



Scenario 7: Related NMIS Visibility



Scenario 8: Service running service fails

Business/Customer Impact:

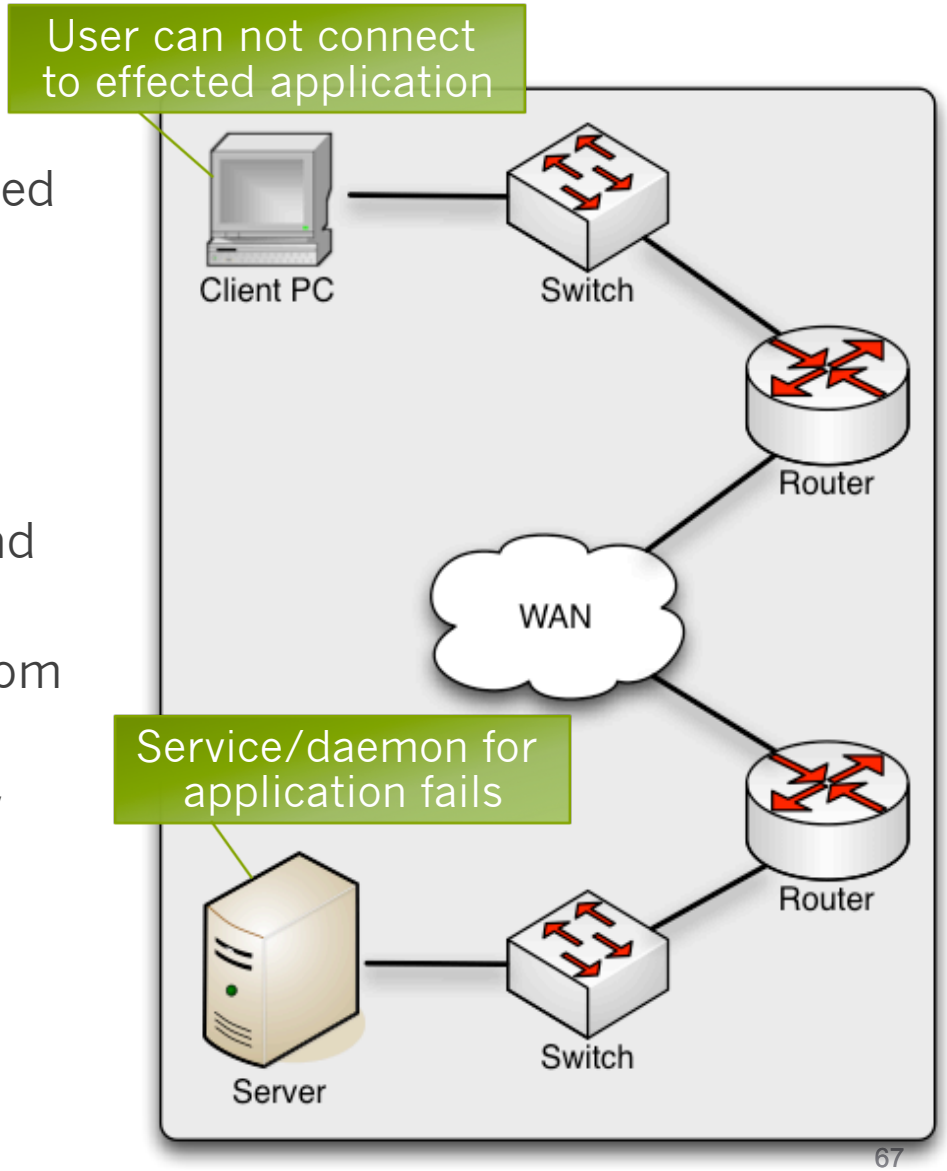
- User(s) unable to connect to effected application.

Technical Symptoms:

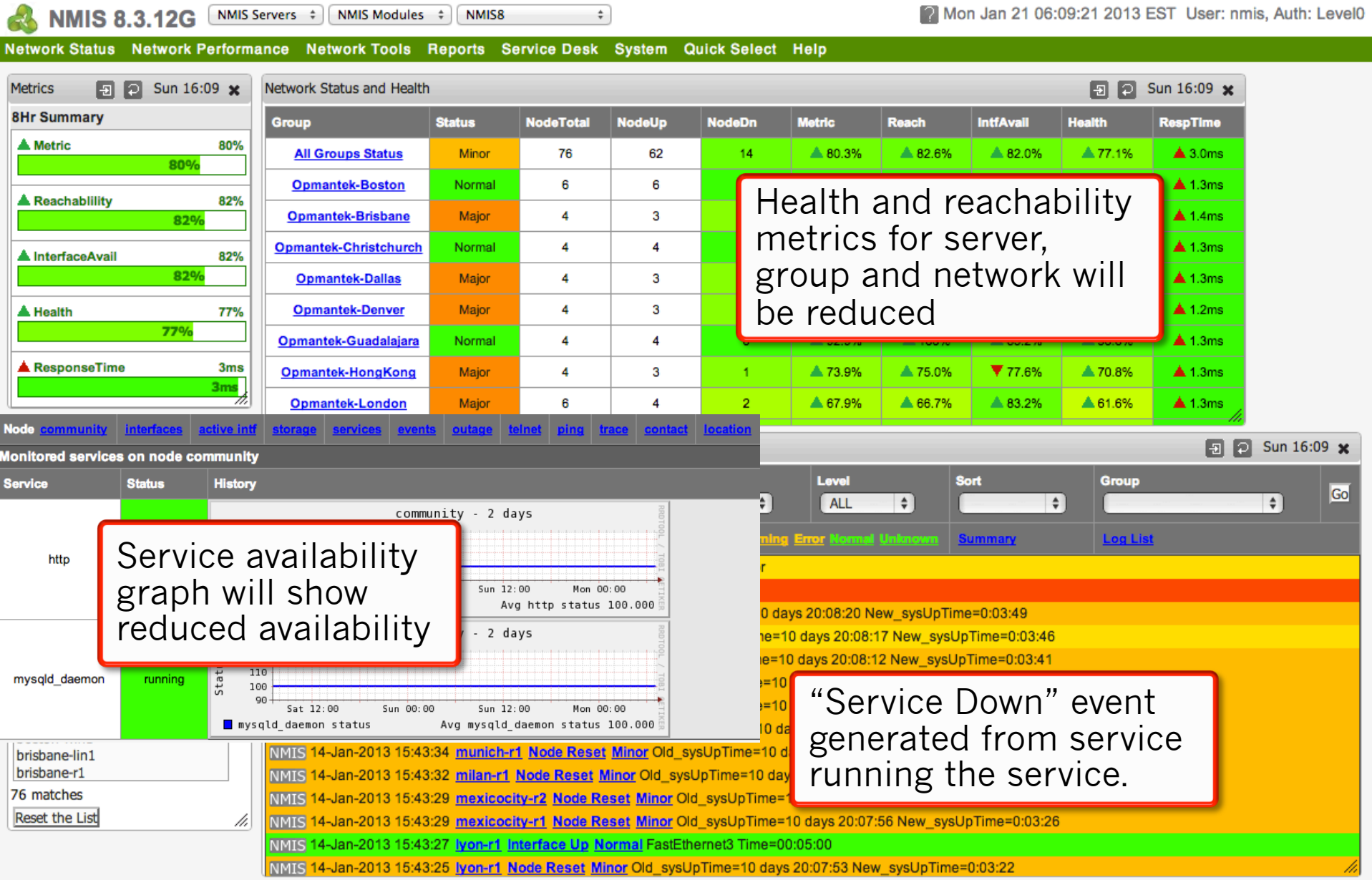
- Network is OK

NMIS8 Visibility:

- Health metrics for server, group and network will be reduced
- “Service Down” event generated from service running the service.
- Service availability graph will show reduced availability



Scenario 8: Related NMIS Visibility



Scenario 9: Routing problem

Business/Customer Impact:

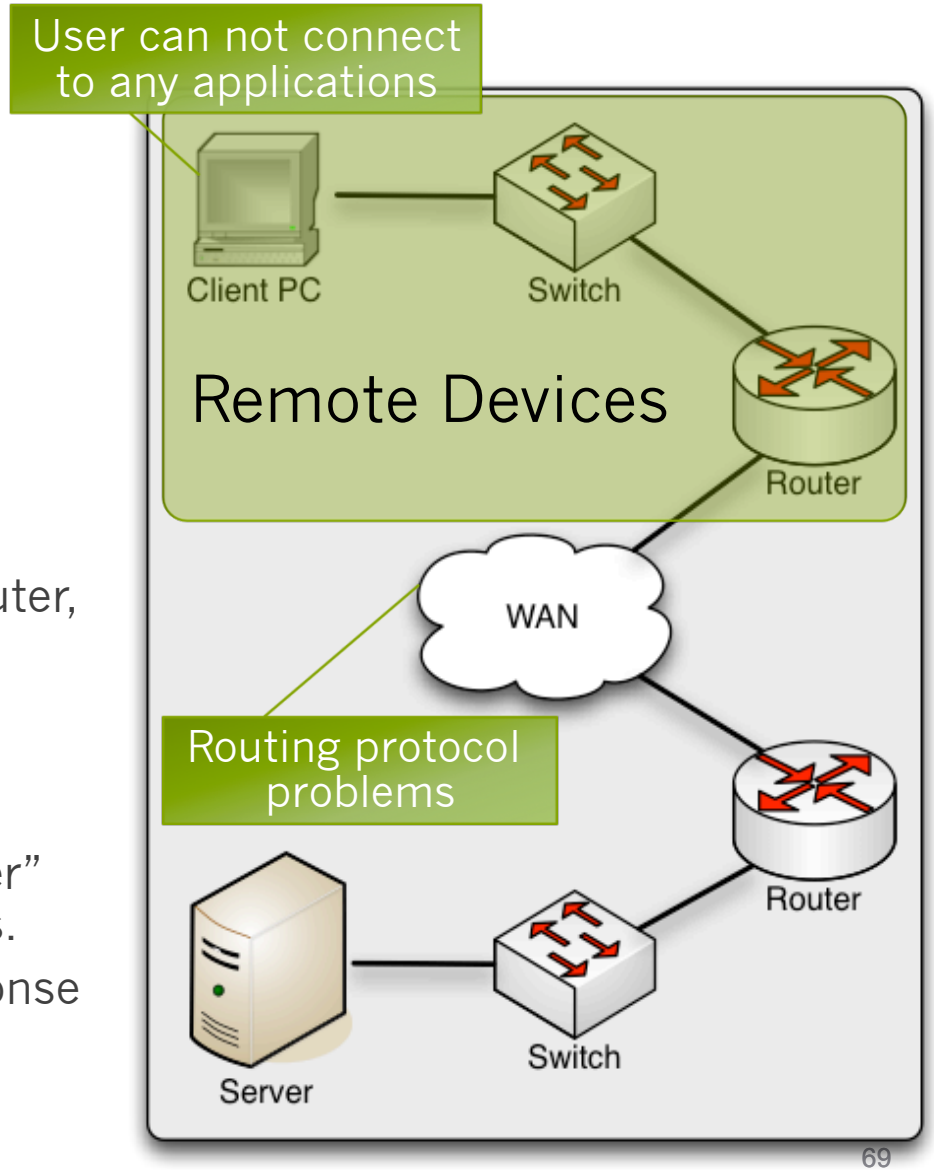
- User(s) unable to connect to any applications.

Technical Symptoms:

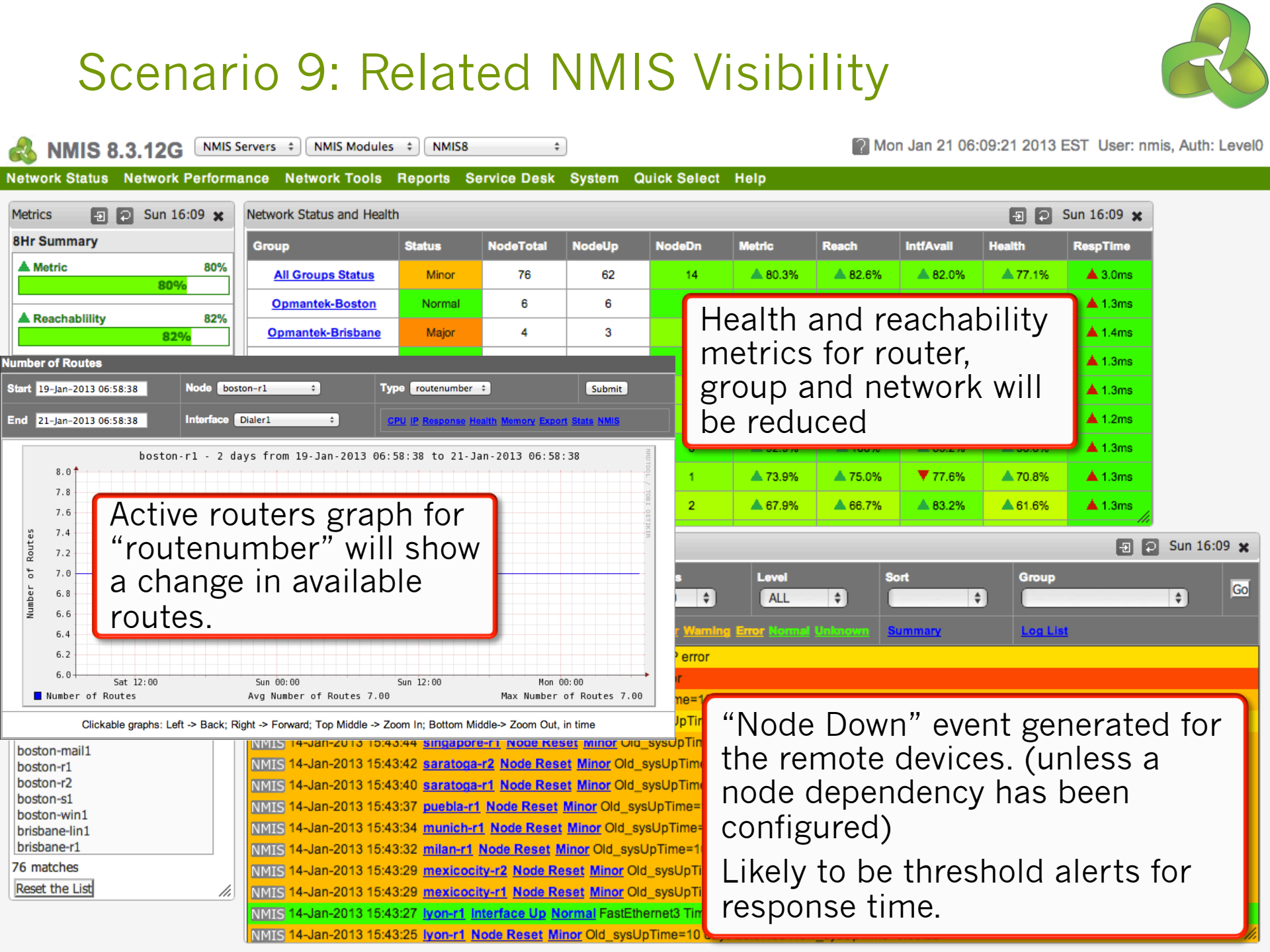
- User has connectivity to switch and router.
- Servers are OK

NMIS8 Visibility:

- Health and availability metrics for router, group and network will be reduced
- “Node Down” event generated for the remote devices. (unless a node dependency has been configured)
- Active routers graph for “routenumber” will show a change in available routes.
- Likely to be threshold alerts for response time.

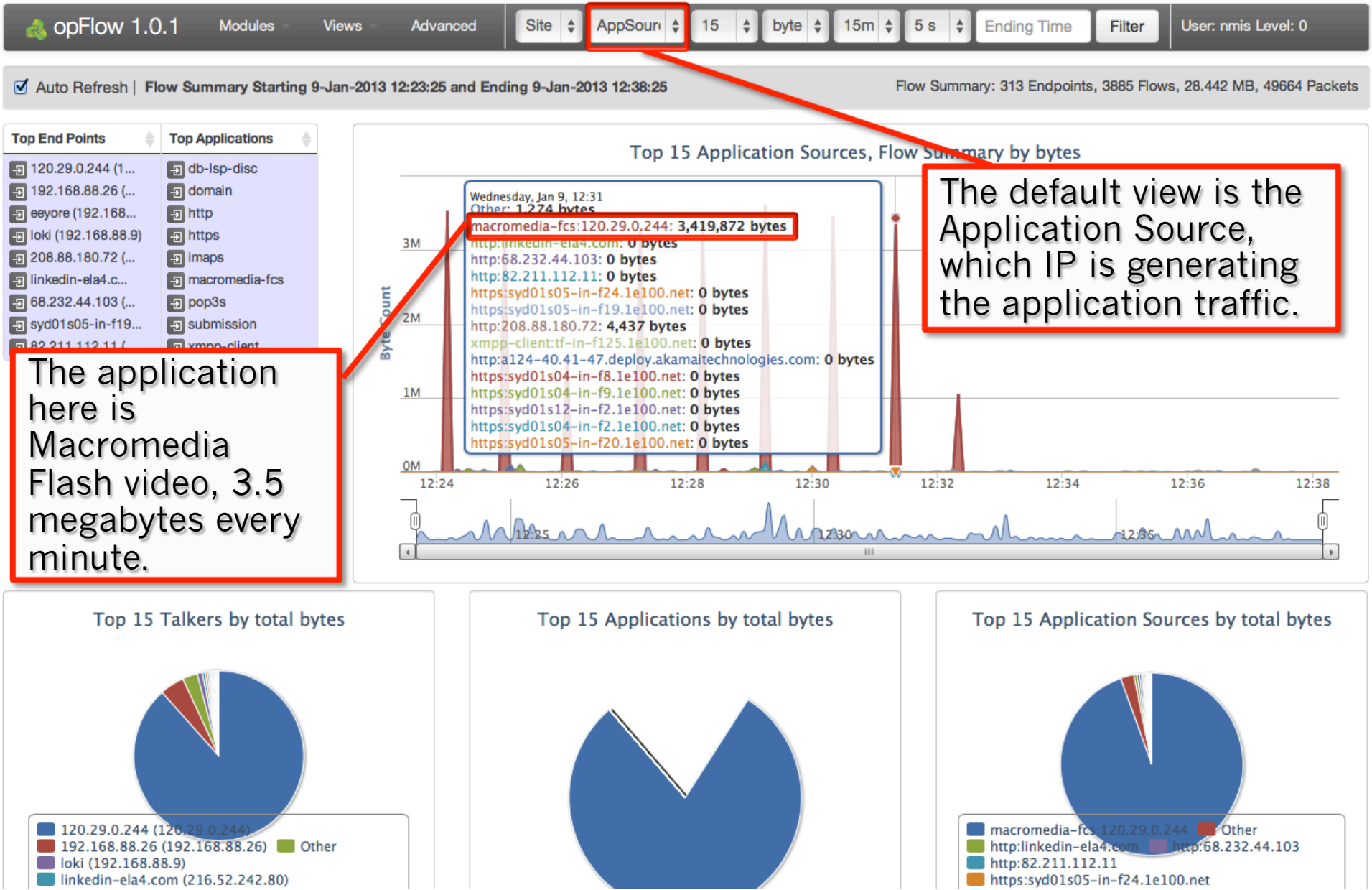


Scenario 9: Related NMIS Visibility

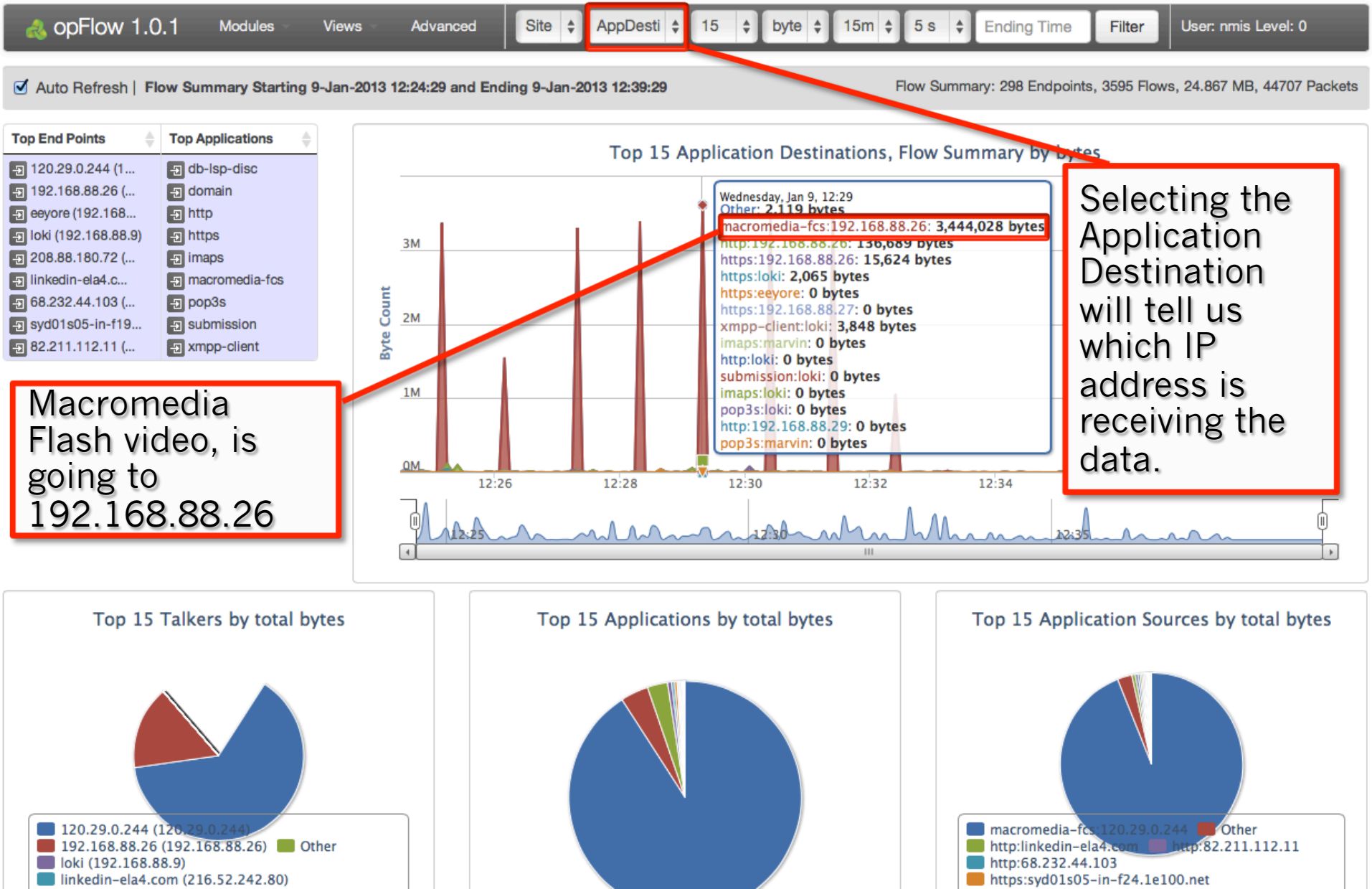


Application Troubleshooting Scenario

Using opFlow to Find Who – AppSource



Using opFlow to Find Who – AppDestination



Macromedia Flash video, is going to 192.168.88.26

Selecting the Application Destination will tell us which IP address is receiving the data.

Using opFlow to Find Who – Conversation Matrix

Selecting View and Conversation Matrix opens a new view with detailed data.

opFlow 1.0.1 | Modules | Views | Advanced | Site | AppSour | 100 | Level: 0

Auto Refresh | **Flow Summary Starting 9-Jan-2013 12:27:17 and Ending 9-Jan-2013 12:42:17** , 36747 Packets

Show 100 entries

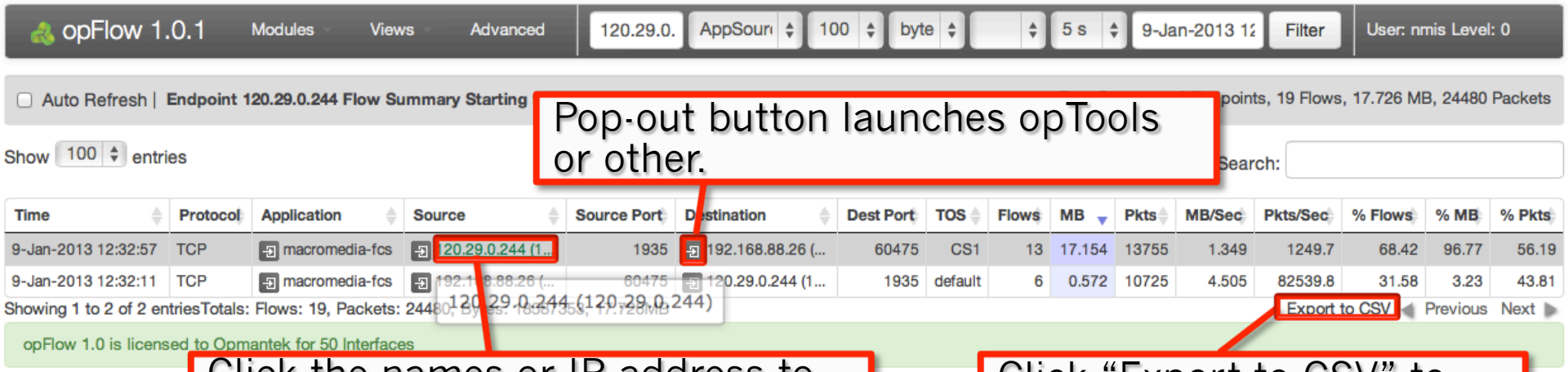
Search:

Time	Protocol	Application	Source	Source Port	Destination	Dest Port	TOS	Flows	MB	Pkts	MB/Sec	Pkts/Sec	% Flows	% MB	% Pkts
9-Jan-2013 12:32:57	TCP	macromedia-fcs	120.29.0.244 (1...	1935	192.168.88.26 (...	60475	CS1	13	17.154	13755	1.349	1249.7	0.36	84.64	37.43
9-Jan-2013 12:27:19	Other	Other			Other (Other)	Other	Other	2876	0.785	6694	0.000		79.80	3.87	18.22
9-Jan-2013 12:32:11	TCP	macromedia-fcs			20.29.0.244 (1...	1935	default	6	0.572	10725	4.505	82539.8	0.17	2.82	29.19
9-Jan-2013 12:40:49	TCP	http	ec2-174-129-201...	80	marvin (192.168...	54261	CS4	3	0.229	171	0.033	30.4	0.08	1.13	0.47
9-Jan-2013 12:39:29	TCP	https	syd01s04-in-f11...	443	marvin (192.168...	54258	CS4	1	0.123	96	0.569	444.4	0.03	0.61	0.26
9-Jan-2013 12:38:39	TCP	https	17.146.232.12 (...	443	loki (192.168.88.9)	56802	CS4	2	0.091	76	0.001	5.6	0.06	0.45	0.21
9-Jan-2013 12:34:38	TCP	https	syd01s05-in-f24...	443	192.168.88.26 (...									0.33	0.26
9-Jan-2013 12:41:49	TCP	imaps	we-in-f109.1e10...	993	loki (192.168.88.9)									0.33	0.28
9-Jan-2013 12:34:20	TCP	http	82.211.112.11 (...	80	192.168.88.26 (...									0.29	0.16
9-Jan-2013 12:41:49	TCP	xmpp-client	loki (192.168.88.9)	55551	tf-in-f125.1e10...									0.23	2.53
9-Jan-2013 12:41:49	TCP	xmpp-client	tf-in-f125.1e10...	5222	loki (192.168.88.9)									0.23	2.53
9-Jan-2013 12:34:20	TCP	http	82.211.112.11 (...	80	192.168.88.26 (...									0.21	0.16
9-Jan-2013 12:32:49	TCP	http	linkedin-ela4.c...	80	192.168.88.26 (...	60424	CS4	5	0.039	46	0.000	6.6	0.14	0.19	0.13
9-Jan-2013 12:32:18	TCP	https	syd01s04-in-f8....	443	eeyore (192.168...	55155	CS4	2	0.039	47	0.041	56.2	0.06	0.19	0.13
9-Jan-2013 12:39:59	TCP	https	loki (192.168.88.9)	56609	syd01s04-in-f2....	443	default	6	0.035	97	0.007	21.2	0.17	0.17	0.26
9-Jan-2013 12:41:29	TCP	https	syd01s05-in-f16...	443	loki (192.168.88.9)	57085	CS4	1	0.033	36	0.024	26.7	0.03	0.16	0.10
9-Jan-2013 12:40:49	TCP	http	ec2-174-129-201...	80	marvin (192.168...	54264	CS4	3	0.031	28	0.005	10.6	0.08	0.16	0.08
9-Jan-2013 12:39:34	TCP	http	s3-2.amazonaws....	80	marvin (192.168...	54287	CS4	1	0.031	24	0.023	17.8	0.03	0.15	0.07
9-Jan-2013 12:40:49	TCP	http	ec2-174-129-201...	80	marvin (192.168...	54262	CS4	3	0.030	27	0.005	10.4	0.08	0.15	0.07
9-Jan-2013 12:39:59	TCP	https	syd01s04-in-f2....	443	loki (192.168.88.9)	56609	CS4	6	0.025	79	0.004	19.0	0.17	0.13	0.21
9-Jan-2013 12:29:47	TCP	http	208.88.180.72 (...	80	192.168.88.26 (...	60483	CS4	4	0.024	33	0.018	28.7	0.11	0.12	0.09
9-Jan-2013 12:29:47	TCP	http	192.168.88.26 (...	60526	82.211.112.11 (...	80	default	1	0.022	66	0.001	2.3	0.03	0.11	0.18
9-Jan-2013 12:28:01	TCP	https	syd01s05-in-f19...	443	eeyore (192.168...	55153	CS4	2	0.021	23	0.016	25.3	0.06	0.11	0.06
9-Jan-2013 12:38:05	TCP	https	syd01s05-in-f19...	443	eeyore (192.168...	55166	CS4	2	0.021	22	0.018	21.9	0.06	0.11	0.06

120.29.0.244 (120.29.0.244)

This is the flow of data causing all the traffic, using 1.3 megabytes per second.

Using opFlow to Find Who – Filter and Export



getFullFlowMatrix-1.csv

Home | Layout | Tables | Charts | SmartArt | Formulas | Data | Review

O1 | packets_per_second

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
1	recv_time	src_ip	dst_ip	proto	tcpflags	src_port	dst_port	dscp	octets	packets	flows	application	duration	octets_per_second	packets_per_second	in_if	time	gate
2	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	3423784	2455	1	macromedia-fcs	0.984	3479455.285	2494.918699	10	1357698621	192.
3	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	18	60475	1935	default	110836	1992	1	macromedia-fcs	0.92	120473.913	2165.217391	1	1357698556	0.0.0
4	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	18	60475	1935	default	35990	649	1	macromedia-fcs	32.544	1105.887414	19.94223206	1	1357698731	0.0.0
5	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	1a	1935	60475	CS4	12753	176	1	macromedia-fcs	0.908	14045.15419	193.8325991	10	1357698439	192.
6	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	1a	60475	1935	default	110211	1924	1	macromedia-fcs	0.004	27552750	481000	1	1357698439	0.0.0
7	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	1049758	749	1	macromedia-fcs	7.968	131746.7369	94.00100402	10	1357698744	192.
8	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS4	3098	44	1	macromedia-fcs	20.804	148.9136704	2.114977889	10	1357698720	192.
9	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	18	60475	1935	default	113742	2044	1	macromedia-fcs	0.272	418169.1176	7514.705882	1	1357698680	0.0.0
10	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	3354925	2388	1	macromedia-fcs	0.94	3569069.149	2540.425532	10	1357698496	192.
11	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	3250406	2341	1	macromedia-fcs	0.832	3906737.981	2813.701923	10	1357698439	192.
12	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS4	13343	178	1	macromedia-fcs	0.132	101083.3333	1348.484848	10	1357698558	192.
13	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS4	13927	188	1	macromedia-fcs	2.576	5406.444099	72.98136646	10	1357698621	192.
14	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	3406836	2430	1	macromedia-fcs	0.96	3548787.5	2531.25	10	1357698680	192.
15	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS4	13036	178	1	macromedia-fcs	0.124	105129.0323	1435.483871	10	1357698691	192.
16	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS1	3430685	2452	1	macromedia-fcs	0.98	3500698.98	2502.040816	10	1357698558	192.
17	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	18	60475	1935	default	113830	2042	1	macromedia-fcs	0.96	118572.9167	2127.083333	1	1357698496	0.0.0
18	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	10	1935	60475	CS1	1492	1	1	macromedia-fcs	0.1	14920	10	10	1357698777	192.
19	2013-01-09T	192.168.88.26 (192.168.88.26)	120.29.0.244 (120.29.0.244)	TCP	18	60475	1935	default	115478	2074	1	macromedia-fcs	0.86	134276.7442	2411.627907	1	1357698621	0.0.0
20	2013-01-09T	120.29.0.244 (120.29.0.244)	192.168.88.26 (192.168.88.26)	TCP	18	1935	60475	CS4	13223	175	1	macromedia-fcs	0.848	15593.16038	206.3679245	10	1357698496	192.
21																		
22																		

Using opFlow to Find Who – opTools

opTools: Endpoint 120.29.0.244, tool traceroute output

Name: , IP: 120.29.0.244

```
/bin/traceroute  120.29.0.244
traceroute to 120.29.0.244 (120.29.0.244), 30 hops max, 60 byte packets
 1  asgard (192.168.88.254)  6.538 ms  8.201 ms  8.264 ms
 2  116.255.63.22 (116.255.63.22)  5.905 ms  5.963 ms  6.432 ms
 3  116.255.63.4 (116.255.63.4)  8.444 ms  8.571 ms  10.188 ms
 4  202.171.175.65 (202.171.175.65)  25.637 ms  26.189 ms  26.258 ms
 5  202.171.175.42 (202.171.175.42)  26.441 ms  26.668 ms  26.737 ms
 6  as24130.sydney.pipenetworks.com (218.100.2.3)  27.123 ms  22.977 ms  23.940 ms
 7  eth3-3.rn-639gardeners-mlx-03.pipenetworks.com (121.101.138.148)  40.555 ms  41.212
41.540 ms
 8  eth6-7.rn-400harris-mlx-03.pipenetworks.com (121.101.138.36)  41.517 ms  41.810 ms
27 ms
 9  eth8-1.rq-148brunswick-mlx-01.pipenetworks.com (121.101.138.167)  41.206 ms  42.874
43.345 ms
10  ve100.rq-148brunswick-cer-01.pipenetworks.com (121.101.138.3)  43.341 ms  44.025 ms
024 ms
11  ip-186-128-161-203.static.pipenetworks.com (203.161.128.186)  44.109 ms  44.448 ms
06 ms
12  * * *
13  v10.pe1.dc1-vars.onthenet.net (121.50.213.126)  40.301 ms  41.056 ms  41.051 ms
14  v10.pe1.dc1-vars.onthenet.net (121.50.213.126)  42.216 ms  42.196 ms  42.323 ms
15  120.29.0.244 (120.29.0.244)  42.433 ms  44.834 ms  44.851 ms
```

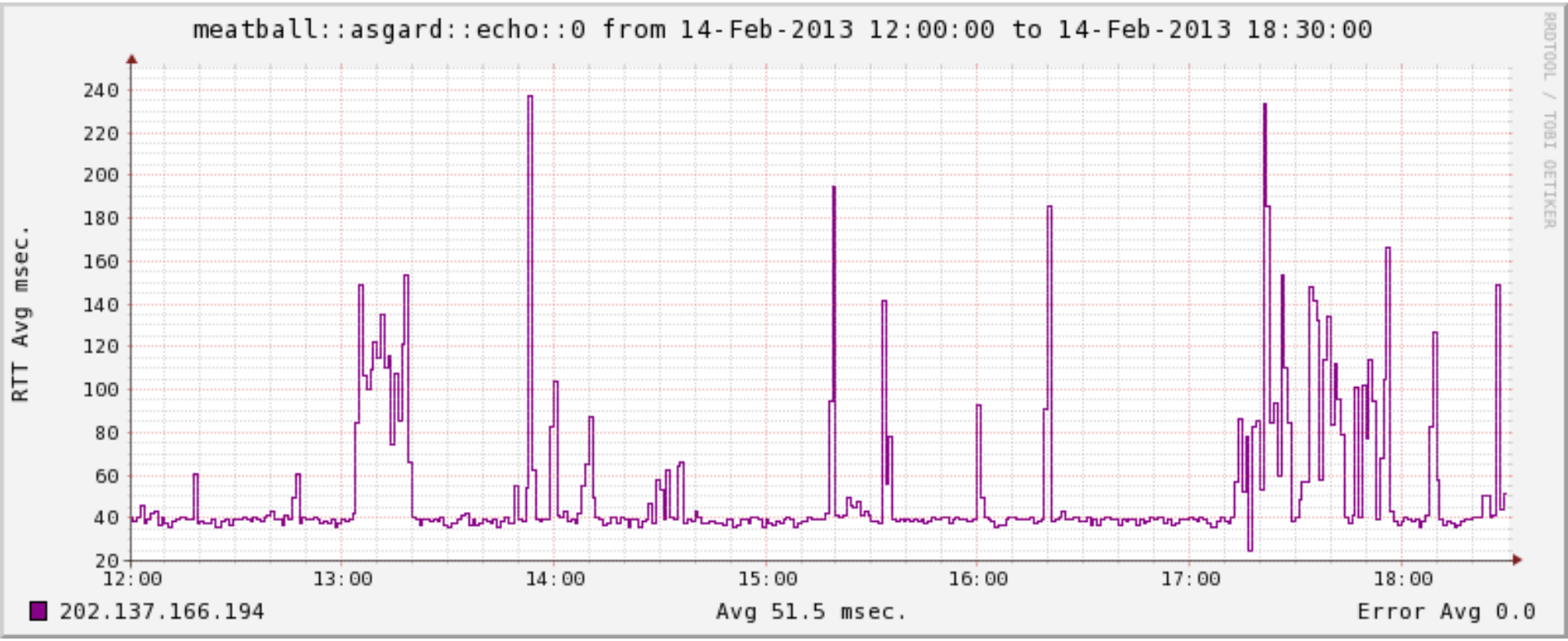
Clicking the Pop-out icon will go to opTools and you can use the tools to determine what and where the server is.

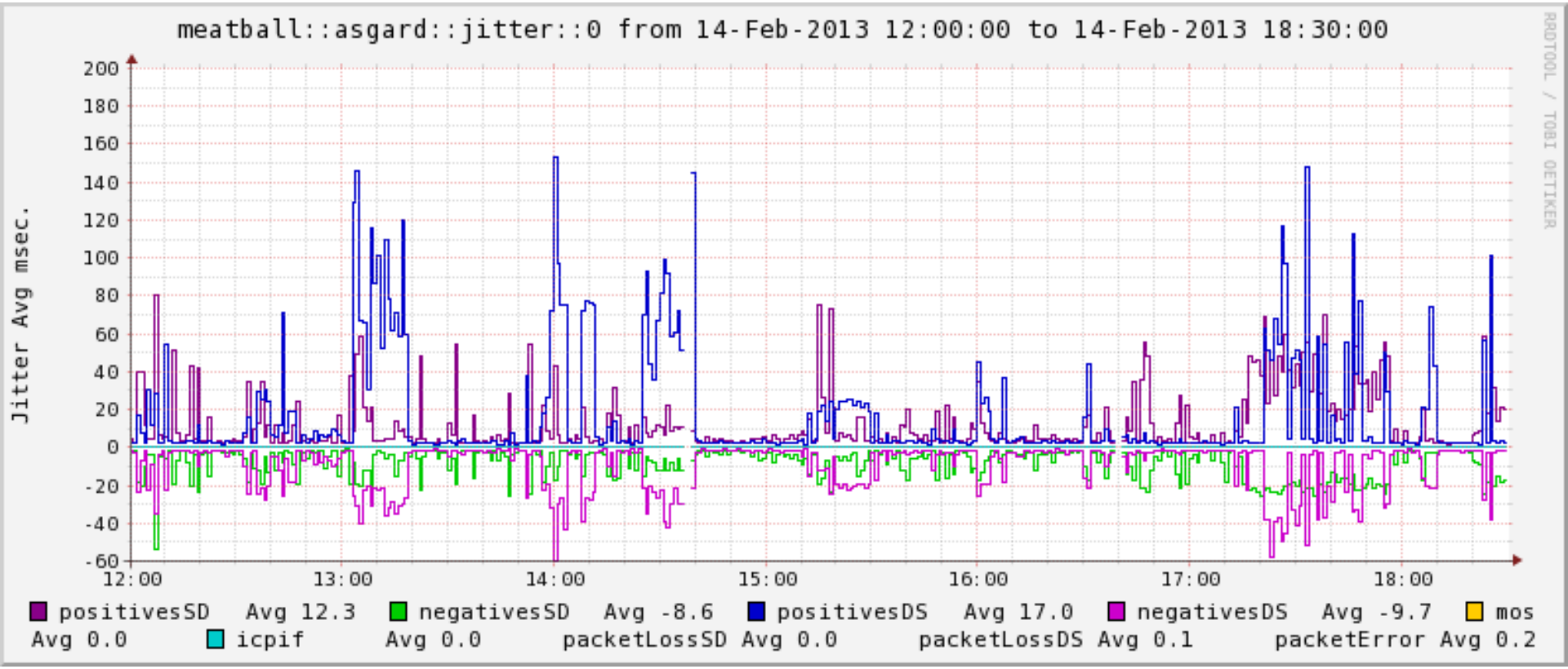
opTools: Endpoint 120.29.0.244, tool nmap output

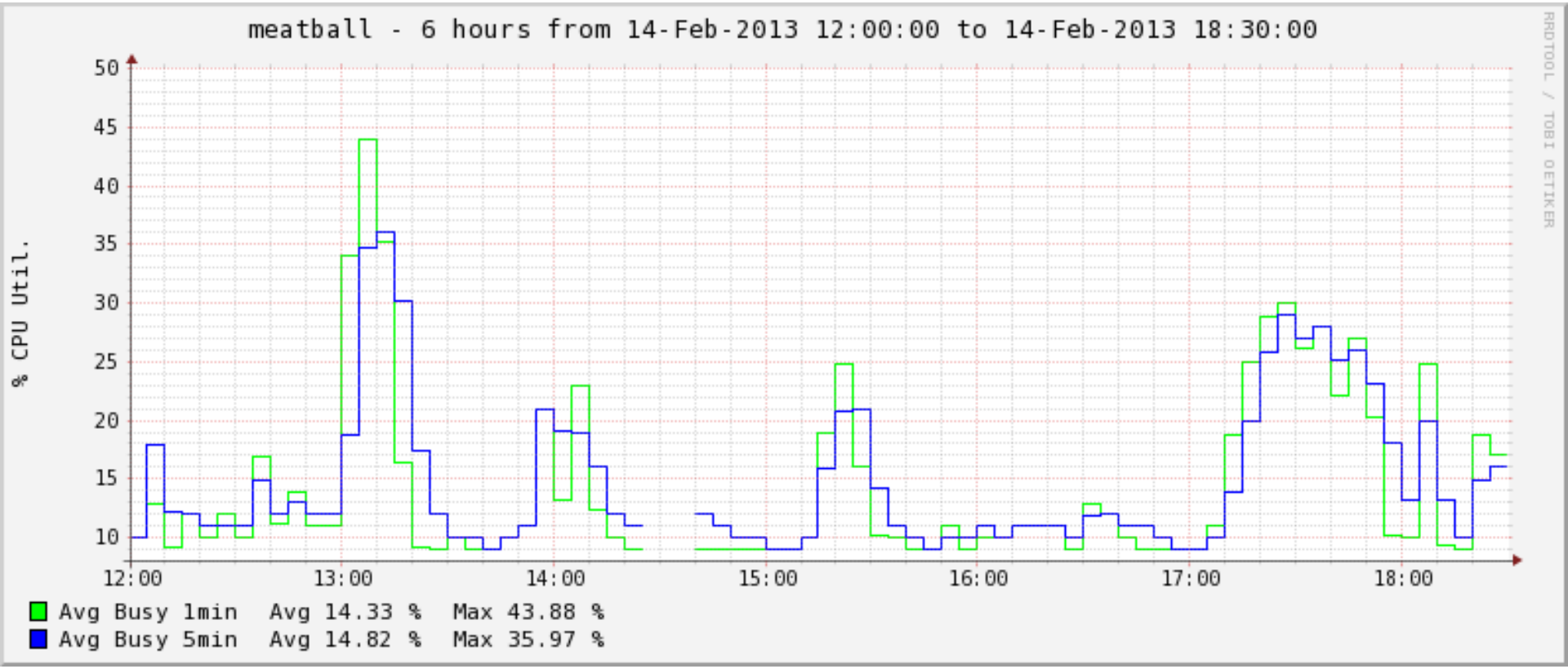
Name: , IP: 120.29.0.244

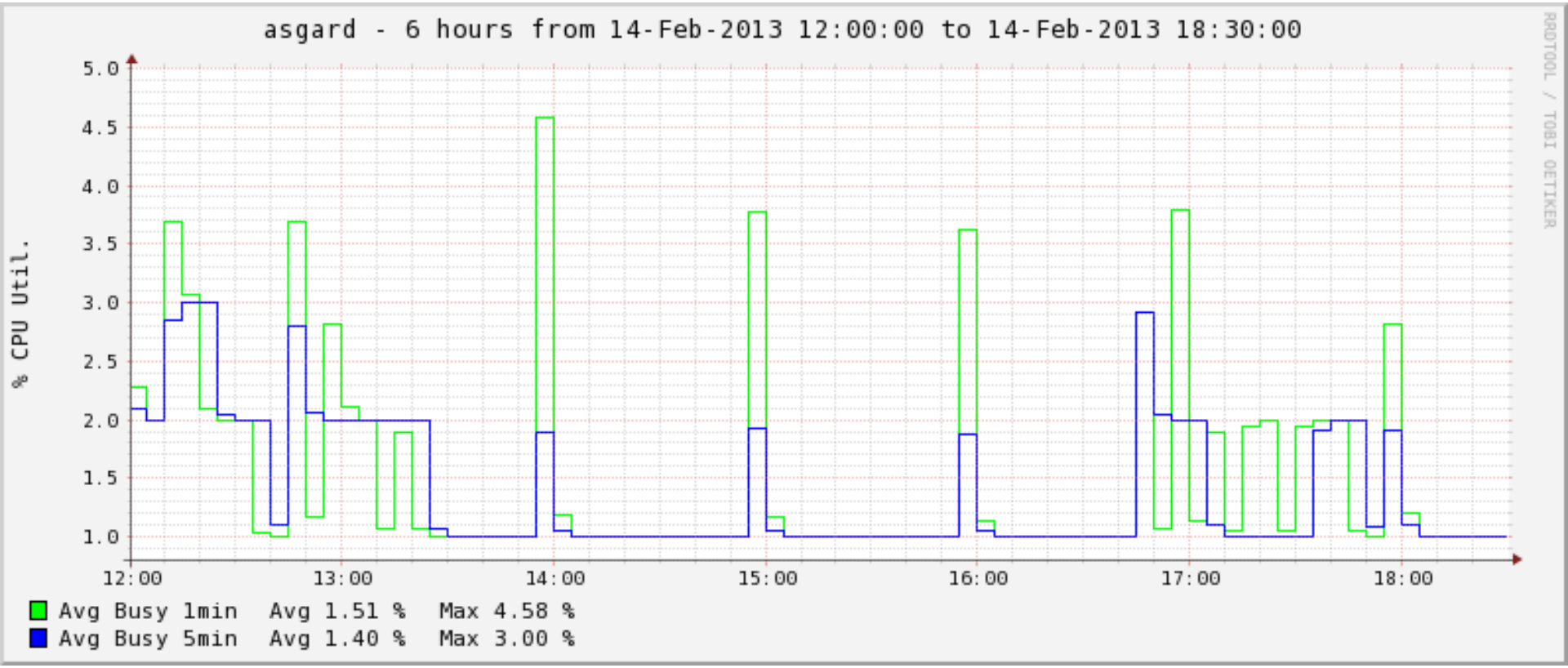
```
/usr/bin/nmap -v -F 120.29.0.244

Starting Nmap 5.21 ( http://nmap.org ) at 2013-01-09 12:44 EST
Initiating Ping Scan at 12:44
Scanning 120.29.0.244 [2 ports]
Completed Ping Scan at 12:44, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:44
Completed Parallel DNS resolution of 1 host. at 12:44, 0.17s elapsed
Initiating Connect Scan at 12:44
Scanning 120.29.0.244 [100 ports]
Discovered open port 111/tcp on 120.29.0.244
Discovered open port 554/tcp on 120.29.0.244
Discovered open port 22/tcp on 120.29.0.244
Discovered open port 80/tcp on 120.29.0.244
Completed Connect Scan at 12:44, 2.35s elapsed (100 total ports)
Nmap scan report for 120.29.0.244
Host is up (0.046s latency).
Not shown: 95 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
111/tcp  open     rpcbind
554/tcp  open     rtsp
2000/tcp filtered cisco-sccp

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```

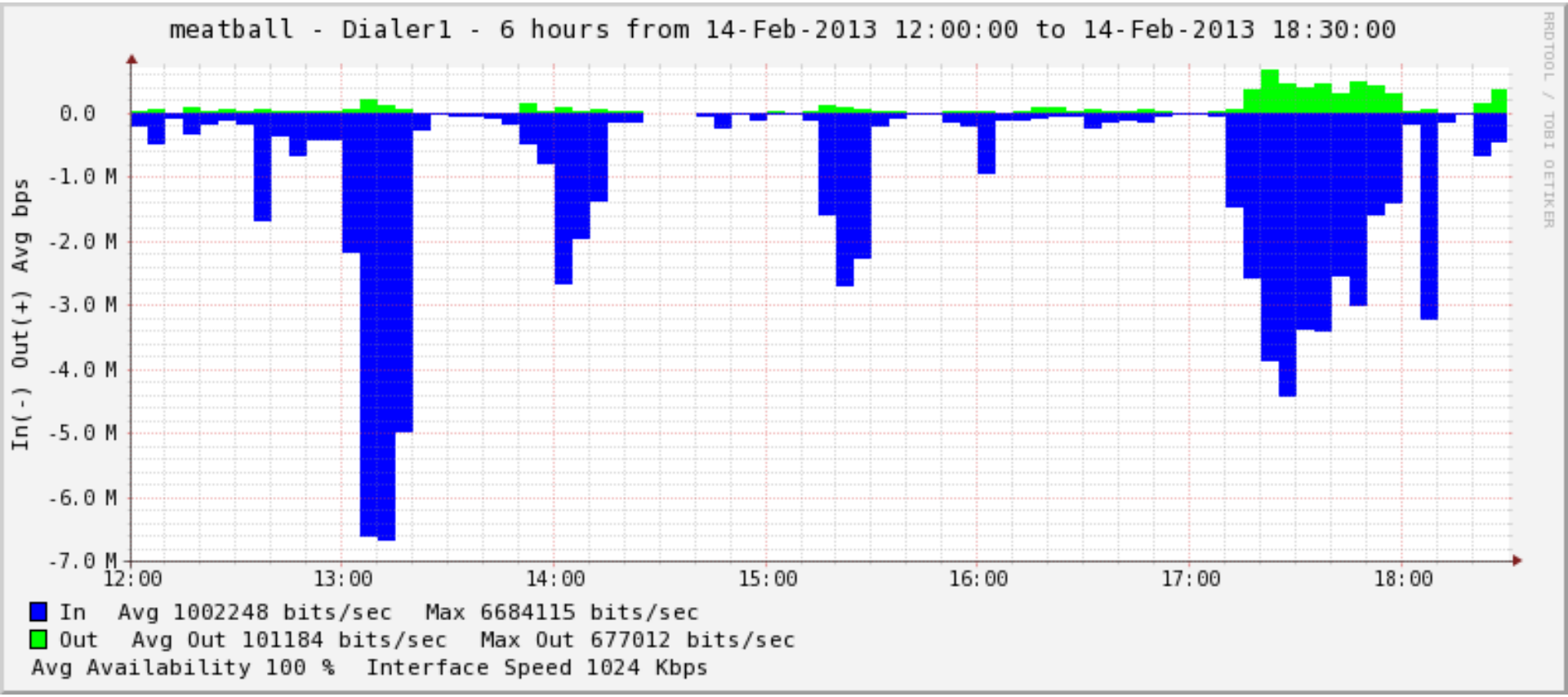
Network Troubleshooting Scenario

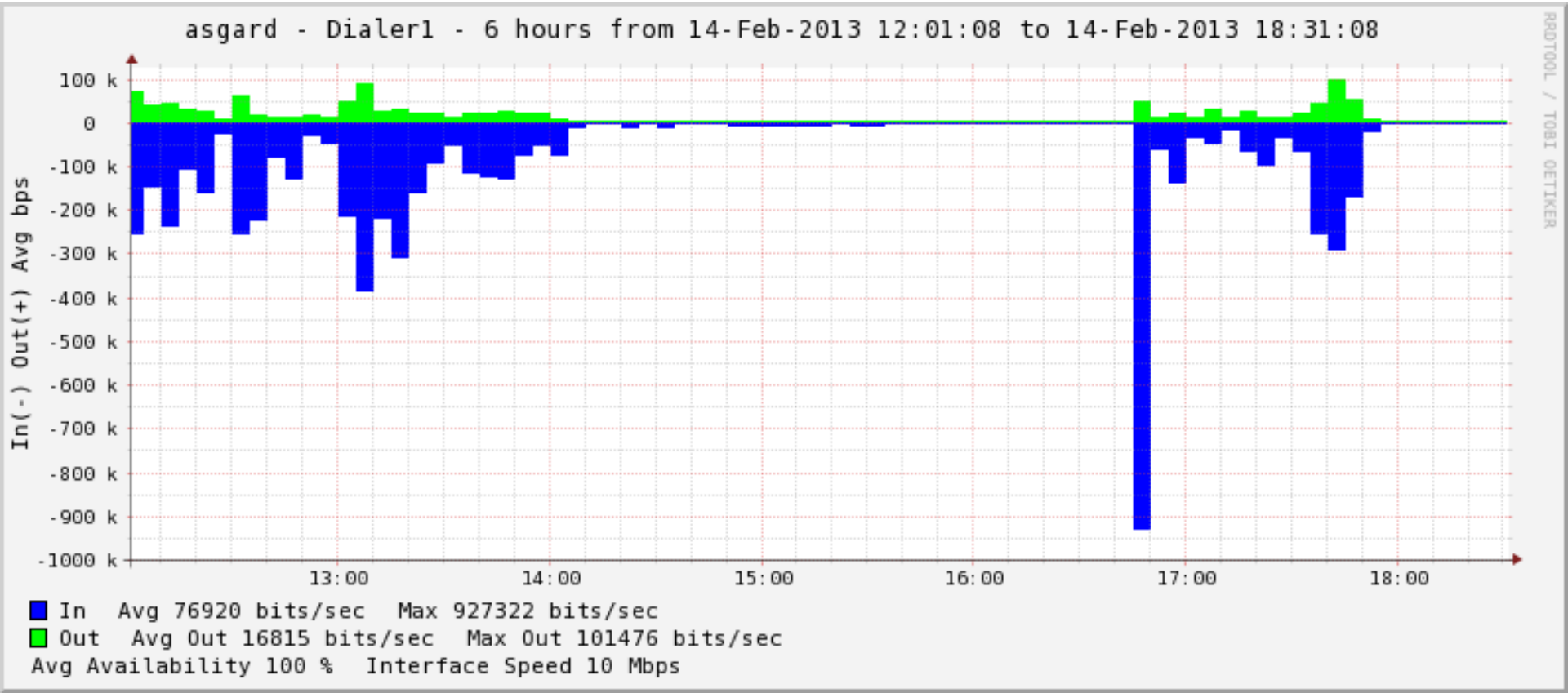

meatball::asgard::echo::0 from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
RTT Avg msec.
240
220
200
180
160
140
120
100
80
60
40
20
12:00
13:00
14:00
15:00
16:00
17:00
18:00
202.137.166.194
Avg 51.5 msec.
Error Avg 0.0
RRDTOOL / TOBI OETIKER

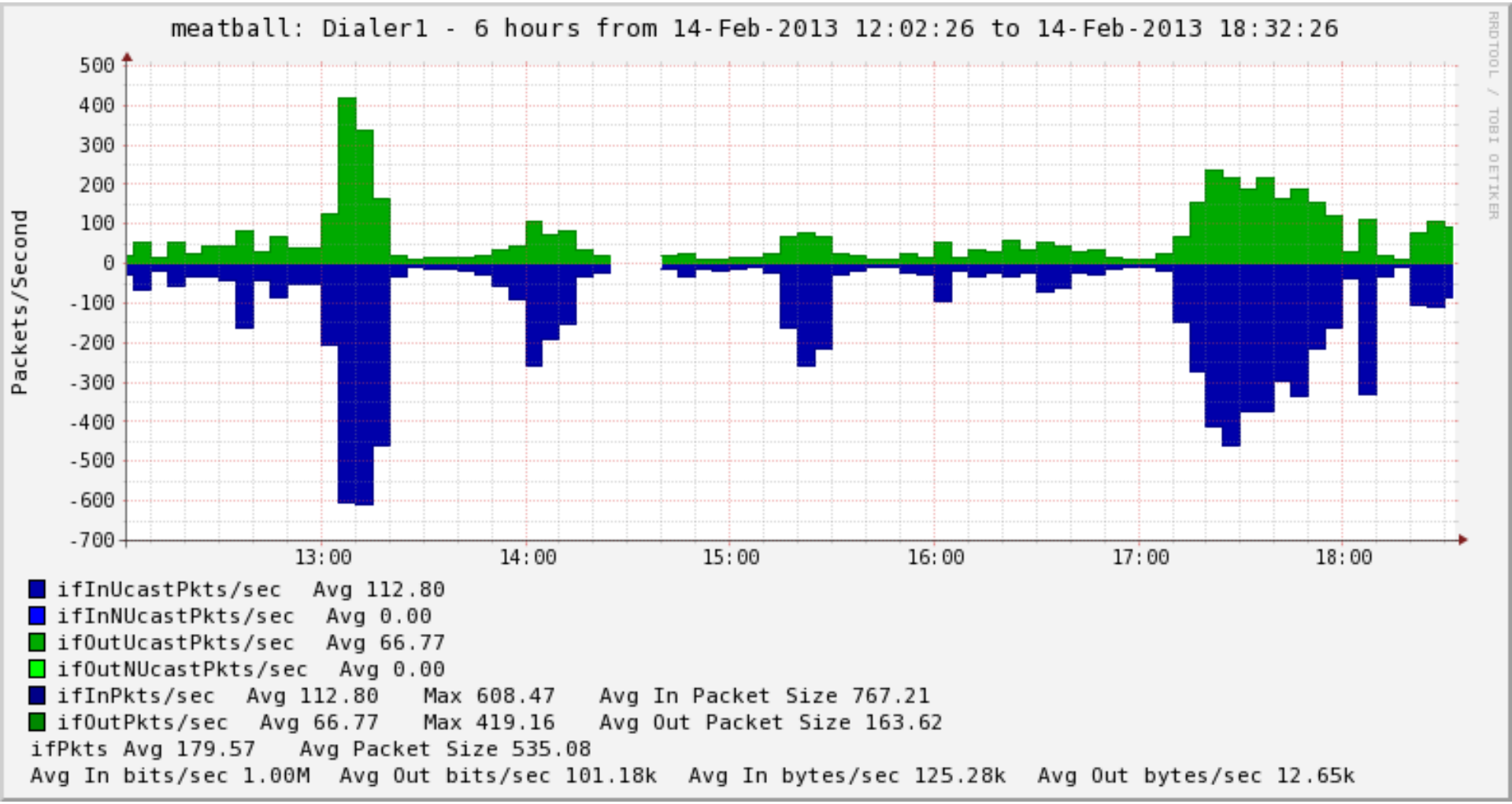

meatball::asgard::jitter::0 from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
Jitter Avg msec.
200
180
160
140
120
100
80
60
40
20
0
-20
-40
-60
12:00
13:00
14:00
15:00
16:00
17:00
18:00
RRDTOOL / TOBI OETIKER
positivesSD Avg 12.3
negativesSD Avg -8.6
positivesDS Avg 17.0
negativesDS Avg -9.7
mos Avg 0.0
icpif Avg 0.0
packetLossSD Avg 0.0
packetLossDS Avg 0.1
packetError Avg 0.2

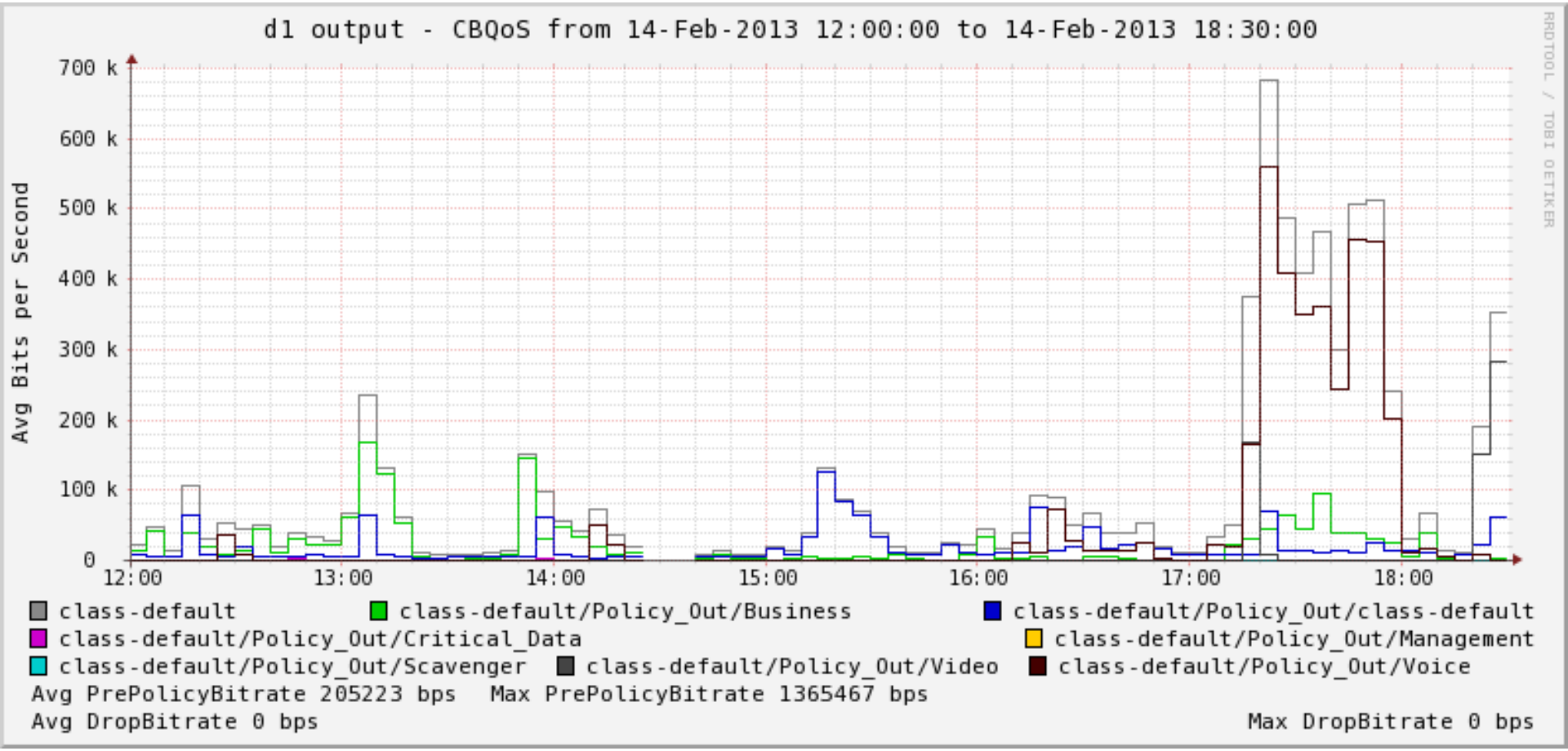

meatball - 6 hours from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
% CPU Util.
50
45
40
35
30
25
20
15
10
12:00
13:00
14:00
15:00
16:00
17:00
18:00
Avg Busy 1min Avg 14.33 % Max 43.88 %
Avg Busy 5min Avg 14.82 % Max 35.97 %
RRDTOOL / TOBI OETIKER

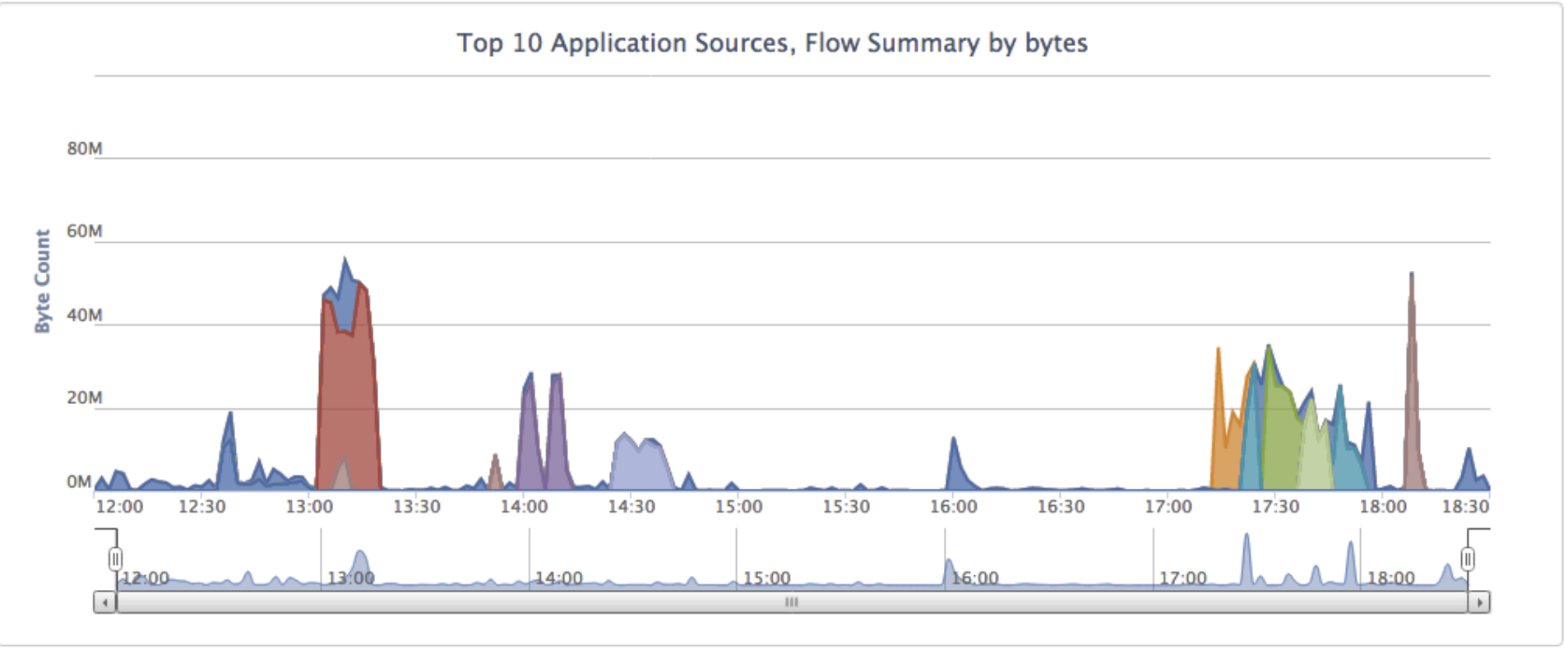

asgard - 6 hours from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
% CPU Util.
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
12:00
13:00
14:00
15:00
16:00
17:00
18:00
Avg Busy 1min Avg 1.51 % Max 4.58 %
Avg Busy 5min Avg 1.40 % Max 3.00 %
RRDTOOL / TOBI OETIKER

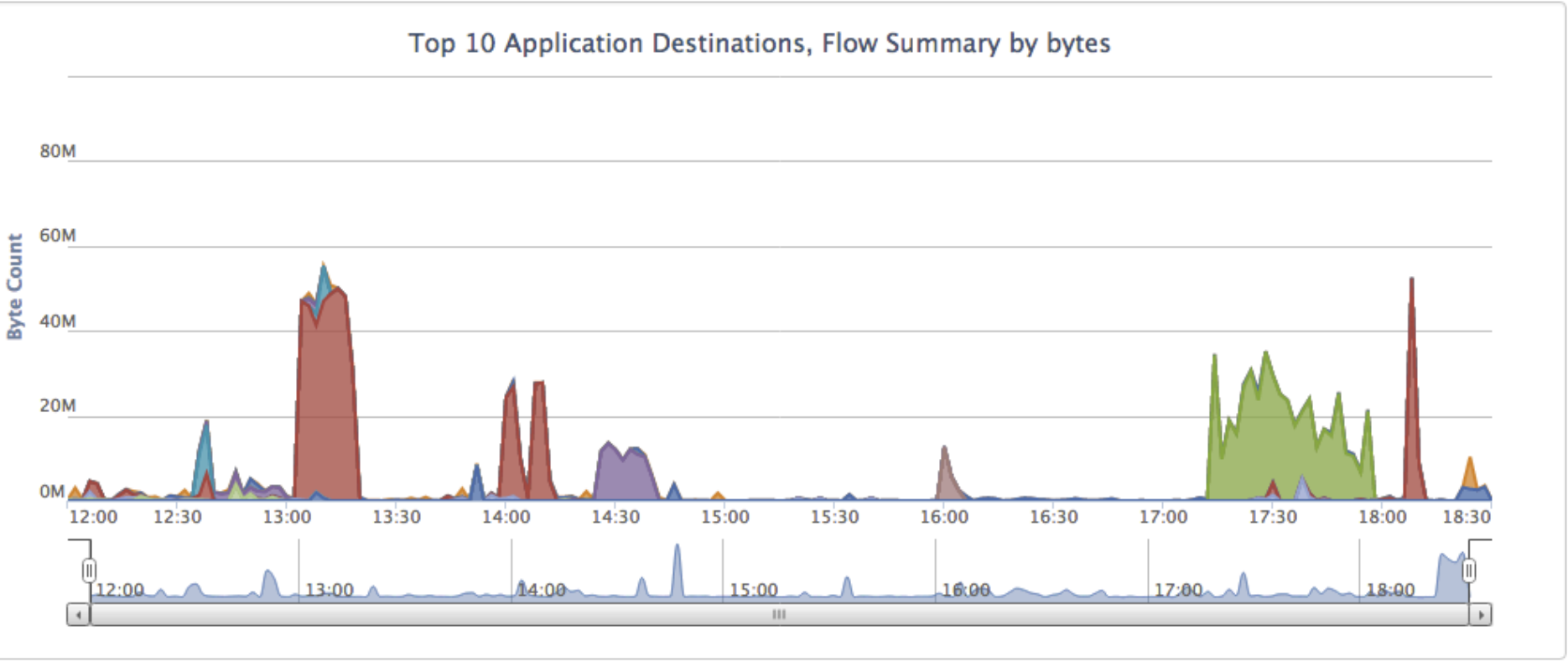

meatball - Dialer1 - 6 hours from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
In(-) Out(+) Avg bps
0.0
-1.0 M
-2.0 M
-3.0 M
-4.0 M
-5.0 M
-6.0 M
-7.0 M
12:00
13:00
14:00
15:00
16:00
17:00
18:00
In Avg 1002248 bits/sec Max 6684115 bits/sec
Out Avg Out 101184 bits/sec Max Out 677012 bits/sec
Avg Availability 100 % Interface Speed 1024 Kbps
RRDTOOL / TOBI OETIKER

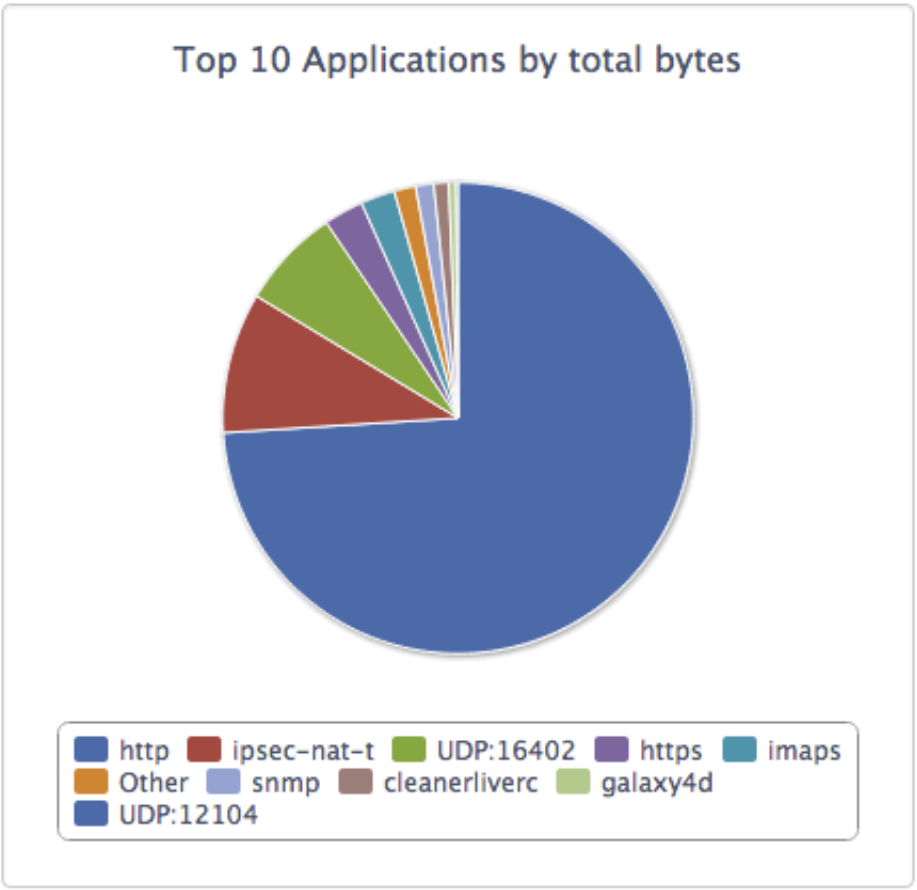

asgard - Dialer1 - 6 hours from 14-Feb-2013 12:01:08 to 14-Feb-2013 18:31:08
In(-) Out(+) Avg bps
100 k
0
-100 k
-200 k
-300 k
-400 k
-500 k
-600 k
-700 k
-800 k
-900 k
-1000 k
13:00
14:00
15:00
16:00
17:00
18:00
In Avg 76920 bits/sec Max 927322 bits/sec
Out Avg Out 16815 bits/sec Max Out 101476 bits/sec
Avg Availability 100 % Interface Speed 10 Mbps
RRDTOOL / TOBI OETIKER

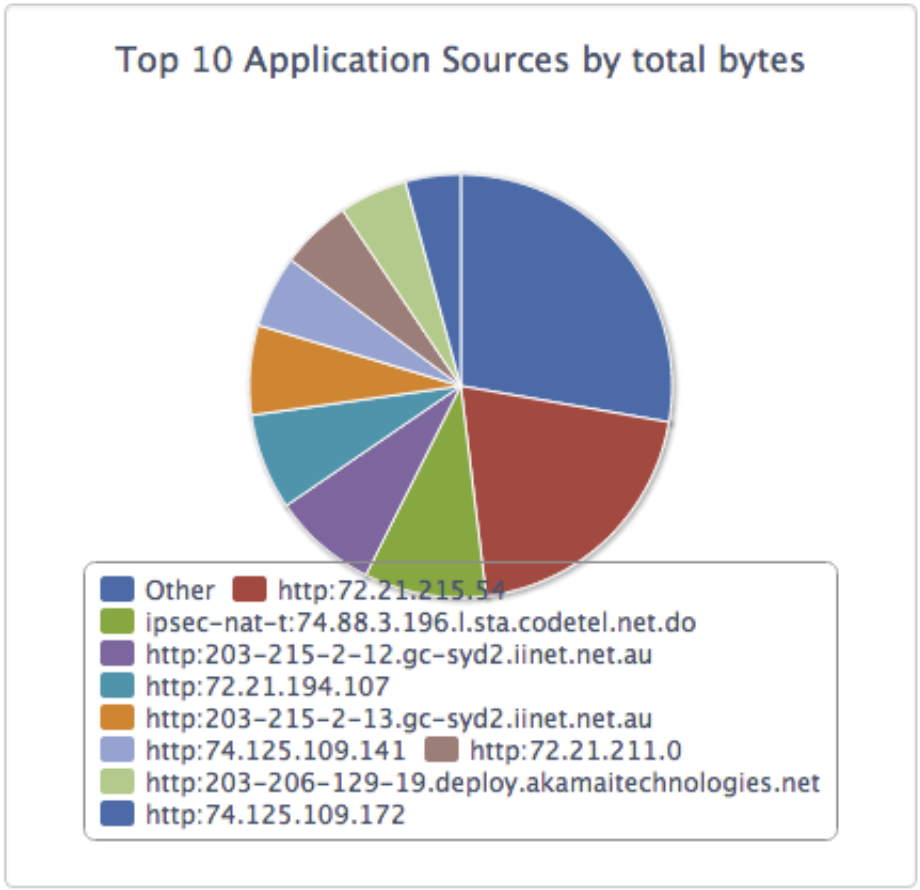

meatball: Dialer1 - 6 hours from 14-Feb-2013 12:02:26 to 14-Feb-2013 18:32:26
Packets/Second
500
400
300
200
100
0
-100
-200
-300
-400
-500
-600
-700
13:00
14:00
15:00
16:00
17:00
18:00
RRDTOOL / TOBI OETIKER
ifInUcastPkts/sec Avg 112.80
ifInNUcastPkts/sec Avg 0.00
ifOutUcastPkts/sec Avg 66.77
ifOutNUcastPkts/sec Avg 0.00
ifInPkts/sec Avg 112.80 Max 608.47 Avg In Packet Size 767.21
ifOutPkts/sec Avg 66.77 Max 419.16 Avg Out Packet Size 163.62
ifPkts Avg 179.57 Avg Packet Size 535.08
Avg In bits/sec 1.00M Avg Out bits/sec 101.18k Avg In bytes/sec 125.28k Avg Out bytes/sec 12.65k

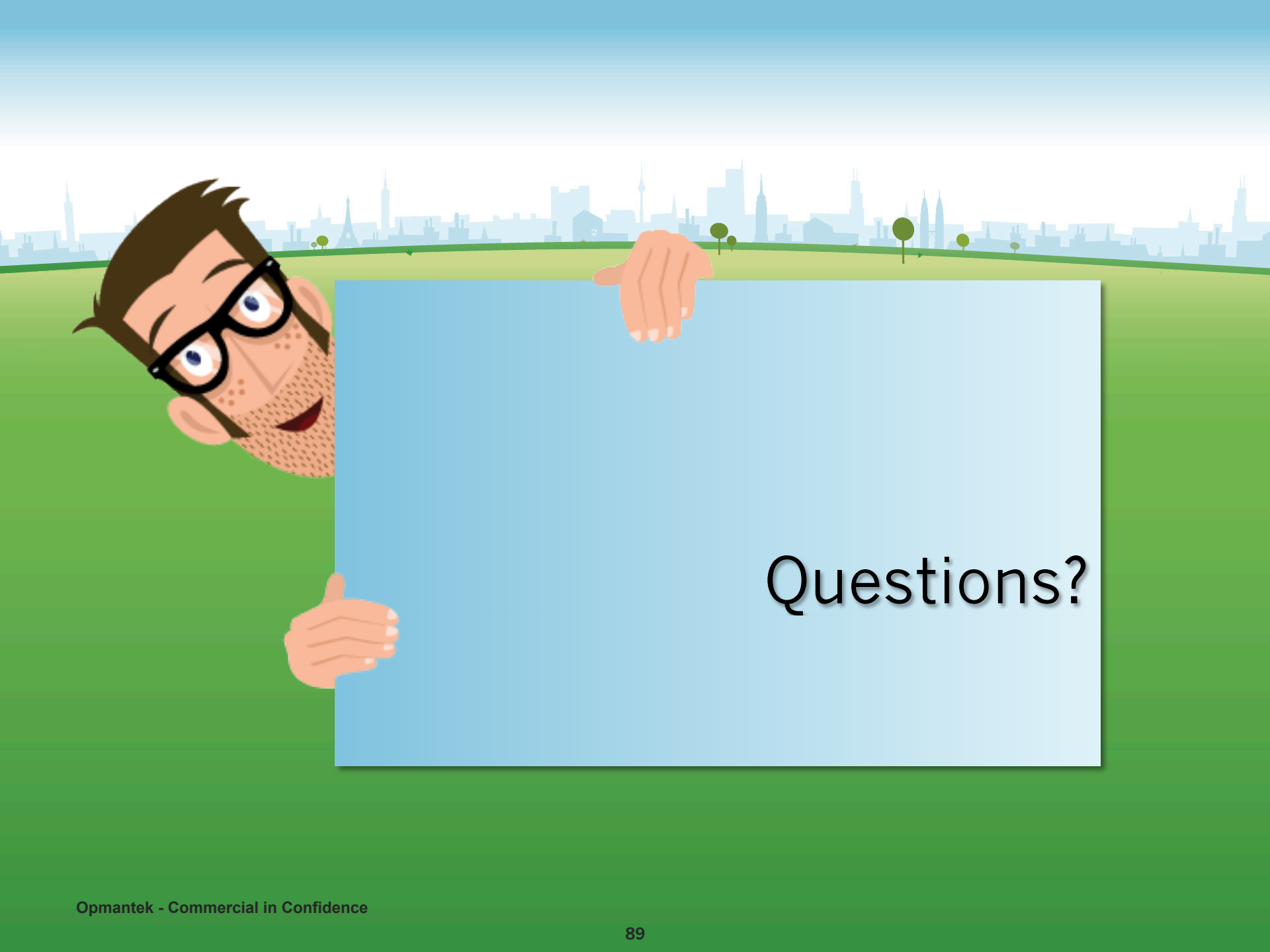

d1 output - CBQoS from 14-Feb-2013 12:00:00 to 14-Feb-2013 18:30:00
Avg Bits per Second
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
12:00
13:00
14:00
15:00
16:00
17:00
18:00
RRDTOOL / TOBI OETIKER
class-default
class-default/Policy_Out/Business
class-default/Policy_Out/class-default
class-default/Policy_Out/Critical_Data
class-default/Policy_Out/Management
class-default/Policy_Out/Scavenger
class-default/Policy_Out/Video
class-default/Policy_Out/Voice
Avg PrePolicyBitrate 205223 bps
Max PrePolicyBitrate 1365467 bps
Avg DropBitrate 0 bps
Max DropBitrate 0 bps


Top 10 Application Sources, Flow Summary by bytes
Byte Count
80M
60M
40M
20M
0M
12:00
12:30
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
17:00
17:30
18:00
18:30
12:00
13:00
14:00
15:00
16:00
17:00
18:00


Top 10 Application Destinations, Flow Summary by bytes
Byte Count
80M
60M
40M
20M
0M
12:00
12:30
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
17:00
17:30
18:00
18:30
12:00
13:00
14:00
15:00
16:00
17:00
18:00


Top 10 Applications by total bytes
http
ipsec-nat-t
UDP:16402
https
imaps
Other
snmp
cleanerliverc
galaxy4d
UDP:12104


Top 10 Application Sources by total bytes
Other
http:72.21.215.54
ipsec-nat-t:74.88.3.196.l.sta.codetel.net.do
http:203-215-2-12.gc-syd2.iinet.net.au
http:72.21.194.107
http:203-215-2-13.gc-syd2.iinet.net.au
http:74.125.109.141
http:72.21.211.0
http:203-206-129-19.deploy.akamaitechnologies.net
http:74.125.109.172


Questions?