Traffic Flow

Introduction

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

Traffic Flow can process only that traffic which is processed by the router CPU, thus HW offloaded traffic will not be seen in Traffic Flow flows (for example, HW offloaded bridged traffic).

Traffic-Flow supports the following NetFlow formats:

- **version 1** - This is the original format used by NetFlow. It provides basic information about IP packets flowing through a router but lacks support for advanced features such as different types of protocols and Type of Service (ToS).
- **version 5** - An enhancement over Version 1, this format supports additional features such as Type of Service (ToS), TCP flags, and autonomous system numbers. In addition to version 1, version 5 can include BGP AS and flow sequence number information. Currently, RouterOS does not include BGP AS numbers.
- **version 9** - This version introduces a template-based export format, which allows for extensibility and support for new record types beyond what previous versions could handle. It can export data based on a defined template and is capable of exporting both IPv4 and IPv6 flow information.
- **IPFIX** - Standardized by the IETF, this protocol is based on NetFlow Version 9. It expands the capabilities further, allowing for more customizable and flexible flow records. IPFIX supports new technologies that were not addressed by NetFlow, like multicast.

General

Sub-menu: `/ip traffic-flow`

This section lists the configuration properties of Traffic-Flow.

Property	Description
interfaces (*string* | *all*; Default: **all**)	Names of those interfaces will be used to gather statistics for traffic-flow. To specify more than one interface, separate them with a comma.
cache-entries (*128k* | *16k* | *1k* | *256k* | *2k* | *...* ; Default: **4k**)	Number of flows which can be in router's memory simultaneously.
active-flow-timeout (*time*; Default: **30m**)	Maximum life-time of a flow.
inactive-flow-timeout (*time*; Default: **15s**)	How long to keep the flow active, if it is idle. If a connection does not see any packet within this timeout, then traffic-flow will send a packet out as a new flow. If this timeout is too small it can create a significant amount of flows and overflow the buffer.
packet-sampling (*no* | *yes*; Default: **no**)	Enable or disable packet sampling feature.
sampling-interval (*integer*; Default: **0**)	The number of packets that are consecutively sampled.
sampling-space (*integer*; Default: **0**)	The number of packets that are consecutively omitted.

> **info**
>
> Packet sampling is available in RouterOS **v7.**

In the following example:

```
/ip/traffic-flow/set packet-sampling=yes sampling-interval=2222 sampling-space=1111
```

2222 packet consecutive packets will be sampled and then 1111 will be omitted. Then the sampling cycle repeats in such a manner.

Targets

Sub-menu: `/ip traffic-flow target`

With Traffic-Flow targets we specify those hosts which will gather the Traffic-Flow information from the router.

Property	Description
src-address *(IP ; Default:)*	IP address used as source when sending Traffic-Flow statistics
dst- address (*IP*; Default:)	IP address of the host which receives Traffic-Flow statistic packets from the router.
Port *(Port; Default:2055)*	Port (UDP) of the host which receives Traffic-Flow statistic packets from the router.
v9-template-refresh (*integer*; Default: **20**)	Number of packets after which the template is sent to the receiving host (only for NetFlow version 9 and IPFIX)
v9-template-timeout (*time*; Default:)	After how long to send the template, if it has not been sent. (only for NetFlow version 9 and IPFIX)
version (*1* | *5* | *9* | *IPFIX*; Default:)	Which version format of NetFlow to use

IPFIX

Sub-menu: `/ip traffic-flow ipfix`

Allows to customize flow records

Property	Description
bytes	Total number of bytes processed in the flow.
ip-total-lenght	Length of the IP packet in bytes.
src-address	The source IP address of the flow.
dst-address	The destination IP address of the flow.
ipv6-flow-label	Label field from an IPv6 header, used to classify flows.
src-address-mask	Network mask for the source address, useful in summarizing data.
dst-address-mask	Network mask for the destination address.
is-multicast	Indicates whether the flow is a multicast flow.
src-mac-address	Source MAC address.
dst-mac-address	Destination MAC address.
last-forwarded	Timestamp of the last packet forwarded in a flow.

src-port	Source port number.
dst-port	Destination port number.
nat-dst-address	Translated destination IP address by NAT.
sys-init-time	System initialization time, can be used for timing analysis.
first-forwarded	Timestamp of the first packet forwarded in a flow.
nat-dst-port	Translated destination port number by NAT.
tcp-ack-num	Acknowledgment number in a TCP connection.
gateway	IP address of the gateway through which the flow was routed.
nat-events	Events related to Network Address Translation for the flow.
tcp-flags	Flags from the TCP header (e.g., SYN, ACK).
icmp-code	ICMP code for error messaging and operational information.
nat-src-address	Translated source IP address by NAT.
icmp-type	Type of ICMP message, important for diagnostic messages.
nat-src-port	Translated source port number by NAT.
tcp-seq-num	Sequence number in a TCP connection.
tcp-window-size	Window size in a TCP connection, indicating the scale of received data buffering.
igmp-type	Type of Internet Group Management Protocol operation.
out-interface	Interface through which packets of the flow are sent out.
in-interface	Interface through which packets of the flow are received.
packets	Number of packets processed in the flow.
ip-header-length	Length of the IP header.
protocol	Protocol number (e.g., TCP, UDP, ICMP).
tos	Type of Service field in the IP header, indicating priority and handling of the packet.
ttl	Time To Live for the packet, decremented by each router to prevent infinite loops.
udp-length	Length of the UDP payload.

Notes

By looking at the packet flow diagram you can see that traffic flow is at the end of the input, forward, and output chain stack. It means that traffic flow will count only traffic that reaches one of those chains.

For example, you set up a mirror port on a switch, connect the mirror port to a router, and set traffic flow to count mirrored packets. Unfortunately, such a setup will not work, because mirrored packets are dropped before they reach the input chain.

Other interfaces will appear in the report if traffic is passing through them and the monitoring interface.

Examples

This example shows how to configure Traffic-Flow on a router

Enable Traffic-Flow on the router:

```
[admin@MikroTik] ip traffic-flow> set enabled=yes
[admin@MikroTik] ip traffic-flow> print
               enabled: yes
            interfaces: all
         cache-entries: 1k
    active-flow-timeout: 30m
  inactive-flow-timeout: 15s
[admin@MikroTik] ip traffic-flow>
```

Specify the IP address and port of the host, which will receive Traffic-Flow packets:

```
[admin@MikroTik] ip traffic-flow target> add dst-address=192.168.0.2 port=2055 version=9
[admin@MikroTik] ip traffic-flow target> print
Flags: X - disabled
 #   SRC-ADDRESS       DST-ADDRESS        PORT     VERSION
 0   0.0.0.0           192.168.0.2        2055     9
[admin@MikroTik] ip traffic-flow target>
```

Now the router starts to send packets with Traffic-Flow information.

> **Note**
>
> To use ntop-ng with MikroTik you need to use Nprobe, which is paid software.

See more

- NetFlow Fundamentals
- Traffic flow with Ntop on MikroTik