Network Administration Visualized – NAV

Валентин Будкін

- MCITP, CSPO
- IT-директор рітейлера КТС (час від часу)
- Цікавлюсь гетерогенними мережами, управлінням бізнес-процесами, Agile-підходами в управлінні

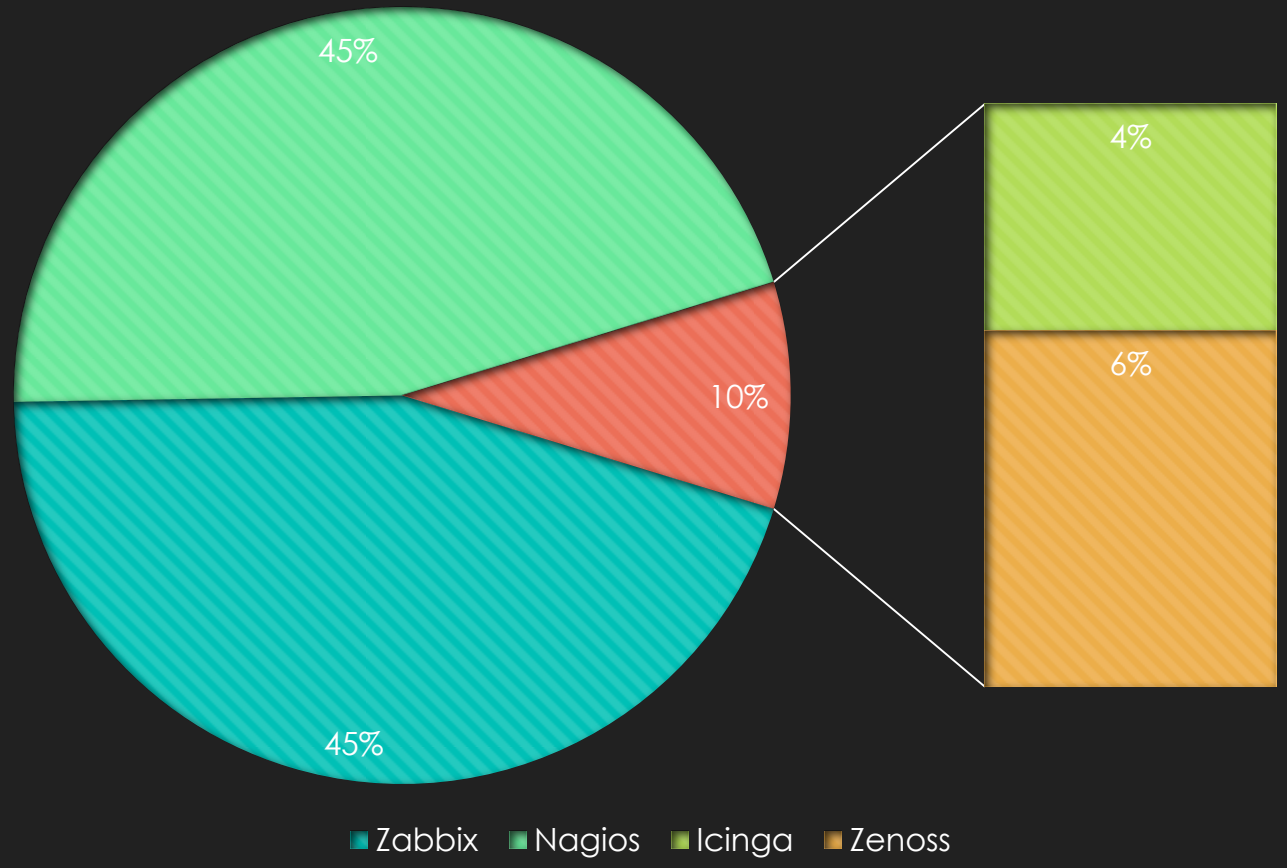
В кого встановлена і використовується система моніторінга мережі?

В кого Zabbix?

В кого Nagios?

Щось специфічне?

Google Trends



Молода динамічна компанія

- Грошей нема
- Щось придумай
- У нас тут є залізка — може є куди приткнути?

IP-відеоспостереження

Пройшло 2 роки

- 150+ камер
- 10+ локацій

- 5 разів в день доводиться перезавантажувати якусь камеру
- Відділ безпеки починає щось підозрювати

Потрібне рішення для лінивих

- Zabbix для технічної підтримки
- POE-комутатори
- Скрипт для вимкнення напруги на порту
- Замучались поки написали під кожну модель свіча
- Але потрібно знати порт в який встромили камеру ☹

NAV

https://nav.uninett.no

Хто винен

- Норвежці
- Університетські мережі
- Open source
- Python
- Django
- PostgreSQL
- Graphite

NAV Search Tools My stuff Logout admin

HOME

Status

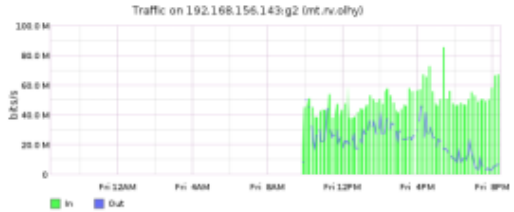
According to your criteria, everything seems ok

Go to the status page Last updated: 2016-11-11 20:23:36

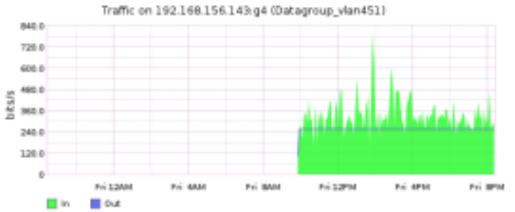
Links

Machine
Tracker
Documentation
Statistics
Reports
About NAV

Traffic on 192.168.156.143:g2 (mt.rv.olhy)



Traffic on 192.168.156.143:g4 (Datagroup_vlan451)

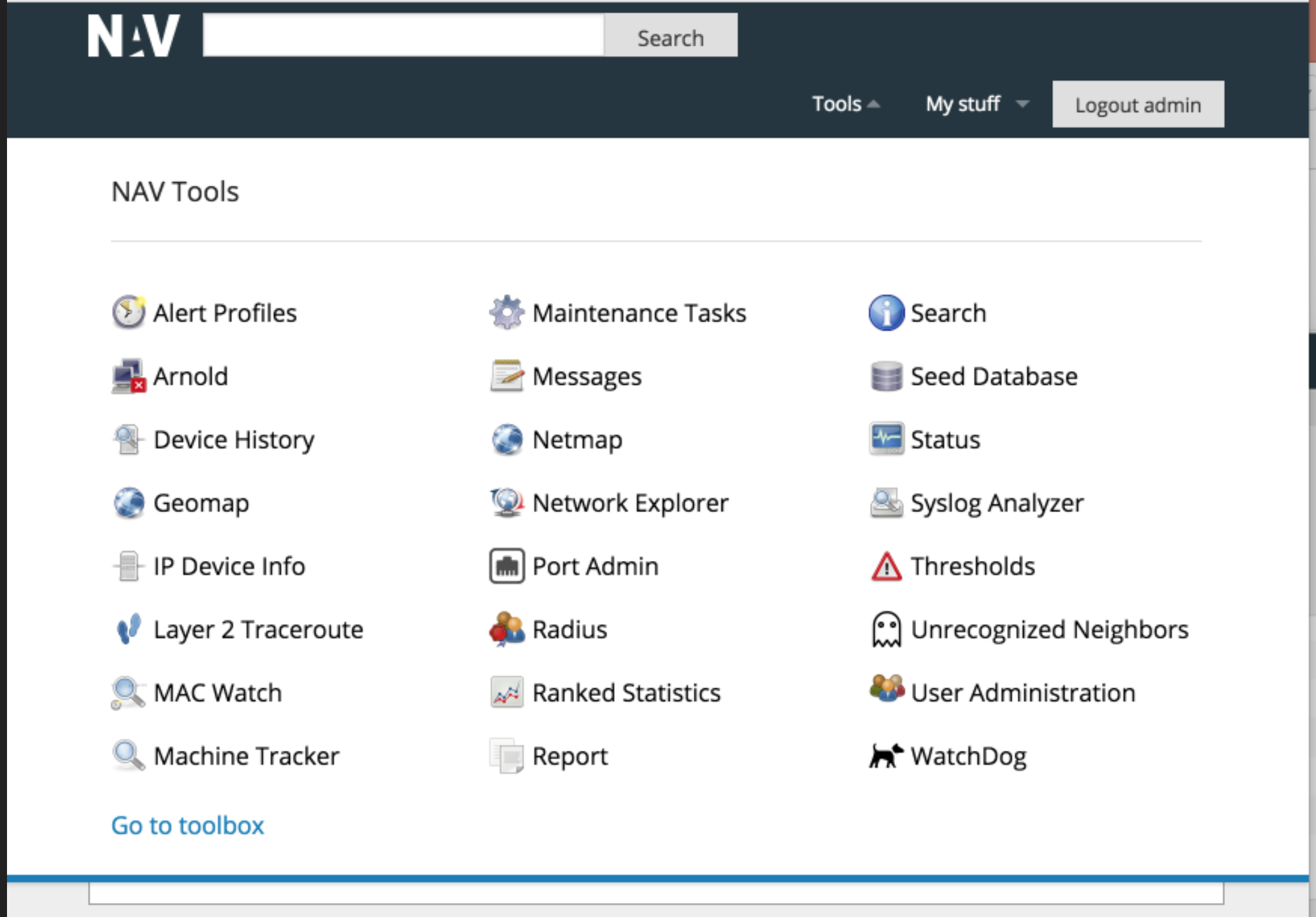


Messages

No messages

Port Admin

Search for ip device or interfa Search


NAV
Search
Tools
My stuff
Logout admin
NAV Tools
Alert Profiles
Arnold
Device History
Geomap
IP Device Info
Layer 2 Traceroute
MAC Watch
Machine Tracker
Maintenance Tasks
Messages
Netmap
Network Explorer
Port Admin
Radius
Ranked Statistics
Report
Search
Seed Database
Status
Syslog Analyzer
Thresholds
Unrecognized Neighbors
User Administration
WatchDog
Go to toolbox

Seed Database

Edit NAV seed data: Which devices and services to monitor, location/room/organization registry, cabling and patch registry.

Seed DB
IP device
Service
Room
Location
Organization
Usage
Type
Vendor
Device Group
Vlan
Prefix
Cabling
Patch

IP Devices

Add new ip device | Bulk import

Back to list

Edit 192.168.100.1

Delete this IP device

Inventory

Ip *
192.168.100.1

Room *
Server Room (Service Center)

Category *
GSW (A layer 2 and layer 3 device)

Organization *
myorg (KTC)

SNMP communities

Read only
write

Read write
write

Check connectivity

Collected info

Sysname
192.168.100.1

Snmp version
2

Type
1.3.6.1.4.1.14988.1 (RouterOS RB1000 from mikrotik)

Meta information

Function

Groups

Attributes

Key | Value

Add row

Save IP device

Geomap

Geographic network weather map, based on OpenStreetMap data.

Variant: Map with open information | Map with sensitive information

Map options

Time interval for load data

2016-11-11 19:10–19:20

Interval size:

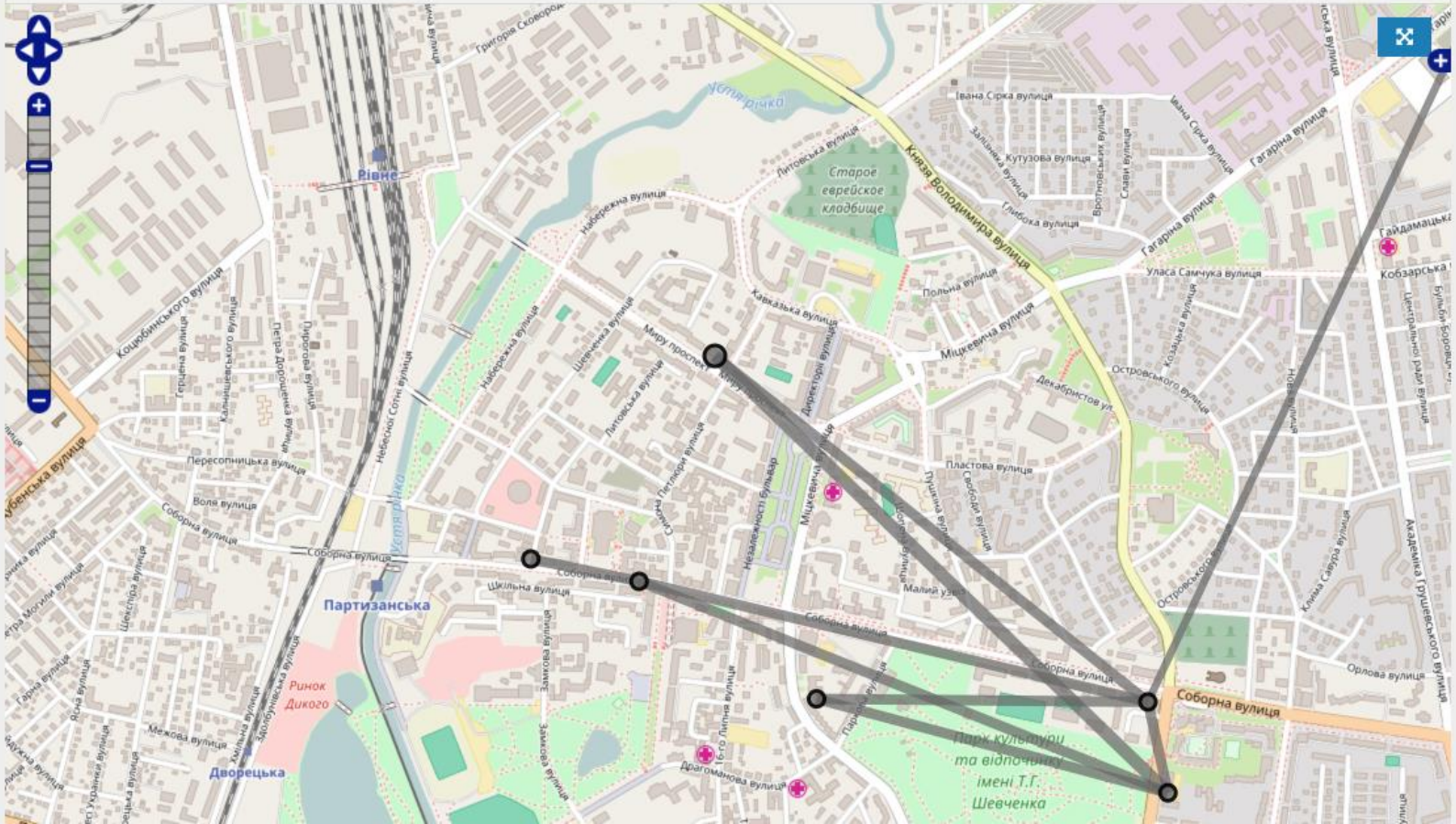
10 minutes

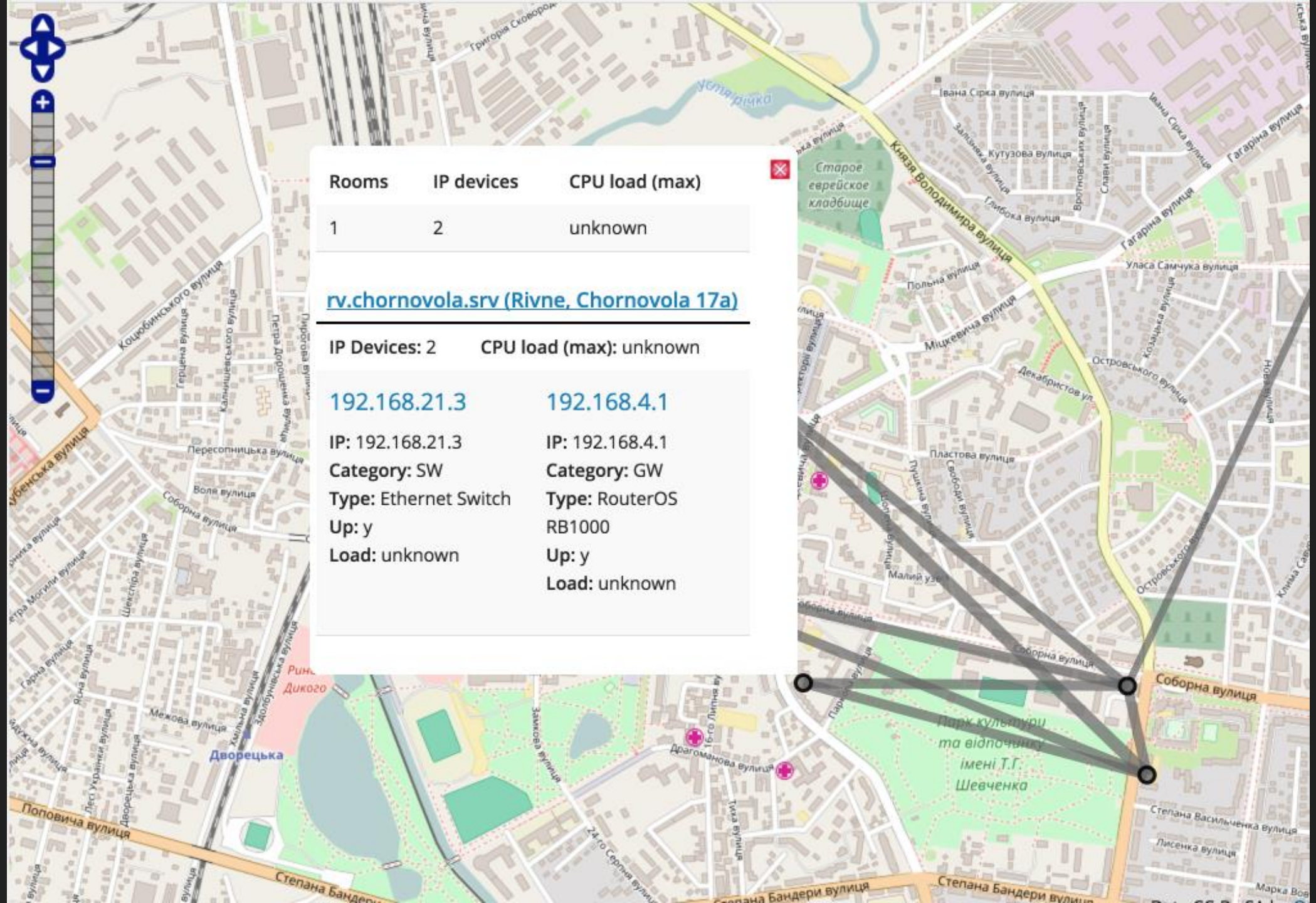
Link to this configuration

Show edges

Show CPU and interface load

<<	<	Nov 2016			>	>>
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

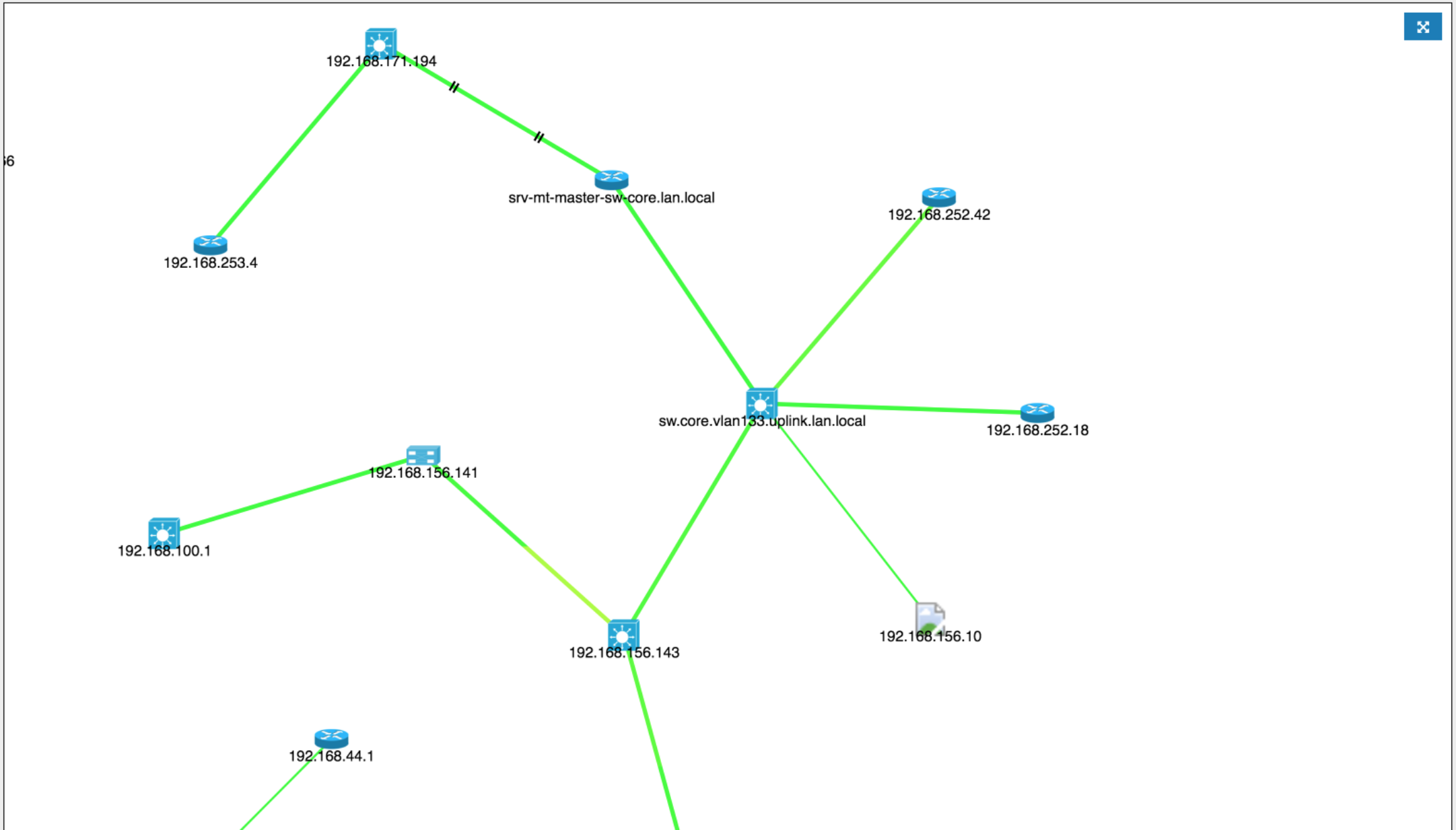



Rooms
IP devices
CPU load (max)
1
2
unknown
rv.chornovola.srv (Rivne, Chornovola 17a)
IP Devices: 2
CPU load (max): unknown
192.168.21.3
IP: 192.168.21.3
Category: SW
Type: Ethernet Switch
Up: y
Load: unknown
192.168.4.1
IP: 192.168.4.1
Category: GW
Type: RouterOS
RB1000
Up: y
Load: unknown
Старое еврейское кладбище
Князя Володимира вулиця
Соборна вулиця
Степана Бандери вулиця
Поповича вулиця
Дворецька
Парк культури та відпочинку імені Т.Г. Шевченка

Netmap

Topological layer 2 and layer 3 network weather map.

Search graph | Search | Reset | View | All layer2 (admin) | View options



Netmap

Topological layer 2 and layer 3 network weather map.

Search graph | Search | Reset | View: All layer2 (admin) | View options

Create and edit views

- Create new view
- Set as default view
- Edit view
- Delete view

Manage saved views

View settings

- [x] GW
- [x] GSW
- [x] SW
- [x] EDGE
- [x] WLAN
- [x] SRV
- [x] OTHER
- [x] ENV
- [x] POWER
- [ ] ELINK

Display isolated nodes [ ]

Layer: 2

Filter by room or locati | Filter

Save view settings

Misc

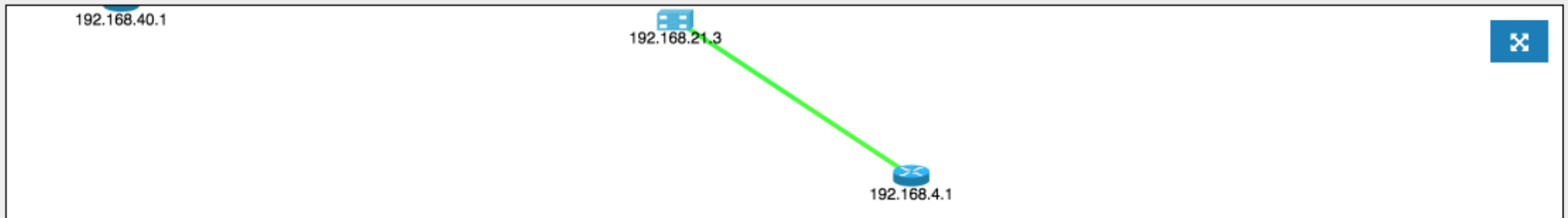
Fix all nodes | Unfix all nodes

Zoom to fit | Reset view

Stop animation

Refresh interval

- (•) Off
- ( ) 2 min
- ( ) 10 min
- [ ] Traffic only



192.168.47.120

Edit IP device | Schedule maintenance | View device history | Configure ports

Device Info | Neighbors | Ports | Port metrics | System metrics | Recent alerts | Power and fans | Services | DNS | What if

IP Device: 192.168.47.120

Full sysname	192.168.47.120
Type	1.3.6.1.4.1.9.1.726 (Cisco IOS Software, CE500 Software (CE500-LANBASEK9-M), Version 12.2(25)SEG6, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Fri 05-Sep-08 20:43 by myl from unknown)
Category	SW (Core switches (layer 2), typically with many vlans)
Function	N/A
Organization	myorg (KTC)
Room	rv.soborna57.srv (Рівне, Соборна 57)
Chassis	1 (serial: FOC0947X1UW, software: 12.2(25)SEG6)
IP address	192.168.47.120
Prefix	192.168.47.64/26 (vlan 2)
Uplinks	N/A
Modules	0
Interfaces	30
Switch ports	26
Router ports	1

Status

Uptime	Up for 2 weeks, 5 days
Availability	100.00% last day, 100.00% last week, 100.00% last month
Response time	0.002s last day, 0.002s last week, 0.002s last month
First discovered	2016-01-04 18:40:19
Active maintenance	Not on maintenance
Planned maintenance	Not scheduled for maintenance

Jobs

Name	End time	Duration	Status
1minstats	2016-11-11 19:08:12	0.12s	
Topo	2016-11-11 19:03:48	3.75s	
Statuscheck	2016-11-11 19:03:47	5.62s	
5minstats	2016-11-11 19:03:46	2.54s	
Snmpcheck	2016-11-11 19:03:43	1.22s	
Dns	2016-11-11 19:03:42	1.13s	
Ip2mac	2016-11-11 19:03:41	0.00s	
Inventory	2016-11-11 17:03:52	10.36s	

192.168.47.120

Edit IP device | Schedule maintenance | View device history | Configure ports

Device Info | Neighbors | Ports | Port metrics | System metrics | Recent alerts | Power and fans | Services | DNS | What if

Switch port status | Switch port activity | Router port status | Physical ports

No module

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10
Fa11	Fa12	Fa13	Fa14	Fa15	Fa16	Fa17	Fa18	Fa19	Fa20
Fa21	Fa22	Fa23	Fa24	Gi1	Gi2				

Show port legend

Port details: Fa1 at 192.168.47.120

Back to 192.168.47.120

Track MAC behind port | Configure port

Interface Fa1 at 192.168.47.120

Interface	FastEthernet1
At module	No module
Port name	N/A
Link	Active
Speed	100.0 Mbit Full duplex
Hardware address	00:15:62:7E:73:83

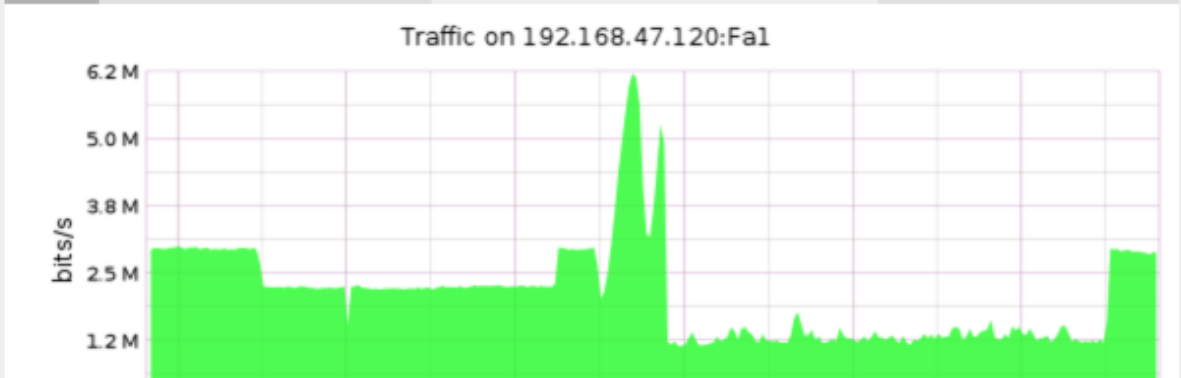
Connection

Trunk	No
Configured VLAN	42
Detected VLANs	N/A
To IP device	N/A
To port	N/A
Patched to	N/A
Last CAM record	0 minutes ago

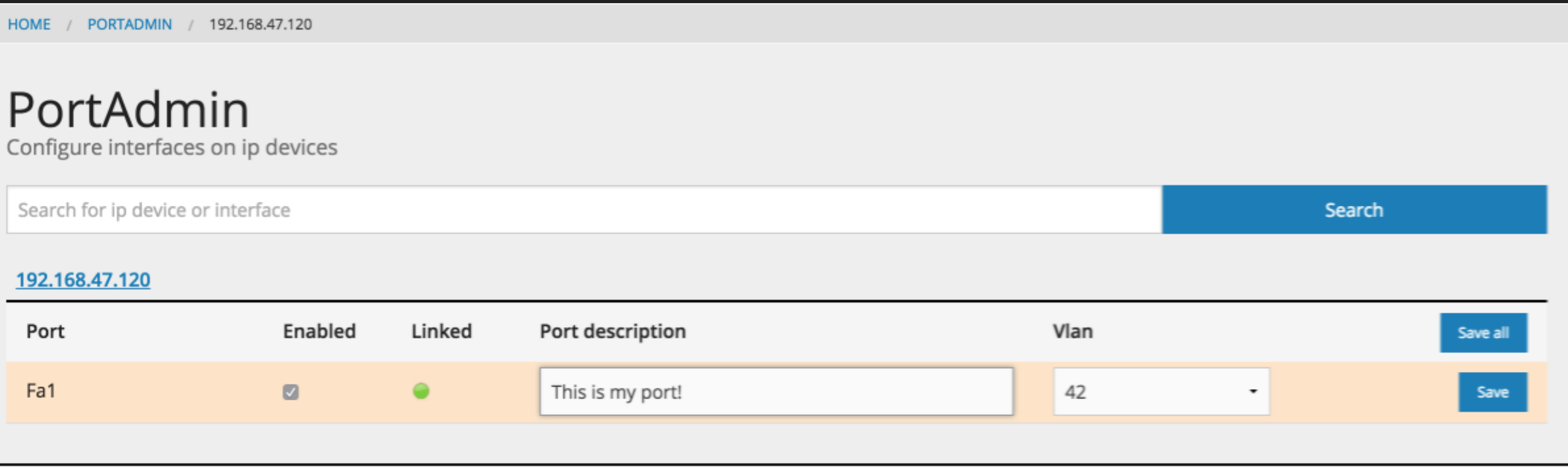
Activity graphs

Day | Week | Month | Year

Add graph to dashboard



Configure port



192.168.47.120

Edit IP device | Schedule maintenance | View device history | Configure ports

Device Info | Neighbors | Ports | Port metrics | System metrics | Recent alerts | Power and fans | Services | DNS | What if

Switch port status | Switch port activity | Router port status | Physical ports

Activity based on CAM records since 2016-10-12.

Days *

30 | Recheck activity

No module

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10
Fa11	Fa12	Fa13	Fa14	Fa15	Fa16	Fa17	Fa18	Fa19	Fa20
Fa21	Fa22	Fa23	Fa24	Gi1	Gi2				

Show port legend

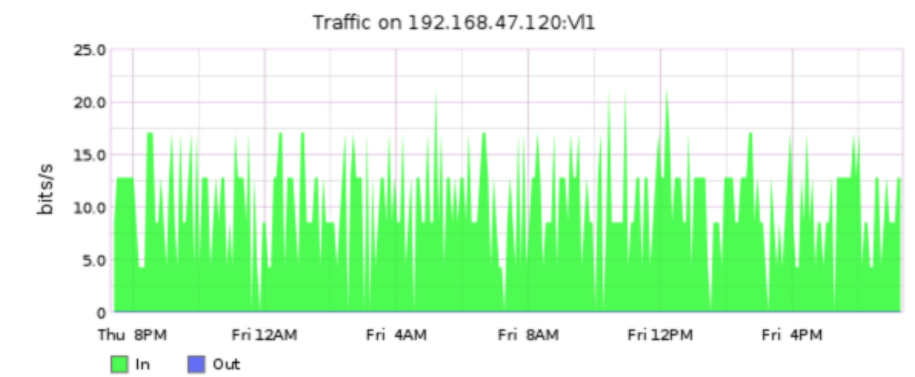
Controls for all graphs

Day | Week | Month | Year | Octets | UcastPkts | Errors | Discards

Vl1

Port details

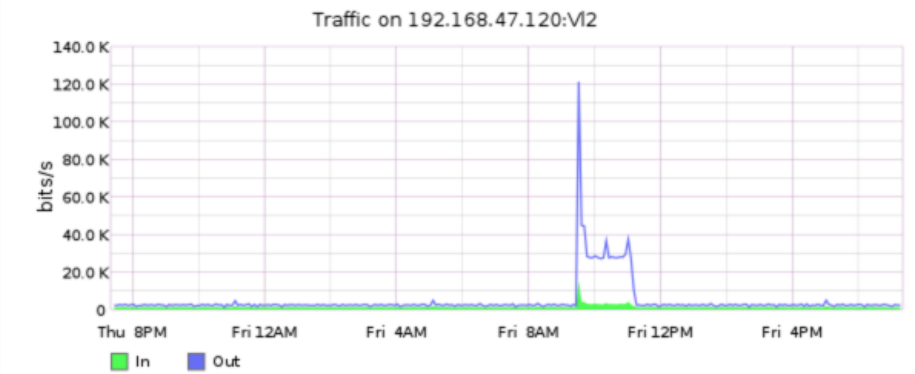
Day | Week | Month | Year | Add graph to dashboard



Vl2

Port details

Day | Week | Month | Year | Add graph to dashboard



Vl55

Fa1

Fa2

Fa3

Fa4

Fa5

192.168.47.120

Edit IP device | Schedule maintenance | View device history | Configure ports

Device Info | Neighbors | Ports | Port metrics | System metrics | Recent alerts | Power and fans | Services | DNS | What if

If this IP device stops working the following will likely be affected.

Devices unreachable

- 192.168.47.120 (SW)

Affected hosts

10 active hosts/users

Organizations

- myorg (KTC) - nobody

Send mail to affected organizations

Maintenance Tasks

Edit device maintenance schedules. Alerts for devices are suppressed while on maintenance.

Back to calendar

New task

Details

Start time *

2016-11-11 19:20

End time

2016-11-18 19:20

No end time

Description *

I'm gonna shutdown everything!
(Trollface)

Selected components

- IP Device: soborna57 → rv.soborna57.srv → 192.168.47.120
- IP Device: Service Center → Server Room → 192.168.100.1
- IP Device: Service Center → Server Room → 192.168.156.141

Select components

Search

↓ Location
↓ Room
↑ IP device

Server Room (Service Center)
  192.168.100.1
  192.168.156.141
azure-ireland (datacenter in Dublin)
  192.168.156.10
  192.168.158.250
  192.168.171.194
  192.168.201.33
  192.168.201.49
  192.168.252.18

Add IP device | Select all

↓ Service

Device History

Browse and search alert history of devices. Delete modules that are no longer in operation.

Device History | Register Error Event | Delete Module

Select and view device history for a location, room, box or module. Use quicksearch to search for a (partial) serialnumber, hostname, IP or room.

Filters

From date: 11/04/2016

To date: 11/12/2016

Type: All

Group by: Netbox

Search

↑ Location

Ivano-Frankivsk (KTC shop Ivano-Frankivsk)
Kostopil (KTC shop Kostopil)
Kuznetsovsk (KTC shop Kuznetsovsk)
mylocation (Example location)
olgi5 (HeadOffice Rivne Olgi 5)
rv.Kyivstar (rv.Kyivstar)
rv.Soborna.shop-4 (м.Рівне вул. Соборна)
Service Center (Server Room)
Shepetivka (KTC shop Shepetivka)
soborna57 (Rivne, Soborna 57)
Ternopil (KTC shop Ternopil)

View location history | Select all

↓ Room

↑ IP device

Server Room (Service Center)
192.168.100.1 [192.168.100.1 - None]
192.168.156.141 [192.168.156.141 - None]

Device History

Browse and search alert history of devices. Delete modules that are no longer in operation.

Device History | Register Error Event | Delete Module

New search

Filters

From date: 11/04/2016

To date: 11/12/2016

Type: All

Group by: Netbox

Filter

Search parameters

Netbox

All netboxes selected.

192.168.156.140 2 items.

Netbox	Serial	Start time	End time	Event type	Alert type	Message
192.168.156.140		2016-06-29 05:30:22	2016-11-11 11:10:55	boxState	boxDown	box down 192.168.156.140 192.168.156.140
192.168.156.140		2016-06-28 21:06:34	2016-11-11 11:10:55	linkState	linkDown	Link down on 192.168.156.140, Slot0/28 ()

2 items.

Machine Tracker

Search NAV's logs of IP and MAC address activity to find where and when hosts in your network have been active.

IP Search | MAC Search | Switch Search | Netbios Search

192.168.55.202 Search Help

Filters

(•) Active ( ) Inactive ( ) Both

Period

Days 7 [ ] Only Active

Columns

[ ] Netbios [x] Dns

IP search results – From 192.168.55.202 to 192.168.55.202 1 hit

DNS	IP	MAC	Start time	End time
	192.168.55.202	00:21:e1:73:14:00	2016-11-11 10:33:39	Still active

1 hit

Клац

Machine Tracker

Search NAV's logs of IP and MAC address activity to find where and when hosts in your network have been active.

IP Search | MAC Search | Switch Search | Netbios Search

00:21:e1:73:14:00 Search

Period

Days 7 Only active ☐

Columns

Dns ☑ Netbios ☐

Uplink search results 1 hit

Sysname	Uplink from	Uplink to	Mac
192.168.55.202	N/A	N/A	00:21:e1:73:14:00

1 hit

Interface search results 48 hits

Клац!

Interface	Alias	Mac
ifc16 (Slot: 1 Port: 16) at 192.168.55.202		00:21:e1:73:14:00
ifc17 (Slot: 1 Port: 17) at 192.168.55.202	107.stil	00:21:e1:73:14:00
ifc18 (Slot: 1 Port: 18) at 192.168.55.202	107.vikno	00:21:e1:73:14:00
ifc19 (Slot: 1 Port: 19) at 192.168.55.202	olgy.corp	00:21:e1:73:14:00
ifc20 (Slot: 1 Port: 20) at 192.168.55.202	107.vhid	00:21:e1:73:14:00
ifc21 (Slot: 1 Port: 21) at 192.168.55.202	olgy.buhgalteria_01	00:21:e1:73:14:00

Port details: ifc17 (Slot: 1 Port: 17) at 192.168.55.202

Back to 192.168.55.202

Track MAC behind port | Configure port

Interface ifc17 (Slot: 1 Port: 17) at 192.168.55.202

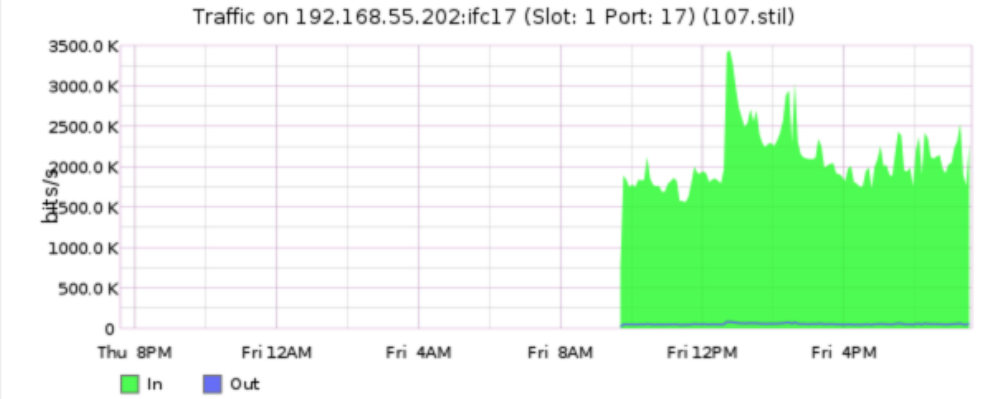
Interface	Avaya Ethernet Routing Switch 4548GT PWR Module - Port 17
At module	No module
Port name	107.stil
Link	Active
Speed	100.0 Mbit Full duplex
Hardware address	00:21:E1:73:14:00

Connection

Trunk	No
Configured VLAN	N/A
Detected VLANs	N/A
To IP device	N/A
To port	N/A
Patched to	N/A
Last CAM record	0 minutes ago

Activity graphs

Day | Week | Month | Year | Add graph to dashboard



Unrecognized Neighbors

List, add or ignore unrecognized neighbors

Ignore selected | Unignore selected

Show ignored neighbors

Filter: Show 10 entries

First | Previous | 1 | 2 | Next | Last

Remote ID	Remote Name	Seen on interface	Source	First seen
00:19:99:a4:37:85		ifc34 (Slot: 1 Port: 34) at 192.168.55.202	lldp	2016-11-11 09:41:36
00:24:00:29:84:00	switch.nortel2	ifc3 (Slot: 1 Port: 3) at 192.168.55.202	lldp	2016-11-11 09:41:36
192.168.56.234	SEP0019305D11D8.ktc.local	ifc13 (Slot: 1 Port: 13) at 192.168.55.202	lldp	2016-11-11 09:41:36
192.168.56.236	SEP001AE2BCBB58.ktc.local	ifc14 (Slot: 1 Port: 14) at 192.168.55.202	lldp	2016-11-11 09:41:36
f8:ca:b8:62:a2:99		Port6 at 192.168.47.66	lldp	2016-08-25 18:19:15

15 neighbors

Network Explorer

Explore the network topology as it expands from each router port.

Sysname

Search exact (no substring)

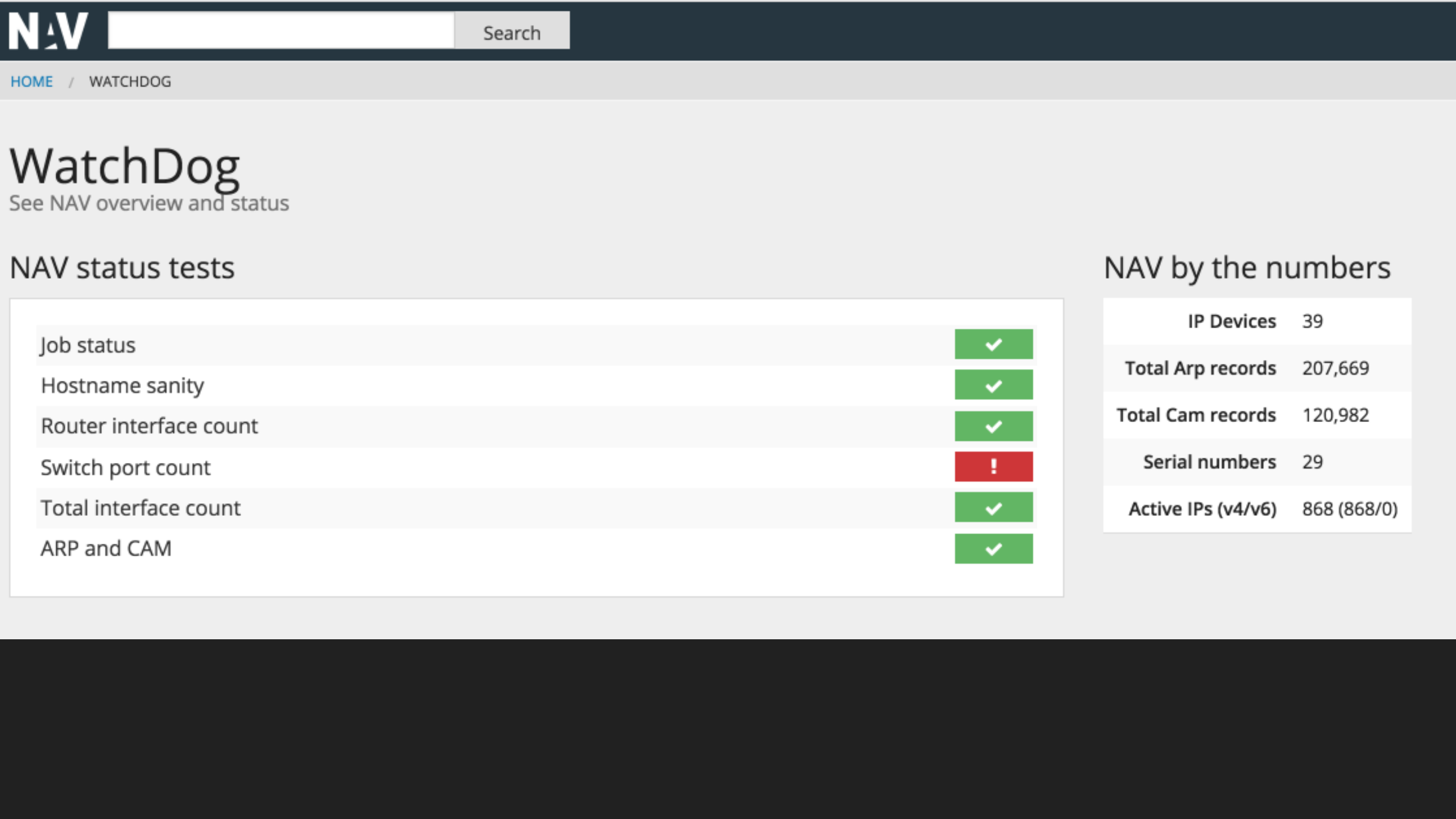
Hide ports with no description

Search

- 192.168.100.1
- 192.168.15.1

Router ports:

- InterNet
  Prefixes:
  (91.197.220.252/32, loopback, None)
- RivneSB
  Prefixes:
  (172.16.3.54/32, loopback, None)
- RivneSMI
  Prefixes:
  (172.16.2.46/32, loopback, None)
- br-vlan3
  Prefixes:
  (192.168.48.65/26, lan, None)
- vlan2
  Prefixes:
  (192.168.47.65/26, lan, None)
- vlan4
  Prefixes:
  (192.168.49.1/24, lan, None)
- vlan5
  Prefixes:
  (192.168.47.1/26, lan, None)
- vlan6
  Prefixes:
  (192.168.15.1/24, lan, None)
- vlan20
  Prefixes:
  (10.0.112.1/24, lan, None)


NAV
Search
HOME / WATCHDOG
WatchDog
See NAV overview and status
NAV status tests
Job status
Hostname sanity
Router interface count
Switch port count
Total interface count
ARP and CAM
NAV by the numbers
IP Devices 39
Total Arp records 207,669
Total Cam records 120,982
Serial numbers 29
Active IPs (v4/v6) 868 (868/0)

API !!!

```
http myhost/api/cam/ \
mac==00:00:00:00:00:00 \
active==true
```


```
{
  "count": 1,
  "next": null,
  "previous": null,
  "results": [
    {
      "id": 875800,
      "netbox": 11,
      "sysname": "mydlink",
      "ifindex": 14,
      "module": "",
      "port": "A00",
      "start_time": "2016-05-13T13:09:40.296",
      "end_time": "9999-12-31T23:59:59.999",
      "miss_count": 0,
      "mac": "00:00:00:00:00:00"
    }
  ]
}
```

А ось і назва інтерфейсу

```
http
myhost/api/interface \
netbox==11 \
ifindex ==14
```


```
{
  "count": 1,
  "results": [
    {
      "id": 329955,
      "netbox": 11,
      "module": 5996,
      "ifindex": 229,
      "ifname": "A00",
      "iftype": 6,
      "speed": 1000,
      "ifphysaddress": "01:23:45:67:89:01",
      "ifconnectorpresent": true,
      "baseport": 55,
      "media": null,
      "vlan": 20,
      "trunk": false,
      "duplex": "t",
      "to_netbox": 85,
    }
  ]
}
```

А що ще є в API?

- alert
- arp
- cam
- room
- netbox
- interface
- prefix
- prefix_usage
- prefic_routed

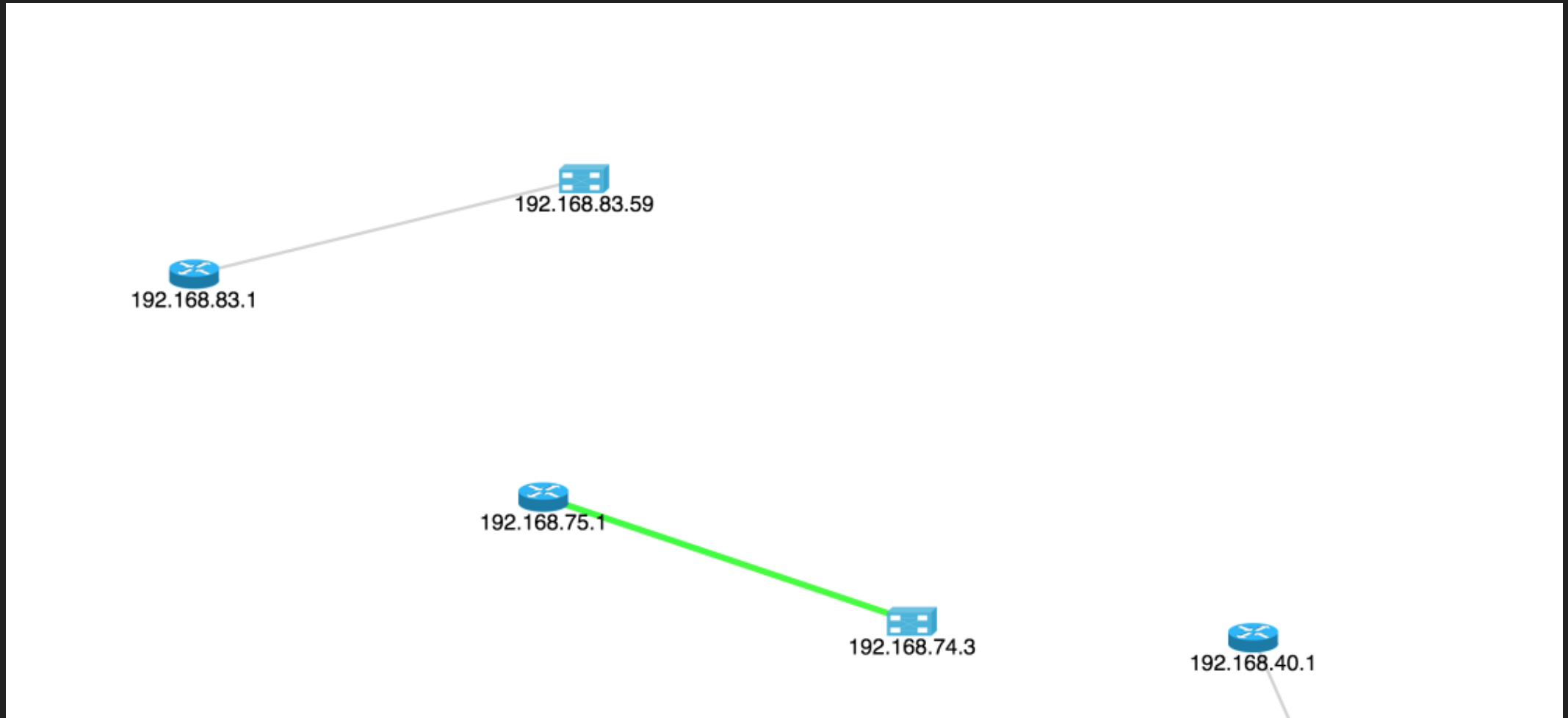
Mikrotik Routerboard ☹

В нас було 2 шасі сімдесят-другої циски, 75 корпусів Catalyst, 5 шаф з Junyper, пів-стійки просто серваків та велика кількість маршрутизаторів усіх кольорів та забарвлень, а також Extreme, Huawei, ящик свічів, пачка віртуалок в чужому датацентрі та Quagga.

Не те щоб це був необхідний набір для провайдера. Але якщо розпочав збирати хлам то стає складно зупинитись. Єдине, що викликало в мене побоювання — це Mikrotik. Немає нічого більш безпорадного та зіпсованого ніж мережі побудовані на Мікротіках.

Я знав, що рано чи піздно ми перейдемо і на цю погань.

L2TP і карта ☹



Висновки

- Drilldown в NAV рулить
- API в NAV рулить
- Zabbix і Nagios зрілі та багатофункціональні системи моніторінгу
- Але якщо з вендорами бардак — з NAV круто!
- Hikvision — непогані камери

NAV – голова. Спробуйте!

https://nav.uninett.no