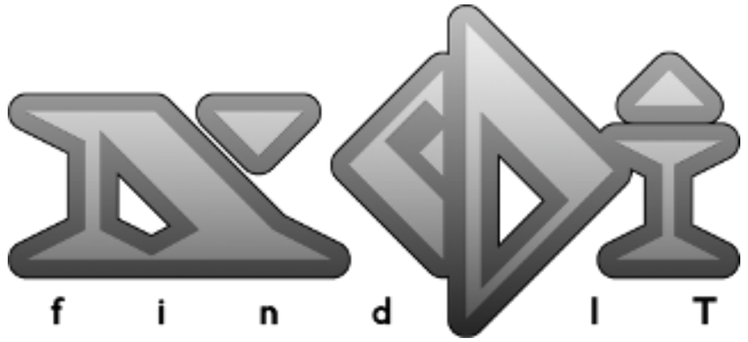


Traffic Analysis

www.nedi.ch

ABOUT ME

SECTOR NORD AG
OpenSource based enterprise solutions

5 years 7 months

08/2008 - ~~present~~ 4.2014
HP Networking Ambassador
Hewlett Packard
www.hp.com

7 years 3 months

05/2001 - 07/2008
Network & Security Engineer
Paul Scherrer Institute
www.psi.ch

1 year 1 month

04/2000 - 04/2001
Security Engineer
UBS
www.ubs.com

2 years 1 month

12/1997 - 12/1999
Rollout Project Manager
Perot Systems
www.dell.com

3 years 1 month

12/1994 - 12/1997
Network Engineer
SBC (UBS)
www.ubs.com

HP MASE - Network Infrastructure
HP ASE - Network Management
HP ASE - Mobility

Invented NeDi

Connecting UBS Investment Bank to the internet

Lived in Florida for 2 years

Bachelor (HTL) Communications Technology

ABOUT NEDI

SECTOR NORD AG
OpenSource based enterprise solutions

- Network Discovery, management & monitoring
- Locate & Track Computers
- Security audits & more
- VM, DC management
- Printer management
- Backup Configs
- IT Inventory
- IT Reports





WHAT DOES IT LOOK LIKE?

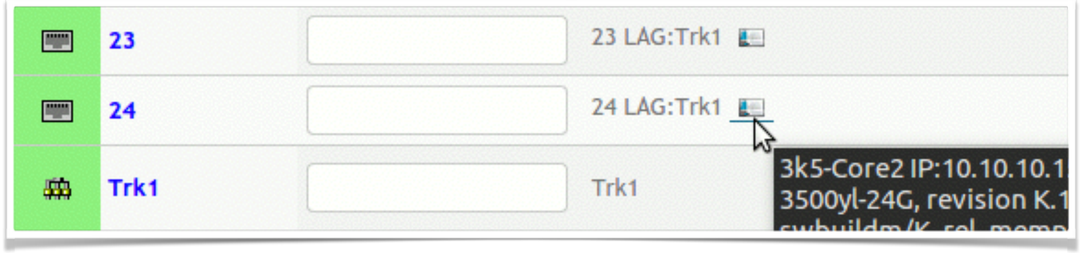
DISCOVERING THE NETWORK

SECTOR NORD AG
OpenSource based enterprise solutions

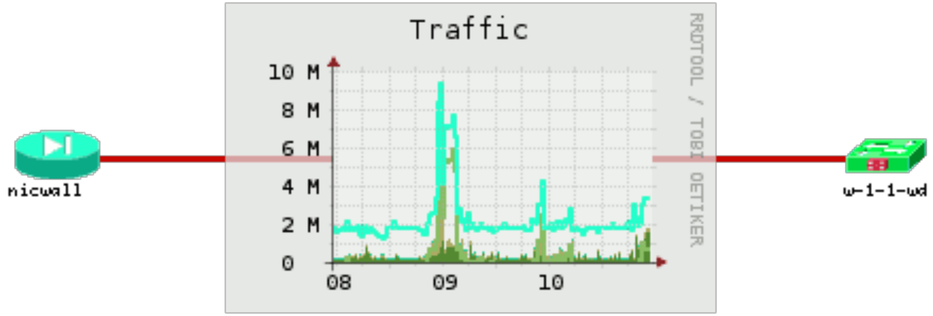
Module Status

Port Status per Fabric Extender

LAG Ports



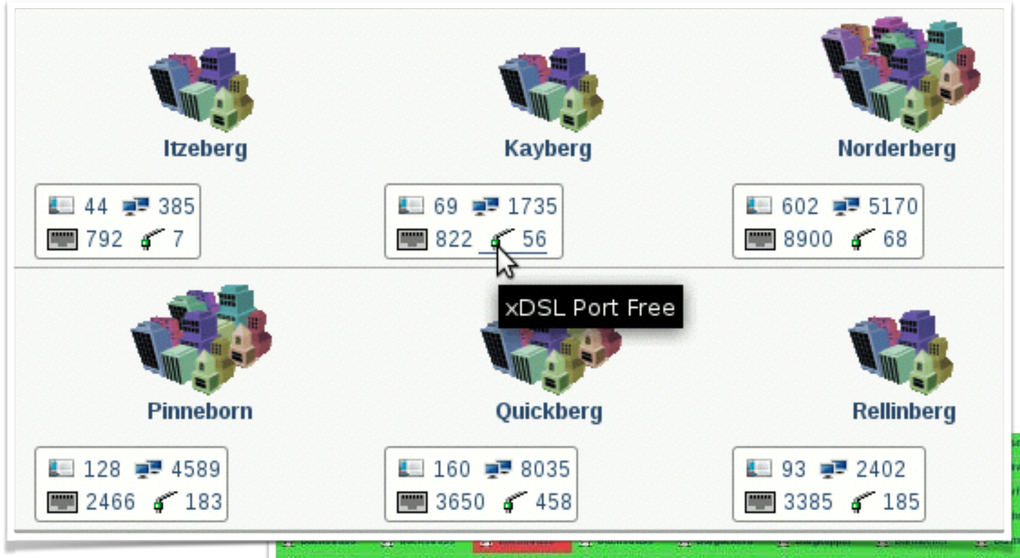
Dynamic Maps

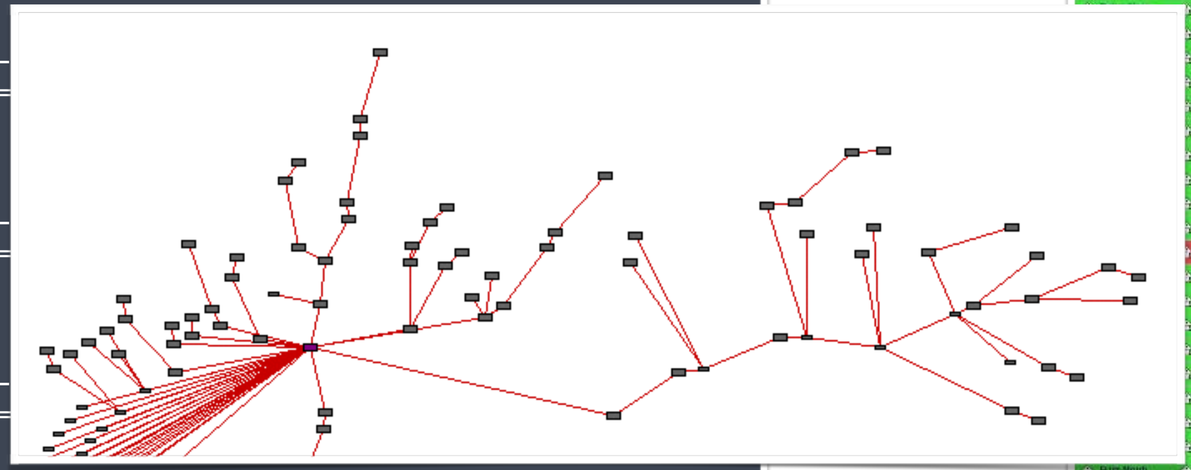


LARGE SCALE

SECTOR NORD AG
OpenSource based enterprise solutions

```
==> /opt/nedi/log/nedi-1.run <==
======================================================================
1055 devices, retire:
END :Took 59 minutes

==> /opt/nedi/log/nedi-2.run <==
======================================================================
1637 devices, retire:
END :Took 99 minutes

==> /opt/nedi/log/nedi-3.run <==
======================================================================
1789 devices, retire:
END :Took 65 minutes

==> /opt/nedi/log/nedi-4.run <==
======================================================================
2107 devices, retire: 54 nod, 5042 nbr, 13745 iftrack, 0 iptrack
END :Took 109 minutes

==> /opt/nedi/log/nedi-
======================
1917 devices, retire:
END :Took 98 minutes

==> /opt/nedi/log/nedi-
======================
856 devices, retire:
END :Took 74 minutes

==> /opt/nedi/log/nedi-
======================
304 devices, retire:
END :Took 10 minutes
```

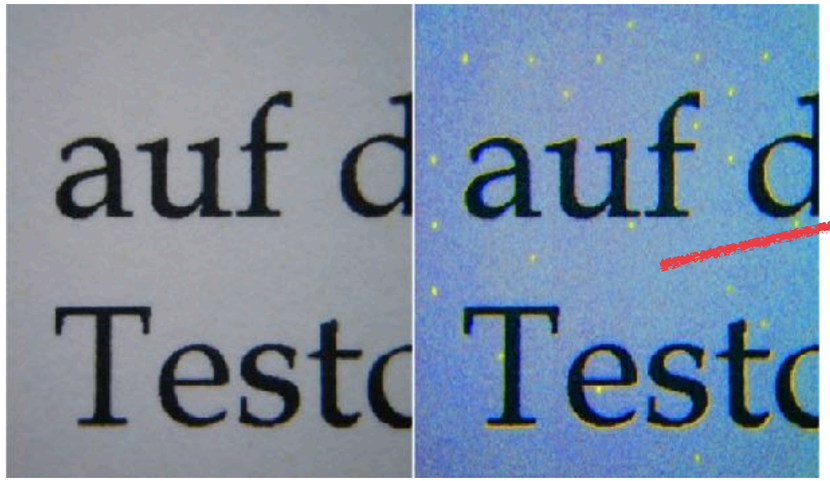




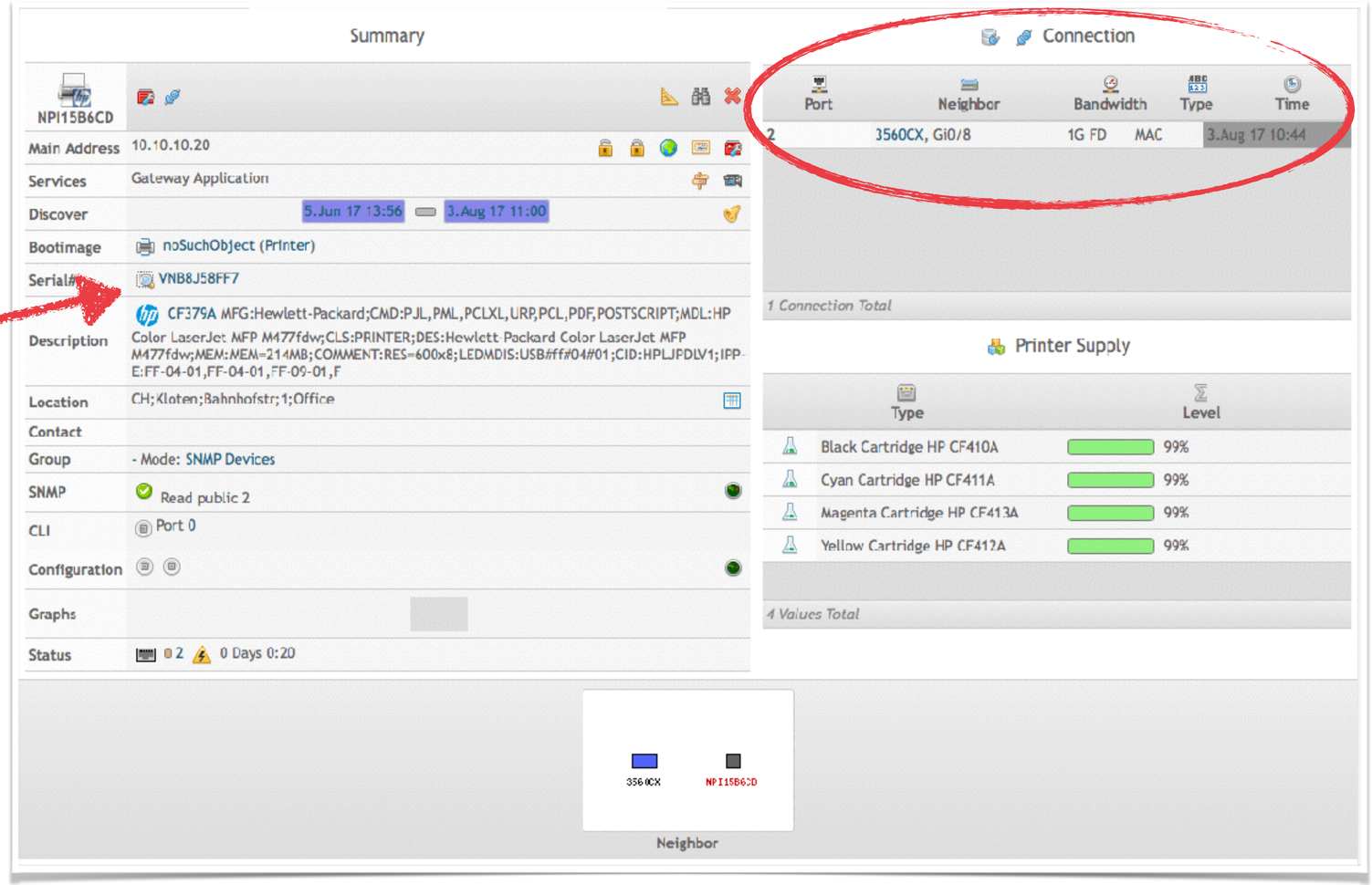
INFORMATION LEAK

SECTOR NORD AG
OpenSource based enterprise solutions

FOLLOW THE MICRO DOTS!



From Wikimedia Commons, the free media repository



TRAFFIC SUMMARY

SECTORNORD AG
OpenSource based enterprise solutions

Protocol	Distribution
TCP	94.9 %
UDP	5.0 %
ICMP	0.1 %
ICMP6	0.0 %
	0.0 %

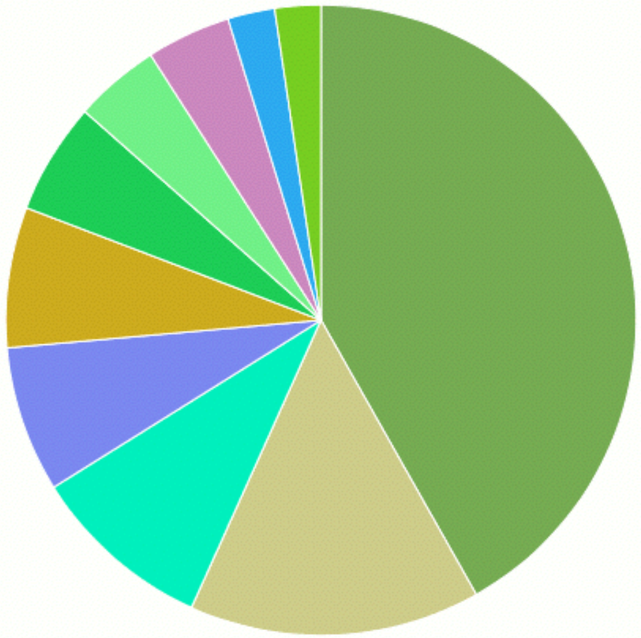
Port	Distribution
80 http	94.5 %
443 https	2.0 %
5060 sip	1.3 %
9001	0.5 %
5353 mdns	0.4 %

Source	Distribution
Remus.home	8.2 %
osiris.home	4.8 %
AKAMAI-PA	3.3 %
10.10.10.1	1.3 %
Apple-TV.home	1.2 %

Destination	Distribution
osiris.home	88.9 %
Remus.home	3.8 %
Apple-TV.home	3.7 %
Andreas-iPad.home	1.5 %
AKAMAI-PA	0.6 %

TRAFFIC VISUALIZATION...

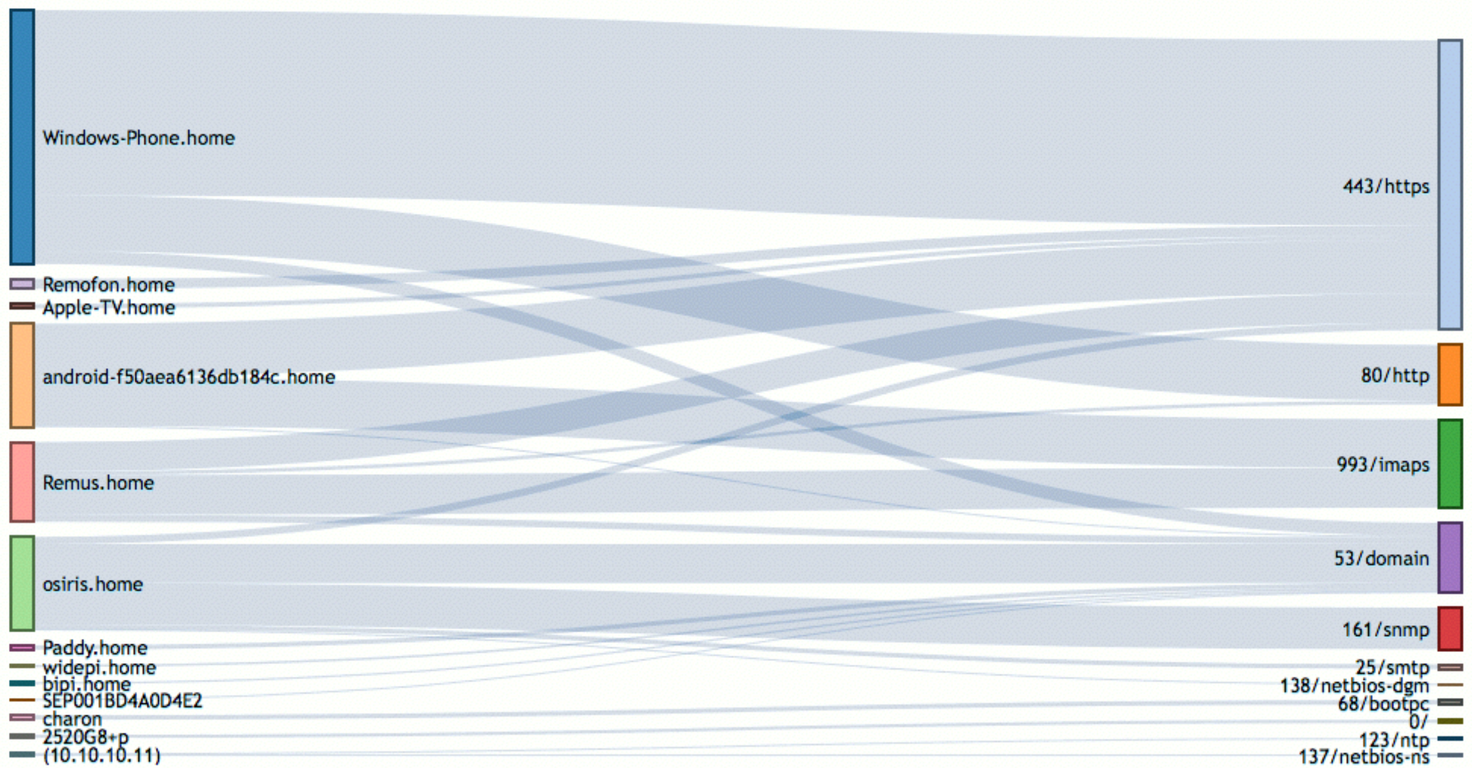
SECTORNORD AG
OpenSource based enterprise solutions



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

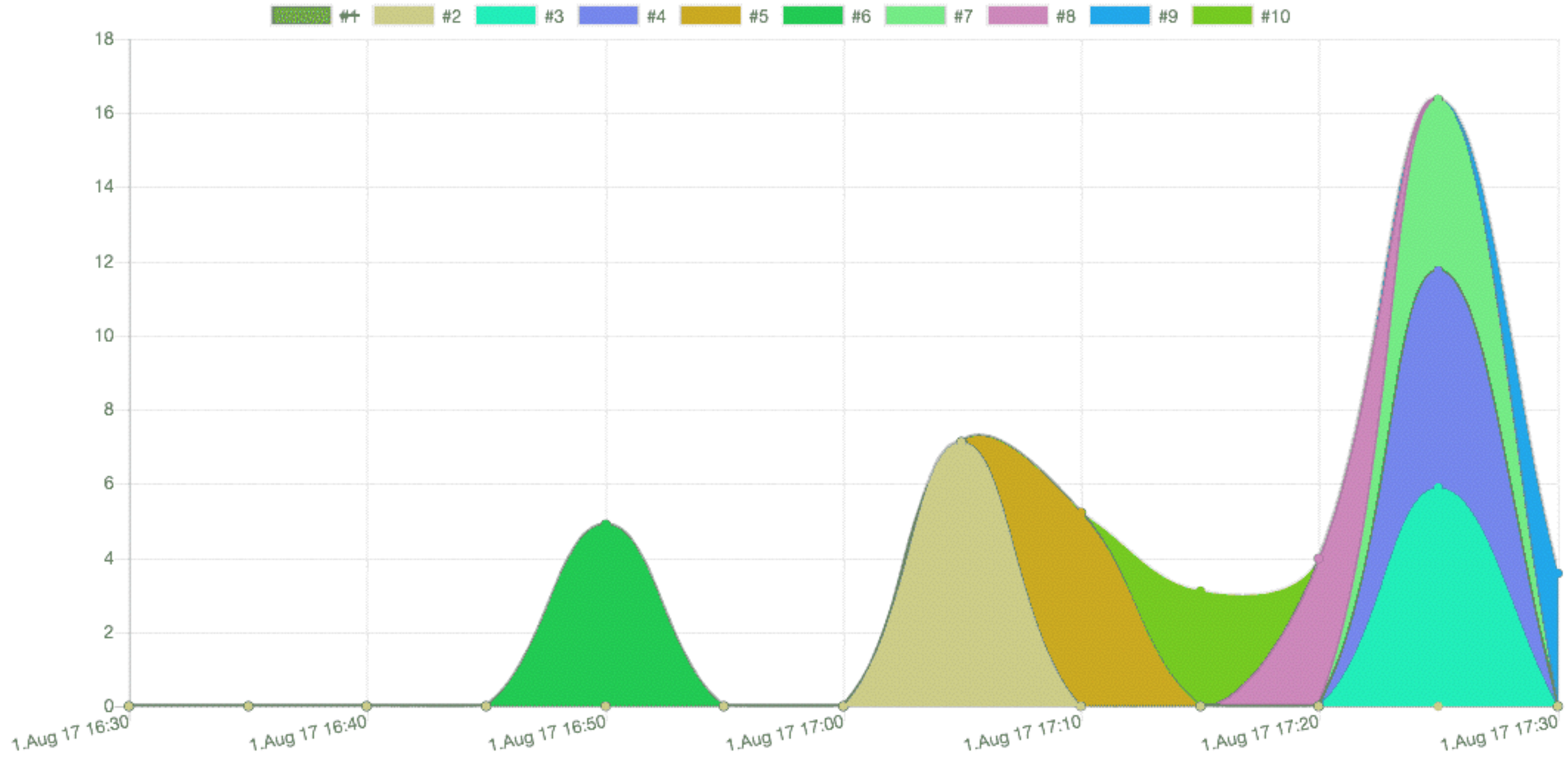


Source Address, Destination Port Summary

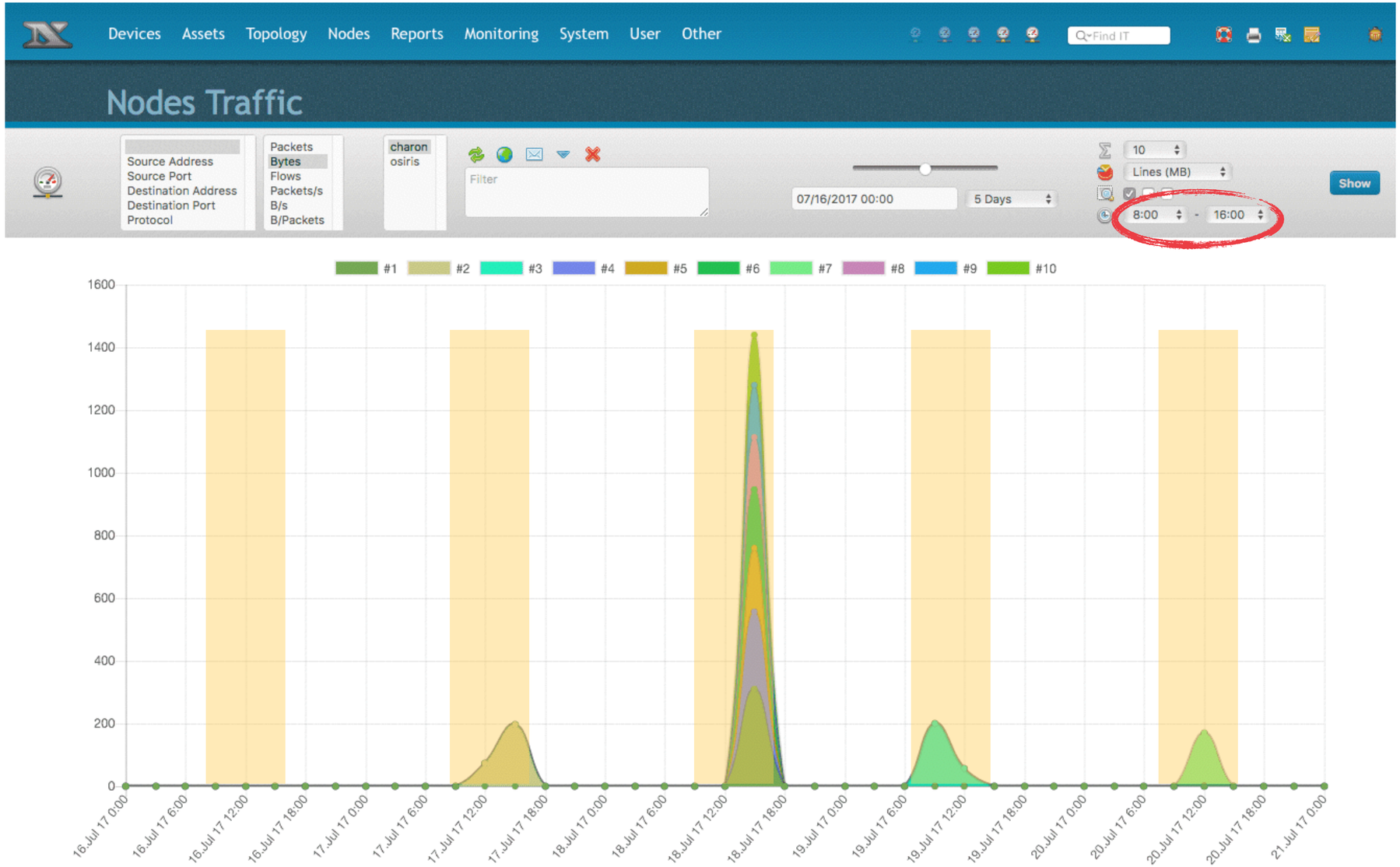
26.Jul 16 16:35 - 26.Jul 16 16:45, Filter: dst port < 1024

INTERACTIVE CHARTS (1.8)

SECTOR NORD AG
OpenSource based enterprise solutions



SKIP BACKUP TRAFFIC



NETFLOW & SFLOW

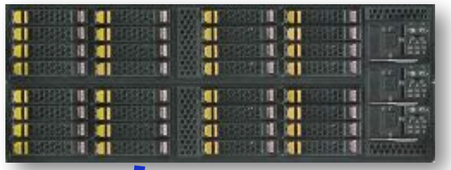
SECTORNORD AG
OpenSource based enterprise solutions

Device

Collector

UI

Netflow/Sflow



Viewable Data

LATENCY ANALYSIS

SECTORNORD AG
OpenSource based enterprise solutions

–

Nodes Traffic

Summary

23.Nov 16 16:50 - 23.Nov 16 16:55

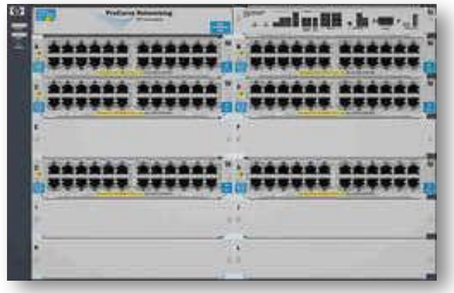
Source Address	Source Port	Destination Address	Destination Port	Protocol	Packets	Bytes	Flows	Packets/s	B/s	B/Packets	Client Latency	Server Latency	App Latency
osiris	3000/	10.10.10.109	49863/	tcp	128k	187M	2	426	5M	1k	96.987 ms	3.133 ms	2.243 ms
10.10.10.109	65295/	osiris	445/microsoft-ds	tcp	11k	2M	2	38	58k	187	1.963 ms	0.465 ms	2508.337 ms
osiris	38720/	C2960-8	23/telnet	tcp	50	1k	2	203	36k	22	0.026 ms	1.270 ms	2.212 ms
10.10.10.101	36201/	osiris	445/microsoft-ds	tcp	42	28k	2		816	666	1.347 ms	0.066 ms	0.833 ms
osiris	51275/	2520G8-P	161/snmp	udp	19	1k	2	59	25k	52	-	-	-
osiris	53193/	2520G8-P	161/snmp	udp	18	1k	2	253	117k	57	-	-	-
osiris	59811/	C2960-8	161/snmp	udp	18	951	2	94	40k	52	-	-	-
osiris	5060/sip	212.117.203.32	5060/sip	udp	16	10k	2		267	596	-	-	-
osiris	50597/	charon	161/snmp	udp	16	842	2	355	150k	52	-	-	-
osiris	36130/	C2960-8	161/snmp	udp	16	880	2	175	77k	55	-	-	-

10 Values, Sort: Packets, Limit: 10

admin, 1479919321

ENDPOINT CLASSIFICATION

Source Address	Source Port	Destination Address
osiris	3000/	10.10.10.109
10.10.10.109	65295/	osiris
osiris	38720/	C2960-8
10.10.10.101	36201/	osiris
osiris	51275/	2520G8-P
osiris	53193/	2520G8-P
osiris	59811/	C2960-8
osiris	5060/sip	212.117.203.32
osiris	50597/	charon
osiris	36130/	C2960-8



TRAFFIC DETAILS

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

SECTORNORD AG
OpenSource based enterprise solutions

TRAFFIC POLICIES

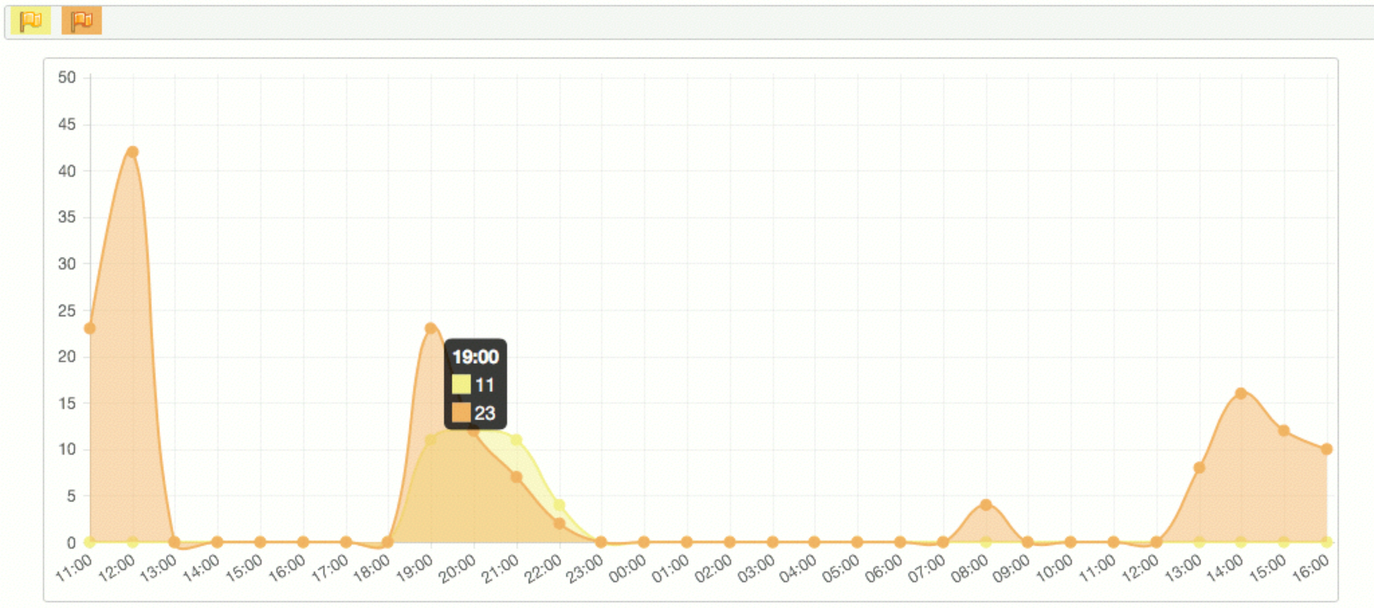
Id	Status	Class	Target	Device	Port	Vlan	Action	Information	User	Time	Execute
19		Bytes	> 500000	Source:charon Filter:src host 10.10.10.109 Group:sa,da					admin	31.Mar 16 12:45	
15		Bytes	< 100	Source:charon Filter:src host 10.10.10.10 and port 5060 Group:sa				SIP underrun	admin	28.Mar 16 16:02	
17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



PORT CONFIG POLICIES (1.8)

SECTORNORD AG
OpenSource based enterprise solutions

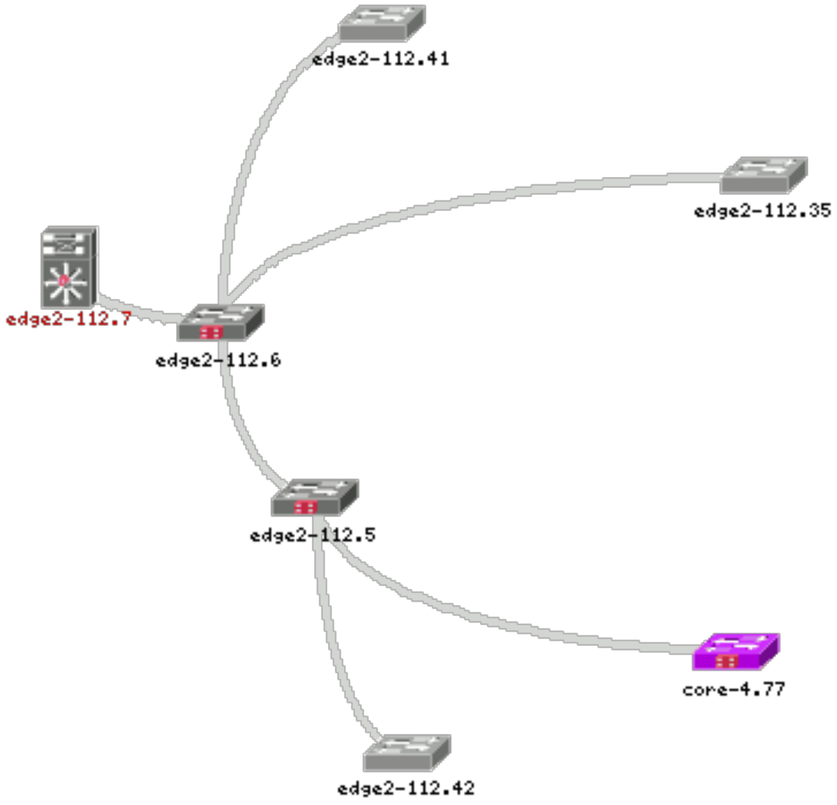
Id	Status	Class	Target	Devices	Port	Vlan	Action	Information	User	Time	Execute
1		Configuration	community public						admin	7.Feb 17 15:07	
3		Configuration	contact Remo						admin	7.Feb 17 15:11	
7		Port Configuration	switchport mode trunk	2960				Tagged voice	admin	19.Jun 17 17:26	
3 Values											

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

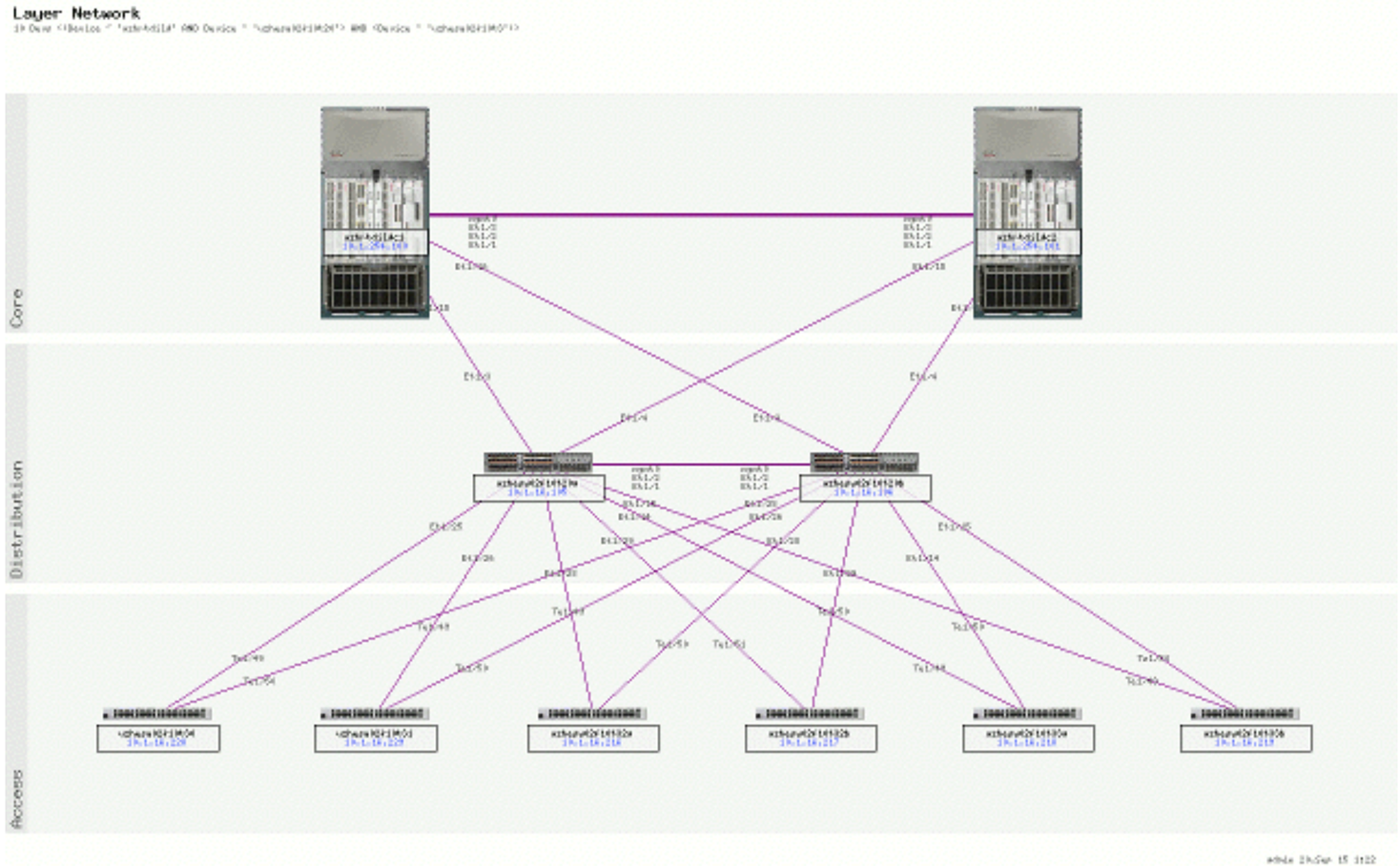
ENHANCED MAPS

SECTOR NORD AG
OpenSource based enterprise solutions

NEIGHBOUR RANGE



LAYER MAP

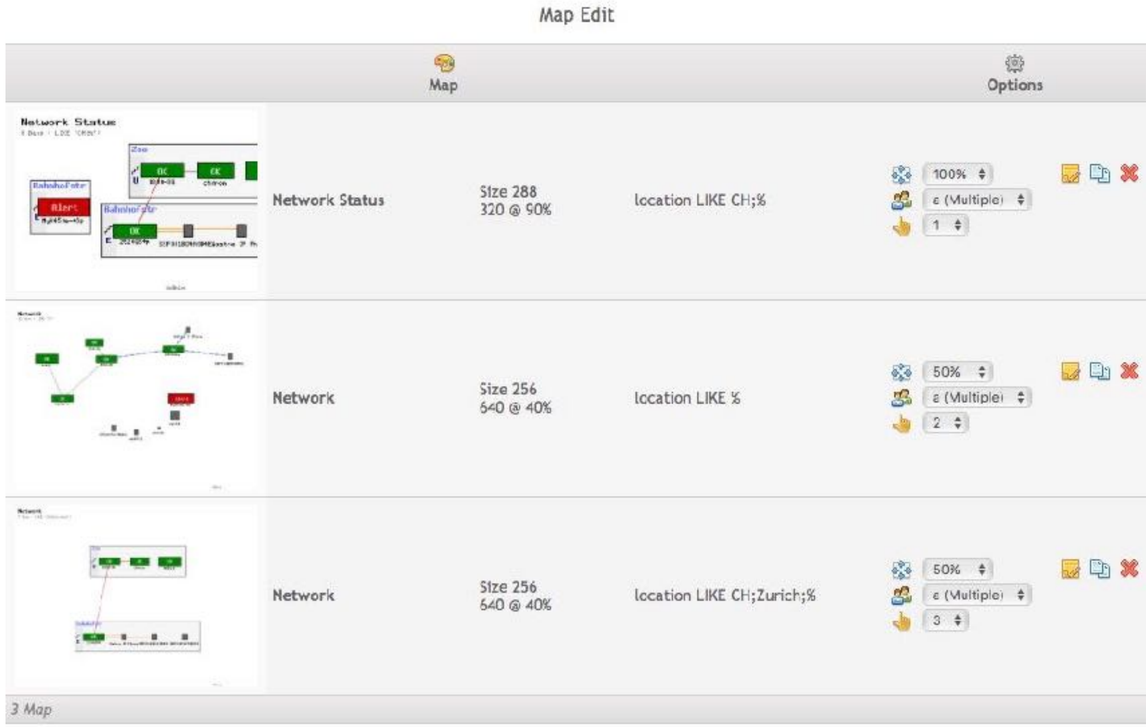


MONITORING MAPS

SECTOR NORD AG
OpenSource based enterprise solutions

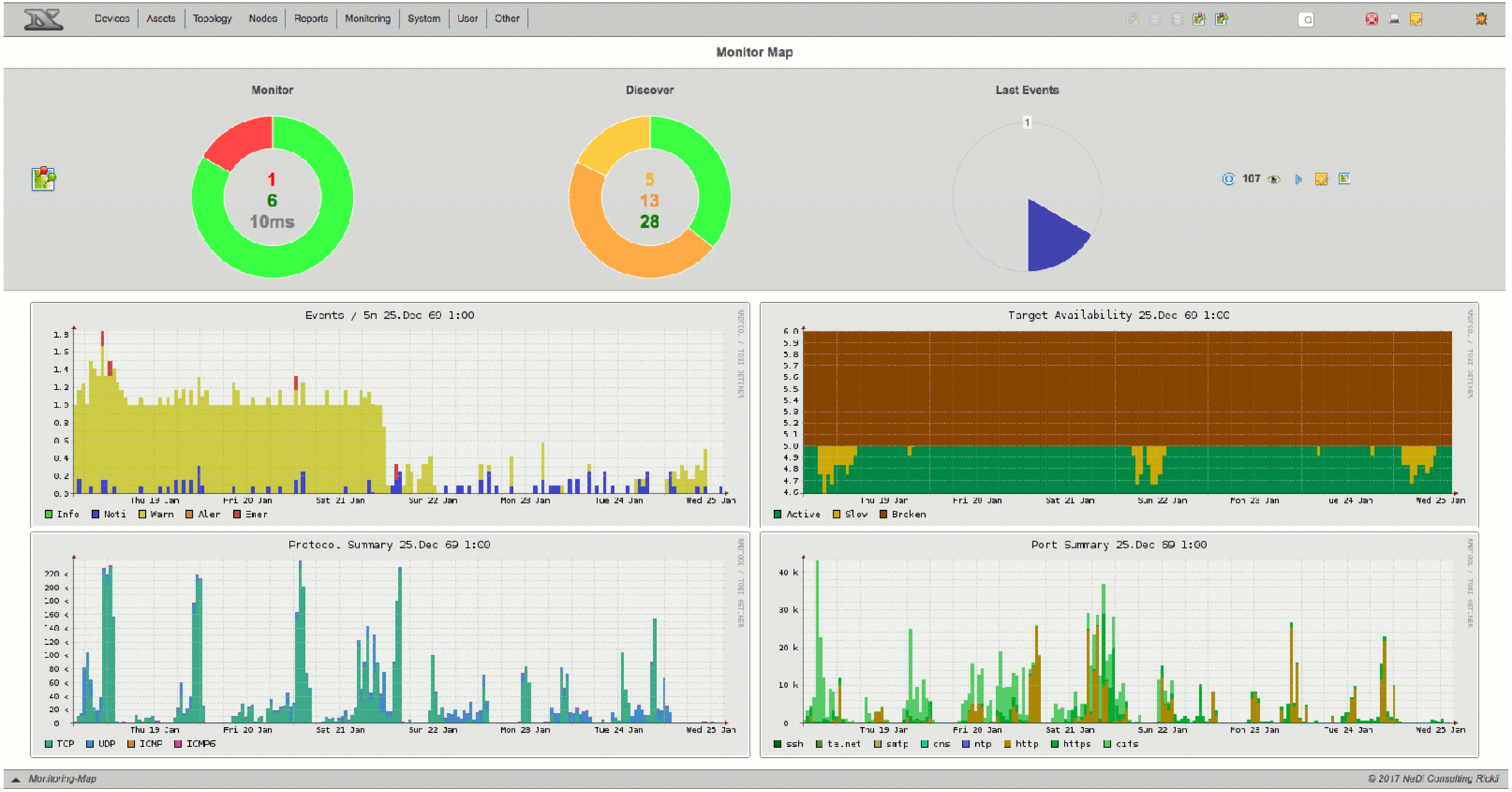
MONITORING MAP

EDITOR



MONITORING GRAPHS

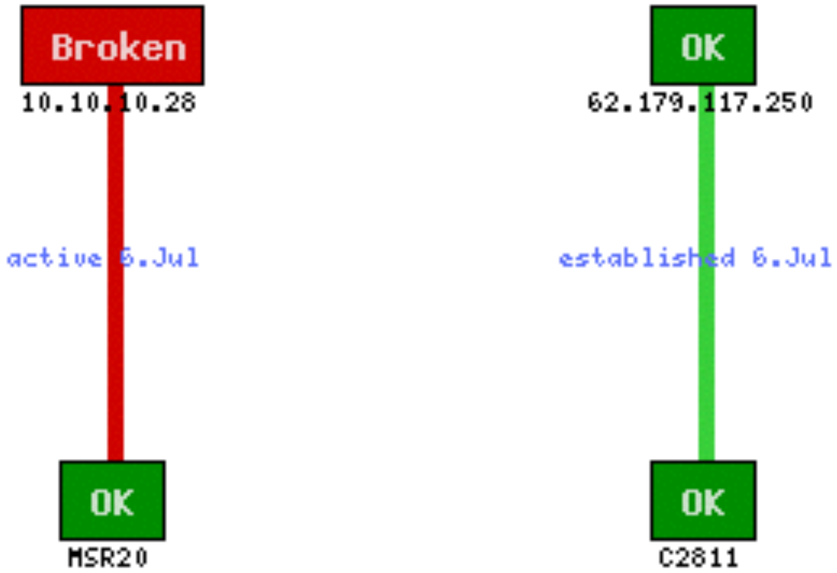
SECTOR NORD AG
OpenSource based enterprise solutions



MONITOR MORE

SECTORNORD AG
OpenSource based enterprise solutions

BGP Peers

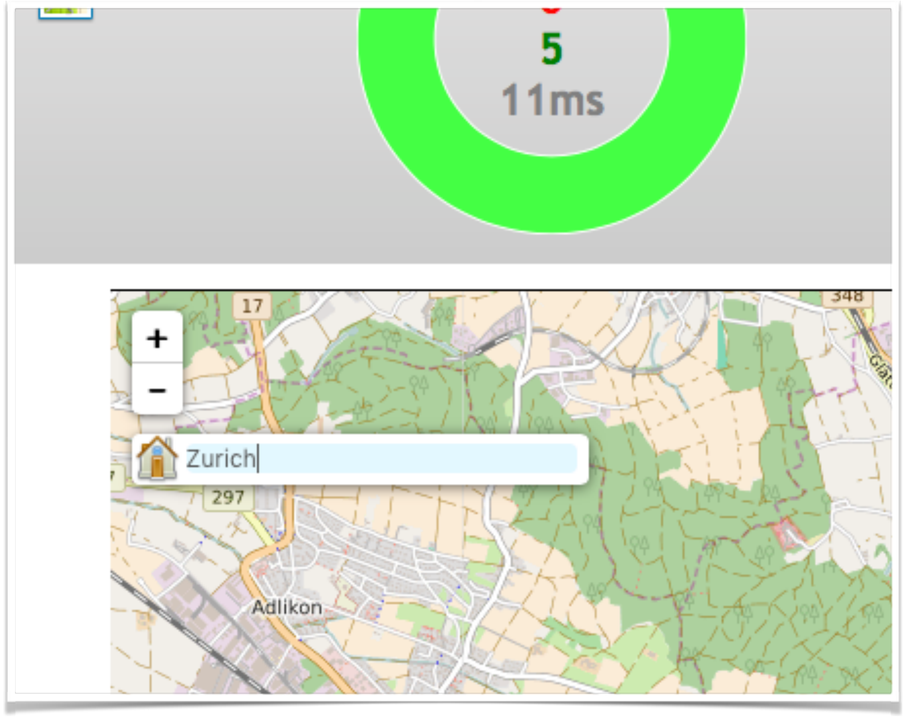


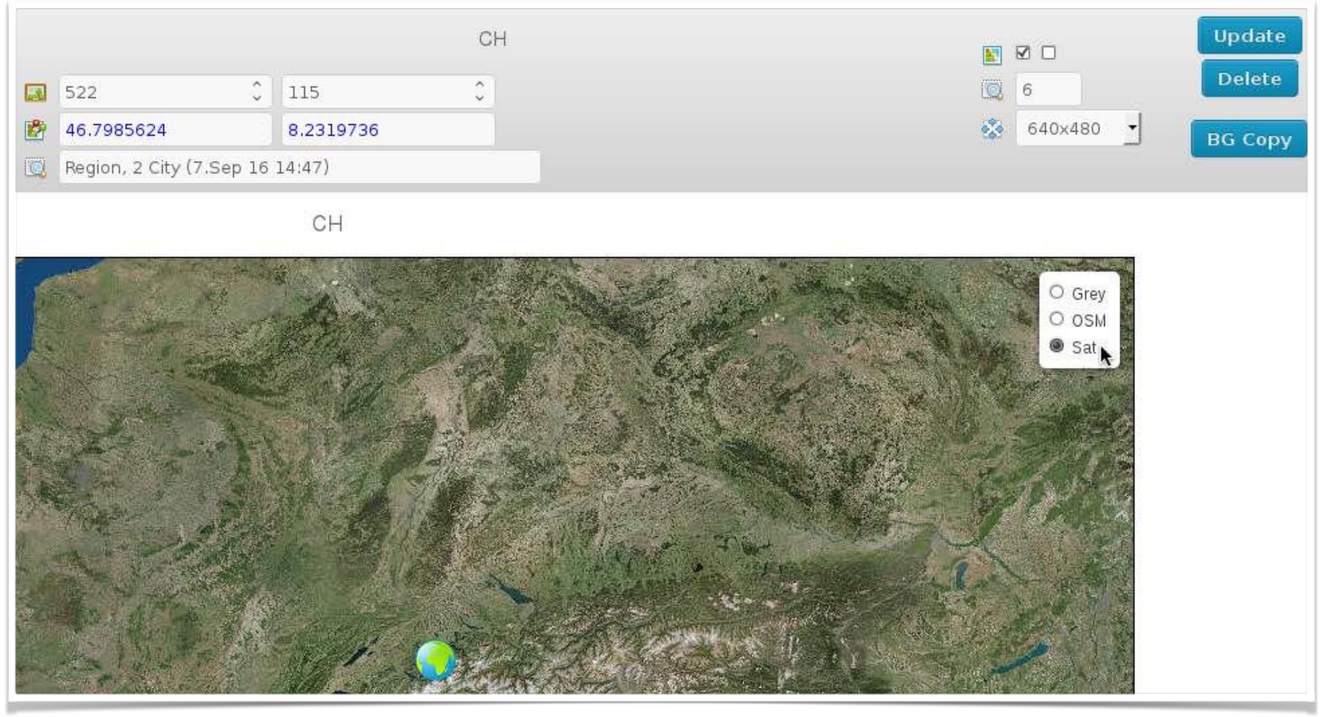
Port Status

Id	Level	Time	Source	Class	
12112		17.Jan 17 11:33	C2960-8		Fa0/1 came up
12111		17.Jan 17 11:33	C2960-8		Fa0/1 went down

MORE GEOGRAPHY

SECTOR NORD AG
OpenSource based enterprise solutions





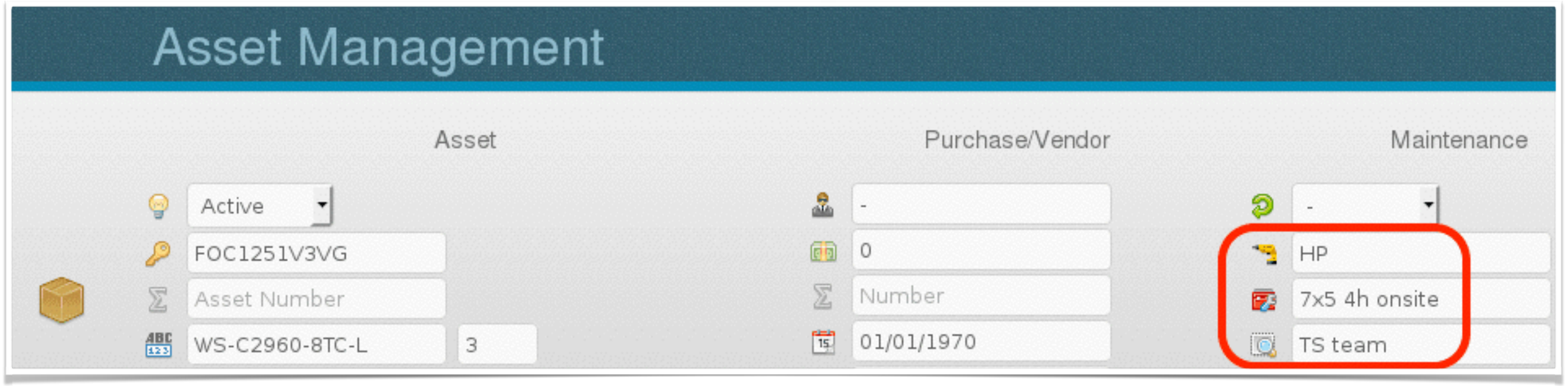
WMI DISCOVERY

SECTORNORD AG
OpenSource based enterprise solutions

Devices Name = 'ROMULUS'

Devices Name	Slot	Model	Modules Description	Serial#	HW Version	FW Version	Software
ROMULUS	CPU0		Intel(R) Core(TM) i7 CPU 950 @ 3.07GHz	BFEBFBFF000106A5	6661		
ROMULUS	DeviceHarddiskVolume1	9641452	Microsoft Windows 10 Pro	00330-80000-00000-AA493			10.0.14393
ROMULUS	DIMM0	Manufacturer00	ModulePartNumber00 (1)	SerNum00	2048 MB	1066	
ROMULUS	DIMM1	Manufacturer01	ModulePartNumber01 (1)	SerNum01	2048 MB	1066	
ROMULUS	DIMM2	Manufacturer02	ModulePartNumber02 (1)	SerNum02	2048 MB	1066	
ROMULUS	DIMM3	Manufacturer03	ModulePartNumber03 (1)	SerNum03	2048 MB	1066	
ROMULUS	DIMM4	Manufacturer04	ModulePartNumber04 (1)	SerNum04	2048 MB	1066	
ROMULUS	DIMM5	Manufacturer05	ModulePartNumber05 (1)	SerNum05	2048 MB	1066	
ROMULUS	PHYSICALDRIVE0	ST31000524AS ATA Device	Fixed hard disk media	6VPCC96T	1000202273280	JC45	
ROMULUS	UID12545_0	GSM	LG TV	16843009	0001	1-2014	
ROMULUS	{02138196-59F1-3672-9FB9-BF868075952E}	Microsoft Corporation	Microsoft Visual Studio 2015 Team Explorer Language Pack - ENU				14.0.23102
ROMULUS	{023FCA1D-E591-3AF9-9D2F-9876639A511A}	Microsoft Corporation	Visual C++ Library PGO X86 Package				14.0.24210
ROMULUS	{02F3B2F2-A9F4-4E9C-AAD6-80184A2A6273}	Microsoft Corporation	Microsoft LightSwitch for Visual Studio 2015 v5.0 ToolsRes - DEU				14.0.23025

EXTENDED ASSET HANDLING



OTHER IMPROVEMENTS

SECTORNORD AG
OpenSource based enterprise solutions

QR Labels

3k5-Core1
10.10.10.155
Remo

3k5-Core2
10.10.10.156
Remo

Population Stats

Device	Main IP	Device Type	Device Status	Total #MAC	Total #ARP	Population
1800-8G	10.10.10.6	1800-8G	0	20		2
2520G8+p	10.10.10.4	2520-8G-PoE	0	18		6
AH-367380	10.10.10.72	HiveAP	0	7		9
C1800a	10.10.10.132	cisco1812	0		4	

THANKS!