

## Traffic Shaper Traffic Shaper

### Operating Manual

<u>Introduction</u>	<b>1</b>
<u>Getting Started</u>	<b>2</b>
<u>Installation</u>	<b>3</b>
<u>Graphical user interface</u>	<b>4</b>
<u>Dataflows</u>	<b>5</b>
<u>Configuration</u>	<b>6</b>
<u>Operating principle</u>	<b>7</b>
<u>Appendix</u>	<b>8</b>

## Legal information

### Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

<b>⚠ DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
<b>⚠ WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
<b>⚠ CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

### Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

### Proper use of Siemens products

Note the following:

<b>⚠ WARNING</b>
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

### Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

### Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

# Table of contents

<b>1</b>	<b>Introduction</b> .....	<b>4</b>
1.1	Security information .....	4
1.2	Useful information .....	5
<b>2</b>	<b>Getting Started</b> .....	<b>6</b>
2.1	Introduction .....	6
2.2	Image processing example .....	7
2.3	Defining sensible limits .....	8
2.4	Setting the upper limits .....	10
<b>3</b>	<b>Installation</b> .....	<b>19</b>
<b>4</b>	<b>Graphical user interface</b> .....	<b>22</b>
4.1	Overview .....	22
4.2	"Configuration" tab .....	24
4.3	"Statistics" tab .....	27
<b>5</b>	<b>Dataflows</b> .....	<b>31</b>
5.1	Introduction .....	31
5.2	Unknown dataflows .....	31
5.3	Multicast dataflows.....	33
5.4	Adding dataflows.....	34
5.5	Changing dataflows .....	36
5.6	Removing dataflows.....	37
<b>6</b>	<b>Configuration</b> .....	<b>38</b>
6.1	What is a configuration? .....	38
6.2	Managing configurations.....	39
<b>7</b>	<b>Operating principle</b> .....	<b>40</b>
7.1	Token bucket algorithm.....	40
7.2	Where is the limit applied?.....	43
<b>8</b>	<b>Appendix</b> .....	<b>44</b>
8.1	Statistics file for limiting output data .....	44

# Introduction

## 1.1 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (<https://www.siemens.com/industrialsecurity>).

## 1.2 Useful information

### Introduction

The "Traffic Shaper" program limits the amount of data that a Windows PC (IPC) can send.

This restriction to a set limit is particularly important for Ethernet networks that transfer real-time data and non-real-time data in industrial applications.

If Windows PCs are also connected to industrial networks, there is a risk that individual Windows programs will send too much data over the Ethernet in a short period of time. Such a burst can disrupt the transfer of real-time data. This delays the arrival of process data and causes faults in production plants.

You can prevent such faults with the Traffic Shaper.

### Important notes

- The Traffic Shaper limits only non-real-time data, for example data that is sent via the TCP/IP protocol. PROFINET I/O data and other real-time data are not limited.
- Only dataflows generated by the Windows PC (IPC) are limited. The Traffic Shaper cannot influence dataflows that are simply transferred via two network adapters.
- Programs that cause a very high processor load, such as Iperf, jeopardize the proper functioning of the Traffic Shaper. The set limits can then possibly not be maintained.
- Improper application of the Traffic Shaper can have an impact on the performance of individual plant parts.

### Suitable hardware

Only Ethernet network adapters from Siemens (reserved MAC address area) are supported, such as network adapters in SIMATIC industrial PCs (IPCs) or the following Siemens network adapters:

- CP 1623 6GK1162-3AA00
- CP 1628 6GK1162-8AA00
- CP 1612 6GK1161-2AA01

You can find additional requirements for the installation of the Traffic Shaper in section Installation (Page 19).

### Information in the Online Support

You can find an overview of the most important technical information and solutions in the Siemens Industry Online Support (<https://support.industry.siemens.com>).

## Getting Started

### 2.1 Introduction

This section uses a simple example to show you how you can work with the Traffic Shaper.

#### Requirement

Traffic Shaper is already installed on the Windows PC whose outgoing Ethernet data is to be limited. For more information on installation, refer to the section Installation (Page 19).

#### Rule

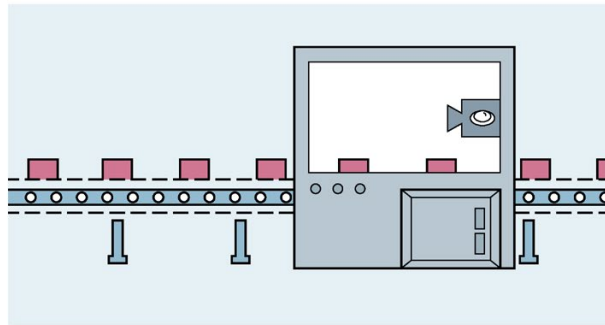
You must install the Traffic Shaper on all Windows PCs (IPC) that are connected to an Ethernet network used to transfer real-time data.

## 2.2 Image processing example

### Requirement

The example relates to a production plant in which processed workpieces are inspected for compliance with specific quality requirements. The surface of the workpieces is checked using image processing technology.

Image processing software is installed in the plant on an industrial PC (IPC) that is positioned close to a CCD camera. The CCD camera records the surfaces of the workpieces.



The images of the individual workpieces are analyzed by the image processing program, which decides whether the requirements have been met (using automatic edge detection, for example).

### Implementation

If a workpiece does not meet the requirements, the image processing program sends a message (50 bytes) over the LAN port of the IPC to a robot. The robot removes the workpiece from the production line. Defective workpieces are not processed further (rejected).

If a workpiece meets the requirements, the image processing program sends a message (50 bytes) to the robot to tell it not to remove the workpiece. Workpieces with no defects are processed further.

The example assumes that a workpiece is inspected and the image processing program sends a 5-byte message to the robot every four seconds.

This message is called "MessageToRobot" in the example.

The image processing program sends an image to the company quality department for each defective workpiece. In the example, this message is called "ImageToControlRoom" and contains an image of the defective workpiece that is around 120 kB.

The message is sent from the LAN connection of the IPC to the Quality department via the Ethernet network of the production plant. The Ethernet network of the production plant is also used to transfer the plant's real-time data.

### Error rate

The example assumes an acceptable error rate of 1/4. This means that every fourth workpiece can be defective. If the error rate increases, the plant must be stopped.

If every fourth workpiece can be defective, the image processing program sends images to the quality department every 16 seconds.

This additional data can disrupt the transfer of real-time data, posing a risk of production plant failure.

The Traffic Shaper enables you to limit the maximum data volume that a Windows PC (IPC) can send.

This protects production plants against Windows programs. The Ethernet network of the production plant is not affected by Windows programs.

The next section shows you how to set sensible limits.

## 2.3 Defining sensible limits

### Limits

The image processing program in the example sends non-real-time data to a robot and to the control room.

The data should be spread out evenly over a longer period and not transferred in one block. This applies in particular to the image data that is sent to the control room if a workpiece is defective and needs to be discarded.

Image files are extremely large (in the example around 120 kB).

Without effective upper limits from Traffic Shaper, the transfer of such image files leads to a series of Ethernet packets. The Ethernet packets are fed in directly to the Ethernet network one after the other via the Ethernet adapter and can disrupt the transfer of real-time data.

#### Spreading out data transfer over time

You should spread out the transfer of non-real-time data over the available time.

The following example uses the following burst and rate settings for the flows of data to the robot (MessageToRobot) and the control room (ImageToControlRoom):

Dataflows [LAN-1]				
Name	Active	Target IP address	Burst [byte]	Data rate [byte/msec]
Unknown dataflows	<input checked="" type="checkbox"/>	Unspecified	3000	10000
Multicast dataflows	<input checked="" type="checkbox"/>	Unspecified	3000	10000
ImageToControlRoom	<input checked="" type="checkbox"/>	192.168.178.41	1530	10
MessageToRobot	<input checked="" type="checkbox"/>	192.168.178.37	1530	10



**Burst**

In the example, 1530 bytes are set for the dataflows "MessageToRobot" and "ImageToControlRoom". That is why only one standard Ethernet frame (1514 bytes) is sent in each case. As only 16 bytes then remain (1530 to 1514), no further standard Ethernet frame is sent immediately after the first standard Ethernet frame. A pause in the dataflow is required. You can find more information on how the Traffic Shaper works in the section "Operating principle (Page 40)".

1530 bytes is the lowest value that can be entered for burst.

**Data rate**

The example uses a value of 10 bytes per millisecond as the data rate. This is the lowest value that can be set.

As only complete standard Ethernet frames with 1514 bytes can be sent, a complete standard Ethernet frame can be sent after around 152 milliseconds with a data rate of 10 bytes per millisecond (1514 bytes divided by 10 bytes per millisecond).

**Reliable transfer**

The burst and rate limits are used to minimize the load on the Ethernet network. This achieves one objective.

The reliable transfer of non-real-time data to the robot and to the control room must also be guaranteed. The situation as a whole therefore needs to be considered:

A standard Ethernet frame is transferred at intervals of around 152 milliseconds. An image size of 120 kB is used in the example. The complete image file of around 120 kB is therefore transferred in a series of 80 Ethernet frames. In each case the Ethernet frames have an interval of 152 milliseconds in between one another.

The transfer of the complete image thus takes around 13 seconds (152 milliseconds multiplied by 80) – sufficient time is therefore available.

## 2.4 Setting the upper limits

This section shows you how to set burst and rate limits.

### Step 1: Starting Traffic Shaper

Click on the following desktop icon to start Traffic Shaper:



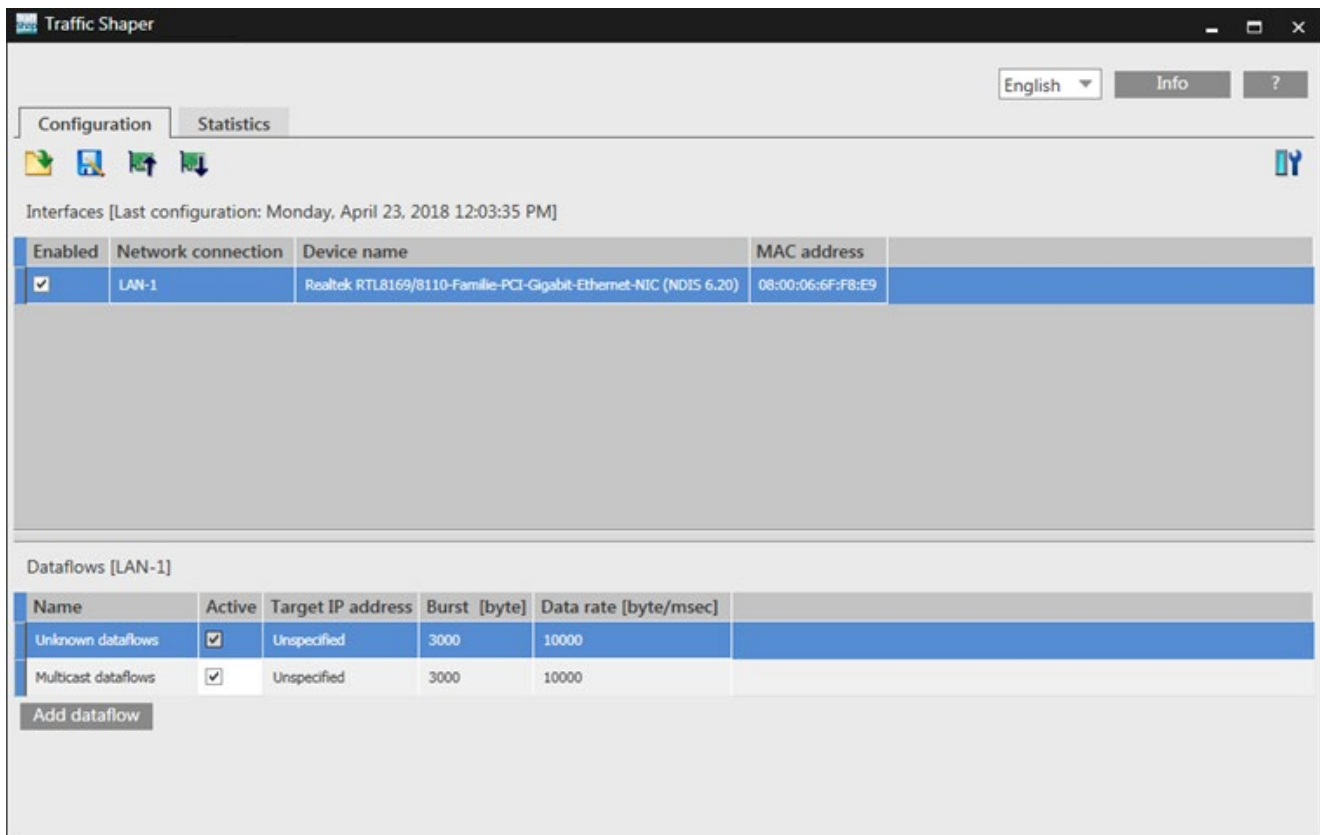
The user account control dialog is displayed.

### Step 2: Allow changes

Click on the "Yes" button to allow changes to your computer and start Traffic Shaper.

The Traffic Shaper is displayed.

The "Configuration" tab in the foreground shows the installed network interface cards and the dataflows of the first network adapter (highlighted in blue):



The following dataflows are already available after the first Traffic Shaper startup:

- Unknown dataflows

"Unknown Flows" contains all data packets for which no separate dataflow has been created in Traffic Shaper. You can not limit these data packets individually.

The "Target IP address" field is designated as "Unspecified".

Defaults are entered for burst and rate.

To limit these flows overall, you can change the burst and rate values. You can find additional information on this in "Step 3: Create the dataflow to the robot".

- Multicast dataflows

"Multicast dataflows" contains all data packets that are sent to all network devices as multicast Ethernet packets.

The "Target IP address" field is designated as "Unspecified".

Defaults are entered for burst and rate.

To limit the multicast dataflows overall, you can change the burst and rate values. You can find additional information on this in "Step 3: Create the dataflow to the robot".

To allow the targeted limiting of dataflows in our example, the next step adds a dataflow for the data packets. The data packets are sent to the robot and to the control room.

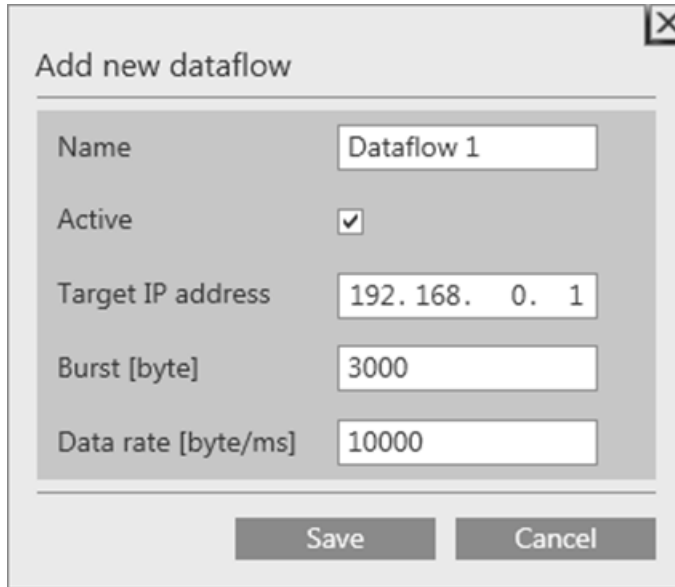
### Step 3: Create the dataflow to the robot

First, select the network adapter to which you want to add a new dataflow.

"LAN-1" is used in the example as the Windows PC is connected to the plant PROFINET/Ethernet network over this interface.

Click on the "Add Dataflow" button to add a dataflow to the selected interface for data packets from the Windows PC (IPC) to the robot.

The following dialog appears:



Enter the following changes in the fields in this dialog:

- Name  
Enter a unique name for the new dataflow in this field.  
In the example, "MessageToRobot" is used as name.
- Active  
When this checkbox is selected, the dataflow is activated. Traffic Shaper limits the dataflow.  
When you clear this check box, the dataflow is not activated and Traffic Shaper does not limit the dataflow. The new dataflow is not part of the "Unknown dataflows" dataflow.
- Target IP address  
This field contains the IP address of the Windows PC to which the data packets are sent: the target address of the dataflow.  
The example uses the IP address 192.168.178.37. This is the IP address of the Windows PC on which the robot control system in our example is installed.  
For your own projects, you will need to enter the IP address that you use in a given project.

- Burst [byte]

In our example, we enter 1530 bytes for the burst. A smaller value is not possible.

To prevent more than one standard Ethernet data packet from being sent to the robot, we use 1530 bytes in our example.

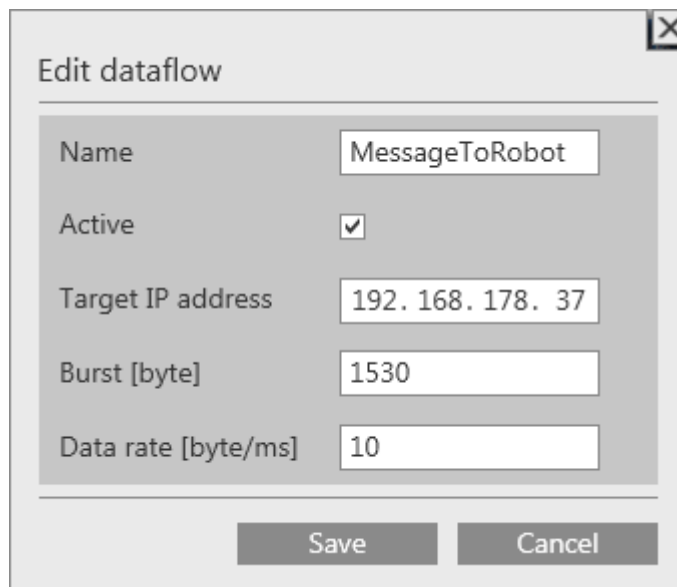
The image processing program only sends 60 bytes at a time, which means one standard Ethernet data packet is therefore quite sufficient. However, other data packets are required for establishing and terminating the TCP/IP connection.

- Data rate [byte/ms]

To spread out the data communication over time, a data rate of 10 bytes per millisecond is used in the example. A smaller value is not possible.

In the example, 10 bytes per millisecond is used to spread out data communication over time, as this minimizes the load on the PROFINET/Ethernet network caused by the dataflow to the robot. The load is detailed in section Defining sensible limits (Page 8).

The figure below shows the new dataflow with the changes:



Field	Value
Name	MessageToRobot
Active	<input checked="" type="checkbox"/>
Target IP address	192.168.178.37
Burst [byte]	1530
Data rate [byte/ms]	10

Click the "Save" button. Traffic Shaper creates the new dataflow and adds it to the list of dataflows for the selected network adapter. In our example, the "LAN-1" interface is selected (shown highlighted in blue).

#### Step 4: Create the dataflow to the control room

In the example, the "LAN-1" interface is also used for the dataflow to the control room. The existing selection is retained.

Now click on the "Add Dataflow" button to add a dataflow to the selected interface "LAN-1" for data packets from the Windows PC (IPC) to the control room.

Enter the following changes in the fields in this "Add new dataflow" dialog:

- Name

In the example, "ImageToControlRoom" is used as name.

- Active

The check mark remains selected. This activates the new dataflow and the limit is enabled.

- Target IP address

This field contains the IP address of the Windows PC to which the data packets are sent: the target address of the dataflow.

In the example, we use the IP address 192.168.178.41 for the Windows PC in the control room. The images of the rejected workpieces are sent to this IP address.

- Burst [byte]

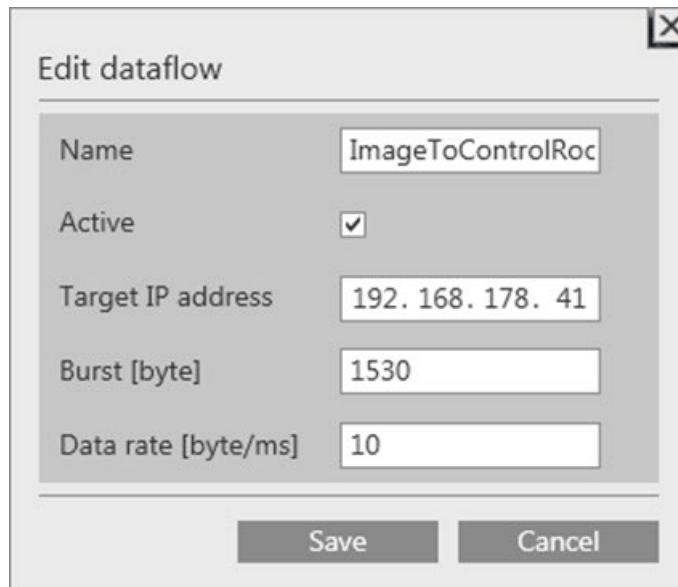
1530 bytes are used in the example. This means that only one standard Ethernet packet is sent to the control room – and then, after a pause, another standard Ethernet packet.

- Data rate [byte/ms]

To spread out the data communication over time, a data rate of 10 bytes per millisecond is used in the example. This minimizes the load on the PROFINET/Ethernet network caused by the dataflow to the control room. The load is detailed in "Defining sensible limits (Page 8)".

With this setting, the image processing program sends an image file (129 kB) in a series of 86 standard Ethernet data packets of 1514 bytes each. There is a pause of 151.4 milliseconds between each data packet.

The figure below shows the new dataflow with the changes:



The screenshot shows a dialog box titled "Edit dataflow". It contains the following fields and values:

Field	Value
Name	ImageToControlRoc
Active	<input checked="" type="checkbox"/>
Target IP address	192.168.178.41
Burst [byte]	1530
Data rate [byte/ms]	10

At the bottom of the dialog are two buttons: "Save" and "Cancel".

Click the "Save" button. Traffic Shaper creates the new dataflow and adds it to the list of dataflows for the selected network adapter. In our example, the "LAN-1" interface is selected.

### Step 5: Transfer new configuration to the interface

So far, you have added new dataflows and set limits for burst and rate.

Before these limits can actually be applied, you need to transfer the new settings to the interface.

Click on the following button to transfer the new values to the interface:



A dialog appears informing you that the new configuration may affect the runtime in your automation system.

- If you are not sure what impact the new configuration will have, click "No". The new configuration is then not transferred.

In this case, the configuration previously used is used. In our example, no configuration, as none has yet been transferred to the interface.

If no configuration has been transferred, the outgoing Ethernet dataflow will not be limited.

- If you are sure that the reliable transfer of real-time data in your plant will also be possible with the new configuration, click "Yes". Download of the new configuration then starts. A dialog appears indicating whether or not the data could be downloaded without errors.

Click "OK" to complete the download.

The settings in the new configuration are now effective and limit the outgoing Ethernet dataflows.

Important: Traffic Shaper also effectively limits outgoing Ethernet dataflows when the program is closed.

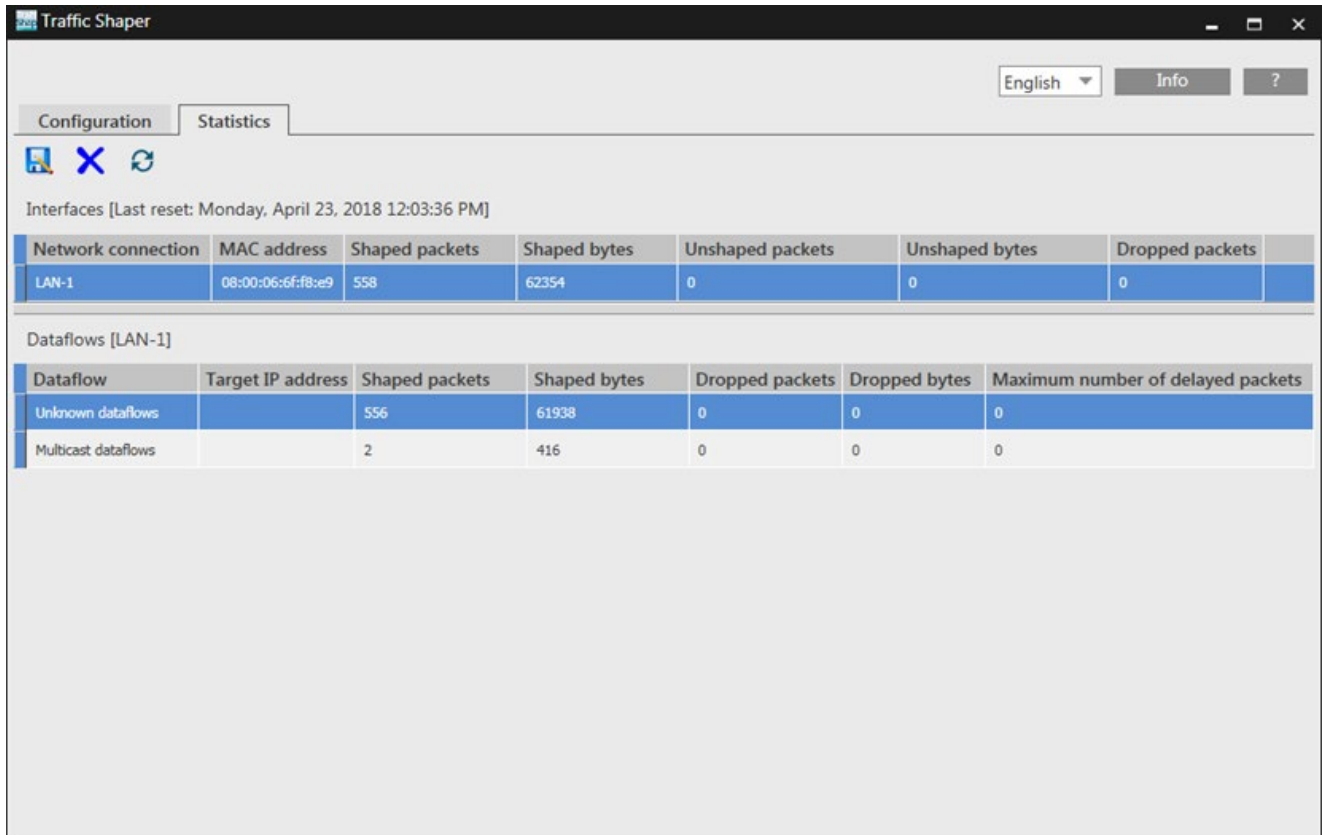


## Step 6: Access dataflow statistics

Traffic Shaper offers statistical functions for the outgoing Ethernet dataflows.

Click in the "Statistics" tab.

The "Statistics" tab is displayed:



The screenshot shows the Traffic Shaper application window with the "Statistics" tab selected. The window title is "Traffic Shaper". In the top right corner, there are buttons for "English", "Info", and "?". Below the tabs, there are icons for help, close, and refresh. The main content area displays two tables. The first table, titled "Interfaces [Last reset: Monday, April 23, 2018 12:03:36 PM]", shows statistics for the LAN-1 interface. The second table, titled "Dataflows [LAN-1]", shows statistics for unknown and multicast dataflows.

Network connection	MAC address	Shaped packets	Shaped bytes	Unshaped packets	Unshaped bytes	Dropped packets
LAN-1	08:00:06:6f:f8:e9	558	62354	0	0	0

Dataflow	Target IP address	Shaped packets	Shaped bytes	Dropped packets	Dropped bytes	Maximum number of delayed packets
Unknown dataflows		556	61938	0	0	0
Multicast dataflows		2	416	0	0	0

The screen above provides an overview of the dataflows in our example.

The figures relate to the period since the last Traffic Shaper reset.

- The "Interfaces" table shows the following values:
  - Number of shaped data packets (Shaped packets) and the amount of data in bytes (Shaped bytes)
  - Number of data packets that could not pass through the interface without limitation (Unshaped packets) and the amount of data in bytes (Unshaped bytes)
- The "Dataflows" table lists the following values for each dataflow:
  - Number of shaped data packets (Shaped packets) and the amount of data in bytes (Shaped bytes)
  - Number of dropped data packets (Dropped packets) and the amount of data in bytes (Dropped bytes)

If data packets could not be transferred, transfer is not reliable. You need to increase the data rate. However, ensure that real-time communication is not disrupted by the transfer of data.
- The column "Maximum number of delayed packets" shows how many data packets in a dataflow would have to wait before being sent in the worst-case scenario.

### Step 7: Update statistics

Traffic Shaper does not continually refresh the overview.

The overview is refreshed if the "Configuration" tab is in the foreground and you then click on the "Statistics" tab.

You can refresh the overview by clicking on the following button:



### See also

[Changing dataflows \(Page 36\)](#)

[Token bucket algorithm \(Page 40\)](#)

## System requirements for installation

The following table shows the minimum software and hardware requirements that have to be met for the installation of Traffic Shaper:

Hardware/software	Requirement
Processor	Intel® Celeron® Dual Core 2.2 GHz (Ivy/Sandy Bridge)
RAM	4 GB
Hard disk	250 GB S-ATA or more (of which at least 20 GB is available)
Network	From 100 Mbit
Network adapter	Only Ethernet network adapters from Siemens (reserved MAC address area) are supported, such as network adapters in SIMATIC industrial PCs (IPCs) or the following network adapters: <ul style="list-style-type: none"><li>• CP 1623 6GK1162-3AA00</li><li>• CP 1628 6GK1162-8AA00</li><li>• CP 1612 6GK1161-2AA01</li></ul>
Screen resolution	1024 x 768
Operating systems <sup>1)</sup>	64-bit version of the following operating systems: Windows 7 Ultimate SP1 Windows Embedded Std 7 SP1

## Recommended software and hardware requirements

The following table shows the recommended software and hardware for the operation of Traffic Shaper.

Hardware/software	Requirement
Computing unit	SIMATIC FIELD PG M5 PREMIUM or higher (or comparable PC)
Processor	Intel® Core™ i5-3320M 3.3 GHz or higher
RAM	16 GB or more
Hard disk	300 GB SSD or larger (of which at least 20 GB must be available)
Network	1 Gbit
Network adapter	Only Ethernet network adapters from Siemens (reserved MAC address area) are supported, such as network adapters in SIMATIC industrial PCs (IPCs) or the following network adapters: <ul style="list-style-type: none"> <li>• CP 1623 6GK1162-3AA00</li> <li>• CP 1628 6GK1162-8AA00</li> <li>• CP 1612 6GK1161-2AA01</li> </ul>
Monitor	15.6" Wide Screen Display (1920 x 1080 or larger)
Operating systems <sup>1)</sup>	64-bit version of the following operating systems: Windows 7 Ultimate SP1 Windows Embedded Std 7 SP1
Browser	An HTML5 compatible browser must be installed to view help. The following browsers have been tested with the help system. Other Web browsers may work as well, especially newer versions. If you have problems with browsers that are not mentioned here, use one of the following browsers: Internet Explorer 10 or 11 Mozilla Firefox (Version 38.3.0) Google Chrome (Version 46.0)

<sup>1)</sup> For more detailed information on operating systems, refer to the help on Microsoft Windows or the Microsoft Web site.

## Installation

1. Download the program package (<https://support.industry.siemens.com/cs/ww/en/view/109750661>) from the Internet.
2. Unpack the program to a folder of your choice in the file system.
3. Open the setup program "start.exe" in the "\DVD\" folder.
4. Follow the instructions in the installation program.

## First start

### Note

Only one instance of Traffic Shaper can be run on a Windows PC.

When you start Traffic Shaper for the first time, the "Interface Selection" dialog appears:

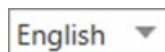


1. Select the interfaces whose data traffic you want to limit using Traffic Shaper. To do this, select the check mark in the "Selected" column.
2. Click on the following button to save your changes:



The user interface of Traffic Shaper appears.

3. If necessary, change the user interface language using the drop-down list:



## Version

For information on the installed version of Traffic Shaper, click on the following button in the top right of the main window:



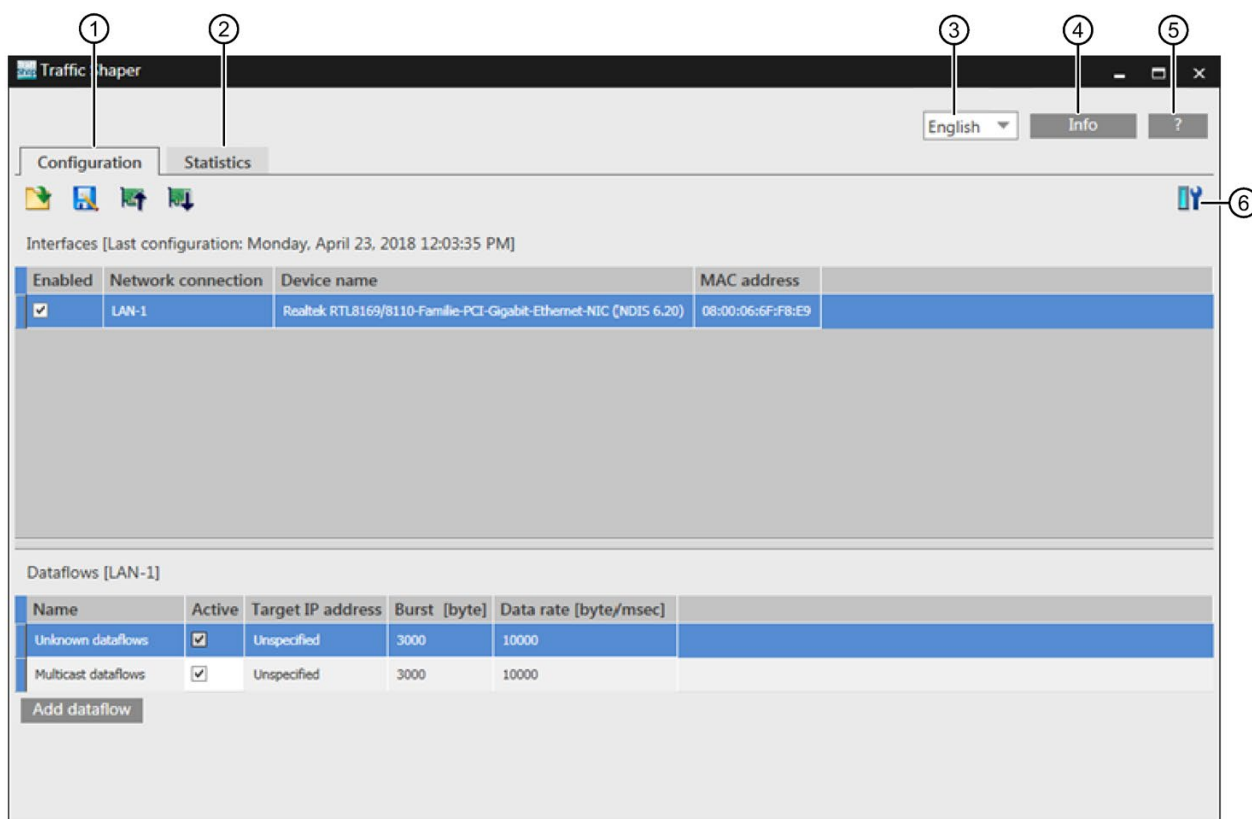
You can find more information on the installed version of Traffic Shaper in the section Overview (Page 22).

## See also

Useful information (Page 5)

# Graphical user interface

## 4.1 Overview



- ① "Configuration" tab
- ② "Statistics" tab
- ③ Change the language of the user interface
- ④ "Info" button
- ⑤ "Help" button
- ⑥ "Interface selection" button

### "Configuration" tab

In the "Configuration" tab, you can execute the following functions:

- Add, change and remove interfaces.
- Add, change, manage and delete dataflows for limiting Ethernet output data.

The "Configuration" tab is in the foreground when Traffic Shaper starts up.

### **"Statistics" tab**

In the "Statistics" tab, you can display information on the number and amount of data for:

- Shaped packets
- Unshaped packets
- Dropped packets
- Maximum number of delayed packets

### **Change the language of the user interface**

You can switch between the following languages using the drop-down list:

- German
- English

### **"Info" button**

You can display information on the installed program version with the "Info" button:

- Traffic Shaper version
- Release date
- Driver version

### **"Help" button**

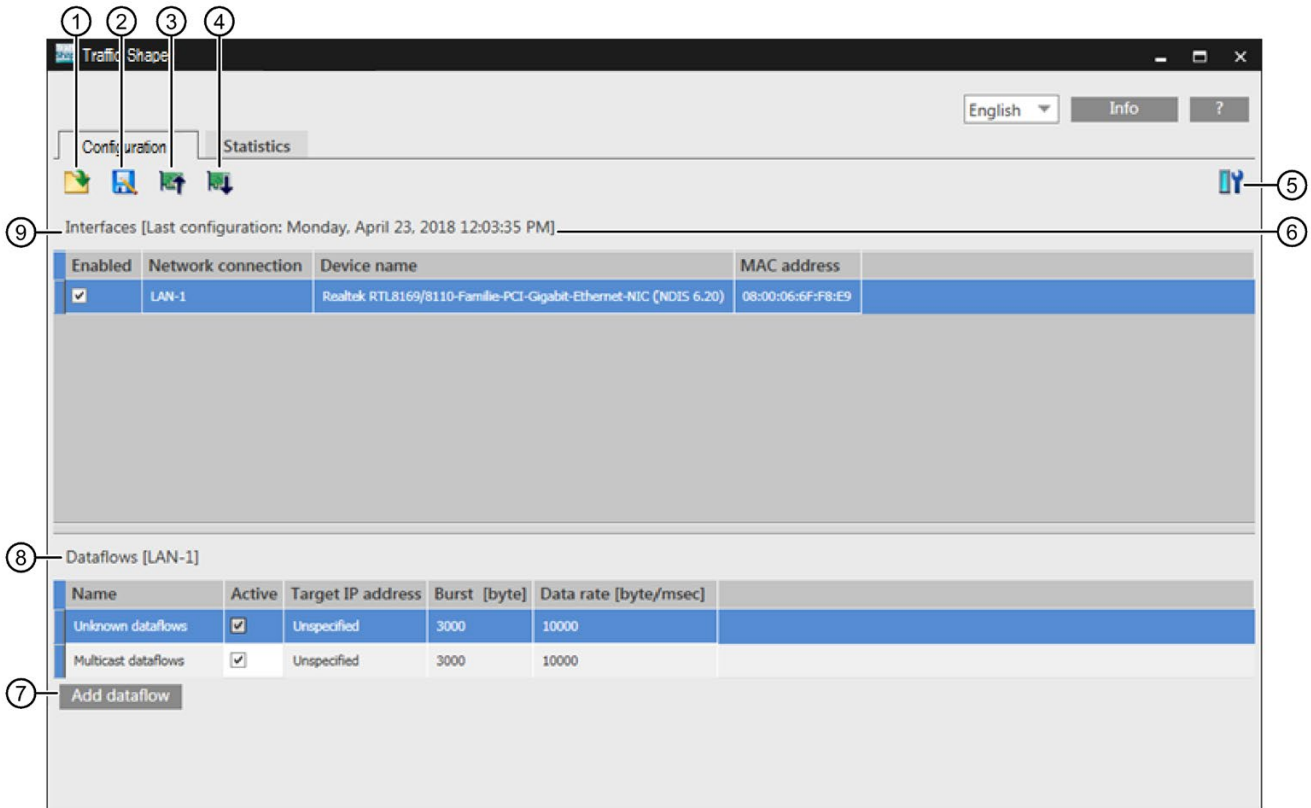
You can display the Traffic Shaper help with the "Help" button.

### **"Interface selection" button**

Using the "Interface Selection" button, you can select the interfaces whose data traffic you want to limit with Traffic Shaper.

## 4.2 "Configuration" tab

### Overview



- ① Load configuration file.  
The file must have the ending ".tsc" (Traffic Shaper Configuration).
- ② Back up current configuration as TSC file.
- ③ Upload and display configuration from driver.
- ④ Download configuration to driver.
- ⑤ Interface selection
- ⑥ Shows when the configuration displayed was last downloaded to the driver and thus became effective.
- ⑦ Opens the "Add new dataflow" dialog.
- ⑧ Table with dataflows for the selected interface
- ⑨ Table with installed and added interfaces



## Interfaces

The table shows the network adapters installed on the Windows PC.

---

### Note

The table only displays network adapters from Siemens.

---

### Note

A maximum of 5 interfaces may be enabled at one time.

---

The interface currently selected in the table is highlighted in blue. The dataflows for the selected interface are listed in the "Dataflows" table.

The following information is displayed for the interfaces listed:

- Enabled
  - Default after adding: Active (checkbox selected)
  - When you deactivate an interface, the dataflows through this interface are no longer limited.
- Network connection
  - Name of the network connection assigned to the network adapter.
- Device name
  - Name of network adapter
- MAC address
  - MAC address of the interface

## Dataflows

The table shows all dataflows that you have added for the selected interface.

The following dataflows are created by default for each interface:

- Unknown dataflows

Default: Activated

Contains all general dataflows that are not individually limited.

- Multicast dataflows

Default: Disabled

Contains all dataflows whose Ethernet data packets are sent to all accessible devices in the PROFINET/Ethernet network.

The following information is displayed for all flows listed:

- Name

You can select any dataflow name when you add the flow.

The names of the default dataflows cannot be changed.

- Active

Default: All flows activated

The Ethernet data packets of all activated dataflows are limited by Traffic Shaper in accordance with the "Burst" and "Rate" settings.

- Target IP address

IPv4 address of the dataflow recipient. Data packets with IPv6 addresses are not limited by Traffic Shaper.

No IP addresses have been entered for the default dataflows.

- Burst [byte]

Maximum number of bytes that can be sent in consecutive Ethernet data packets without the need for a pause between the individual packets.

- Data rate [byte/ms]

Maximum number of bytes that can be sent per millisecond.

## 4.3 "Statistics" tab

### Overview

Interfaces [Last reset: Monday, April 23, 2018 12:03:36 PM]

Network connection	MAC address	Shaped packets	Shaped bytes	Unshaped packets	Unshaped bytes	Dropped packets
LAN-1	08:00:06:6f:f8:e9	8544	1364530	1	42	0

Dataflows [LAN-1]

Dataflow	Target IP address	Shaped packets	Shaped bytes	Dropped packets	Dropped bytes	Maximum number of delayed packets
Unknown dataflows		8395	1322894	0	0	0
Multicast dataflows		149	41636	0	0	4

- ① Back up current statistics as XML file.
- ② Reset statistics to zero.
- ③ Update statistics.  
The statistics are automatically updated when you switch from the "Configuration" tab to the "Statistics" tab.
- ④ Shows when the statistics were last reset.
- ⑤ Table with dataflows for the selected interface
- ⑥ Table with installed and added interfaces

### Update statistics

1. Click on the following button to reset the statistics:



Counting starts again from zero.

2. Click on the following button to update the information:



### XML file

The information in the XML file allows you to analyze unknown flows and to determine the largest dataflows in "Unknown dataflows".

You can find an example of statistics in an XML file in Appendix (Page 44).

## Interfaces

The table shows the Siemens network adapters installed on the Windows PC.

---

### Note

The table only displays network adapters from Siemens.

Traffic Shaper only limits dataflows that are sent through Siemens network adapters.

---

The interface selected in the table is highlighted in blue. The dataflows for the selected interface are listed in the "Dataflows" table.

The following information is displayed for the interfaces listed:

- Network connection  
Name of the network connection assigned to the network adapter.
- MAC address  
MAC address of the interface
- Shaped packets  
Number of data packets that could not pass through the interface unaffected since the statistics were last reset.
- Shaped bytes  
Number of bytes of the data packets that could not be forwarded to the interface unaffected.
- Unshaped packets  
Number of data packets that could be forwarded to the interface unaffected.
- Unshaped bytes  
Number of bytes in the unaffected data packets
- Dropped packets  
Number of data packets that the recipient has not received and that have been lost since the statistics were last reset.

## Dataflows

The table shows all dataflows that you have added for the selected interface, and the default dataflows.

The following information is displayed for the dataflows:

- Dataflow

Dataflow name that you entered when you created the dataflow.

- Target IP address

IPv4 address of the dataflow recipient. Data packets with IPv6 addresses are not limited by Traffic Shaper.

No IP addresses have been entered for the default dataflows.

- Shaped packets

Number of data packets that could not pass through the interface unaffected since the statistics were last reset.

- Shaped bytes

Number of bytes in the affected data packets that were not forwarded unaffected to the interface.

- Dropped packets

Number of data packets that the recipient has not received and that have been lost since the statistics were last reset.

- Dropped bytes

Number of bytes in the data packets that the recipient has not received and that have been lost since the statistics were last reset.

- Maximum number of delayed packets

Maximum number of data packets that had to queue for this dataflow until they could be sent since the last time the statistics were reset.

## Dataflows

### 5.1 Introduction

#### Definition

Traffic Shaper defines a dataflow as a sequence of Ethernet data packets that are sent to a specific Windows PC or to all Windows PCs in a network.

A dataflow comprises all Ethernet data packets structured in accordance with IPv4. IPv6 data packets are not affected.

A dataflow consists of all data packets that are sent to the TCP or UDP ports of a Windows PC.

The burst and rate settings for a dataflow apply to this dataflow as a whole.

You can find more information on the properties of dataflows in "Configuration" tab (Page 24).

#### Limitation

You cannot limit individual ports with Traffic Shaper. The dataflow of individual programs is therefore not limited.

### 5.2 Unknown dataflows

#### Definition

Traffic Shaper uses the designation "Unknown Flows" for all dataflows that are not individually limited. These dataflows are created as a collective dataflow.

The same maximum burst and rates apply for all dataflows in this collective flow.

**Procedure**

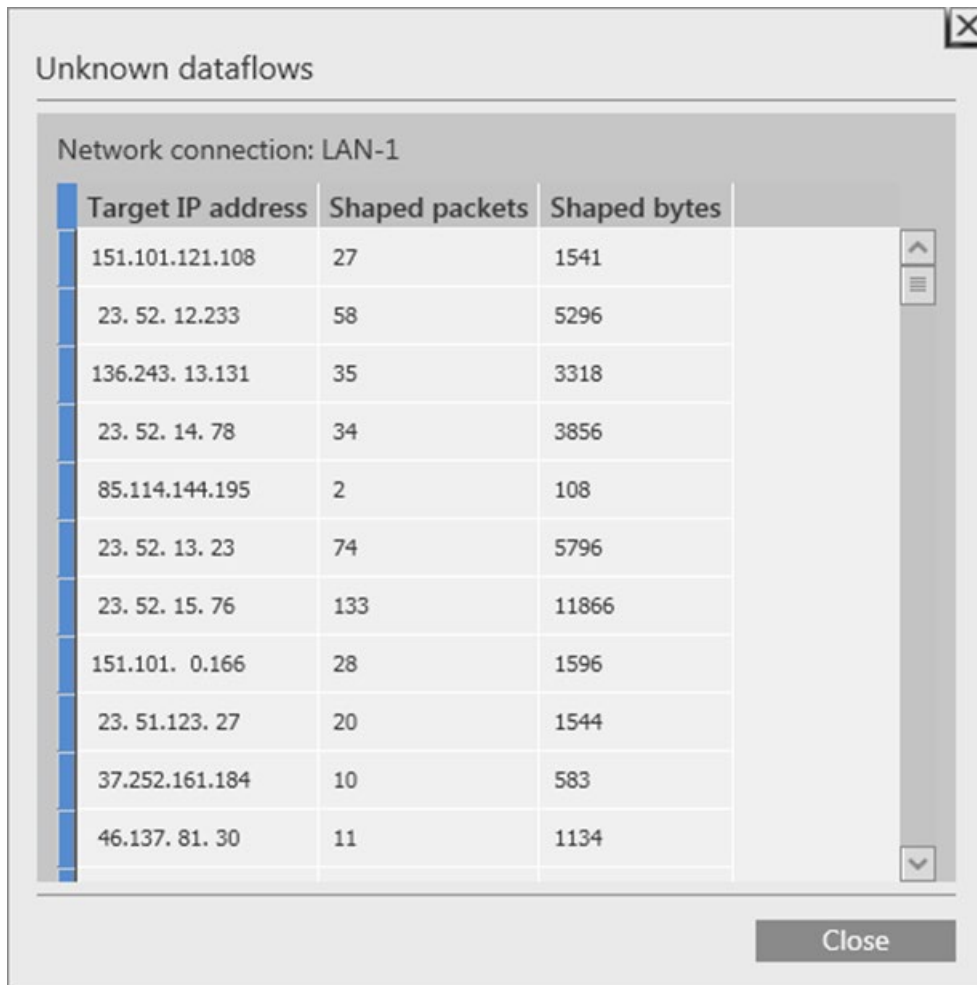
Proceed as follows to get an overview of the unknown flows that your Windows PC sends to the connected PROFINET/Ethernet.

1. Select the "Statistics" tab.
2. In the "Interfaces" table, right-click on an interface to view its unspecified dataflows.  
The context menu is displayed.
3. Click on "Show IP addresses from unknown dataflows" in the context menu.

Alternative:

1. Select the "Statistics" tab.
2. In the "Interfaces" table, click on an interface to view its unspecified dataflows.
3. Right-click on the "Dataflows" table.
4. Click on "Show IP addresses from unknown dataflows" in the context menu.

The "Unknown dataflows" dialog appears:





The following information is displayed for the flows listed:

- Target IP address  
IPv4 address of the dataflow recipient. Data packets with IPv6 addresses are not limited by Traffic Shaper.
- Shaped packets  
Number of data packets that could not pass through the interface unaffected since the statistics were last reset.
- Shaped bytes  
Number of bytes in the affected data packets that were not forwarded unaffected to the interface.

If you add a dataflow on the "Configuration" tab, the dataflow is then no longer one of the unknown dataflows.

You can find more information on adding dataflows in Adding dataflows (Page 34).

## Benefits

The "Unknown dataflows" dialog provides an overview of the unknown data packets in the outgoing Ethernet data traffic of your Windows PC.

Create separate dataflows for all unknown dataflows. Set the upper limits for burst and rate individually for each dataflow. Limit the outgoing dataflows as far as possible.

You can copy and paste the IP address of a dataflow from the "Unknown dataflows" dialog to the dialog for creating dataflows.

## 5.3 Multicast dataflows

### Definition

Multicast dataflows consist of a sequence of Ethernet data packets that your Windows PC sends to all accessible devices in the PROFINET/Ethernet network over its Ethernet interface.

## 5.4 Adding dataflows

### Procedure

1. Select the "Configuration" tab.
2. In the "Interfaces" table, click on the interface to which you want to add a new dataflow.
3. Click on the following button below the "Dataflows" table:

**Add dataflow**

The "Add new dataflow" dialog appears:

The "Add new dataflow" dialog box contains the following fields and values:

Field	Value
Name	Dataflow 1
Active	<input checked="" type="checkbox"/>
Target IP address	192.168.0.1
Burst [byte]	3000
Data rate [byte/ms]	10000

Buttons: Save, Cancel

4. Fill in the input boxes in the dialog.

See the explanations on burst and rate in Defining sensible limits (Page 8) and Operating principle (Page 40).

– Name

Enter a unique name for the dataflow.

Use the source and the target of the dataflow in the name.

The names of the default dataflows cannot be changed.

– Active

Default: Activated

The Ethernet data packets of all activated dataflows are limited by Traffic Shaper in accordance with the Burst and Rate settings.

– Target IP address

IPv4 address of the dataflow recipient. Data packets with IPv6 addresses are not limited by Traffic Shaper.

– Burst [byte]

Maximum number of bytes that can be sent in consecutive Ethernet data packets without the need for a pause between the individual packets.

– Data rate [byte/ms]

Maximum number of bytes that can be sent per millisecond.

5. Click on "Save" to save your changes.

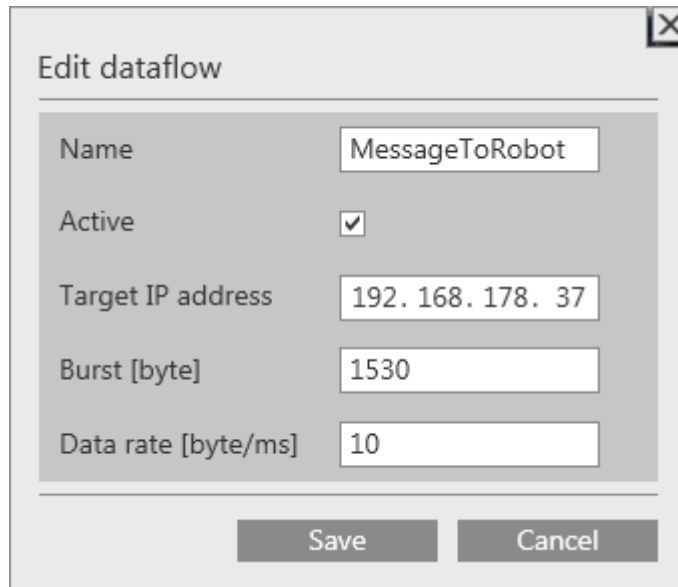
The newly created dataflow is displayed in the "Dataflows" table.

## 5.5 Changing dataflows

### Procedure

1. Select the "Configuration" tab.
2. In the "Interfaces" table, click on an interface to change its dataflows.  
The "Dataflows" table shows the dataflows that belong to the selected interface.
3. In the "Dataflows" table, right-click on the dataflow that you want to change.  
The context menu is displayed.
4. Click "Edit dataflow" in the context menu.

The "Edit dataflow" dialog appears:



The "Edit dataflow" dialog box contains the following fields and values:

Field	Value
Name	MessageToRobot
Active	<input checked="" type="checkbox"/>
Target IP address	192.168.178.37
Burst [byte]	1530
Data rate [byte/ms]	10

Buttons: Save, Cancel

5. Change the input boxes in this dialog.  
See the explanations on burst and rate in Defining sensible limits (Page 8) and Operating principle (Page 40).
6. Click on "Save" to save your changes.  
The dataflow is now displayed with the changes in the "Dataflows" table.

## 5.6 Removing dataflows

### Procedure

1. Select the "Configuration" tab.
2. In the "Interfaces" table, click on an interface to remove its dataflows.  
The "Dataflows" table now shows the dataflows that belong to the selected interface.
3. In the "Dataflows" table, right-click on the dataflow that you want to remove.  
The context menu is displayed.
4. Click on "Remove dataflow" in the context menu.  
The dataflow is deleted and is no longer displayed in the "Dataflows" table.

# Configuration

## 6.1 What is a configuration?

### Definition

Traffic Shaper limits the amount of data that a Windows PC can send to an Ethernet network over its Ethernet interface.

A configuration contains burst and rate limits for the individual dataflows. These limits must not be exceeded.

See the explanations on burst and rate in [Defining sensible limits \(Page 8\)](#) and [Operating principle \(Page 40\)](#).

## 6.2 Managing configurations

### Procedure

#### Downloading a configuration from a TSC file

1. Select the "Configuration" tab.
2. Click on the following button in the "Configuration" tab:



#### Backing up a configuration to a TSC file

1. Select the "Configuration" tab.
2. Click on the following button in the "Configuration" tab:



#### Upload configuration from driver and display

1. Select the "Configuration" tab.
2. Click on the following button in the "Configuration" tab:



#### Download configuration to driver

1. Select the "Configuration" tab.
2. Click on the following button in the "Configuration" tab:



You can find more information on changing a configuration by adding, changing and removing dataflows in Dataflows (Page 31).

## Operating principle

### 7.1 Token bucket algorithm

#### Token

The token bucket algorithm works with tokens: A token gives the right to send 1 byte (transfer right). If a dataflow has 1530 tokens, for example, 1530 bytes can be sent.

Once all tokens have been used, the dataflow must wait until enough tokens are available again. This allows a dataflow to be evenly spread over a longer time and reduces the load on the connected Ethernet network.

#### Bucket

A bucket is a container in which the tokens of a dataflow are collected.

The bucket receives a certain number of tokens at intervals of one millisecond.

You specify the number of tokens that the bucket receives per millisecond when you set the rate (byte/ms).

You can find additional information on setting the data rate in [Setting the upper limits](#) (Page 10).

#### Rate

If you set a data rate of 306 bytes/ms, the bucket receives 306 tokens per millisecond. After five milliseconds, a standard Ethernet data packet with 1514 bytes can be sent as there are now 1530 tokens in the bucket.

Low data rates allow the transfer of data packets to be delayed and the load on the Ethernet network to be reduced.

The rate set must be at least 10 bytes/ms.

---

#### Note

If no data packet is sent over a prolonged period of time or fewer tokens are used than become available, there is a risk of too many tokens collecting in the bucket. When data packets then have to be sent again, too many data packets are sent at once as there are enough tokens in the bucket.

---

#### Burst

If too many tokens have collected in the bucket, a very large file (for example, image file) can be transferred over the Ethernet network in a close sequence of standard Ethernet data packets (burst). This can seriously disrupt the transfer of real-time data.

Traffic Shaper therefore applies a limit to the number of tokens that can be in the bucket. The burst for a dataflow is set in bytes and must be at least 1530 bytes.

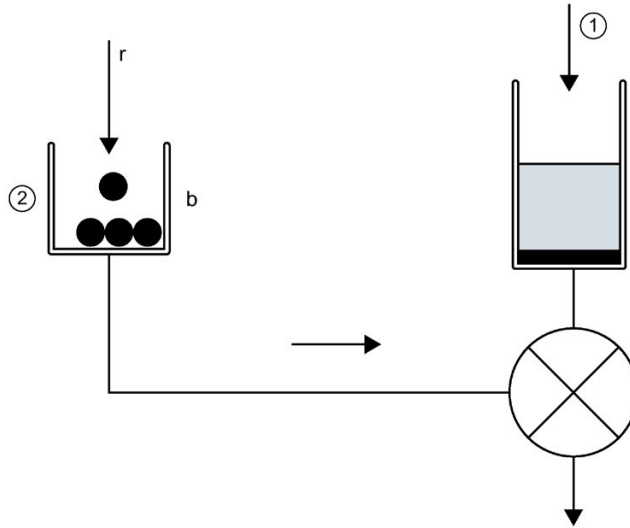
You can find additional information on setting the burst and data rate in [Setting the upper limits](#) (Page 10).



### Mode of operation (example)

**Initial situation:**

- 1530 bytes can be sent every 5 milliseconds.
- A data packet has either 60 bytes or 1514 bytes.



- ① Data packets
- ② Token

1. Every millisecond, the bucket **b** receives 306 tokens as a result of the set data rate *r*. After 5 milliseconds, the bucket **b** contains enough tokens for 25 data packets of 60 bytes each or 1 standard Ethernet data packet of 1514 bytes.
2. One standard Ethernet data packet of 1514 bytes is sent. 1 token is removed from the bucket **b** for each byte transferred. 16 tokens remain in the bucket.

After another 5 milliseconds, there are again enough tokens in the bucket **b** and the next standard Ethernet data packet of 1514 bytes can be sent.

**Problem:** For a standard Ethernet data packet with 1514 bytes, not all available tokens in the bucket are used. For example, after 20 milliseconds there are enough tokens in the bucket **b** to send more than 25 data packets of 60 bytes each.

Sample calculation:

Time (ms)	New tokens in the bucket	Use (bytes)	Tokens remaining in the bucket after standard Ethernet data packet is sent
1	306	-	306
5	1530	1514	16
10	1530	1514	32
15	1530	1514	48
20	1530	1514	64

After 20 ms, the maximum permissible data volume of 1530 bytes per 5 milliseconds is exceeded.

7.1 Token bucket algorithm

---

**Solution:** The maximum number of tokens in the bucket is limited to 1530 tokens by setting a burst. The set data volume of 1530 bytes per 5 milliseconds is not exceeded.

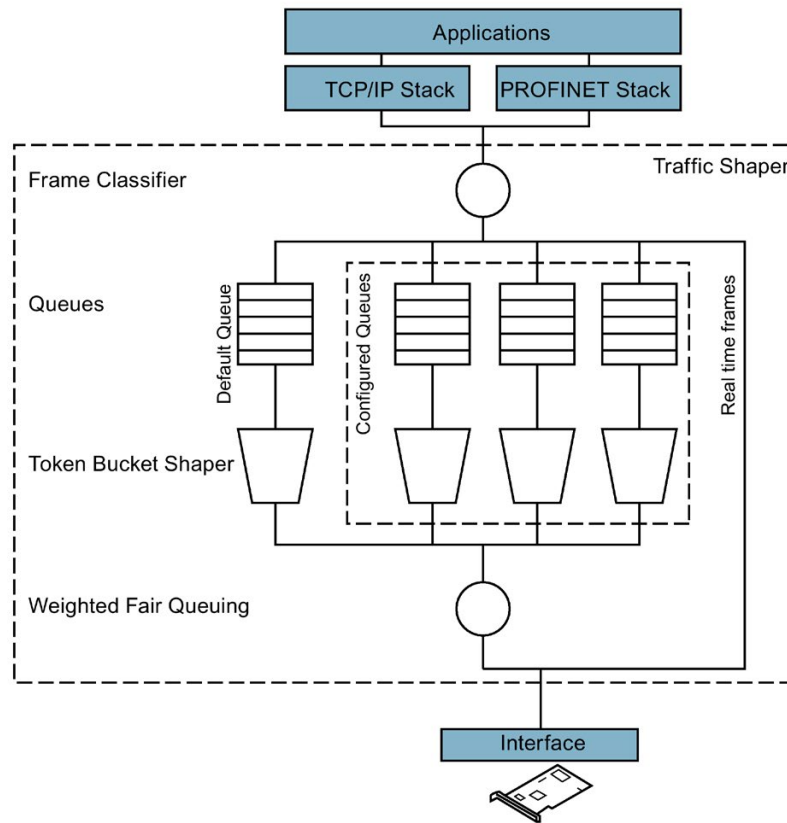
Sample calculation:

Time (ms)	New tokens in the bucket	Use (bytes)	Tokens remaining in the bucket after standard Ethernet data packet is sent
1	306	-	-
5	1530	1514	16
10	1514	1514	16
15	1514	1514	16
20	1514	1514	16

## 7.2 Where is the limit applied?

### Where are dataflows limited?

Traffic Shaper uses a driver to limit dataflows. This driver is located below the TCP/IP stack and above the assigned Ethernet network adapter:



All outgoing Ethernet data packets pass through the Token Bucket Shaper and are shaped by it. Real-time data is not affected by Traffic Shaper.

If the "Multicast dataflows" dataflow is enabled, Traffic Shaper also shapes Traffic Multicast and Broadcast data packets. You can find more information on "Multicast dataflows" in the section Dataflows (Page 31).

If you add a dataflow in Traffic Shaper, a separate queue (configured queue) is set up for the data packets of that dataflow.

A separate Token Bucket Shaper comes after each queue. It limits the dataflow in line with the set values for burst and rate. You can find more information on burst and rate in Defining sensible limits (Page 8) and Token bucket algorithm (Page 40).

A process scheduler combines the individual dataflows again and forwards them to the network adapter.

## Appendix

### 8.1 Statistics file for limiting output data

#### Example

```
<?xml version="1.0"?>
<Statistics xmlns:xsd="http://www.w3.org/2001/XMLSchema"
StatisticCounterResetTime="Wednesday, February 15, 0417 10:15:04
AM">
  <Interfaces>
    <XmlStatisticInterface ShapedFrames="6154" ShapedBytes="680821"
UnShapedFrames="1144" UnShapedBytes="455616" DroppedFrames="0"
NetworkId="LAN-1" Mac="00:24:81:60:75:f3">
      <Flow Name="EN - unknown flows">
        <ShapedFrames>4924</ShapedFrames>
        <ShapedBytes>458253</ShapedBytes>
        <DroppedFrames>0</DroppedFrames>
        <DroppedBytes>0</DroppedBytes>
        <MaxDelayedFrames>0</MaxDelayedFrames>
        <UnknownFlows>
          <XmlUnknownFlow DestinationIp="151.101.1.69">
            <ShapedFrames>143</ShapedFrames><ShapedBytes>10688</ShapedByte
s>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="172.217.21.193">
            <ShapedFrames>7</ShapedFrames><ShapedBytes>3553</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="192.0.73.2">
            <ShapedFrames>15</ShapedFrames><ShapedBytes>1703</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="104.121.185.71">
            <ShapedFrames>17</ShapedFrames><ShapedBytes>2476</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="54.243.104.69">
            <ShapedFrames>27</ShapedFrames><ShapedBytes>5524</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="104.17.27.15">
            <ShapedFrames>30</ShapedFrames><ShapedBytes>3706</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="104.121.150.8">
            <ShapedFrames>7</ShapedFrames><ShapedBytes>944</ShapedBytes>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="172.217.21.206">
            <ShapedFrames>42</ShapedFrames><ShapedBytes>10330</ShapedBytes
>
          </XmlUnknownFlow>
          <XmlUnknownFlow DestinationIp="104.121.150.9">
            <ShapedFrames>9</ShapedFrames><ShapedBytes>2629</ShapedBytes>
          </XmlUnknownFlow>

```

```

    <XmlUnknownFlow DestinationIp="95.172.94.62">
      <ShapedFrames>5</ShapedFrames><ShapedBytes>1604</ShapedBytes>
    </XmlUnknownFlow>
    <XmlUnknownFlow DestinationIp="50.17.181.149">
      <ShapedFrames>9</ShapedFrames><ShapedBytes>2159</ShapedBytes>
    </XmlUnknownFlow>
    <XmlUnknownFlow DestinationIp="50.17.205.172">
      <ShapedFrames>9</ShapedFrames><ShapedBytes>2163</ShapedBytes>
    </XmlUnknownFlow>
    <XmlUnknownFlow DestinationIp="65.55.252.71">
      <ShapedFrames>13</ShapedFrames><ShapedBytes>1826</ShapedBytes>
    </XmlUnknownFlow>
  </UnknownFlows>
</Flow>
<Flow Name="EN - multicast flows">
  <ShapedFrames>577</ShapedFrames>
  <ShapedBytes>138000</ShapedBytes>
  <DroppedFrames>0</DroppedFrames>
  <DroppedBytes>0</DroppedBytes>
  <MaxDelayedFrames>5</MaxDelayedFrames>
</Flow>
<Flow Name="MessageToRobot">
  <IPAddress>192.168.178.37</IPAddress>
  <ShapedFrames>377</ShapedFrames>
  <ShapedBytes>39158</ShapedBytes>
  <DroppedFrames>0</DroppedFrames>
  <DroppedBytes>0</DroppedBytes>
  <MaxDelayedFrames>0</MaxDelayedFrames>
</Flow>
<Flow Name="ImageToControlRoom">
  <IPAddress>192.168.178.41</IPAddress>
  <ShapedFrames>276</ShapedFrames>
  <ShapedBytes>45410</ShapedBytes>
  <DroppedFrames>0</DroppedFrames>
  <DroppedBytes>0</DroppedBytes>
  <MaxDelayedFrames>6</MaxDelayedFrames>
</Flow>
</XmlStatisticInterface>
  <XmlStatisticInterface ShapedFrames="0" ShapedBytes="0"
UnShapedFrames="0" UnShapedBytes="0" DroppedFrames="0"
NetworkId="WLAN" Mac="00:21:00:cf:fa:71">
  <Flow Name="EN - unknown flows">
    <ShapedFrames>0</ShapedFrames>
    <ShapedBytes>0</ShapedBytes>
    <DroppedFrames>0</DroppedFrames>
    <DroppedBytes>0</DroppedBytes>
    <MaxDelayedFrames>0</MaxDelayedFrames>
  </Flow>
</XmlStatisticInterface>
</Interfaces></Statistics>

```

