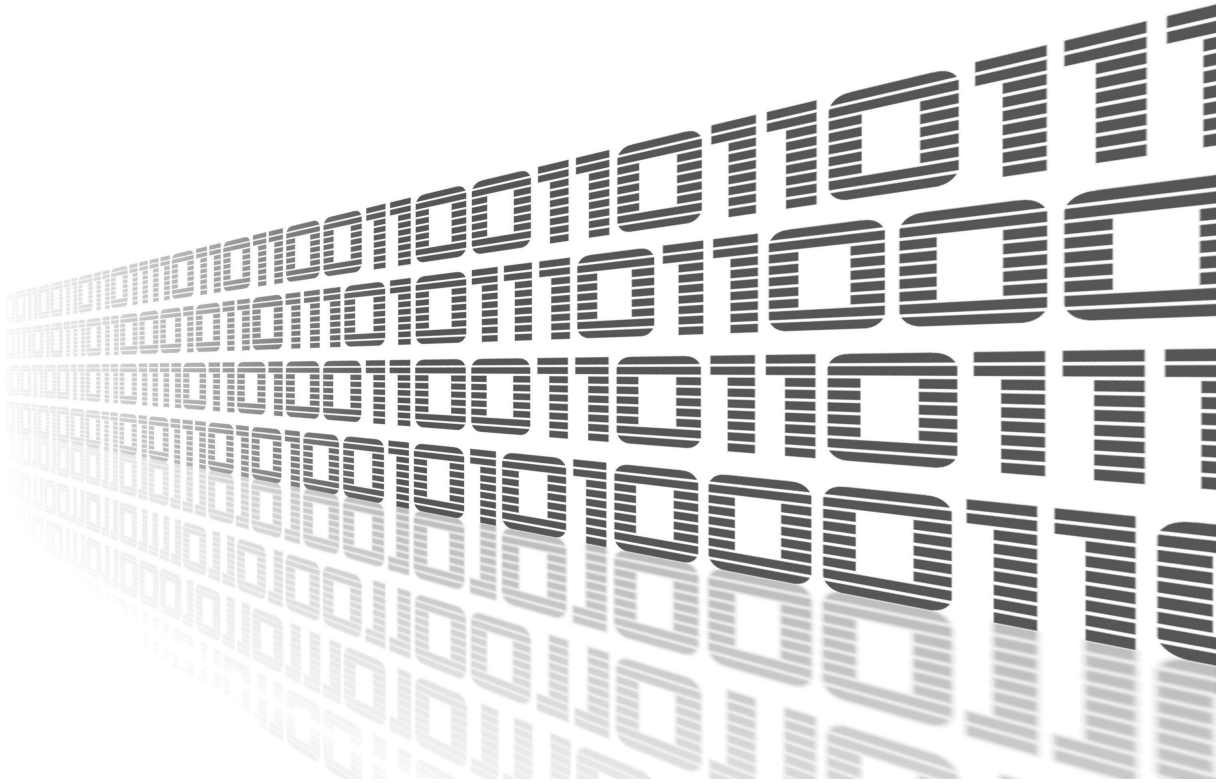
RouterApp

User Module

NetFlow/IPFIX

APPLICATION NOTE



ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that may arise in specific situations.

Information or notice – Useful tips or information of special interest.

Example – example of function, command or script.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0085-EN, revised on July 29, 2020. Released in the Czech Republic.

Contents

List of Figures

1. Description of the module

This user module is not installed on *Advantech* routers by default. See *Configuration Manual* for the description how to upload a user module to the router. For more information see the *Configuration manual*, chapter *Customization –> User Modules*.

The user module is v2 and v3 router platforms compatible.

User module NetFlow/IPFIX is determined for monitoring network traffic. NetFlow enabled routers have a probe that collects IP traffic information and submits them to a NetFlow collector and analyzer.

This user module contains:

- NetFlow **probe** that can submit information to compatible Network collector and analyzer, e. g. the `httsp://www.paessler.com/prtg`.
- NetFlow **collector** that stores the collected information to a file. It can also receive and store NetFlow traffic from other devices.

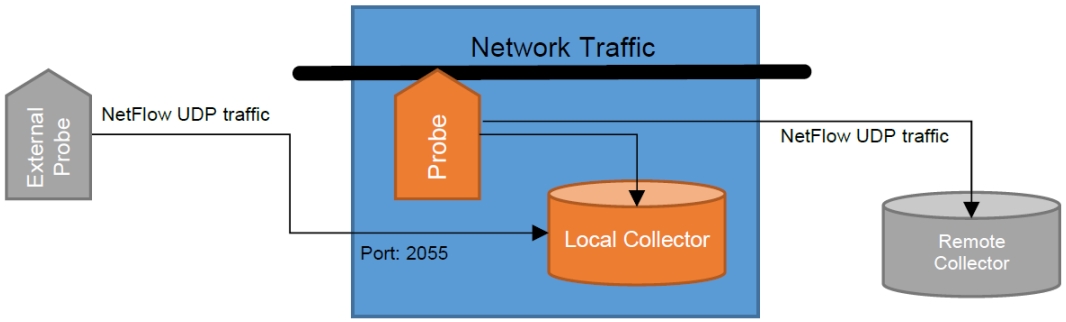


Figure 1: User Module NetFlow/IPFIX

2. Web Interface

Once the installation of the module is complete, the module's GUI can be invoked by clicking the module name on the User modules page of router's web interface.

Left part of this GUI contains menu with Configuration menu section and Information menu section. Customization menu section contains only the Return item, which switches back from the module's web page to the router's web configuration pages. The main menu of module's GUI is shown on Figure 2.

Figure 2: Menu

2.1 Configuration

2.1.1 Global

All NetFlow/IPFIX user module settings can be configured by clicking on the *Global* item in the main menu of module web interface. An overview of configurable items is given below.

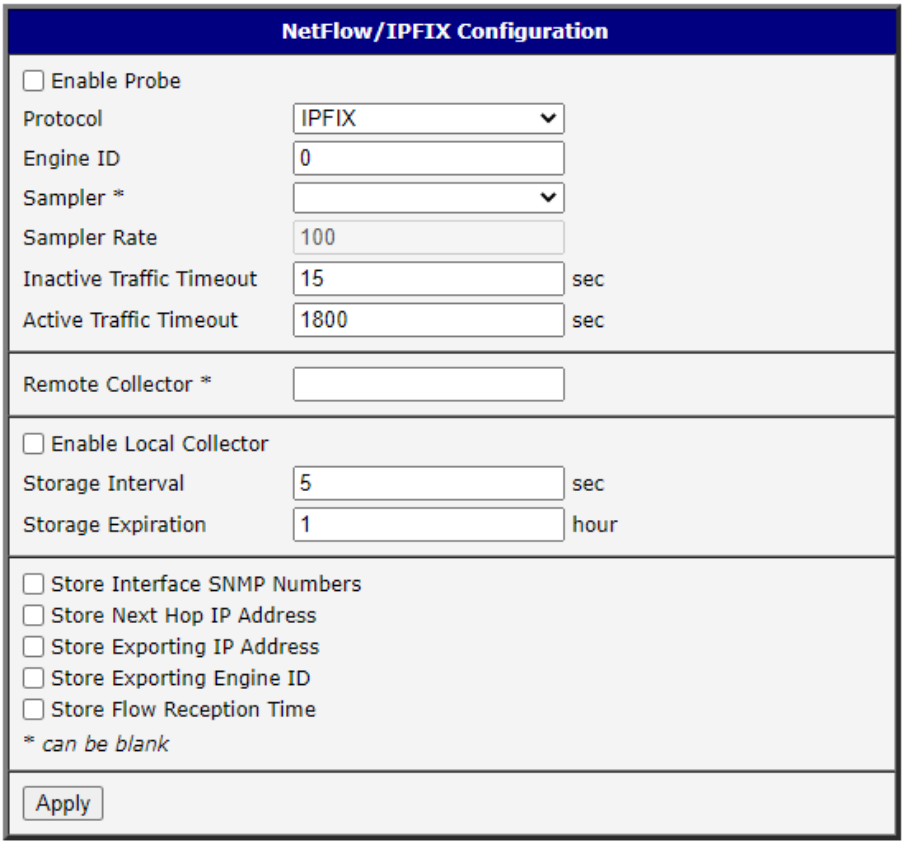


Figure 3: Status Overview

Item	Description
Enable Probe	Start sumbitting the NetFlow information to a Remote Collector (when defined), or to the Local Collector (when enabled).
Protocol	Protocol to be used: **NetFlow v5**, **Netflow v9**, **IPFIX** (NetFlow v10)

Continued on the next page

Continued from previous page

Item	Description
Engine ID	Observation Domain ID (on IPFIX, Source Id on NetFlow v9, or Engine Id on NetFlow v5) value. This may help your collector to distinguish between multiple exporters. See also section on Engine ID Interoperability.
Sampler	**(empty)**: submit every observed flow; **deterministic**: submit each N-th observed flow; **random**: select randomly one out of N flows; **hash**: select hash-randomly one out of N flows.
Sampleer Rate	The value of N.
Inactive Traffic Timeout	Submit flow after it's inactive for 15 seconds. Default value is 15.
Active Traffic Timeout	Submit flow after it's active for 1800 seconds (30 minutes). Default value is 1800. See also section on traffic timeouts.
Remote Collector	IP address of a NetFlow collector or analyzer, where to submit the collected NetFlow traffic information. Port is optional, default 2055. Detination can contain a comma separated list of multiple IP addresses (and ports) to mirror the NetFlow to two or more collectors/analyzers.
Enable Local Collector	Start receiving NetFlow information from the local Probe (when enabled) or from a remote probe.
Storage Interval	Specifies the time interval in seconds to rotate files. The default value is 300s (5min).
Storage Expiration	Sets the max life time for files in the directory. A value of 0 disables the max lifetime limit.
Store Interface SNMP Numbers	Check to store SNMP index of the input/output interface (%in, %out) in addition to the standard set of information, see below.
Store Next Hop IP Address	Check to store IP address of the next hop of outbound traffic (%nh).
Store Exporting IP Address	Check to store IP address of the exporting router (%ra).
Store Exporting Engine ID	Check to store Engine ID of the exporting router (%eng).
Store Flow Reception Time	Check to store timestamp when the flow info was received (%tr).

Table 1: Configuration items description

2.2 Information

2.2.1 Licences

Summarizes Open-Source Software (OSS) licenses used by this module.

NetFlow/IPFIX Licenses

Project	License	More Information
bzip2	BSD	License
ipt-netflow	GPLv2	License
nfdump	BSD	License

Figure 4: Licences

3. Usage Instructions

The NetFlow data should **not** be sent over WAN, unless VPN is used. The data are not inherently encrypted or obfuscated, so an unauthorized person may intercept and view the information.

3.1 Collected Information

The following standard set of information are always sent by the probe and stored by the collector:

- Timestamp when the traffic was first seen (%ts) and last seen (%te), using clock of the probe
- Number of bytes (%byt) and packets (%pkt)
- Protocol used (%pr)
- TOS (%tos)
- TCP flags (%flg)
- Source IP address (%sa, %sap) and port (%sp)
- Destination IP address (%da, %dap) and port (%dp)
- ICMP type (%it)

The following are also sent, but stored only upon request (see config above):

- SNMP index of the input/output interface (%in, %out)
- IP address of the next hop of outbound traffic (%nh)
- IP address (%ra) and Engine ID (%eng) of the exporting router (probe)
- Timestamp when the flow info was received (%tr), using clock of the collector

The value in brackets (%xx) indicates the formatter to be used with nfdump to display this value (see next chapter).

3.2 Retrieval of Stored Information

Data are stored in /tmp/netflow/nfcapd.yyyymmddHHMM, where yyyymmddHHMM is the creation time. The directory also includes the .nfstat file, which is used to monitor the expiration time. Do not alter this file. To configure expiration use the admin GUI.

The files can be read using the nfdump command.

nfdump [options] [filter]

Display UDP packets sent by 192.168.88.100:

```
nfdump -r nfcapd.202006011625 'proto udp and src ip 192.168.88.100'
```

Display all flows between 16:25 and 17:25, aggregating bidirectional flows (-B):

```
nfdump -R /tmp/netflow/nfcapd.202006011625:nfcapd.202006011725 -B
```

Display Engine Type/ID, source address+port and destination address+por for all flows:

```
nfdump -r /tmp/netflow/nfcapd.202006011625 -o "fmt:%eng %sap %dap"
```

3.3 Engine ID Interoperability

Netflow v5 defines two 8-bit identifiers: Engine Type and Engine ID. Probe on Advantech routers sends only Engine ID (0..255). The Engine Type will always be zero (0). Hence, a flow sent with Engine ID = 513 (0x201) will be received as Engine Type/ID = 0/1.

	1B	1B
Sent	0	Engine ID
Received	Engine Type	Engine ID

Figure 5: NetFlow v5

Netflow v9 defines one 32-bit identifier. Probe on Advantech routers can send any 32-bit number, however other manufacturers (e.g. Cisco) split the identifier into two reserved bytes, followed by Engine Type and Engine ID. The receiver follows the same approach. Hence, a flow sent with Engine ID = 513 (0x201) will be received as Engine Type/ID = 2/1.

	1B	1B	1B	1B
Sent	Engine ID			
Received	(ignored)	(ignored)	Engine Type	Engine ID

Figure 6: NetFlow v9

IPFIX defines one 32-bit identifier. Probe on Advantech routers can send any 32-bit number, but the local collector does not store this value yet. Hence any flow will be received as Engine Type/ID = 0/0.

	1B	1B	1B	1B
Sent	Engine ID			
Received	(ignored)	(ignored)	(ignored)	(ignored)

Figure 7: IPFIX

Recommendation: If you want to store Engine ID in the local collector, check *Store Exporting Engine ID in the configuration*, use Engine ID < 256 and avoid using the IPFIX protocol.

3.4 Traffic Timeouts

The probe exports whole flows, i.e. all packets that belong together. If no packets are observed for a given period (**Inactive Traffic Timeout**), the flow is considered as complete and the probe sends traffic information to the collector.

Information about a file transfer will thus appear in the collector once the transfer is completed, which may take a significant amount of time. If the transmission is active for too long (**Active Traffic Timeout**) it will appear as multiple shorter flows. For example, with a 30 minutes active traffic timeout, a 45 minutes communication will show as two flows: one 30 min and one 15 min.

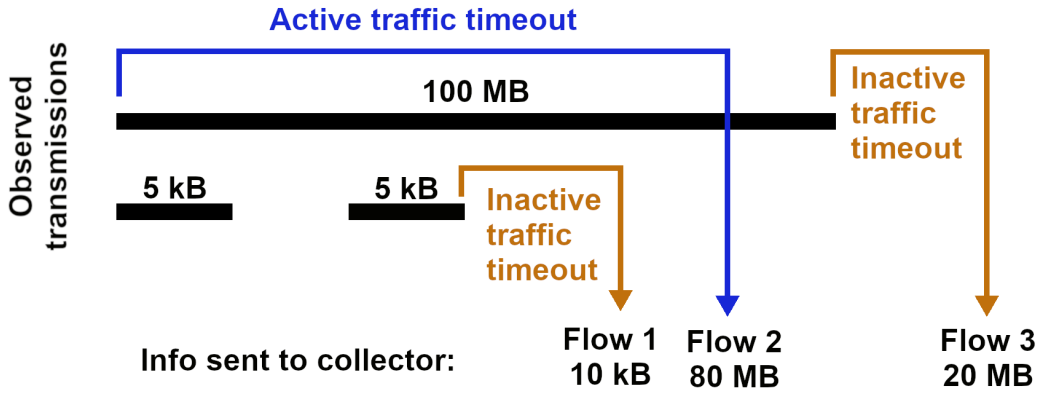


Figure 8: Traffic Timeouts

4. Related Documents

[1] Advantech Czech: **v2 Routers Configuration Manual** (MAN-0021-EN)
[2] Advantech Czech: **SmartFlex Configuration Manual** (MAN-0023-EN)
[3] Advantech Czech: **SmartMotion Configuration Manual** (MAN-0024-EN)
[4] Advantech Czech: **SmartStart Configuration Manual** (MAN-0022-EN)
[5] Advantech Czech: **ICR-3200 Configuration Manual** (MAN-0042-EN)

Product related documents can be obtained on *Engineering Portal* at `https://ep.advantech-bb.cz/` address.