

Monitoring your network with LibreNMS

DKNOG8 Mar 8-9th 2018

www.librenms.org

Neil Lathwood

History

History

Fork of

- Actual fork was Oct 2013
- Last GPL code May 2012
- 18 months code regression

Initial fork was done by:

- Paul Gear (Project founder) (@paulgear1)
- Tyler Christiansen (@supertylerc)

Overview

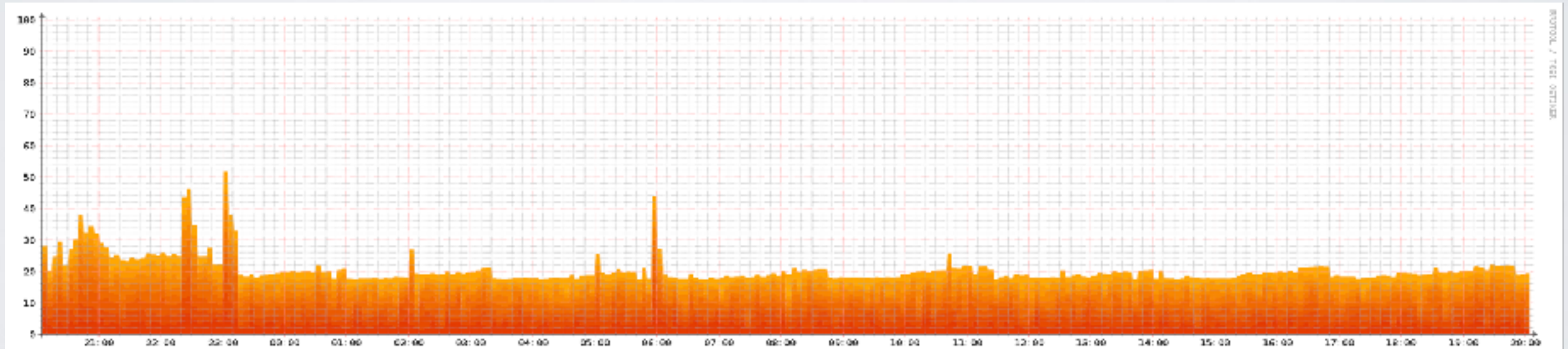
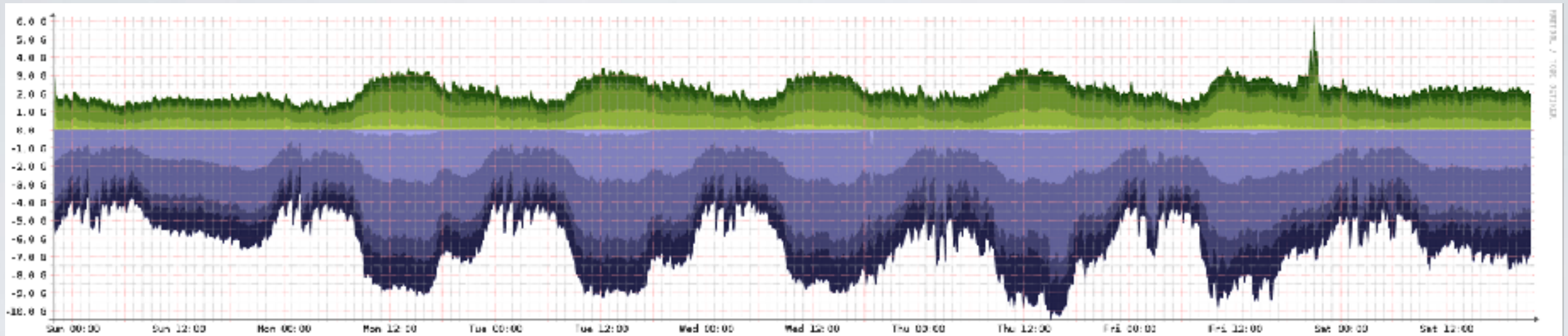
- Open source - GPLv3
- Community driven
- Aim to be inclusive to everyone
- 5 Years old this year - Party?

What is LibreNMS?

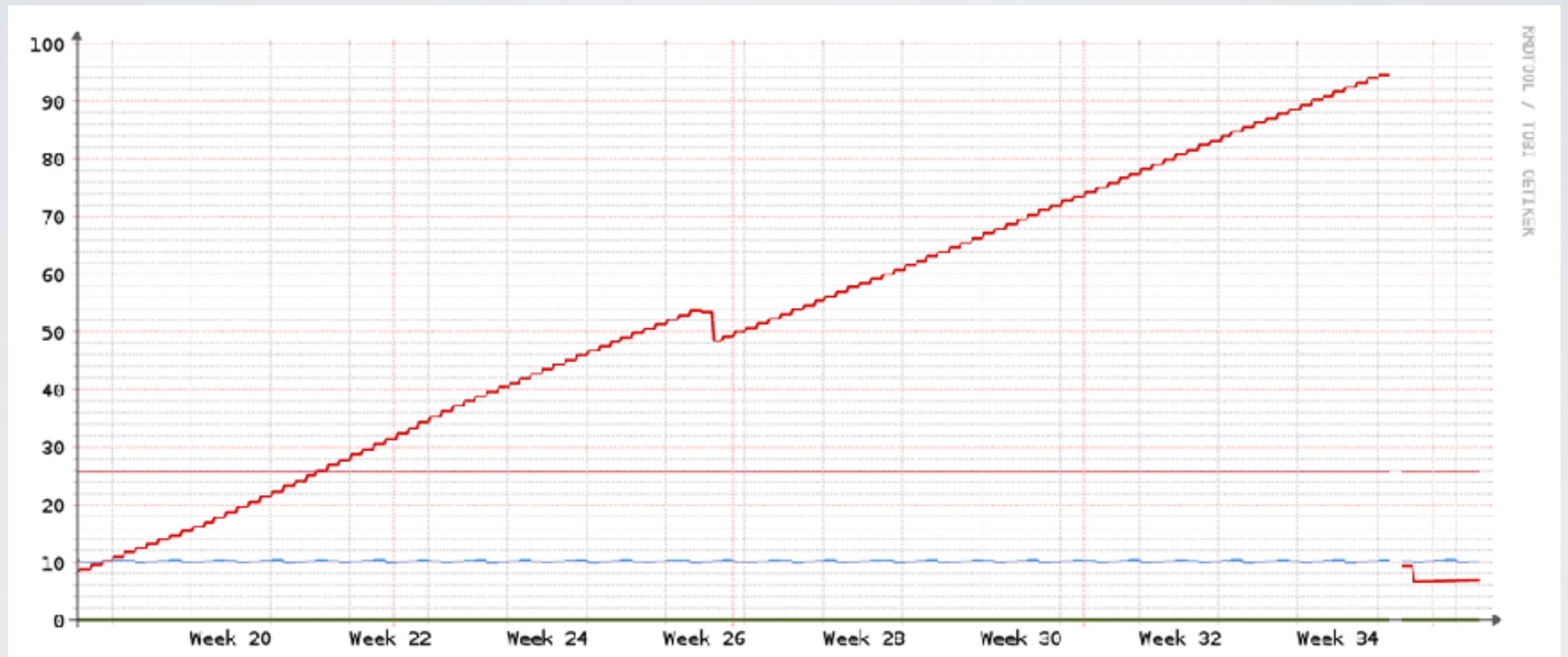
Auto-discovering NMS

- PHP / MySQL based
- Network and Inventory information
- Data collection is done via SNMP
- Data storage via RRDTool / InfluxDB / Graphite / OpenTSDB
- Graphing via RRDTool - up and to the right

Like this



But not like this :(



GitHub Statistics

- 480+ Contributors
- 14k+ Commits
- 5k+ Pull requests
- 2.5k+ Issues

Installation

Installation

Manual install from GitHub / Composer

Virtual images available including 3rd party docker container.

User contributed automation scripts

- Ansible
- Chef

Vendor support

Vendor Support

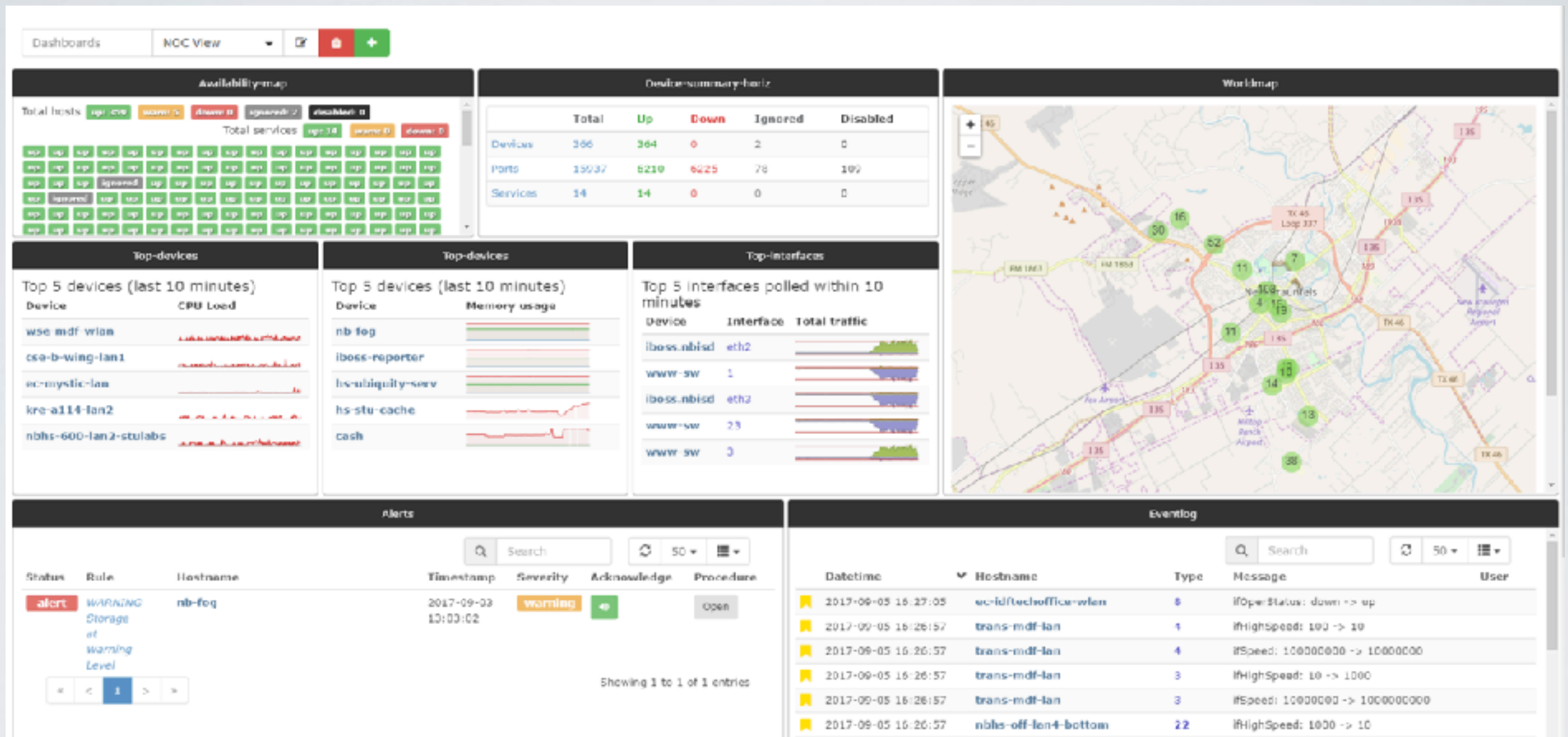
- Detection for over 350 vendors
- Continuously adding or improving support
- Working to simplify adding additional support
- Moving to yaml for detection
- OS Discovery done
- Health / Sensor Discovery done
- Processor Discovery done

Features

Auto-discovery

- CDP, LLDP or FDP
- SNMP Scan
- Even OSPF, ARP and BGP
- Service discovery

Dashboards



Alerting

Simple rule

```
%bgpPeers.bgpPeerState != "established" && x
```

```
%macros.device_up = "1" && x
```

Not so simple rule

%macros.device_up = "1" && x

%devices.os = "ios" && x

%devices.serial ~ "SN123.*" && x

%devices.hostname ~ "lax01.dc01.*" && x

%devices.version ~ "15.2.*" && x

%devices.location != "Buckingham Palace" && x

%devices.sysContact = "webmaster@librenms.org" && x

%devices.bgpLocalAs = "65001" && x

Alert rules v2

☐ NOT **AND** ☒ OR

[+ Add rule](#) [+ Add group](#)

bgpPeers.bgpPeerState

not equal

established

Delete

macros.device_up

equal

☐ No ☒ Yes

Delete

☐ NOT **AND** ☒ OR

[+ Add rule](#) [+ Add group](#)

wireless_sensors.senso...

greater or equal

`wireless_sensors.sensor_limit`

Delete

wireless_sensors.senso...

equal

1

Delete

macros.device_up

equal

☐ No ☒ Yes

Delete

Transports

- 20+ transports available
- Email, IRC, Slack + More
- Even obscure ones like Syslog and Elasticsearch

Templates

:(Needs to be re-done

%title

Severity: %severity

{if %state == 0}

Time elapsed: %elapsed

{/if}Timestamp: %timestamp

Unique-ID: %uid

Rule: %name

{if %faults}Faults:

{foreach %faults} #%key: %value.string

{/foreach}

{/if}

Templates

Alert for device localhost - Testing localhost

Severity: critical

Timestamp: 2018-03-05 18:32:11

Unique-ID: 1271

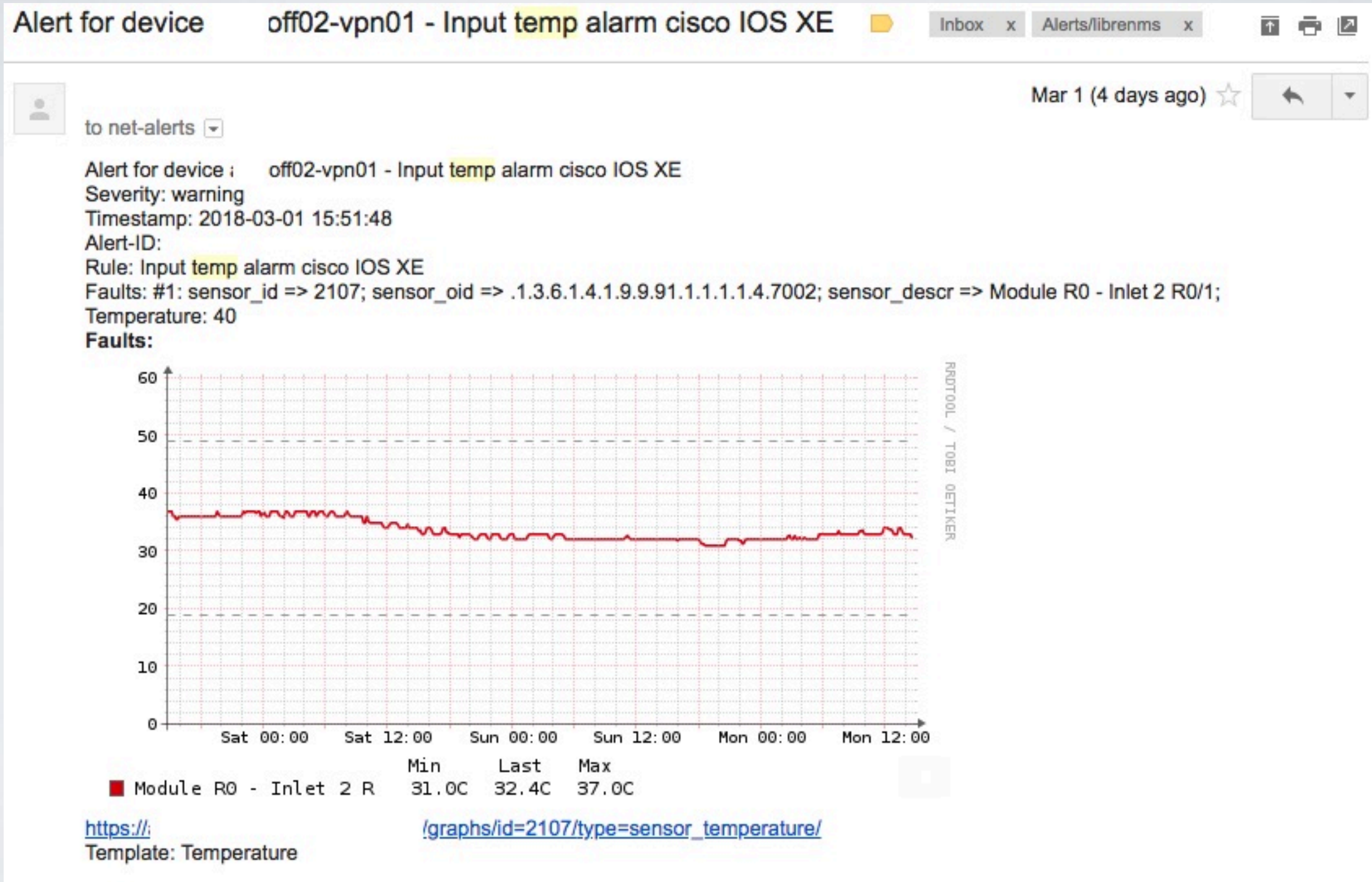
Rule: Testing localhost

Faults:

#1: sysObjectID => .1.3.6.1.4.1.8072.3.2.10; sysDescr => Linux
web01.1.novalocal 3.10.0-514.26.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC
2017 x86_64;

Alert sent to: <n@laf.io>

Templates



Templates

Alert for device off03-core02 - Processor Single Core usage over 90%



Inbox

x

Alerts/librenms

x



librenms@

to net-alerts

Mar 3 (2 days ago)



Alert for device , off03-core02 - Processor Single Core usage over 90%

Severity: warning

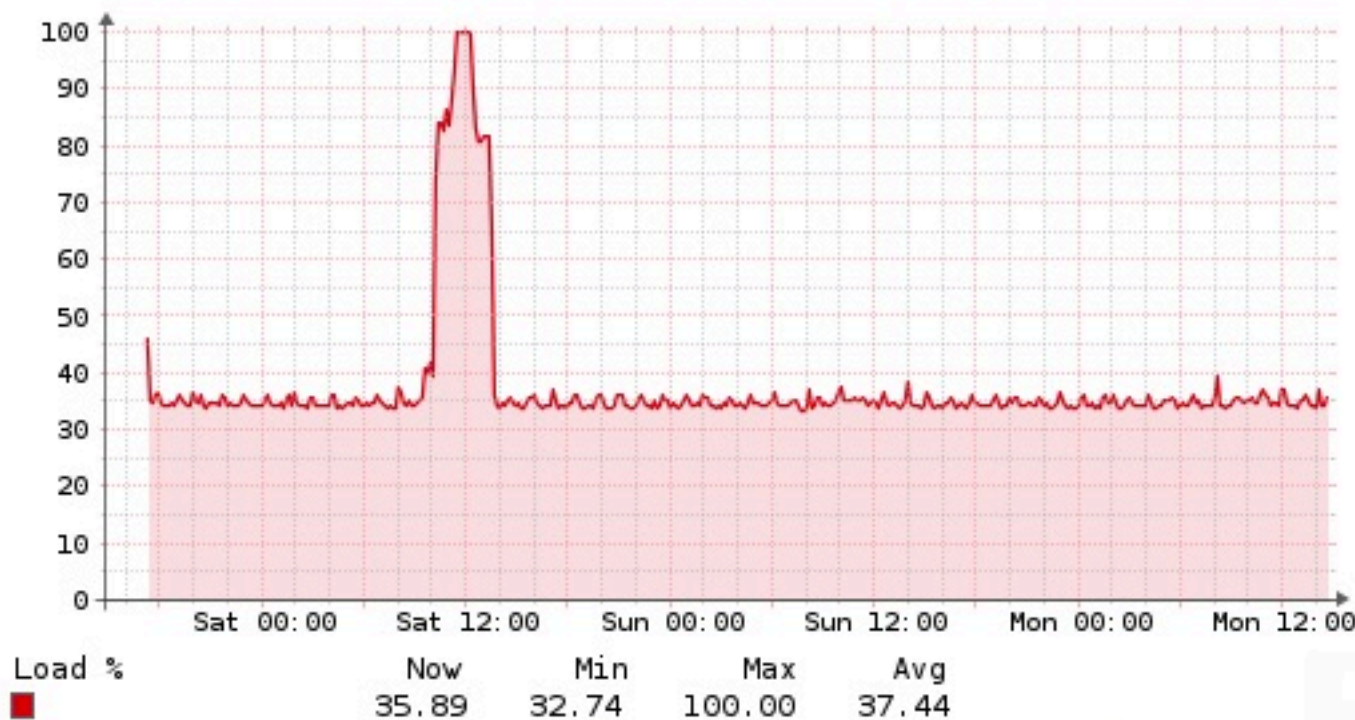
Timestamp: 2018-03-03 11:17:18

Alert-ID:

Rule: Processor Single Core usage over 90%

Faults: #1: sysObjectID => enterprises.1588.3.3.1.131; sysDescr => off03-core, BR-VDX6740, Network Operating System Software Version 7.0.1b.; override_sysLocation => 1; processor_id => 170; processor_oid => 1.3.6.1.4.1.1588.2.1.1.1.26.1; processor_descr => CPU;

Faults:



<https://>

Template: CPU alert

/graphs/id=143/type=device_processor/

Templates



LibreNMS APP 9:58 AM

Alert for device

Alert for device

Severity: critical

Timestamp: 2018-02-27 09:52:53


Unique-ID: 64727

Rule: BGP Session established [Show more...](#)

- BGP Session established

- BGP Session established

Device Dependency

rtr01 rtr01	None	 
sw01 sw01	rtr01	 
sw02 sw02	rtr01	 

Device Dependency for Multiple Devices

Bulk Add

Clear All

Here you can modify multiple device dependencies. Setting the parent device to "None" will clear the dependency.

Parent Host:

× rtr01 (undefined)

Child Hosts:

× sw01 (undefined)

× sw02 (undefined)

Cancel

Save

Alerting system 2018

- Introduce new templating system
- Per rule transports
- Multiple recipients per rule
- Improved UI for group mapping

Authentication

Authentication

- Active Directory
- HTTP
- LDAP
- Radius
- SSO
- 2FA

Logging

Syslog and Graylog2



<div>All Devices ▾ All Programs ▾ All Priorities ▾</div> <div>From To Filter</div>					
<div><div>Q Search</div><div><div>↺</div>50 ▾<div>≡ ▾</div></div></div>					
	Datetime	▼ Hostname	Program	Message	Message
🔊	2017-09-05 19:07:13	demo	RRDCACHED	removing old journal /var/lib/rrdcached/journal/rrd.journal.1504631233.762573	3
🔊	2017-09-05 19:07:13	demo	RRDCACHED	started new journal /var/lib/rrdcached/journal/rrd.journal.1504638433.762537	3
🔊	2017-09-05 19:07:13	demo	RRDCACHED	rotating journals	3
🔊	2017-09-05 19:07:13	demo	RRDCACHED	flushing old values	3
ℹ	2017-09-05 19:07:01	demo	CRON	pam_unix(cron:session): session closed for user root	0
ℹ	2017-09-05 19:07:01	demo	/USR/SBIN/CRON	(root) CMD (/opt/librenms/alerts.php >> /dev/null 2>&1)	0
ℹ	2017-09-05 19:07:01	demo	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	0
ℹ	2017-09-05 19:06:27	demo	CRON	pam_unix(cron:session): session closed for user root	0
ℹ	2017-09-05 19:06:01	demo	CRON	pam_unix(cron:session): session closed for user root	0
ℹ	2017-09-05 19:06:01	demo	/USR/SBIN/CRON	(root) CMD (/opt/librenms/alerts.php >> /dev/null 2>&1)	0
ℹ	2017-09-05 19:06:01	demo	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	0
ℹ	2017-09-05 19:05:52	demo	POSTFIX/SMTPD	disconnect from unknown[31.149.66.65]	0
ℹ	2017-09-05 19:05:52	demo	POSTFIX/SMTPD	connect from unknown[31.149.66.65]	0
⚠	2017-09-05 19:05:52	demo	POSTFIX/SMTPD	warning: hostname static.kpn.net does not resolve to address 31.149.66.65: Name or service not known	1
ℹ	2017-09-05 19:05:32	demo	SSHD	PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=113.195.145.21 user=root	0

Device configs

Rancid and Oxidized

Oxidized

Node List [Config Search](#)

Hostname	Last Status	Last Update	Model	Group
rtr01		2017-09-05 19:12:35 UTC	Edgeos	default
sw01		2017-09-05 19:12:40 UTC	IOS	default

Sync status: **success**

Node: rtr01

IP: 192.168.80.1

Model: Edgeos

Last Sync: 2017-09-05 19:12:35 UTC

Config
version

*2 :: 2017-09-05 20:12:35 +0100 ↕

Show version

Show diff

Hide line numbers

```
1. firewall {
2.     all-ping enable
3.     broadcast-ping disable
4.     group {
```

API

API

- Extensive restful API - Currently v0
- Supports Devices, Ports, Routing, Switching
- Alerting, Inventory, Bills and Logs
- Powers the myLibreNMS mobile apps

Scaling

Distributed Polling

- Allows you to scale out your install
- Supports $n+1$ for resilience
- Supports polling within NAT environments

Poller Name	Devices Polled	Total Poll Time
poller-1	1888	124 Seconds
poller-2	1969	125 Seconds
poller-3	365	125 Seconds
poller-4	281	125 Seconds

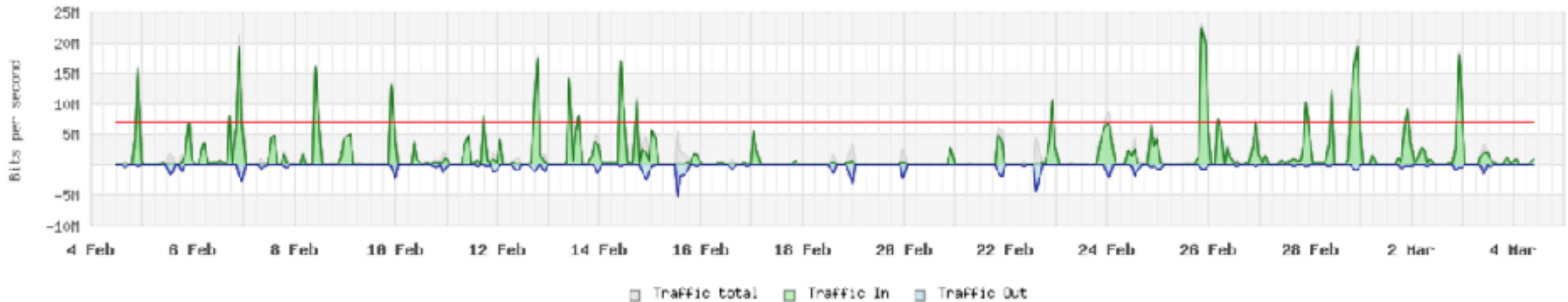
Traffic billing

Traffic Billing

- CDR or Quota based
- Customer and billing references
- Data available via API
- Granular graphs available

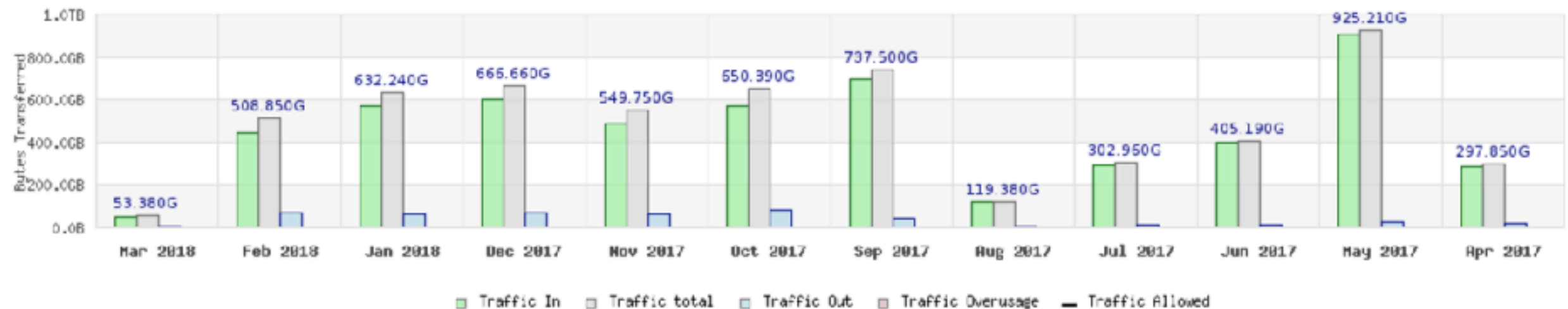
Traffic Billing

Monthly View



Historical Usage

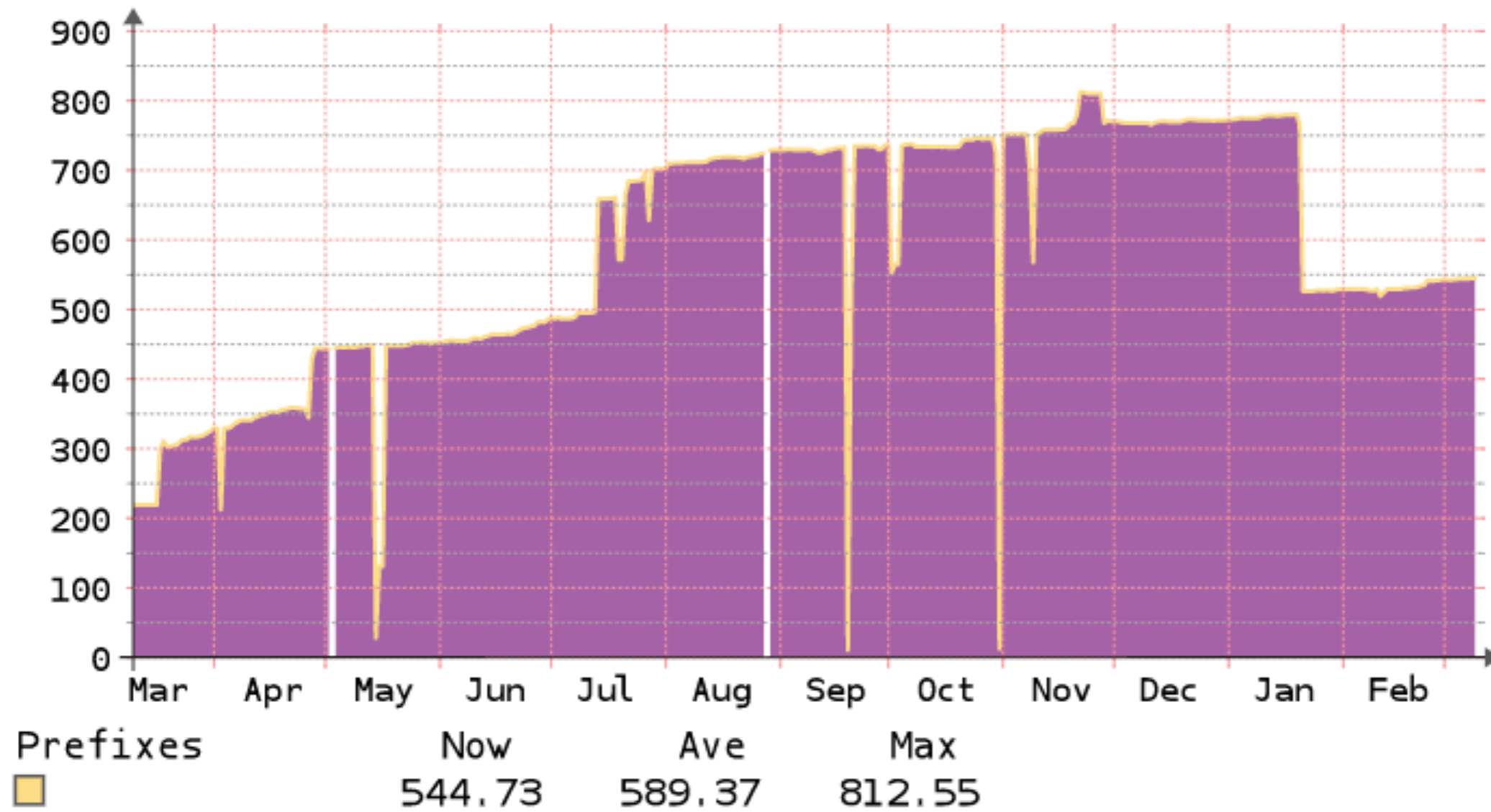
Monthly Usage



Routing Support

BGP

RRDTOOL / TOBI OETIKER

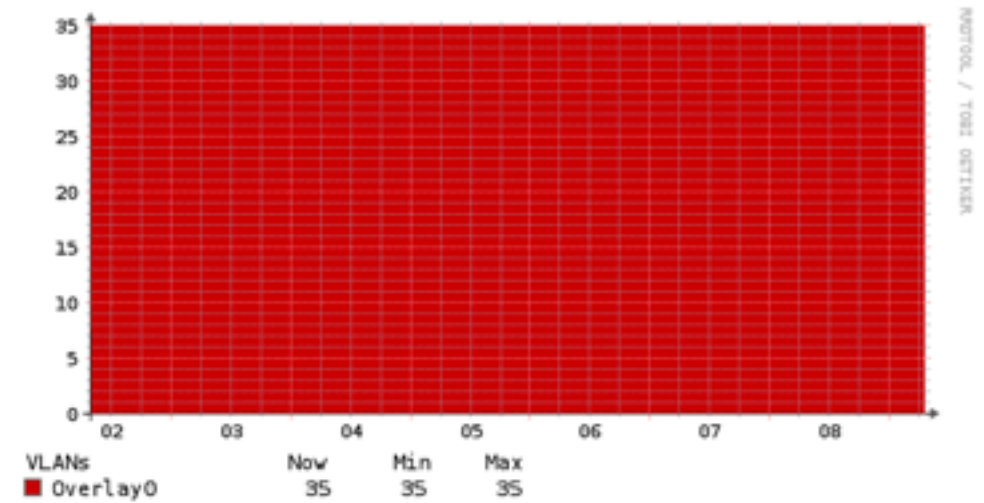
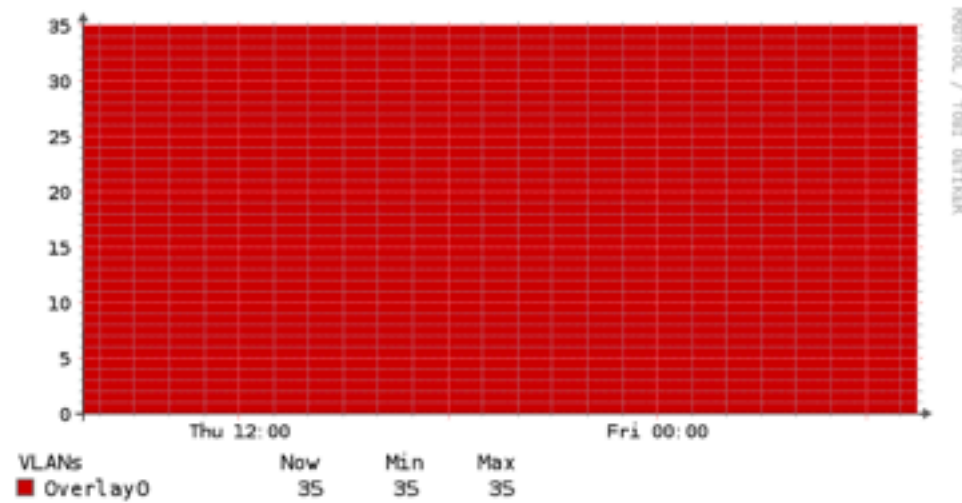


OSPF

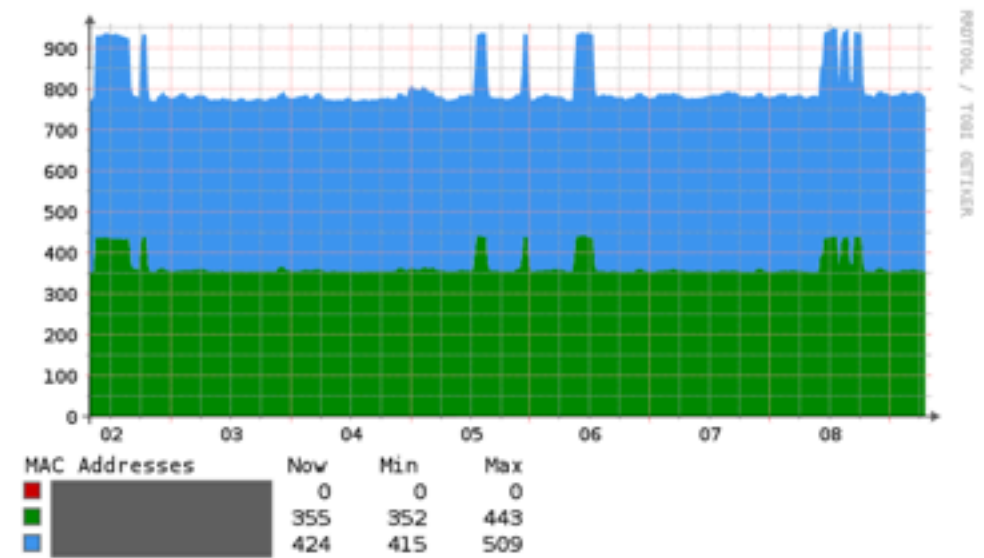
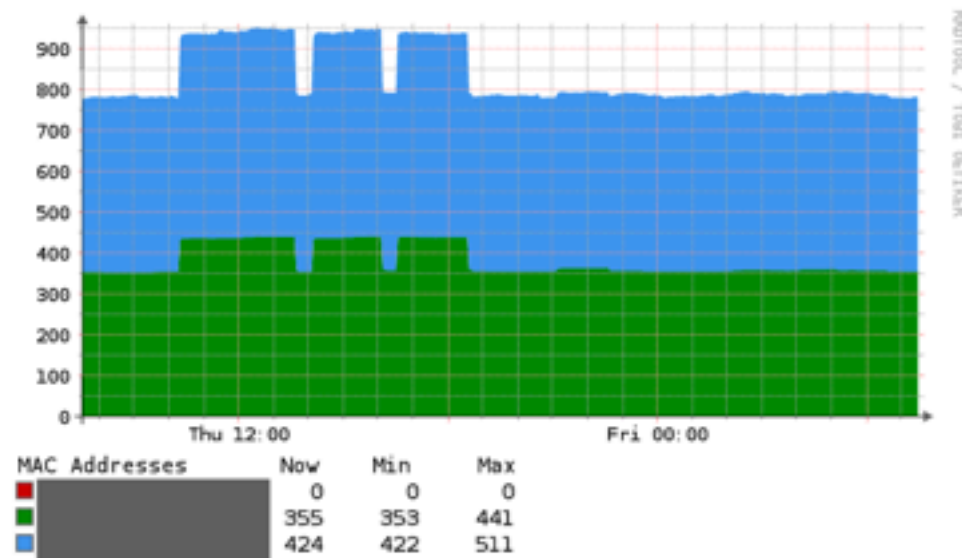
Device	Router ID	Status	ABR	ASBR	Areas	Ports(Enabled)	Neighbours
		enabled	false	false	1	2(2)	1
		enabled	false	false	1	2(2)	1
		enabled	false	false	1	3(3)	2
		enabled	false	true	0	3(0)	0
		enabled	false	false	1	2(2)	1
		enabled	false	false	1	3(3)	2
		enabled	false	false	1	3(3)	2

OTV

AED Enabled VLAN's



MAC Addresses













CEF

Device	Entity	AFI	Path	Drop	Punt	Punt2Host
	cpu R0/0 (ASR1000-RP1)	ipv4	RP RIB	0	0	0
	cpu R0/0 (ASR1000-RP1)	ipv4	RP LES	0	3299	0
	cpu R0/0 (ASR1000-RP1)	ipv6	RP LES	0	0	0
	cpu R0/0 (ASR1000-RP1)	ipv4	RP RIB	0	0	0
	cpu R0/0 (ASR1000-RP1)	ipv4	RP LES	0	34	0
	cpu R0/0 (ASR1000-RP1)	ipv6	RP LES	0	0	0
	NPE-G1 0 (NPE-G1)	ipv4	RP RIB	0	0	0
	NPE-G1 0 (NPE-G1)	ipv4	RP LES	2	252578061	0
	NPE-G1 0 (NPE-G1)	ipv4	RP PAS	128276417	252578118	12037555
	NPE-G1 0 (NPE-G1)	ipv6	RP LES	41951	54541291	82
	1 (WS-C3750X-48T-S)	ipv4	RP RIB	0	0	0
	1 (WS-C3750X-48T-S)	ipv4	RP LES	0	0	0
	1 (WS-C3750X-48T-S)	ipv6	RP LES	0	0	0
	NPE-G1 0 (NPE-G1)	ipv4	RP RIB	0	0	0
	NPE-G1 0 (NPE-G1)	ipv4	RP LES	0	22839045	0

PeeringDB Support

PeeringDB

ASN	IP	Peer	Connected	
13237	195.66.224.99	LAMBDANET-AS European Backbone of AS13237, DE	✗	
13238	195.66.226.69	YANDEX, RU	✗	
13285	195.66.224.136	OPALTELECOM-AS TalkTalk Communications Limited, GB	✓	
13285	195.66.225.17	OPALTELECOM-AS TalkTalk Communications Limited, GB	✓	
132876	195.66.226.241	SYMPHONY-AP-TH Symphony Communication (Thailand) PCL., TH	✗	
13335	195.66.225.179	CLOUDFLARENET - Cloudflare, Inc., US	✓	
13414	195.66.225.142	TWITTER - Twitter Inc., US	✗	
13414	195.66.226.61	TWITTER - Twitter Inc., US	✗	
13445	195.66.225.110	13445 - Cisco Webex LLC, US	✗	
136620	195.66.227.100	VMHAUSLIMITED-AS-AP VMHaus Limited, GB	✗	

Updates

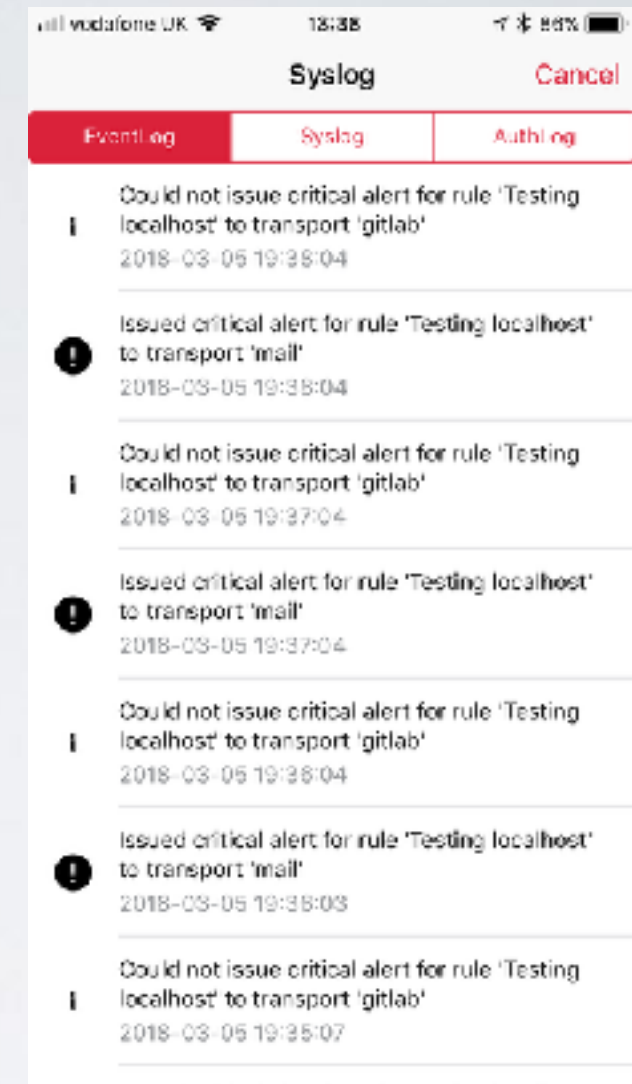
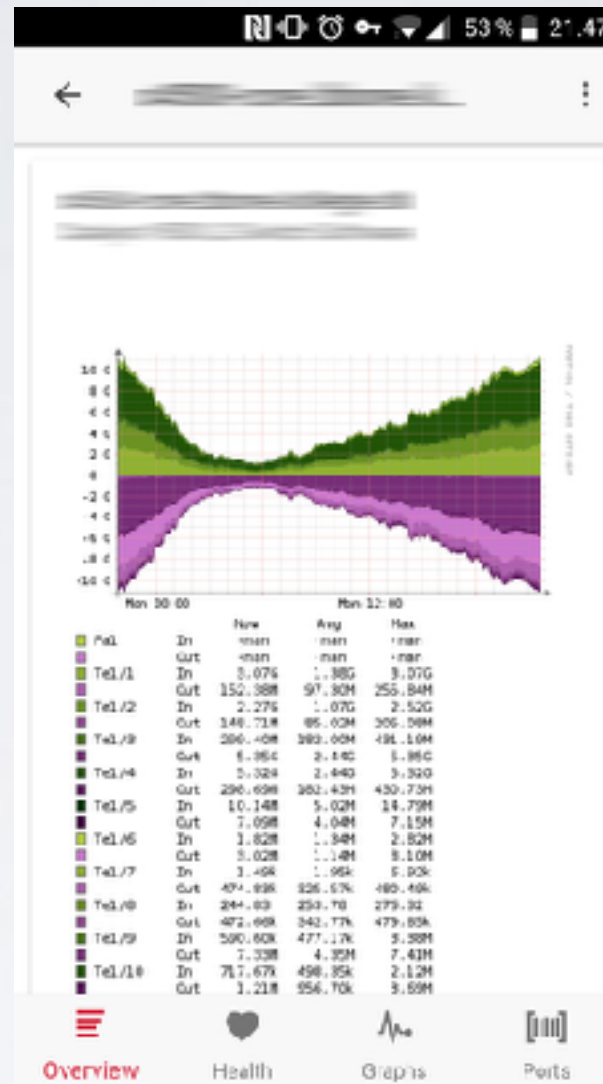
Automatic updates

Two available update channels:

- Development (master branch)
- Stable (GitHub releases)

Mobile Apps

Mobile Apps



Made available courtesy of Paul @ WaveDirect
Now released as Open Source

Support

How you think Open Source apps are maintained



How Open Source apps are really maintained



Asking for help

- Discord – Primary method
- Community site
- Reddit
- GitHub for bugs

Getting involved

- Code contributions / pull requests
- Documentation
- Help others
- Find / report bugs and ask for device support

Contact



<https://github.com/librenms/librenms>



<https://community.librenms.org>



<https://www.twitter.com/librenms>



<https://www.facebook.com/LibreNMS/>



<https://www.reddit.com/r/LibreNMS/>



team@librenms.org



<https://t.libren.ms/discord>