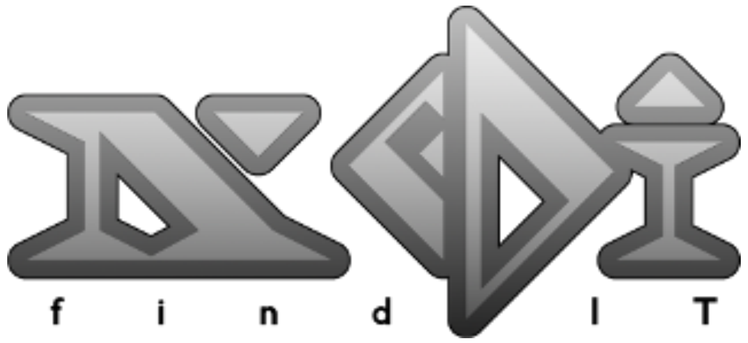


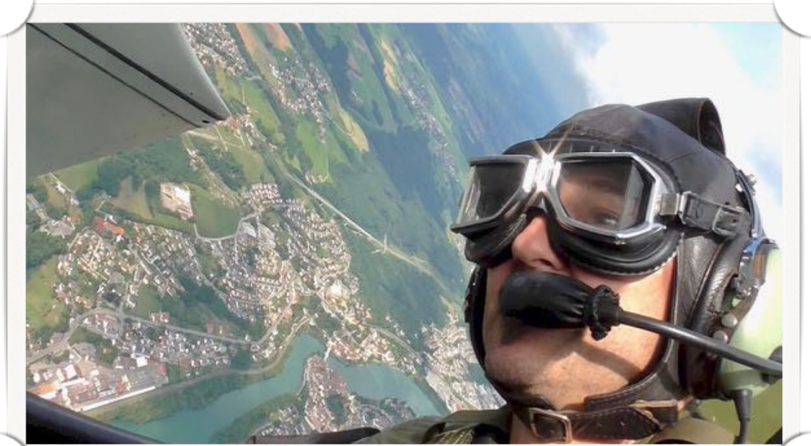
Why it's still here

www.nedi.ch

I LIKE FLYING AND…

2008

2017



2018

2019

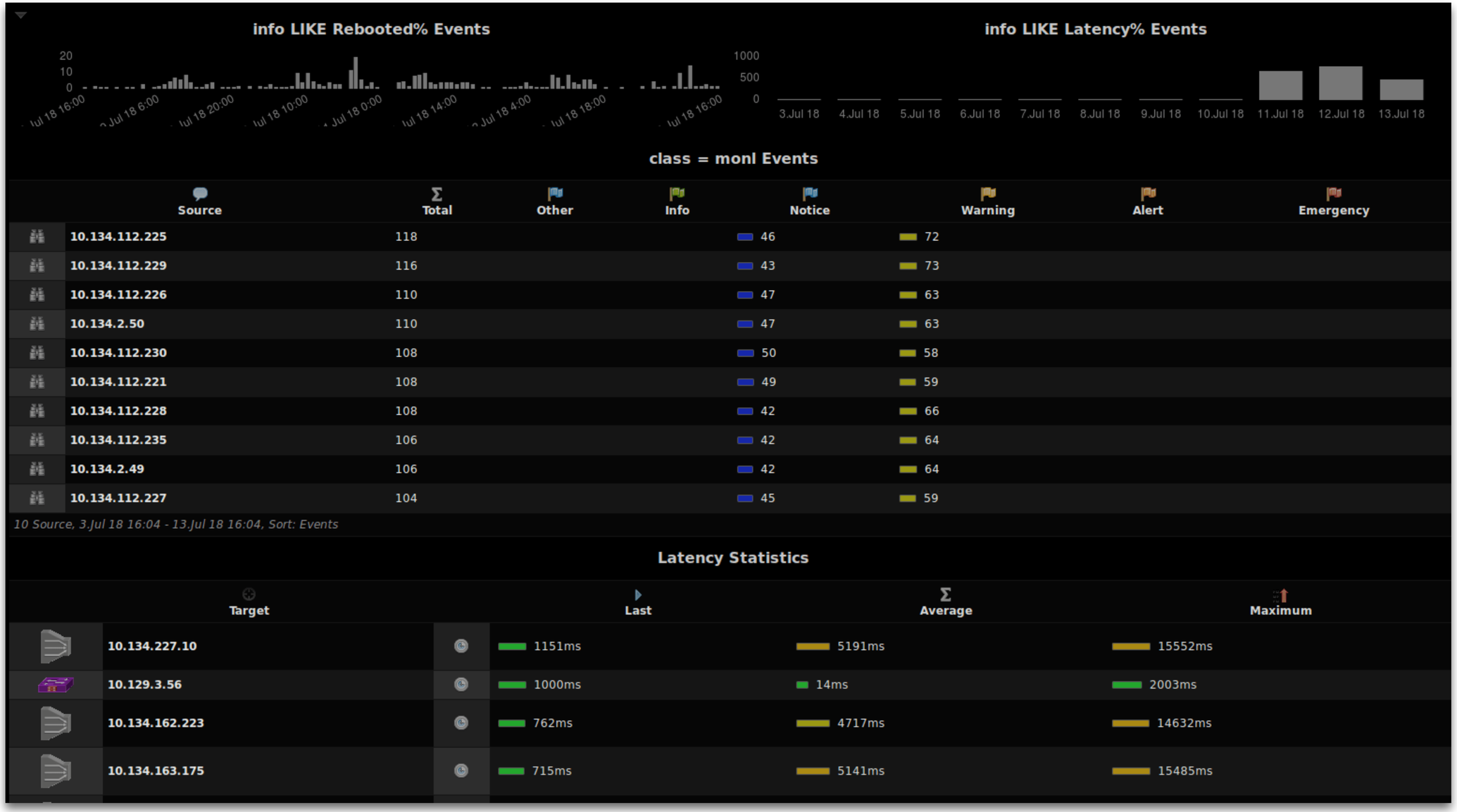
MACRO FOTOGRAFY

HOW IT ALL STARTED

Back in 2001…

…available solutions were like:

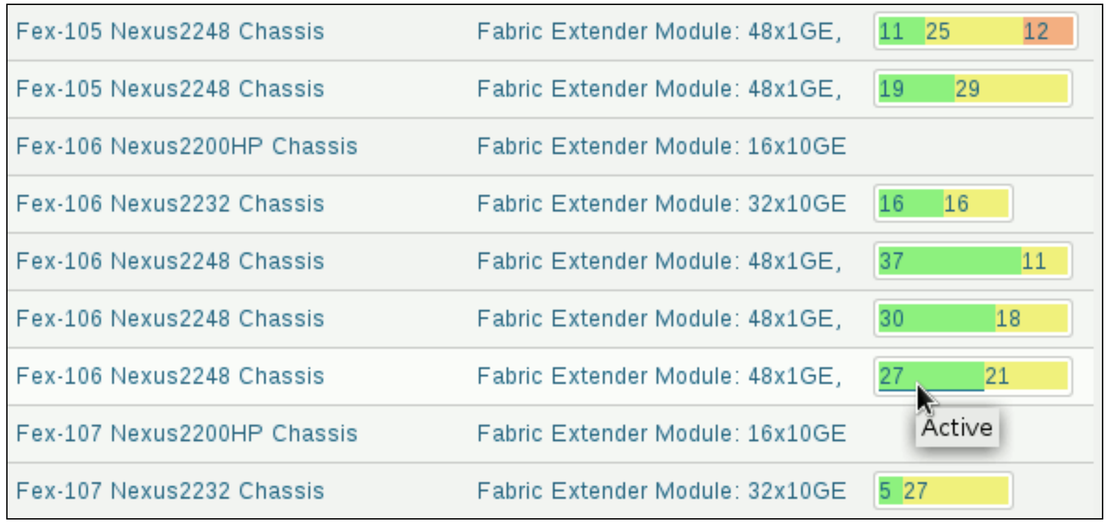
WHAT IT DOES


info LIKE Rebooted% Events
20
10
0
Jul 18 16:00
Jul 18 6:00
Jul 18 20:00
Jul 18 10:00
Jul 18 0:00
Jul 18 14:00
Jul 18 4:00
Jul 18 18:00
Jul 18 16:00
info LIKE Latency% Events
1000
500
0
3.Jul 18
4.Jul 18
5.Jul 18
6.Jul 18
7.Jul 18
8.Jul 18
9.Jul 18
10.Jul 18
11.Jul 18
12.Jul 18
13.Jul 18
class = monl Events
Source
Total
Other
Info
Notice
Warning
Alert
Emergency
10.134.112.225 118 46 72
10.134.112.229 116 43 73
10.134.112.226 110 47 63
10.134.2.50 110 47 63
10.134.112.230 108 50 58
10.134.112.221 108 49 59
10.134.112.228 108 42 66
10.134.112.235 106 42 64
10.134.2.49 106 42 64
10.134.112.227 104 45 59
10 Source, 3.Jul 18 16:04 - 13.Jul 18 16:04, Sort: Events
Latency Statistics
Target
Last
Average
Maximum
10.134.227.10 1151ms 5191ms 15552ms
10.129.3.56 1000ms 14ms 2003ms
10.134.162.223 762ms 4717ms 14632ms
10.134.163.175 715ms 5141ms 15485ms

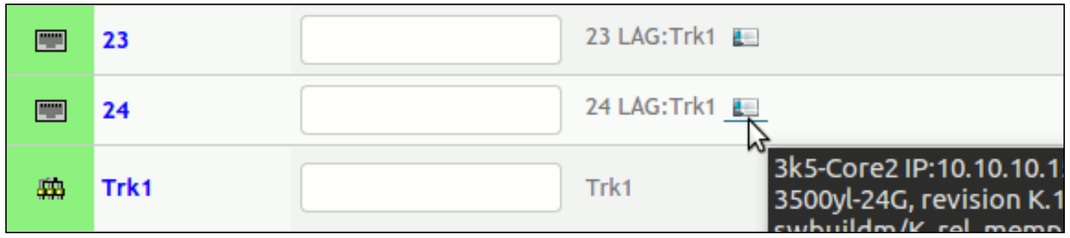
DISCOVERING THE NETWORK

Module Status

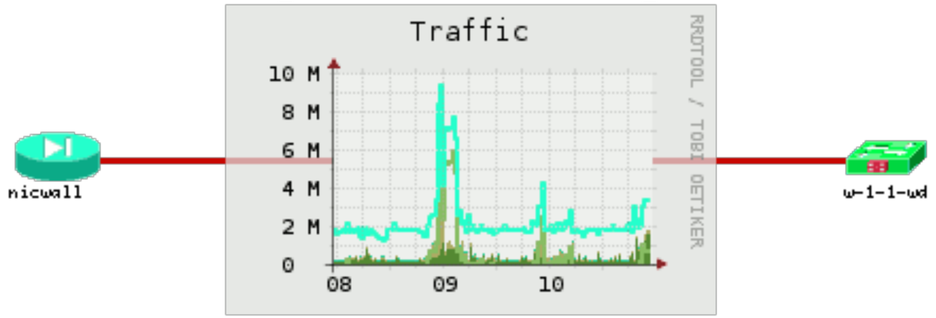
Port Status per Fabric Extender



LAG Ports



Dynamic Maps

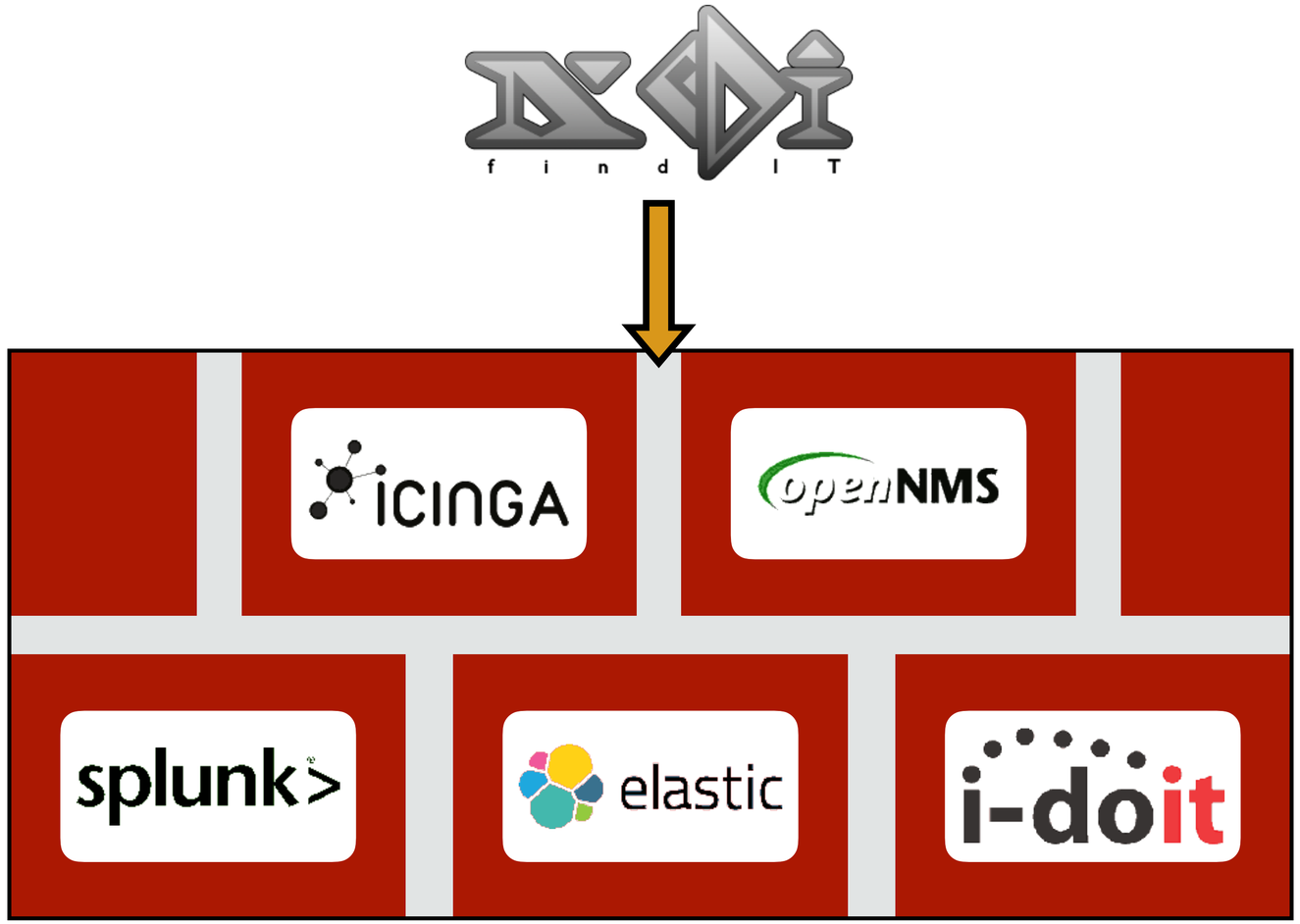


NEDI IS GREEN TECHNOLOGY

```
-rw-r--r-- 1 rickli rickli 4.0M Jul  6 14:16 nedi-1.9.187.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul  9 09:15 nedi-1.9.190.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul 12 12:44 nedi-1.9.193.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul 17 16:10 nedi-1.9.198.pkg
```

- Tarball 4MB in Size
- Not resource hungry
- Developed on solar powered keyboard
- Using clean waterpower

NEDI & THE BIG GUYS



SECURITY

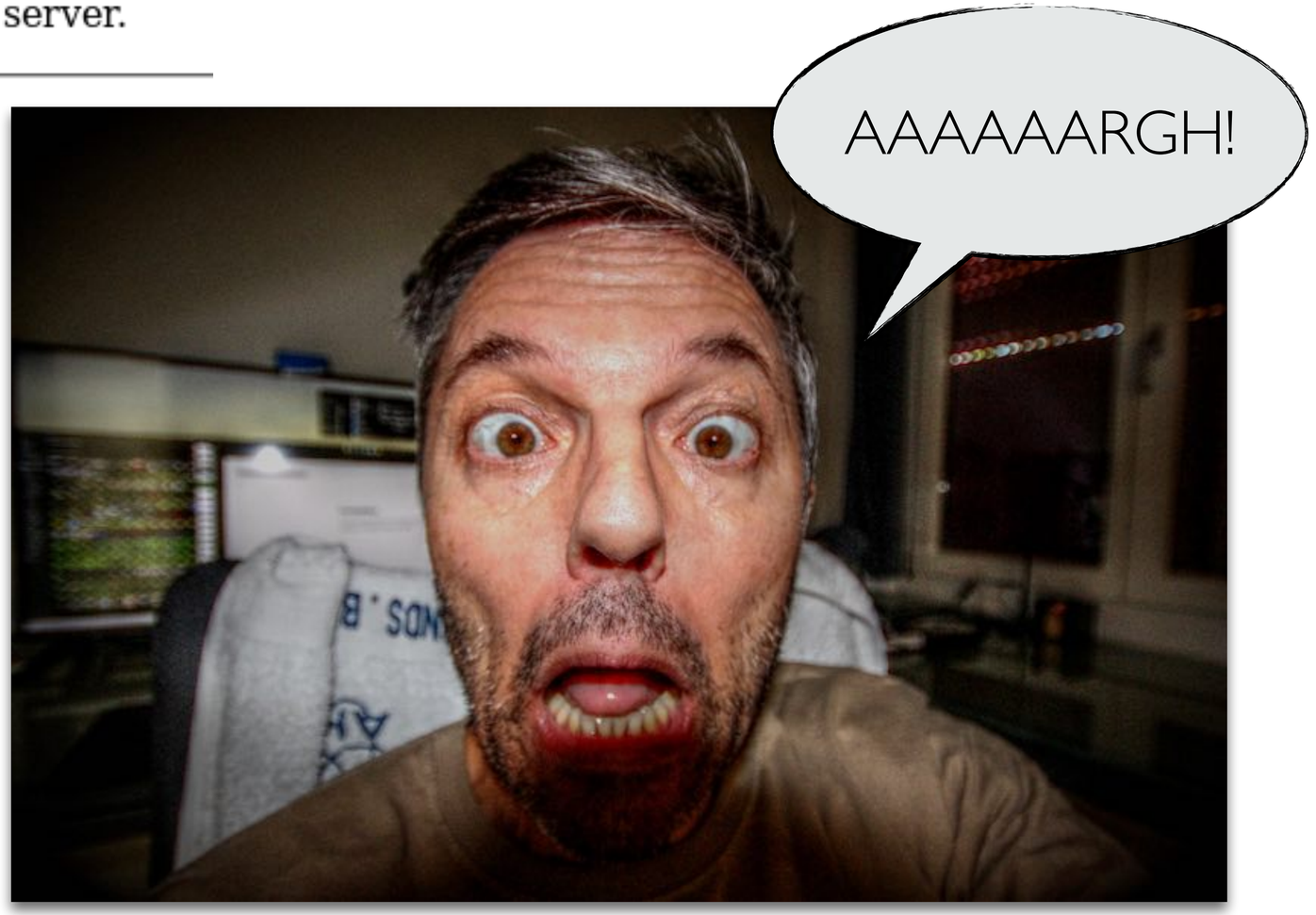
THE NEDI COMMUNITY

AAAAAAAAAAAAAARGH!

Forbidden

You don't have permission to access /gfds on this server.

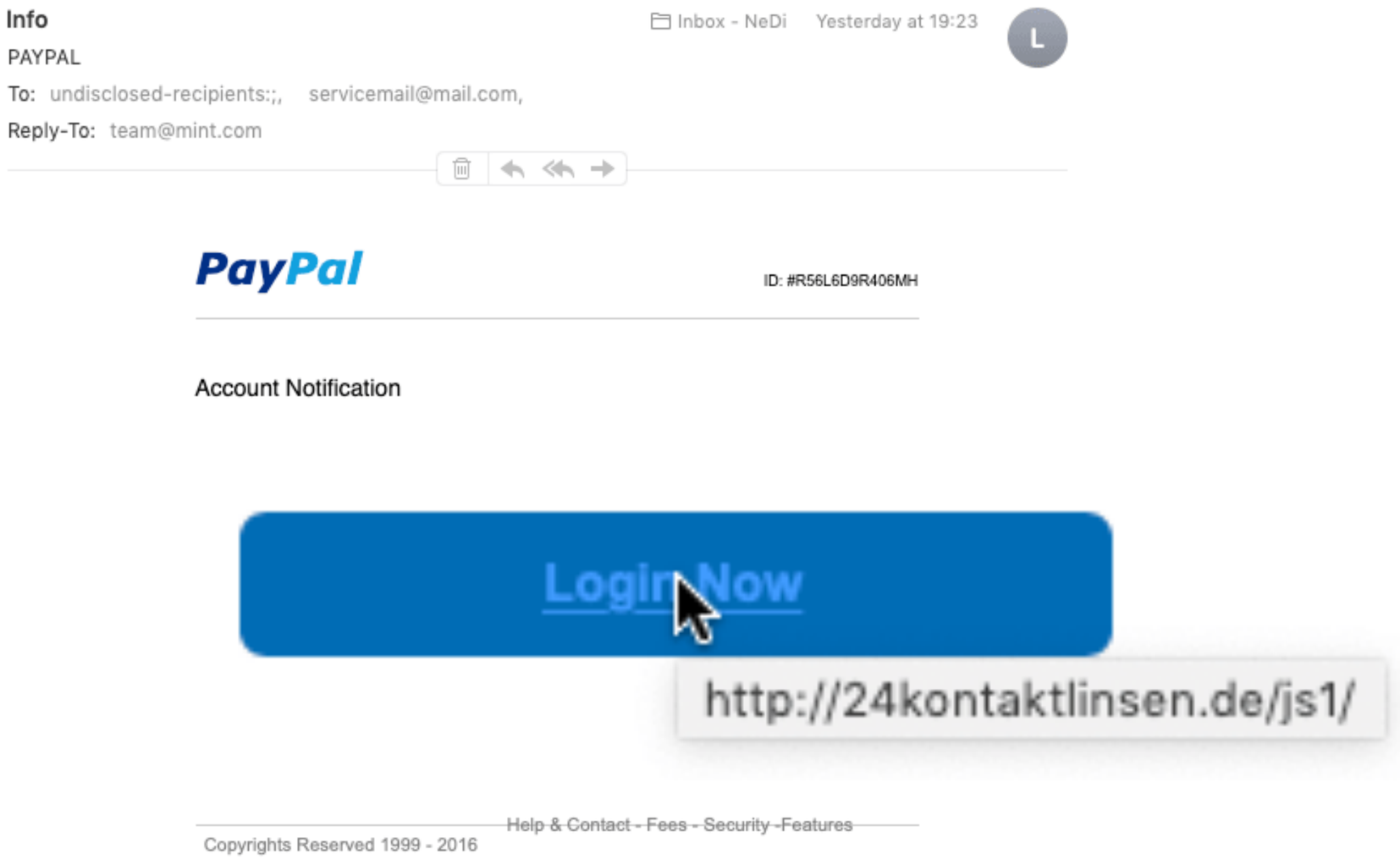
Apache/2.2.20 (Ubuntu) Server at q Port 80



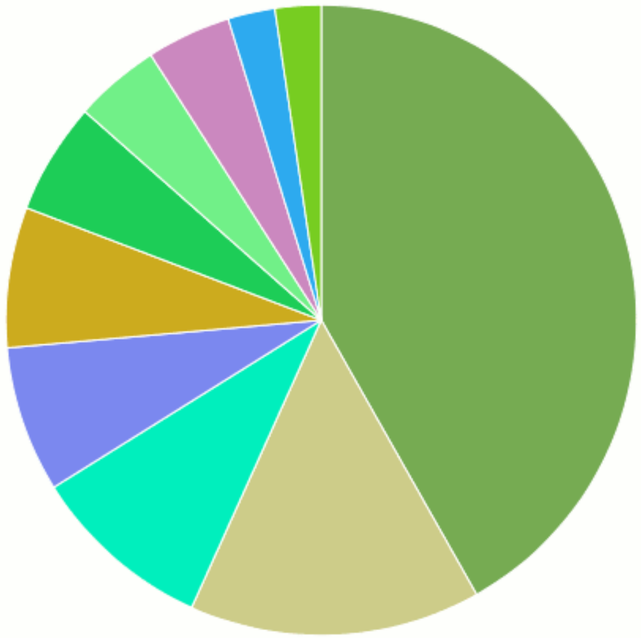
LOOKING AT WEBSTATS

Top 30 von 2002 URLs					
#	Anfragen		kb		URL
1	204629	40.85%	1210665	23.81%	/
2	14169	2.83%	71554	1.41%	/tajogw.php
3	10250	2.05%	86070	1.69%	/feed/
4	7183	1.43%	36463	0.72%	/robots.txt
5	6989	1.40%	6535	0.13%	/favicon.ico
6	6294	1.26%	49095	0.97%	/Themes/default/scripts/script.js
7	6292	1.26%	5002	0.10%	/Themes/default/scripts/theme.js
8	6058	1.21%	55195	1.09%	/hpn/
9	6051	1.21%	47705	0.94%	/Themes/default/css/

PHISHING MAILS



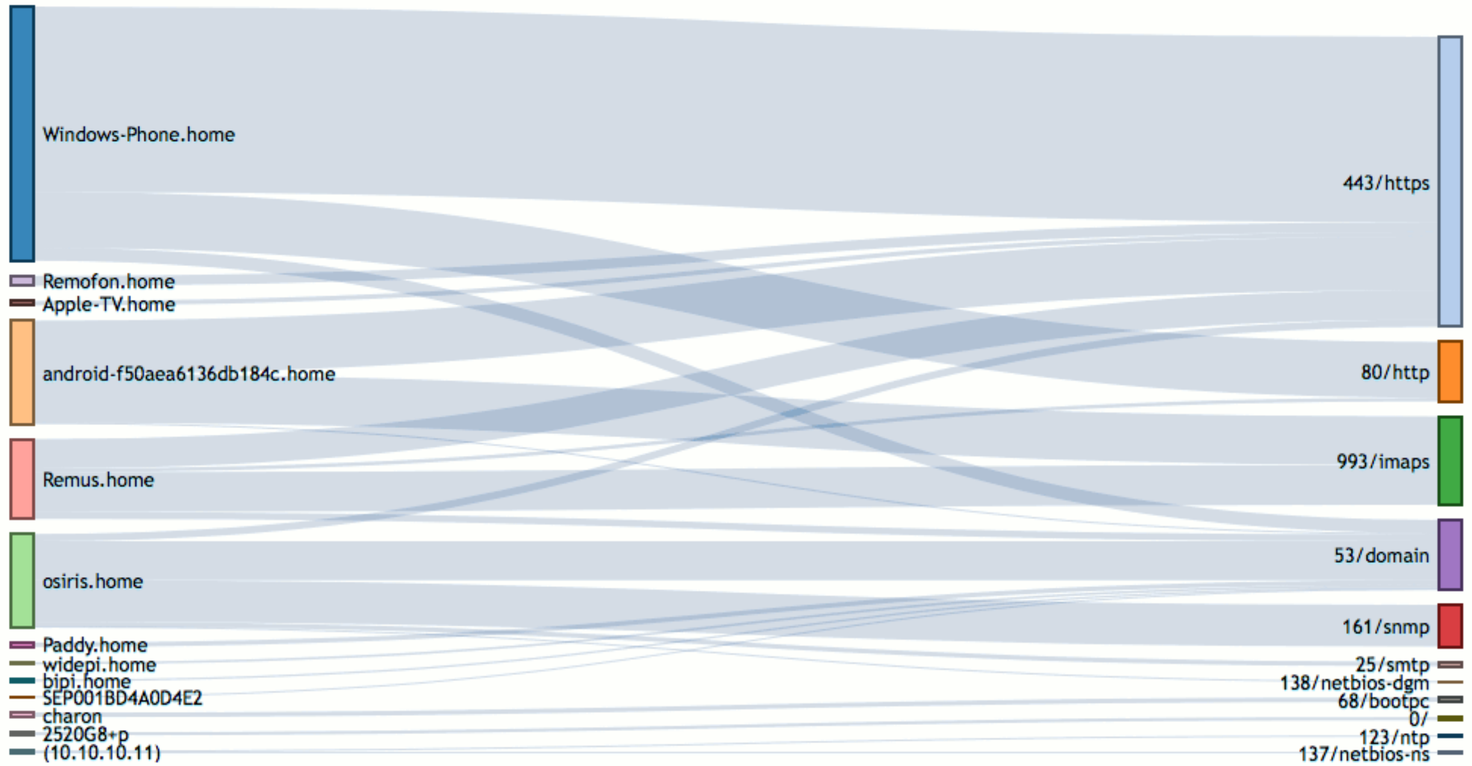
TRAFFIC ANALYSIS



Summary

12.Aug 16 11:05 - 12.Aug 16 11:10, Filter: dst port < 1024

Destination Address	Destination Port	Packets	Bytes
Google Inc.	443/https	10k	595k
Google Inc.	443/https	3k	213k
Google Inc.	443/https	2k	133k



Source Address, Destination Port Summary

26.Jul 16 16:35 - 26.Jul 16 16:45, Filter: dst port < 1024

TRAFFIC INFO

1	Amazon Technologies Inc.		443 https	Remus.home
2	Google Inc.		443 https	android-44005e8124817138.home
3	charon		63150	osiris

	216.58.207.46/24
Network	1e100.net
Customer	Google Inc.
Mail	google.com
Phone	+1-650-253-0000
Address	1600 Amphitheatre Parkway, Mountain View, CA
Description	GOOGLE
Origin AS	AS15169
Update	15.Jul 17 8:44

ALERTS

TRAFFIC POLICIES

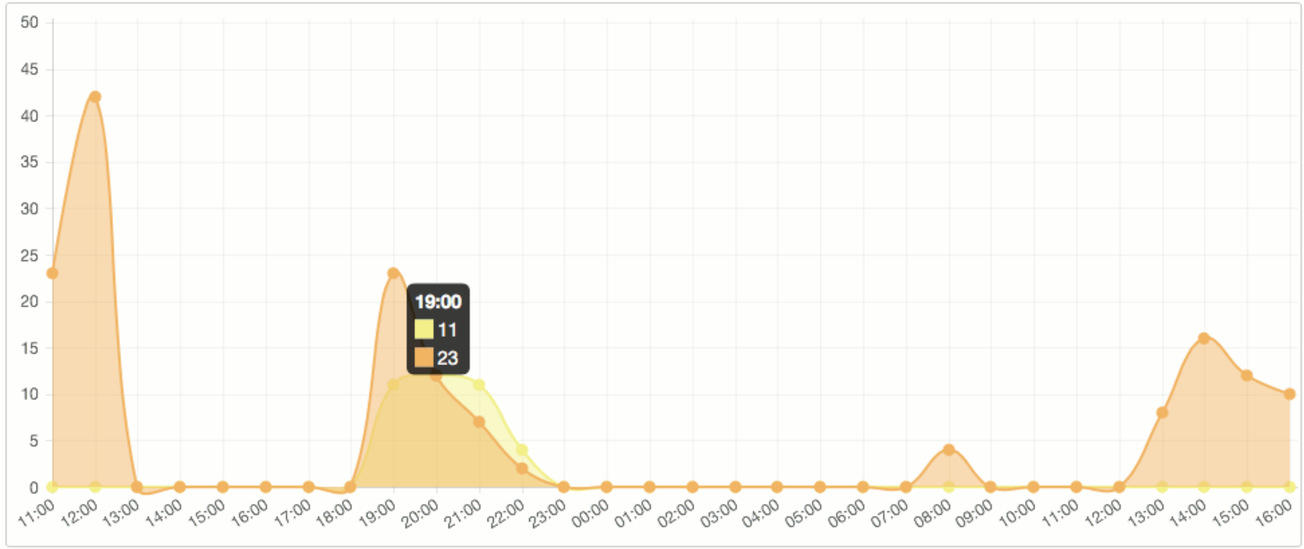
Id	Status	Class	Target	Device	Port	Vlan	Action	Information	User	Time	Execute
19		Bytes	> 500000	Source:charon Filter:src host 10.10.10.109 Group:sa,da					admin	31.Mar 16 12:45	
15		Bytes	< 100	Source:charon Filter:src host 10.10.10.10 and port 5060 Group:sa				SIP underrun	admin	28.Mar 16 16:02	
17		Packets	> 1000	Source:charon Filter:host 10.10.10.109 Group:				Noisy Host	admin	28.Mar 16 17:47	

3 Values

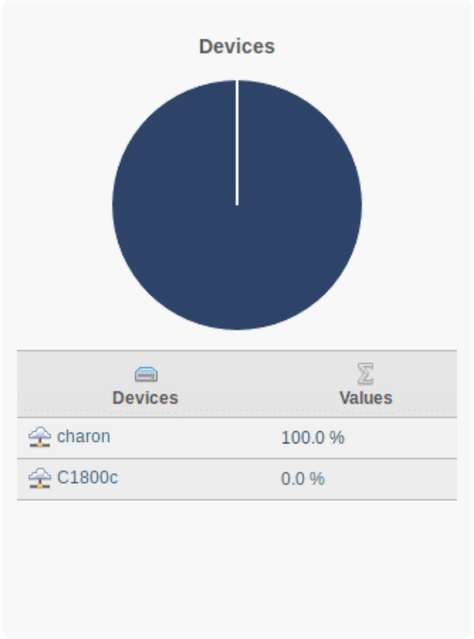
TIMELINE ANALYSIS

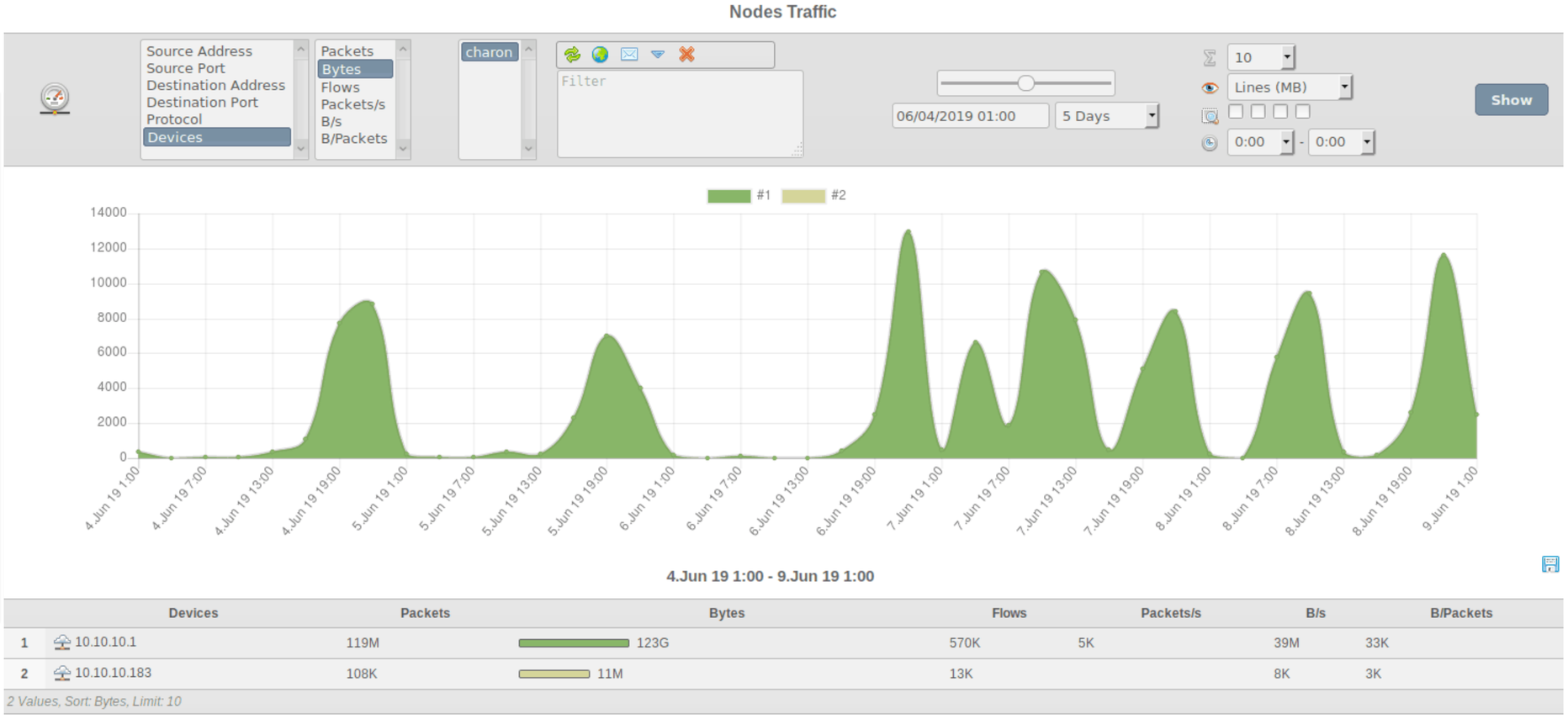
31.Mar 16 11:40 - 1.Apr 16 17:40

Class LIKE 'sp%'



TRAFFIC SOURCES (2.0)

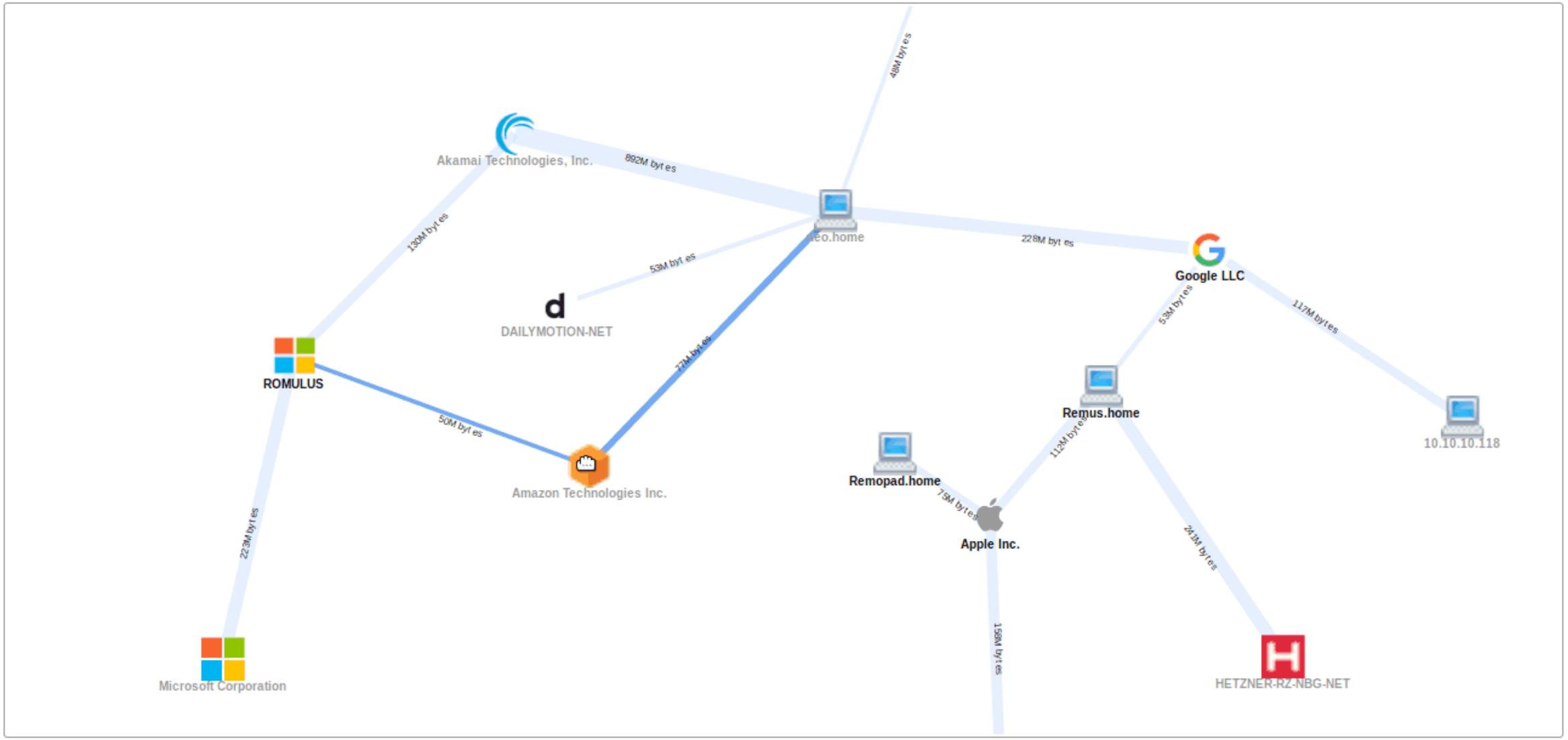




	Devices	Packets	Bytes	Flows	Packets/s	B/s	B/Packets
1	10.10.10.1	119M	123G	570K	5K	39M	33K
2	10.10.10.183	108K	11M	13K		8K	3K

2 Values, Sort: Bytes, Limit: 10

TRAFFIC MAP (2.0)



IMPROVED IP INFORMATION (2.0)

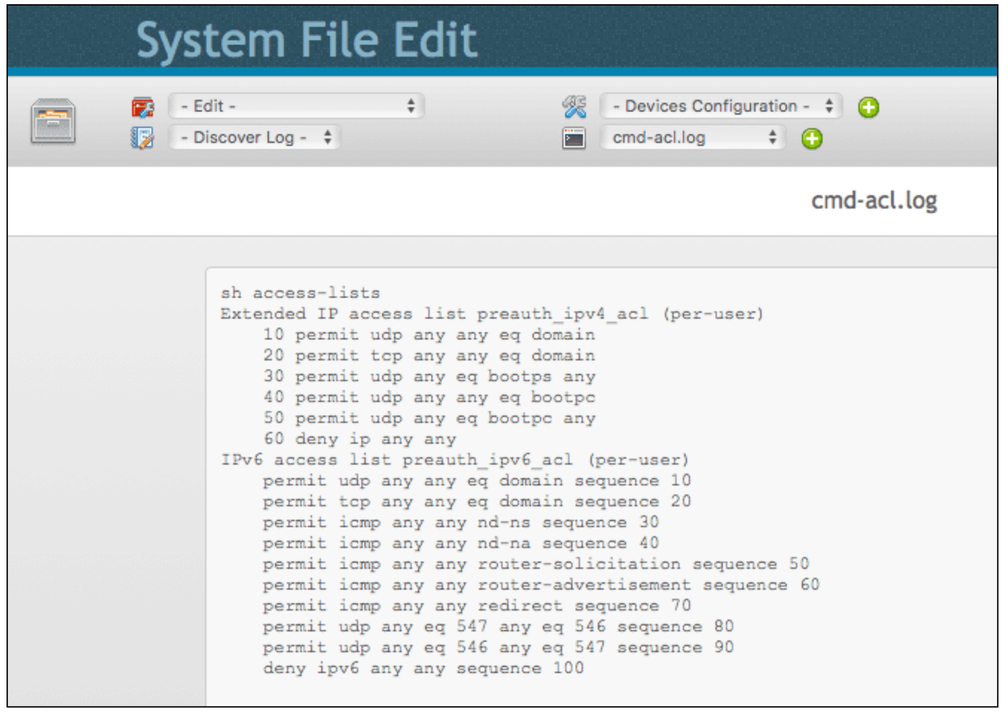
ARP Values

MAC		IP	Update	Services	Operating System	Devices	Port
EDIMAX	74da3825d964	10.10.10.100	10.Apr 19 22:45	SSH-2.0-OpenSSH_6.0p1,nginx/1.2.1,	Debian	charon	igb0
	34ab3731ae83	10.10.10.112	11.Apr 19 9:25			charon	igb0
	b827ebd0b99a	10.10.10.113	11.Apr 19 7:20	SSH-2.0-OpenSSH_7.4p1,	Raspbian	charon	igb0
SAMSUNG	f47b5e0b8b5c	10.10.10.115	11.Apr 19 1:25			charon	igb0
hmd.	ac57755cb432	10.10.10.118	11.Apr 19 8:30		Android 8.0	charon	igb0
	5254006e7f4e	10.10.10.120	11.Apr 19 6:40			charon	igb0
CISCO	000dbd7408ee	10.10.10.124	11.Apr 19 5:40			charon	igb0
CISCO	001bd4a0d4e2	10.10.10.125	11.Apr 19 9:50	SSH-2.0-1.00 ,	Cisco IP Phone	charon	igb0

DHCP-fingerprinting: https://github.com/dumplab/dhcpfingerprint

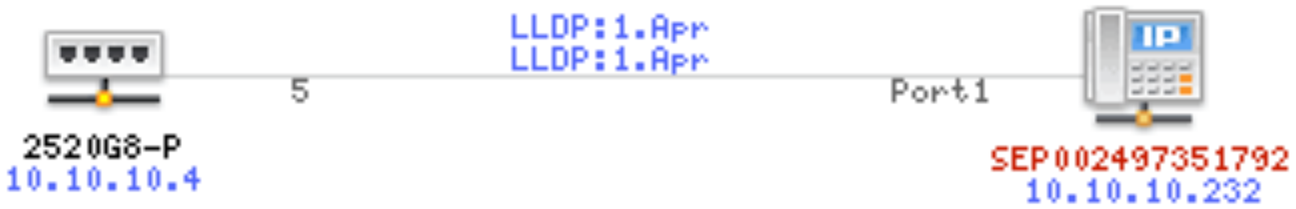
```
nedi.pl -sid -O10.10.10.0/24 Portscan by ARP entries
nedi.pl -sid -a10.10.10.0/24 Portscan by fping
```

ACL MONITORING




```
/var/nedi/nedi.pl -SAFGgadobewitjumpvs -a 10.10.10.7 -c diff-cmd-acl
```

CONFIG CONTEXT POLICIES



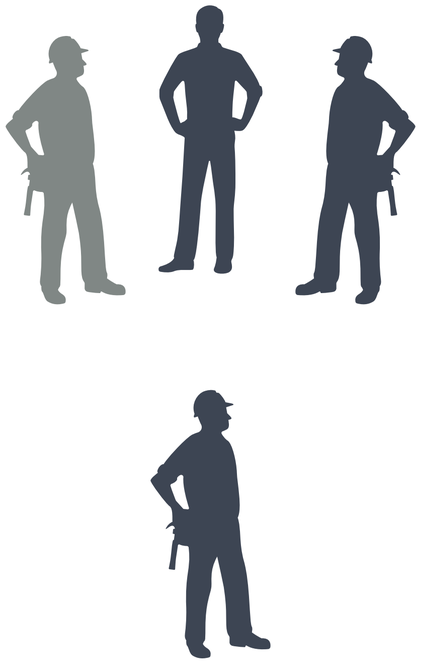
1333122		19.Jun 17 17:26	C2960-8		Policy 7: Portconfig is missing switchport mode trunk on Fa0/7 Tagged voice
1333121		19.Jun 17 17:26	C2960-8		Policy 7: Portconfig is missing switchport mode trunk on Fa0/3 Tagged voice
1333120		19.Jun 17 17:26	C2960-8		Policy 1: Config matches community public
1333119		19.Jun 17 17:26	C2960-8		Policy 3: Config matches contact Remo

Id	Status	Class	Target	Devices	Port	Vlan	Action	Information	User	Time	Execute
1		Configuration	community public						admin	7.Feb 17 15:07	
3		Configuration	contact Remo						admin	7.Feb 17 15:11	
7		Port Configuration	switchport mode trunk	2960				Tagged voice	admin	19.Jun 17 17:26	
3 Values											

NETWORKING

A NETWORKER'S LIFE

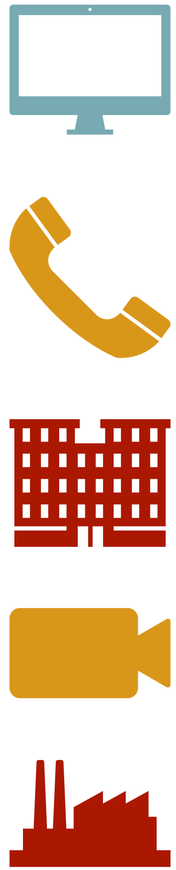
Network Team



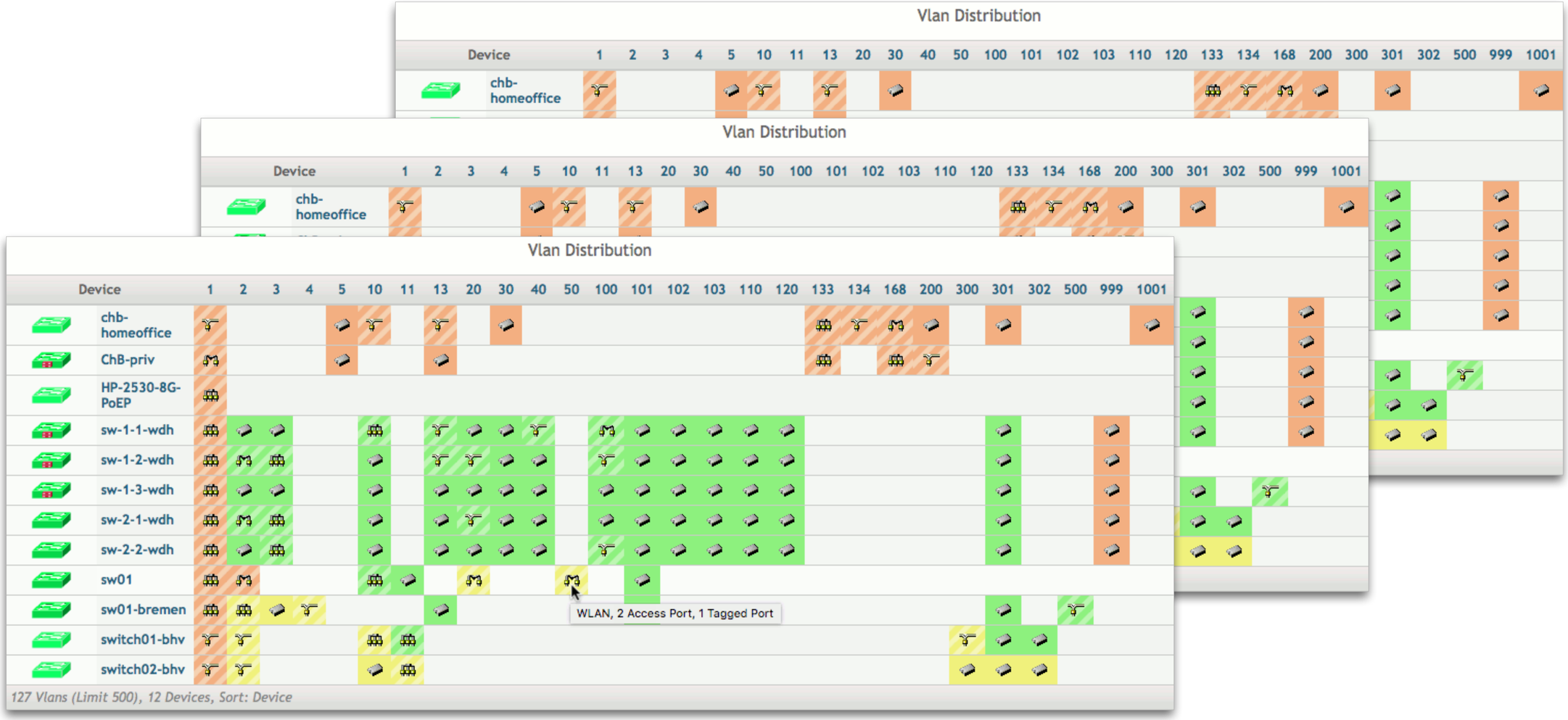
The Network

192.168.0.0
192.168.0.0

The Services



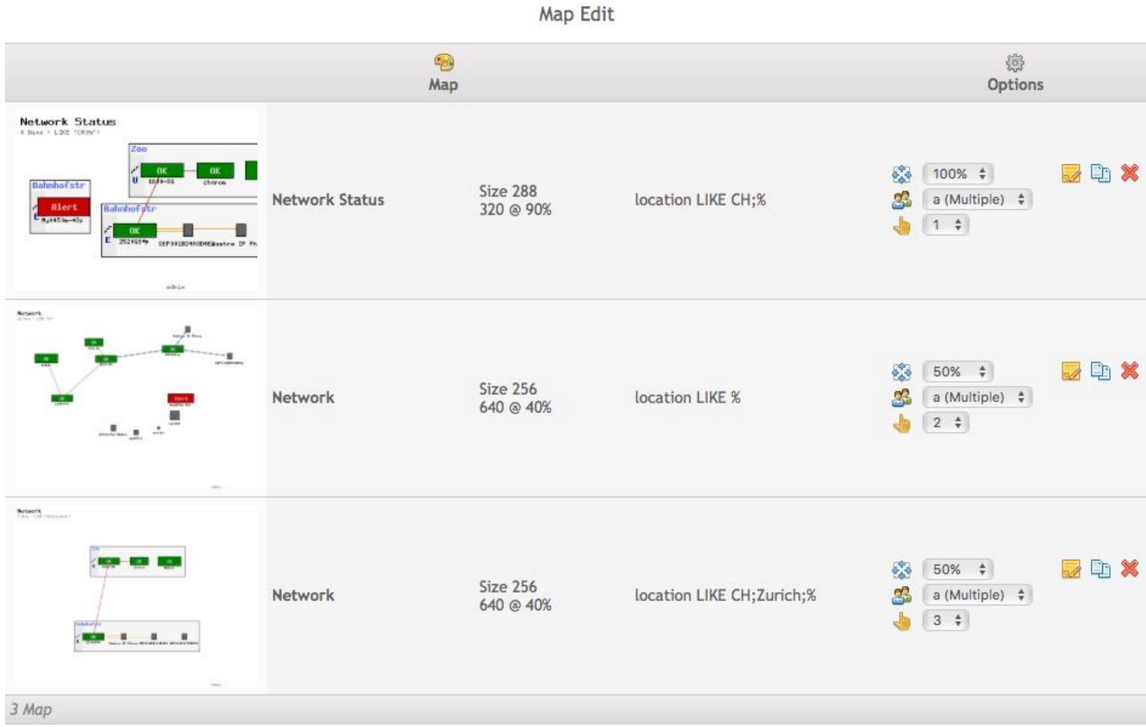
TIME MACHINE



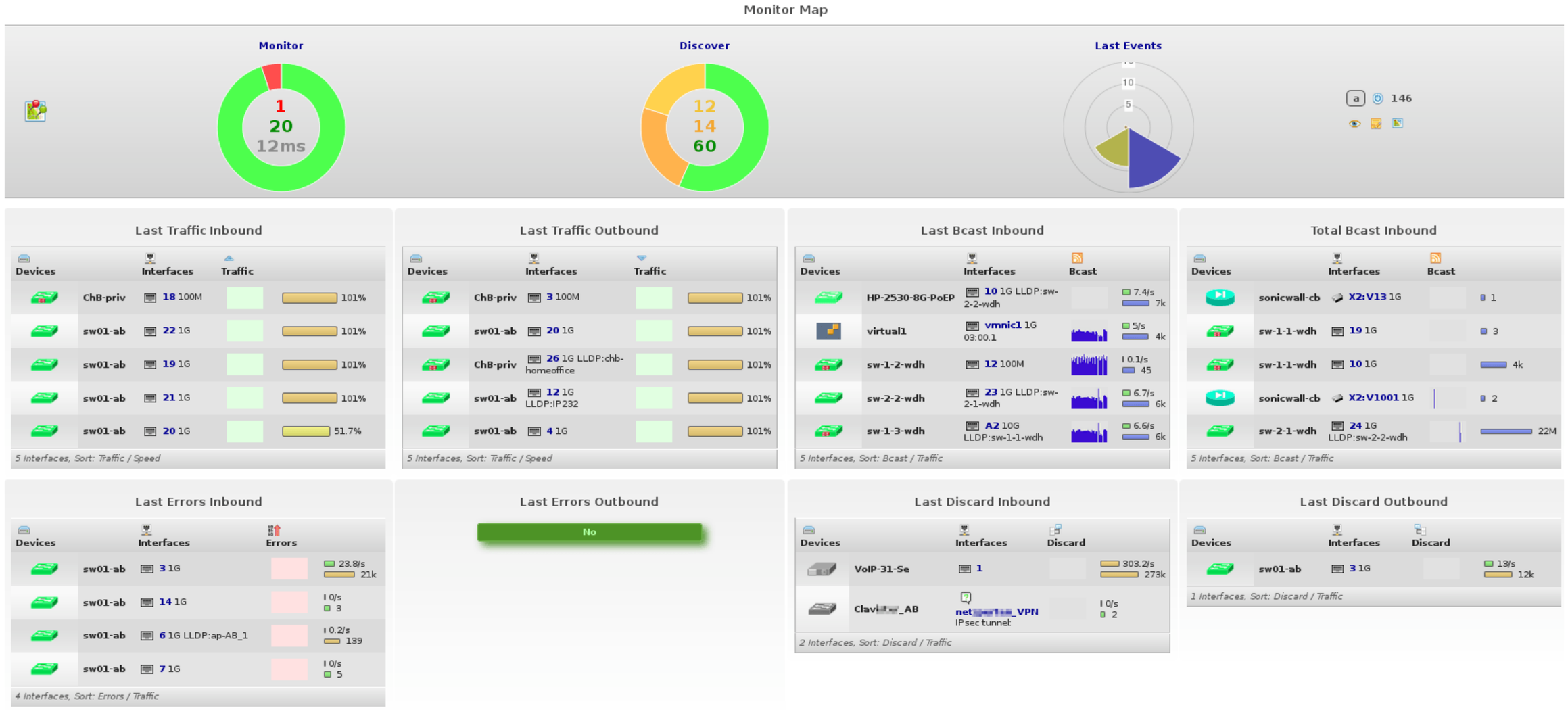
MONITORING

MONITORING MAP

EDITOR



REPORTS IN MONITORING MAP



OPTICAL MONITORING

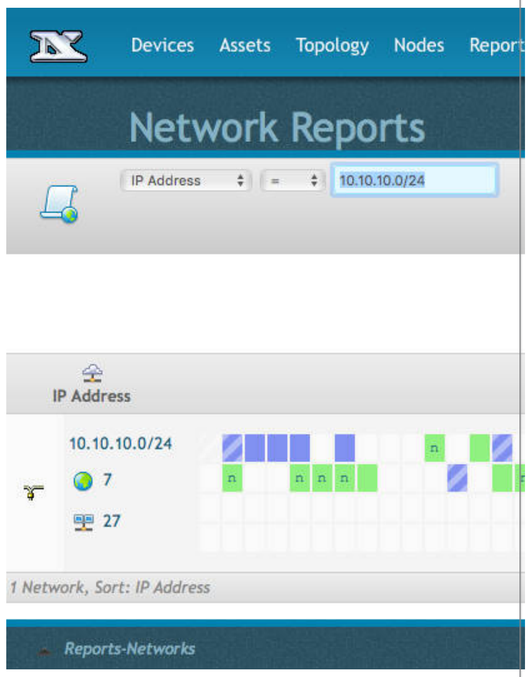
Module

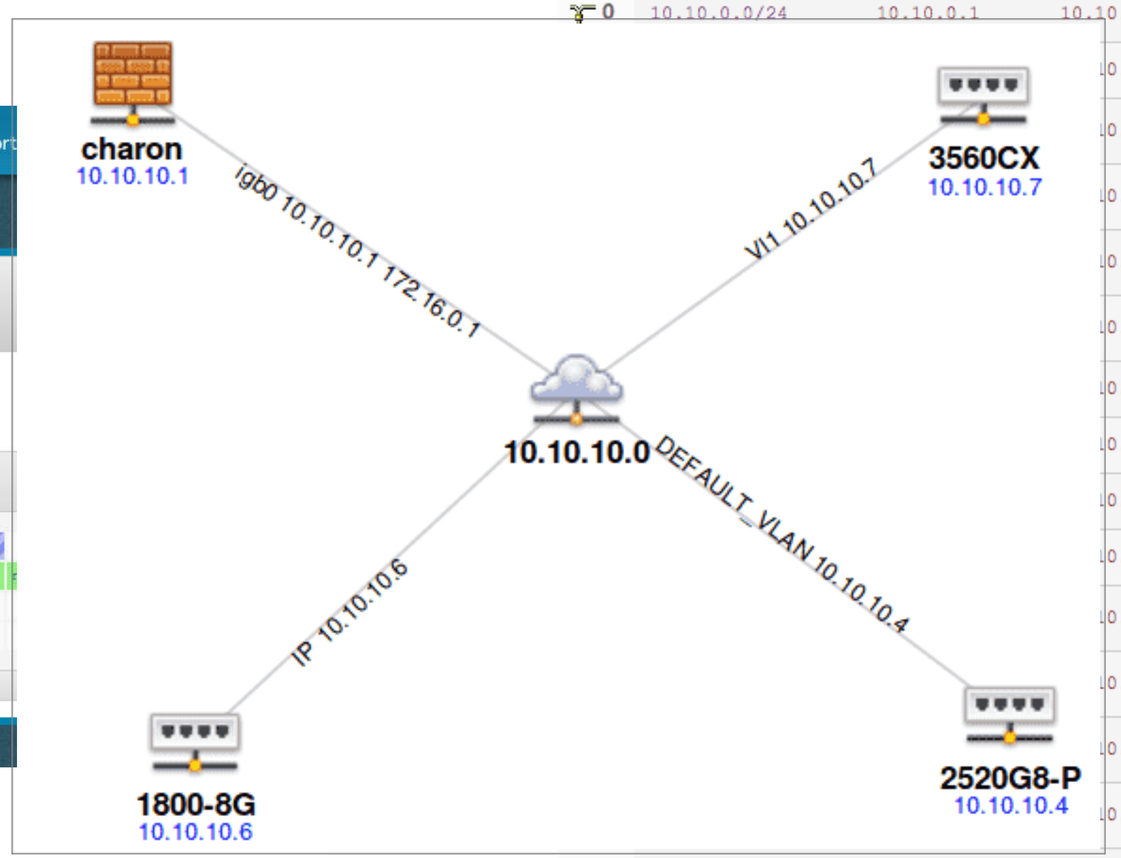
	Information
Eter1-14	LX2122IDR - RX:-6dBm TX: -8dBm
Eter1-15	LX2122IDR - RX:-5dBm TX: -8dBm
Eter1-16	LX2122IDR - RX:-5dBm TX: -37dBm
Eter1-17	LX2502IDR - RX:-6dBm TX: -8dBm
Eter1-18	LX2502IDR - RX:-6dBm TX: -15dBm
225 Module Total	

nedi.conf

```
#           type    TX-hi   TX-lo   RX-hi   RX-lo   description (replaces module description)
dom-alert   default 3       -10     3       -12     default-settings
```

VERIFY YOUR IPAM

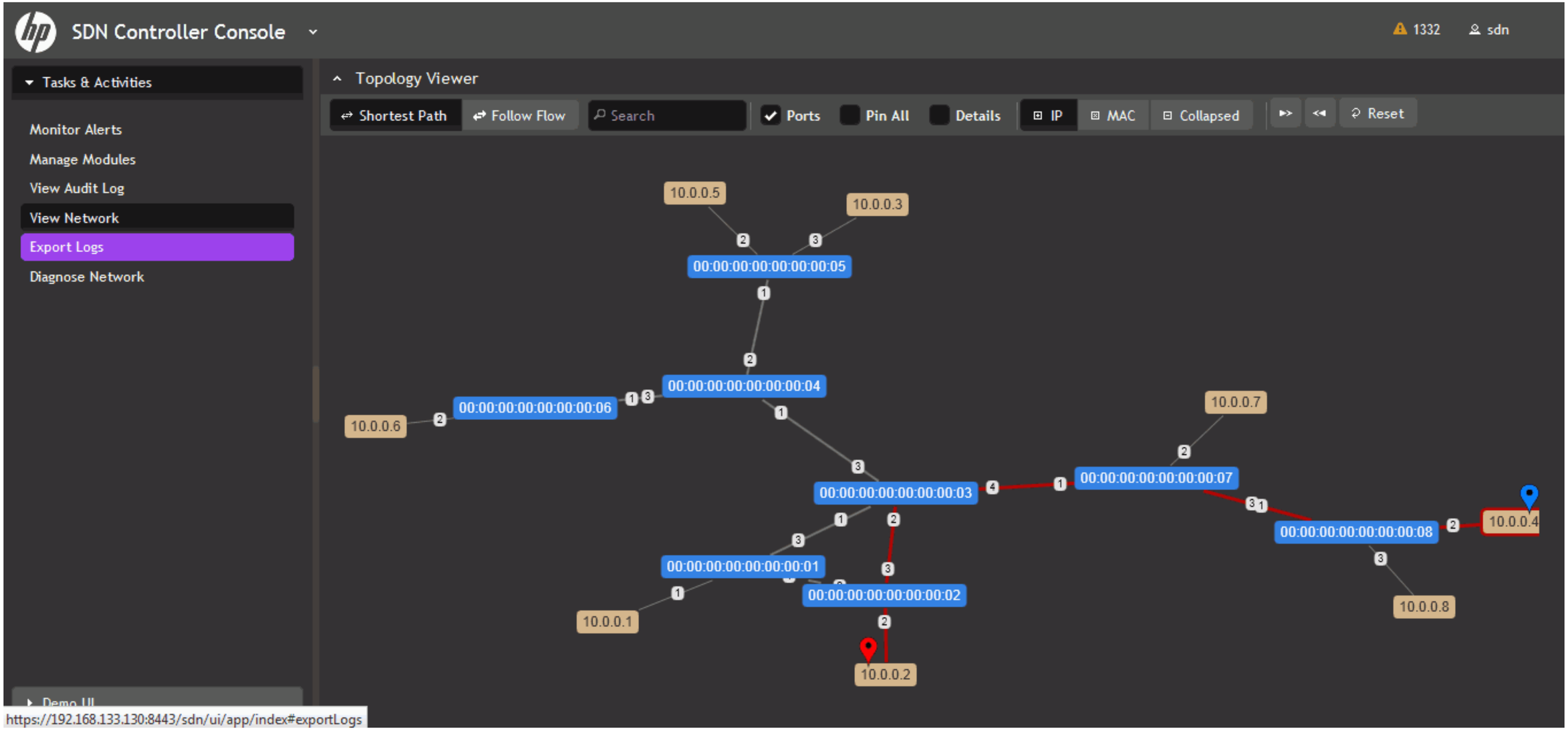




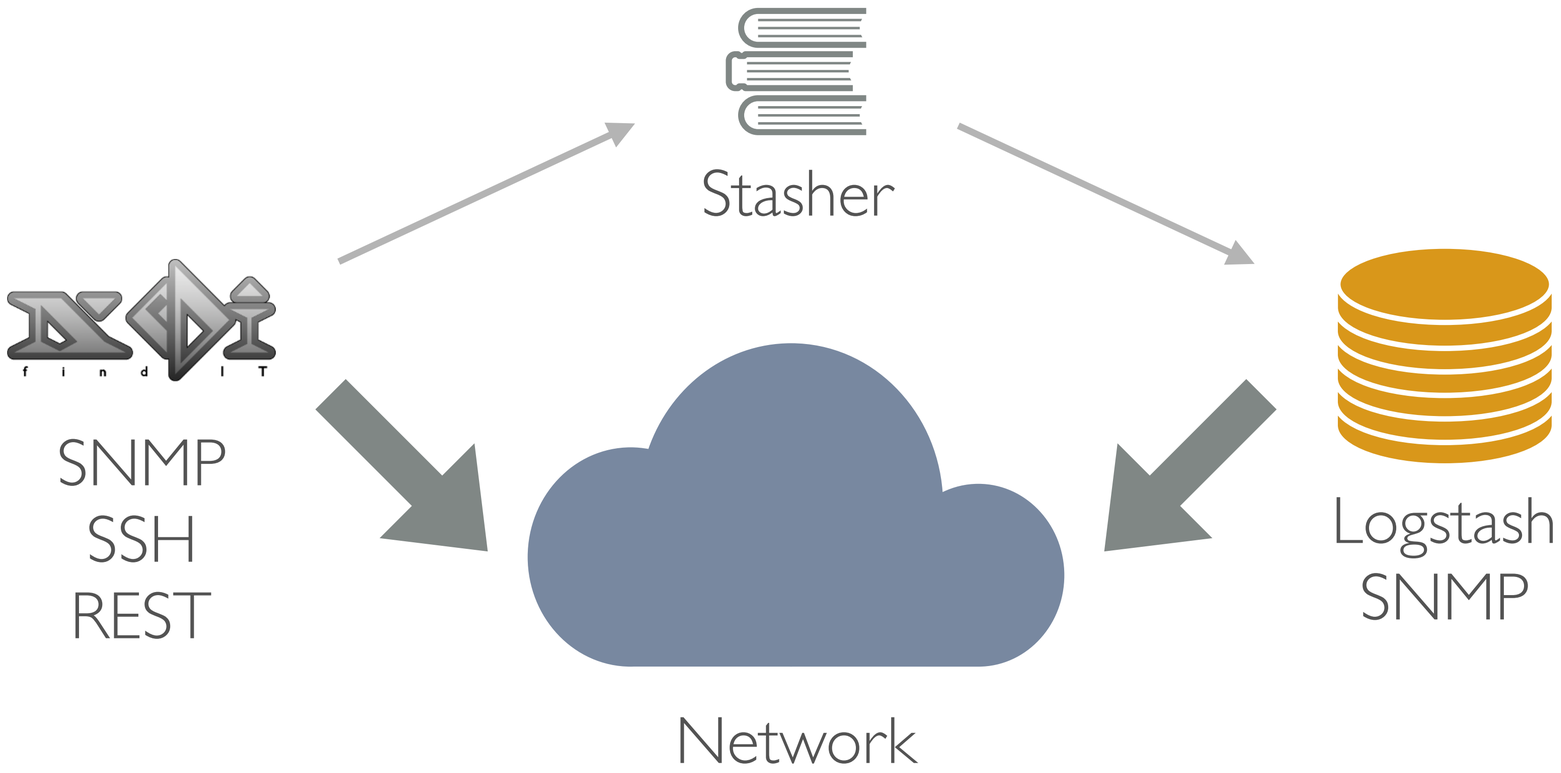
Subnet List

	Network	Start	End	Bcast	Total Population
0	10.10.0.0/24	10.10.0.1	10.10.0.254	10.10.0.255	254
			10.10.1.254	10.10.1.255	508
			10.10.2.254	10.10.2.255	762 1
			10.10.3.254	10.10.3.255	1016 1
			10.10.4.254	10.10.4.255	1270 1
			10.10.5.254	10.10.5.255	1524 1
			10.10.6.254	10.10.6.255	1778
			10.10.7.254	10.10.7.255	2032
			10.10.8.254	10.10.8.255	2286
			10.10.9.254	10.10.9.255	2540
			10.10.10.254	10.10.10.255	2794 25 23 25
			10.10.11.254	10.10.11.255	3048 1
			10.10.12.254	10.10.12.255	3302 1
			10.10.13.254	10.10.13.255	3556 1
14	10.10.14.0/24	10.10.14.1	10.10.14.254	10.10.14.255	3810
15	10.10.15.0/24	10.10.15.1	10.10.15.254	10.10.15.255	4064

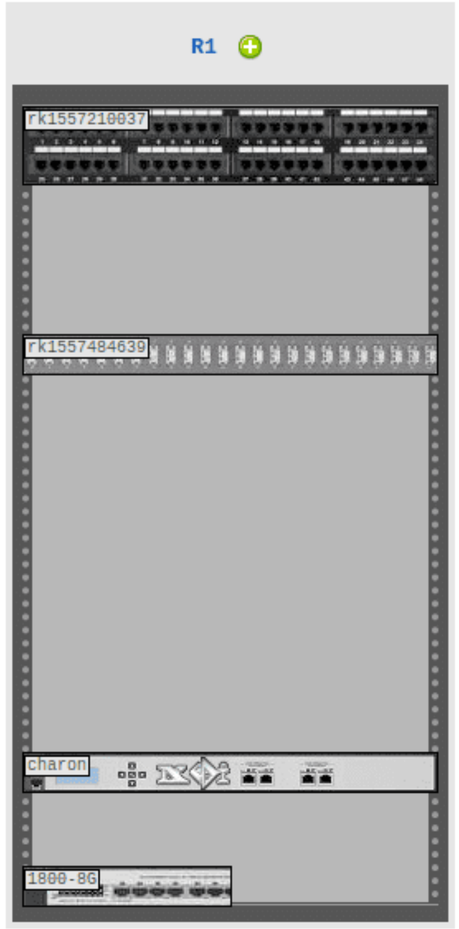
VERIFY YOUR SDN

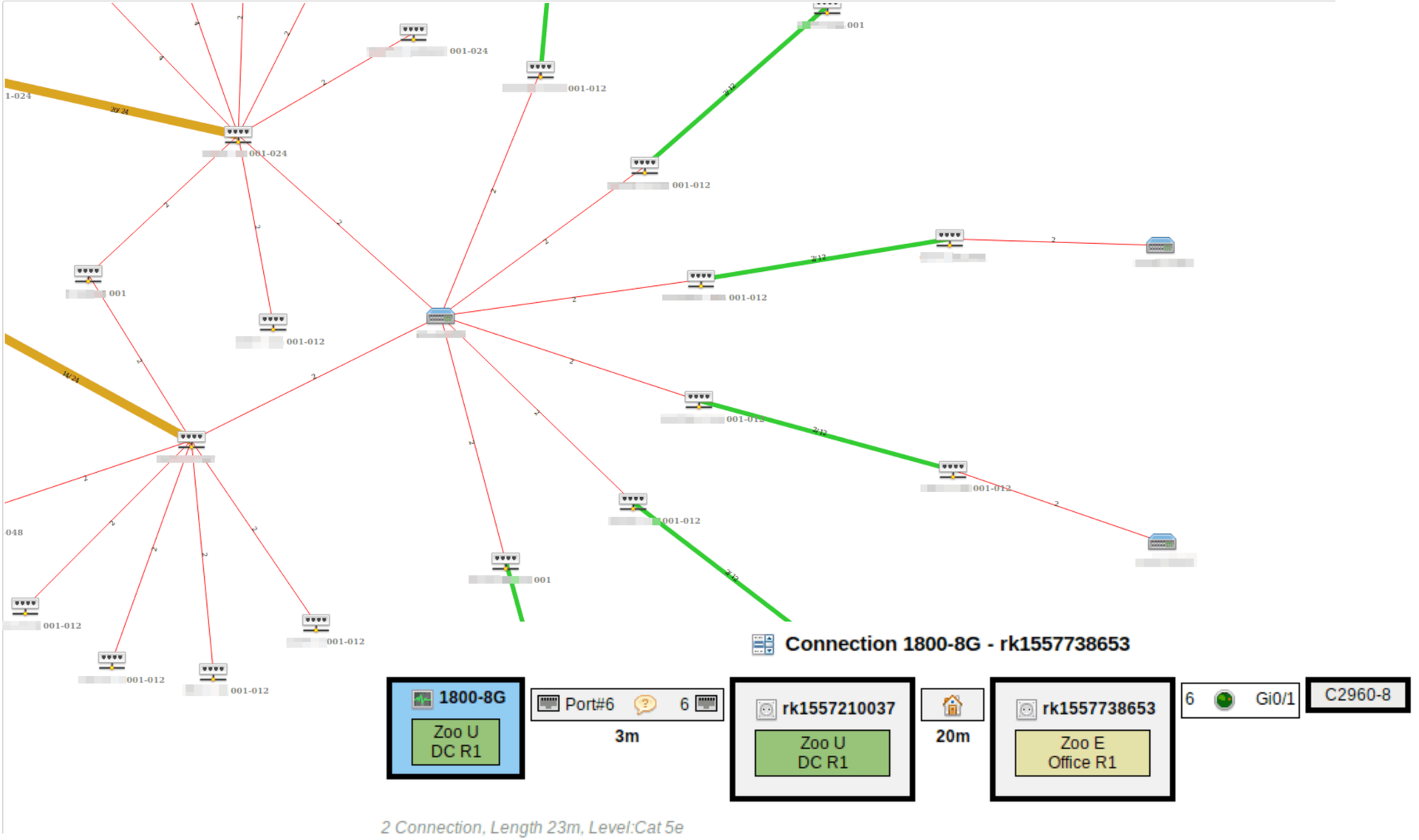


NEDI 2 LOGSTASH



CABLE MANAGEMENT





COMPLETE END TO END VIEW

NeDi+

- Network infrastructure discovery
- Lifecycle management
- Topology discovery & visualisation
- IP address and subnet verification
- Monitoring & network policies
- Traffic analysis

Addons

- Cable Management

THANKS!