



# Why it's still here

[www.nedi.ch](http://www.nedi.ch)

# I LIKE FLYING AND...

---

2008



2017



2018

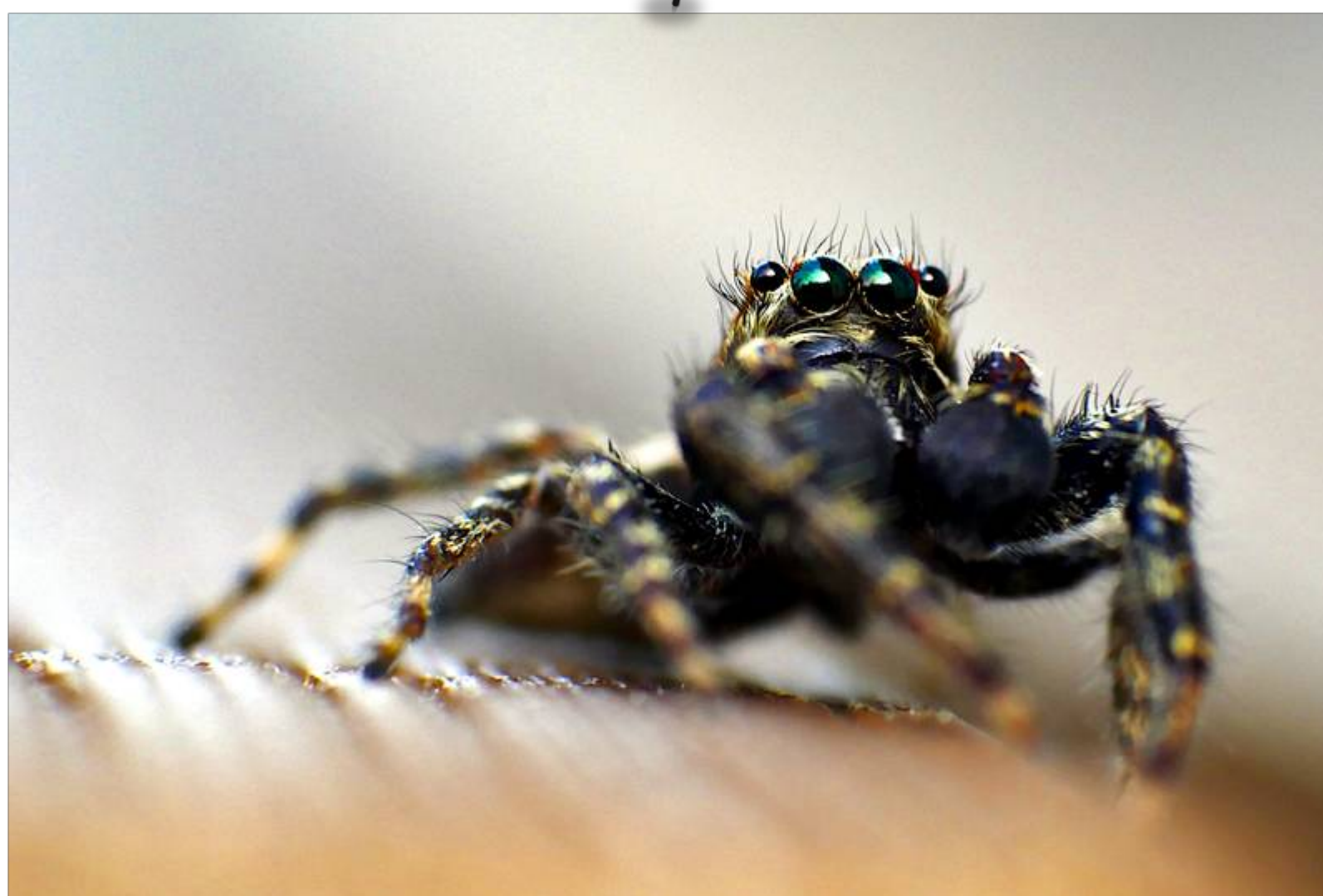


2019



# MACRO FOTOGRAFY

---



# HOW IT ALL STARTED

---

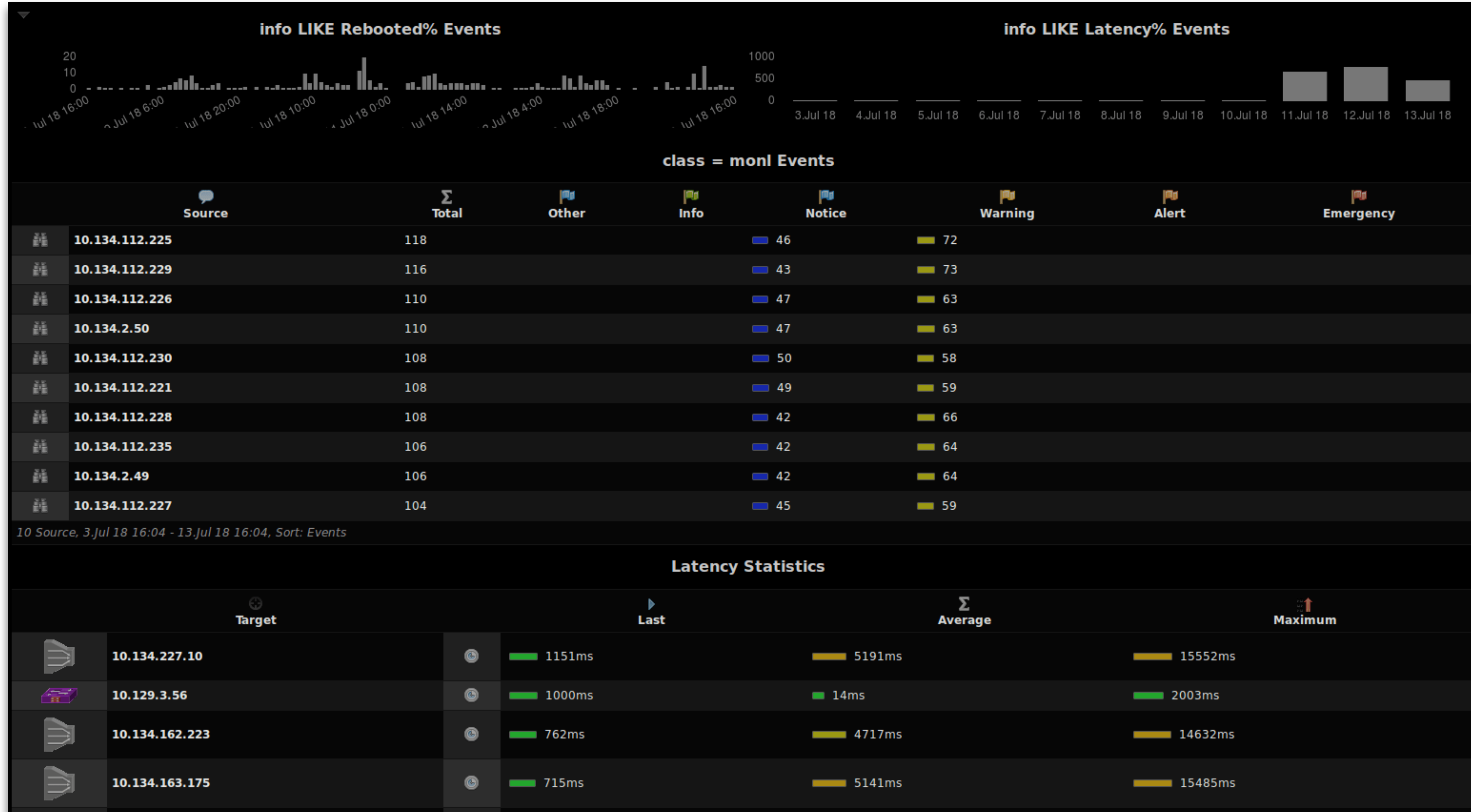
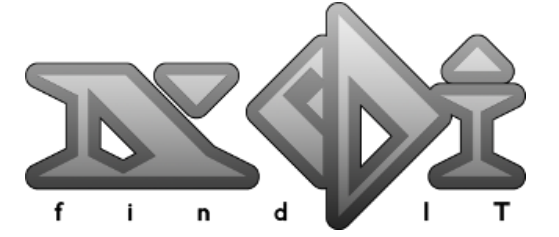
Back in 2001 ...



...available solutions were like:



# WHAT IT DOES



# DISCOVERING THE NETWORK

## Module Status

	Cat4k5	Linecard(slot 1)	WS-X4013+
	Cat4k5	Linecard(slot 2)	WS-X4248-RJ45V
	Cat4k5	Linecard(slot 3)	WS-X4248-RJ45V
	Cat4k5	Linecard(slot 6)	WS-X4306-GB
	Cat4k5	Power Supply 1	PWR-C45-2800ACV
	Cat4k5	Power Supply 2	PWR-C45-2800ACV

12 Modules, Sort: slot, Limit: 250

## Port Status per Fabric Extender

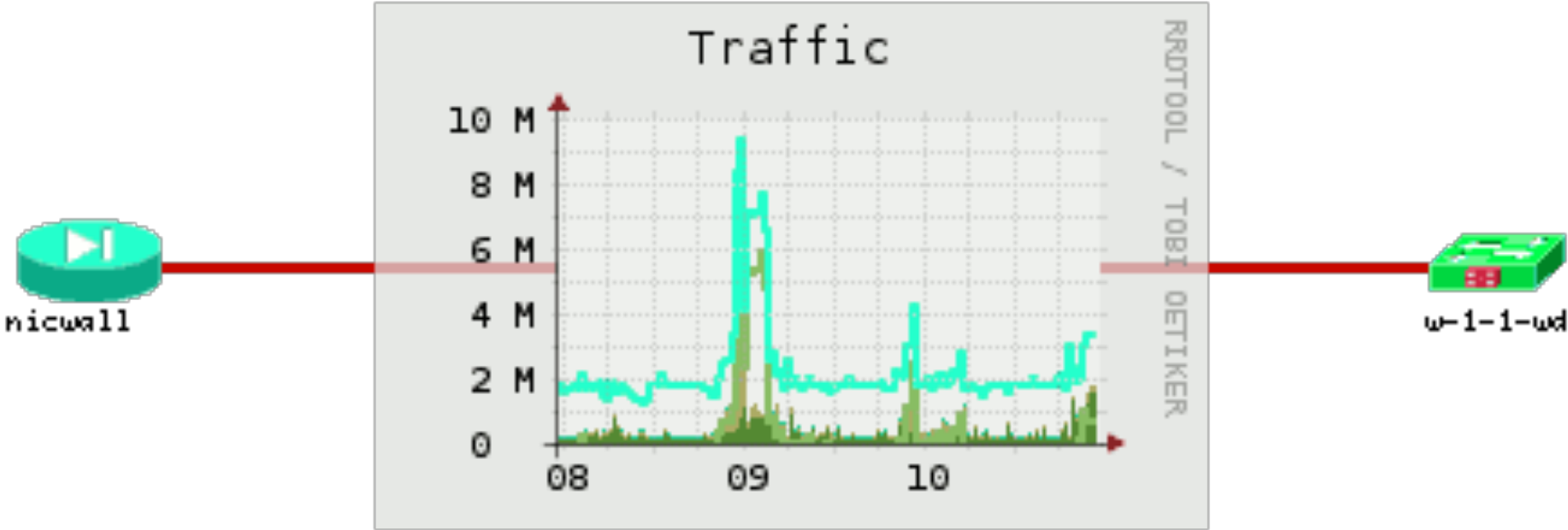
Fex-105 Nexus2248 Chassis	Fabric Extender Module: 48x1GE,	11 25 12
Fex-105 Nexus2248 Chassis	Fabric Extender Module: 48x1GE,	19 29
Fex-106 Nexus2200HP Chassis	Fabric Extender Module: 16x10GE	
Fex-106 Nexus2232 Chassis	Fabric Extender Module: 32x10GE	16 16
Fex-106 Nexus2248 Chassis	Fabric Extender Module: 48x1GE,	37 11
Fex-106 Nexus2248 Chassis	Fabric Extender Module: 48x1GE,	30 18
Fex-106 Nexus2248 Chassis	Fabric Extender Module: 48x1GE,	27 21
Fex-107 Nexus2200HP Chassis	Fabric Extender Module: 16x10GE	Active
Fex-107 Nexus2232 Chassis	Fabric Extender Module: 32x10GE	5 27

## LAG Ports

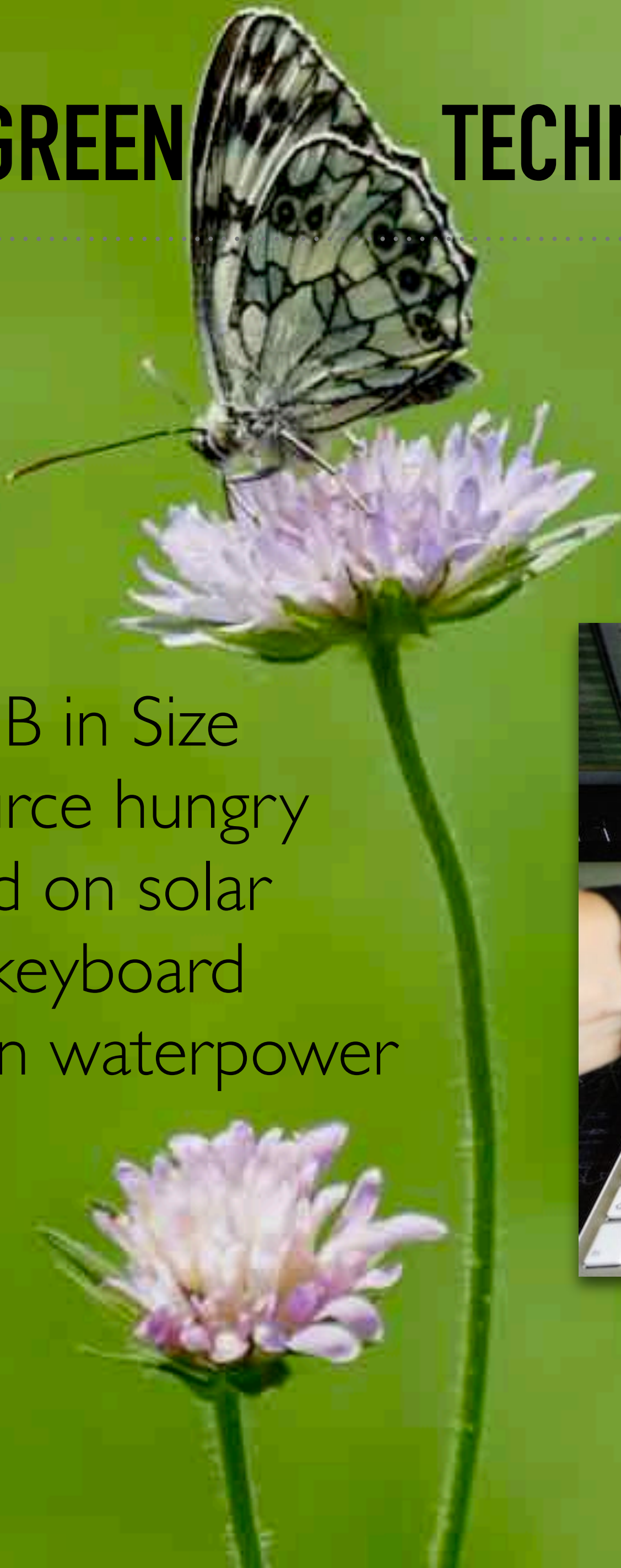
23		23 LAG:Trk1
24		24 LAG:Trk1
Trk1		Trk1

3k5-Core2 IP:10.10.10.1  
3500yl-24G, revision K.1  
subbuildm/K\_rel\_memo

## Dynamic Maps

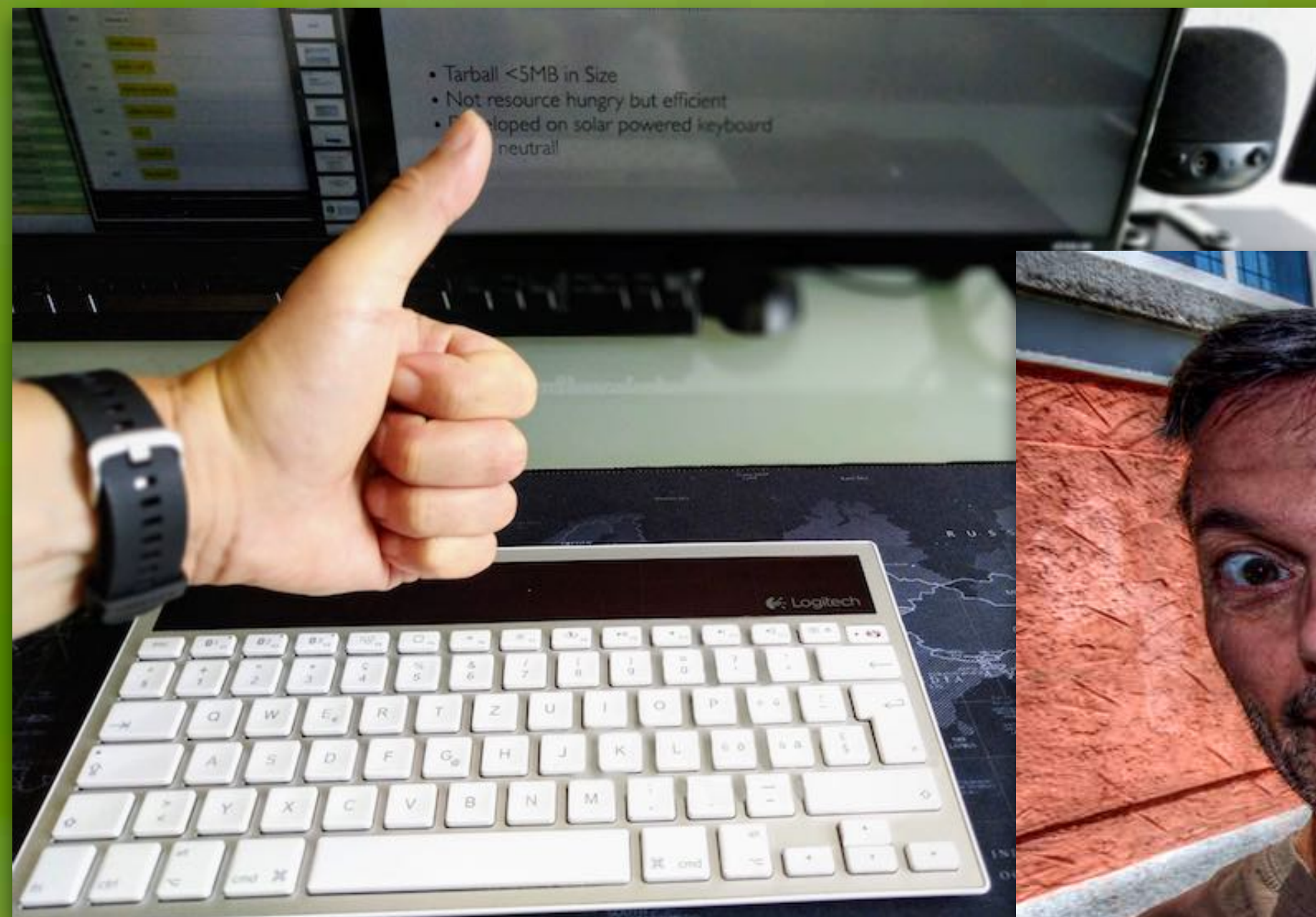


# NEDI IS GREEN TECHNOLOGY



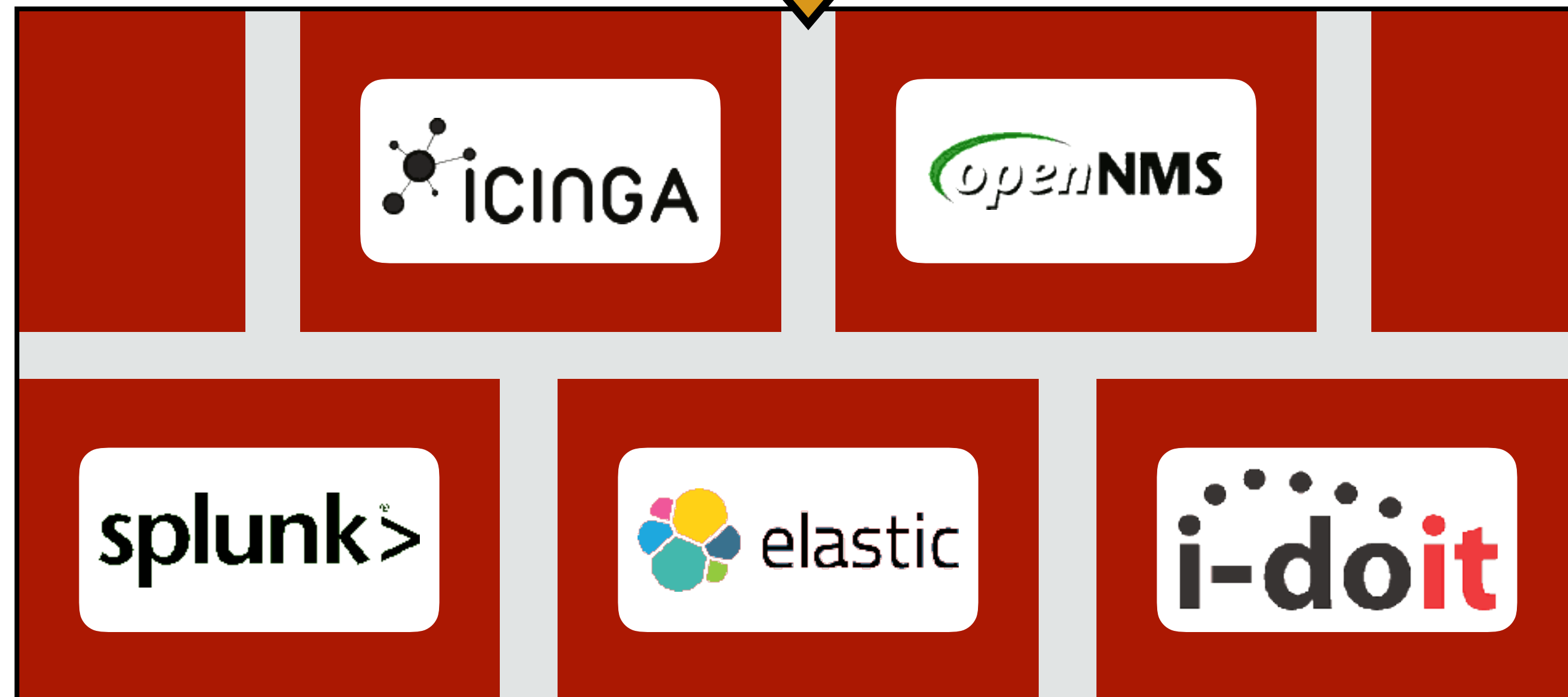
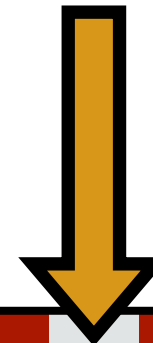
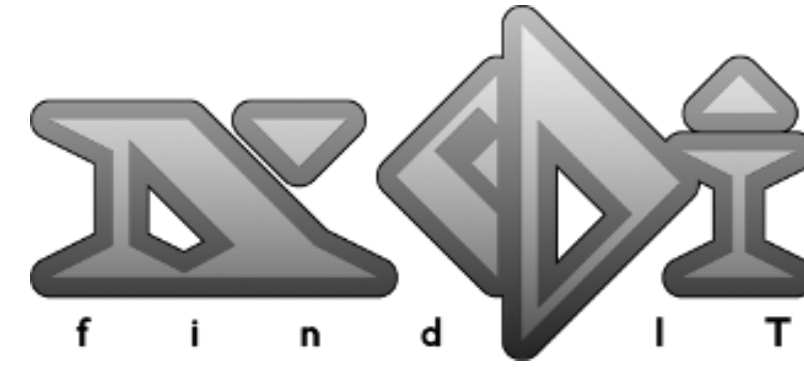
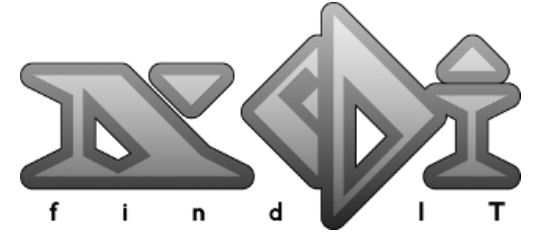
```
-rw-r--r-- 1 rickli rickli 4.0M Jul 6 14:16 nedi-1.9.187.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul 9 09:15 nedi-1.9.190.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul 12 12:44 nedi-1.9.193.pkg
-rw-r--r-- 1 rickli rickli 4.0M Jul 17 16:10 nedi-1.9.198.pkg
```

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



# NEDI & THE BIG GUYS

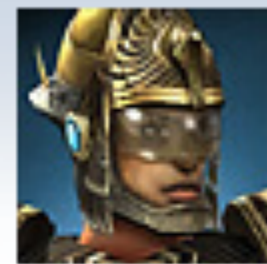
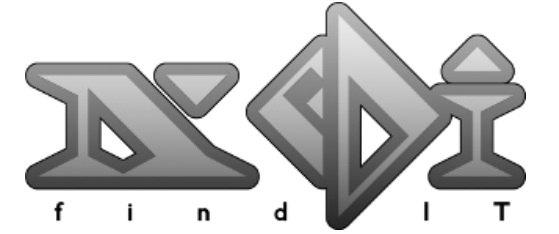
---





**SECURITY**

# THE NEDI COMMUNITY



**Hello rickli**

Show unread posts since last visit.  
Show new replies to your posts.  
There are 2 members awaiting approval.  
October 31, 2013, 09:15:49 PM

[Home](#) [Help](#) [Search](#) [Admin](#) [Moderate](#) [Profile](#) [My Messages](#) [Members](#) [Logout](#)

NeDi Community

Mem

## News

**NeDi 1.0.9 beta released (see [www.nedi.ch](http://www.nedi.ch))!!!**

## NeDi General



### News

Announcements, Press releases and more...

638 Posts  
23 Topics

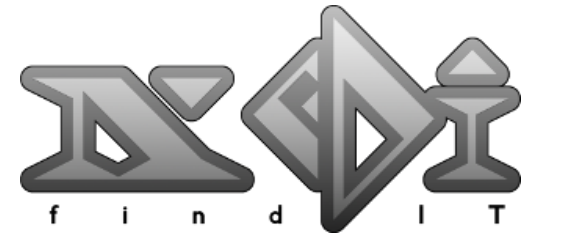


### Other

Integration with other tools or other fancy ideas

301 Posts  
54 Topics

AAAAAAAAAAAAAARGH!



## Forbidden

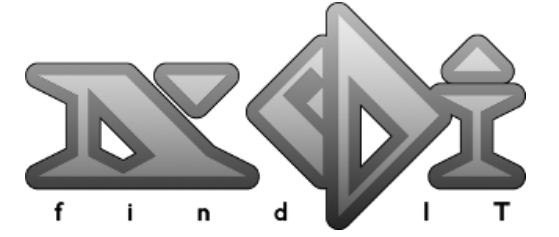
You don't have permission to access /gfds on this server.

---

*Apache/2.2.20 (Ubuntu) Server at q Port 80*

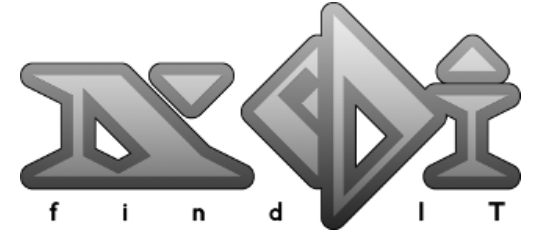


# LOOKING AT WEBSTATS



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

# PHISHING MAILS



## Info

Inbox - NeDi Yesterday at 19:23



PAYPAL

To: undisclosed-recipients;; servicemail@mail.com,

Reply-To: team@mint.com



**PayPal**

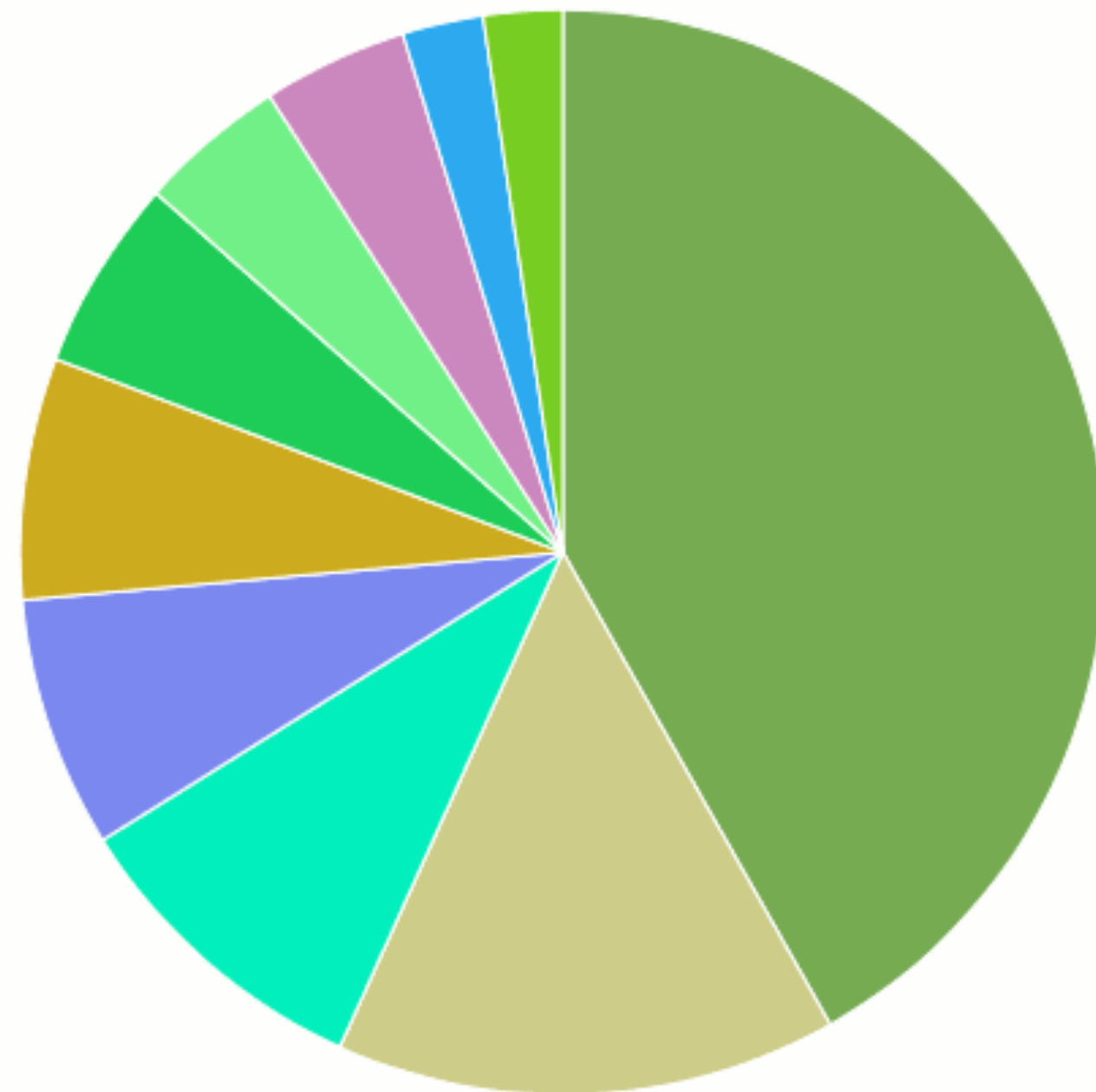
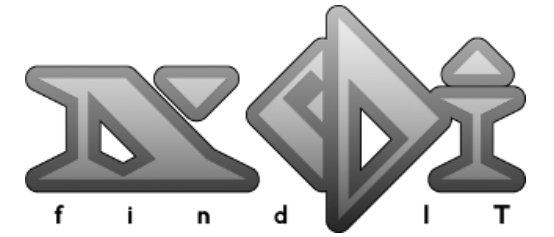
ID: #R56L6D9R406MH

Account Notification

[Login Now](#)










<http://24kontaktlinsen.de/js1/>

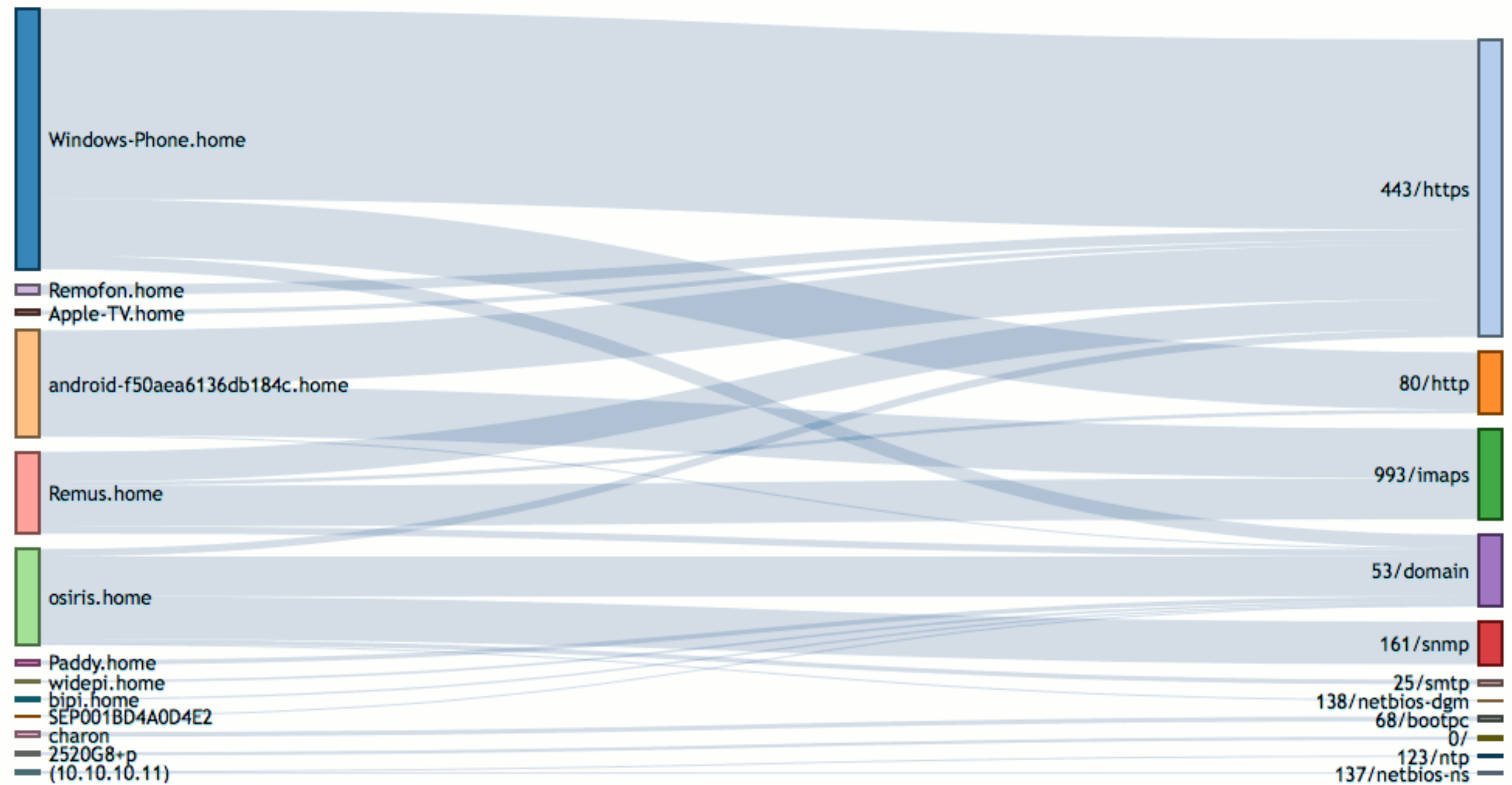
# TRAFFIC ANALYSIS



Summary

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

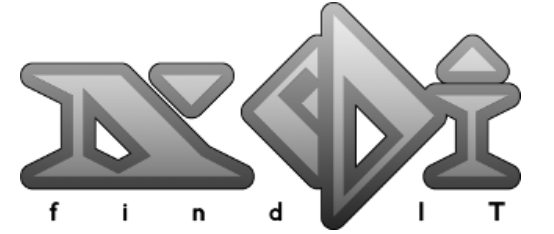
Destination Address	Destination Port	Packets	Bytes
Google Inc.    443/https	443/https	10k	595k
Google Inc.    443/https	443/https	3k	213k
Google Inc.    443/https	443/https	2k	133k















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

	<b>216.58.207.46/24</b>
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

## TRAFFIC POLICIES

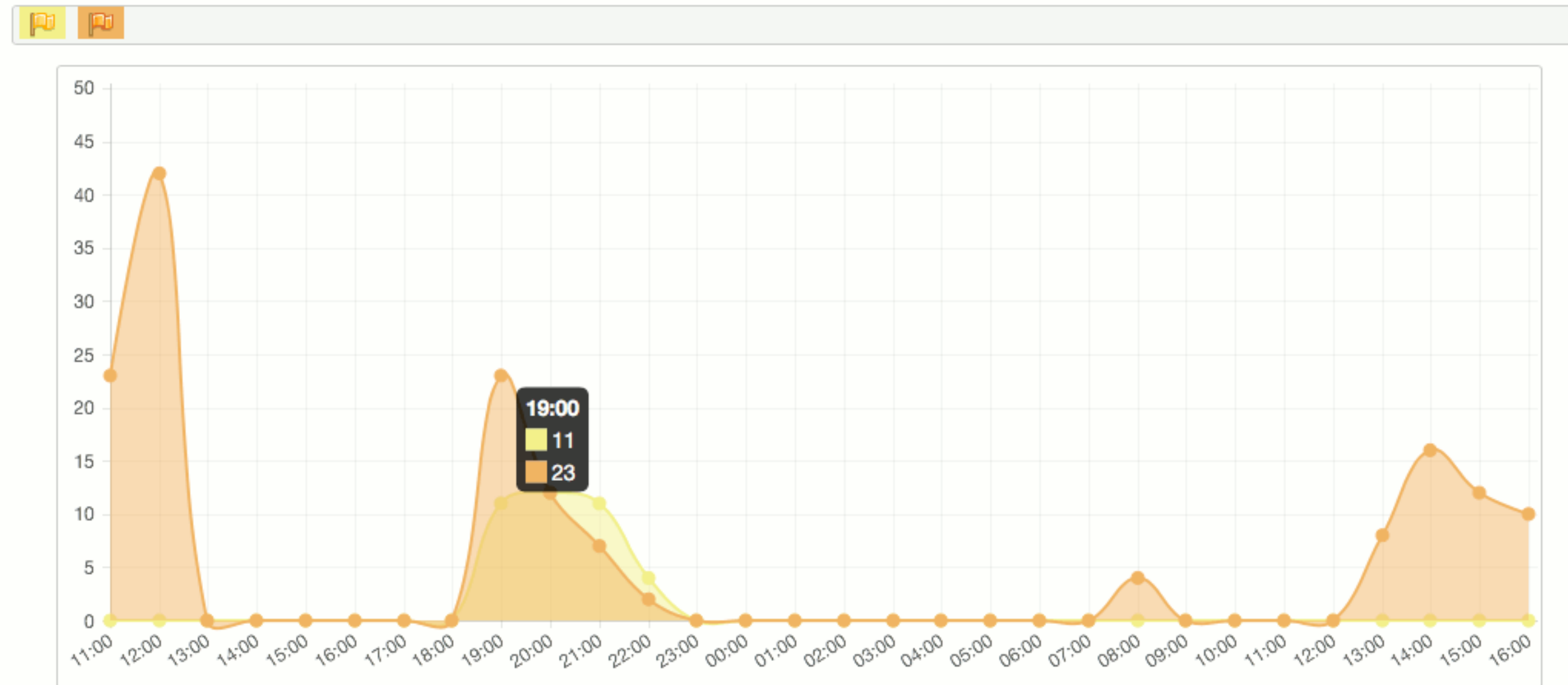
Id	Status	Class	Target	Device	Port	Vlan	Action	Information	User	Time	Execute
19	⚡	Bytes	> 500000	Source:charon Filter:src host 10.10.10.109 Group:sa,da					admin	31.Mar 16 12:45	📄 ⏹ ❌
15	⚡	Bytes	< 100	Source:charon Filter:src host 10.10.10.10 and port 5060 Group:sa			👉	SIP underrun	admin	28.Mar 16 16:02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

3 Values

## TIMELINE ANALYSIS

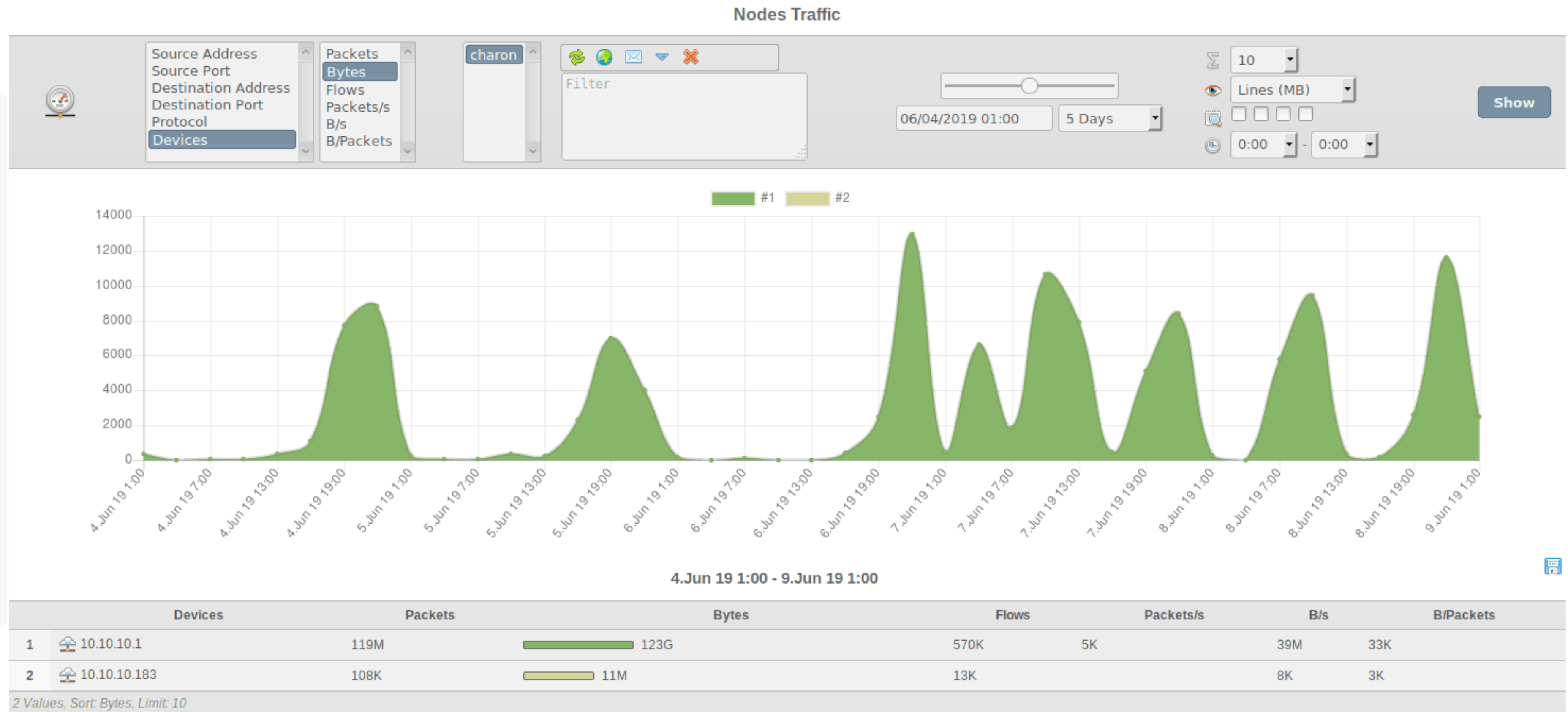
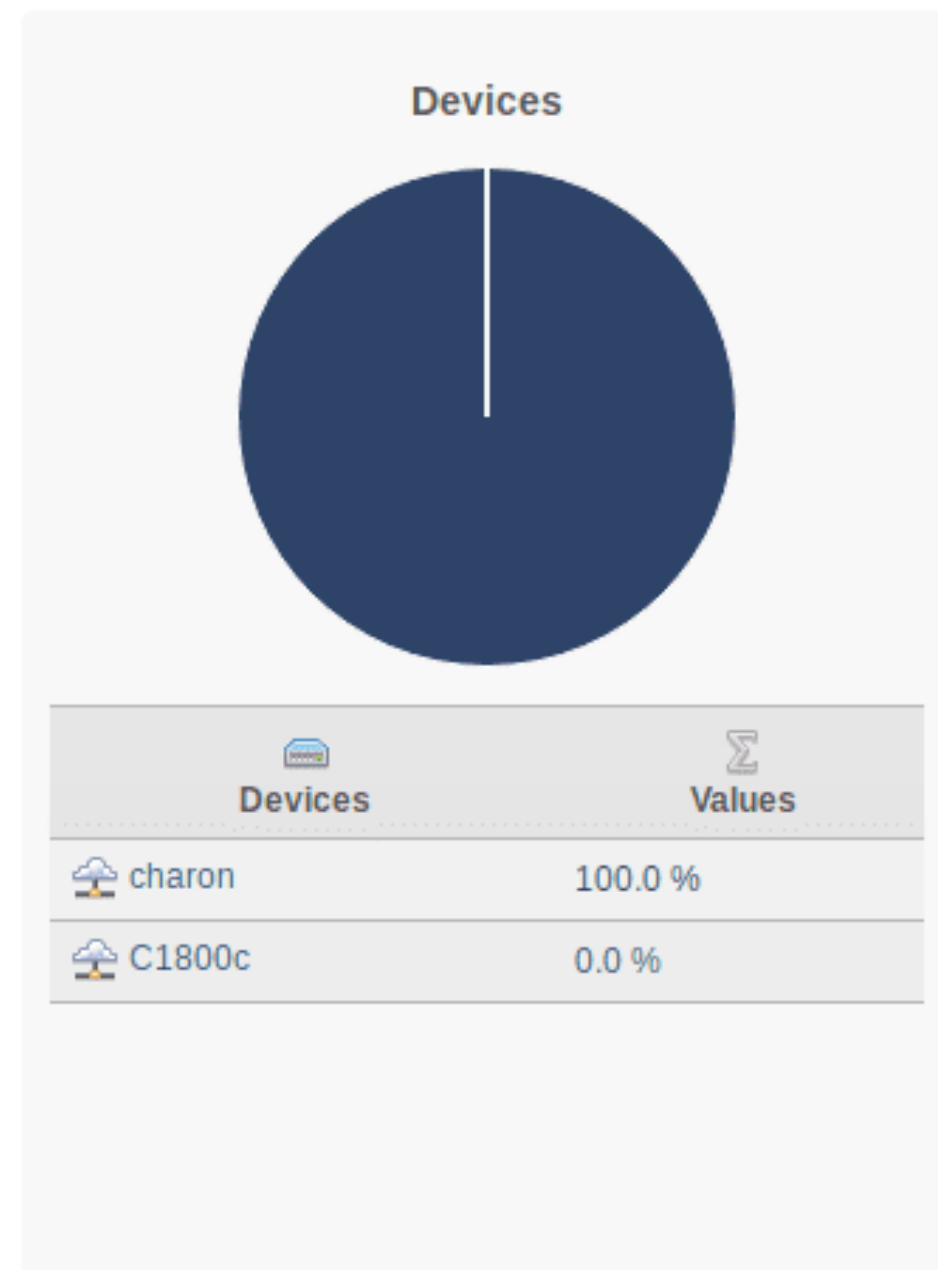
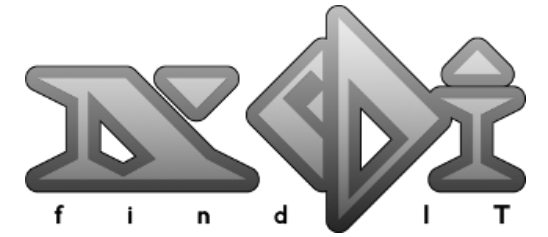
31.Mar 16 11:40 - 1.Apr 16 17:40

Class LIKE 'sp%'

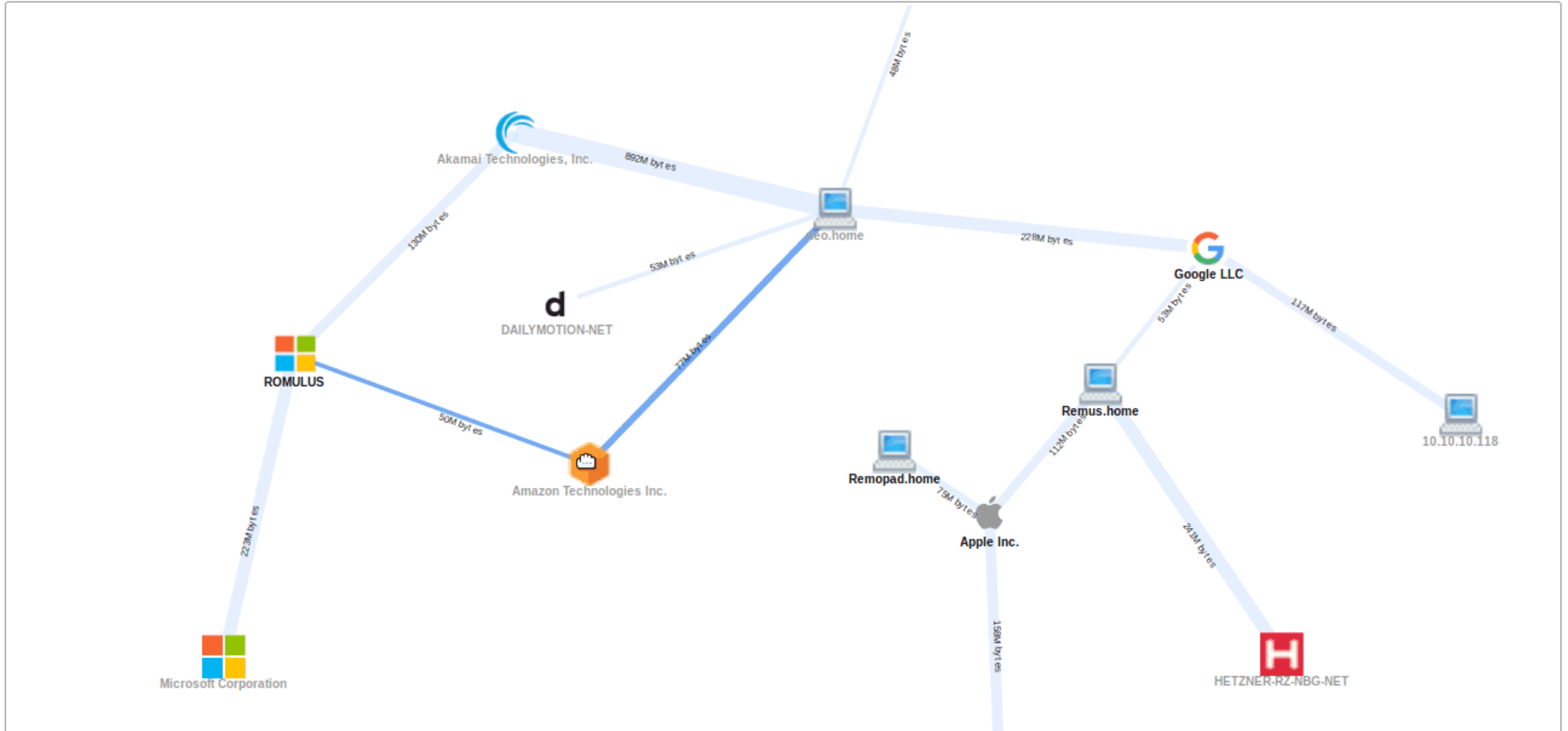
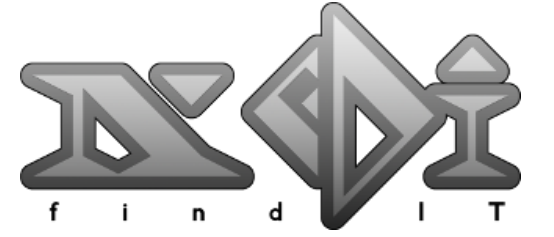




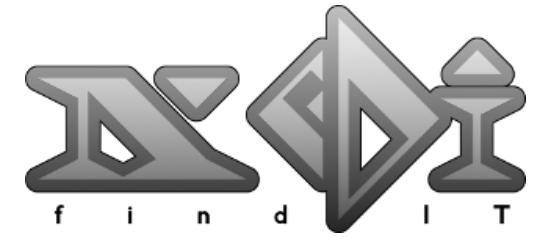
# TRAFFIC SOURCES (2.0)





















# TRAFFIC MAP (2.0)



# IMPROVED IP INFORMATION (2.0)



## ARP Values

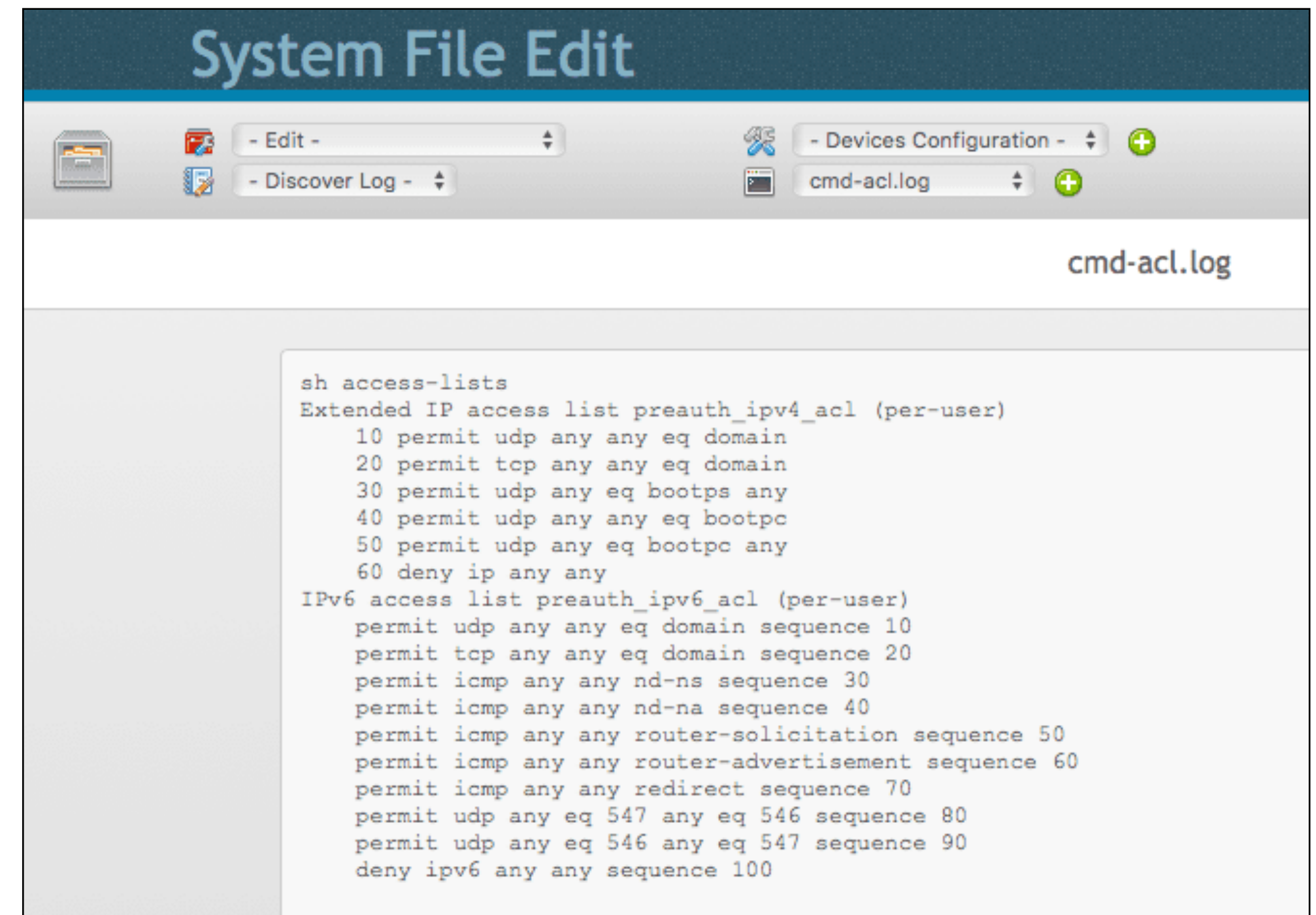
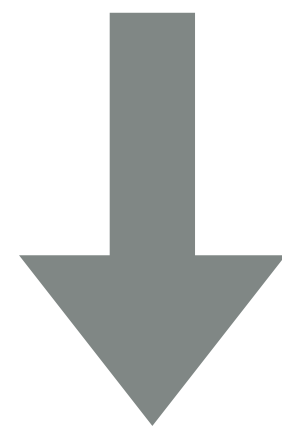
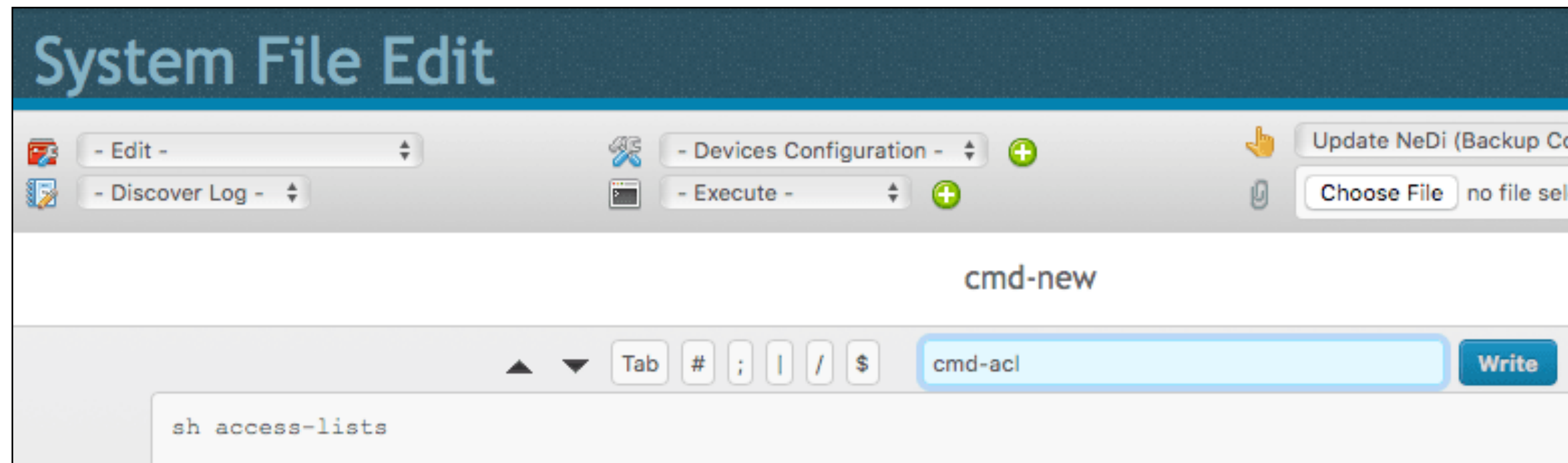
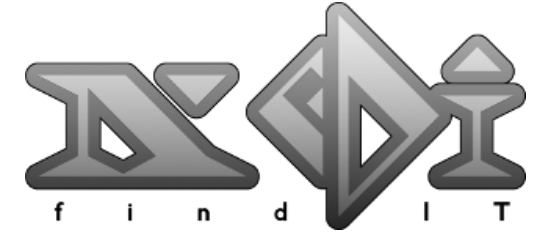
 MAC	 IP	 Update	 Services	 Operating System	 Devices	 Port
 74da3825d964	10.10.10.100	10.Apr 19 22:45	SSH-2.0-OpenSSH_6.0p1,nginx/1.2.1,	 Debian	charon	igb0
 34ab3731ae83	10.10.10.112	11.Apr 19 9:25			charon	igb0
 b827ebd0b99a	10.10.10.113	11.Apr 19 7:20	SSH-2.0-OpenSSH_7.4p1,	 Raspbian	charon	igb0
 f47b5e0b8b5c	10.10.10.115	11.Apr 19 1:25			charon	igb0
 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
 000dbd7408ee	10.10.10.124	11.Apr 19 5:40			charon	igb0
 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
```

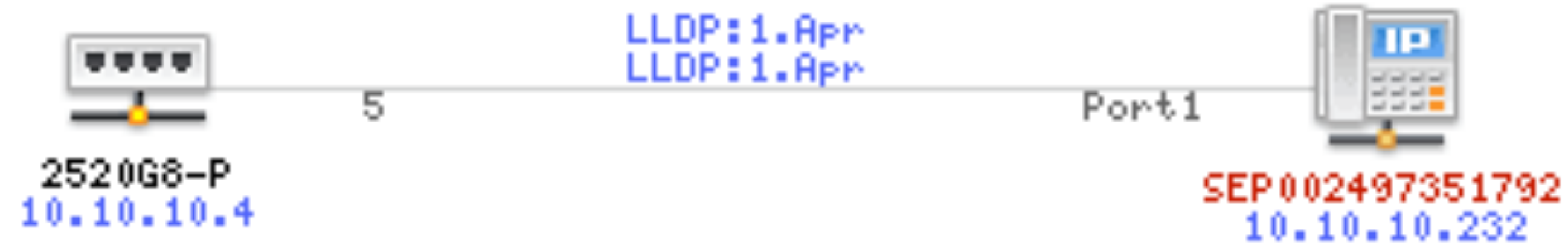
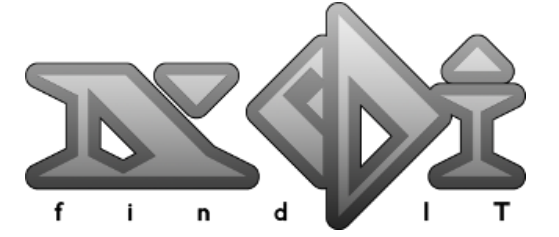
```
nedi.pl -sid -a10.10.10.0/24 Portscan by fping
```

# ACL MONITORING



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

# CONFIG CONTEXT POLICIES



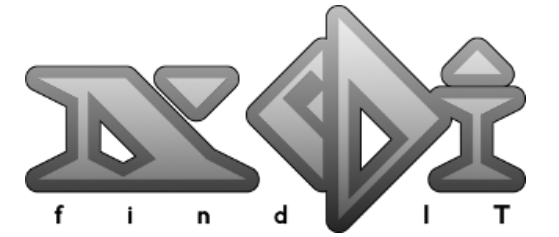
1333122		19.Jun 17 17:26	C2960-8		Policy 7: Portconfig is missing switchport mode trunk on Fa0/7 Tagged voice
1333121		19.Jun 17 17:26	C2960-8		Policy 7: Portconfig is missing switchport mode trunk on Fa0/3 Tagged voice
1333120		19.Jun 17 17:26	C2960-8		Policy 1: Config matches community public
1333119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

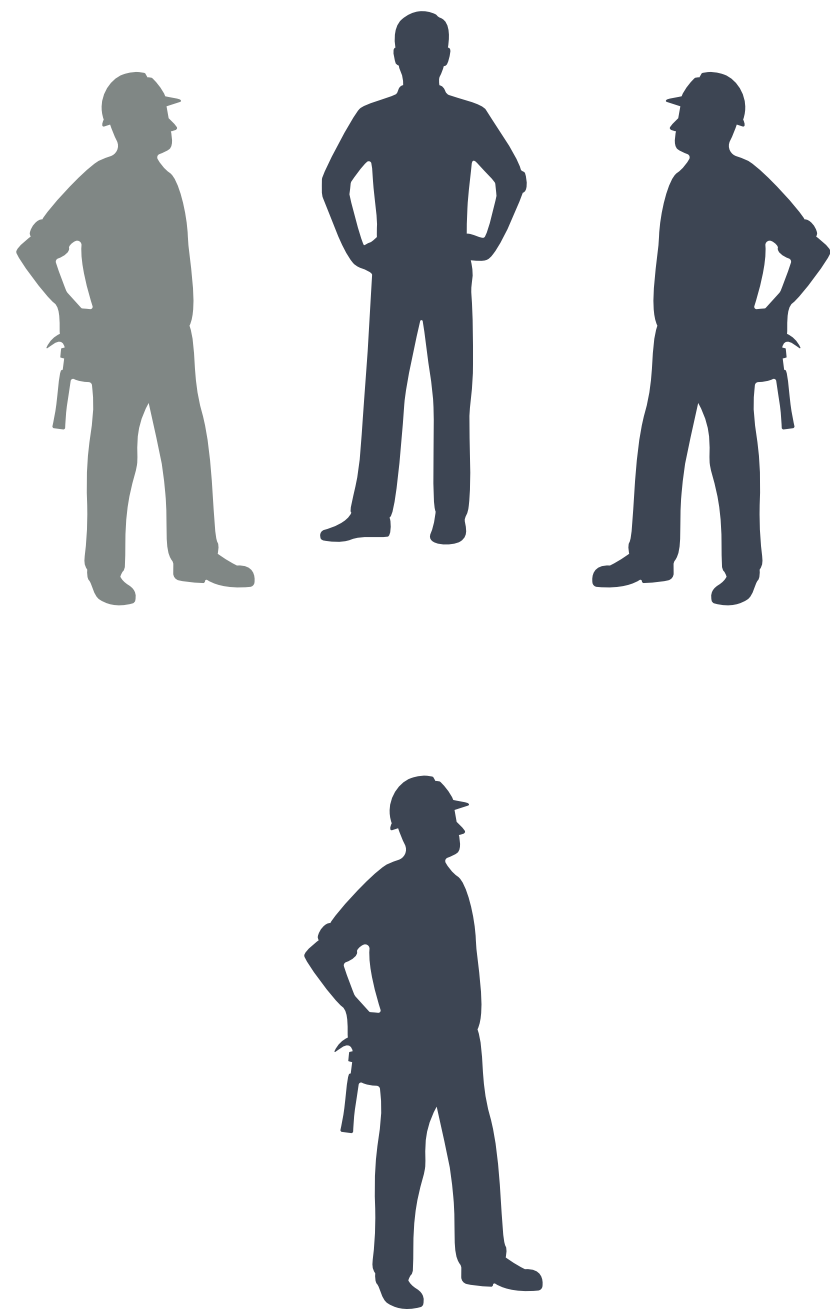
**NETWORKING**

# A NETWORKER'S LIFE

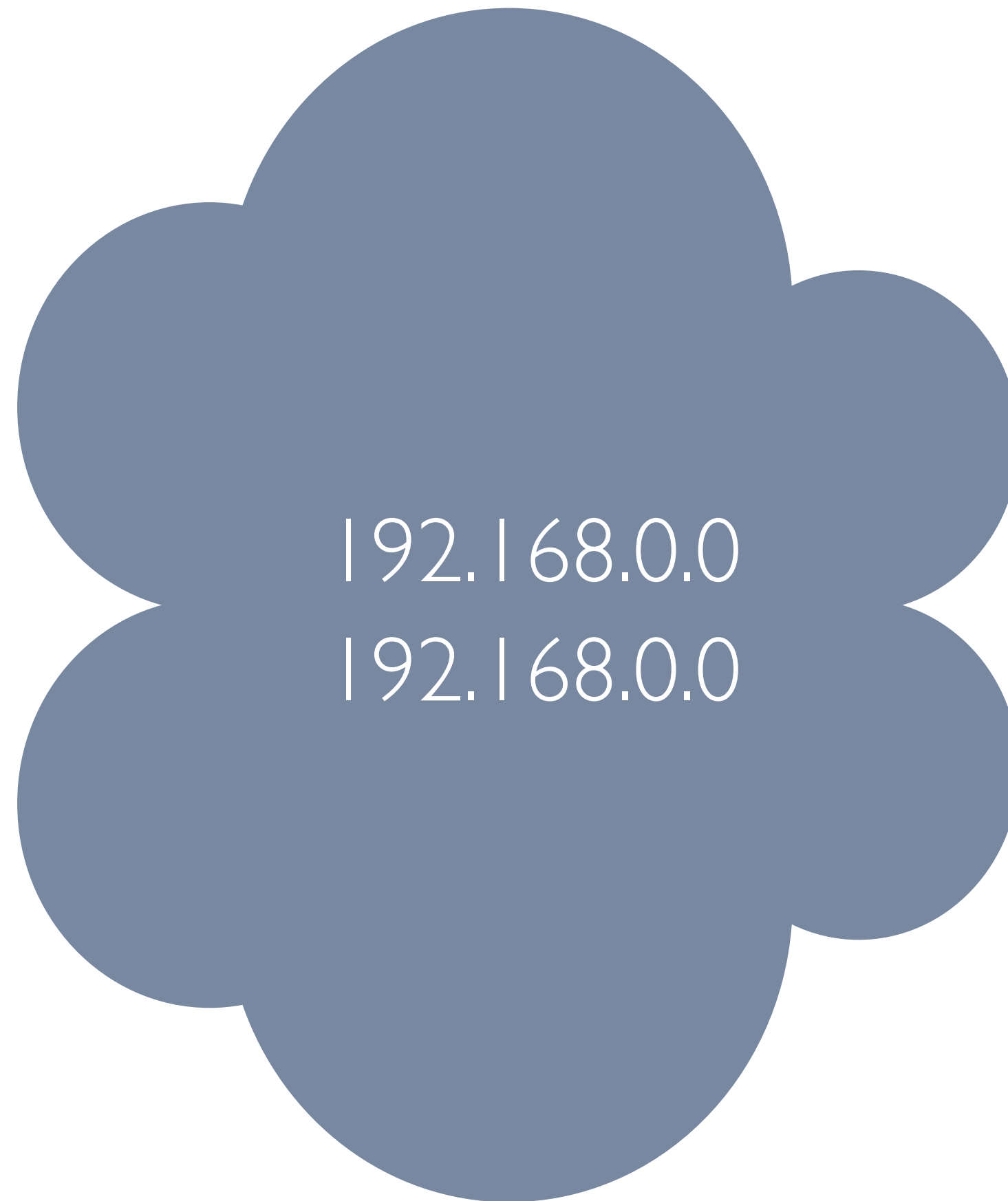
---



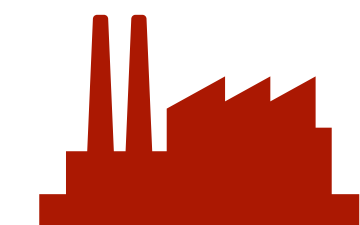
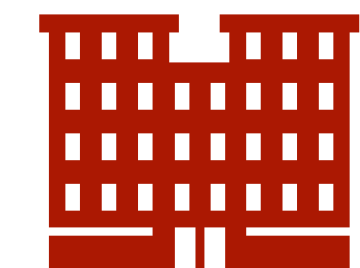
## Network Team



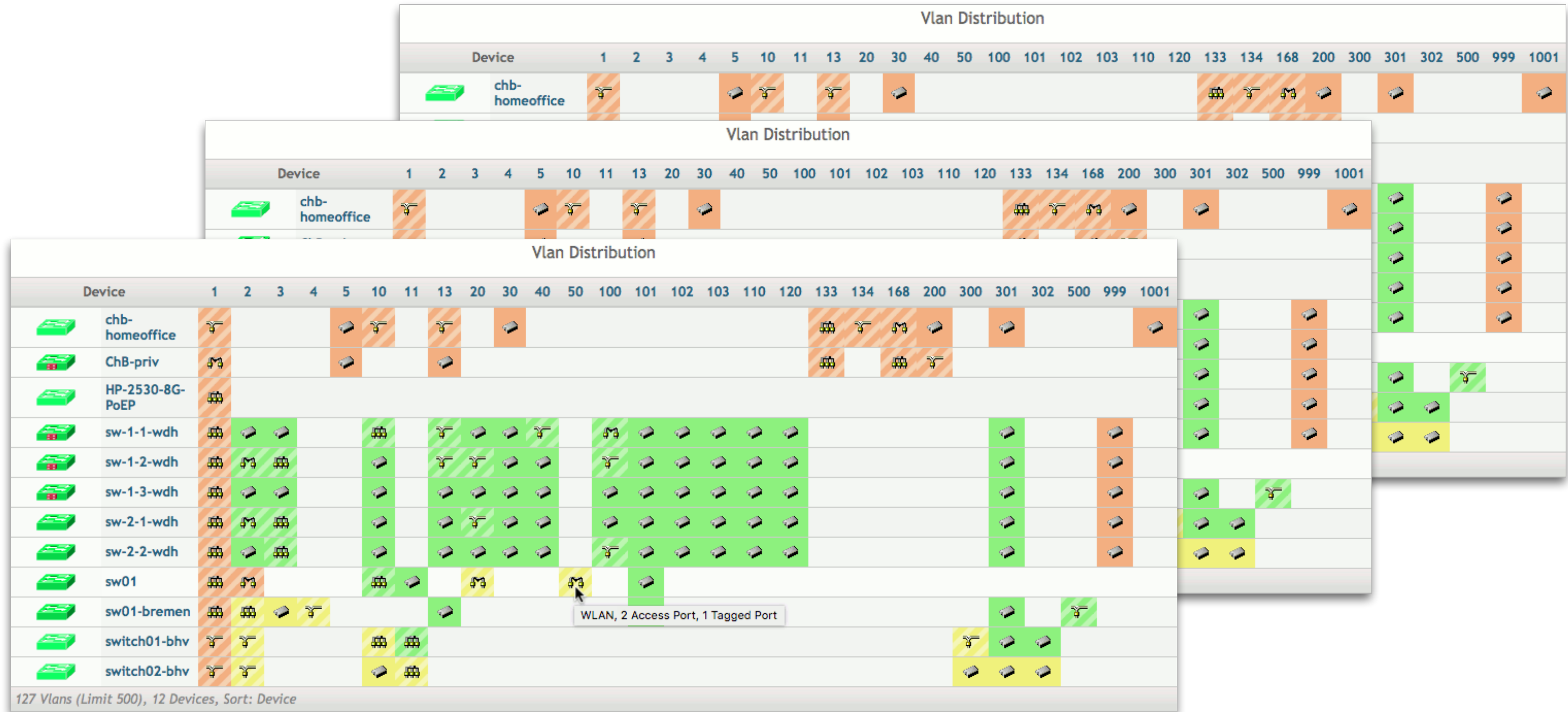
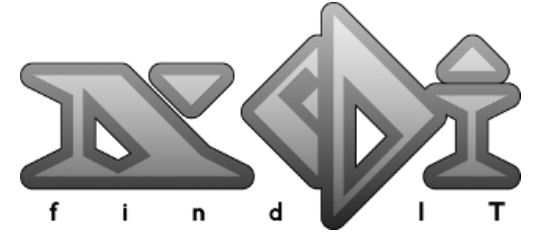
## The Network



## The Services

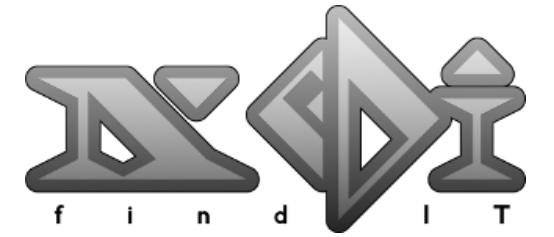


# TIME MACHINE





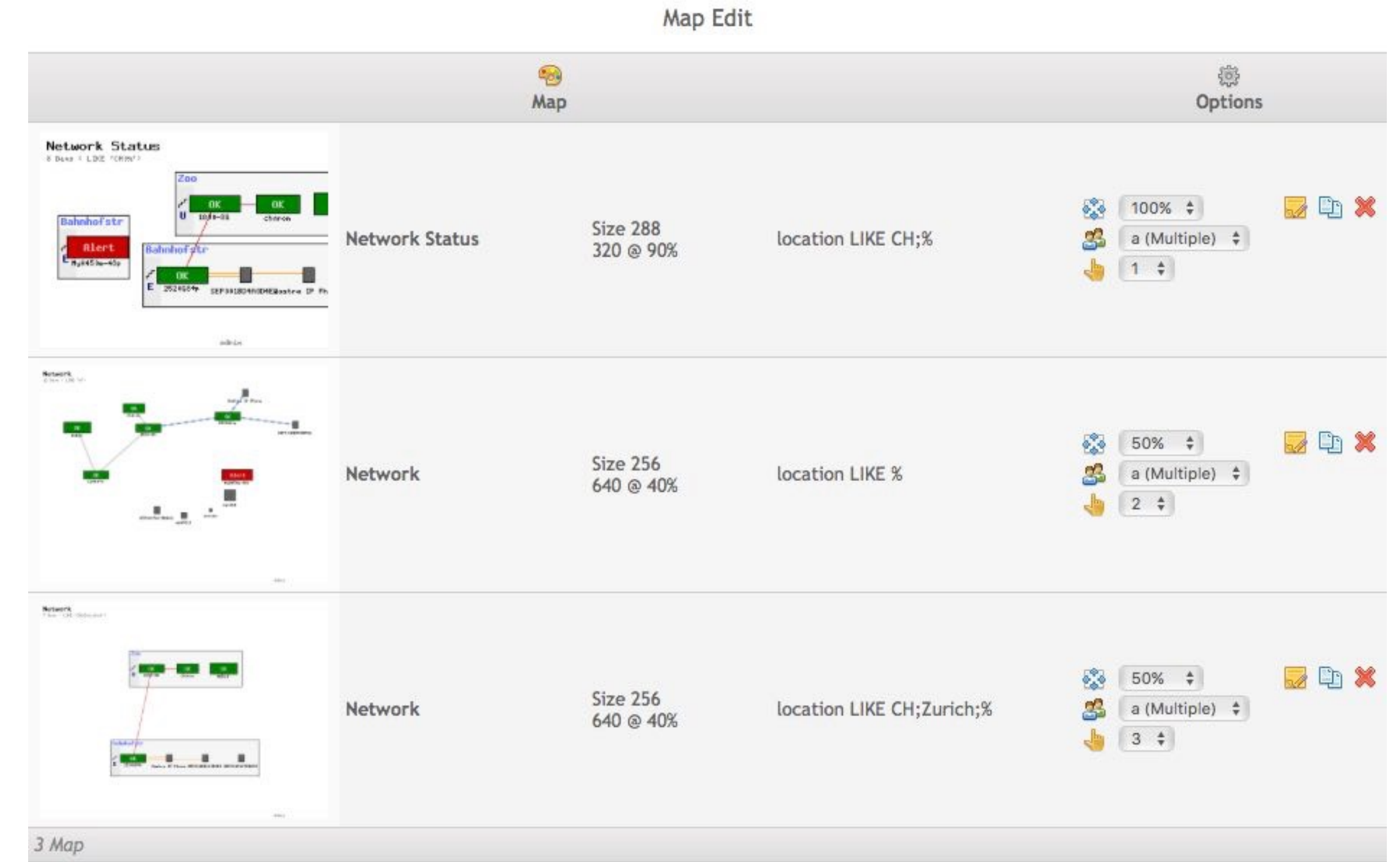
# MONITORING



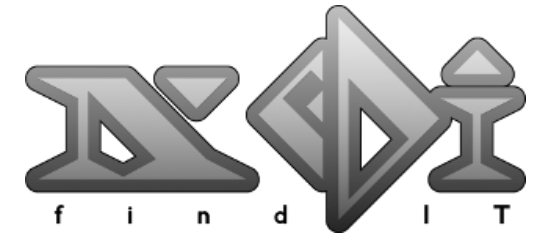
## MONITORING MAP



## EDITOR



# REPORTS IN MONITORING MAP



## Monitor Map

**Monitor**

1  
20  
12ms

**Discover**

12  
14  
60

**Last Events**

a 146

### Last Traffic Inbound

Devices	Interfaces	Traffic
ChB-priv	18 100M	101%
sw01-ab	22 1G	101%
sw01-ab	19 1G	101%
sw01-ab	21 1G	101%
sw01-ab	20 1G	51.7%

5 Interfaces, Sort: Traffic / Speed

### Last Traffic Outbound

Devices	Interfaces	Traffic
ChB-priv	3 100M	101%
sw01-ab	20 1G	101%
ChB-priv	26 1G LLDP:chb-homeoffice	101%
sw01-ab	12 1G LLDP:IP232	101%
sw01-ab	4 1G	101%

5 Interfaces, Sort: Traffic / Speed

### Last Bcast Inbound

Devices	Interfaces	Bcast
HP-2530-8G-PoEP	10 1G LLDP:sw-2-2-wdh	7.4/s 7k
virtual1	vmnic1 1G 03:00.1	5/s 4k
sw-1-2-wdh	12 100M	10.1/s 45
sw-2-2-wdh	23 1G LLDP:sw-2-1-wdh	6.7/s 6k
sw-1-3-wdh	A2 10G LLDP:sw-1-1-wdh	6.6/s 6k

5 Interfaces, Sort: Bcast / Traffic

### Total Bcast Inbound

Devices	Interfaces	Bcast
sonicwall-cb	X2:V13 1G	1
sw-1-1-wdh	19 1G	3
sw-1-1-wdh	10 1G	4k
sonicwall-cb	X2:V1001 1G	2
sw-2-1-wdh	24 1G LLDP:sw-2-2-wdh	22M

5 Interfaces, Sort: Bcast / Traffic

### Last Errors Inbound

Devices	Interfaces	Errors
sw01-ab	3 1G	23.8/s 21k
sw01-ab	14 1G	10/s 3
sw01-ab	6 1G LLDP:ap-AB_1	10.2/s 139
sw01-ab	7 1G	10/s 5

4 Interfaces, Sort: Errors / Traffic

### Last Errors Outbound

No

### Last Discard Inbound

Devices	Interfaces	Discard
VoIP-31-Se	1	303.2/s 273k
Clavi..._AB	net..._VPN IPsec tunnel:	10/s 2

2 Interfaces, Sort: Discard / Traffic







### Last Discard Outbound

Devices	Interfaces	Discard
sw01-ab	3 1G	13/s 12k

1 Interfaces, Sort: Discard / Traffic

# OPTICAL MONITORING

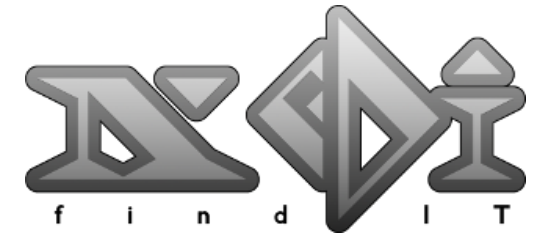
 Module

		 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
<i>225 Module Total</i>		

## 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



[Devices](#)
[Assets](#)
[Topology](#)
[Nodes](#)
[Reports](#)

## Network Reports

IP Address:

IP Address

10.10.10.0/24

7

27

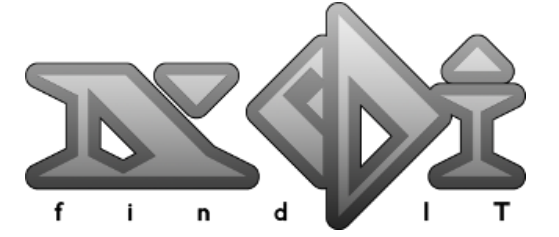
1 Network, Sort: IP Address

Reports-Networks

**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
				10.1.254	508
				10.2.254	762
				10.3.254	1016
				10.4.254	1270
				10.5.254	1524
				10.6.254	1778
				10.7.254	2032
				10.8.254	2286
				10.9.254	2540
				10.10.254	2794
				10.11.254	3048
				10.12.254	3302
				10.13.254	3556
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



hp SDN Controller Console 1332 sdn

Tasks & Activities

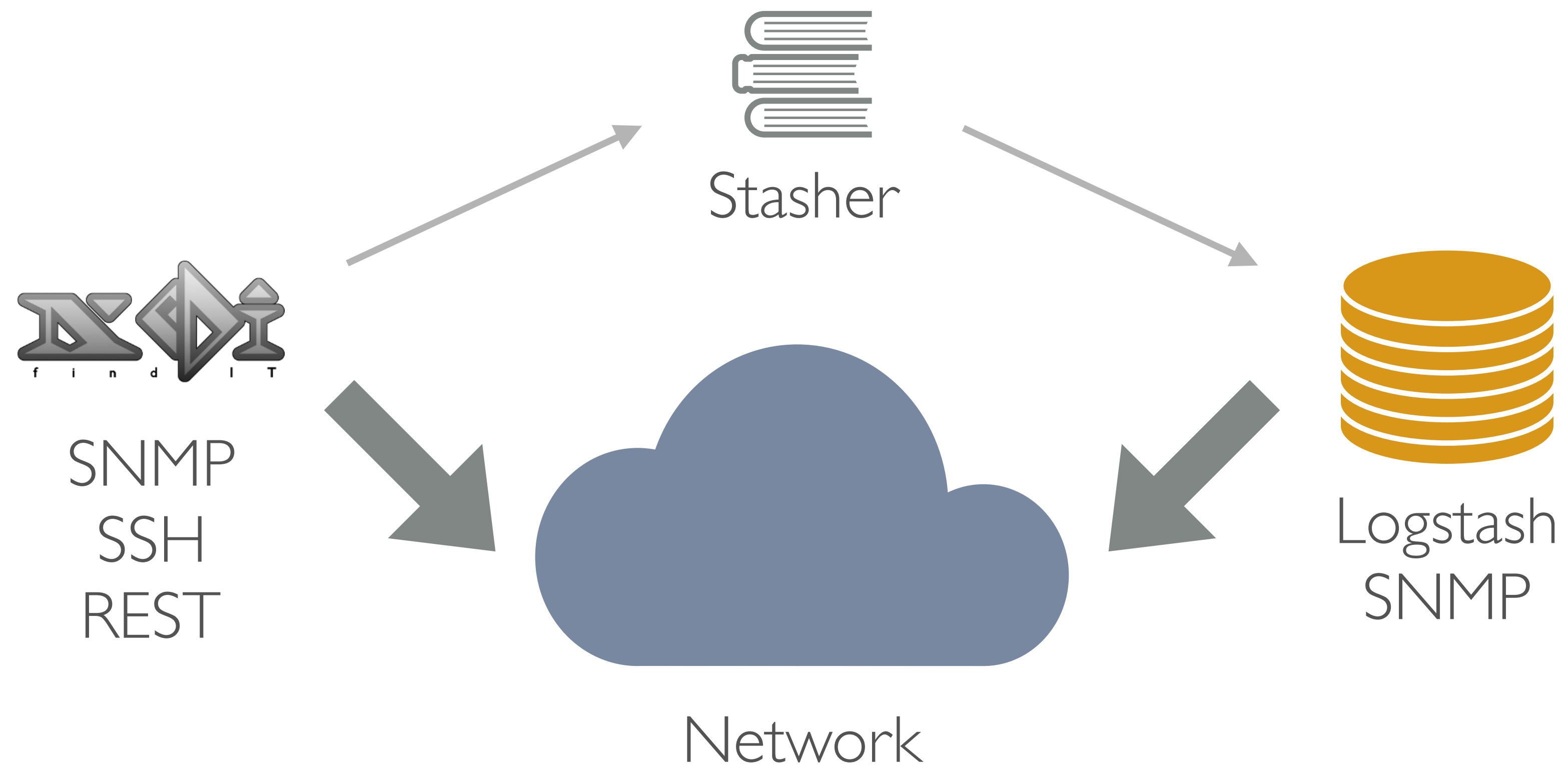
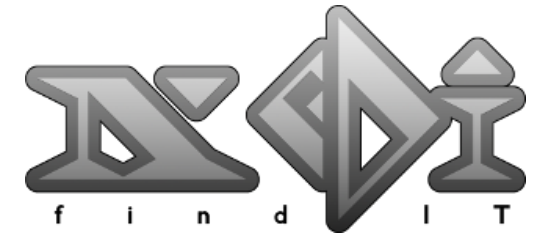
- Monitor Alerts
- Manage Modules
- View Audit Log
- View Network
- Export Logs**
- Diagnose Network

Topology Viewer

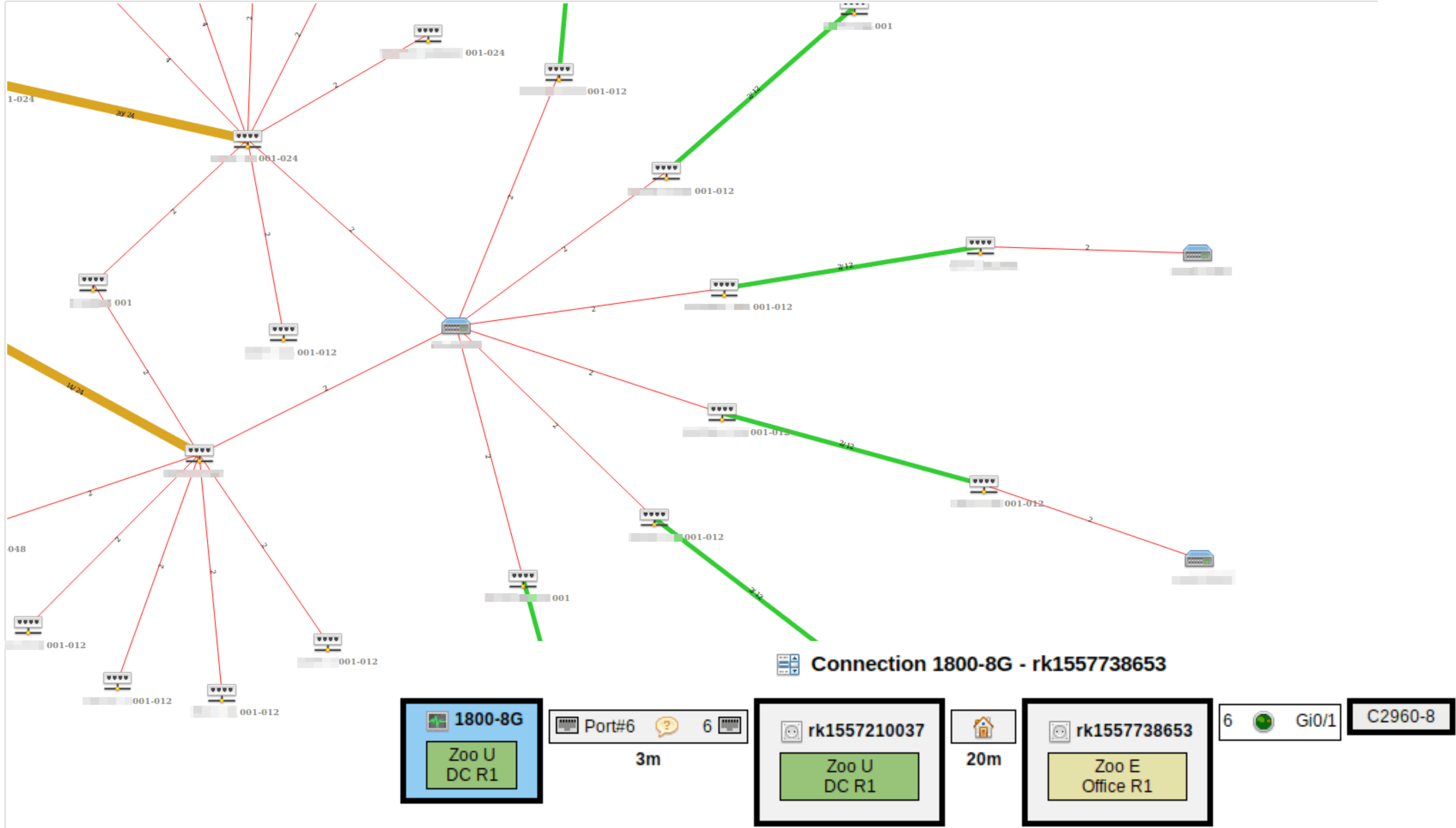
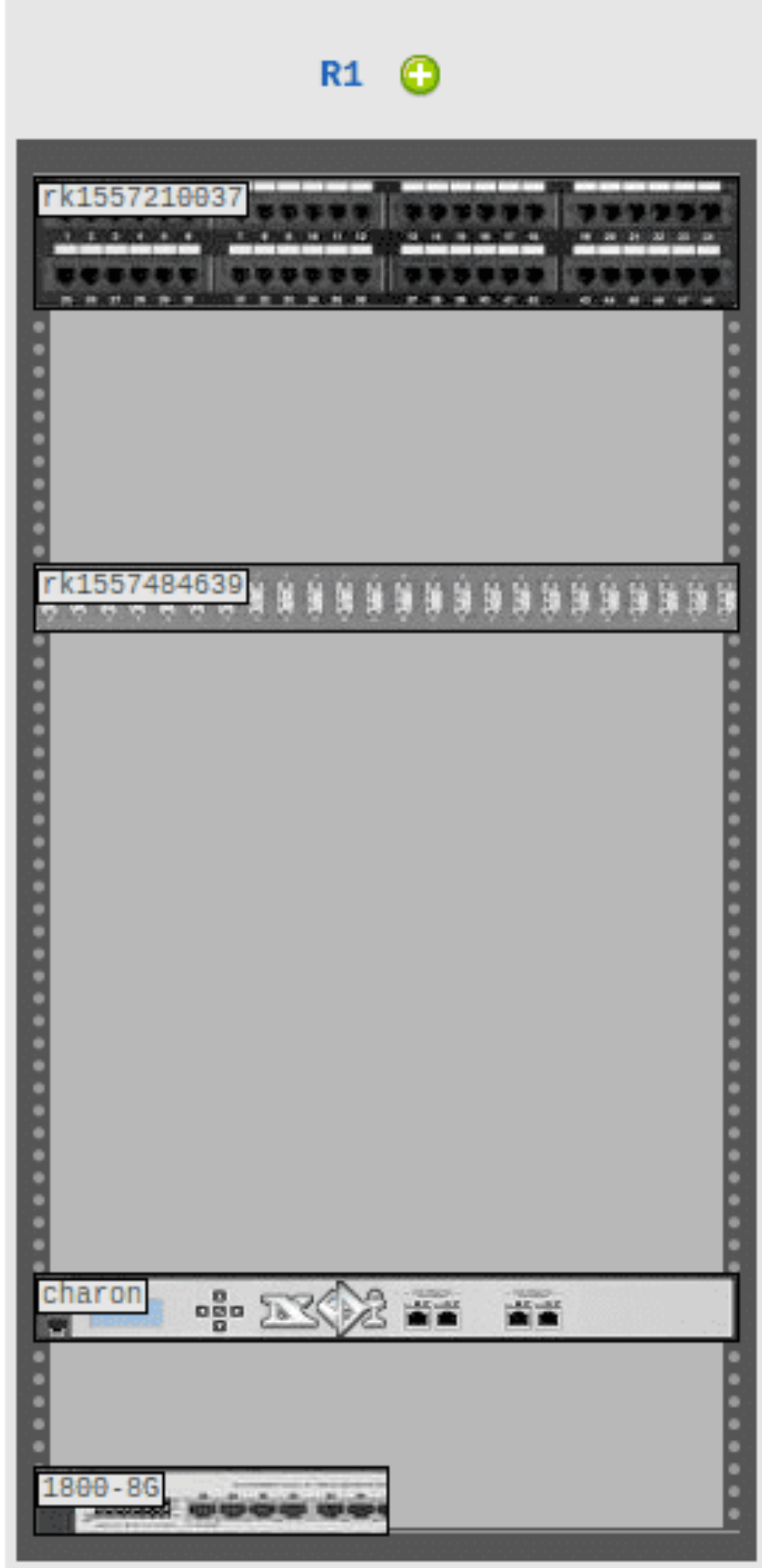
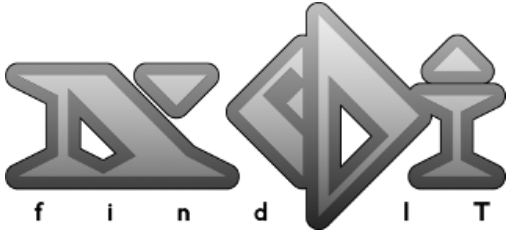
Shortest Path Follow Flow Search Ports Pin All Details IP MAC Collapsed >> << Reset

The diagram shows a network topology with nodes and their connections. Nodes are represented by yellow boxes with IP addresses and blue boxes with MAC addresses. Connections are shown as lines with numbers indicating the link ID. A red path is highlighted, starting from node 10.0.0.2 (MAC 00:00:00:00:00:02) and ending at node 10.0.0.4 (MAC 00:00:00:00:00:08). The path includes nodes 10.0.0.1, 10.0.0.3, 10.0.0.7, and 10.0.0.4. Other nodes include 10.0.0.5, 10.0.0.3, 10.0.0.6, 10.0.0.7, 10.0.0.1, 10.0.0.2, and 10.0.0.8.

# NEDI 2 LOGSTASH



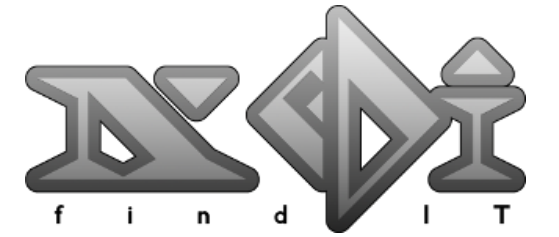
# CABLE MANAGEMENT



2 Connection, Length 23m, Level:Cat 5e

# 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!**