Traffic Flow

Document revision 1.1 (February 6, 2008, 1:40 GMT)
This document applies to V3.0

Table of Contents

General Information

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/ip traffic-flow***
Hardware usage: ***Not significant***

Related Documents

- Cisco NetFlow
- NTop
- Integrating ntop with NetFlow

Description

MikroTik Traffic-Flow is a system that provides statistic information about packets which 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 supports the following NetFlow formats:

- **version 1** - the first version of NetFlow data format, do not use it, unless you have to
- **version 5** - in addition to version 1, version 5 has the BGP AS and flow sequence number

information included

- **version 9** - a new format which can be extended with new fields and record types, thanks to its template-style design

General Configuration

Description

This section describes the basic configuration of Traffic-Flow.

Property Description

active-flow-timeout (*time*; default: **30m**) - maximum life-time of a flow

cache-entries (*1k* | *2k* | *4k* | *8k* | *16k* | *32k* | *64k* | *128k* | *256k* | *512k*; default: **1k**) - number of flows which can reside in the router's memory simultaneously

enabled (yes | no) - whether to enable traffic-flow service or not

inactive-flow-timeout (*time*; default: **15s**) - how long to keep the flow active, if it is idle

interfaces (*name*) - names of those interfaces which will be used to gather statistics for traffic-flow. To specify more than one interface, separate them with a comma (",")

Traffic-Flow Target

Home menu level: ***/ip traffic-flow target***

Description

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

Property Description

address (*IP addressport*) - IP address and UDP port of the host which receives Traffic-Flow statistics 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)

v9-template-timeout - after how long to send the template, if it has not been sent

version (*1* | *5* | *9*) - which version format of NetFlow to use

Application Examples

Traffic-Flow Example

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

1. 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>
```

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

```
[admin@MikroTik] ip traffic-flow target> add address=192.168.0.2:2055 \
\... version=9
[admin@MikroTik] ip traffic-flow target> print
Flags: X - disabled
 #   ADDRESS               VERSION
 0   192.168.0.2:2055      9
[admin@MikroTik] ip traffic-flow target>
```

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

Some screenshots from NTop program, which has gathered Traffic-Flow information from our router and displays it in nice graphs and statistics. For example, where what kind of traffic has flown:

Host Information

Traffic Unit: [**Bytes**] [Packets]

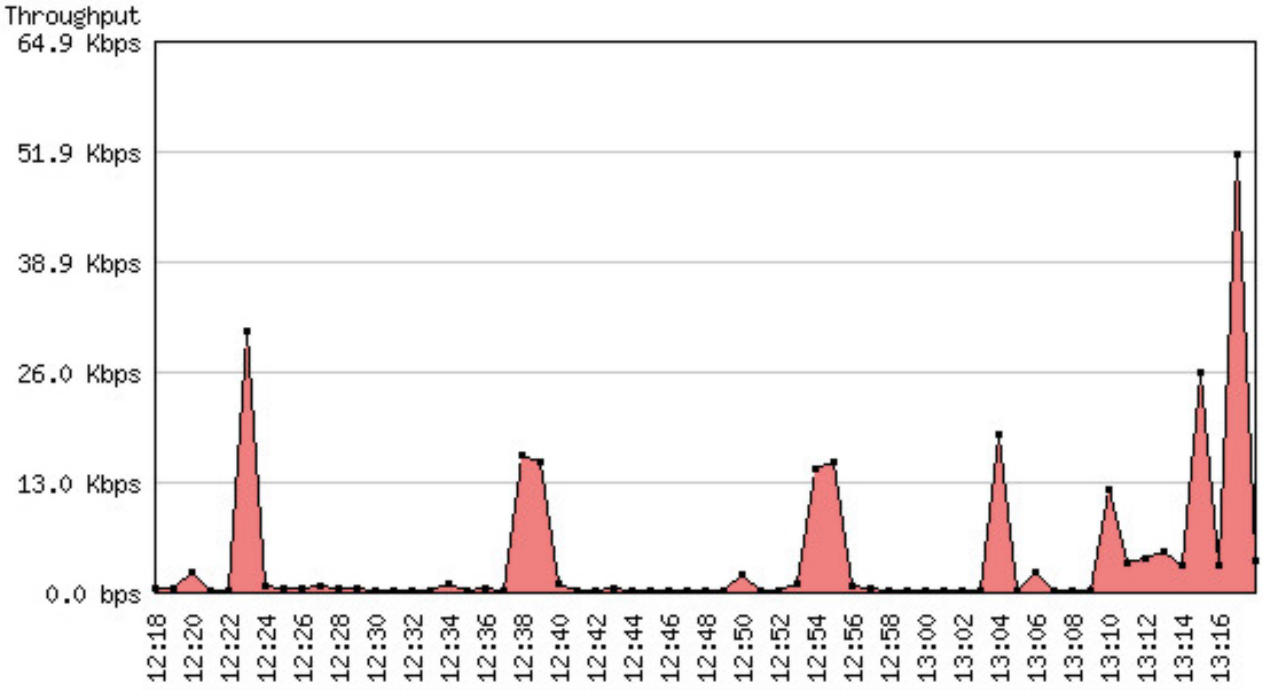
Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Host Contacts	Age/Inactivity		AS
10.5.7.4		10.5.7.4				17	14 days 0:37:58	5 sec	
81.94.227.50		81.94.227.50				2	14 days 0:33:02	5:01	
255.255.255.255		255.255.255.255				6623	14 days 0:37:59	0 sec	
3.3.3.3		3.3.3.3				1	14 days 0:35:16	48 sec	
192.168.10.11		192.168.10.11				3	14 days 0:37:46	16 sec	
192.168.1.1		192.168.1.1				1	14 days 0:37:16	35 sec	
192.168.10.10		192.168.10.10				3	14 days 0:37:46	16 sec	
1120730533.383		10.5.5.3				1	14 days 0:36:29	39 sec	
webproxy.mt.lv		10.5.5.1				3	14 days 0:36:15	47 sec	
1120730600.335		10.5.5.2				1	14 days 0:35:16	48 sec	
dator1		10.5.5.111				2	14 days 0:35:02	33 sec	
daces		10.5.5.124				4	14 days 0:37:18	36 sec	
10.5.5.50		10.5.5.50				3	14 days 0:37:16	40 sec	

Top three hosts by upload and download each minute:

Network Load Statistics Matrix

Sampling Period	Average Thpt	Top Hosts Sent Thpt		Top Hosts Rcvd Thpt	
13:16 - 13:17	4.0 Kbps	10.5.7.4	872.0 bps	10.5.7.4	1.1 Kbps
		159.148.172.197	648.0 bps	195.13.237.141	640.0 bps
		10.5.7.1	640.0 bps	0.0.0.0	504.0 bps
13:15 - 13:16	51.9 Kbps	159.148.147.196	91.9 Kbps	10.5.7.14	91.9 Kbps
		10.5.7.14	3.4 Kbps	159.148.147.196	3.4 Kbps
		10.5.7.1	664.0 bps	10.5.7.4	1.1 Kbps
13:14 - 13:15	3.5 Kbps	10.5.7.4	856.0 bps	10.5.7.4	1.1 Kbps
		10.5.7.1	624.0 bps	195.13.237.141	624.0 bps
		195.13.237.141	608.0 bps	0.0.0.0	496.0 bps
13:13 - 13:14	26.2 Kbps	159.148.172.197	33.6 Kbps	10.5.54.1	33.6 Kbps
		10.5.54.1	968.0 bps	159.148.172.197	968.0 bps
		10.5.7.4	752.0 bps	192.168.10.10	48.0 bps
13:12 - 13:13	3.2 Kbps	10.5.7.4	1.8 Kbps	10.5.7.4	2.3 Kbps
		195.13.237.141	1.3 Kbps	195.13.237.141	1.3 Kbps
		192.168.10.10	960.0 bps	0.0.0.0	1.0 Kbps
13:11 - 13:12	4.9 Kbps	10.5.7.4	840.0 bps	10.5.7.4	1.1 Kbps
		195.13.237.141	624.0 bps	195.13.237.141	640.0 bps
		192.168.10.10	400.0 bps	0.0.0.0	480.0 bps

Overall network load each minute:



Traffic usage by each protocol:

Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Percentage
FTP	112.3 MB	32%
HTTP	204.5 MB	59%
DNS	124.1 KB	0%
Telnet	4.5 MB	1%
NBios-IP	1.0 MB	0%
Mail	1.7 MB	0%
DHCP-BOOTP	22.0 KB	0%
Messenger	0.3 KB	0%
Other TCP/UDP-based Protocols	17.0 MB	4%