Monitoring RouterOS

Simple Network Management Protocol

ElasticSearch, LogStash & Kibana

MUM Cambodia 2019

Author: Soragan Ong

ALAGAS NETWORK
www.mikrotik.sg

AlagasNetwork

ABOUT ME

My name is Soragan Ong

I am MikroTik Certified Trainer

Also IPv6 Forum certified engineer

ខ្ញុំធ្វើការឱ្យ Alagas Network

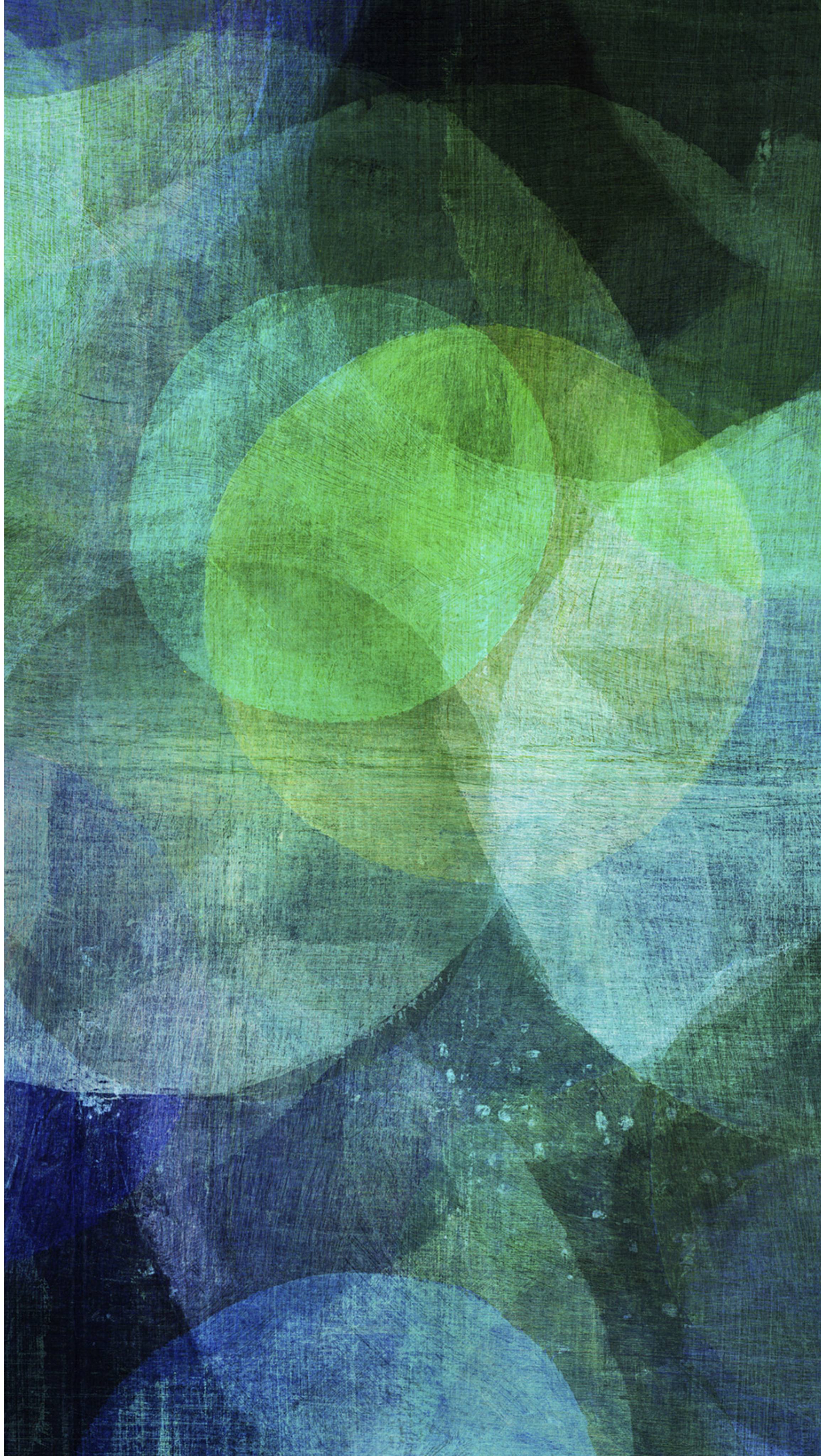
WHO IS ALAGAS NETWORK?

- MikroTik VAD based in Singapore
- Distributing MikroTik since 2010
- 2Gbps in Singapore in 2014, second in the world after Japan
- MikroTik Training Centre Since 2016

HOW CAN WE MONITOR?

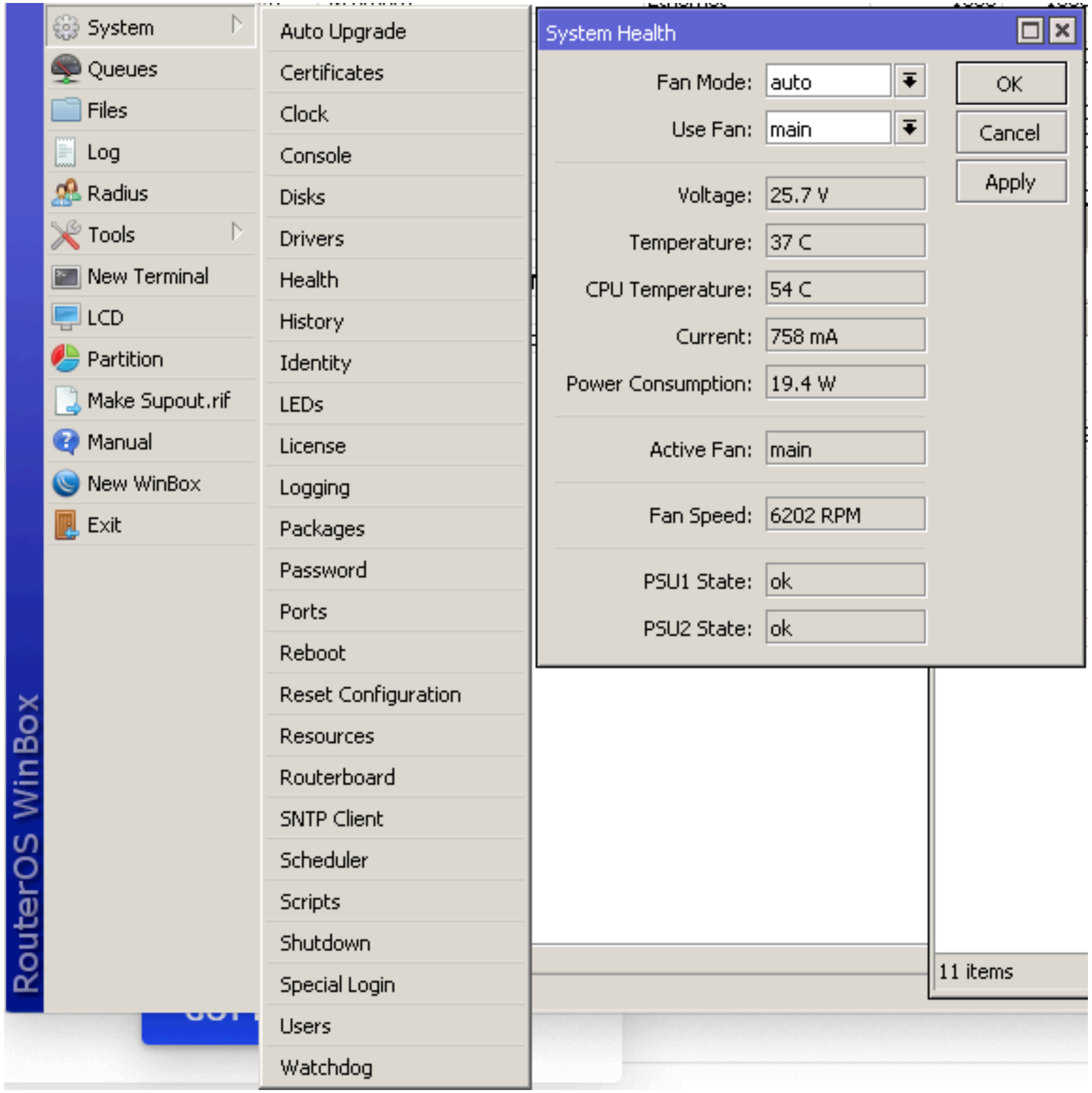
- Does NOT require extra software:
    - Built-in Tools
- Require external software
    - Simple Network Management Protocol
    - Flows / ELK Stack
- The Dude

ROUTEROS BUILT-IN TOOLS



ROUTEROS BUILT-IN TOOLS

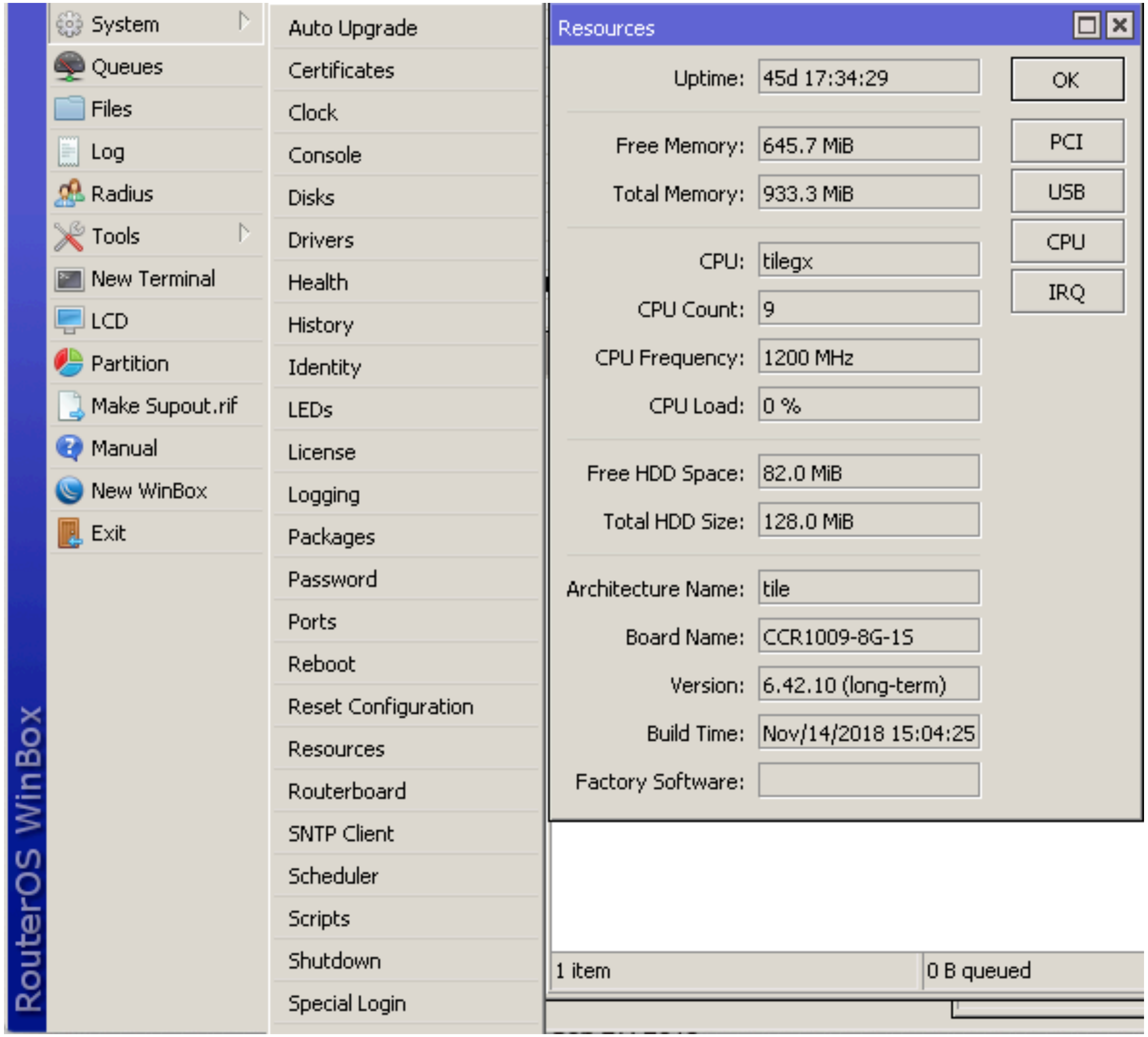
- Hardware Health
  - Fan status
  - Electricity Supply
  - Temperature
- Hardware Failure: Fan, PSU
- Power Outage



Fan Mode: auto
Use Fan: main
Voltage: 25.7 V
Temperature: 37 C
CPU Temperature: 54 C
Current: 758 mA
Power Consumption: 19.4 W
Active Fan: main
Fan Speed: 6202 RPM
PSU1 State: ok
PSU2 State: ok

ROUTEROS BUILT-IN TOOLS

- Resource Usage
  - CPU
  - Memory / RAM
  - Storage
- Hardware Upgrade



Resources

Uptime: 45d 17:34:29

Free Memory: 645.7 MiB

Total Memory: 933.3 MiB

CPU: tilegx

CPU Count: 9

CPU Frequency: 1200 MHz

CPU Load: 0 %

Free HDD Space: 82.0 MiB

Total HDD Size: 128.0 MiB

Architecture Name: tile

Board Name: CCR1009-8G-1S

Version: 6.42.10 (long-term)

Build Time: Nov/14/2018 15:04:25

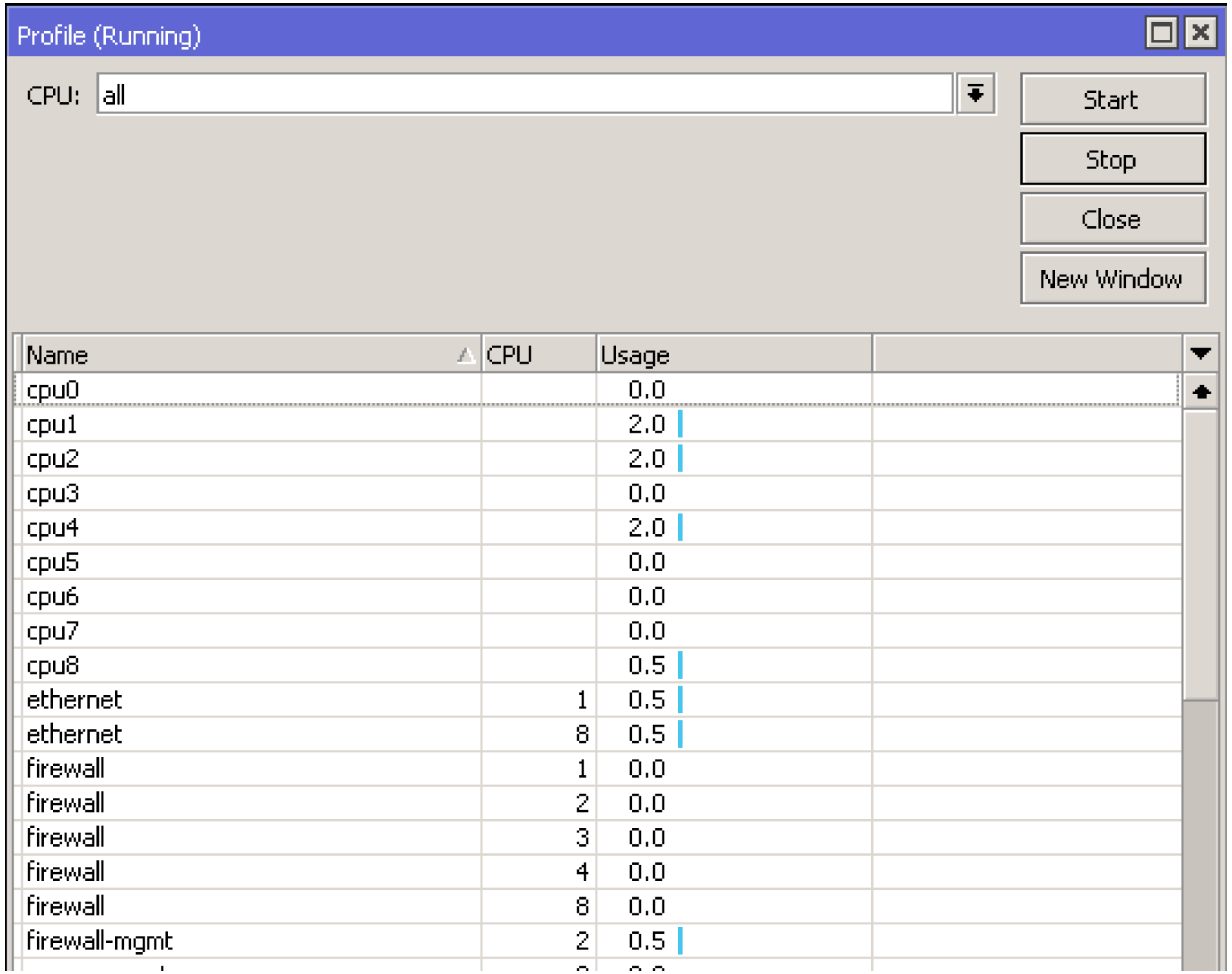
Factory Software:

1 item | 0 B queued

ROUTEROS BUILT-IN TOOLS

- Tool > Profile
  - Your best friend when you experiencing high CPU usage

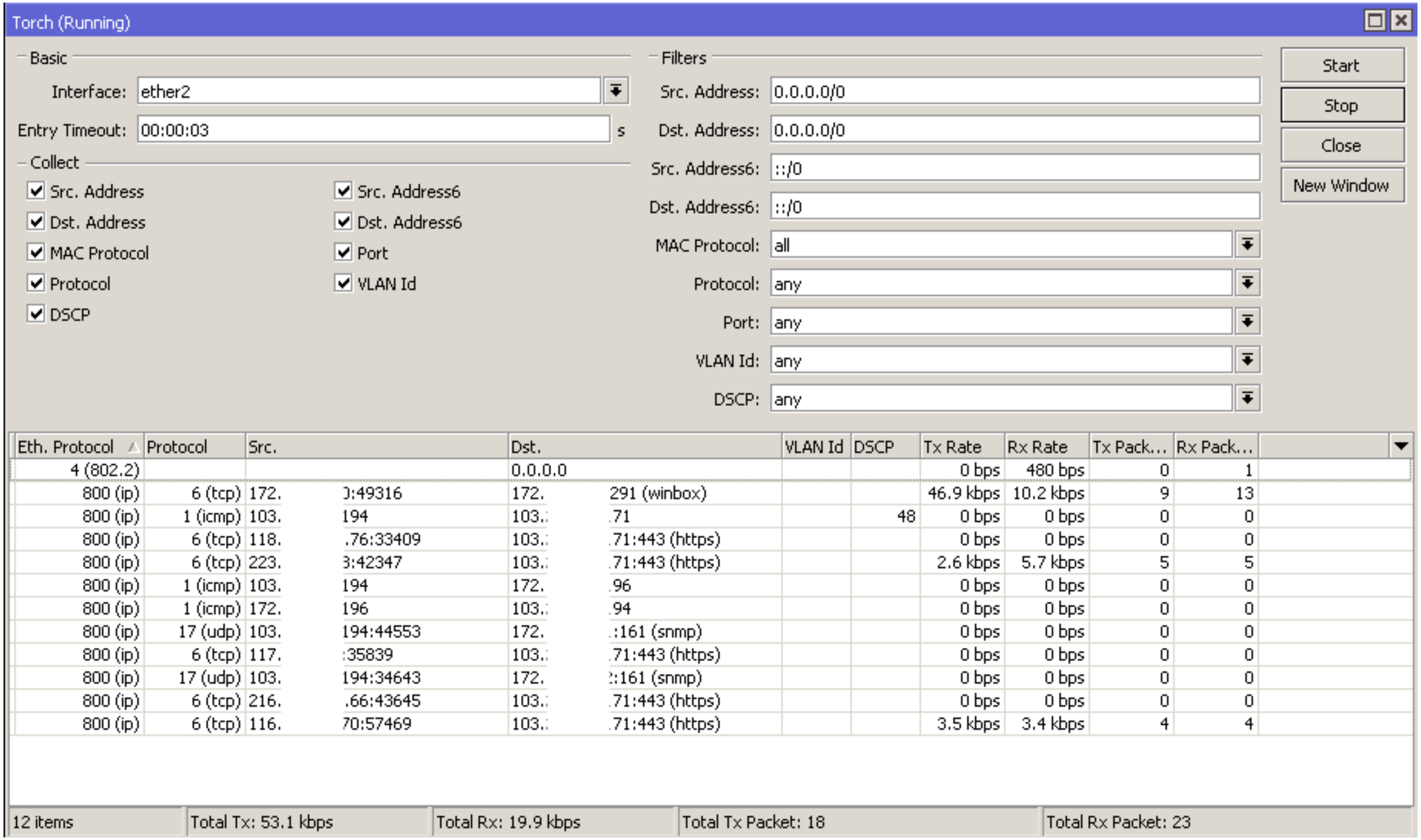
https://wiki.mikrotik.com/wiki/Manual:Tools/Profiler



CPU: all

Name	CPU	Usage
cpu0		0.0
cpu1		2.0
cpu2		2.0
cpu3		0.0
cpu4		2.0
cpu5		0.0
cpu6		0.0
cpu7		0.0
cpu8		0.5
ethernet	1	0.5
ethernet	8	0.5
firewall	1	0.0
firewall	2	0.0
firewall	3	0.0
firewall	4	0.0
firewall	8	0.0
firewall-mgmt	2	0.5

ROUTEROS BUILT-IN TOOLS



Basic

Interface: ether2

Entry Timeout: 00:00:03 s

Collect

☑ Src. Address
☑ Dst. Address
☑ MAC Protocol
☑ Protocol
☑ DSCP
☑ Src. Address6
☑ Dst. Address6
☑ Port
☑ VLAN Id

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

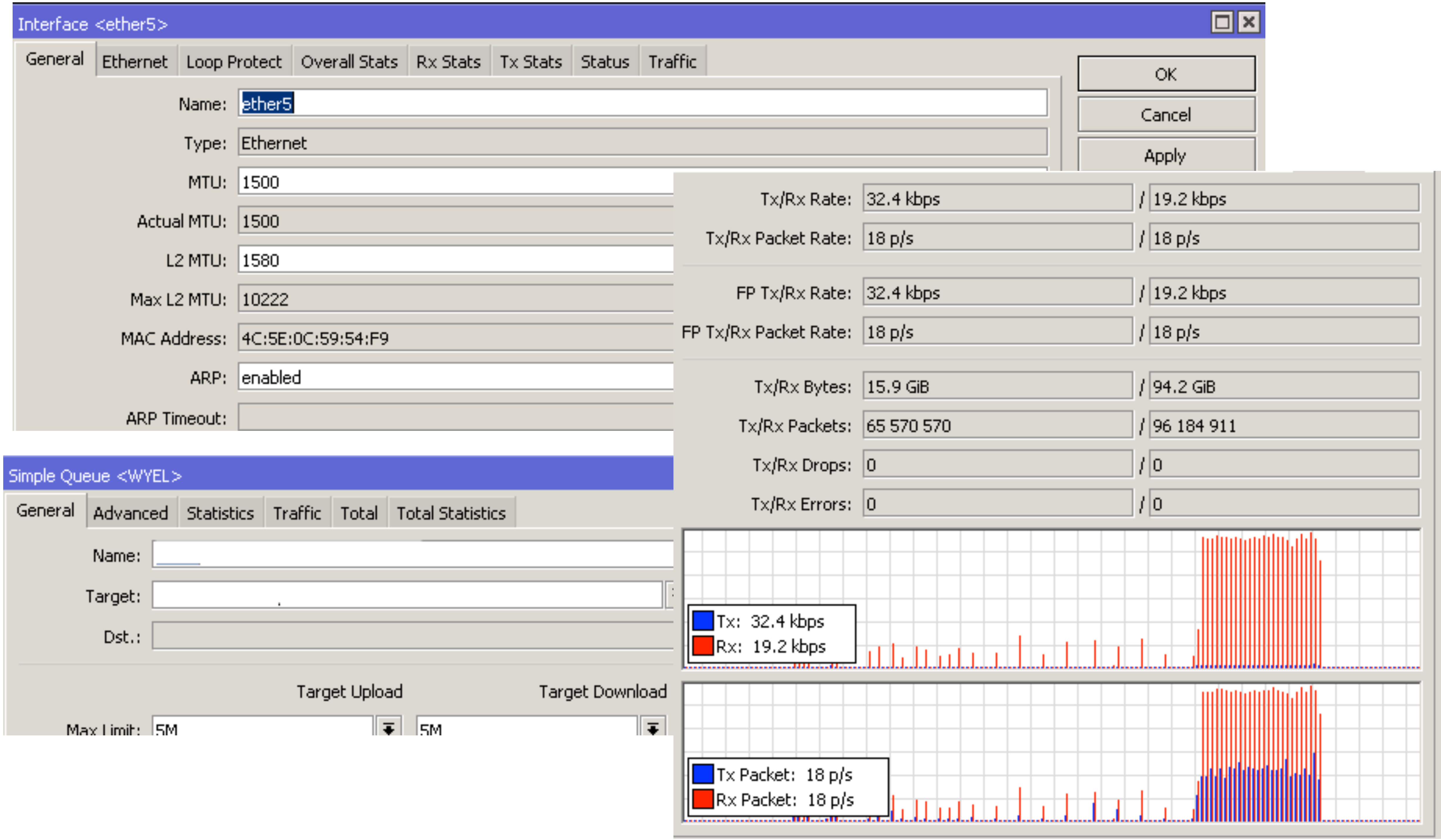
Eth. Protocol	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
4 (802.2)			0.0.0.0			0 bps	480 bps	0	1
800 (ip)	6 (tcp)	172.[redacted]:49316	172.[redacted]291 (winbox)			46.9 kbps	10.2 kbps	9	13
800 (ip)	1 (icmp)	103.[redacted]194	103.[redacted].71		48	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	118.[redacted].76:33409	103.[redacted].71:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	223.[redacted]:42347	103.[redacted].71:443 (https)			2.6 kbps	5.7 kbps	5	5
800 (ip)	1 (icmp)	103.[redacted]194	172.[redacted].96			0 bps	0 bps	0	0
800 (ip)	1 (icmp)	172.[redacted]196	103.[redacted].94			0 bps	0 bps	0	0
800 (ip)	17 (udp)	103.[redacted]194:44553	172.[redacted]:161 (snmp)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	117.[redacted]:35839	103.[redacted].71:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	103.[redacted]194:34643	172.[redacted]:161 (snmp)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	216.[redacted].66:43645	103.[redacted].71:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	116.[redacted]70:57469	103.[redacted].71:443 (https)			3.5 kbps	3.4 kbps	4	4

12 items | Total Tx: 53.1 kbps | Total Rx: 19.9 kbps | Total Tx Packet: 18 | Total Rx Packet: 23

- Torch
  - Live data on network traffic

ROUTEROS BUILT-IN TOOLS

- Interface / Queue live network utilisation



Interface <ether5>

Name:	ether5
Type:	Ethernet
MTU:	1500
Actual MTU:	1500
L2 MTU:	1580
Max L2 MTU:	10222
MAC Address:	4C:5E:0C:59:54:F9
ARP:	enabled
ARP Timeout:	

Tx/Rx Rate:	32.4 kbps	/ 19.2 kbps
Tx/Rx Packet Rate:	18 p/s	/ 18 p/s
FP Tx/Rx Rate:	32.4 kbps	/ 19.2 kbps
FP Tx/Rx Packet Rate:	18 p/s	/ 18 p/s
Tx/Rx Bytes:	15.9 GiB	/ 94.2 GiB
Tx/Rx Packets:	65 570 570	/ 96 184 911
Tx/Rx Drops:	0	/ 0
Tx/Rx Errors:	0	/ 0

🟦 Tx: 32.4 kbps
🟥 Rx: 19.2 kbps

🟦 Tx Packet: 18 p/s
🟥 Rx Packet: 18 p/s

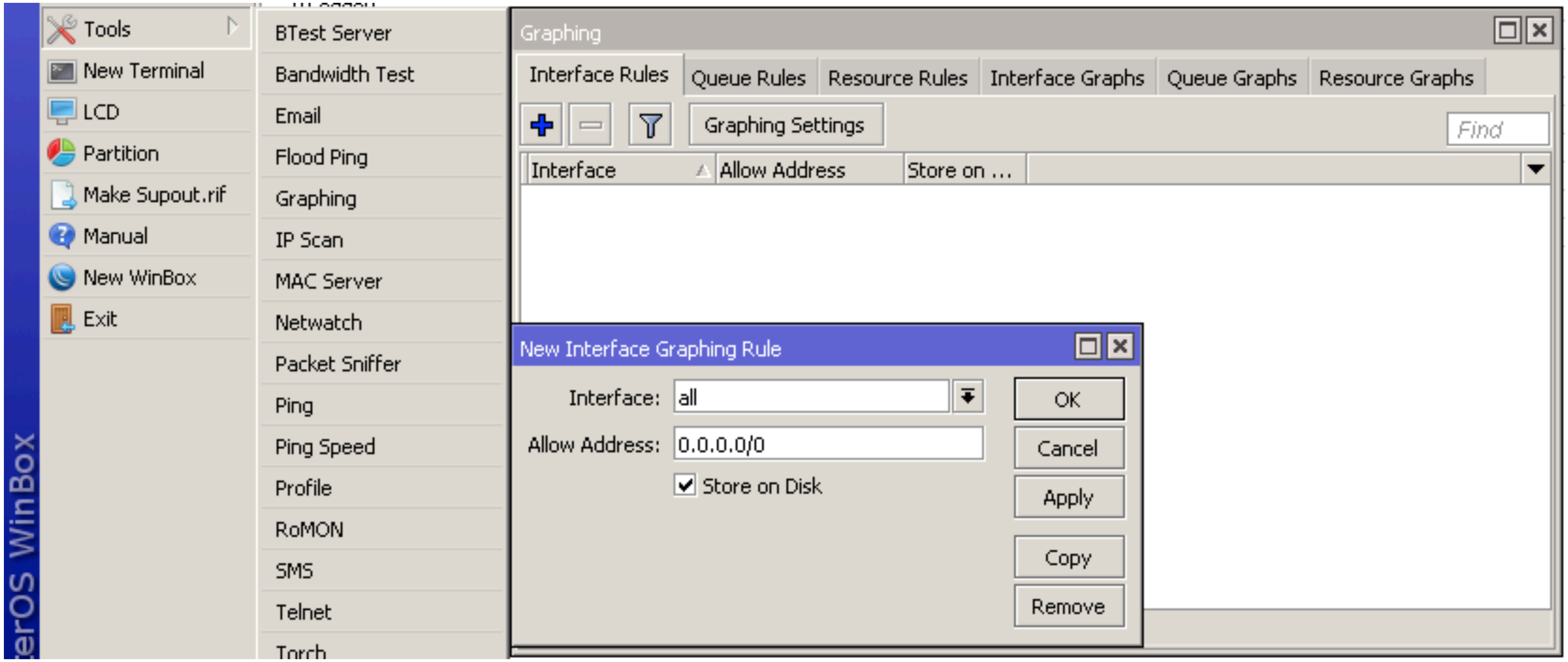
Simple Queue <WYEL>

Name:		
Target:		
Dst.:		
	Target Upload	Target Download
Max Limit:	5M	5M

ROUTEROS BUILT-IN TOOLS

- Graphing

Store information, continuous recording

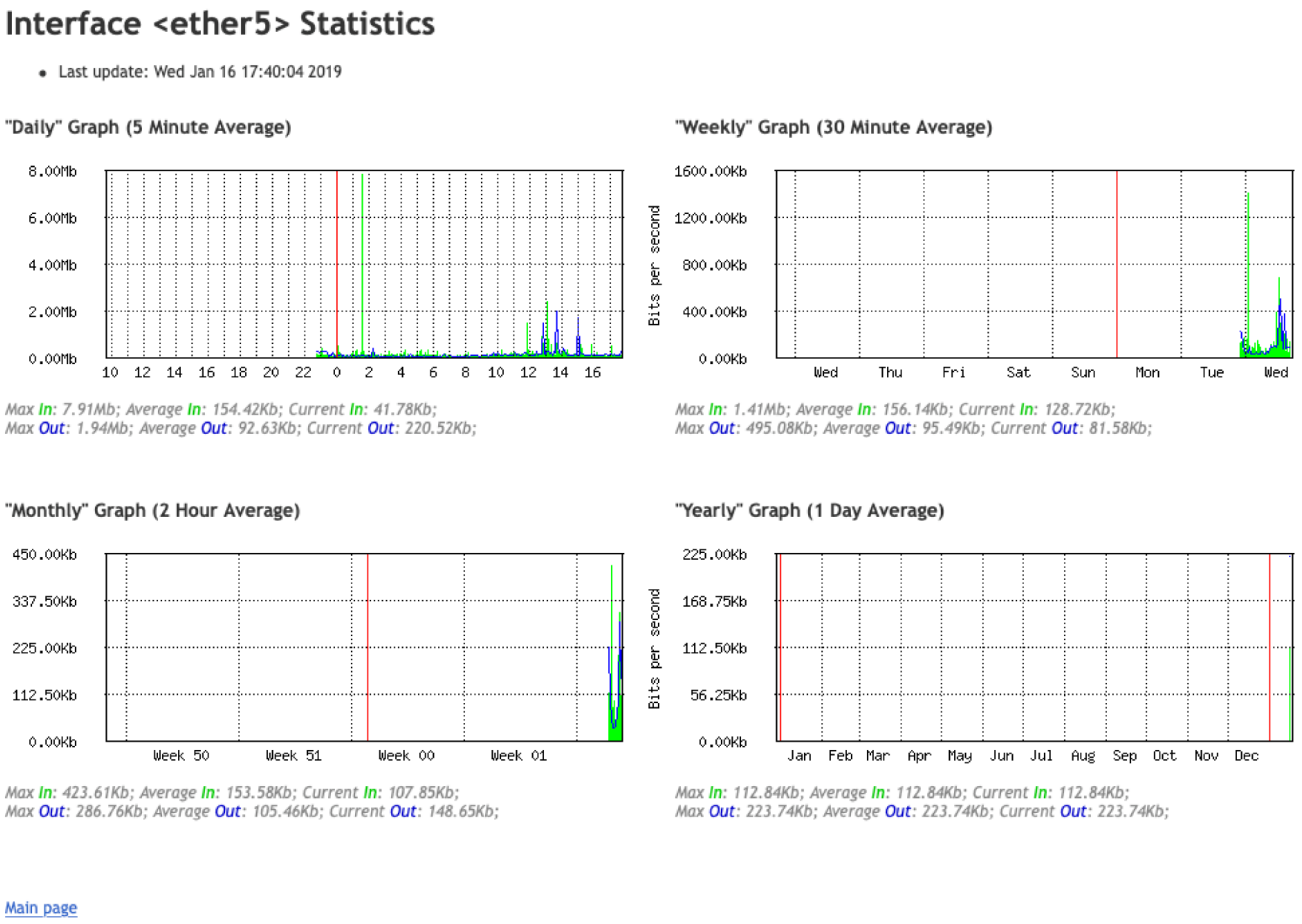


Interface: all

Allow Address: 0.0.0.0/0

☑ Store on Disk

ROUTEROS BUILT-IN TOOLS



Interface <ether5> Statistics

- Last update: Wed Jan 16 17:40:04 2019

"Daily" Graph (5 Minute Average)

Max In: 7.91Mb; Average In: 154.42Kb; Current In: 41.78Kb;
Max Out: 1.94Mb; Average Out: 92.63Kb; Current Out: 220.52Kb;

"Weekly" Graph (30 Minute Average)

Max In: 1.41Mb; Average In: 156.14Kb; Current In: 128.72Kb;
Max Out: 495.08Kb; Average Out: 95.49Kb; Current Out: 81.58Kb;

"Monthly" Graph (2 Hour Average)

Max In: 423.61Kb; Average In: 153.58Kb; Current In: 107.85Kb;
Max Out: 286.76Kb; Average Out: 105.46Kb; Current Out: 148.65Kb;

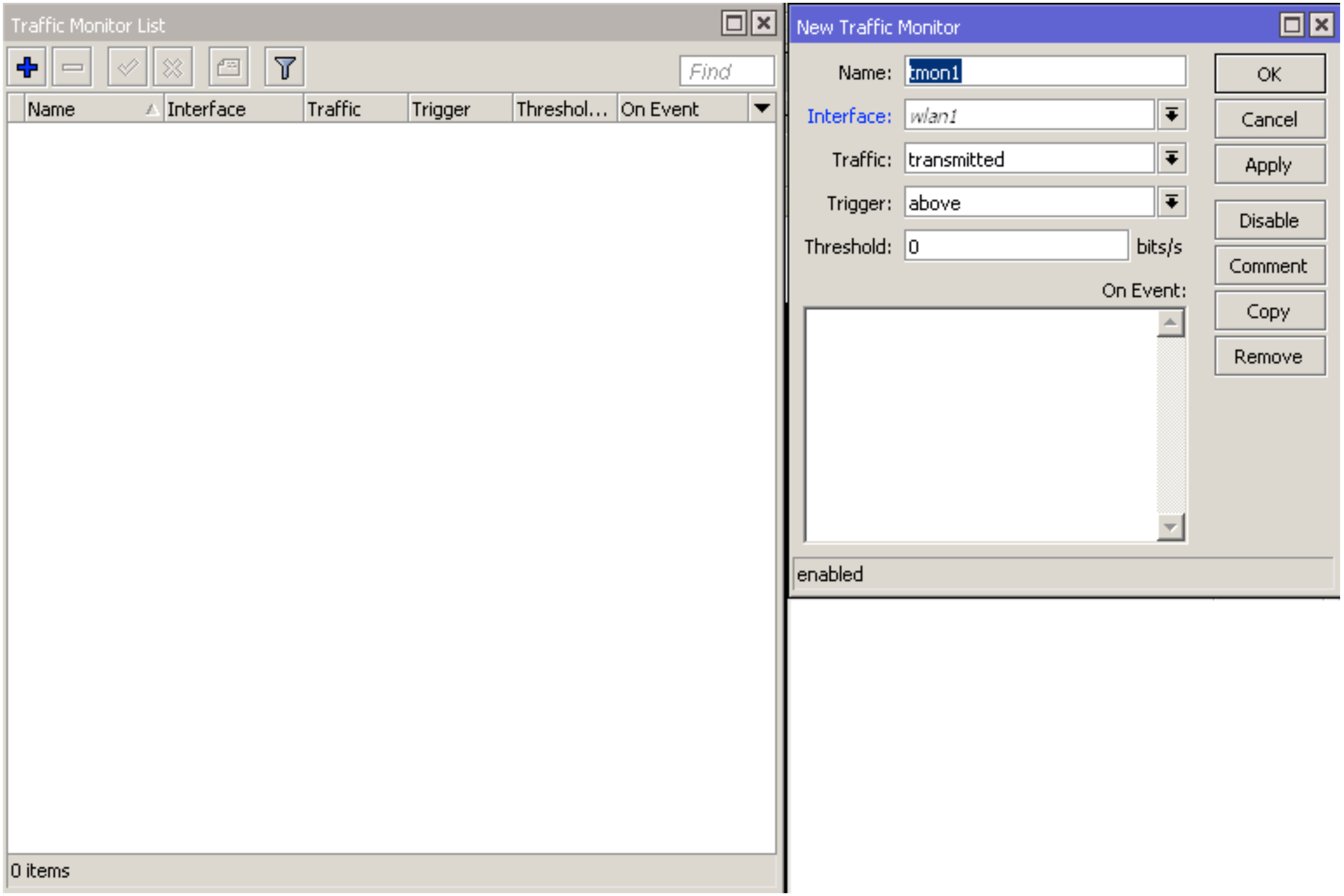
"Yearly" Graph (1 Day Average)

Max In: 112.84Kb; Average In: 112.84Kb; Current In: 112.84Kb;
Max Out: 223.74Kb; Average Out: 223.74Kb; Current Out: 223.74Kb;

Main page

ROUTEROS BUILT-IN TOOLS

- Traffic Monitor
  - Proactive monitoring with action script



Traffic Monitor List

Name	Interface	Traffic	Trigger	Threshol...	On Event

0 items

New Traffic Monitor

Name: tmon1

Interface: wlan1

Traffic: transmitted

Trigger: above

Threshold: 0 bits/s

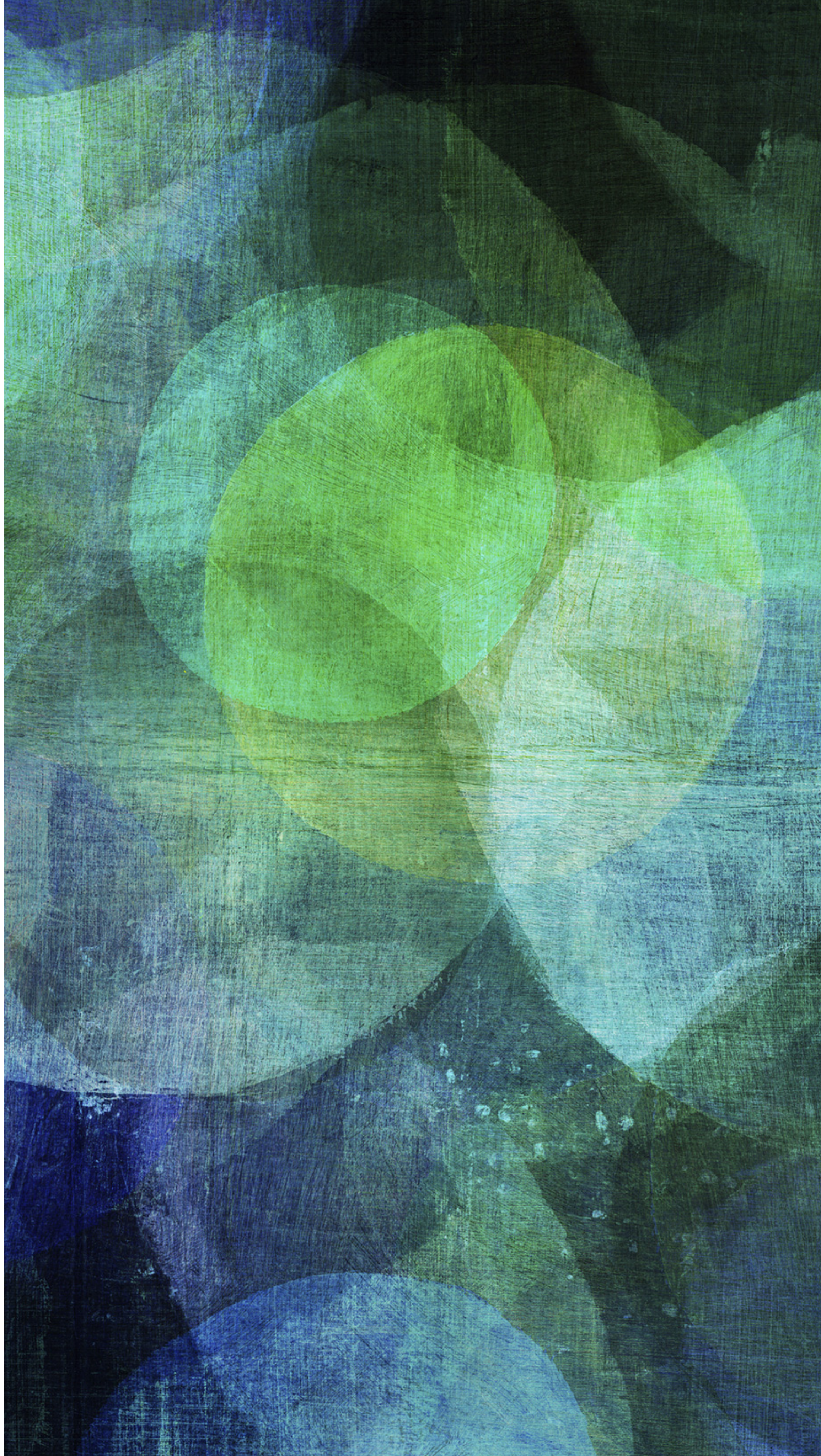
On Event:

enabled

Demo

Basic Monitoring with internal tools

SIMPLE NETWORK MANAGEMENT PROTOCOL



WHAT IS SNMP?

- **S**imple **N**etwork **M**anagement **P**rotocol
- Define by Internet Engineering Task Force (IETF)
- Started in 1989, finalised in 1991
- Application Layer protocol
- MikroTik support SNMP version: 1, 2c, 3

WHY SNMP?

- Open Standard hence widely used
- It is **Simple**
- Remote monitoring
- Requires minimal bandwidth and CPU
- Ability to monitor many data

SNMP ARCHITECTURE

- Agent
  - Process running in nodes that collect information
  - Listening on UDP 161
- Manager
  - Process running in a host that request information from Agent
  - Send request to UDP 161
- Trap
  - Process running in a host that receive event from nodes

SNMP ARCHITECTURE

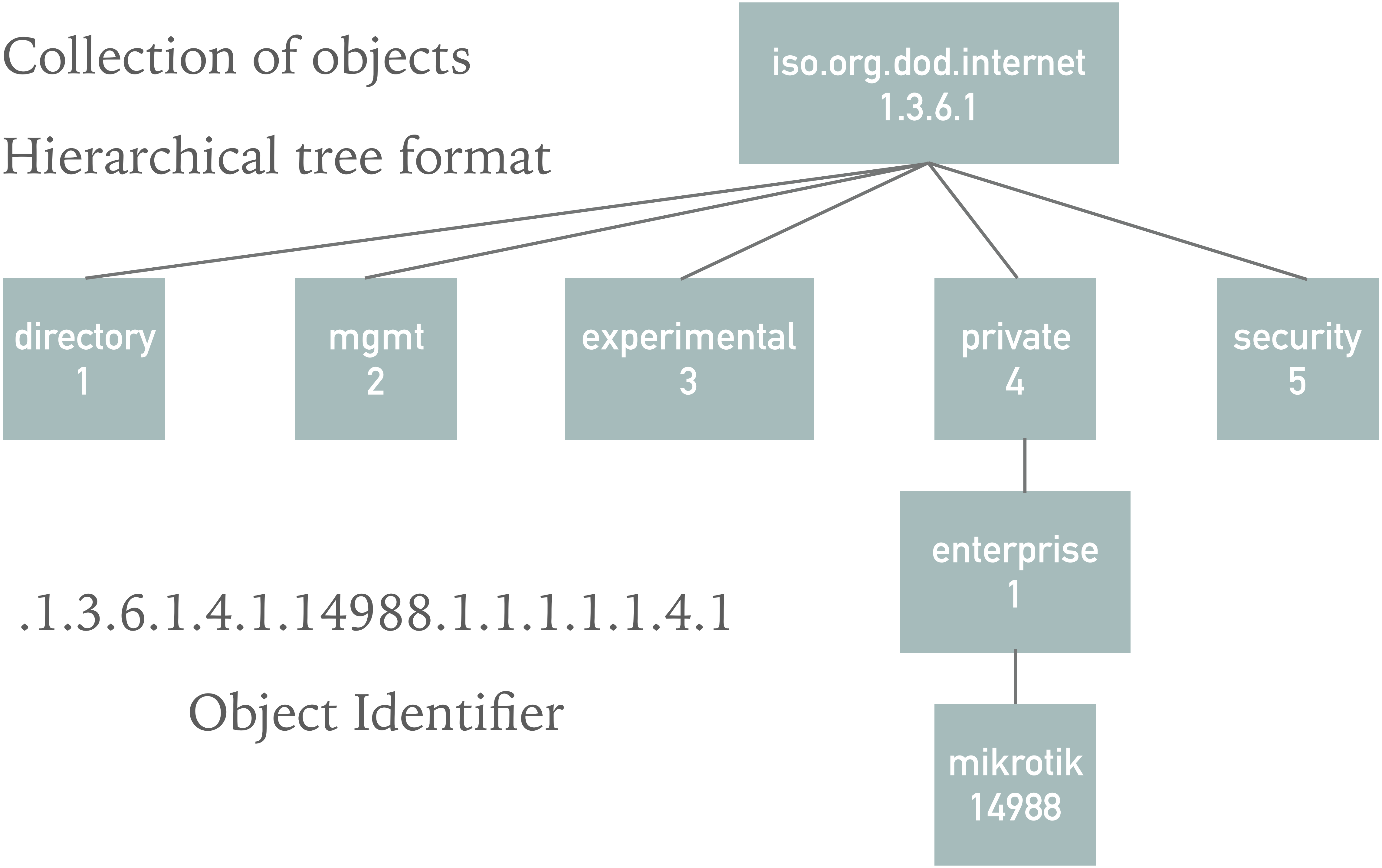
- Trap
  - Process running in a host that receive trap event from agent in nodes
  - Listening on UDP 162

SNMP COMPONENTS

- Management Information Base (MIB)
- Object Identifier (OID)
- Structure of Management Information (SMI)

MANAGEMENT INFORMATION BASE

- Database
- Collection of objects
- Hierarchical tree format

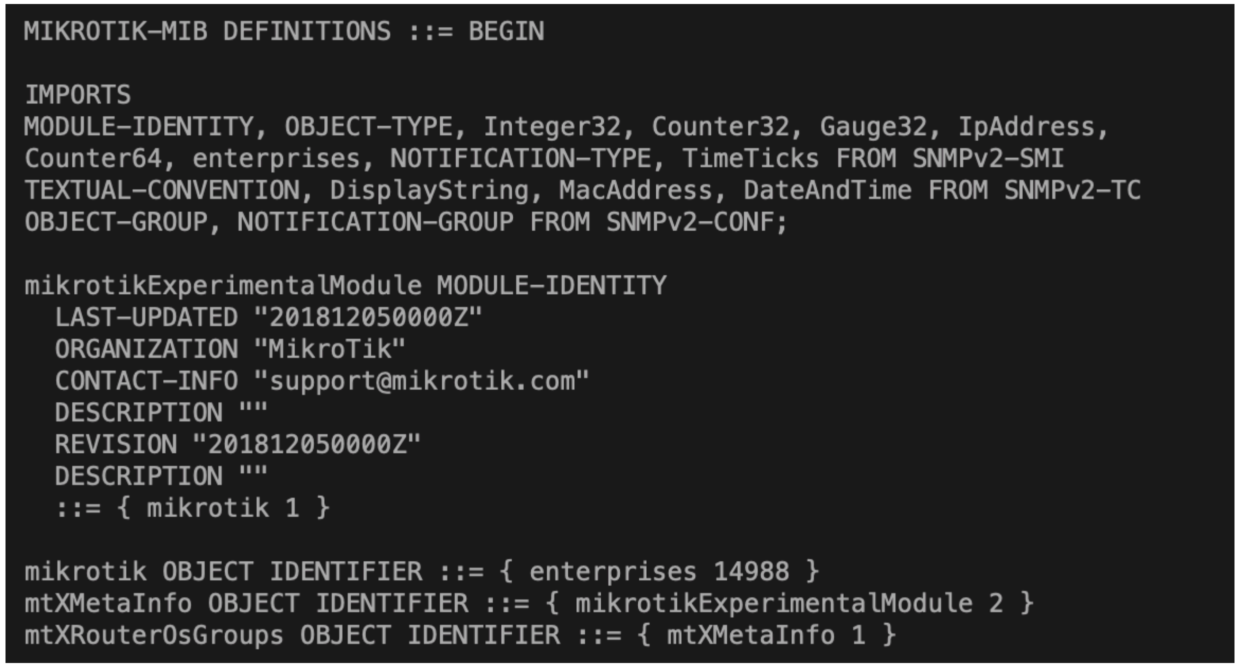


.1.3.6.1.4.1.14988.1.1.1.1.1.4.1

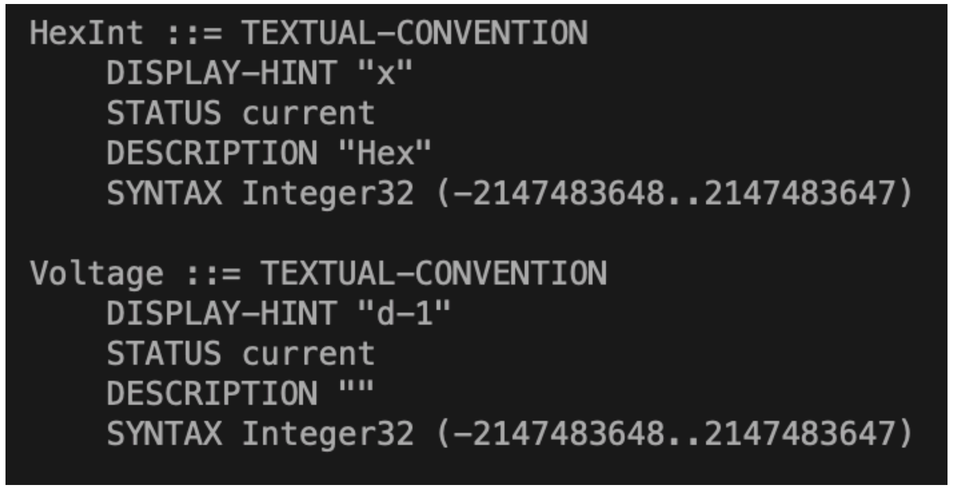
Object Identifier

MIKROTIK MIB

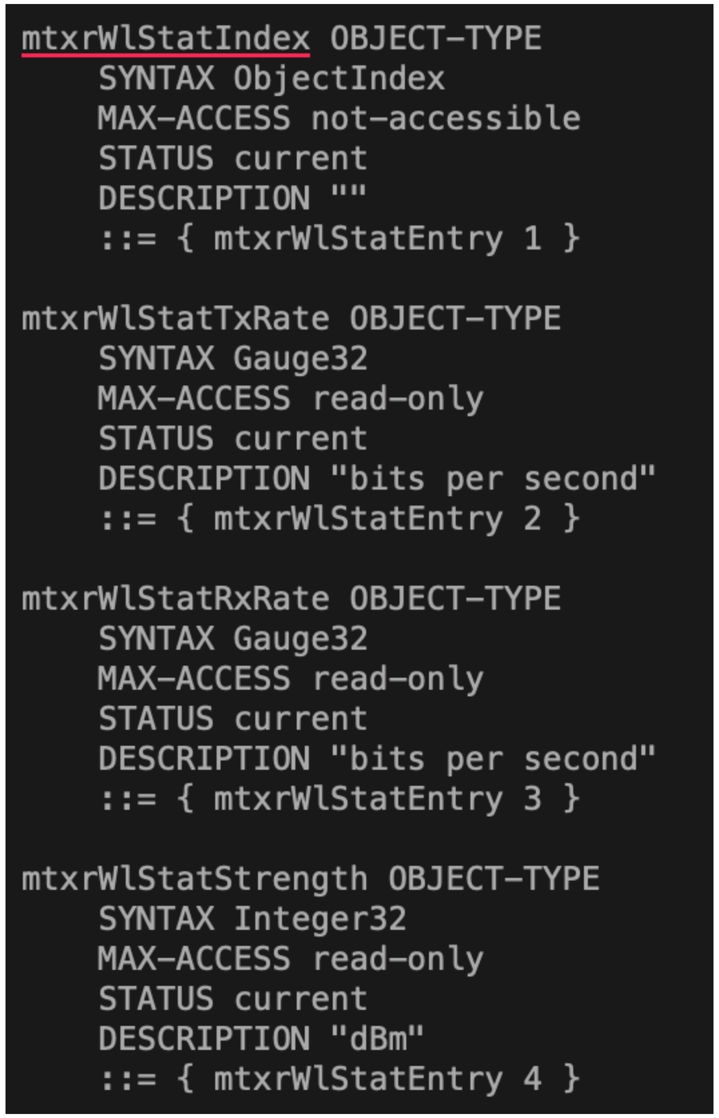
- https://wiki.mikrotik.com/wiki/Manual:SNMP
- Last updated 5 December 2018



```
MIKROTIK-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter32, Gauge32, IpAddress,
Counter64, enterprises, NOTIFICATION-TYPE, TimeTicks FROM SNMPv2-SMI
TEXTUAL-CONVENTION, DisplayString, MacAddress, DateAndTime FROM SNMPv2-TC
OBJECT-GROUP, NOTIFICATION-GROUP FROM SNMPv2-CONF;

mikrotikExperimentalModule MODULE-IDENTITY
  LAST-UPDATED "201812050000Z"
  ORGANIZATION "MikroTik"
  CONTACT-INFO "support@mikrotik.com"
  DESCRIPTION ""
  REVISION "201812050000Z"
  DESCRIPTION ""
  ::= { mikrotik 1 }

mikrotik OBJECT IDENTIFIER ::= { enterprises 14988 }
mtXMetaInfo OBJECT IDENTIFIER ::= { mikrotikExperimentalModule 2 }
mtXRouterOsGroups OBJECT IDENTIFIER ::= { mtXMetaInfo 1 }
```



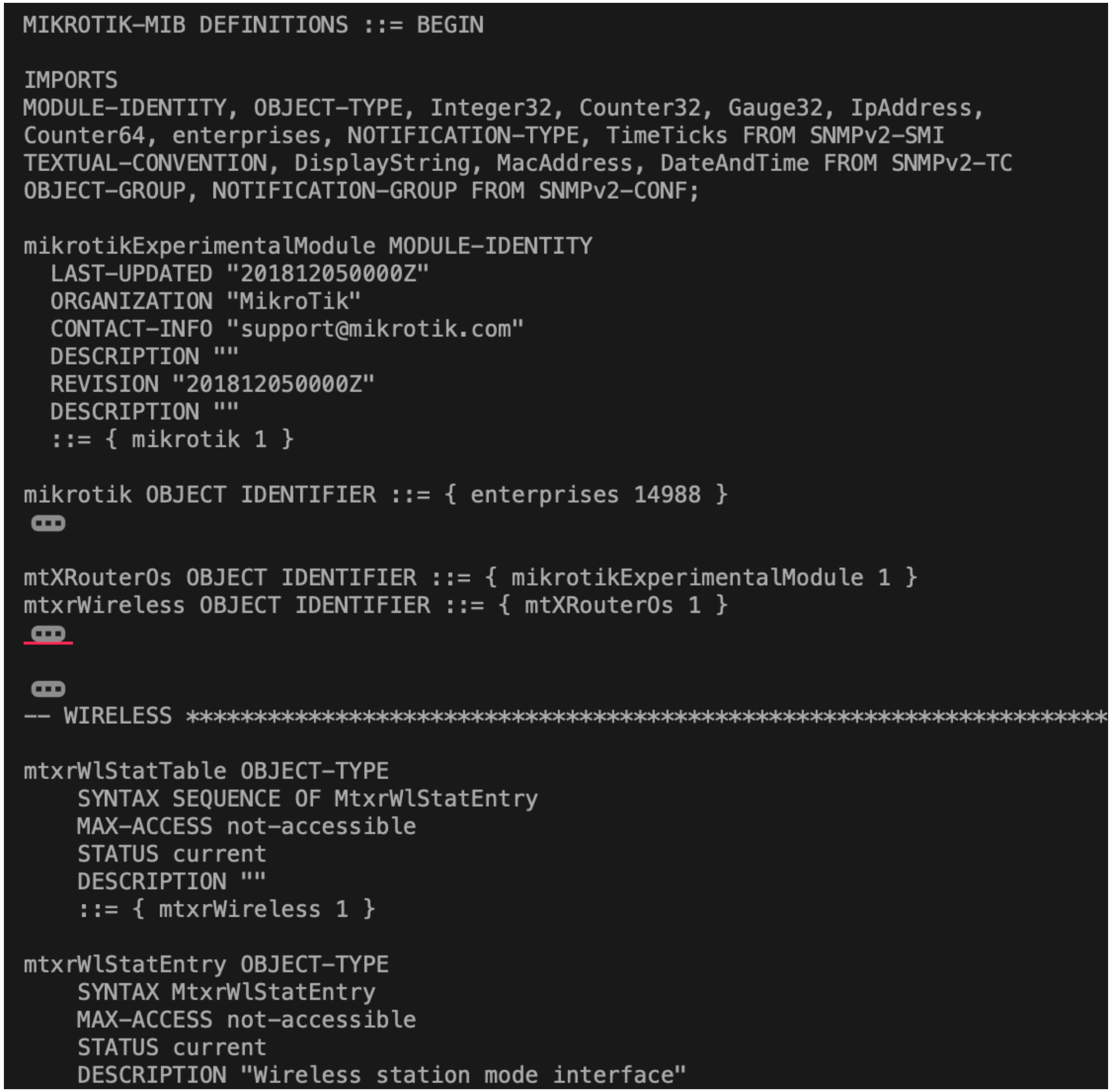
```
HexInt ::= TEXTUAL-CONVENTION
     DISPLAY-HINT "x"
     STATUS current
     DESCRIPTION "Hex"
     SYNTAX Integer32 (-2147483648..2147483647)

Voltage ::= TEXTUAL-CONVENTION
     DISPLAY-HINT "d-1"
     STATUS current
     DESCRIPTION ""
     SYNTAX Integer32 (-2147483648..2147483647)
```



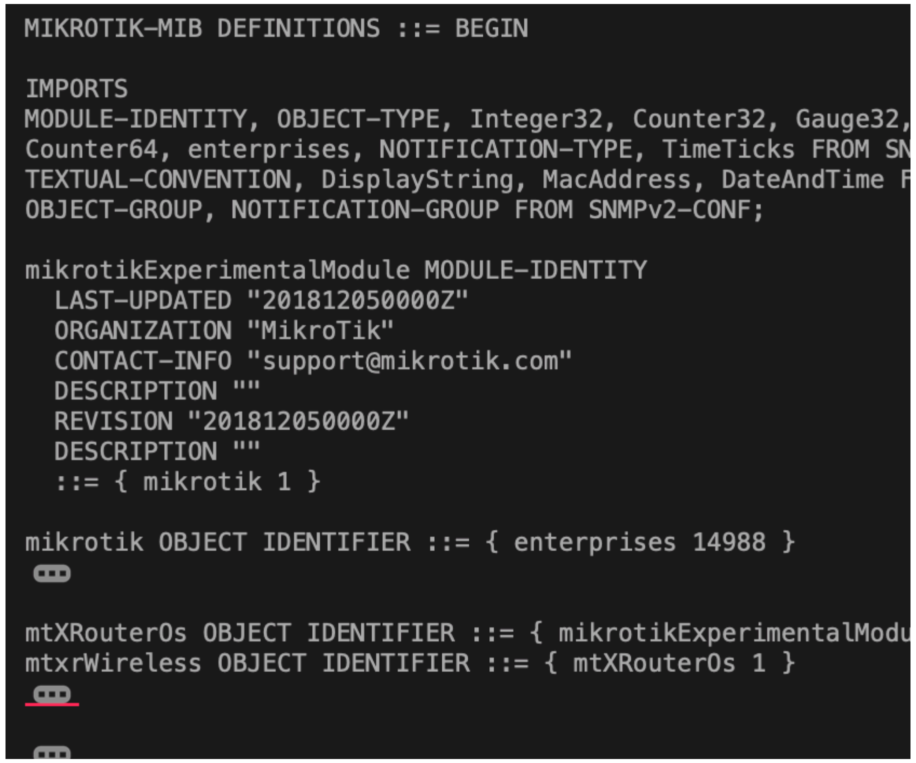
```
mtxrWlStatIndex OBJECT-TYPE
     SYNTAX ObjectIndex
     MAX-ACCESS not-accessible
     STATUS current
     DESCRIPTION ""
     ::= { mtxrWlStatEntry 1 }

mtxrWlStatTxRate OBJECT-TYPE
     SYNTAX Gauge32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION "bits per second"
     ::= { mtxrWlStatEntry 2 }

mtxrWlStatRxRate OBJECT-TYPE
     SYNTAX Gauge32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION "bits per second"
     ::= { mtxrWlStatEntry 3 }

mtxrWlStatStrength OBJECT-TYPE
     SYNTAX Integer32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION "dBm"
     ::= { mtxrWlStatEntry 4 }
```

STRUCTURE OF MANAGEMENT INFORMATION (SMI)

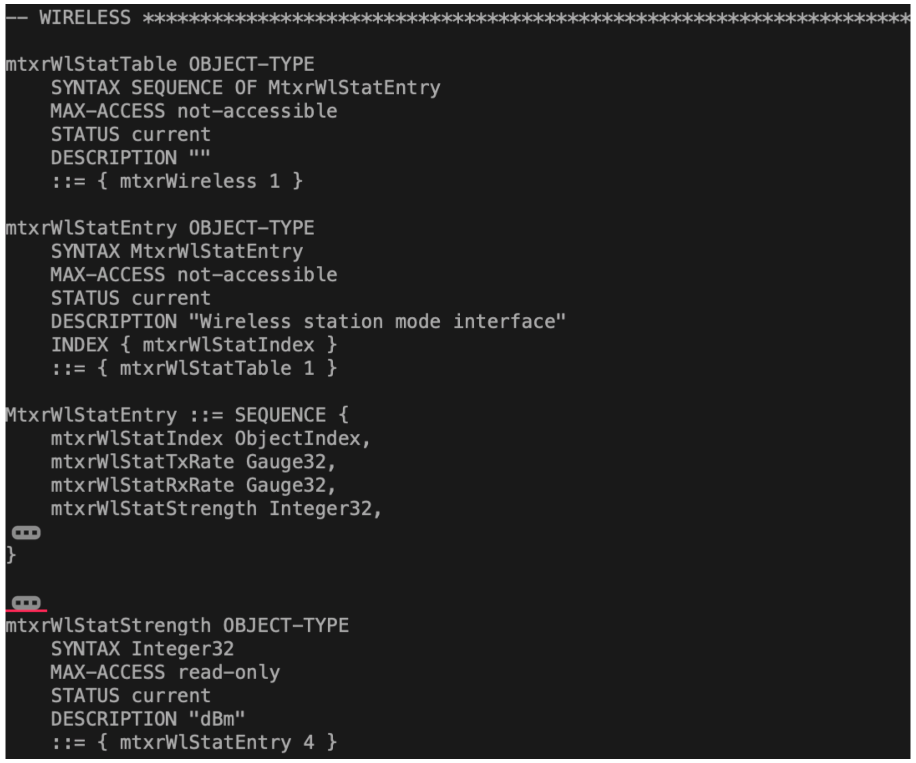
- Define rules for object:
  - Name
  - Type
  - Encoding
  - Etc



```
MIKROTIK-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter32, Gauge32, IpAddress,
Counter64, enterprises, NOTIFICATION-TYPE, TimeTicks FROM SNMPv2-SMI
TEXTUAL-CONVENTION, DisplayString, MacAddress, DateAndTime FROM SNMPv2-TC
OBJECT-GROUP, NOTIFICATION-GROUP FROM SNMPv2-CONF;

mikrotikExperimentalModule MODULE-IDENTITY
  LAST-UPDATED "201812050000Z"
  ORGANIZATION "MikroTik"
  CONTACT-INFO "support@mikrotik.com"
  DESCRIPTION ""
  REVISION "201812050000Z"
  DESCRIPTION ""
  ::= { mikrotik 1 }

mikrotik OBJECT IDENTIFIER ::= { enterprises 14988 }
 ⋯

mtXRouterOs OBJECT IDENTIFIER ::= { mikrotikExperimentalModule 1 }
mtxrWireless OBJECT IDENTIFIER ::= { mtXRouterOs 1 }
 ⋯

 ⋯
-- WIRELESS ********************************************************************

mtxrWlStatTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MtxrWlStatEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    ::= { mtxrWireless 1 }

mtxrWlStatEntry OBJECT-TYPE
    SYNTAX MtxrWlStatEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION "Wireless station mode interface"
```



```
MIKROTIK-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter32, Gauge32,
Counter64, enterprises, NOTIFICATION-TYPE, TimeTicks FROM SN
TEXTUAL-CONVENTION, DisplayString, MacAddress, DateAndTime F
OBJECT-GROUP, NOTIFICATION-GROUP FROM SNMPv2-CONF;

mikrotikExperimentalModule MODULE-IDENTITY
  LAST-UPDATED "201812050000Z"
  ORGANIZATION "MikroTik"
  CONTACT-INFO "support@mikrotik.com"
  DESCRIPTION ""
  REVISION "201812050000Z"
  DESCRIPTION ""
  ::= { mikrotik 1 }

mikrotik OBJECT IDENTIFIER ::= { enterprises 14988 }
 ⋯

mtXRouterOs OBJECT IDENTIFIER ::= { mikrotikExperimentalModu
mtxrWireless OBJECT IDENTIFIER ::= { mtXRouterOs 1 }
 ⋯

 ⋯
```



```
-- WIRELESS ********************************************************************

mtxrWlStatTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MtxrWlStatEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION ""
    ::= { mtxrWireless 1 }

mtxrWlStatEntry OBJECT-TYPE
    SYNTAX MtxrWlStatEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION "Wireless station mode interface"
    INDEX { mtxrWlStatIndex }
    ::= { mtxrWlStatTable 1 }

MtxrWlStatEntry ::= SEQUENCE {
    mtxrWlStatIndex ObjectIndex,
    mtxrWlStatTxRate Gauge32,
    mtxrWlStatRxRate Gauge32,
    mtxrWlStatStrength Integer32,
 ⋯
}

 ⋯
mtxrWlStatStrength OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "dBm"
    ::= { mtxrWlStatEntry 4 }
```

How to read MIB file??

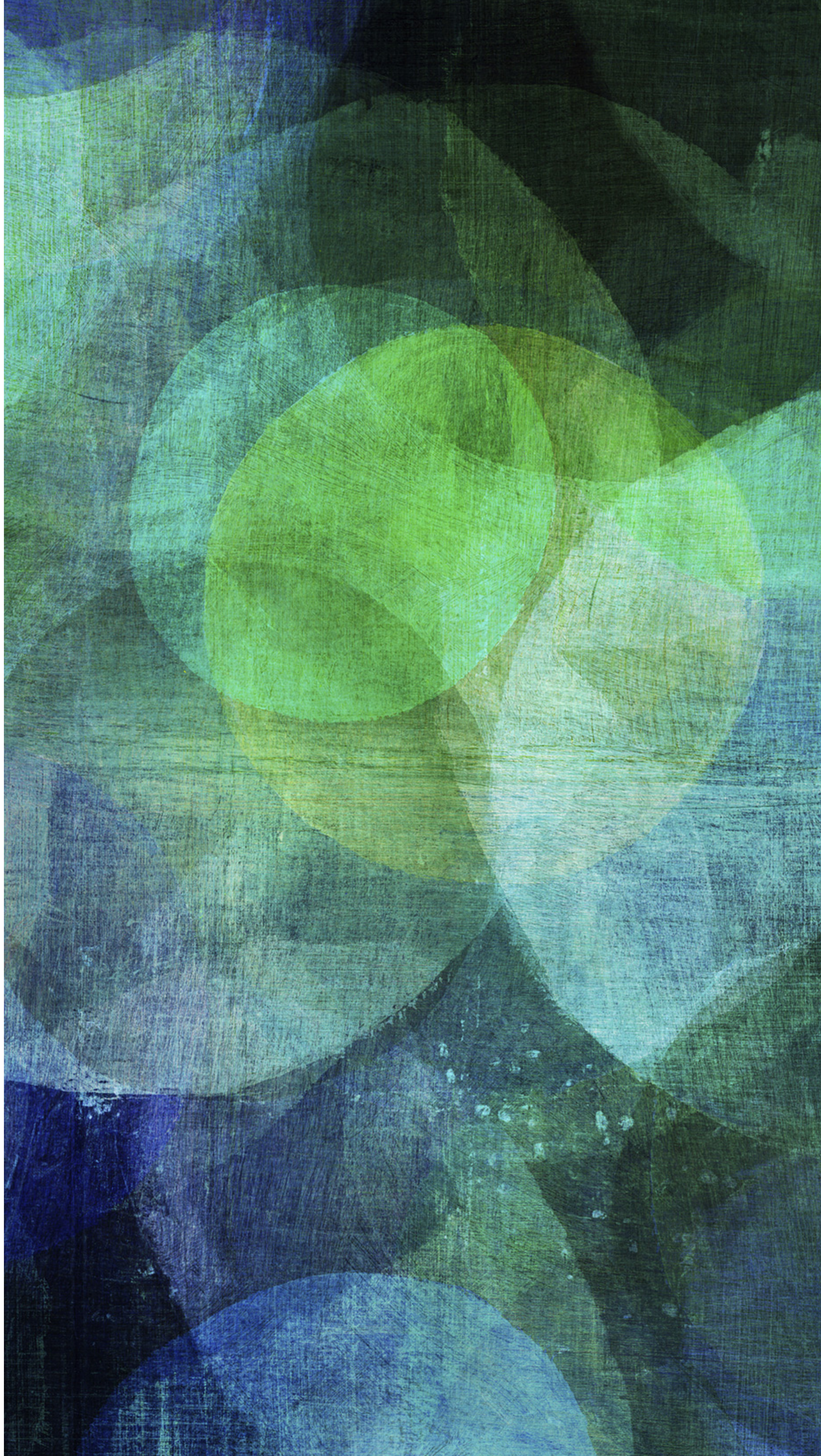
EXTERNAL SOFTWARE

- Command Line: Net-SNMP
- Visual: MRTG, Zabbix, Nagios, PRTG, etc

Demo

Getting RouterOS version via SNMP

ROUTEROS TRAFFIC FLOW

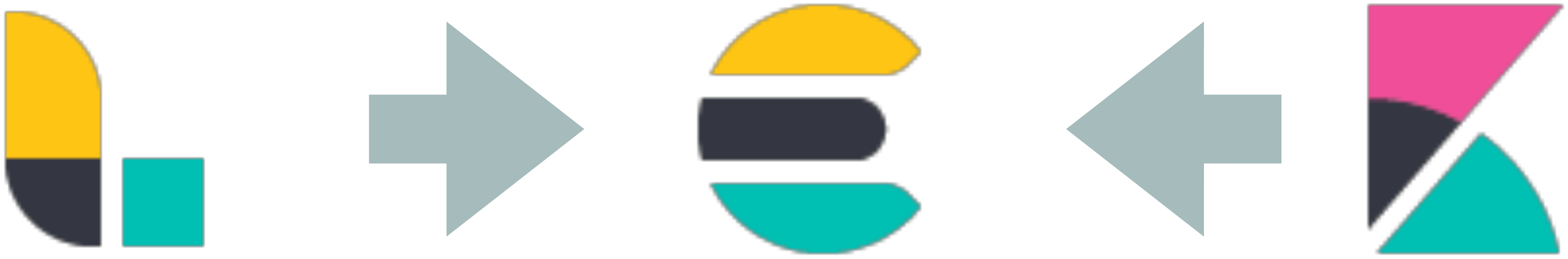


ROUTEROS TRAFFIC FLOW

- Provide statistics of network traffic
- Compatible with Cisco Netflow
- Version 1, 5 & 9

WHAT IS ELK

- ElasticSearch (Database)
- Logstash (Input)
- Kibana (Visual)



WHY ELK?

- Open Source
- SNMP information is not detailed enough
- It support more than just Flow
- Support Clustering
- Direct query into the data is possible
- High performance: 5Gbps, more than 100.000 flows

logstash

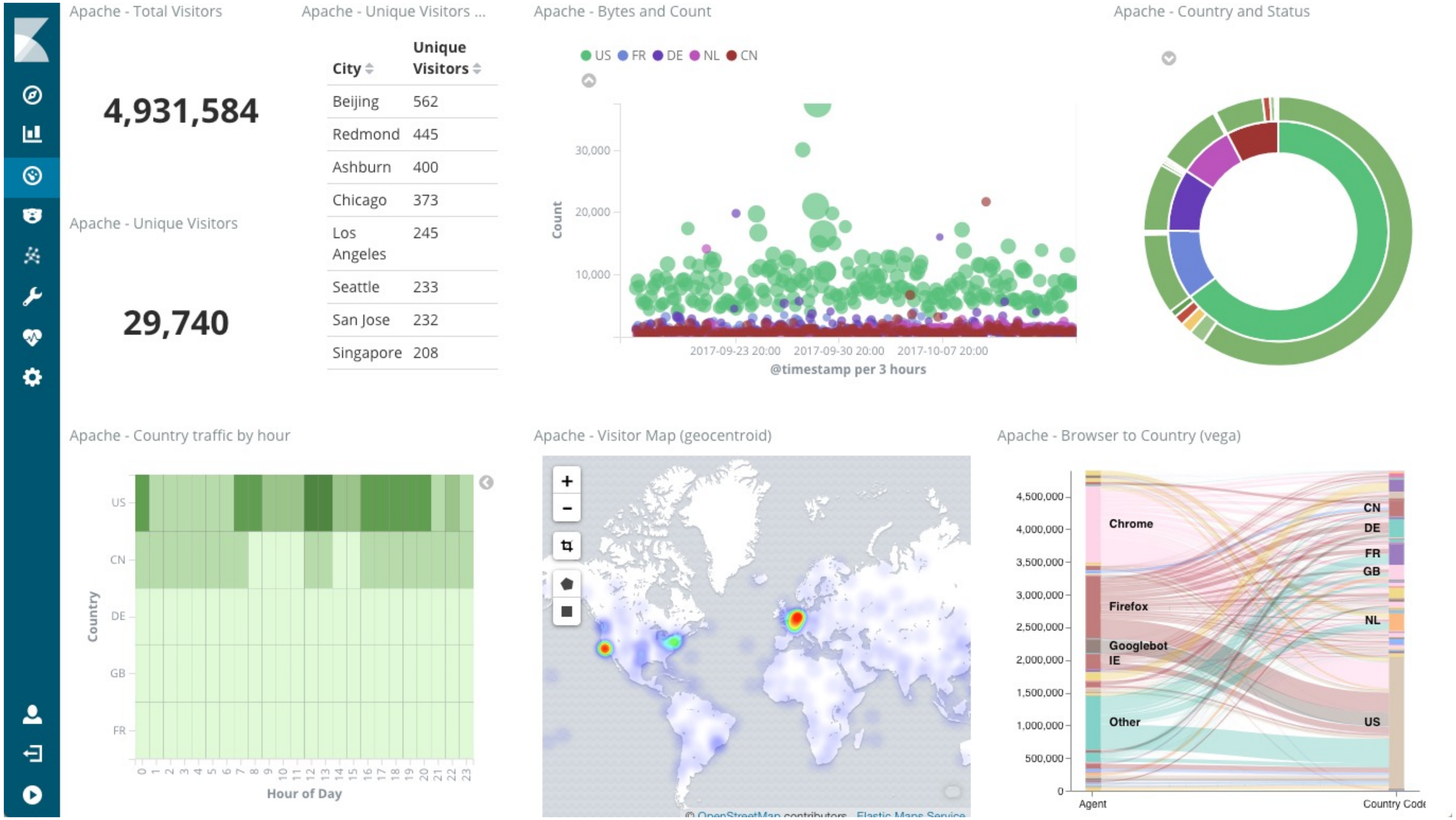
- Open Source
- Server Side data processing
- Ingest Data from multitude of sources simultaneously
- Input Plugins: https://www.elastic.co/guide/en/logstash/current/input-plugins.html
- Amazon CloudWatch & S3, File, Github Webhook, HTTP/HTTPS, SNMP & Trap, Syslog, TCP, UDP, etc
- Filters: Parse & Transform
- Output

elasticsearch

- Open Source
- Distributed, RESTful search
- Centrally store data in the ELK stack
- Really really really FAST
- Numbers, text, geo, structured, unstructured. All data types are welcome

kibana

- ➤ Open Source
- ➤ Graphical User Interface
- ➤ Created to visualise your ElasticSearch data



Apache - Total Visitors

4,931,584

Apache - Unique Visitors

29,740

Apache - Unique Visitors ...

City	Unique Visitors
Beijing	562
Redmond	445
Ashburn	400
Chicago	373
Los Angeles	245
Seattle	233
San Jose	232
Singapore	208

Apache - Bytes and Count

Apache - Country and Status

Apache - Country traffic by hour

Apache - Visitor Map (geocentroid)

Apache - Browser to Country (vega)

INSTALLATION

- Download source package, compile, install, edit config
- Binary Installation: YUM, APT, MSI, PKG
- Docker

BINARY INSTALLATION

- CentOS 7 / YUM / RPM
- Yum Repository: easy, fast, manageable

```
[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

```
$ sudo yum install elasticsearch
```

```
/etc/elasticsearch/elasticsearch.yml
```

```
network.host: localhost
```

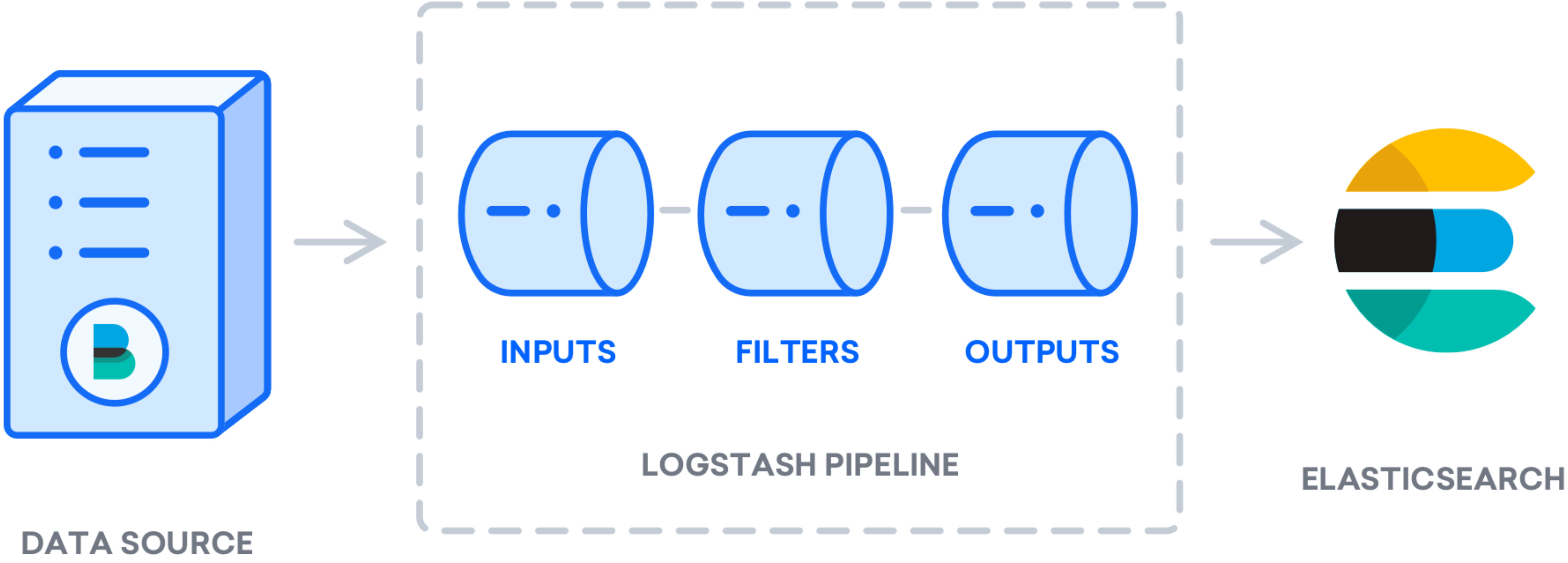
You can test whether your Elasticsearch service is running by sending an HTTP request:

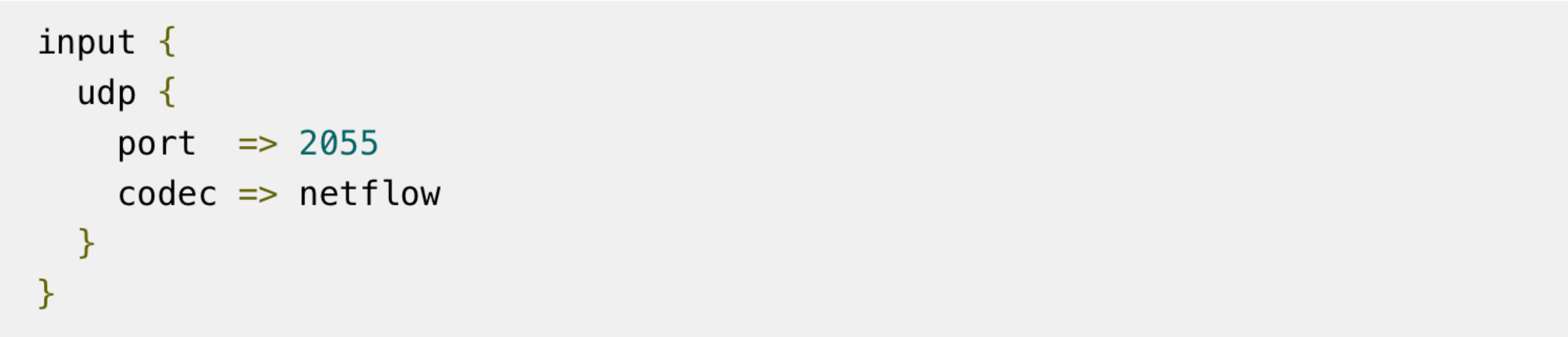
```
$ curl -X GET "localhost:9200"
```

You will see a response showing some basic information about your local node, similar to this:

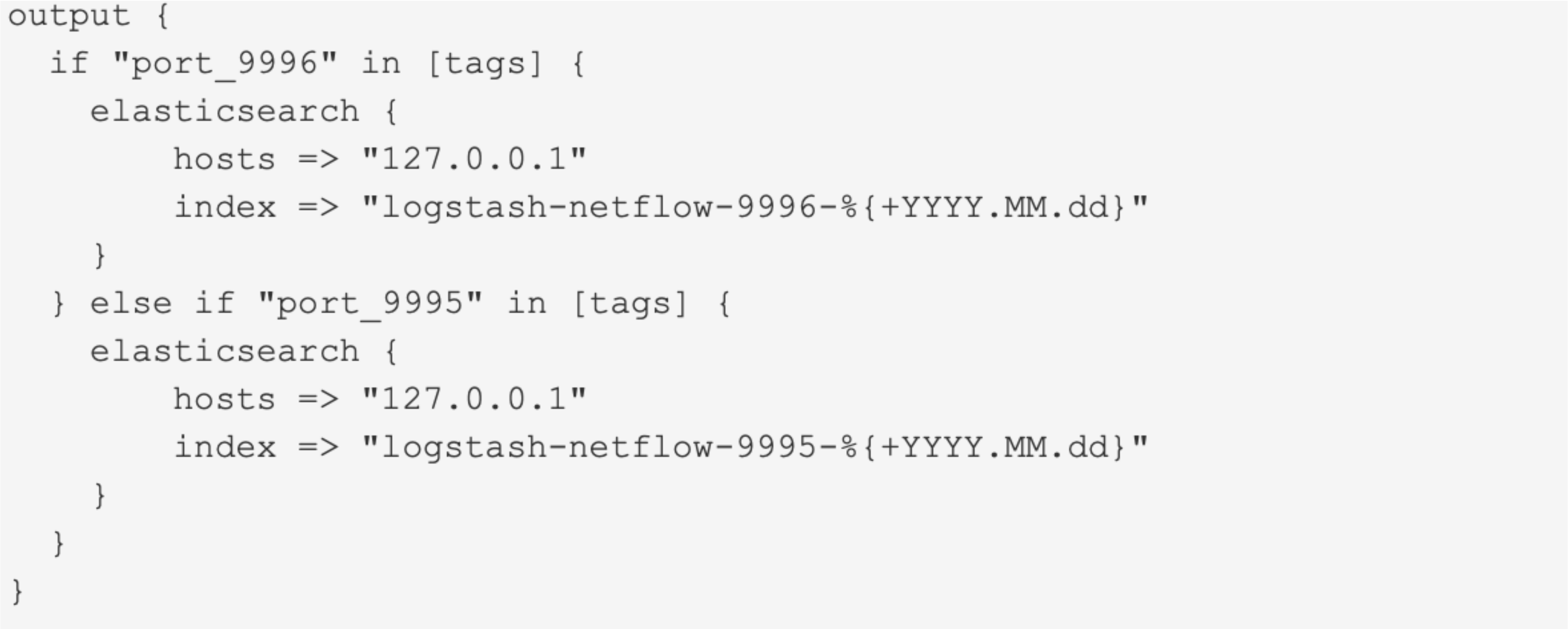
```
Output
{
  "name" : "8oSCBFJ",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "1Nf9ZymBQaOWKpMRBfisog",
  "version" : {
    "number" : "6.5.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "9434bed",
    "build_date" : "2018-11-29T23:58:20.891072Z",
    "build_snapshot" : false,
    "lucene_version" : "7.5.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

```
$ sudo yum install Logstash
```





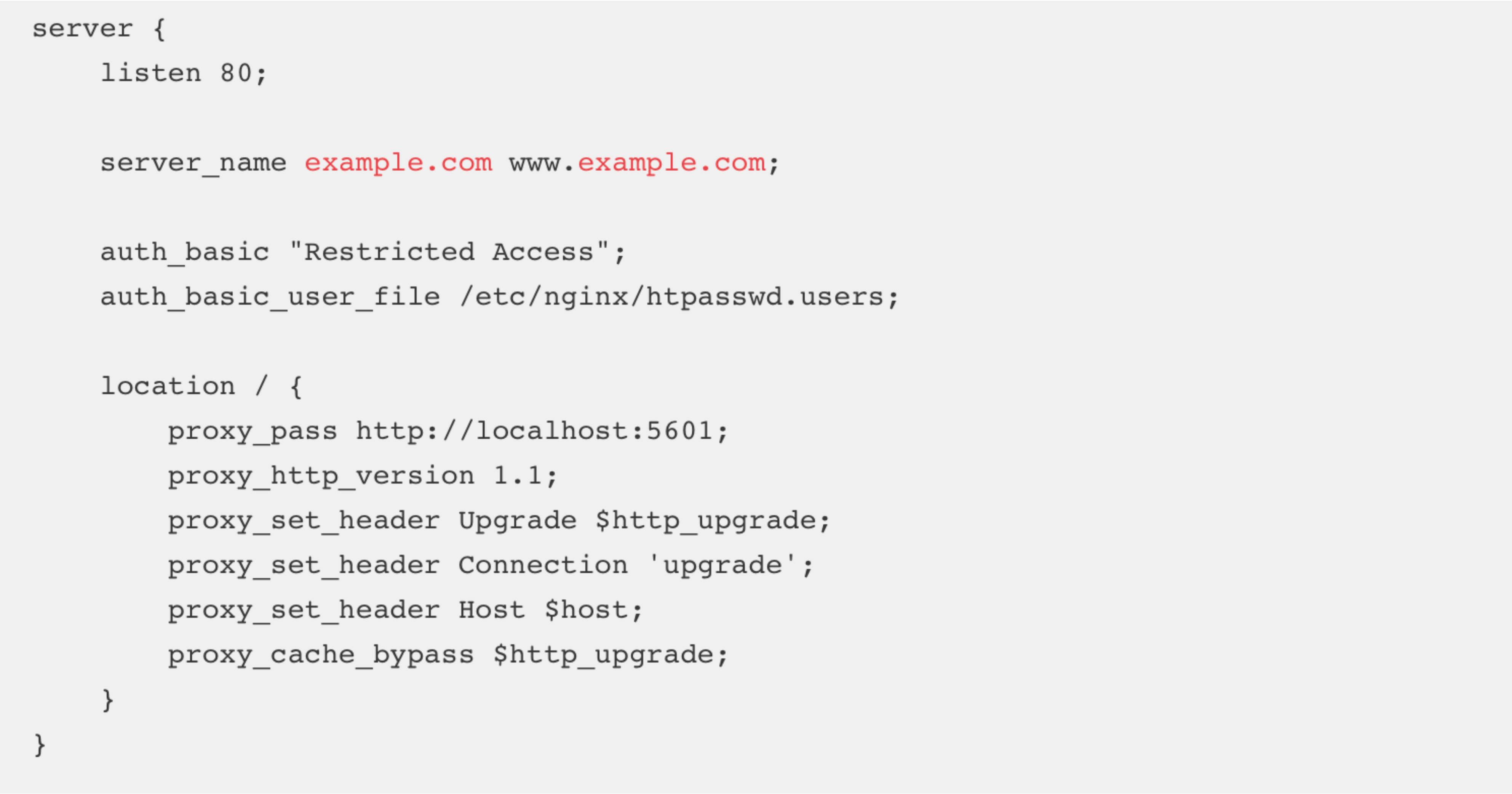
```
input {
  udp {
    port  => 2055
    codec => netflow
  }
}
```



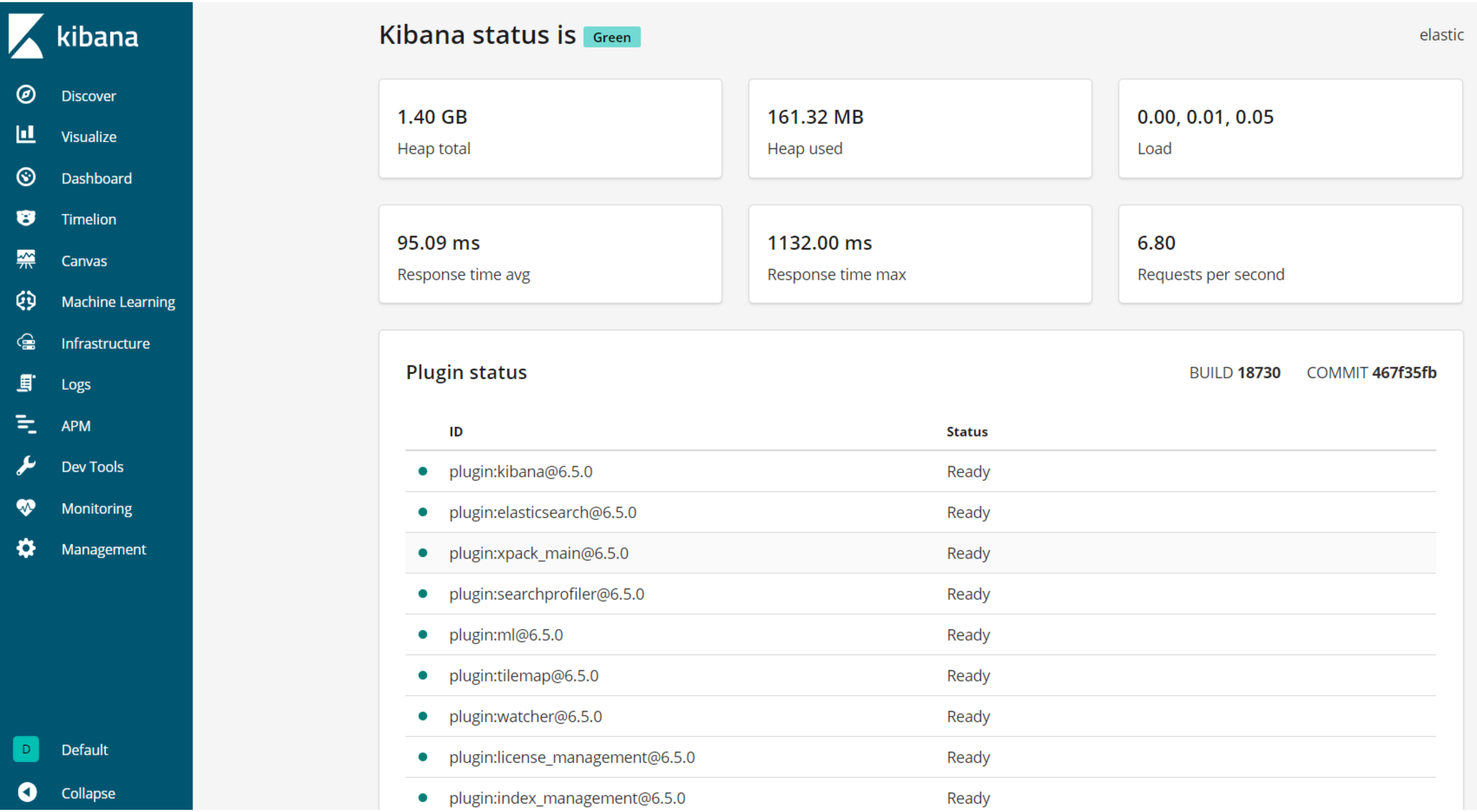
```
output {
  if "port_9996" in [tags] {
    elasticsearch {
        hosts => "127.0.0.1"
        index => "logstash-netflow-9996-%{+YYYY.MM.dd}"
    }
  } else if "port_9995" in [tags] {
    elasticsearch {
        hosts => "127.0.0.1"
        index => "logstash-netflow-9995-%{+YYYY.MM.dd}"
    }
  }
}
```

```
$ sudo yum install Kibana
```

- Run on its own port, def 561
- Use Nginx as reverse proxy



```
server {
    listen 80;

    server_name example.com www.example.com;

    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.users;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```



Kibana status is Green

1.40 GB
Heap total

161.32 MB
Heap used

0.00, 0.01, 0.05
Load

95.09 ms
Response time avg

1132.00 ms
Response time max

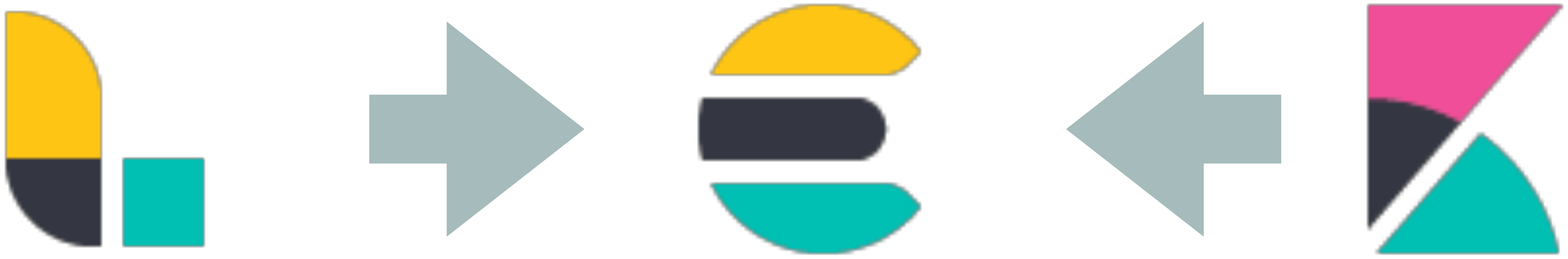
6.80
Requests per second

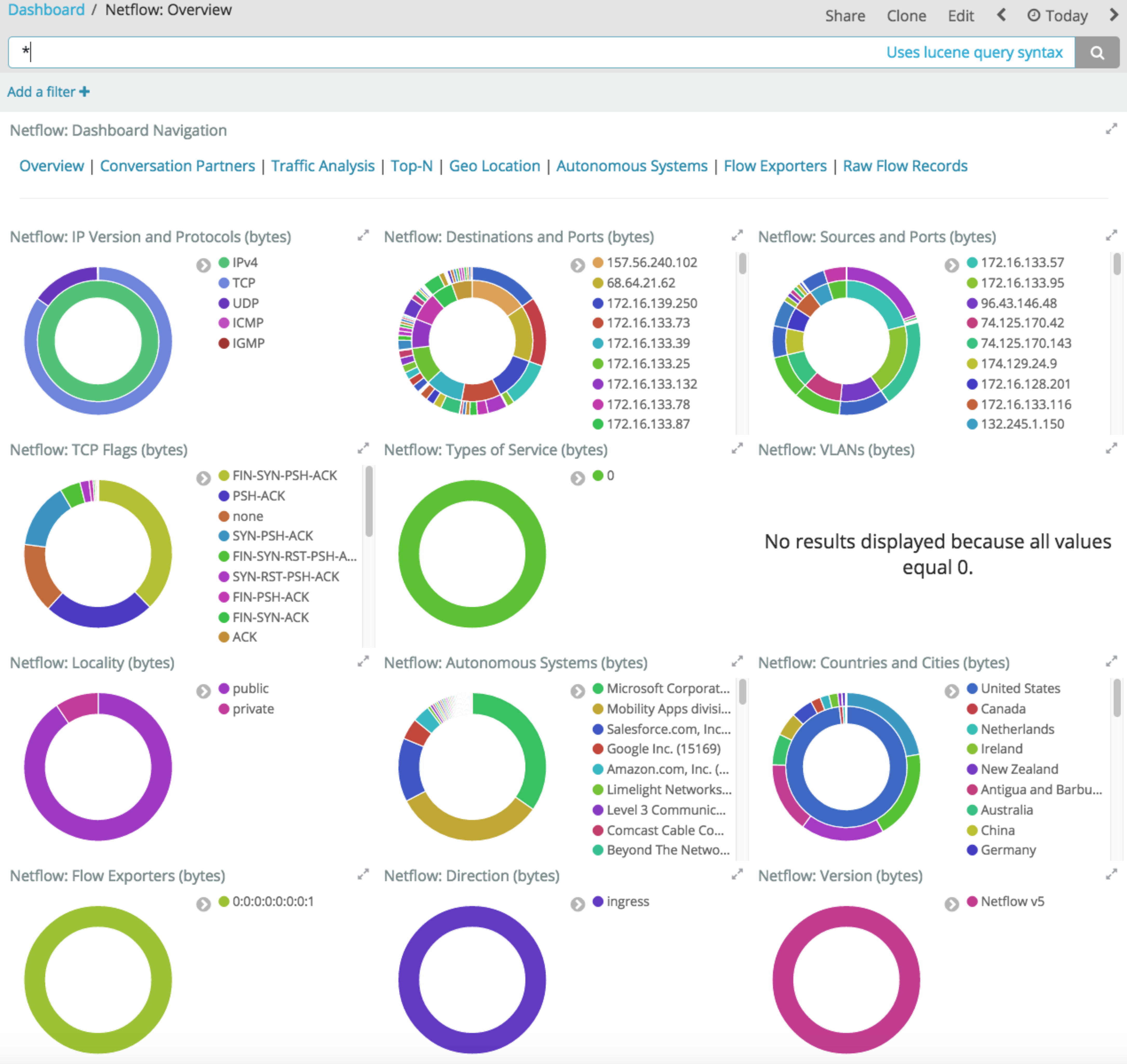
Plugin status

BUILD **18730** COMMIT **467f35fb**

	ID	Status
●	plugin:kibana@6.5.0	Ready
●	plugin:elasticsearch@6.5.0	Ready
●	plugin:xpack_main@6.5.0	Ready
●	plugin:searchprofiler@6.5.0	Ready
●	plugin:ml@6.5.0	Ready
●	plugin:tilemap@6.5.0	Ready
●	plugin:watcher@6.5.0	Ready
●	plugin:license_management@6.5.0	Ready
●	plugin:index_management@6.5.0	Ready

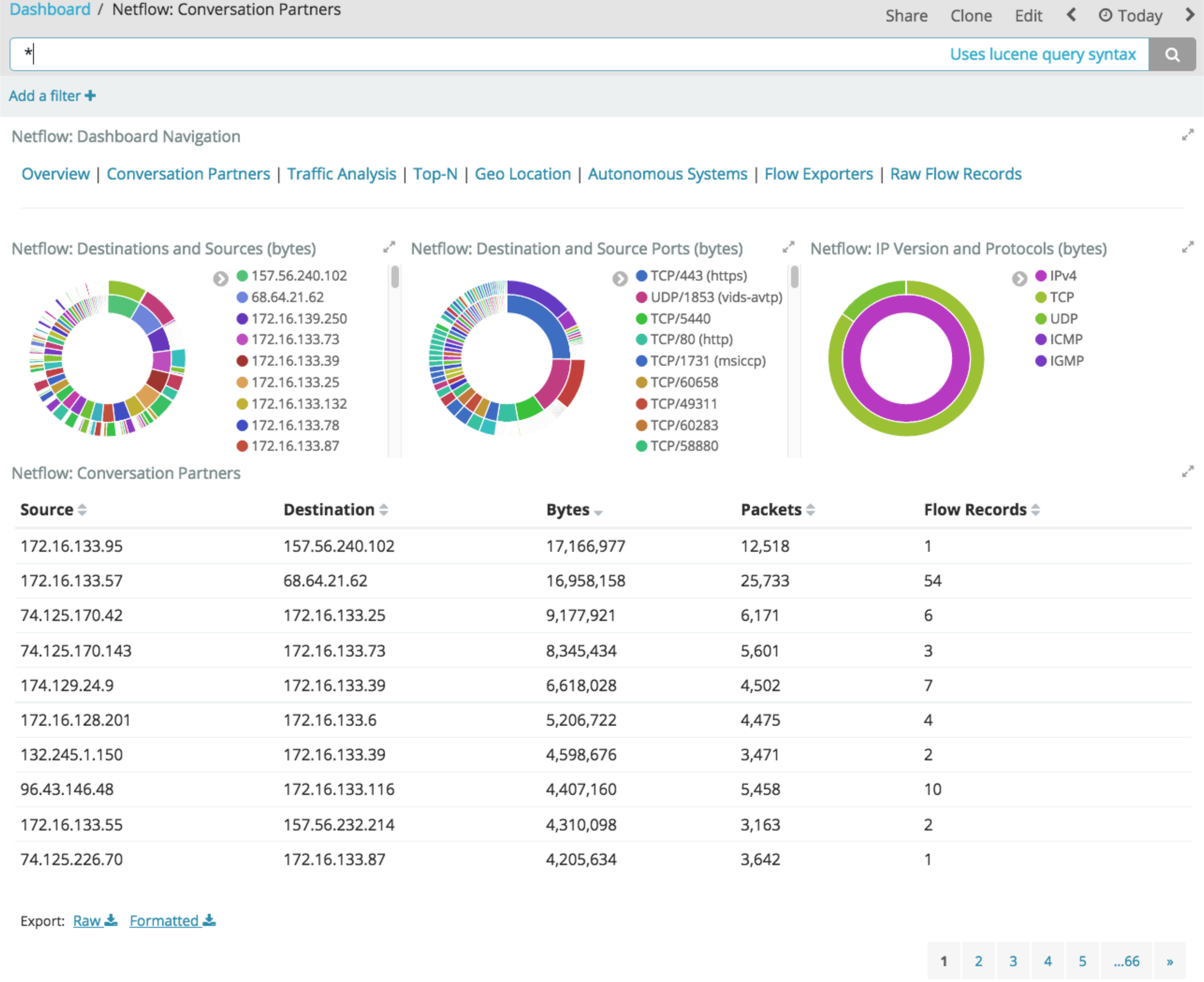
LOGSTASH + ELASTICSEARCH + KIBANA





*

No results displayed because all values equal 0.



Dashboard / Netflow: Conversation Partners

Share Clone Edit ‹ Today ›

*

Uses lucene query syntax

Add a filter +

Netflow: Dashboard Navigation

Overview | Conversation Partners | Traffic Analysis | Top-N | Geo Location | Autonomous Systems | Flow Exporters | Raw Flow Records

Netflow: Destinations and Sources (bytes)

- ● 157.56.240.102
- ● 68.64.21.62
- ● 172.16.139.250
- ● 172.16.133.73
- ● 172.16.133.39
- ● 172.16.133.25
- ● 172.16.133.132
- ● 172.16.133.78
- ● 172.16.133.87

Netflow: Destination and Source Ports (bytes)

- ● TCP/443 (https)
- ● UDP/1853 (vids-avtp)
- ● TCP/5440
- ● TCP/80 (http)
- ● TCP/1731 (msiccp)
- ● TCP/60658
- ● TCP/49311
- ● TCP/60283
- ● TCP/58880

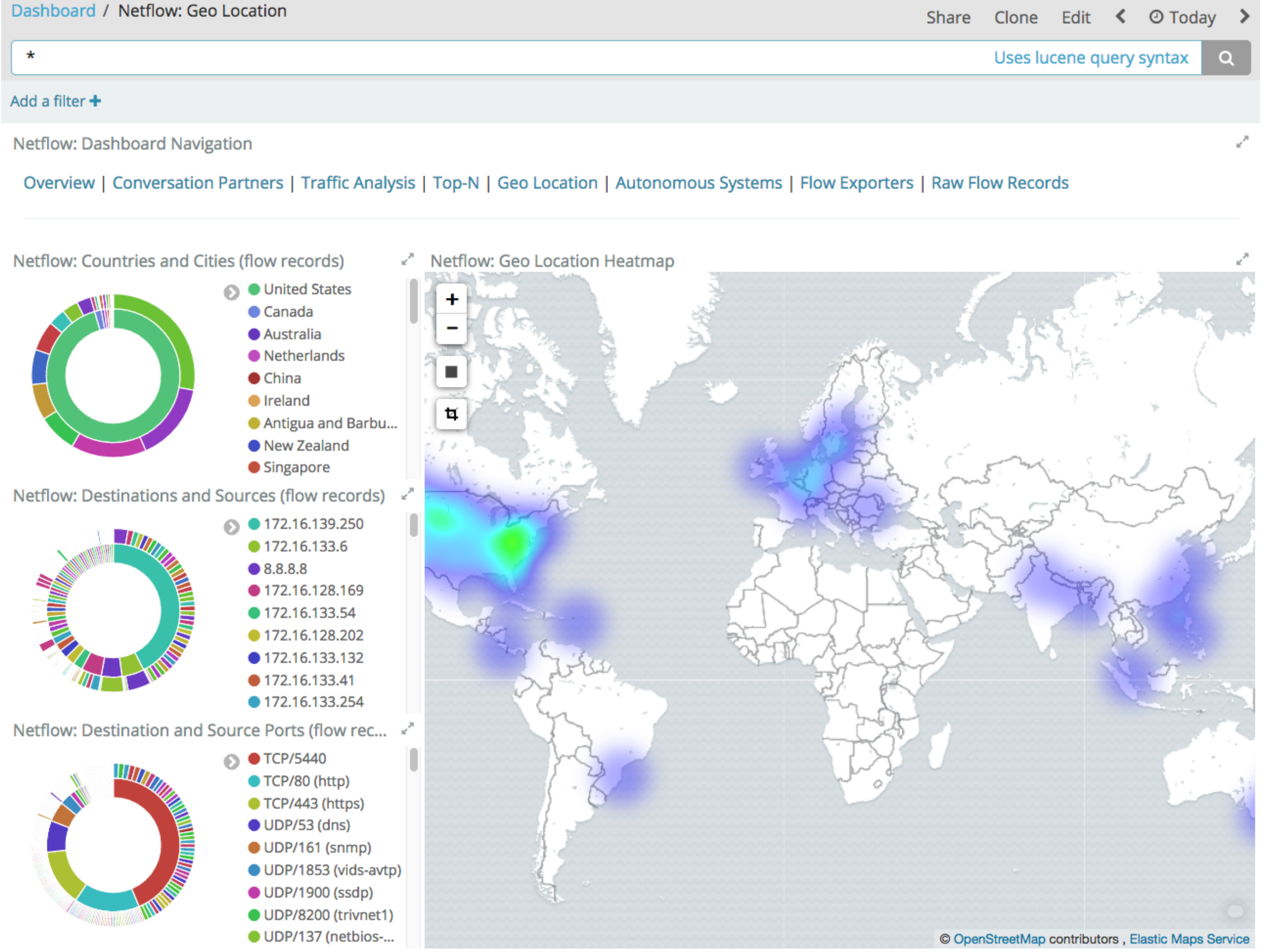
Netflow: IP Version and Protocols (bytes)

- ● IPv4
- ● TCP
- ● UDP
- ● ICMP
- ● IGMP

Netflow: Conversation Partners

Source	Destination	Bytes	Packets	Flow Records
172.16.133.95	157.56.240.102	17,166,977	12,518	1
172.16.133.57	68.64.21.62	16,958,158	25,733	54
74.125.170.42	172.16.133.25	9,177,921	6,171	6
74.125.170.143	172.16.133.73	8,345,434	5,601	3
174.129.24.9	172.16.133.39	6,618,028	4,502	7
172.16.128.201	172.16.133.6	5,206,722	4,475	4
132.245.1.150	172.16.133.39	4,598,676	3,471	2
96.43.146.48	172.16.133.116	4,407,160	5,458	10
172.16.133.55	157.56.232.214	4,310,098	3,163	2
74.125.226.70	172.16.133.87	4,205,634	3,642	1

Export: Raw Formatted



Dashboard / Netflow: Geo Location

Share Clone Edit ‹ Today ›

*

Uses lucene query syntax

Add a filter +

Netflow: Dashboard Navigation

Overview | Conversation Partners | Traffic Analysis | Top-N | Geo Location | Autonomous Systems | Flow Exporters | Raw Flow Records

Netflow: Countries and Cities (flow records)

- ● United States
- ● Canada
- ● Australia
- ● Netherlands
- ● China
- ● Ireland
- ● Antigua and Barbu...
- ● New Zealand
- ● Singapore

Netflow: Destinations and Sources (flow records)

- ● 172.16.139.250
- ● 172.16.133.6
- ● 8.8.8.8
- ● 172.16.128.169
- ● 172.16.133.54
- ● 172.16.128.202
- ● 172.16.133.132
- ● 172.16.133.41
- ● 172.16.133.254

Netflow: Destination and Source Ports (flow rec...

- ● TCP/5440
- ● TCP/80 (http)
- ● TCP/443 (https)
- ● UDP/53 (dns)
- ● UDP/161 (snmp)
- ● UDP/1853 (vids-avtp)
- ● UDP/1900 (ssdp)
- ● UDP/8200 (trivnet1)
- ● UDP/137 (netbios-...

Netflow: Geo Location Heatmap

© OpenStreetMap contributors , Elastic Maps Service

SINGAPORE MIKROTIK USER GROUP

- March 8th 2019
- ELK Stack + MikroTik Router
- https://www.meetup.com/MikroTik-User-Group-Singapore-MUG-SG/events/257894335/

Question?

📱 *Approach me :)*

✉ *soragan.ong@alagasnetwork.com*

f *soragan.ong*

✈ *@sguox*