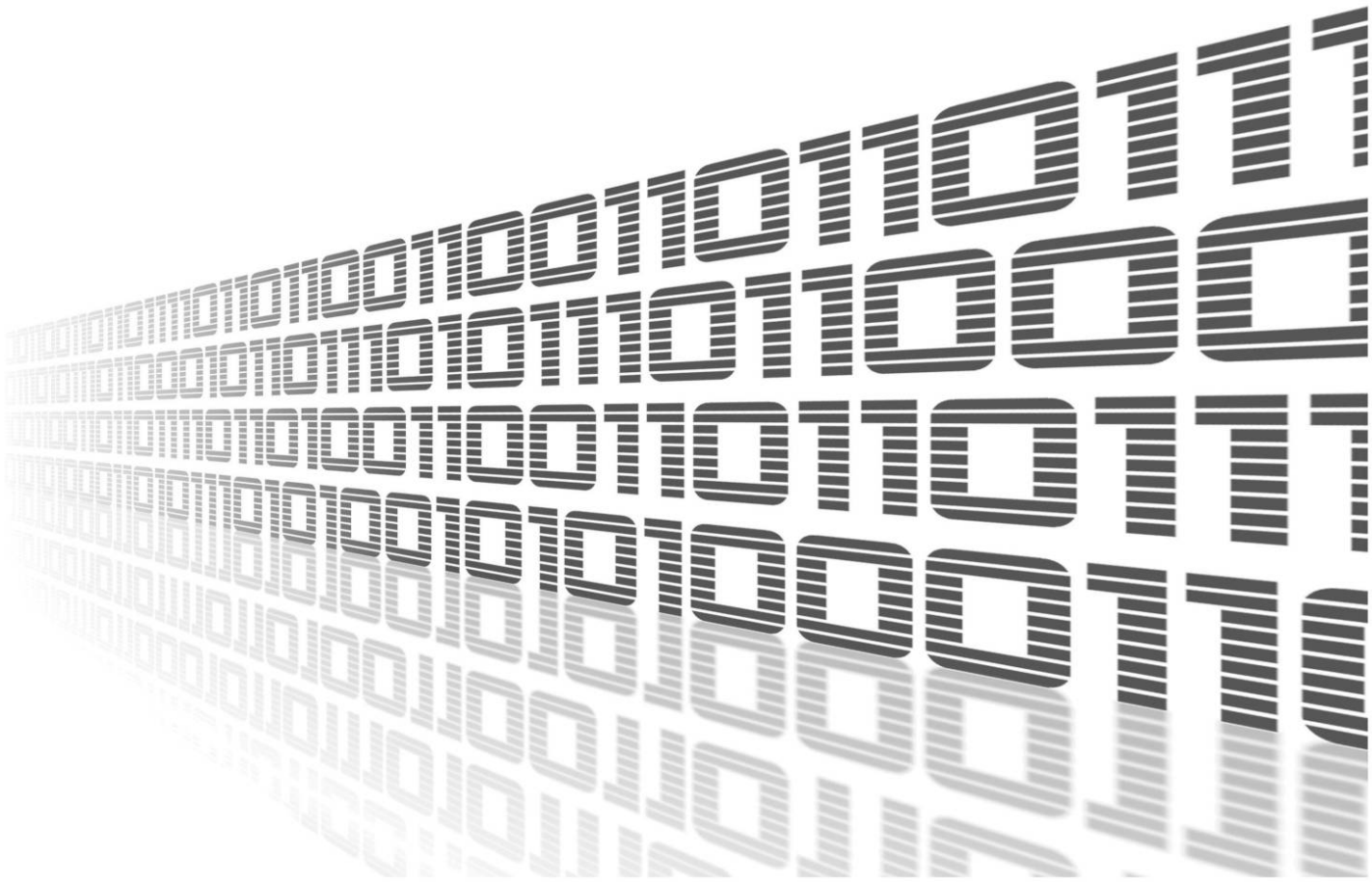
ADVANTECH

RouterApp

NetFlow/IPFIX



Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0085-EN, revised on July 3, 2025.

Used symbols

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

Attention – Problems that can arise in specific situations.

Information – Useful tips or information of special interest.

Contents

List of Figures

List of Tables

1. Description of the Module

The *NetFlow/IPFIX* router app is not included in the standard router firmware. For instructions on how to upload and install this app, refer to the *Configuration Manual* (see Chapter Related Documents).

The *NetFlow/IPFIX* router app is designed for monitoring network traffic. Routers with NetFlow enabled run a probe that collects IP traffic information and submits it to a NetFlow collector and analyzer.

This router app provides:

- A NetFlow **probe** that can send flow information to a compatible network collector or analyzer, e.g., https://www.paessler.com/prtg.
- A NetFlow **collector** that stores collected flow data to files. It can also receive and store NetFlow traffic from other devices.

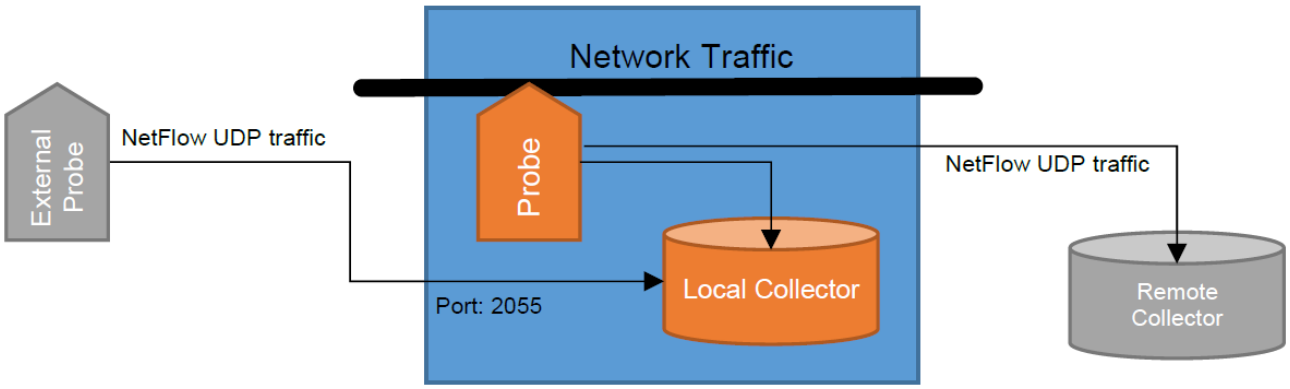


Figure 1: Router app NetFlow/IPFIX

2. Web Interface

Once the module is installed, its web interface can be accessed by clicking the module name on the *Router Apps* page of the router's web interface.

The left pane of the GUI contains the *Configuration* and *Information* sections. The *Customization* section contains only the *Return* item, which returns you from the module's web page to the router's main web configuration interface. The main menu of the module's GUI is shown in Figure 2.

Figure 2: Menu

2.1 Configuration

2.1.1 Global

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

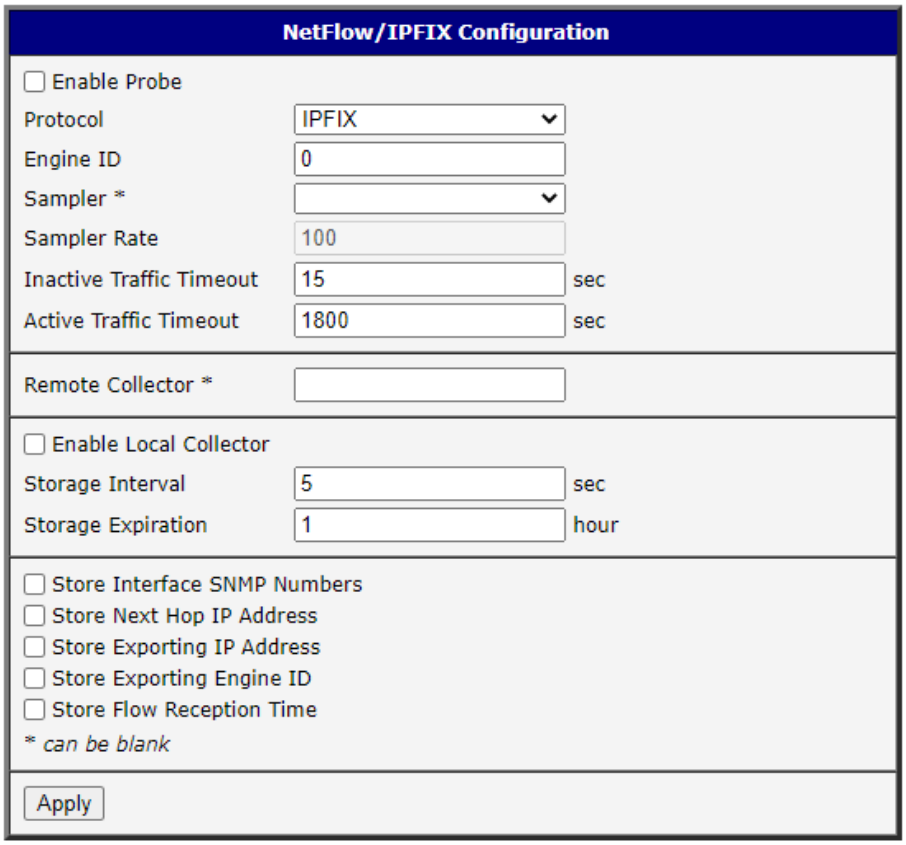


Figure 3: Status Overview

Item	Description
Enable Probe	Starts submitting NetFlow information to a remote collector (when defined) or to the local collector (when enabled).
Protocol	Protocol to be used: **NetFlow v5**, **NetFlow v9**, or **IPFIX** (NetFlow v10).
Engine ID	Sets the Observation Domain ID for IPFIX, Source ID for NetFlow v9, or Engine ID for NetFlow v5. This helps your collector distinguish between multiple exporters. See section 3.3.
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.
Sampler Rate	The value of N for the selected sampling method.
Inactive Traffic Timeout	Submits a flow after it has been inactive for the specified number of seconds. Default is 15.

Continued on the next page

Continued from previous page

Item	Description
Active Traffic Timeout	Submits a flow after it has been active for the specified number of seconds (default: 1800, i.e., 30 minutes). See also section 3.4.
Remote Collector	IP address of a NetFlow collector or analyzer to which the collected flow information is submitted. Port is optional (default: 2055). You can specify a comma-separated list of multiple IP addresses (and ports) to mirror NetFlow data to multiple collectors/analyzers.
Enable Local Collector	Enables receiving NetFlow information from the local probe (when enabled) or from a remote probe.
Storage Interval	Specifies the time interval (in seconds) for rotating storage files. Default is 300 seconds (5 minutes).
Storage Expiration	Sets the maximum lifetime for files in the directory. A value of 0 disables the lifetime limit.
Store Interface SNMP Numbers	If checked, stores the SNMP index of the input/output interface (%in, %out) in addition to the standard set of information.
Store Next Hop IP Address	If checked, stores the IP address of the next hop for outbound traffic (%nh).
Store Exporting IP Address	If checked, stores the IP address of the exporting router (%ra).
Store Exporting Engine ID	If checked, stores the Engine ID of the exporting router (%eng).
Store Flow Reception Time	If checked, stores the timestamp when the flow info was received (%tr).

Table 1: Configuration items description

2.2 Information

2.2.1 Licenses

This section summarizes the Open-Source Software (OSS) licenses used by this module.

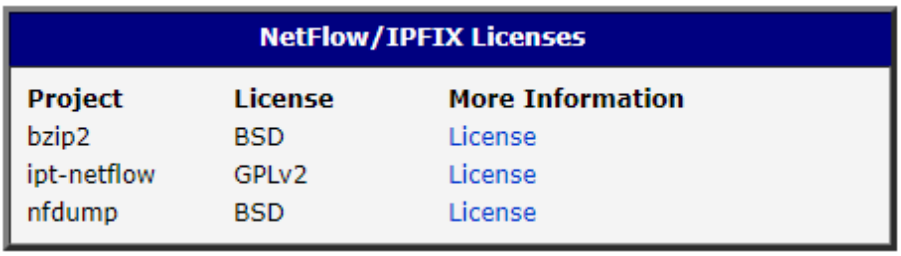


Figure 4: Licenses

3. Usage Instructions

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

3.1 Collected Information

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

- Timestamp when the traffic was first seen (%ts) and last seen (%te), using the probe's clock
- 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 data are also sent, but stored only if enabled in configuration:

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

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

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 expiration. Do not alter this file. To configure expiration, use the admin GUI.

Files can be read using the `nfdump` command, which has the syntax `nfdump [options] [filter]` . See the following examples:

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+port 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. The probe on Advantech routers sends only Engine ID (0..255). The Engine Type is always zero (0). Thus, 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. The 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. Thus, 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. The probe on Advantech routers can send any 32-bit number, but the local collector does not store this value yet. Thus, 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 complete and the probe sends the 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-minute active traffic timeout, a 45-minute communication will show as two flows: one 30 min and one 15 min.

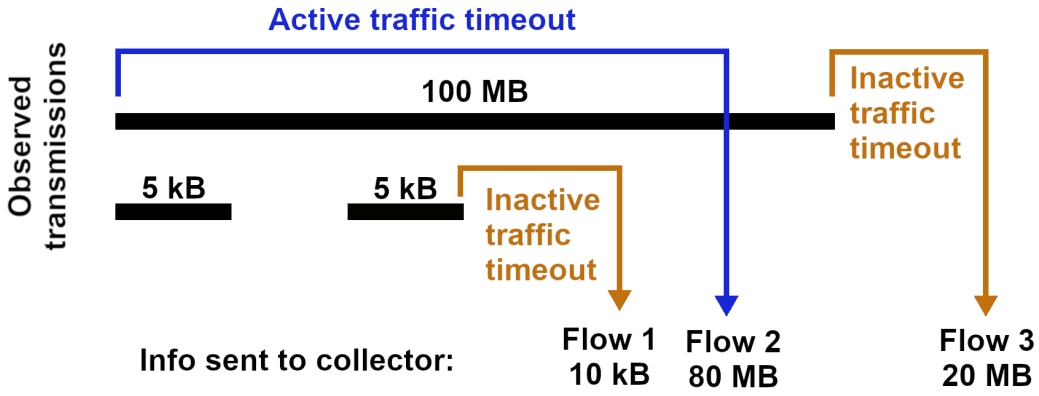


Figure 8: Traffic Timeouts

4. Related Documents

You can obtain product-related documents on *Engineering Portal* at *icr.advantech.com* address.

To get your router's *Quick Start Guide*, *User Manual*, *Configuration Manual*, or *Firmware* go to the *Router Models* page, find the required model, and switch to the *Manuals* or *Firmware* tab, respectively.

The *Router Apps* installation packages and manuals are available on the *Router Apps* page.

For the *Development Documents*, go to the *Development* page.