

MikroTik Traffic Flow

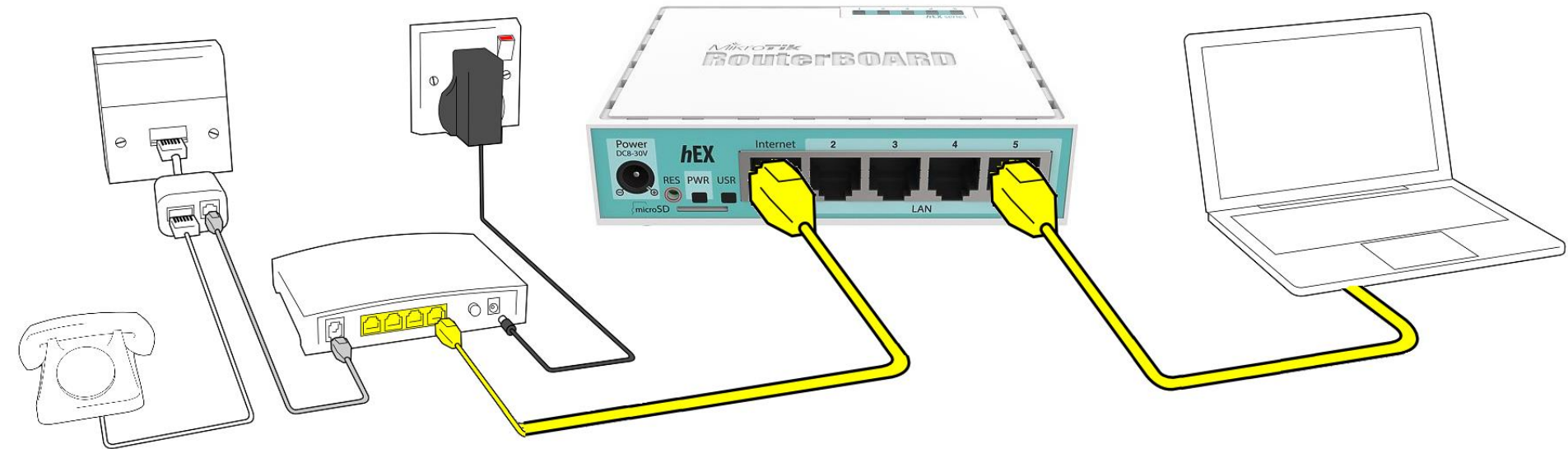
Network Monitoring / PRTG

MikroTik User Meeting

26-January-2019

Beirut - Lebanon

MikroTik RouterOS is rich in many features

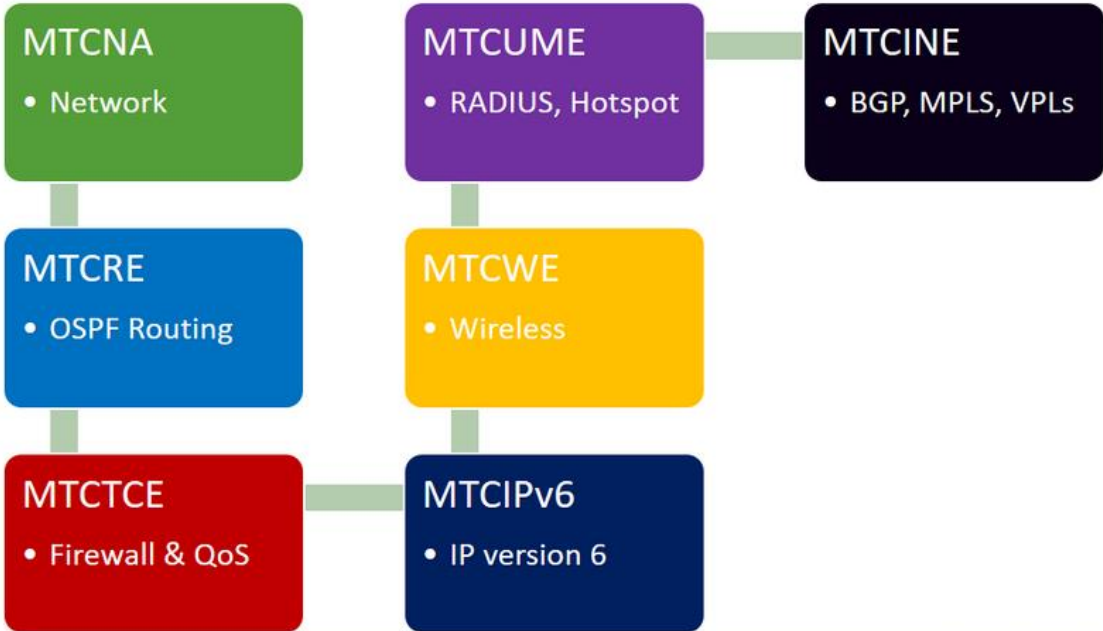


About me, the MikroTik Certified Trainer

- Name: Khalil Chamseddine
- Experience: Software, Hardware and Networking
- MikroTik Certified Trainer in Lebanon and Region:
 - MTCNA
 - MTCWE
 - MTCTCE
 - MTCUME
 - MTCRE
 - MTCIPv6
 - MTCINE
- Contact:
 - <https://Tahandos.com>
 - E-Mail: khalil@tahandos.com
 - Phone: +961-3-892792



All MikroTik Certifications – 4 weeks



7 certifications - Flexible Schedule



MikroTik MikroTik
Certified Trainer Certified Consultant



Networking - Routing - Traffic Control
Firewall - Gateway - Bandwidth - VPN

Outline

- Network Monitoring and FLOW
- MikroTik Traffic Flow
- MikroTik RouterOS and PRTG
 - How To, Step By Step
 - Sample Reporting

Simple question: What do we want to know?

- Who is consuming the bandwidth?
 - From inside out
 - From outside in

- What they are consuming?

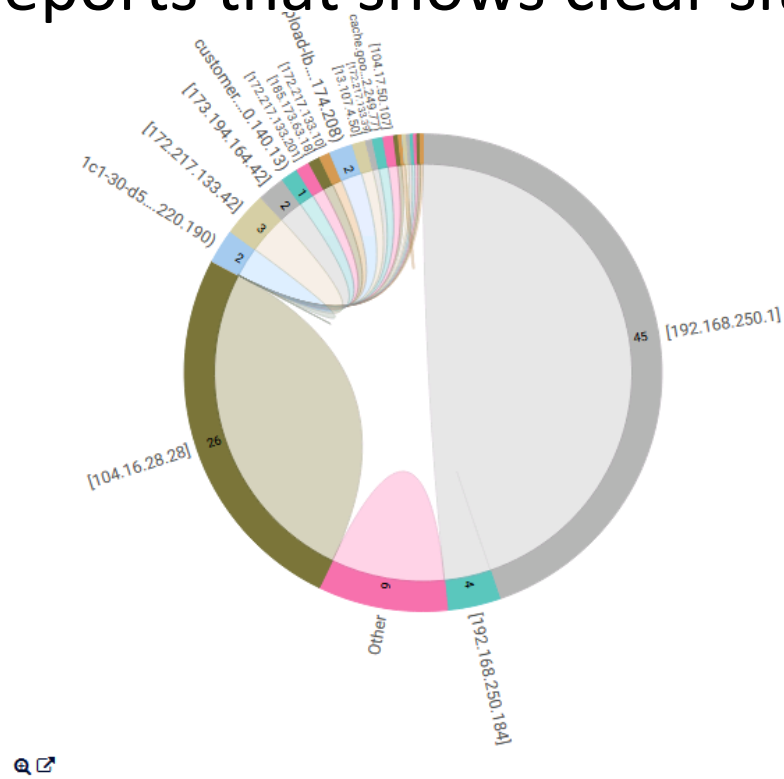
- Which protocols and services?
 - HTTP
 - Email
 - Video
 - Voice
 - Torrent
 - ...

Simple question: Why do we want to know?

- Identification / Solving
 - Traffic Classification
 - Flow-based detection
 - DoS Trace back
 - ...
- Traffic Analysis
 - Inter-AS traffic analysis
 - Reporting on application proxies
 - ...
- Accounting
 - Cross verification from other sources
 - ...

Simple question: What do we need to get?

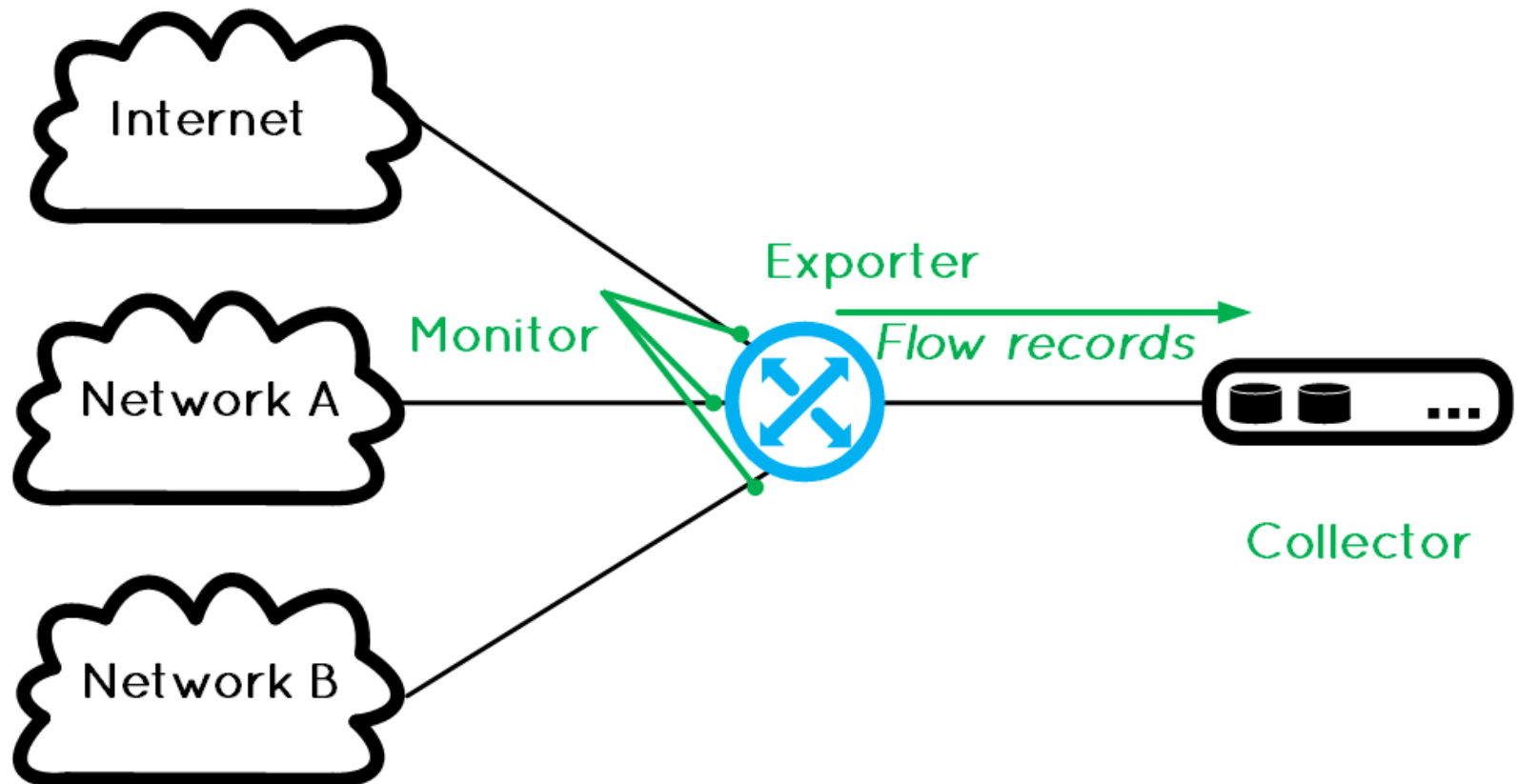
- Nice presented reports that shows clear situation



Source IP	Source Port	Destination IP	Destination Port	Protocol	Channel	IP	Port	Sender IP	Bytes
a23-56-177-96.de...	443	[192.168.1.64]	52935	TCP	WWW	a23-56-177-96.de...	443	[10.111.222.33]	2,238 KByte
[185.173.63.18]	443	[192.168.1.64]	52396	TCP	WWW	[192.168.1.64]	52396	[10.111.222.33]	2,220 KByte
cloudproxy10113...	443	[192.168.1.64]	55504	TCP	WWW	cloudproxy10113...	443	[10.111.222.33]	2,201

How we are supposed to know it?

- Observation Point / Interface
- Flow Exporter: Exports Flow Records
- Flow Collector: Receives Flow Records / present them nicely



Bandwidth Monitoring Alternatives

- Bandwidth monitoring is a method for measuring the actual bandwidth available on a local system
- SNMP
 - Usually it is considered lighter than other options
 - Gets total amount of traffic and some layer 2 and layer 3 statistics like number of errors, number of broadcasts...
- Packet Sniffer
- ...
- xFlow

General Flow Definition

- A flow is defined as a set of packets having common properties:
 - one or more packet header fields (e.g. destination IP address, transport header field),
 - one or more characteristics of the packet
 - ...
- a packet belongs to a flow record if it completely matches all defined flow properties.

Flow Exporting Protocols

- CISCO NetFlow
- Juniper...
- HPE...
- IETF IPFIX

- MikroTik Traffic Flow
 - a system that provides statistic information about packets which pass through the router.
 - network monitoring and accounting
 - identify various problems that may occur in the network
 - analyze, optimize the overall network performance
 - MikroTik Traffic-Flow is compatible with Cisco NetFlow, it can be used with various utilities which are designed for Cisco's NetFlow.

NetFlow Flow definition

- NetFlow defines a flow as the combination of the following seven key-fields:
 - Source IP address.
 - Destination IP address.
 - Source port number.
 - Destination port number.
 - Layer 3 protocol type.
 - ToS byte
 - Logical interface, whether input (ingress) or output (egress)

Flow formats

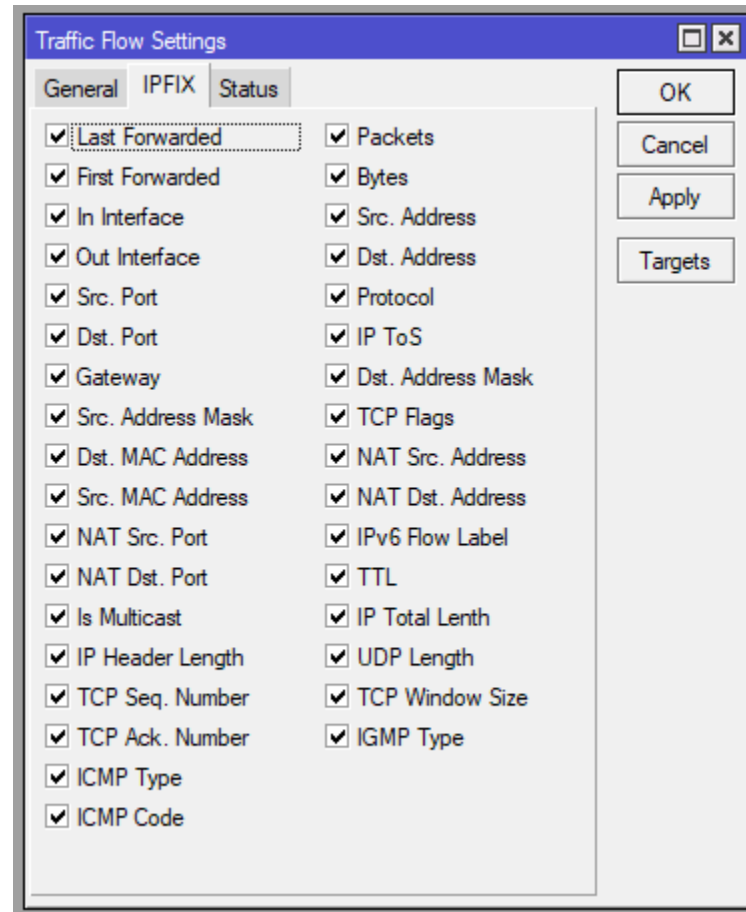
- Differ in the format of the export message
- Version 1 - never use it 😊
- Version 5 – limited to inbound traffic (ingress) and IPv4.
- Version 9 - a new format which can be extended with new fields and record types because of its template-style design
 - Version 9 is independent of the underlying transport protocol whether it is TCP, UDP, or SCTP
 - Support for IPv6 and bi-directional flows (ingress and egress)
 - Support for MPLS/VLAN...

IPFIX: IP Flow Information Export

- IETF: Internet Engineering Task Force
- IPFIX: Official Standard for all flow technologies
 - Sometimes described as NetFlow Version 10
 - used CISCO NetFlow version 9 as a base
 - common, universal standard of export for Internet Protocol flow information from routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing
 - defines how IP flow information is to be formatted and transferred from an exporter to a collector
- IPFIX is a push protocol, i.e. each sender will periodically send IPFIX messages to configured receivers without any interaction by the receiver.

MikroTik IPFIX

- MikroTik Traffic Flow template

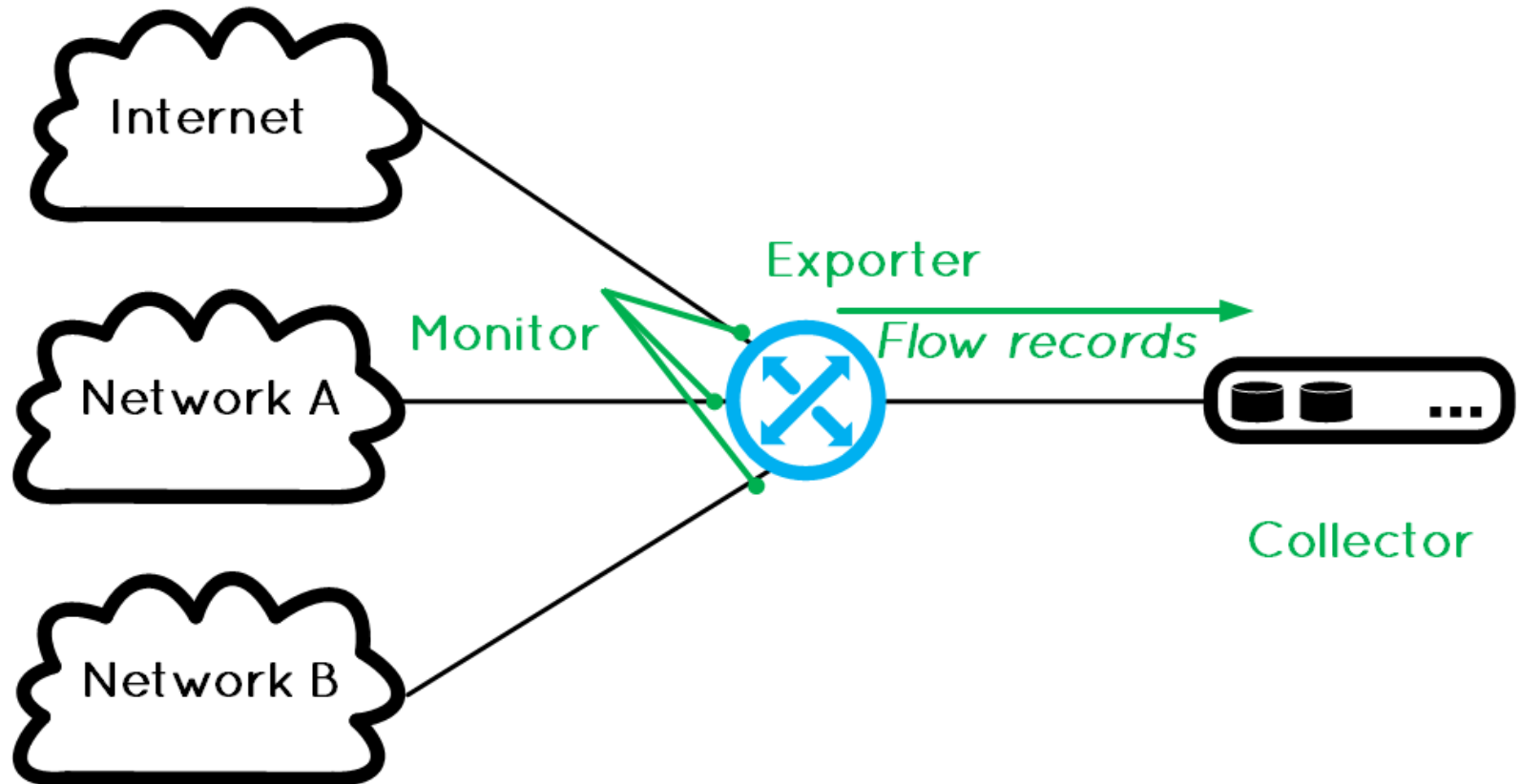


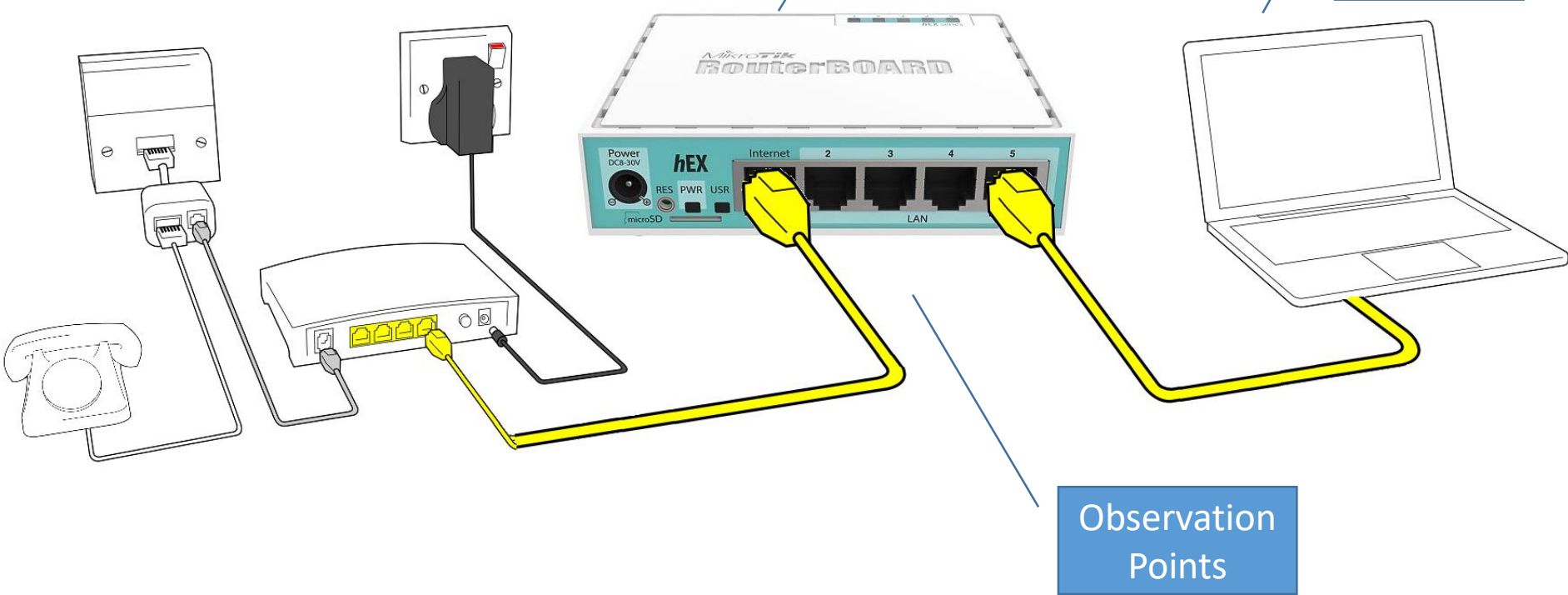
How To

- Configure the Exporter (MikroTik)
- Configure the Flow Record (MikroTik)
- Apply it to the Interface (MikroTik)
- Configure the Flow Monitor (PRTG)

How we are supposed to know it?

- Observation Point / Interface
- Flow Exporter: MikroTik RouterBoard
- Flow Collector: PRTG





PRTG, the collector

- PRTG Network Monitor
 - PRTG: Paessler Router Traffic Grapher
 - Agentless network monitoring software
 - German Company: Paessler AG
 - First release: 2003

- PRTG is a full-service monitoring solution
 - It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications



PRTG, the collector

- Sensors
 - over 200 different predefined sensors
 - application sensors and hardware-specific sensors
- Web Interface and Desktop Client
 - AJAX-based web interface
 - desktop application for Windows and macOS (beta status)
- Notifications and Reports
 - Email and SMS
 - push notification on smartphones using an app
 - customizable reports
- Pricing
 - based on sensors
 - 100 integrated sensors is available free of charge
 - Usually, each MikroTik Traffic-Flow device represents one sensor

PRTG, IPFIX Sensor

- The IPFIX sensor receives traffic data from MikroTik Traffic-Flow and shows traffic by type. It filters traffic into different channels:
 - Chat (IRC, AIM)
 - Citrix
 - FTP/P2P (file transfer)
 - Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
 - Mail (mail traffic: IMAP, POP3, SMTP)
 - NetBIOS
 - Remote control (RDP, SSH, Telnet, VNC)
 - WWW (web traffic: HTTP, HTTPS)
 - Total traffic
 - Other protocols (other UDP and TCP traffic)

PRTG Download and Install

- Go to <https://www.paessler.com/>
- Download PRTG (prtg.zip) and extract it; save the License name and key in a text file for later use
- Run the executable install. Steps are easy to follow.
 - Enter an email address to receive alerts
- When installation is complete
 - Login, Watch the video that pops up, change the password, set the SSL; it is yours to discover.. A lot of helping pop ups.. Read and follow..

Your PRTG License Name

prtgtrial

Your PRTG License Key

000014-192KFM-8FFHZB-Z14TQJ-X2FKN4-
DAU5ZG-5Q7JZJ-3XGQUX-D1AAAD-
2DDW7B

If your PRTG download didn't start automatically:

DOWNLOAD PRTG



PRTG
NETWORK
MONITOR

PRTG Network Monitor

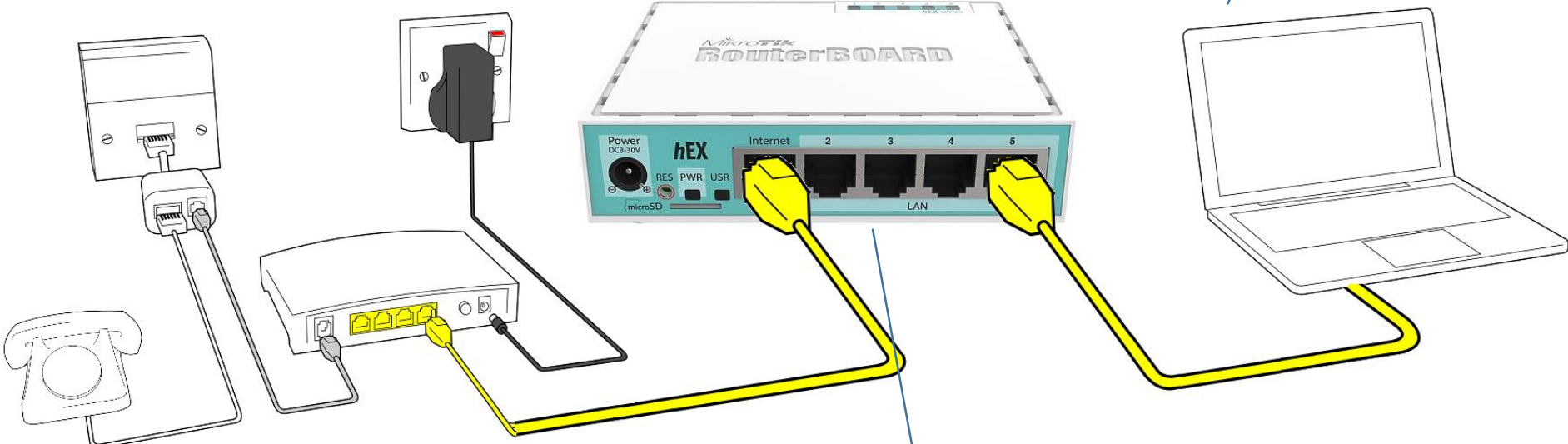
```
8:20:11 AM Init License
8:20:11 AM Init License Done
8:20:11 AM - 0% - Starting PRTG Core Server (1/1/2019)
8:20:12 AM - 1% - Read basic OSK Definitions: OK
8:20:12 AM - 2% - Read template defaults: OK
8:20:20 AM - 3% - Initialize Sensor Types: OK
8:20:32 AM - 4% - Initializing Help System
```

PRTG First things first

- PRTG auto discovery will attempt to discover your network and create a sensor for each probe it discovers
- Wait till auto-discovery finishes. Review the discovered devices and the created sensors. You will see a lot of sensors: ping, DNS, HTTP, SSL
 - Better to stop auto-discovery: Automatic auto-discovery is set on group or device level. You can change it in your group's or device's settings, section Group Type or Device Type, setting Sensor Management.
- Delete all the sensors discovered automatically because PRTG is free for the first 100 sensors only
 - You can disable the initial auto-discovery in a fresh PRTG installation. Simply run the installer in command prompt and add `/NoInitialAutoDisco=1` as parameter

How To

- Configure the Exporter (MikroTik)
- Configure the Flow Record (MikroTik)
- Apply it to the Interface (MikroTik)
- Configure the Flow Monitor (PRTG)



Exporter:
MikroTik

Collector:
PRTG

Observation Points:
MikroTik Interfaces

MikroTik Traffic Flow Configuration

The screenshot displays the MikroTik WinBox interface with the following components:

- Left Sidebar:** A menu with categories like IP, System, Queues, Files, Log, RADIUS, Tools, New Terminal, MetaROUTER, Partition, Make Supout.tif, Manual, New WinBox, and Exit. A sub-menu is open under 'Tools', listing: ARP, Accounting, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, Hotspot, IPsec, Kid Control, Neighbors, Packing, Pool, Routes, SMB, SNMP, Services, Settings, Socks, TFTP, Traffic Flow, UPnP, and Web Proxy.
- Traffic Flow Settings (General tab):**
 - Enabled:
 - Interfaces: bridgeWiFi
 - Cache Entries: 16k
 - Active Flow Timeout: 00:30:00
 - Inactive Flow Timeout: 00:00:15
- Traffic Flow Targets:**

Src. Address	Dst. Address	Port	Version
0.0.0.0	10.111.222.44	1234	IPFIX

1 item (1 selected)
- Traffic Flow Target <10.111.222.44>:**
 - Src. Address: 0.0.0.0
 - Dst. Address: 10.111.222.44
 - Port: 1234
 - Version: IPFIX
 - v9/IPFIX Template Refresh: 20
 - v9/IPFIX Template Timeout: 1800
 - Status: enabled

MikroTik Traffic Flow Configuration

- /ip traffic-flow set
 - #Settings for the exporter
 - interfaces=bridgeWiFi
 - #interfaces which will be used to gather statistics for traffic-flow
 - cache-entries=2k
 - #flows which can be in router's memory simultaneously
 - active-flow-timeout=30m
 - #maximum life-time of a flow
 - inactive-flow-timeout=15s
 - #how long to keep the flow active
 - enabled=yes
- /ip traffic-flow target
 - #Settings for the collector
 - add disabled=no
 - dst-address=10.111.222.44
 - port=1234
 - src-address=0.0.0.0
 - v9-template-refresh=20
 - v9-template-timeout=30m
 - version=ipfix

PRTG: Configure the Flow Monitor

- Select Add sensor
- Create a new device if necessary or use existing device
 - Usually the MikroTik RouterBoard is already discovered under network infrastructure
- Select Sensor type IPFIX
- Set the sensor settings. Most important:
 - Sensor Name
 - UDP Port
 - Active Flow Timeout

Add a sensor

Add Sensor to Device hAP Mikrotik Traffic Flow [10.111.222.33]

Monitor What?

- Availability/Uptime
- CPU Usage
- Hardware Parameters
- Bandwidth/Traffic
- Disk Usage
- Network Infrastructure
- Speed/Performance
- Memory Usage
- Custom Sensors

< Cancel sensor creation


Search ipf

Matching Sensor Types

IPFIX ?

Monitors a switch using IPFIX


The router/switch must be configured to send compatible flow data to PRTG.



IPFIX (Custom) ?

Monitors a switch using IPFIX (customizable)

The router/switch must be configured to send compatible flow data to PRTG.






Add Sensor to Device hAP Mikrotik Traffic Flow [10.111.222.33]

< Cancel

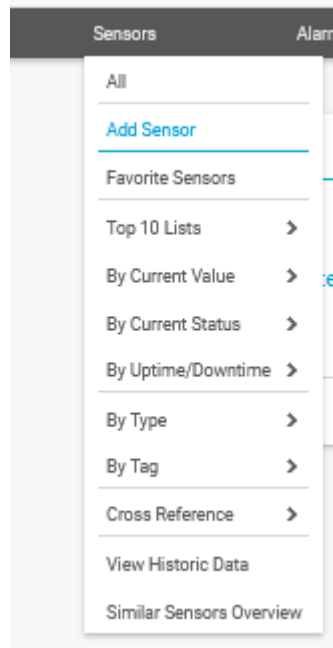
Basic Sensor Settings

- Sensor Name IPFIX
- Parent Tags
- Tags bandwidthsensor x netflowsensor x 
- Priority ★★☆☆☆

IPFIX Specific Settings

- Receive IPFIX Packets on UDP Port **This field is required.**
- Sender IP
- Receive IPFIX Packets on IP Probe's Local IPs
- 10.0.2.15
- Active Flow Timeout (Minutes) **This field is required.**
- Sampling Mode Off
 On
- Log Stream Data to Disk (for Debugging) None (recommended)
 Only for the 'Other' channel
 All stream data

Configure the Flow Monitor (PRTG)



Edit Object IPFIX

Basic Sensor Settings

Sensor Name

Parent Tags

Tags

Priority

IPFIX Specific Settings

Receive IPFIX Packets on UDP Port

Sender IP

Receive IPFIX Packets on IP Probe's Local IPs

10.0.2.15

Active Flow Timeout (Minutes)

Edit Object IPFIX

Sampling Mode Off On

Log Stream Data to Disk (for Debugging) None (recommended) Only for the 'Other' channel All stream data

Channel Configuration

Channel Selection

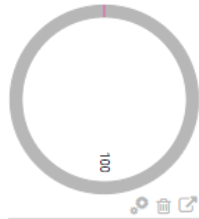
Group	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Content
Web	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WWW Traffic: HTTP, HTTPS
File Transfer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	File Transfer: FTP (Control)
Mail	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mail Traffic: IMAP, POP3, SMTP
Chat	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Chat, Instant Messaging: IRC, AIM
Remote Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remote Control: RDP, SSH, Telnet, VNC
Infrastructure	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Network Services: DHCP, DNS, Ident, ICMP, SNMP
NetBIOS	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	NetBIOS: NETBIOS
Citrix	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Citrix: Citrix
Other Protocols	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Various: OtherUDP, OtherTCP

Sensor Overview

✓ Sensor IPFIX ★★★★☆
OK

[Overview](#)
(📶) Live Data
2 days
30 days
365 days
📊 Historic Data
📄 Log
⚙️ Settings

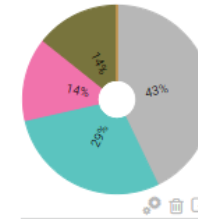
Top Talkers



Top Connections

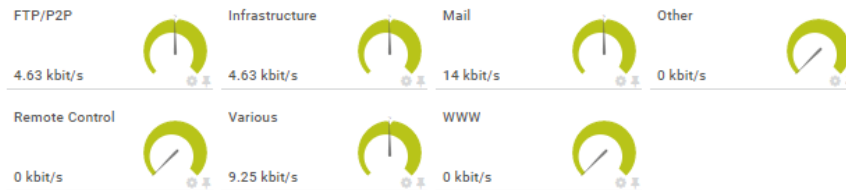
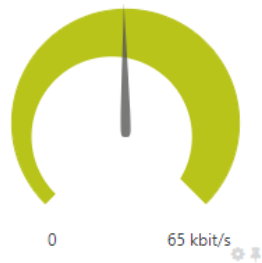


Top Protocols



Add Toplist

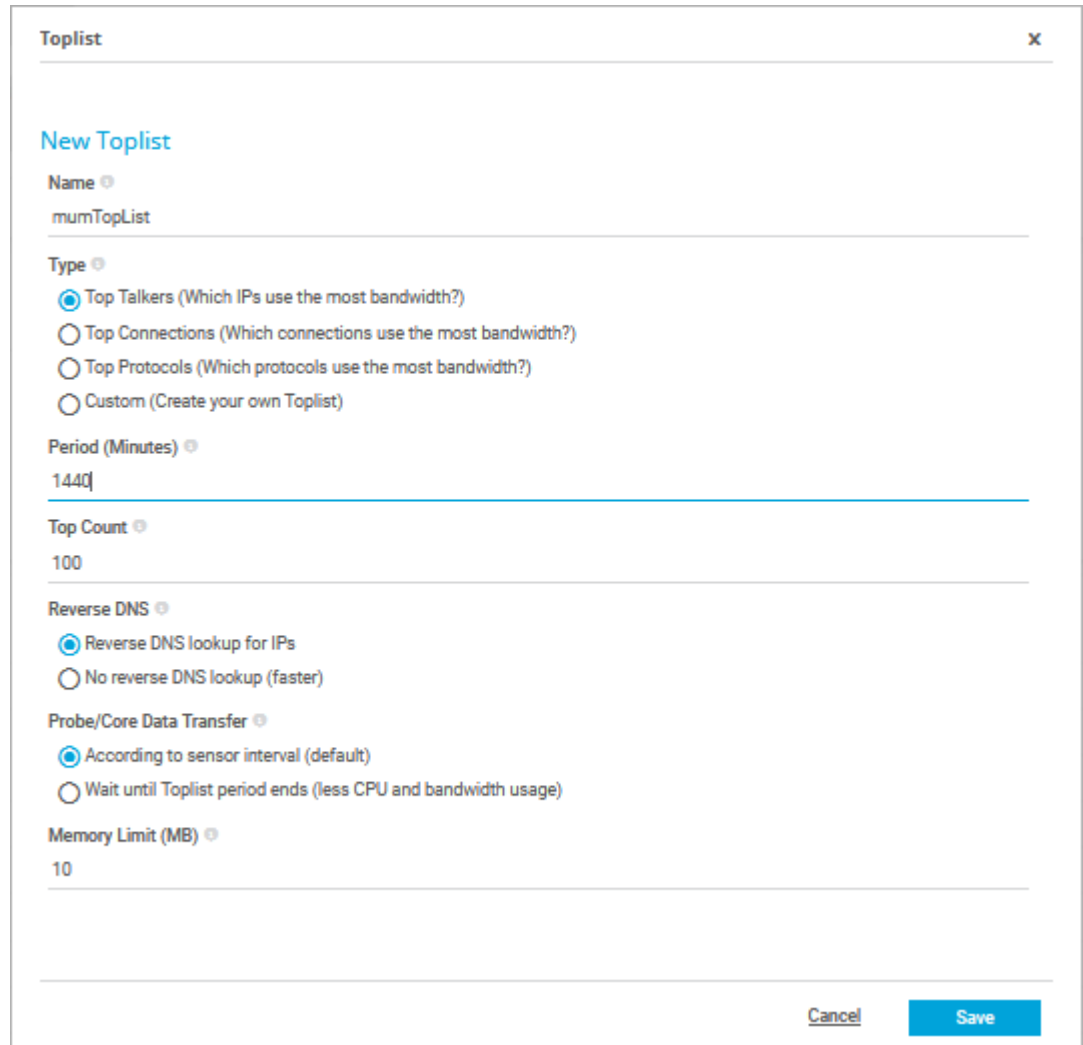
Total



Channel ▾	ID ↕	Last Value (volume) ↕	Last Value (speed) ↕	Minimum ↕	Maximum ↕	
Downtime	-4					⚙️
FTP/P2P	3002	34 KByte	4.63 kbit/s	0 kbit/s	9.30 kbit/s	⚙️
Infrastructure	3007	34 KByte	4.63 kbit/s	0 kbit/s	9.31 kbit/s	⚙️
Mail	3003	102 KByte	14 kbit/s	0 kbit/s	28 kbit/s	⚙️
Other	0	0 KByte	0 kbit/s			⚙️
Remote Control	3005	0 KByte	0 kbit/s			⚙️

PRTG: Add Top lists

- PRTG comes with primary top lists
 - Top Talkers
 - Top Connections
 - Top Protocols
 - Custom Toplist

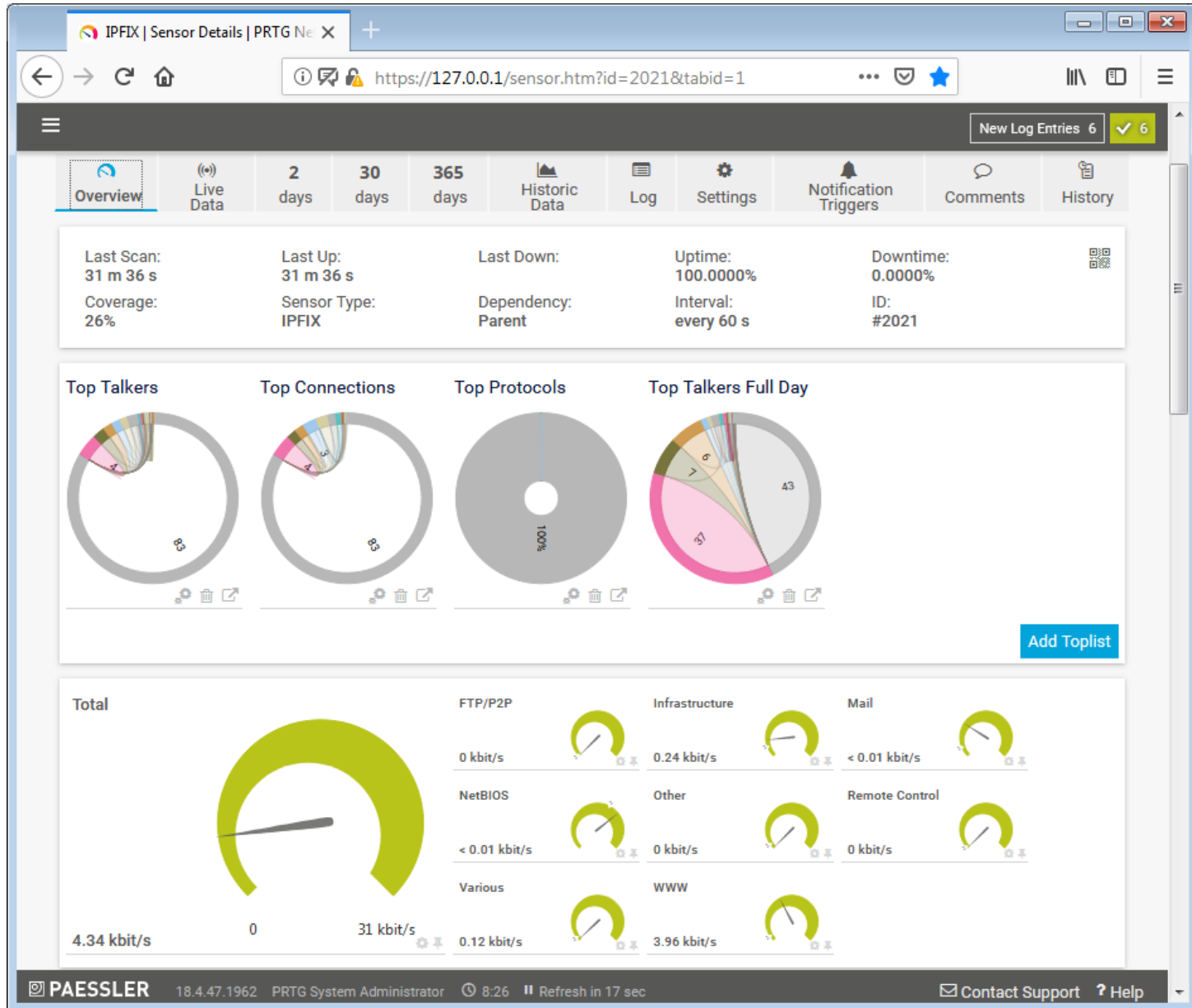


The screenshot shows the 'New Toplist' configuration window in PRTG. The window title is 'Toplist' with a close button (x) in the top right corner. The configuration fields are as follows:

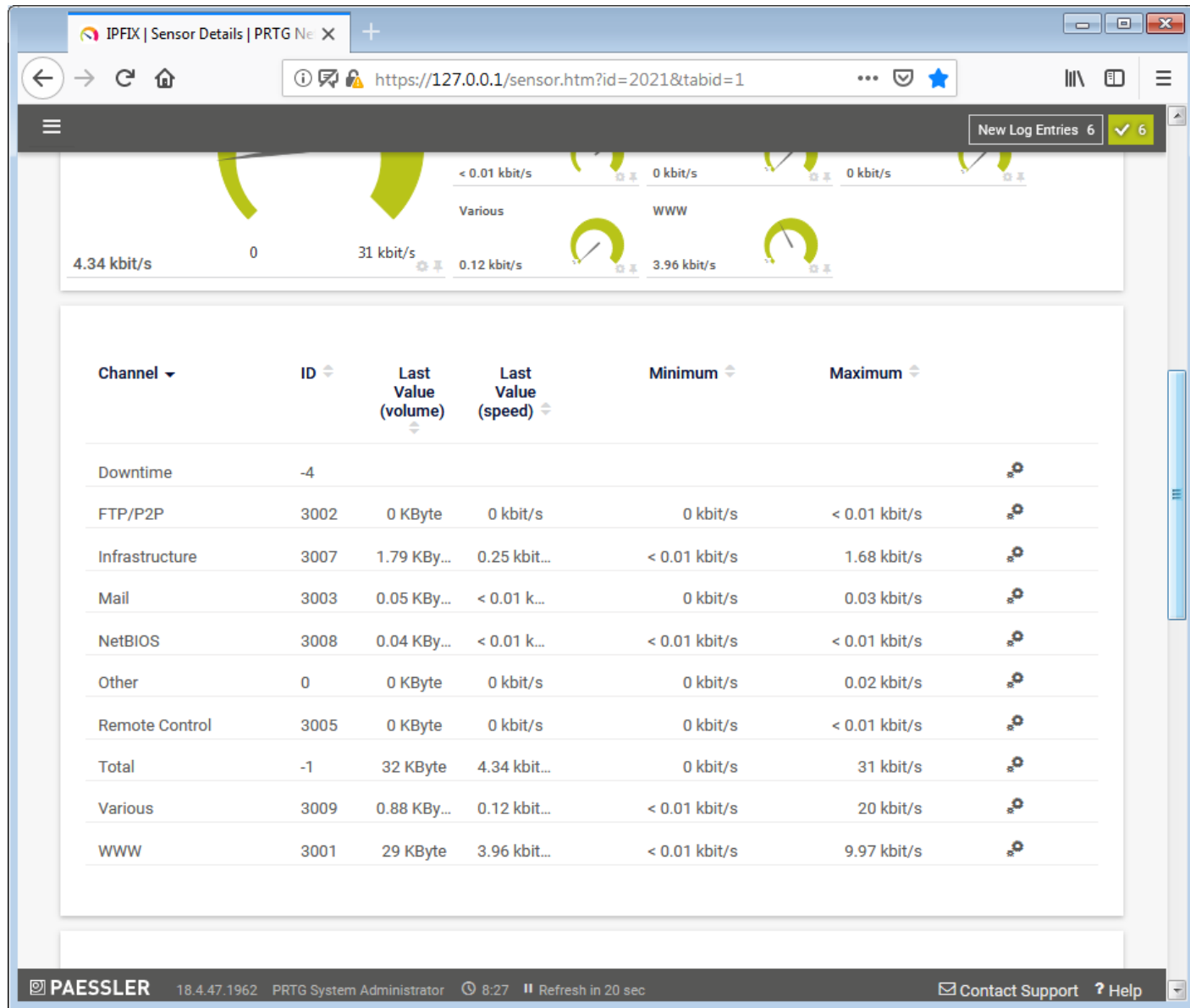
- Name:** mumTopList
- Type:** Radio buttons for:
 - Top Talkers (Which IPs use the most bandwidth?)
 - Top Connections (Which connections use the most bandwidth?)
 - Top Protocols (Which protocols use the most bandwidth?)
 - Custom (Create your own Toplist)
- Period (Minutes):** 1440
- Top Count:** 100
- Reverse DNS:** Radio buttons for:
 - Reverse DNS lookup for IPs
 - No reverse DNS lookup (faster)
- Probe/Core Data Transfer:** Radio buttons for:
 - According to sensor interval (default)
 - Wait until Toplist period ends (less CPU and bandwidth usage)
- Memory Limit (MB):** 10

At the bottom right, there are 'Cancel' and 'Save' buttons.

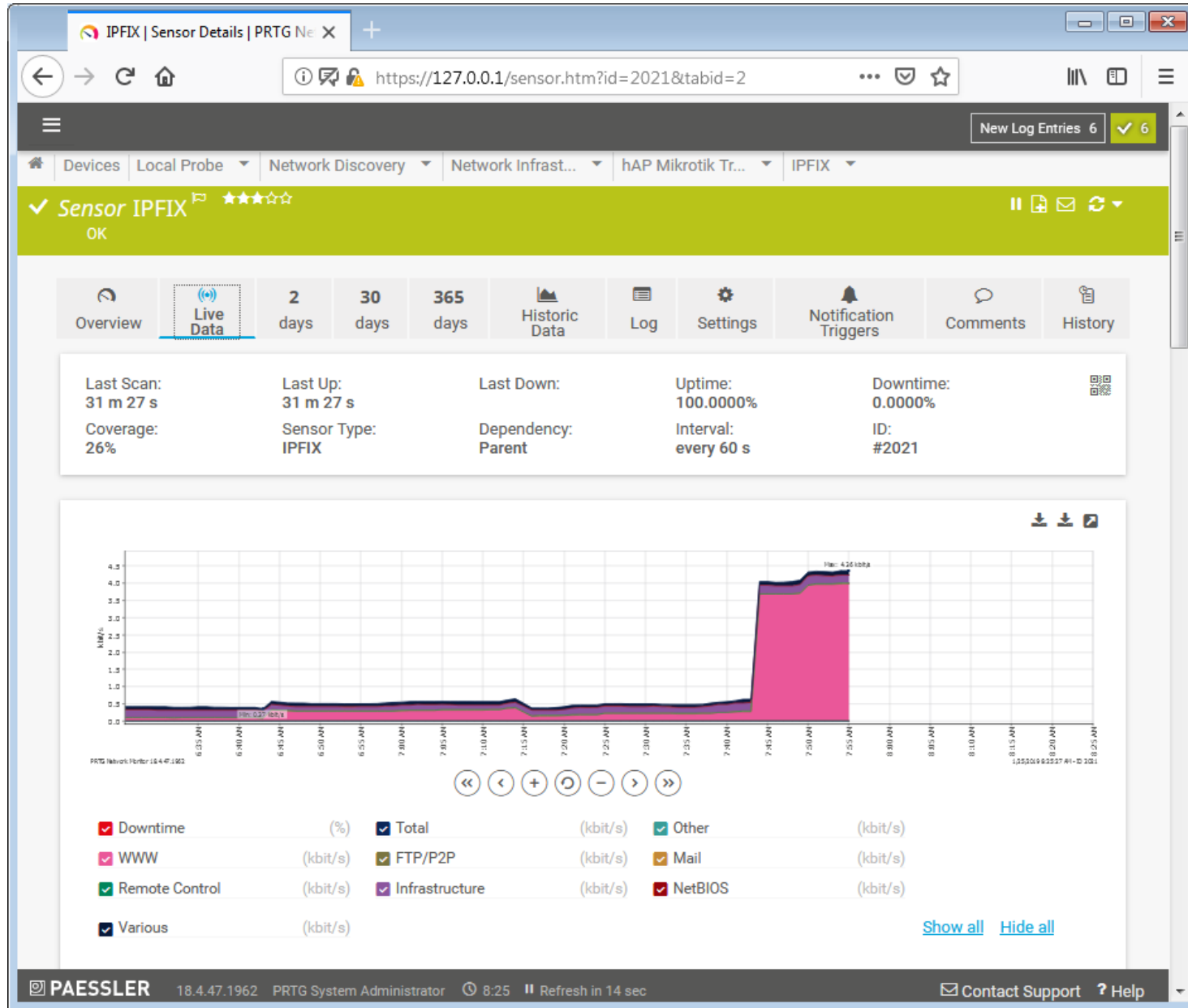
Sensor Overview



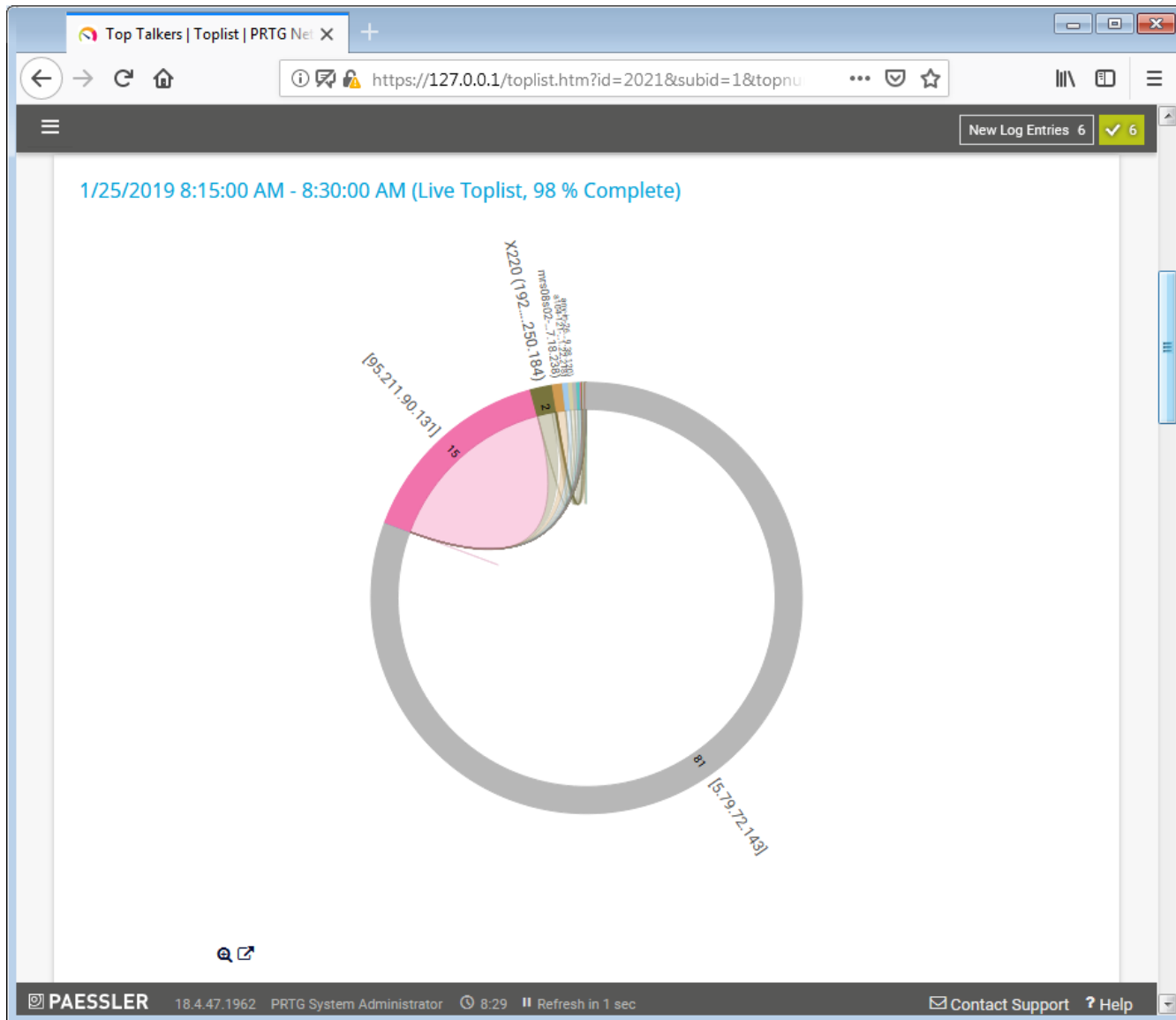
Sensor Channels



Sensor Live Data



Sensor Live Data



Sensor Live Data Detailed list

Top Talkers | Toplist | PRTG Net

https://127.0.0.1/toplist.htm?id=2021&subid=1&topnu

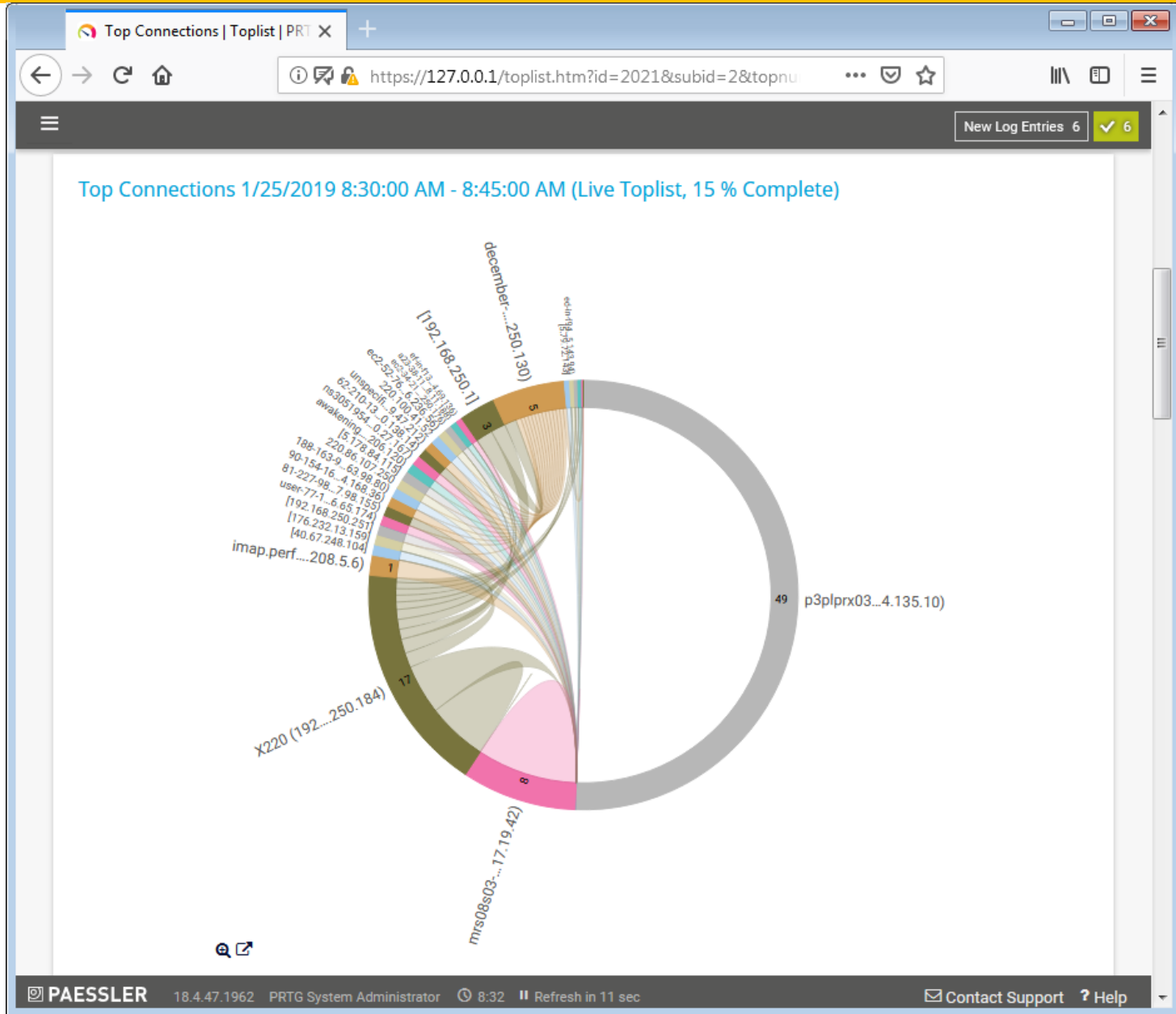
New Log Entries 6 ✓ 6

Items: 50

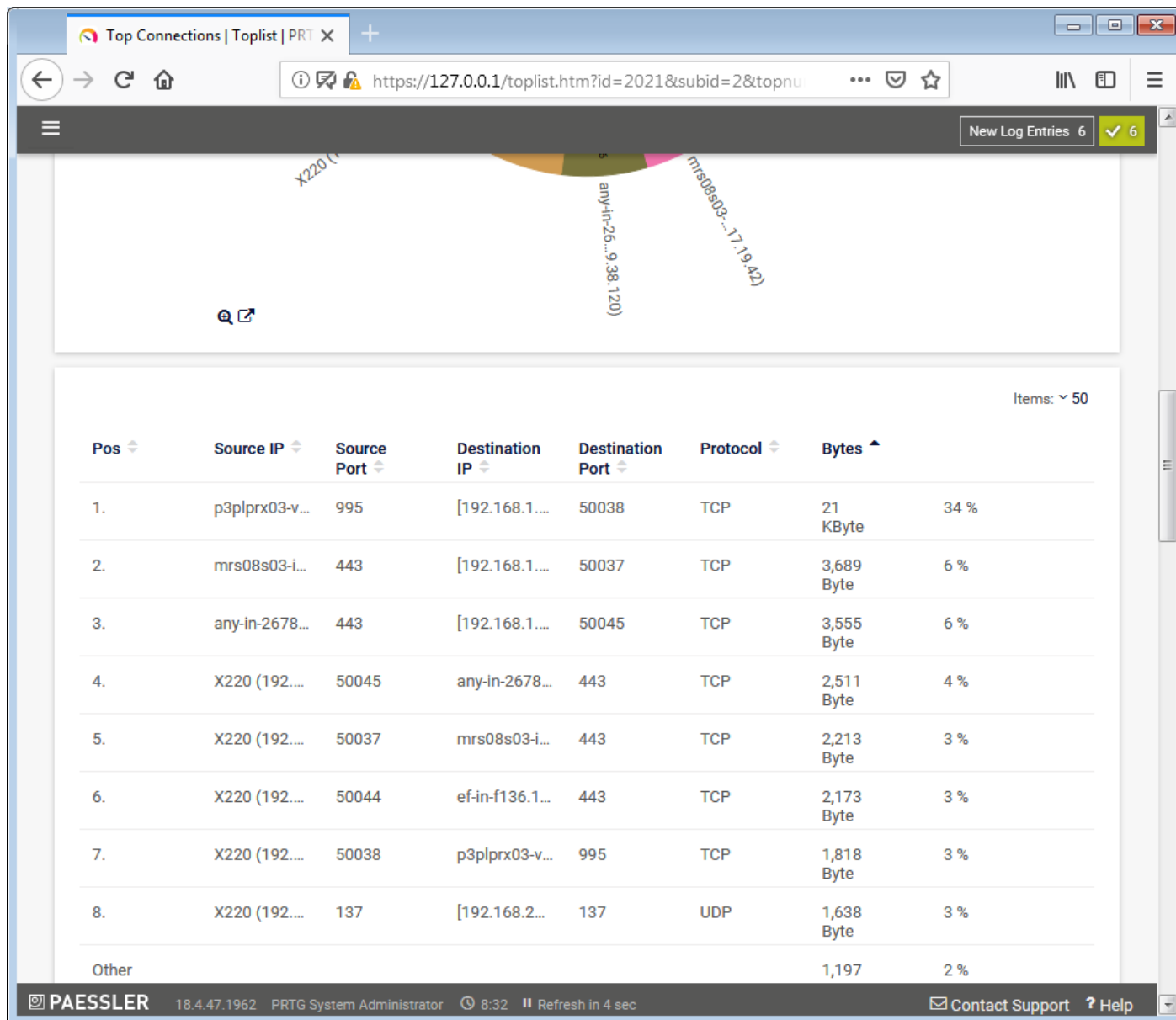
Pos	Source IP	Destination IP	Bytes	
1.	[5.79.72.143]	[192.168.1.64]	527 MByte	81 %
2.	[95.211.90.131]	[192.168.1.64]	99 MByte	15 %
3.	X220 (192.168.250.184)	[5.79.72.143]	8,483 KByte	1 %
4.	mrs08s02-in-f14.1e100....	[192.168.1.64]	5,119 KByte	< 1 %
5.	a104-121-22-218.deploy...	[192.168.1.64]	2,834 KByte	< 1 %
6.	any-in-2678.1e100.net (...)	[192.168.1.64]	2,205 KByte	< 1 %
7.	[159.148.147.205]	[192.168.1.64]	1,975 KByte	< 1 %
8.	[159.148.172.231]	[192.168.1.64]	1,776 KByte	< 1 %

PAESSLER 18.4.47.1962 PRTG System Administrator 8:30 Refresh in 11 sec Contact Support ? Help

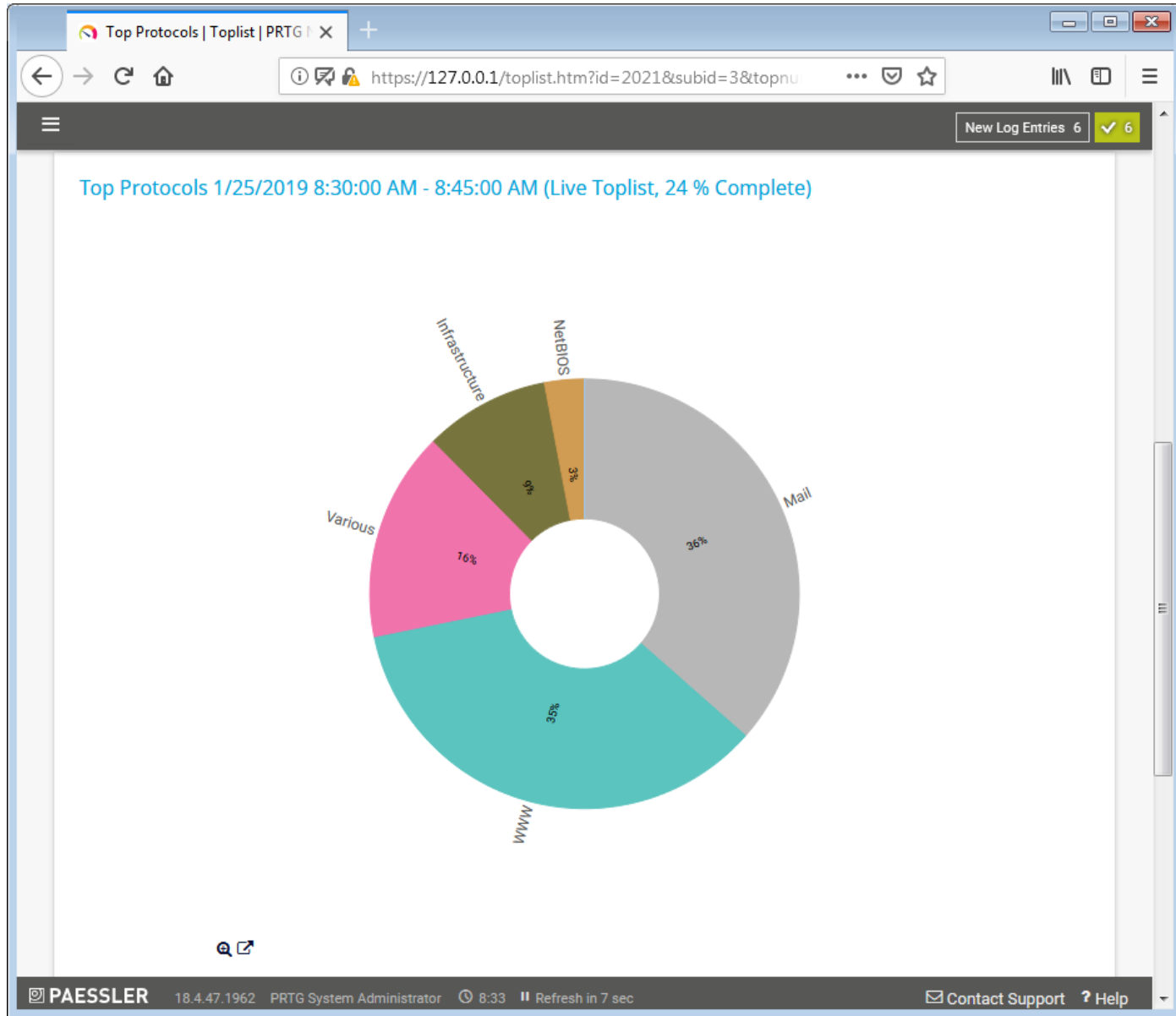
Top Connections



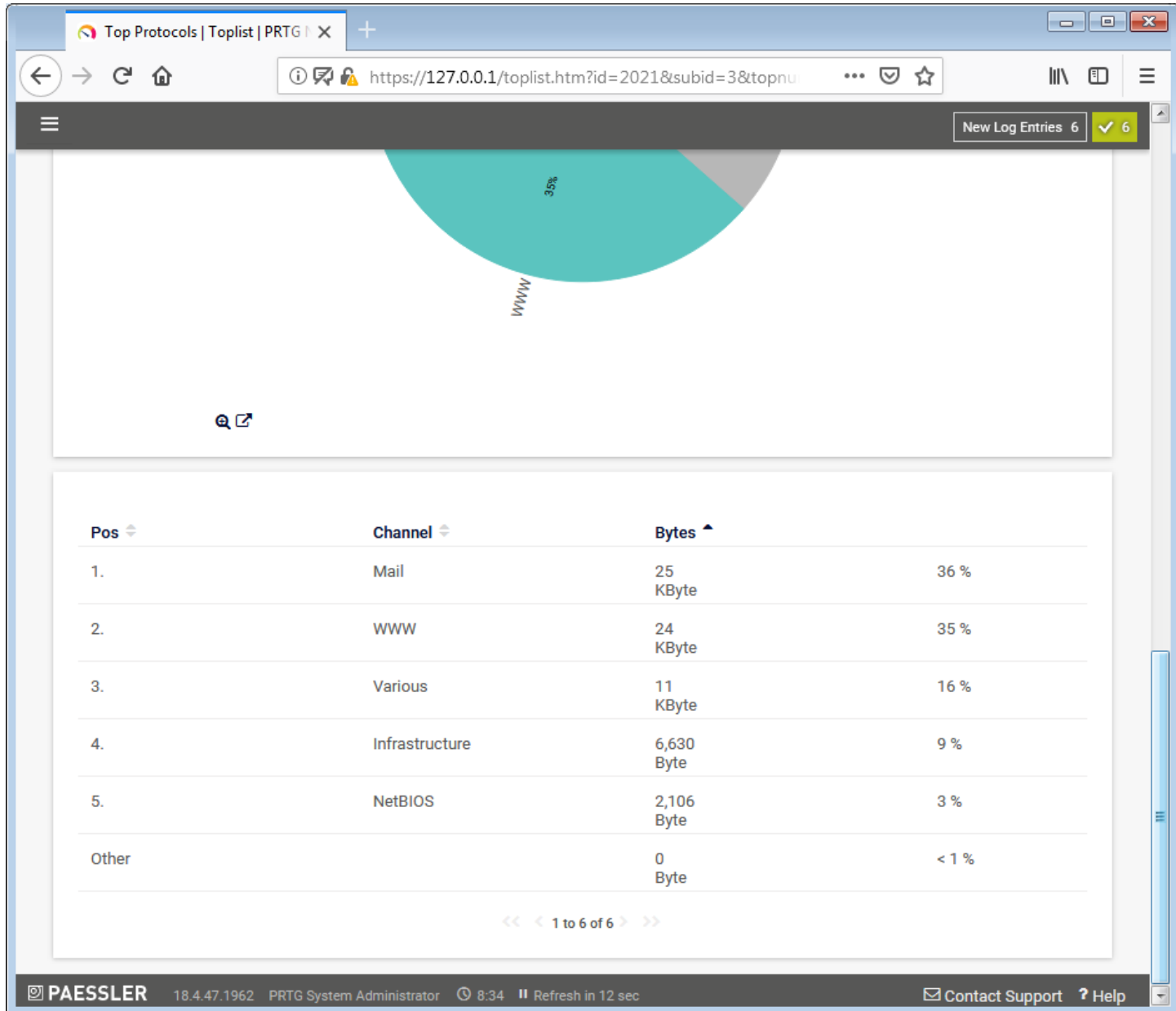
Top Connections Detailed List



Top Protocols



Top Protocols details



Thank you

Questions?