TRAFip Manual

TRAFip Manual

Table of Contents

Preface x
- Target audience x
- Conventions used in this manual x

1. Introduction 1
- About 1
- Main features 1
- Minimum requirements 2
  - Hardware 2
  - Browser 2

2. Basic concepts 3
- Netflow 3
- jFlow 3
- IPFIX 3
- Huawei Netstream 3
- sFlow 3
- Objects definition 4
- TRAFip analysis scenarios 4
  - Full mesh networks 4
  - Point-multipoint networks 5
  - Internet Service Provider networks 6

3. Quick startup guide 8
- Accessing the WEB interface 8
- Interface traffic analysis 9

4. Telcomanager grapher 10
- Period 10
  - Daily graph 10
  - Weekly graph 10
  - Monthly graph 10
  - Quarterly graph 10
  - Yearly graph 10
  - Biennially graph 10
  - Five years graph 11
  - Custom graph 11
- Features 11
  - Statistics box 11
  - Show value 11
  - Vertical zoom 11
  - Single curve 11
  - Relative mode 11
  - Axis configuration 11
  - Add to graphset 12
  - Graph type 12
  - Save image 12
  - Aggregated chart 12
  - Zoom in and zoom out 12
  - Export 12
  - Auto refresh 12
  - Report 12
  - Keys 13

5. Historical data 14
- Network Overview 14

Favorites 15
Adding objects to the Favorites 15
Removing objects from the Favorites 15
Totals 15
Subnets 15
Definitions 15
Configuration 15
Import subnets file 16
Subnet groups 17
Definitions 17
Configuration 17
Aggregation 17
Devices 18
Create Device using Wizard 21
Verifying mapped objects for the device 21
Import devices file 22
Interface group 22
Unmatched traffic 23
Applications 23
Classification 24
Import applications file 24
Application groups 25
Protocols 25
Import protocols file 26
Autonomous Systems 26
Import autonomous system file 27
Autonomous system group 27
Type of service 27
Import ToS file 28
ToS group 28
Reports 29
Templates 29
Suspect traffic 30
Top N 31
Traffic profile 32
Syslog 33
Rawdata 34
Trend Analysis 36
Graph set 37
Definitions 37
Creation 37
Adding graphs 38
Visualizing a Graph set 38
Editing a Graph set 38
Generating graphs for a Graph set 38
NOC Display 39
6. Configuration 40
Traffic profiles 40
Definitions 40
Configuration 40
Analysis types 41
Domains 42
Definitions 42
Configuration 42

RFI interfaces 43
Collectors 44
Import collectors file 45
Objects 45
Importing object files 45
Mappers 45
Cross OID mapping 47
Associating devices to mappers 47
Exporting and importing mappers 47
EPM (Extended Processing Module) 47
Rules 48
Creating rules 48
No Response filter 48
Device Credential 48
7. Tools 50
External Software 50
Telcomanager Windows Collector 50
Telcomanager Host Agent 50
Telcomanager Windows Security Agent 50
Discovery 50
8. System 51
Access Log 51
User access 51
Simultaneous access 51
Users 51
Editing users 51
User Groups 52
User profiles 53
Alarm Console 53
Backup/Restore 54
Local configuration backup 54
Local configuration restore 54
Remote backup 54
Remote restore 55
Restore status 55
Parameters 55
Active directory 55
ALARMmanager 56
Association agents 56
Auto login 56
Backup 57
Capture agent configuration 57
Cisco WAAS 57
Configuration history 57
Data storage 58
dbn0/Altaia integration 59
Distributed architecture 60
EPM 60
Expiration warning 60
File transfer 61
Flow exporters verification 61
Grapher 61
HTTPS Configuration 62
Interface customization 62

Local preferences 62
Login redirection 62
Log level 62
Logo 63
Object Mapper 63
Redundancy 63
Regional settings 64
Reports 64
SMS server 65
Simple filter 65
SMTP 66
SNMP 66
System Version Check 67
TACACS 67
Theme 67
Threat Analysis 68
TRAFip 68
Trend Analysis 68
User access history 68
Web Services 68
Diagnostics 69
Network information 69
Connectivity tests 69
Packet Capture 69
Objects 70
Flow exporters 70
Flow statistics 70
Summarizer 70
Storage usage 70
Log files 70
Configuration Logs 71
Suspect Traffic Statistics 71
Timezone 71
Support 71
About 72
9. ALARMmanager 73
Reports 73
Suppressed reports 73
Consolidated reports 73
Email Template 74
Introduction 74
Customizing the email 74
Alarm urgency level 75
Changing the urgency level priority 75
Adding a new urgency level 75
Alarms 76
Default alarm configuration 76
Behavior change alarm configuration (History Alarms) 78
Actions 81
Alarm suppression management 82
Alarm profile 82
Service Alarms 83
Introduction 83
Formula 83

Console 83
Introduction 83
Console operation 83
10. License enabled features 87
Redundancy 87
Concepts 87
Enabling the redundancy 87
Distributed architecture 87
Concepts 87
Prerequisites 87
Deployment 88

List of Tables

1. Manual conventions x
4.1. Keys 13
5.1. Icons list 15
5.2. New subnet form 16
5.3. Fields from subnet file 16
5.4. New subnet group form 17
5.5. New aggregation form 18
5.6. New device form 18
5.7. Fields from device file 22
5.8. Interface group form 23
5.9. Application form 23
5.10. Fields from application file 24
5.11. Application group form 25
5.12. Protocol form 25
5.13. Fields from protocol file 26
5.14. AS form 26
5.15. Fields from autonomous system file 27
5.16. AS group form 27
5.17. ToS form 28
5.18. Fields from ToS file 28
5.19. ToS group form 29
5.20. Template Form 29
5.21. Suspect traffic report 31
5.22. Top N report 31
5.23. Traffic profile report 32
5.24. Syslog report 34
5.25. Raw data report 34
5.26. Trend analysis configuration form 36
5.27. Trend analysis report form 37
5.28. Graph set creation 37
6.1. Traffic profile form 40
6.2. Domain form 42
6.3. Collector form 44
6.4. Fields from collectors file 45
6.5. Mapper form 46
6.6. Automatic profile rules 48
6.7. Device credential form 48
8.1. User form 51
8.2. User form 52
8.3. User form 53
8.4. ALARMmanager console columns 53
8.5. Remote backup form 54
8.6. Active directory form 55
8.7. ALARMmanager parameters form 56
8.8. Automatic association agent for mappers form 56
8.9. Capture agent configuration form 57
8.10. Cisco WAAS form 57
8.11. Log history parameters 57
8.12. Data storage form 58
8.13. dbn0/Altaia integration form 59
8.14. Distributed architecture parameters form 60

8.15. EPM form 60
8.16. Expiration warning form 61
8.17. Grapher parameters form 61
8.18. Https parameters form 62
8.19. Device formula name 62
8.20. Local preferences form 62
8.21. Object mapper configuration parameters form 63
8.22. Redundancy settings 63
8.23. Regional settings form 64
8.24. Scheduled reports configuration form 64
8.25. TRAFip raw data 64
8.26. SMPP server form 65
8.27. SMTP parameters form 66
8.28. TRAP fields 67
8.29. Theme configuration 67
8.30. Threat analysis configuration 68
8.31. User access history form 68
8.32. Configurations API form 68
8.33. TRAFip's raw data form 69
8.34. Packet Capture 69
9.1. Suppressed alarms report form 73
9.2. Consolidated alarm report form 73
9.3. Email template 74
9.4. Email variables 74
9.5. ALARM urgency level form 75
9.6. Default alarm form 76
9.7. Metrics representation 77
9.8. Behavior change alarm form 78
9.9. Metrics representation 80
9.10. Alarm profile form 82
9.11. ALARMmanager console 84

Preface

Target audience

This manual was designed for network administrators, network consultants and Telcomanager partners.

To fully understand this manual, the reader should have intermediate knowledge on network management, TCP/IP protocol and SNMP protocol.

Conventions used in this manual

This document uses the following conventions:

Table 1. Manual conventions

Item	**Convention**
Selecting a menu item	**Menu** → **Submenu** → **Menu item**
Commands, buttons and keywords	**Boldface** font.

Chapter 1. Introduction

About

TRAFip is a traffic characterization system for IP networks. It is deployed in the network in a non-intrusive way and receives information about IP traffic using the Netflow protocol or through direct capture in one of its network interfaces.

Main features

- Support for NetFlow, jFlow, sFlow, IPFIX and Huawei netstream.
- Access to all system features through a web browser.
- Syslog collection and reporting.
- Formula creation, allowing users to define their own KPIs (Key Performance Indicators).
- Scalable architecture. The system can grow on the number collected elements by the use of remote collectors appliances and on the number of users and reports supported through the deployment of EPMs (Expanded Processing Modules), which are appliances responsible to perform load sharing with the central system.
- High Availability can be provided trough the use of the redundant solution, in which two appliances work in HOT-STANDBY.
- Trend analysis reports.
- All reports can be saved as templates, scheduled and exported in PDF, HTML and CSV format.
- Mass graph image export.
- Flexible graph creation.
- Interactive HTML5 grapher, with features like vertical and horizontal zoom, auto-scale and aggregated charts.
- High performance database for historical data storage.
- Top N reports for all monitored elements.
- Traffic classification on subnets, subnet groups, interface groups, applications, devices, protocols, autonomous systems and ToS (Type of Service).
- Traffic profiles allowing the user to put together objects of the same type and then use the profile to classify traffic of any system object. For example, a traffic profile containing subnets from a network can be created and then associated to each subnet to produce graphs showing traffic exchanged between them.
- RFI (repeated flow interface) filters, which will filter repeated traffic exported by routers.
- Traffic capturing directly on the appliance's network interfaces to be used in environments where Netflow or other flow protocol are not available.

Minimum requirements

These requisites are for the computers that will access the system through a web browser.

Hardware

- Processor Pentium 2 400 MHZ or above.
- 128 MB RAM memory.

Browser

- Internet explorer 9+.
- Chrome 4.0+.
- Firefox 7.0+.

Chapter 2. Basic concepts

Netflow

The most scalable way to analyze IP traffic is through the use of Netflow protocol, developed by Cisco Systems.

In Netflow, the routers export UDP packets containing information about all traffic that went through them.

TRAFip is able to capture this traffic and use the information to qualify the traffic in different ways.

Each UDP packet can have up to 1500 bytes in size and carry information of up to 50 flows.

A flow is defined as a unidirectional traffic containing 7 keys: origin IP address, destination IP address, origin TCP/UDP port, destination TCP/UDP port, level 3 protocol, ToS byte and logical input interface index.

It is important to notice that to have full visibility of the traffic going through a router, it is recomended to enable Netflow in all its interfaces.

jFlow

J-Flow is a Juniper's flow monitoring implementation. This tool allows network devices to collect flow data and export the information to flow collectors.

This monitoring tool is also used as a flow recording technique. Each packet that flows inside a network is monitored and the network data flow trends are saved. After this, all this recorded information is compared, so it is possible to detect an anomaly.

IPFIX

IPFIX is a proposed standard released by Internet Engineering Task Force (IETF).

Internet Protocol Flow Information eXport (IPFIX) is a unidirectional protocol for data export and it is based on NetFlow v9's data export format.

A big benefit of IPFIX is that it allows for variables length fields and this is very useful in case you want to export URLs.

This protocol is designated to be used mainly for exporting at high flow rates and to be deployed in high speed routers.

Huawei Netstream

NetStream is a technology that provides traffic statistics and analysis developed by Huawei Technologies.

It's similar to NetFlow: once a network management system (NMS) has the NetStream software installed, it will receive the statistics about service traffic and resource usage collected by NetStream.

sFlow

sFlow is a technology developed by InMon.

Unlike NetFlow, J-Flow, IPFIX and NetStream, which are more often supported on routers, sFlow is more popular on switches.

The biggest difference between sFlow and NetFlow is that NetFlow records all packets, but sFlow collects samples.

It makes possible to discover the network data trends and it generates less traffic.

Objects definition

The objects below can be configured in order to classify traffic.

TRAFip objects

Subnet	IP network block.
Subnet group	Group of subnets.
Device	Flow exporting network elements. Usually a router
Interfaces	Logical device interfaces.
Interface group	Group of interfaces.
Application	Set of TCP/UDP ports,IP network blocks and protocols.
Protocol	TCP/IP transport layer protocol number
AS (Autonomous Systems)	AS number
AS group	Group of ASs
ToS (Type of Service)	ToS number
ToS group	Group of ToS

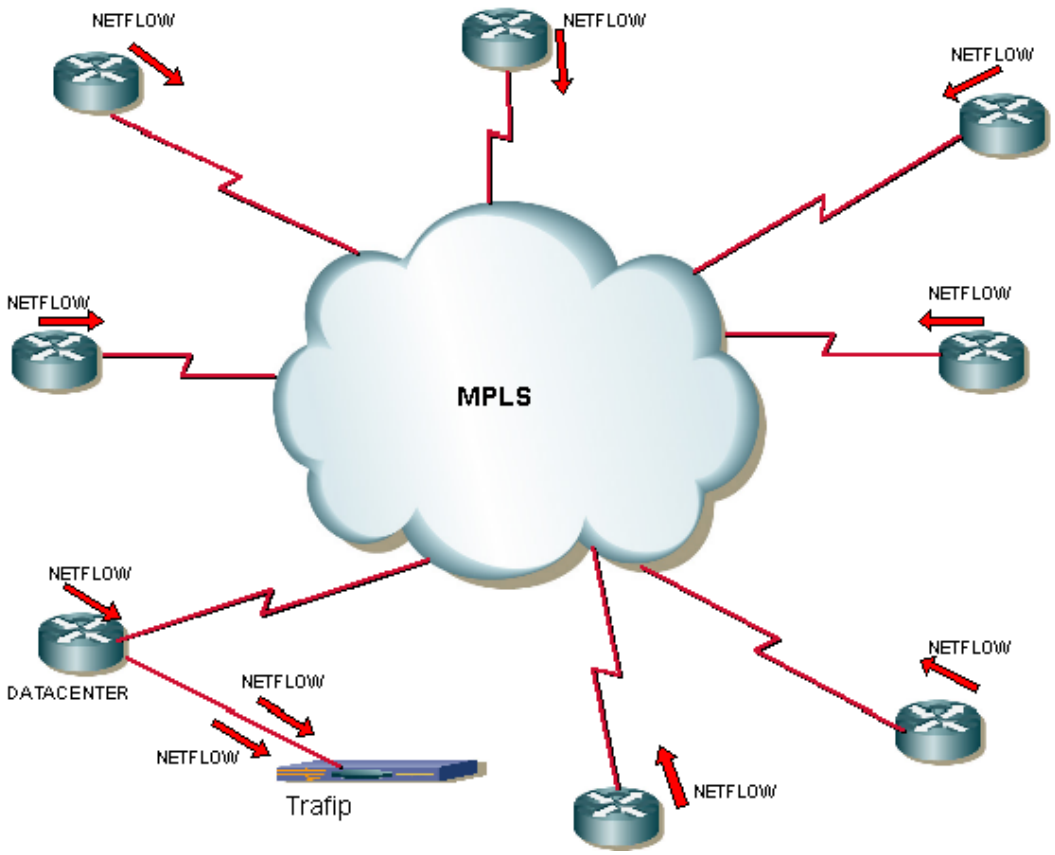
TRAFip analysis scenarios

Full mesh networks

TRAFip should be positioned as close as possible to the router that treats the higher amount of traffic, so there will not be unnecessary flow traffic going across the network.

In order to have all traffic analyzed, it is recommended that all routers exports traffic on all its interfaces.

The image below illustrates all routers from MPLS network exporting traffic to TRAFip.

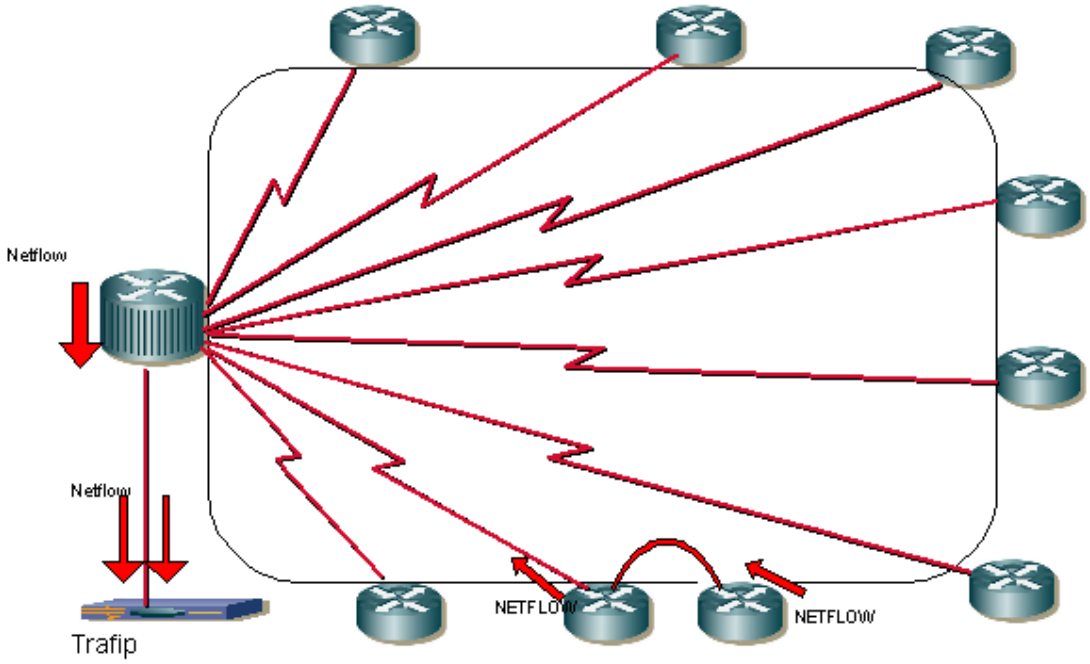


Full mesh network example

Point-multipoint networks

In this case, TRAFip should be positioned as close as possible to the central router.

Since all traffic goes through the central router, it is only necessary to enable flow export on the border routers, except when there is traffic flowing between two border routers, as illustrated below:



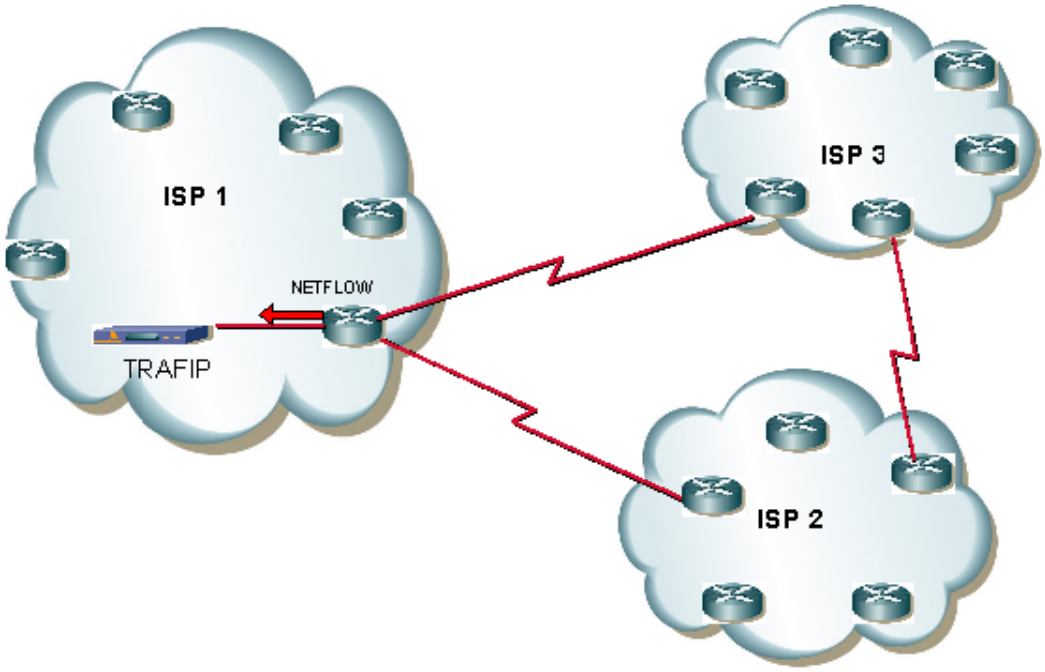
Point-multipoint network example

Internet Service Provider networks

In this environment, TRAFip should be positioned as closer as possible to the router that forwards the largest amount of traffic

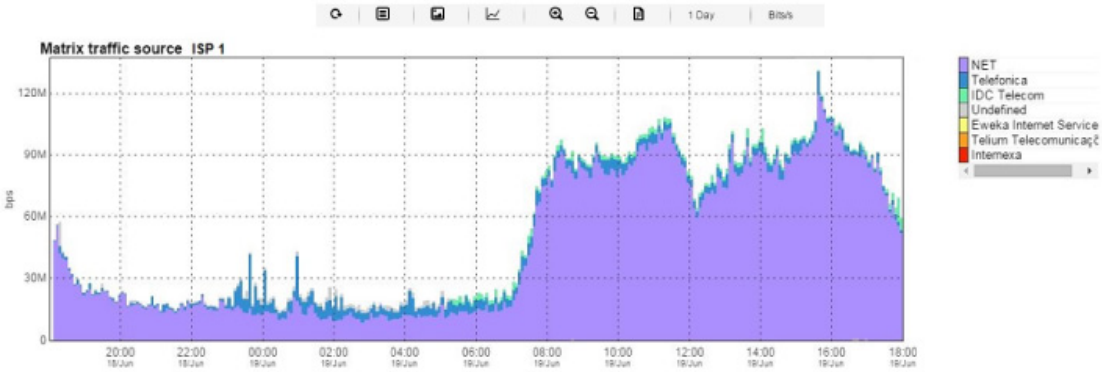
TRAFip can then be used to analyze traffic exchanged between this ISP and others with the AS (autonomous system) object. This will help the network administrators to improve traffic exchange policies.

The image below illustrates this scenario.



ISP network example

The graph below is an example of AS traffic qualification, showing how much of the traffic flowing out of ISP1 is going to each of the ISPs represented as graph curves.



Autonomous system graph example

Chapter 3. Quick startup guide

Accessing the WEB interface

Once the TRAFip server is accessed typing its IP address in a web browser, choose TRAFip system by clicking the TRAFip icon located at the up right corner of the window.

The initial access to the system can take place using the user telco_adm and password sysoper. At this point, it is recommended a password change.

If the authentication is successful, the screen below is presented to the user.

The session can be closed at any time by clicking the Logout icon at the up right corner of the window.

TRAFip main screen

The main system screen is divided in the following areas:

Area 1: tree menu. Used to navigate through system objects and configuration items.

Area 2: data display. Used to display graphs, reports and configurations forms.

Area 3: main menu. Used to select all system features.

Area 4: graph selection. Used to select object graphs and properties.

Area 5: control panel. Used to access the graph features.

Area 6: header. Used to indicate which user is logged in, logout and switch between TRAFip and SLAview system.

Interface traffic analysis

Once the routers are exporting flows to TRAFip,you will be able to configure devices in the system and perform flow analysis on its interfaces according to the following procedure.

1. Make sure that there is connectivity between all netflow exporting network elements and TRAFip's appliance on UDP port 161 (for snmp traffic), 63636 (for netflow export) and 6343 (for sFlow export).

2. Wait around 5 minutes after router configuration and access **System** → **Diagnostics** → **Flow Exporters** .

3. Click the **Edit** button next to the identified routers and fill the form:

    a. Modify **Name** and **Management IP address** fields. The second one should be an IP address where the router can receive SNMP queries.

    b. Fill **SNMP version** and **Community** according to router configuration. After, with the field (Sampling rate configuration) on Manual mode, insert the value 1 in the field **Netflow sampling rate**.

    c. In the field **Mappers**, select **Interface**, so the router interfaces will be discovered.

4. Wait 5 minutes to the system can map the router interfaces and access **Historical Data** → **Devices** → **Interface group** . Then click the New button and fill the interface group configuration form:

    a. Fill the **name** field.

    b. At the **Interfaces** field, use the * character to filter the desired interfaces.

    c. At the **Alarm Profile** select box, select **Profiles in content** tab and then select **Protocols** and **Applications**.

5. Wait around 10 minutes, then access the interface group created and click the **Applications** graph icon in the graph navigation area to check the applications classified in the interface group traffic.

6. Click the **right mouse** button in the graph area and select the **Generate Report** option. In the form presented, click the Send button to check source/destination IPs and ports that are generating the traffic.

7. At the report window, mark the checkbox **Flows to application translation** to check the applications for each line.

Chapter 4. Telcomanager grapher

The Historical Data menu will be used to visualize all of the system graphs. Below this menu, there are the monitored system objects, like devices and interfaces. When you click on an object icon, its graphs are presented in the graph selection area. When you click on an icon at this area, the Telcographer is loaded in the data display area.

The Telcographer is a highly interactive grapher written in HTML5. The functions of this application will be explained below.

Period

The grapher reads its information from the TelcoDatabase, in which all information is stored in a 5 minute period.

The 5 minute period information is available for the full period that is stored for each monitored object.

Daily graph

In this period, the information is presented with the greatest level of detail. The time period is 24 hours. There is 1 sample for each 5 minutes and 288 total samples.

Weekly graph

Each sample is the mean value of 6 5 minute samples, which corresponds to 30 minutes. The time period is 7 days with 336 samples. The maximum curve is obtained by calculating the maximum value from every 6 5 minute samples.

Monthly graph

Each sample is the mean value of 24 5 minute samples, wwhich corresponds to 2 hours. The time period is 30 days with 360 samples. The maximum curve is obtained by calculating the maximum value from every 24 5 minute samples.

Quarterly graph

Each sample is the mean value of 72 5 minute samples, which corresponds to 6 hours. The time period is 90 days with 360 samples. The maximum curve is obtained by calculating the maximum value from every 72 5 minute samples.

Yearly graph

Each sample is the mean value of 288 5 minute samples, which corresponds to one day. The time period is 364 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 288 5 minute samples.

Biennially graph

Each sample is the mean value of 576 5 minute samples, which corresponds to two days. The time period is 728 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 576 5 minute samples.

Five years graph

Each sample is the mean value of 1440 5 minute samples, which corresponds to five days. The time period is 1820 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 1440 5 minute samples.

Custom graph

You can choose a custom period for your graph. To do it, select the **Custom** period and enter the initial date and time and the final date and time.

Features

The Telcographer has many features that are available at control panel. Some of them can also be accessed by clicking the right mouse button at any point on the graph.

Statistics box

The mouse over action on the curve label will display a statistics box with the following information: maximum, minimum, mean, total value and standard deviation for the curve.

Show value

This feature will cause the mouse pointer to display the x and y axis value for the pointer position.

Vertical zoom

To use this resource, follow the steps below:

1. Select this option on the Options menu at control panel.
2. Press and hold the mouse button on the initial y axis position.
3. While holding the button, move the mouse cursor to the final y axis position and release the mouse button.

Single curve

Select this option on the Options menu at control panel and then click on one of the curves label. This action will cause the graph to show only the selected curve.

Relative mode

Click this option on the popup menu to display each curve sample in the graph relatively to the other curves, which means that for each sample, the sum of the data represents 100%.

This mode only works if all the graph curves are in stack mode.

Axis configuration

Select this option on the Options menu at control panel to open a window where you will be able to select the curves that will be displayed using the left or right x axis scales.

Add to graphset

Click the right mouse button on the graph and after select this option to open a box where you will be able to associate the graph to a previously created graphset.

Graph type

With the **Graph type** menu at control panel, you can choose the display type of the graph: line, pie or bar.

Save image

Click this option on the graph popup menu option to save the graph as a jpeg image.

Aggregated chart

Select this option on the graph popup menu to open aggregated charts representation of the graph. There are 2 options of charts: pie and bar. Those charts can be filtered by a period of the day. For example, if you open a pie chart from a weekly graph and filter from 10:00h to 17:00h, the pie chart will represent the weekly data only for that period of the day.

Even if you don't enable the filter, you can configure the graph period using the field **Period**. When this field is filled with **1 day**, another field is displayed: **Last hours**. For instance, when this field is filled with 1, it means the graph values are related to the last hour. The maximum value that can be configured in this field is **24**, which represents the last 24 hours.

Tip

You can remove a curve from the graph just by clicking on it in the label.

Zoom in and zoom out

Click this option on the graph popup menu to zoom in and out on the time scale. For example, using it on an annual graph, it is possible zoom in the daily graph for one particular day.

Important

These options are only available at line graphs.

Export

Access this option by clicking the right mouse button on the graph. The graph data can be exported in HTML, CSV or TSV formats.

Auto refresh

Select this option to cause the graph to refresh automatically every 5 minutes. This feature have to be previously enabled at **System** → **Parameters** → **Grapher** , where you can also set the refresh interval.

Report

From any graph, it is possible to generate a report that will fetch the flows that were used to build the graph.

Right click at any point within the graph area and move the mouse into **Raw data report** option. After this, you can generate a **custom** report or select a pre-configured one.

Available pre-configured reports:

- Top source IPs
- Top destination IPs
- Top source AS
- Top destination AS
- Top conversations
- Unmatched traffic

Tip

The graphs in **Packets/s** (pps) and **Bit/s** (bps) have a curve for no sample applied. So, to check this curve's information, pass the mouse over the label named "**No sample total**".

Keys

Some keys on your keyboard have special functionalities. Check them below and their descriptions.

Table 4.1. Keys

Key	Description
D	Transforms the graph into derivative mode.
I	Indicates detailed information about the graph such as resolution, curves, samples and timestamps.
L	Lists the timestamp and the value of each point from a curve.
N	Changes graph curves format, once all of them are in stack mode.
P	Provides a projection curve considering only the points between the signalized lines. When you move down the mouse, the number of points decrease, otherwise the number of points increase.
R	Adjusts the graph to get the max resolution.
S	Save the graph as a PNG image.
W	Changes the curve configuration to waas accell.
-	Zoom out.
+	Zoom in.
LEFT	Moves the graph to left.
RIGHT	Moves the graph to right.
*	Graph returns to its normal size.

Tip

You can convert the timestamp to date using the **ts2date** command at CLI.

Chapter 5. Historical data

This chapter describes the elements on the historical data tab.

Under this tab, you can access all the processed data for the monitored objects.

The data can be accessed through graphs and reports.

Network Overview

This tab provides an absolute traffic overview in the last hour.

The data can be visualized in a list, in a pie chart or a bar chart.

You can configure which type of objects will be shown on this overview as well as the display mode of each one.

Important

If you drag the Top 10 and modify the display order and/or remove one of them by clicking on "**X**", the system will save your alterations.

The available type of objects are:

- Application
- Application groups
- Autonomous system
- Autonomous systems group
- Device
- Interfaces group
- Mapped object
- Protocol
- Subnet
- Subnets group
- ToS
- ToS group

Tip

Click on any object to open its graph in a new tab.

To open this tab in a new window, use the icon  .

To configure the exhibited objects and their display modes, click on . Thereafter, select and drag the elements to configure the display order. Check below the meaning of each icon.

Table 5.1. Icons list

Icon	Description
	Lists the objects top 10.
	Shows the objects top 10 in pie charts.
	Shows the objects top 10 in bar charts.

Favorites

Using this feature, each user can configure its objects of interest for fast access.

Adding objects to the Favorites

To add objects to your Favorites, simply click the gold star icon shown as the first element of the graph selection area for the desired object.

Removing objects from the Favorites

To remove objects from your Favorites, simply click the gold star icon shown as the first element of the graph selection area for the desired object.

Totals

This tab contains only three graphs, which represent the traffic for a domain.

Subnets

The subnets object allows the analysis of IP block ranges. It is also possible to use the subnet group object to create a set of subnets to be analyzed.

Definitions

- Subnet destination traffic: composed by the sum of all flows in which the destination IP address belongs to the IP block range of the subnet.
- Subnet source traffic: composed by the sum of all flows in which the source IP address belongs to the IP block range of the subnet.

Configuration

To manage the system subnets, access **Historical data** → **Subnets**.

Click the **Subnets** tree menu item to have the list of subnets configured.

To add a new subnet, click on **New** button and fill the form.

Table 5.2. New subnet form

Field	Description
Name	Subnet name.
Description	Subnet description.
IP address blocks	Subnets can have more than one address range. Ex: 10.0.0.0/24, 10.0.1.0/24, 2001:db8:abcd:2000::/64, 2001:cdba:9abc:5678::/64.
Traffic reference line (bps)	This value will be plotted in the object graph as a dotted red line.
Origin activity factor threshold	Limit of origin **Activity factor**.
Destination activity factor threshold	Limit of destination **Activity factor**.
Enable trend analysis	Use trend analysis default parameters or set them. Refer on to trend analysis section for hints on how to configure these parameters.
Threat profile	Select a threat profile for this subnet to be used in threat analysis or leave blank.
Subnet groups	Subnet group association.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the traffic profiles and way they should be applied in this subnet.
Alarm profile	Alarm profile association.

Import subnets file

To import a file of subnets, access **Historical data** → **Subnets**.

Click the **Subnets** tree menu item.

Click the Import button and load the file.

A import subnets file has the following fields:

Table 5.3. Fields from subnet file

Field	Description
Name	Possible characters for name field.
Description	General characters (optional).
IP address blocks	Subnets can have more than one address range. Input format: IP1/Mask1,IP2/Mask2. (IP/32 in the case of using a single IP). Ex: 10.0.0.1/32,10.0.1.0/24
Traffic reference line (bps)	Integer value greater than or equals to 0.
Enable threat analysis	Fill with **yes** or **no**.

Subnet groups

Subnet groups can be used to organize your subnets.

Definitions

- The traffic from the group is the sum of all the individual IP BLOCKs from the subnets contained in the group. This means that duplicated IP BLOCKS will be summed only once in the group traffic.
- When a subnet group is created, it must be associated to a higher group level, which is only organizational.
- TRAFip has by default three such groups and the user can modify their names and create more at **Historical Data** → **Subnets** → **Aggregation list** .

Configuration

To manage the subnet groups, access **Historical data** → **Subnets**.

Click the **Subnet groups** tree menu item to have the list of subnets configured.

To add a new subnet, fill the form below accordingly:

Table 5.4. New subnet group form

Field	Description
Name	Subnet group name
Description	Subnet description.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
Traffic reference line (bps)	This value will be plotted in the object graph as a dotted red line.
Aggregation	Higher organizational group level.
Subnets	Subnet belonging to this group.
Alarm profile	Alarm profile association.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the traffic profiles and way they should be applied in this subnet.

Aggregation

This object is only a organizational level where that you can use to organize the TRAFip subnet groups.

Each subnet group can be place in only one aggregation.

To manage the aggregation, access **Historical Data** → **Subnets** → **Aggregation list** menu.

To add a new aggregation, fill the form below accordingly:

Table 5.5. New aggregation form

Field	Description
Name	Aggregation name
Aggregation Groups	Subnet groups association

Devices

To map logical and physical device's objects like interfaces, the system has a mapper process that periodically runs and performs the mappings (See Mappers configuration section). There is a pre-configured mapper to map device's interfaces that uses the ifDescr OID to perform this task.

Procedure 5.1. Device configuration steps

1. Select **Historical data** → **Devices** → **Device** .
2. Click the **New** button and fill the form below.

Table 5.6. New device form

Field	Description
Name	Device name.
Description	Device description.
Management IP address	Device IP address. This IP address should respond SNMP read queries for SNMP monitoring and ICMP echo requests for ICMP monitoring.
Type	Type of device, the user can use this field to freely categorize all devices configured.
Manufacturer	Name of the device manufacturer.
Latitude	Geographic coordinate, in decimal degrees (DD), used to locate the device on georeferenced maps. Example: -22.9035.
Longitude	Geographic coordinate, in decimal degrees (DD), used to locate the device on georeferenced maps. Example: -43.2096.
SNMP credential	Choose a SNMP credential.
SNMP Version	Choose the SNMP version. Possible values are: SNMP v1 or SNMP v2c — Specify an SNMP community SNMP v3 — Specify the authentication type and its parameters
SNMP community	Enter the SNMP community.

Field	Description
Use Default SNMP configuration	This option lets you define specific values to be used specifically for this device. The default values are specified at SNMP collector parameters configuration.
Use sysUpTime OID to discard results	Discard the collection if the device is not allowed for more than 5 minutes. Prevents miscalculations.
SNMP Timeout	Time limit in seconds to wait for a SNMP reply packet. Value range: 1-10.
SNMP Retries	Number of retries that will be issued to the device if it does not respond to a SNMP query. Value range: 1-10.
Number of OIDs per packet	Number of OIDs that will be sent in each SNMP packet. Value range: 1-100.
Maximum packet rate (pps)	Maximum number of packets per second that a SNMP collector will send for each device.
SNMP window	Number of SNMP packets that will be sent without answer from the device being polled.
SNMP port	The SNMP port.
Agents	This option lets you define one or multiple SNMP agents in the same IP address and different ports. Now you can specify OID masks and SNMP port for this mask. This means that the SNMP collector will use the specified UDP port if the OID to be collected on this device matches the specified mask. Example: • OID prefix .1.3.4.6.9.9.1.2.* SNMP port: 163 • OID prefix .1.3.4.6.9.9.1.3.* SNMP port: 164
Connection credential	Choose a Connection credential.
Connection protocol	Choose **SSH** or **Telnet**.
SSH port	When the **Connection protocol** is SSH, enter the SSH port. The default value is **22**.
Telnet port	When the **Connection protocol** is Telnet, enter the Telnet port. The default value is **23**.
User	User to be used to access the device. This string is available as a wildcard %username% for provisioning scripts.
User password	Password to be used to access the device. This string is available as a wildcard %passwd% for provisioning scripts.

Field	Description
Enable secret	Enable password to be used to access the device. This string is available as a wildcard %enable_passwd% for provisioning scripts.
Enable TRAFip collect	Enables the collection by TRAFip.
Netflow exporter ip address	Fill the IP address that the netflow exporter will use to send flows. Next to this field, there is a magnifying glass icon. Click to fill automatically based on Management IP address.
Sampling rate configuration	Can be set manually or based on flow.
Netflow sampling rate	If you are exporting sampled flows, choose whether to consider a manual configured rate or to detect the rate from the flow records.
Enable SLAview collect	Enables the collection by SLAview.
Automatic profile	Select this option to enable the use of this device and its mapped objects on automatic profiles. The association will only occur if the device or its objects match the profile rules. (See Profile configuration section) .
Enable configuration management	Enables the configuration management by CFGtool.
Configuration export mode	Select **Active** to export the device configuration according to the interval configured at **System → Parameters → Configuration management** . To export configuration using trap filter, select **Passive**.
Topology mapping method	Select the protocol to be used for topology mapping. Available options are CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol or both. Using either method, SLAview uses the SNMP protocol to fetch information from these protocols on the monitored devices MIB tables.
Enable provisioning	Enable provisioning to configure automatically Cisco IP SLA probes, Telcomanager probes and Netflow exportation.
Collector	Device association to a remote collector. This field is available only when the distributed architecture is enabled.
Authentication script	When the Connection protocol is **Telnet**, you have to select a Login script.
Provisioning script	Fill this option for Netflow provisioning in distributed architecture systems and probes configuration. This script will be used to reconfigure Netflow export to a backup collector if a collector fails.
Polling templates	Choose an ICMP polling template for the device.

Field	Description
	The polling template lets you configure the specific times to poll the devices and measure their availability.
Device type	Field used to pick an icon to represent the device graphically on Maps. You can choose between: Camera, Firewall, Router, Server, Switch or Wireless. The default device type is **Router**.
Configuration exporter script	Select running and startup configuration exporter scripts.
Domain	Device domain association.
Groups	Click the **List** button and select the desired groups to place this device in one or more points in the group hierarchy.
Mappers	Select the desired mappers to map objects like interfaces and cpus on this device.(See Mappers configuration section)
Alarm profiles	Associate the device with an alarm profile.

Create Device using Wizard

There is a wizard for device creation that will guide you and validate each step at a time.

1. Select **Historical Data** → **Devices** → **Wizard** .
2. Fill the fields according to the table above.
3. During the creation, you are able to test the equipment connectivity, map the device's object and test mapped objects association to profiles, for instance.
4. After this, you can view and save your new device.

Verifying mapped objects for the device

Click the Mapped objects icon in the tree menu area to see all the mapped objects of the system. Acessing the form of each one, you can enable the trend analysis and enter a description.

It is also possible to check the configuration history and delete the object using the **History** and **Delete** buttons.

There is a filter at the top of the page with options to select located and not located objects. Not located itens are mapped objects that are not being located by one of the device's mappers. Ex: an interface module that was removed from a router will cause its interfaces to go to not located state.

At the tree menu area, below each device, the system shows its mapped objects. The icons color indicates the following conditions:

Green icon	The object has a profile associated to it.
Uncolored icon	The object does not have a profile associated to it.

Red blinking icon The object was not located by the object mapper process.

Import devices file

To import a file of devices, access **Historical data** → **Devices**.

Click the **Devices** tree menu item.

Click the **Import** button and load the file.

A import devices file has the following fields:

Table 5.7. Fields from device file

Field	Description
Name	Possible characters for name field.
Description	Possible characters for description field (optional).
Management IP address	IP Address. Ex.: 10.0.0.1
SNMP Version	Type **1** for SNMP version 1, **2c** for version 2 and **3** for version 3.
SNMP community	Possible characters for snmp community.
Connection protocol	Type **SSH** or **TELNET**.
User	Possible characters for name field (optional).
User Password	Possible characters for password field (optional).
Enable Secret	Possible characters for password field (optional).
Enable TRAFip collect	YES to enable and NO to disable the TRAFip collect.
Netflow exporter ip address	IP Adress list separated by comma. Ex.: 10.0.0.1,10.0.0.2
Sampling rate configuration	Enter 0 for manual and 1 for flow.
Netflow sampling rate	Integer value greater than 0.
Enable SLAView collect	YES to enable and NO to disable the SLAview collect.
Automatic profile	Select **YES** to enable the use of this device and its mapped objects on automatic profiles.
Device Type	Field used to pick an icon to represent the device graphically on Maps. Choice camera, firewall, router, server, switch or wireless.

Important

If the device icon is red, it means all its exports IP's are down.

Interface group

Interface groups allow the detailed analysis of a single interface or a group of interfaces, because profiles can be applied to them and one interface can be associated to more than one interface group.

To create a new interface group, access the **Historical data** → **Devices** → **Interface group** menu and click the **New** button.

Table 5.8. Interface group form

Field	Description
Name	Interface group name.
Description	Interface group brief description.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
Interface group aggregation	Higher interface group level, only organizational. Access **Configuration** → **Objects** → **Interface group aggregation** to configure new groups.
Domain	Domain to which this interface group belongs.
Interfaces	Select the interfaces that belong to this group.
Alarm profile	Alarm profile association.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the profiles and how they should be applied in this interface group.

Unmatched traffic

All traffic that does not have an input interface or an output interface. This may occur for several reasons: packet loss, traffic destined or originated to the device itself, routing problems, etc.

Applications

The application object are represented by a match rule that combines IP addresses, ports and a Layer 4 OSI protocol.

Access **Historical data** → **Applications** → **Application** to manage currently configured applications and add new ones.

Table 5.9. Application form

Field	Description
Name	Application name.
Description	Application brief description.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Application ID match	Enable this field to identify the application by the application ID.
Source subnets	Subnets to match against the source IP address flow field. Ex: 10.0.0.0/24,10.1.0.0/16,192.168.1.1/32.

Field	Description
Operation	Operation to perform between the source and destination fields. Ex: 80,443-446,455
Source ports	Ports to match against the source port flow field.
Destination subnets	Subnets to match against the destination IP address flow field.
Destination ports	Ports to match against the destination port flow field.
Classification engine ID	A specific registry for application assignments.
Selector ID	A specific registry for application assignments.
Application group	Application group association.
Protocols	Select the Layer 4 OSI protocols to be used in this application.
Traffic profile	Check the Traffic profile section.

Classification

The applications will be classified according to the priority list at **Historical data** → **Applications** → **Application** .

Each flow will match for only one application.

To change the classification priority, select one or more application and click the UP or DOWN arrows that appear on the left above the application list.

Import applications file

To import a file of applications, access **Historical data** → **Applications**.

Click the **Applications** tree menu item.

Click the **Import** button and load the file.

A import applications file has the following fields:

Table 5.10. Fields from application file

Field	Description
Name	Possible characters for name field.
Description	General characters (optional).
Traffic reference line (bps)	Integer value greater than or equals to 0.
Source subnet(s)	Subnet list. Input format: IP1/Mask1,IP2/Mask2. (IP/32 in the case of using a single IP). Ex: 10.0.0.0/24,10.0.1.0/24. You can use * for all source subnets.
Source ports	Integer list between 1 and 65535, separated by comma. You can use * for all source ports.

Field	Description
Operation	Enter 1 for OR operation, 2 for AND operation.
Destination subnet(s)	Subnet list. Input format: IP1/Mask1,IP2/Mask2. (IP/32 in the case of using a single IP). Ex: 10.0.0.0/24,10.0.1.0/24. You can use * for all destination subnets.
Destination port	Integer list between 1 and 65535, separated by comma. You can use * for all destination ports.
Protocols	Layer 4 OSI protocols, separated by comma. Ex: UDP,TCP (opcional).

Application groups

Application groups will be useful to organize your applications. Using this object type, you can have a consolidated view of a group of Applications.

To configure a new application group, access **Historical data** → **Applications** → **Application group** .

Table 5.11. Application group form

Field	Description
Name	Define a name.
Description	Describe the application group.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Application	Select the applications to be associated to this application group.
Traffic profile	Check the Traffic profile section.

Protocols

This object refers to the transport layer of the TCP/IP model. The object is basically represented by a number indicating the protocol for each flow. Example: 17 for UDP traffic and 6 for TCP traffic.

Access **Historical data** → **Protocols** → **Protocol** to manage currently configured protocols and add new ones.

Table 5.12. Protocol form

Field	Description
Name	Protocol name.
Description	Protocol description.
Number	Protocol number.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Traffic profile	Check the Traffic profile section.

Import protocols file

To import a file of protocols, access **Historical data** → **Protocols**.

Click the **Protocols** tree menu item.

Click the **Import** button and load the file.

A import protocols file has the following fields:

Table 5.13. Fields from protocol file

Field	Description
Name	Possible characters for name field.
Number	Integer value between 0 to 255.
Description	General characters (optional).
Traffic reference line (bps)	Integer value greater than or equals to 0.

Autonomous Systems

As defined in RFC 1930, an autonomous system is a collection of connected IP routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the internet.

This object matches the origin AS flow field to form its source traffic and the destination AS flow field to form its destination traffic.

> **Tip**
> Some routers can populate the AS flow fields with the final destination/source AS or with the peer AS information. In Cisco routers, you should configure the command **ip flow-export version {1|5|9 [origin-AS|peer-AS/}**.

To configure a new AS, access **Historical data** → **Autonomous system** → **Autonomous system** .

Table 5.14. AS form

Field	Description
Name	AS name.
Description	AS description.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
Number	AS number. To enter a numbers list, separate them by comma.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
AS group	AS group association.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the profiles and how they should be applied in this AS.

Import autonomous system file

To import a file of devices, access **Historical data** → **Autonomous systems**.

Click the **Autonomous system** tree menu item.

Click the **Import** button and load the file.

A import autonomous system file has the following fields:

Table 5.15. Fields from autonomous system file

Field	Description
Name	Possible characters for name field.
Number	Integer list between 1 and 65535, separated by comma.
Description	General characters (optional).
Traffic reference line (bps)	Integer value greater than or equals to 0.

Autonomous system group

You can use the AS groups to have a consolidated view of a group of Autonomous Systems. For example, the ASs from each continent.

To configure a new AS group, access **Historical data** → **Autonomous system** → **Autonomous system group** .

Table 5.16. AS group form

Field	Description
Name	AS name.
Description	AS description.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Autonomous system	Autonomous systems that should be placed in this group.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the profiles and how they should be applied in this AS group.

Type of service

The type of service object represents the ToS field of the IP protocol header. This field is exported for each flow and it does not have source nor destination.

This field is usually used to mark packets at the network edge, so they can be treated by the appropriate QoS policies by the core network routers.

Important

Be aware that Cisco netflow will not export the ToS field with the correct value for traffic going out of the border routers to core routers if the packets are being marked at the WAN interface. So only packets coming from the core routers will have the correct values exported in the ToS field, because they are already marked when they reach the edge router. To have the flow packets from the edge routers correctly marked, you should mark the packets at the LAN interface.

To manage the ToS objects, access **Historical data** → **ToS** → **ToS** .

Table 5.17. ToS form

Field	Description
Name	ToS name.
Description	ToS description.
Number	ToS number.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
ToS group	ToS group association.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the profiles and how they should be applied in this ToS.

Import ToS file

To import a file of ToS, access **Historical data** → **ToS**.

Click the **ToS** tree menu item.

Click the Import button and load the file.

A import ToS file has the following fields:

Table 5.18. Fields from ToS file

Field	Description
Name	Possible characters for name field.
Number	Integer list between 1 and 65535, separated by comma.
Description	General characters (optional).
Traffic reference line (bps)	Integer value greater than or equals to 0.

ToS group

You can use the ToS groups to have a consolidated view of a group of ToSs. For example, the ToSs used to mark video traffic.

To configure a new ToS group, access **Historical data** → **ToS** → **ToS group** .

Table 5.19. ToS group form

Field	Description
Name	ToS group name.
Description	ToS group description.
Enable trend analysis	Trend analysis default parameters. Refer on to trend analysis section for hints on how to configure these parameters.
Traffic reference line (bps)	This value will be plotted in the traffic graph as a dotted red line.
ToS	ToS objects that should be placed in this group.
Traffic profile	Check the Traffic profile section.
Profile selection box	Select the profiles and how they should be applied in this ToS group.

Reports

Templates

For almost all reports available on the system, you have the option to save them as templates once you fill the report fields.

Saving

1. Open the desired report and select the Save template option.
2. Fill the fields below:

Table 5.20. Template Form

Fields	Values
Name	Report name.
Write permission	Select who can alter this report. The group option is based on user groups.
Read permission	Select who can read this report. The group option is based on user groups.
Send report by email	Send the report by email.
Attachment format	Choose the desired format: PDF or CSV.

3. Fill the other report fields and click the **Send** button.

After executing the steps above, the saved report is available at the **Template list** for each report type.

Scheduling

1. Open the Template list for the report or create a new report.

2. Select the Schedule template option.
3. Select the apropriate schedule option.

Schedule options

- One execution: the data start and end times will be the start time and end times of the report.
- Daily: the data start and end times will be from 00:00 h to 23:59 h of the previous day
- Weekly: the data start and end times will be from Sunday 00:00 h to Saturday 23:59 h of the previous week.
- Monthly: the data start and end times will be from day 01 00:00 h to the last day at 23:59 h of the previous month.

Tip

In order to schedule a report, you must save it as a template.

Tip

When a report is ready, it is sent an e-mail to users. The SMTP server should be configured and also each user email at the user configuration form.

Editing

After the template is saved, an **Edit** button appears at the template list and can be used to change the report parameters.

Visualizing reports

After the system runs a template, a new report instance is generated.

All report instances can be accessed through the Details button available for each template.

To visualise a report instance, follow the procedure below:

1. Click the **Details** button for the desired template.
2. Choose the desired output format between HTML, CSV and PDF.
3. Click the **Show** button for the desired report instance.

Managing disk space

The total space available and currently used by the template reports is listed below the template list.

The system has a reserved storage area that is shared for all reports.

You can increase or decrease this space by going to **System** → **Parameters** → **Data storage** .

You can delete generated reports by clicking the Details button at template list for the desired template.

Suspect traffic

The suspect traffic report provides more detailed information about the statistics shown at **System** → **Diagnostics** → **Suspect traffic statistics** .

To generate a new report, access **Historical data → Reports → Suspect traffic** .

The form will be already filled, but you can edit it. Then, click the **Send** button.

Table 5.21. Suspect traffic report

Field	Description
Start time	Enter the initial period time.
End time	Enter the final period time.
Filter by subnet	Select **None** to do not filter by subnet or select the desired one.
Number of lines	Choose a limit to the report output.
Attack type	You can choose **High data flow between two IP address** or **IP Flood**.
Format	You can choose **Rate** or **Total**.

Tip

You can generate **Raw data report** to have detailed and consolidated statistics for each flow and, to do it, click on icon shown next to IP address.

Top N

Definitions

Top N reports provides consolidated statistics for all object types.

The report output wil display statistics from all objects of the selected type, including the percentage of limit.

Launch a new report

1. Access **Historical data → Reports → Top N** .
2. Choose the desired object type or a template from the template list.
3. Fill the form:

Table 5.22. Top N report

Field	Description
Generate report | Save template	Choose **Generate report** for a one time report or **Save template** to save the report as a template
Object type	Automatically filled with selected object type
Filter by name	You have to use Regular Expressions to filter.
IfAlias filter	Filter by the ifAlias SNMP OID in case of interface reports.
* Manufacturer	Filter by objects manufacture. You have to use Regular Expressions to filter.
* Manufacturer Type	Filter by objects manufacturer type. You have to use Regular Expressions to filter.

Field	Description
Start time	Start time for data selection.
End time	End time for data selection.
Exclude weekends	Exclude weekend periods from the report data.
Interval	If all day option is marked, this field is ignored, otherwise the data is selected within that range for each day.
Way	Choose a way to filter traffic. When you select **Both**, you can **Group objects**, it means that the report will show the Source and Destination of each object in two consecutive rows.
Sort by	Option available only when the **Way** is filled with **Both**. Choose if the report will be sorted by source, destination, usage percentage of limit or maximum usage percentage of limit.
Unit	Choose the unit to display the traffic.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Percentile	Use percentile to compute report results.

* Only available for Device, Interfaces and Interfaces SNMP reports.

Tip

If you select packets or flows under the unit field, you will be able to detect some suspicious activities, like a subnet with a number of packets or flows that is not compatible with its traffic.

Traffic profile

Definitions

This report is based on the summarized data.

To have data on this report, you need to configure objects and associate those objects to traffic profiles, which should contain other objects.

This way, you will be able to obtain traffic matrix of, for example, subnets against subnets, subnets against applications, interfaces against subnets and so on.

Launch a new report

1. Access **Historical data** → **Reports** → **Traffic profile** → **New report** .
2. Fill the form:

Table 5.23. Traffic profile report

Field	Description
Generate report | Save template	Choose report for a one time report or Save template to save the report as a template

Field	Description
Domain	Choose the domain.
Profile association type	Choose the profile association type. For example, for application profiles choose content.
Profile object type	Choose the profile type.
Object type filter	Filter for the profile objects. The profile objects will be placed in the report columns.
Object type	Choose the type of the objects.
Object filter	Filter for the report objects. Those objects will be place in the report lines. You have to use Regular Expressions to filter.
Unit	Choose the unit for the report data.
Way	Choose the traffic way.
Start time	Choose the report start time to select the data.
End time	Choose the report end time to select the data.
Exclude weekends	Exclude weekend periods from the report data.
Interval	If all day option is marked, this field is ignored, otherwise the data is selected within that range for each day.
Percentage of limit	Choose this option to have the report data as a percentage of the traffic limit configured in each object. This option will only work when the select unit is bytes, since the traffic limit is also in bytes.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Rate average in Mbps	Show the rate average in Mbps.
Use SI prefix	Use the SI prefix to show 40.469722M instead of 40469722, for example.

Syslog

Definitions

You can configure any device to send syslog messages to TRAFip.

The messages are received at UDP port 514.

The syslog messages will be stored and deleted based on the syslog storage configuration.

Launch a new report

1. Access **Historical data** → **Reports** → **Syslog** → **New report** .
2. Fill the form:

Table 5.24. Syslog report

Field	Description
Begin	Choose the report start time to select the data.
End	Choose the report end time to select the data.
Source	Select the source IP or host for the syslog messages. Leave blank to have all hosts.
Priority	Select the message priority. Leave the 0 to have all priorities.
Message	Filter the syslog message. Leave blank to have all messages.
Level	Select the syslog message level. The default is all messages.
Number of lines	Choose a limit to the report output.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.

3. Click the Send button.

Rawdata

Definitions

Rawdata reports provides detailed and consolidated statistics for all flows collected by TRAFip.

The more fields you select, the bigger and more detailed the report output will be.

Launch a new report

1. Access **Historical data** → **Reports** → **Raw data** .
2. Choose the **Schedule new report** option or a template from the **Scheduled reports** option.
3. Fill the form:

Table 5.25. Raw data report

Field	Description
Generate report | Save template	Choose **Generate report** for a one time report or **Save template** to save the report as a template
Output format	Option available only for non-template reports. Choose the desired output format.
Number of lines	Option available only for non-template reports. You can change the maximum number of lines at **System** → **Parameters** → **Scheduled reports** in the **Max lines per report** option.

Field	Description
Show interfaces IP	Mark this option to have the interface IP displayed in the report when the interface field is selected.
From	Choose the initial time to select the raw data. The summarization proccess runs every five minutes. So, the minute has to be a multiple of 5.
Object type	Object type to be used in this report.
Object	Select the object for this report. The available objects will depend on the object type selected.
Interval	Select the interval for the report. Ex: If you select 10 min, the report data will be selected from the **From** field plus 10 minutes.
Direction	Select the direction traffic should be filtered.
Sort by	Select the unit to sort the report data.
Exclude objects from profile	This option will filter out the objects on the selected profile. This is very usefull to find out undefined traffic.
Sampling rate treatment	Choose if the number of packets and bytes from the flows should be multiplied by the Sampling Rate configured for the device. If you choose the configuration option, you should set the Sampling rate configuration field located in the device configuration form.
Time based flow consolidation	Mark yes and the entries in the report with the same keys will be summarized in time. In this case the initial time is the initial time of the first flow, the final time is the final time of the last flow and the duration is the diference between those values.
Format duration	Mark this option to have the flow duration formated in hours, minutes and seconds.
Netflow fields	Choose the netflow fields for this report. They can be edited too on the generated report and it will be reloaded.
Flows listing	Mark this option to have all flows listed.
Filters	The filters will be automatically filled depending on the graph options. For example, if you select only a curve label, the filters will reflect that. You can also add more filters to the report.

4. On the generated report, you will can translate: IP address to group, IP address to subnet, IP address to hostname, IP address to netbios, AS numbers, flows to application, flows to ToS and flows to ToS group. Furthermore, it's possible to visualize the objects Top 10 in a pie chart (for this purpose, click on icon ).

5. By clicking on source IP or destination IP, it will be displayed an animation showing the flow-to-flow in the selected IP in a period of 5 minutes.

Tip

The rawdata database is indexed by the exporters ip addresses, so if you know the device or interface that exported the traffic you want to check out, you should issue the rawdata report on the specific device or interface. This way the report will be faster and demand less system resources.

Trend Analysis

Once this feature is enabled, the system is able to predict the behavior for any graph curve and inform a violation date for a given threshold or given the date, inform curve value.

Configuration

Access **System** → **Parameters** → **Trend analysis**

Table 5.26. Trend analysis configuration form

Field	Description
Degree of freedom	The polynomial order to be used. Currently only first degree polynomials are supported.
Sampling	Configure the sampling for day, week or month granularity for the trend analysis process.
History	Configure the number of samples that will be analyzed. Ex: If you choose the value **6** for history and **week** for sampling, the system will analyse 6 weeks back to predict the trend.
Interval	If **All day** option is marked, this field is ignored, otherwise the analysis will consider only the configured range for each day.

Enabling projection for a graph curve

1. Access **Configuration** → **Traffic Profiles**.
2. Click the Edit button for the desired profile or create a new one.
3. Click **Yes** at the **Enable trend analysis** select box and choose **Standard configuration** or customize configurations for that curve.

Important

The Trend Analysis reports will be available one day after enabling the feature, since the trend analysis process runs on a daily basis.

Graphical reports

1. Access the graph that contains a curve configured for projection, right click on it and select the **Projection violation** option.
2. Select the desired curve in the popup box, insert a value for it and click OK to have the growth rate and violation date.

Launch a new report

1. Access **Historical data** → **Reports** → **Trend analysis** → **New report** .

2. Fill the form:

Table 5.27. Trend analysis report form

Field	Description
Projection type	Choose Profile object or Object.
Profile	Select the object profile.
Profile object	Select the profile object.
Object type	Select the object type.
Object filter	Filter by objects associated to the profile.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Limit violation | Estimate	By choosing **Violation limit**, provide a value and TRAFip will return a violation date. If you choose **Estimate**, provide a date and TRAFip will return the curve value at that date.
Data input	It is possible to apply an operation (**Addition** or **Subtraction**) to perform on curve value to calculate the trend. You can also choose the data input type (**Absolute** or **Relative [%]**). Just to select the desired options and enter the value, in bits/s.

3. After filling the form, click on the **Send** button to launch the report, which will display the objects, the direction, the estimated date or the estimated value, the object's traffic reference line (in bps) and how much of this limit was used.

Graph set

The graphset is a graphical report where you can visualize multiple graphs in a grid at the data display area.

Definitions

Operator and **Configurator** users are only able to manage their own graphsets.

Administrator users are able to visualize, edit and delete all graph sets, but cannot create a graph set for a specific user.

Creation

Access the path **Historical data** → **Graph set** → **New graph set** .

Table 5.28. Graph set creation

Field	Description
Name	Graph set name.
Description	Description about the graph set.

Field	Description
Time between slides	Time in seconds to switch slides used in NOC display.
Display in NOC	Select **Yes** and the graph set will be available in NOC display.
Save at	Path to save an image of the graph set. Example: C:\Users\Telco\Images
Dimensions	Dimensions of saved image.

Adding graphs

1. Access any graph;
2. Click the right mouse button on the graph;
3. Access the option **Add to graph set** on the popup menu and select the desired graph set.

There is another way to add graphs to the graph set. It makes possible to add pie and/or bar charts. Check the procedure below:

1. Access the graph set;
2. Click on + symbol;
3. Fill the fields (object type, objects, graphs, graph type and period);
4. Click on **Insert graph**.

Tip

To desassociate a graph, just click on **X** by his side.

Visualizing a Graph set

1. Access the path **Historical data** → **Graph set**
2. Click on the icon for the desired Graph set, that it's on the tree menu.

Editing a Graph set

1. Click on **Historical data** → **Graph set**.
2. Choose one of the following buttons:
   - **Dependencies** to view and delete graphs from a graph set.
   - **Edit** to change the name and description fields from the Graph set.
   - **Delete** to erase the graph set.

Generating graphs for a Graph set

1. Access the graph set;

2. Click on ⚙ symbol;
3. Choose one of the following options:
   - **View graphs** to set an initial time for the graphs displayed on screen.
   - **Save images** to generate and save each graph as one PNG image.
4. Fill the fields:
   - **From**: Initial time of the graph;
   - **Save at**: Path to save an image of the graph set. Example: C:\Users\Telco\Images;
   - **Dimensions**: Dimensions of the image to be saved.
5. Click on **Generate graphs** button.

NOC Display

The NOC display mode is a view of the Graph sets. This display automatically switches between all user's enabled graph sets after a period previously configured in each graph set.

This feature is useful when the operator must constantly check all graphs on the graph set.

Chapter 6. Configuration

Traffic profiles

Definitions

Traffic profiles gives you the ability to build analysis where traffic from certain objects can be broken down based on other objects.

To build this type of analysis, you have to configure a profile, insert objects into it and then associate the profile to another object.

The database formed from this configuration will be the base to display the profile graphs and reports, like the traffic profile reports.

Examples of profile analysis are: interfaces against applications, subnets against subnets, subnets against applications and so on.

Configuration

1. Access **Configuration** → **Traffic profiles**.
2. Click the New button to create a new profile.
3. Fill the form below:

Table 6.1. Traffic profile form

Field	Description
Name	Profile name
Type	The profile type will enable you to select objects from that type to associate to this profile. Check the available objects below.
Graph curves	Choose the objects that will belong to this profile and their curve colors on the graph. To this purpose, move the objects from the left to the right box and then click on **Edit colors** button.
Default undefined label	If you deserve to rename the **Undefined** curve, select **No** and fill the **Label** field.
Enable trend analysis	Choose if you want to enable Trend Analysis. Refer on trend analysis section for hints on how to configure its parameters.
Object selection box	Use this menu to select the objects whose traffic will be analyzed by this profile. At the first layer, select the object type, so the system will display the available objects and, at the second layer, select the analysis type.

Available objects

- Application
- Application group
- Autonomous system
- Autonomous systems group
- Interfaces group
- Mapped object
- Protocol
- Subnet
- Subnets group
- ToS
- ToS group

Analysis types

The analysis type that you select when an object is associated to a profile will dictate the way traffic will be classified.

There are three analysis types available, which are explained next.

Matrix

The traffic profile objects are searched at the opposite direction of the traffic that is under analysis.

For example, lets suppose that a traffic profile composed of subnets is associated to a subnet under this analysis type. Then for the subnet's destination traffic, TRAFip will try to match the traffic profile subnets against the IP source field. For the subnet's origin traffic, TRAFip will try to match the traffic profile subnets against the IP destination field.

This type of profile association enables analysis like traffic exchanged between the central office and the regional offices of an enterprise.

To implement this analysis, follow the procedure below:

1. Create a subnet for each regional office and one for the central office subnet.
2. Create a traffic profile containing the regional offices subnets.
3. Associate the traffic profile to the central office subnet using the matrix analysis type.

Distribution

The traffic profile objects are searched at the same direction of the traffic that is under analysis.

For example, lets suppose that a traffic profile composed of subnets is associated to a subnet under this analysis type. Then for the subnet's destination traffic, the system will try to match the traffic profile

subnets against the IP destination field. For the subnet's origin traffic, the system will try to match the traffic profile subnets against the IP source field.

This type of profile association enables analysis like detailing traffic incoming or outgoing from a group of subnets. This is usefull, for example, to check the load balance of a group of servers.

To implement this analysis, follow the procedure below:

1. Create a subnet for each server.
2. Create a subnet group containing the server subnets.
3. Create a traffic profile containing the server subnets.
4. Associate the traffic profile to the subnet group using the distribution analysis type.

Content

The content analysis type is used for objects where there is not the notion of source or destination traffic.

Those objects are, for example, Protocols, Applications, ToS and ToS Group. So for each flow, there is only one protocol, one application and one ToS.

Whenever you create profiles with this type of object, use the content analysis type.

Domains

This object allows all objects except for devices, interfaces and interface groups to be summarized considering only the flows for each domain.

Domains are usually used to separate similar traffic flowing through different routers. Ex: border routers and backbone routers.

To switch between domains, use the select box that appears at the **Historical data** tab with each domain name.

Definitions

- A domain is composed of devices.
- A device can only be associated to one domain.
- Domain total traffic: composed by the sum of all flows belonging to the domain's devices.

Configuration

To create a new domain access **Configuration** → **Domains** and click the New button.

Table 6.2. Domain form

Field	Description
Name	Enter a name for the domain.

Field	Description
Interval between alarms (seg)	When an alarm type is triggered, another alarm of the same time can only be triggered once this interval is over.
Time limit to accumulate traffic (sec)	This limit defines when the analysis will occur. In the case, only it will be consider the data with the time difference between the first and last one within this limit.
Bytes threshold (accumulated in the period)	Limit of bytes received/sent by/to a host to trigger an alarm. A High data flow between two IP address alarm will be trigger once this threshold is reached.
Packets threshold (accumulated in the period)	Limit of packets received/sent by/to a host to trigger an alarm. A High data flow between two IP address alarm will be trigger once this threshold is reached.
Flows threshold (accumulated in the period)	Limit of flows received/sent by/to a host to trigger an alarm. A High data flow between two IP address alarm will be trigger once this threshold is reached.
IP Flood threshold (number of IPs accumulated in the period)	Limit of connections received/sent by/to a host. The minimum value is **2** to trigger an alarm.
Minimum percentage for traffic characterization	When in distributed architecture, the traffic can be characterised as suspect on collectors when only a percentage of the total thresholds is reached. Define this minimum percentage using this field.
Tolerance for time difference between local system time and flow exporter time	Define the tolerance time, in seconds, to consider a flow is within the analysed period so it will not be discarded. The minimum value is **60**.
IPs excluded from suspect traffic analysis (IP/mask)	Enter the subnets IP address to be excluded from the suspect traffic analysis. Separate by comma.
Interfaces group aggregation	Select the interfaces grop aggregation that will be part of the domain.
Device domain	Select the devices that will compose the domain.

Once a domain is created, you should configure the RFI interfaces depending on your network topology.

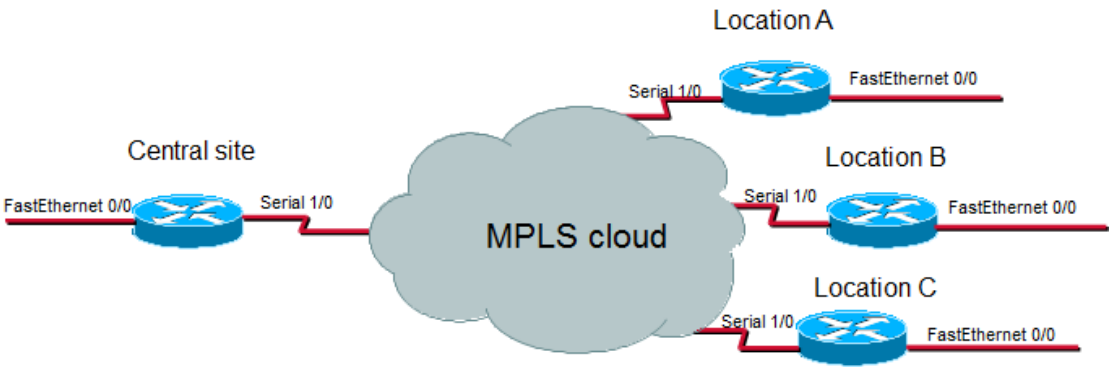
RFI interfaces

The RFI configuration will make the system filter the same traffic exported by more than one router in a domain

This filter is based on the input interface field, so it will not be used for interfaces, interfaces groups and devices.

All flows are stored on disk, so the filter will be used only when the system is summarizing traffic or for raw data reports. The filter will not prevent the flows from being received.

The example below illustrated a scenario where the RFI filter is necessary. For the correct analysis of this scenario, it is necessary that all routers export flows on all their interfaces.



RFI interfaces example

What happens is that when a packet flows from the central site to a remote location, it is exported 2 times. One time when it ingresses the central site's router and the other time when it ingresses the location router.

For correct summarization of the central site subnet, for example, only one of the flows must be considered.

If all LAN interfaces, in this case, the FastEthernet interfaces, are configured as RFI interfaces, the flows exported having these interfaces as input interfaces will not be considered, therefore the final summarization result will be correct.

TRAFip can automatically configure the RFI interfaces, by considering that all interfaces in the same 30 bit mask network are linked to each other and setting the as RFI. This discover is performed using the SNMP protocol and the interfaces to be considered should be marked as auto rfi.

Configuration

Access **Configuration** → **Domains** and click the RFI button for the domain will wish to configure RFI interfaces.

Collectors

This section should be used if you are deploying the system in distributed architecture mode.

For more details on distributed architecture deployment, refer to distributed architecture parameters section.

Table 6.3. Collector form

Field	Description
Name	Name to identify a collector appliance.
Key	Fill a string key. This string should match the **collector key** field at the **System** → **Parameters** → **Distributed architecture** menu in the collector appliance.
IP address	IP address that the collector will use to access the central appliance.
Exporter IP	IP address used by the collector to receive flows from routers. This IP address is used in case

Field	Description
	you want the system to automatically reconfigure netflow export in the routers if a collector appliance crashes.
Password	This password should match the **password** field at the **System** → **Parameters** → **Distributed architecture** menu in the collector appliance..
Backup collector	Collector that will be the backup for this collector in case of failure.
Devices	Devices that this collector will collect.

Import collectors file

To import a file of collectors, access **Configuration** → **Collectors**.

Click the **Import** button and load the file.

A import devices file has the following fields:

Table 6.4. Fields from collectors file

Field	Description
Name	Possible characters for name field.
Key	Alphanumeric characters.
IP Address	IP Address. Ex.: 10.0.0.1
Password	Possible characters for password field.

Objects

In this section you can access and edit the already configured objects and create new ones.

For some object types, you have the option to upload a configuration file. This means you can configure more than one object at once.

Importing object files

1. Access **Configuration** → **Objects** and click the Import button for the desired object type.
2. Upload the formated file according to the instructions on screen.
3. Click the Add button.
4. Adjust the configurations and click the Save button.

Mappers

Mappers are used to discover objects related to a device using the SNMP protocol or TCS script. Examples of those objects are: network interfaces, processors, memory banks, storage units, probes and so on.

Mappers can have Devices automatically associated to them, considering Rules that must be set as conditions.

Procedure 6.1. Creating a mapper

1. Select **Configuration → Mappers**.

2. Click the New item button and fill the form as detailed below:

Table 6.5. Mapper form

Field	Description
Name	Mapper name
Icon	Image that will be exhibited next to the objects discovered by this mapper at the tree menu. See step 3 for instructions on customizing this image.
Automatic removal	If you want the objects mapped by this mapper to be removed after a certain number of consecutive days in which they are missing, select **Yes** and fill the number of days.
Include prefix	Include the mapper name as a prefix for objects discovered by this mapper.
OID instance used as object name	Mark this option if instead of populating the object name with the OID value, the mapper should populate it with the OID instance. This option should be used for objects that do not have an OID whose values can represent them. So you can use a statistics OID and map the object instances with this option.
Name	Name of the OID to be used for mapping objects.
OID	OID that will be used.
MIB	OID MIB.
Filter by SNMP collect	Filtering by SNMP collect response.
Devices association	Enable automatic device association to this mapper considering Rules. When enabled the form will show auto removal option that will remove the associated devices when the conditions are not met anymore
Devices	Select the devices associated with the mapper.

Tip

Under the section Mapping Setup, you should specify an OID (Object Identifier) from a device MIB (Management Information Base) where the system can find unique instance names as the returned values, so the objects can be identified. This OID can be loaded using the MIB Browse tool by clicking the Search OID button.

Use the Find OID button to browse the MIB and fill the last three form fields.

3. Configure the mapper icons.

a. Select the **Configuration** → **Mappers** menu and click the Change icons button.

b. Click the New icon button.

c. Fill the mapper name and upload a icon for each object condition.

d. Click the Send button.

Cross OID mapping

This feature allows you to create a mapper specifing 2 OIDs. The mapper will then find the values of the first OID and use then as indexes to find a value in the second OID.

So the mapper will map the index of the first OID with the value of the second OID.

This mapper can be used, for example, to map Cisco CPUs, where you can specify the following OIDs:

1.3.6.1.4.1.9.9.109.1.1.1.1.2;1.3.6.1.2.1.47.1.1.1.1.7

The first OID is the cpmCPUTotalPhysicalIndex from the CISCO-PROCESS-MIB and the second is the entPhysicalName from the ENTITY-MIB, where you can find the name of each CPU.

Associating devices to mappers

After configuring a new mapper, you should associate it to the devices where the objects should be discovered. This association can be done at each device configuration or by clicking the Devices association button at the mappers list.

Exporting and importing mappers

The **Export** button exports all mapper configuration to a file. To import back the configuration, you can use the **Import** button and then download this file.

EPM (Extended Processing Module)

EPM is another appliance in addition to the already installed one in the client. It is an extended module of the monitoring solution.

It needs to be enabled at **System** → **Parameters** → **EPM** .

EPM is a scalable solution for the amount of users accessing the system by the web interface, visualizing graphics e summarized data reports. The summarized data are replicated to the EPM machines making data access faster and data redundant.

1. Click **Configuration** → **EPM**.
2. Click New to create a new EPM entry.
3. Fill the name and IP adress fields.
4. Set administrative status.
5. Click Save.

Rules

Creating rules

1. Select **Configurations** → **Rules** and select the kind of rule at left, if it's Device or Mapped object.
2. Click the New button to create a new rule and fill the form:

Table 6.6. Automatic profile rules

Field	Description
Name	Rule name.
Description	Rule description
Database field filter	Filter based on database fields. For instance, the **Name** field is the object name and the **Mapper** field (only for mapped object rules) is the mapper name.
Filter by SNMP collect	Filter based on OIDs that will be polled when the rules are tested. Select the option **Use mapped object index** when using OIDs that should be tested against mapped objects, like, for example, ifConnectorPresent.

No Response filter

The 'No Response' filter, that is located in 'Filter by SNMP collect', consists in validate a object in case it returns a specific error message.

To use it, you must choose the 'No Response' operator in the filter. In the 'value' field you have to use one of this values:

- $nosuchobject$ - It's used to validate 'No such object' response from an object.
- $nosuchinstance$ - It's used to validate 'No such instance' response from an object.

Device Credential

Many devices use the same SNMP and Connection configuration.

It's possible to create a credential for these configuration parameters and then associate it to the devices that have the same configuration.

To create a new credential, access **Configuration** → **Device Credential** → **New device credential** or **Configuration** → **Device Credential** → **Device Credential** and click on **New** button.

Table 6.7. Device credential form

Field	Description
Name	Define the credential name.

Field	Description
Protocol	Choose **SNMP**, **SSH** or **Telnet**.
SNMP Version	Choose the SNMP version. Possible values are: SNMP v1 or SNMP v2c — Specify an SNMP community SNMP v3 — Specify the authentication type and its parameters
SNMP community	Enter the SNMP community.
SSH port	Enter the SSH port. The default value is **22**.
Telnet port	Enter the Telnet port. The default value is **23**.
User	User to be used to access the device. This string is available as a wildcard %username% for provisioning scripts.
User password	Password to be used to access the device. This string is available as a wildcard %passwd% for provisioning scripts.
Enable secret	Enable password to be used to access the device. This string is available as a wildcard %enable_passwd% for provisioning scripts.
Devices	Associate the devices that will use the credential.

Chapter 7. Tools

External Software

Telcomanager Windows Collector

Download the executable **Telcomanager Windows Collector** to install the Netflow collector for Windows.

It replicates all the Netflow packets received by a Windows machine to a TRAFip appliance.

Telcomanager Host Agent

Download the executable **Telcomanager Host Agent** (THA) to install it on Windows.

This agent collects information about the running processes.

Telcomanager Windows Security Agent

Download the executable **Telcomanager Windows Security Agent** (TSA) to install it on Windows.

This agent gathers information about the files monitored by the Security Integrity system and send it to CFGtool.

Discovery

The discovery feature is used to discover every host in a network. Fill the IP/Mask field and click Execute button to start the discovery function.

When the process is finished, the system will show a list with all the discovered hosts.

Chapter 8. System

Access Log

User access

This option displays a report summarized by day containing user access logs. Each report line is a link for a detailed report for the day.

Simultaneous access

This report displays the number of user logged in the system for each user group.

Users

The system has three user types:

User types

Administrator	Has full access to the system
Configurator	Can create, remove and edit any system objects. Cannot make changes to System configurations.
Operator	Can only visualize system monitored objects and reports.

When you associate groups to users, you will restrict this user visualization to objects within the group hierarchy.

Users can also be limited on the menus that they will access and on the number of simultaneous users that will access the system.

Editing users

1. Select **System** → **Users** → **User list** .
2. Click the New or Edit buttons and fill the form below:

Table 8.1. User form

Field	Description
Username	User login.
Name	User name.
Password	Password.
Password check	Repeat the password.
E-mail	E-mail to send alarms and when a scheduled report is available. You must configure the SMTP server .

Field	Description
SMS	Celular phone number to send alarms using the SMPP protocol or celular@teste.com to send short emails with alarms. The system can also send SMSs through the integration with a web portal.
Enable Favorites	Enable Favorites feature.
Use compact graph	Visualize graphs in a default size or compact them.
Local authentication	This field is visible only when Active Directory or TACACS is enabled. To configure the Active Directory, access **System** → **Parameters** → **Active Directory** and to configure the TACACS, access **System** → **Parameters** → **TACACS** .
Theme	Set user theme. Choose the Default Theme in **System** → **Parameters** → **Theme**
User group	Associate this user to a user group in order to restrict the number of simultaneous accesses to the system within the group.
Language	Set user language.
Profile	Set user profile to restrict alarm and service alarm visualization and notification.
Type	Choose the user type.
Menu	Use the **Customize** option to restrict the user to specific menus.
Groups	Select the subnet groups that the user will be able to access.
Subnets	Select the subnets the user will be able to access.

User Groups

The user groups are used to manage how many users can login simultaneously to the system.

Procedure 8.1. Managing user groups

1. Select **System** → **Users** → **User group** .
2. Click the New or Editbuttons and fill the form below:

Table 8.2. User form

Field	Description
Name	User group name.
Description	User group description.
Limit simultaneous access	Select a number between 1 and 255. This will limit simultaneous access to the system within the users of this group.

Field	Description
Users	Specify the users that will be placed in the group. A user can belong to one group only.

User profiles

The user profiles are used to associate alarms to users.

Procedure 8.2. Managing user profiles

1. Select **System** → **Users** → **User profiles** .
2. Click the New or Edit buttons and fill the form below:

Table 8.3. User form

Field	Description
Name	User profile name.
Telegram bot token	Token obtained after creating a new bot in Telegram.
Telegram chat ID	Chat ID of the chat which the bot partakes.
Users	Associate users to this profile.
Profile -> Alarms	Associate pair of Profile -> Alarm to this profile.
Service alarms	Associate service alarms to this profile.

Alarm Console

You can select the columns that will be shown at ALARMmanager console. Furthermore, you are able to configure the order the columns will appear. For this purpose, click and drag the lines.

Table 8.4. ALARMmanager console columns

Column	Description
START TIME	The time of the first occurrence.
END TIME	The time of the last occurrence. Displays ACTIVE if the alarm has not ended.
USER	User that acknowledged the alarm.
TYPE	Object type, can be device of mapped object.
OBJECT	Object name.
DESCRIPTION	Object description.
IFALIAS	If the object is an interface, displays its ifAlias.
STATE	Alarm state, can be active or inactive.
ALARM	Alarm name.
LEVEL	The level for the alarm defined at the level configuration.
TRAP	Yes if it was generated by a trap and no otherwise.

Column	Description
COMMENTS	Comments by the operator. To insert a comment, click two times in that cell.

Backup/Restore

You can perform backup and restore of all system data to and from an ftp server or a simple file download/upload with all system configurations.

Go to **System** → **Backup/Restore** to work with the following backup/restore options:

Local configuration backup

Click on this icon to display all current configuration backup files.

You can create a new file by clicking the Create new button.

The Setup button is used to set the number of backup files to keep.

Click the Download button to download the configuration file to your desktop.

The Copy to restore button is used to copy a configuration file to the restore area in order to restore this backup file.

Local configuration restore

This option is to be used to restore a backup file. By doing that, all current system configuration will be replaced by the definitions contained in the restored file.

To perform a system restore, you should either upload a configuration file from your local machine or copy an old backup file available in the system and then click the Restore button for that file.

Remote backup

This option can be used to save the system configuration files and historical database to a remote backup server.

Table 8.5. Remote backup form

Field	Description
IP version	Select IPv4 or IPv6.
Backup Server	IP address of the backup server.
Backup Directory	Directory on the backup server.
User	User to authenticate on the backup server.
User Password	Password.
Backup protocol	Protocol to be used for backups.
Protocol port number	Port number.

Field	Description
Server size (GB)	The server size in Gigabytes.
Activate backup	Select **Yes** to activate the backup feature.
Backup start time	Enter the time of the day to execute backups.

Important

This feature will not save the raw flow data, since this data is mostly used for troubleshooting and it usually takes up a high volume of storage space.

Remote restore

Select a single system to perform data restore or click the Request complete restore to fetch data from both systems.

Important

- The ftp server must be online, since the data will be fetched from it.
- Only perform this operation on a new and empty TRAFip or SLAview installation, since all system data will be replaced.

Restore status

This option will display the restore status once you request a remote restore operation.

Parameters

This section is used to configure various system parameters that are used for different processes.

Active directory

This option will enable users to access TRAFip using the Active Directory Kerberos authentication method.

In order for a user to authenticate using this method, it must be configured in the system.

Table 8.6. Active directory form

Field	Description
Enable Active Directory authentication	Once **Yes** is selected, the **Local authentication** field will be available in the user form.
Server	Enter the server address. Example: kerberos.example.com
Domain	Enter the Active Directory domain. Example: ATHENAS.MIT.EDU

When this method is enabled, there isn't local authentication, it means **Operator** and **Configurator** users can only log in TRAFip using Active Directory.

Important

The **Administrator** user can choose to log locally or not, however, it's recommended to always have a **administrator** user with **Local authentication** enabled, when there is a external access control.

ALARMmanager

Table 8.7. ALARMmanager parameters form

Field	Description
Maximum events storage period	Number of hours that the ocurrence table will hold ocurrences. This table is used only for deep level debugging purposes, since the ocurrences are not used after they are processed.
Maximum alarms storage period	After this period, the alarms will be deleted.
Maximum inactive alarms storage period	Once an alarm becomes inactive, it will be available at the ALARMmanager console for this period. After that, the alarm can be visualized at the ALARMmanager reports.

Alarm ocurrences or events are generated by the following processes:

- SlaSumCaching: generates ocurrences for all configurable alarms created with summarization variables.
- ICMPAgent: generates ocurrences for the **Not replying ICMP** alarm.
- MIBget: generates ocurrences for the **Not replying SNMP** alarm.
- ObjectMapper: generates ocurrences for the **Object not found** alarm.

Caution

You can check the **Configurations** item under the **System** → **Diagnostics** → **Storage usage** section to check if the database is too big, indicating that the system is generating too many alarms. If that is the case, you can decrease the alarm storage period or adjust the alarm settings to generate less alarms.

Association agents

Automatic association agent for mappers

Define the time to start the automatic association for mappers. It will happen twice a day.

Table 8.8. Automatic association agent for mappers form

Field	Description
First execution time	Set the first execution time.
Second execution time	Set the second execution time.

Auto login

This feature enables the authentication bypass for URL requests coming from another system.

To enable this feature, follow the procedure below:

1. Go to **System** → **Parameters** → **Auto login** .
2. Select Yes on **Enable auto login** option.
3. Fill the referer URL in the format, which is the page from which the requests will be originated.
4. On your web server, fill the following URL: http://TelcoApplianceIP.

Backup

- Data: Parameters to perform remote backup. Refer to remote backup section.
- Configuration: configure the number of old configuration backup files to keep in the system.

Capture agent configuration

Set the allowed number of simultanous executing agents.

Table 8.9. Capture agent configuration form

Field	Description
Number of simultanous executing agents	Choose a integer smaller than or iqual to 10. The default is **3**.

Cisco WAAS

Cisco WAAS (Wide Area Application Services) is a Cisco Systems technology. It improves the performance of applications on a wide area network (WAN).

Table 8.10. Cisco WAAS form

Field	Description
Enable Cisco WAAS monitoring	Select **Yes** to enable the Cisco WAAS (Wide Area Application Services) monitoring, select **No** otherwise.

Configuration history

Set the storage period for different configuration areas.

Table 8.11. Log history parameters

Field	Description
Maximum configuration data storage period	This includes all configuration changes, except for the user related operations. This data can be displayed at **System** → **Diagnostics** → **Configuration Logs** .

Field	Description
Maximum user configuration data storage period	This is specific for user operations. This data can be displayed at **System** → **Diagnostics** → **Configuration Logs** by selecting the User option on **Object type** field.
Maximum flow statistics storage period (months)	This field is related only to the flow processes. This statistic can be visualized at **System** → **Diagnostics** → **Flow statistics** .
Maximum summarization statistics storage period	This is related only to the summarization processes. This statistic can be checked at **System** → **Diagnostics** → **Summarizer** .

Data storage

In this area, you should configure the storage space that should be allocated for each type of system data.

The field **Available distribution space** will display the space that can still be distributed.

To check how much space each area is consuming, you should login to the desired system (TRAFip or SLAview) and access **System** → **Diagnostics** → **Storage Usage** . The TDB database item corresponds to the summarized data for each system.

You can perform redistribution of storage space between different areas at any time.

Table 8.12. Data storage form

Field	Description
Start process from occupation at %	When this value is reached, the agent will be executed. Fill with a value between **1** and **85**.
Execution type	Choose if the agent will run at each **Time interval** or in a **Time schedule**.
Execution time interval (minutes)	Define the time interval, in minutes, to the agent be executed. The minimum value is **10**.
Scheduled report time	Define the time when the agent execution will start.
SYSLOG storage	Storage dedicated to SYSLOG raw files.
Scheduled reports	Storage dedicated to scheduled report files.
Trap receiver storage	Storage dedicated to trap receiver files.
Capture files storage	Storage dedicated to capture files.
TRAFip raw data storage	Storage area dedicated to TRAFip raw flow files. This storage usually grows a lot faster than the summarized data. If you configure it with the same size of the summarized data, you will typically end up with 10 times less historical data.
TRAFip summarized data storage	Storage dedicated to TRAFip processed data or TDB - Telco Database. This data is used for graphs and Top N reports.

Field	Description
TRAFip summarization remote files	Storage dedicated to TRAFip processed data files sent from collectors on distributed architecture environment.
TRAFip behavior change data	Storage dedicated to TRAFip behavior change files, for instance, history alarms data.
SLAview raw data storage	Storage dedicated to SLAview raw files. This is in general the collected SNMP OIDs.
SLAview summarized data storage	Storage dedicated to SLAview processed data. This data is used for graphs and reports.
SLAview summarization remote files	Storage dedicated to SLAview processed data files sent from collectors on distributed architecture environment.
SLAview behavior change data	Storage dedicated to SLAview behavior change files, for instance, history alarms data.
CFGtool versions data	Storage dedicated to device configuration files. Even when this value is reached, the version data of devices with just one version will not be excluded.

When the fields **Raw data (MB)** and **Summarized data (MB)** are filled with '**0**' (zero), it means the system is distributing automatically the **Available distribution space** between the **TRAFip raw data storage**, **SLAview raw data storage**, **TRAFip summarized data storage** and **SLAview summarized data storage**.

You are able to set manually these values, but don't forget the raw data storage usually grows a lot faster than the summarized data. To redistribute the storages, divide the **Available distribution space** by four and you will have each storage size value.

Caution

If you reduce the storage space of any of these areas, the next time the garbage collector process runs, it will clear the data to adequate the storage space.

dbn0/Altaia integration

Altaia is a performance and QoS management platform. Fill the fields in the form and configure the dbn0/Altaia integration.

Table 8.13. dbn0/Altaia integration form

Field	Description
Enable dbn0/Altaia integration	Choose **Yes** or **No**.
Server IP Address	Enter the server IP address.
Directory to send the file	Enter the directory.
Server user	Enter the server.
User Password	Enter the user password.
5 minutes steps	Enter a number.
5 minutes delay	Enter a integer equal to or greater than 2.

Distributed architecture

These parameters should be used if you wish to run the system on distributed architecture mode.

For more details about distributed architecture's concepts and prerequisites, refer on distributed architecture feature section.

Table 8.14. Distributed architecture parameters form

Field	Description
Maximum number of consecutive collector fails	This number represents how many times the central node will wait for the processed files from a collector node until this node is considered down. This check is performed every 5 minutes by the sum-control processes for TRAFip and SLAview systems. After a collector is set to down by the central node, the backup collector, if set, will take on the faulty collector operations.
Enable Distributed Architecture	Select this option if this appliance will be part of a distributed architecture system.
Is collector?	Mark **Yes** at this option if this appliance will take a collector role on the system. Otherwise this appliance will be considered a central node.
Collector key	Fill with a string to identify this collector on the central node.
IP version	Select IPv4 or IPv6.
Central Storage IP	Fill with the IP address of the appliance to be used as a central node.
Password	Password used for authentication.

EPM

EPM (Extended Processing Module) is another appliance in addition to the already installed one in the client. It is an extended module of the monitoring solution.

Table 8.15. EPM form

Field	Description
Enable EPM	Select this option if you deserve to enable this module of the monitoring solution.
Is EPM?	Mark **Yes** at this option if this appliance will be used as EPM.

Important

By changing this setting you'll lost all your historical data, so be careful!

Expiration warning

Set when you will be informed about the license expiration date.

Table 8.16. Expiration warning form

Field	Description
Warn expiration lasting	Define the number of days between 10 and 30.

File transfer

These parameters are used to configure the transfer of files, using the FTP protocol, containing selected objects 15-minute statistics.

FTP Server IP address	IP address of the FTP server.
Port	TCP port to connect to the FTP server
Server user	Username used to connect to the FTP server.
User password	Password used to connect to the FTP server.

Flow exporters verification

With this feature enabled, all Flow exporters configured will be checked from time to time, and for each exporter that is a given time without exporting flows it's icon will change, showing the users the lack of flows being received from that exporter.

Flow exporters verification form

Enable exporters verification	Choose **Yes** or **No**.
Export inactivity time	Choose the limit time, in minutes, for each exporter will be flagged not-exporting.

Grapher

Adjust the grapher parameters.

Table 8.17. Grapher parameters form

Field	Description
Enable Derivative Graph as Default	On standard mode, graphs points are connected using linear interpolation. On derivative mode, the piecewise interpolation is used.
Enable auto-refresh	Select this option to have all graphs automatically refreshed. You can also enable this option at runtime for each graph.
Show business hours	Enabling this option, the business hours will be shown on the graphs. Set the business hours period at Local preferences.
Exclude weekends	Enabling this option, the weekend days will be shown in brighter colours on the graphs.
Auto-refresh interval	Interval between refreshes.

HTTPS Configuration

Configure the HTTPS (HyperText Transfer Protocol Secure) mode.

Table 8.18. Https parameters form

Field	Description
Enable https	Choose **Yes** and the server will restart in https mode.
Certified	Select the https certified.

Interface customization

You can customize how the devices will be displayed on **Historical Data** → **Devices** → **Device** tree menu.

To do this, just fill the **Device formula name** field with what you desire to be shown on menu.

The formula has special tags which use the device information. Here they are:

Table 8.19. Device formula name

Tag	Description
%n	Refers to device **name**.
%a	Refers to device **management IP address**.
%t	Refers to device **type**.
%m	Refers to device **manufacturer**.
%d	Refers to **device type** (Camera, Firewall, Router, Server, Switch or Wireless).

Local preferences

Table 8.20. Local preferences form

Field	Description
PDF page size	Page size to be used for PDF reports.
Search limit	Fill with a positive integer to limit your researches. The default number is **2500**.
Business hours first period	Set the start time and the end time for the business hours first period.
Business hours second period	Set the start time and the end time for the business hours second period.

Login redirection

Fill the **Destination page after login** field to be redirected to another system after login. On the redirected system, you will be able to access all TRAFip/SLAview objects without authentication.

Log level

Choose the ALARMDaemon level: **Low**, **Medium** or **High**.

This level will determine the amount of details in alarm log.

Logo

Pick an image file from your Desktop and upload it, so the image will be displayed at the top right corner.

Remember the image must be of fixed height of 43 pixels and variable width from 20 to 200 pixels.

Object Mapper

For more details about object mapping, refer to mapper configuration section.

Table 8.21. Object mapper configuration parameters form

Field	Description
Execution Interval	Set the interval between mapper executions.
Configuration history storage period	Set the period for storing logs from configurations performed by the mapper.
Simultaneous TCS mappers limit	Define the maximum number of simultaneous TCS mapper executions. Fill with a value between **1** and **200**. The misconfiguration of this parameter can affect the system performance, so be careful!

Redundancy

This section is used to specify the redundancy setting.

Table 8.22. Redundancy settings

Field	Description
Enable redundancy	Choose Yes.
IP version	Select IPv4 or IPv6.
Local IP Synchronization	Fill with the IP address configured for the interface directly connected to the other appliance.
Remote IP synchronization	Fill with the IP address configured for the remote appliance.
Max history size	Configure the max history size in MB. The minimal historic size is 16MB.
Commutation interfaces	Select the interfaces that will share IP addresses between the two appliances. Use the **CTRL** key to select multiple interfaces. At least one interface must be reserved to have an exclusive IP address for management purposes. One interface must be used for the back-to-back connection and the others can be used to share IPs.
Prefered state	Select **Master** or **Slave**.

Refer to redundancy section for details on enabling this feature.

Regional settings

Table 8.23. Regional settings form

Field	Description
Decimal separator	Decimal separator to be used for system reports.
System Language	Choose the default system language. Each user can define its own language settings under user configuration.
Number of decimals in export files	Configuration used to format number fields on exported reports.
Csv file separator	Separator to CSV reports.

Reports

This section shows how to make advanced configurations for reports.

Scheduled Reports

You have the option to schedule your reports. In this section, configure this mode.

Table 8.24. Scheduled reports configuration form

Field	Description
Refresh time of the wait page (seconds)	Enter a integer number.
Max Time of Execution (minutes)	Enter a integer number.
Max Simultaneous Processes	Enter a integer number.
Email subject prefix	Define the default email subject prefix.
Hostname for link in email	Configure the email hostname.

Summarized data

Configure the maximum period for report data in days. The default is **180** and the maximum value is **360**.

TRAFip raw data

Fill these fields to configure raw data report form. For further information about this report, access: Raw Data Report section.

Table 8.25. TRAFip raw data

Field	Description
Maximum data period per report (hours)	Enter a integer. The default is **18** and the maximum value allowed is **24**.
Max lines per report	Enter a integer number.
Make sampling rate threatment by configuration default	Choose **Yes** to fill the **Sampling rate treatment** field with **Configuration** automatically.

SMS server

SMPP(Short message peer-to-peer protocol) method

Use this method if your mobile operator provides a SMPP account.

Table 8.26. SMPP server form

Field	Description
SMS Protocol	Choose the SMPP option.
Host	SMPP host.
Port	SMPP port.
System ID	SMPP system ID.
System Type	SMPP system type.
Password	SMPP password.
URL	Refer to URL section.
Origin phone number	phone number that will be displayed as the caller on SMS messages.

SMSs can be sent using two distinct methods. Both configured through this form.

URL(Uniform Resource Locator) method

This method should be used if you have a http gateway.

SLAview will perform an http GET operation using the provided URL.

You should use the $CELLPHONE$ and MSG wildcards in the URL.

The $CELLPHONE$ wildcard will be replaced by the SMS field that you filled in the user configuration form.

The MSG wildcard will be replaced by the alarm message, which contains the following information:

- Alarm name.
- Alarm urgency level.
- Alarm state.
- Date and time that the alarm switched to that state.
- Alarm varbind.

Simple filter

When there is a considerable amount of subnet groups configured, this filter is a big help for system users.

Once the **Number of characters of subnet filter** is set, a selectbox will appear in the **Historical data** → **Subnets** main menu cointaining all subnet groups, but just with the amount of characters delimited by you.

Thus, when you select one of these groups shown on filter, the section **Subnet groups** will only display the chosen and the subsequent groups.

It's important to emphasize that, when the simple filter is configured, the subnets menu isn't displayed. So, the subnets can only be visualized through the subnet groups.

Important

When this field is filled with **0** (zero), this filter isn't shown.

SMTP

Fill this form with the SMTP parameters to send emails.

Table 8.27. SMTP parameters form

Field	Description
SMTP Server	Configure the SMTP Server. The port used by the SMTP server can be changed in this field. Follow the example: smtp.server.com:port
SMTP user	Enter the email.
SMTP password	Enter the user password. If the SMTP server does not require authentication this field should be left blank.
SMTP from	Set a sender for the email.

You can verify SMTP configuration before saving: click on **SMTP test** and enter the email address for test.

SNMP

SNMP Collector

These parameters will be used for all processes that perform SNMP polling. These are the default configurations, but they can be fine tuned at the device level.

For a reference of all system processes, go to the log files section.

SNMP parameters

SNMP Timeout — Time limit in seconds that the collector will wait for a SNMP reply packet. Value range: 1-10.

SNMP Retries — Number of retries that will be issued to the device if it does not respond to a SNMP query. Value range: 1-10.

Number of OIDs per packet — Number of OIDs the collector will send in each SNMP packet. Value range: 1-100.

Maximum packet rate (pps) — Maximum number of packets per second that a SNMP collector will send for each device.

SNMP window — Number of SNMP packets that will be sent without answer from the device being polled.

SNMP port — Default TCP port to connect to the SNMP agent

Enable SNMP polling	Enable SNMP polling for TRAFip. Mark this option to enable the InterfaceCollect process to poll interface traffic counters.
Ignore interfaces	Fill the expression to ignore these interfaces.
High counter interfaces	Fill the expression to use the high counter OIDs (ifHCInOctets and ifHCOutOctets) on these interfaces.
SecRate Interfaces	Fill the expression to use the sec rate OIDs (IfHCIn1SecRate and IfHCOut1SecRate) on these interfaces.

SNMP Trap

Fill the fields below to specify the hosts that will receive traps. This traps can be alarms from ALARMmanager or self generated traps from TELCOMANAGER MIBS.

Table 8.28. TRAP fields

Field	Description
Trap forwarding hosts	IP addresses of the hosts. Ex: 10.0.0.1,10.0.0.2.
Trap Communities	SNMP communities of the trap hosts.

System Version Check

Every day between 2 a.m. and 3 a.m., the system version check verifies if there is a new available build version. Once this is true, the user will be informed.

TACACS

Enables TACACS+ authentication method. Two servers can be configured for redundancy.

The username and password for each user should be configured in the system exactly like the TACACS (Terminal Access Controller Access-Control System) server.

When this method is enabled, there isn't local authentication, it means **Operator** and **Configurator** users can only log in using TACACS.

Theme

In this section, you can set the Default system theme.

Table 8.29. Theme configuration

Field	Description
Default theme	Choose the default system theme: Dark, Green & Yellow or Telcomanager.

Tip

Notice that each user can define him own theme in user configuration.

Threat Analysis

In this section, you will configure if you desire to use TRAFip to detect suspect traffic or to use the threat analysis module, TRAFwatcher.

Table 8.30. Threat analysis configuration

Field	Description
Maximum suspect traffic events storage period (days)	Set the maximum period, in days, to storage the suspect traffic events.
Use legacy threat analysis engine	Select **Yes** to use TRAFip suspect traffic analysis, otherwise the TRAFwatcher will realize the threat analysis.

Important

When using TRAFwatcher engine, it is necessary to enable the threat analysis in the desired subnet form.

TRAFip

Enable or disable the automatic detection of RFI (Repeated flow interface) interfaces. For further information about RFI's, refer to RFI interfaces section.

Trend Analysis

Trend analysis default parameters. Refer to trend analysis section for hints on how to configure these parameters.

User access history

There is a tool that offers a daily summarized report containing user access logs. For further information about it, refer to Access log section.

Configure this user access history storage period.

Table 8.31. User access history form

Field	Description
Maximum user access log storage period (months)	Enter a integer smaller than or iqual to 36. The default is **12**, that is, 1 year.

Web Services

Configurations API

Table 8.32. Configurations API form

Field	Description
Hosts with access granted to the configurations API	Configure the hosts that are allowed to access the API configurations.

Field	Description
Username used by configurations API	Enter the username.

TRAFip's raw data

Configure the access to TRAFip's raw data.

Table 8.33. TRAFip's raw data form

Field	Description
IP used to access	Enter the IP.
Password	Enter the password.

Diagnostics

Network information

Displays system date and time, network interfaces information and default gateway.

Connectivity tests

Tests like ping, nslookup and traceroute to test the connectivity between the appliance and network elements.

Packet Capture

Using this tool, you can analyze the packets passing through the appliance interfaces.

Click **System** → **Diagnostics** → **Packet capture** .

Click on New button.

Table 8.34. Packet Capture

Column	Description
Network interface card	Choose the interface to analyze.
Maximum file size	Choose the maximum file size where the result of the analysis will be written.
Maximum number of packets	Fill the maximum number of packets to analyze. Fill 0 for no limit.
Port	Filter ports to analyze. Type * for every port or comma separated values.
Exclude Port	Exclude ports to analyze. Type * for every port or comma separated values.
Host	Choose one host to filter or select **All** for every host.

Click Send to start the capture and then Back to back to the list of capture files.

If you wish to stop the capture, click Stop. A Download button will show up and you can download the capture file.

Objects

Displays the number of objects and profiles configured.

Flow exporters

Lists all the IP exporters and the flow statistics in the last 30 minutes.

Flow statistics

Displays the maximum and the average flow statistics by the period of 30 minutes, 2 hours and 24 hours.

Set the maximum flow statistics storage period at **System** → **Parameters** → **Configuration history** .

Summarizer

This section displays the time that the summarizer process took to run for the last day.

When deploying the system in distributed architecture, the time to send the summarized files from all collectors is also displayed.

Important

The summarization process runs every five minutes, so the time to run the process should be below 5 minutes for good system performance.

Storage usage

Displays information about storage areas usage.

System registries	Logs from the operating system.
SLAview registries	SLAview logs.
TRAFip registries	TRAFip logs.
SLAview TDB database	Storage usage for the SLAview Telco database, which is used to hold SLAview summarized data.
TRAFip TDB database	Storage usage for the TRAFip Telco database, which is used to hold TRAFip summarized data.
TRAFip raw data	Storage used for the TRAFip raw data.
SLAview raw data	Storage used for the SLAview raw data.
Data details	raw data storage by day for the system you are currently logged in.

Log files

In this area, you can visualize the system log files. Below a list of available files.

LOG Files

createMark.log	Logs from to the version update process.
backupgen.log	Daily configuration backup process logs.
dbackupArchive.log	Logs from the remote backup process.
summarizer.log	Logs from the summarizer process. This process calls the TRAFIPsum process, which processes the TRAFip rawdata. When the system is in distributed architecture, the summarizer is responsible for sending the sumlog (files containing summarized data) files to the central machine.
TRAFIPsum.log	Logs from the TRAFIPsum process, which is responsible for processing the TRAFip rawdata according to the configurations. This process runs every 5 minutes. On distributed architecture, the TRAFIPsum runs at the collector nodes.
TRAFIPlookupd.log	Logs from the process responsible for performing various translations that are used by the TRAFip rawdata reports. Examples: IP addresses to subnets, DNS, Netbios and application translations.
Gc*	Logs from the garbage collector process.

Configuration Logs

This option contains a form where you can display system configuration logs.

These logs are kept for a period defined at **System** → **Parameters** → **Configuration history** → **Maximum configuration data storage period** .

Suspect Traffic Statistics

The average suspect traffic statistics, as source and destination bytes, packets, flows and IP Flood, are shown for each domain.

Timezone

This menu is used to set the correct timezone for the server. There are 4 system pre-defined time zones: **Brasília**, **Acre**, **Fernando de Noronha** and **Amazônia**. You can select one of them or to upload a new one.

This procedure is usually necessary if there are daylight savings date modifications.

Support

This option can be used to stablish a secure connection to the Telcomanager internet support servers.

Once the connection is stablished, you can contact the Telcomanager support team with the service code used.

Tip

If your service code does not work, try to enter a different service code.

About

This section lists the currently installed version and the licensed options.

You can also check the number of existent devices, the historical data series and the limit bits/s or flow/s.

Chapter 9. ALARMmanager

Reports

To access ALARMmanager reports, go to **ALARMmanager → Reports**

Suppressed reports

This report provides the logs for all the suppression operations performed by the users.

Table 9.1. Suppressed alarms report form

Field	Description
Output format	Select HTML, PDF or CSV format.
Object type	The object type for the alarms.
Start time	The start time for the report.
End time	The end time for the report.
Operation	Filter for the suppression operation.
User filter	Filter for the user that performed the operation.
Object filter	Filter for the object in which the operation was performed.
Alarm filter	Filter for the alarm in which the operation was performed.

Consolidated reports

This report provides a view of all alarm events in a detailed or resumed way.

This report can be saved as a template. For instruction on working with report templates, go to templates section on this manual.

Table 9.2. Consolidated alarm report form

Field	Description
Alarm filter	Use Regular Expressions and click the filter button to select the desired alarms.
Object filter	Use Regular Expressions to filter the desired objects.
Manufacturer	Filter by the manufacturer of the object. You have to use Regular Expressions to filter.
Manufacturer Type	Filter by manufacturer type of the object. You have to use Regular Expressions to filter.
Object type	Type of the object.
ifAlias filter	Filter based on interface ifAlias OID. You have to use Regular Expressions to filter.
Start time	The start of the analysis period.

Field	Description
End time	The end of the analysis period.
Period	If **All day** option is marked, this field is ignored, otherwise the data is selected within that range for each day.
Exclude weekends	Exclude weekend periods from the report data.
Active only	To display only active alarms.
Consolidated	This option will summarize all occurrences of an alarm for each object.
Generated by trap only	Shows only alarms generated by **link down** traps.
Output format	Select HTML, PDF or CSV format.
Groups	This field can be used to filter objects associated to some root groups.

Tip

To sort report results, click at each column header.

Email Template

Introduction

You can select the ALARMmanager email format and choose if you want to use the default template or to personalize it.

Table 9.3. Email template

Field	Description
Enable default email template	Select **No** to customize the email template.
Email content	You can choose the email format you will receive (HTML or Txt).

Customizing the email

When you are editing your email template, it's possible restore the default one just by clicking the **Restore default template** button.

If the email content is in the HTML format, you can visualize the preview before save the new template. To do this, click on the **Preview** button.

You will have the following keywords enclosed by '**$**' and you may substitute them for your alarm configuration:

Table 9.4. Email variables

Variables	Description
$date$	Alarm start/end time.
$objtype$	Object type: Mapped object or Device. Service alarm does not have any type of object.

Variables	Description
$object$	Object name.
$path$	Shows the path for the object in the SLAview groups.
$alarm$	Alarm name.
$action$	Alarm state: active or inactive.
$level$	Alarm urgency level.
$formula$	Alarm formula.
$varbind$	Varbind.
$suppressed$	Indicates if alarm is suppressed.
$color$	Variable to be used in HTML email. Green to disabled and red to enabled.

Alarm urgency level

The urgency levels in the ALARMmanager application are customizable and you can configure as many as you want.

To manage the alarm levels access **ALARMmanager** → **Alarm urgency level** menu.

Here you have a list of pre-configured levels. You can edit levels or add new ones.

Changing the urgency level priority

To change an urgency level priority, select the desired level and click the UP or DOWN arrows located on the upper left corner.

Adding a new urgency level

To add a new urgency level, click the New and fill the form.

Table 9.5. ALARM urgency level form

Field	Description
Label	A label for the urgency level. This label is displayed on a column at the ALARMmanager console.
Background color	Background color that will be displayed in the ALARMmanager console.
Text color	Text color that will be displayed in the ALARMmanager console.
Beep	Enable sound warning for this alarm. The sound warning will be played by the Java ALARMmanger console if this function is also enable at the console. To enable it, access **ALARMmanager** → **Console** → **ALARMmanager button** → **Tools**
Alarms	Select the alarms that will receive this priority.

Field	Description
Service alarms	Select the service alarms that will receive this priority.

Alarms

Alarms are based on traffic measured from objects configured in the system. There are two types of alarm: Default and History.

To configure either alarm type, select **ALARMmanager** → **Alarms**, click the **New** button and fill out the form.

You can create an alarm for every type of object you deserve:

- Device
- Interface
- Interface Group
- Subnet
- Subnet Group
- Applications
- Applications Group
- Protocols
- Autonomous Systems
- Autonomous Systems Group
- ToS
- ToS Group
- Tag

Default alarm configuration

This type of alarm is used for imediate traffic analysis, when there are known conditions for which it is possible to define a formula. Use this alarm to keep control over boundary conditions that need treatment when detected.

Table 9.6. Default alarm form

Field	Description
Name	Descriptive text for the alarm. Ex.: high traffic, no HTTP traffic.
Alarm type	Choose Default.
Formula	Refer to Default alarms formula section.
Varbind	A free text field that can be used to recognize the alarms that are forwarded as traps.

Field	Description
Mail	Refer to Actions section.
Mobile	Refer to Actions section.
Trap	Refer to Actions section.
Mail delay	Refer to Actions section.
Mobile delay	Refer to Actions section.
Trap delay	Refer to Actions section.
Disable trap for suppressed alarms	If the option **No** is selected, the trap will be sent and the suppressed condition will be indicated in the trap. The **Yes** option will prevent the trap from being sent.
Disable sms for suppressed alarms	If the option **No** is selected, the sms will be sent and the suppressed condition will be indicated in the sms. The **Yes** option will prevent the sms from being sent.
Disable mail for suppressed alarms	If the option **No** is selected, the email will be sent and the suppressed condition will be indicated in the email. The **Yes** option will prevent the email from being sent.
Consecutive occurrences to activate	Choose the number of consecutive ocurrences of the alarm formula that should trigger the alarm. Not used by Trap alarms.
Consecutive non-occurrences to deactivate	Choose the number of consecutive non-ocurrences of the alarm formula that should disarm the alarm. Not used by Trap alarms.
Urgency level	Select an alarm urgency level for the alarm.
Alarm profiles	Select the alarm profiles this alarm should belong to.

Default alarms formula

TRAFip measures and divides traffic in three different ways: bps, packets and flows. Each of these is used as metric in an alarm formula. These metrics can be absolute or they can belong to a traffic profile. This way, we can reference metrics in an alarm formula through the following syntax:

1. **Absolute:** "Domain name".self.<metric>
2. **Traffic profile:** "Domain name".self.<profile type>[<"profile name">.<"profile item name">].<metric>

The metrics above can be called **curves**.

Analysis types can be Matrix, Distribution and Content, represented by **MTX**, **DST** and **CNT**, respectively.

Metrics can be represented according to the following table:

Table 9.7. Metrics representation

Metric	Syntax
Source bps (bits/s)	**bytAb**
Destination bps (bits/s)	**bytBa**

Metric	Syntax
Source packets	**pktAb**
Destination packets	**pktBa**
Source flows	**flwAb**
Destination flows	**flwBa**
Object limit	**limit** (Check the note below)

Important

The metric **limit** refers to the limit of the object associated to the alarm and, if there is no limit (device), so it will be ignored. Using it, you do not need to specify the domain. Check the following example: (self.limit) > 0

You should construct the formula using the following rules:

- Use round brackets "()" for operator precedence.
- Use the AND and OR logical operators.
- Use the ==,!=,<,>,<=,>= comparison operators.
- Use the *,-,+ and / symbols to perform these operations.

Take the examples below:

1. **Absolute:** ("Default".self.bytAb) > 0
2. **Traffic profile:** ("Default".self.CNT["Applications"."ssh"].bytAb) > 0

Behavior change alarm configuration (History Alarms)

This type of alarm is usually configured for when you can not define boundaries explicitly, but still want to be aware of changes in the typical object behavior.

Typically, this type of alarm is used for objects that show a gradual evolution over time (an increasing use of bandwith, for instance). In these cases defining static boundaries may lead to an unnecessary alarm trigger. To solve this, you can configure the system to define, in a daily basis, a standard behavior line for the object you wish to monitor - this line represents the expected future object behavior.

The alarm will be triggered by comparing both, the expected and the collected metric, taking a user-defined tolerance in consideration. The expected value for the curve configured in the alarm is calculated considering a time period defined by you.

Table 9.8. Behavior change alarm form

Field	Description
Name	Descriptive text for the alarm. Ex.: high traffic, no HTTP traffic.
Alarm type	Choose **History**.
Varbind	A free text field that can be used to recognize the alarms that are forwarded as traps.
Activation time formula	Refer to Activation alarm formulas section.
Curve	Refer to Behavior change alarms curves section.

Field	Description
Minimum history (days)	Minimum amount of days necessary to fill the analysis period.
Maximum history (days)	Maximum amount of days allowed to fill the analysis period.
Number of consecutive violations (days)	Refer to Number of consecutive violations section.
Tolerance factor	This factor is measured in amount of standard deviation and it is used to compare the expected value with the actual value. Refer to Tolerance factor.
Alarm period (minutes)	Refer to Alarm period section.
Mail	Refer to Actions section.
Mobile	Refer to Actions section.
Trap	Refer to Actions section.
Email delay	Refer to Actions section.
Mobile delay	Refer to Actions section.
Trap delay	Refer to Actions section.
Disable trap for suppressed alarms	If the option "No" is selected, the trap will be sent and the suppressed condition will be indicated in the trap. The "Yes" option will prevent the trap from being sent.
Disable sms for suppressed alarms	If the option "No" is selected, the sms will be sent and the suppressed condition will be indicated in the sms. The "Yes" option will prevent the sms from being sent.
Disable mail for suppressed alarms	If the option "No" is selected, the email will be sent and the suppressed condition will be indicated in the email. The "Yes" option will prevent the email from being sent.
Consecutive occurrences to activate	Choose the number of consecutive ocurrences of the alarm formula that should trigger the alarm.
Consecutive non-occurrences to deactivate	Choose the number of consecutive non-ocurrences of the alarm formula that should disarm the alarm.
Urgency level	Select an alarm urgency level for the alarm.
Alarm profile	Select the alarm profiles this alarm should belong to.

History alarms formula

This field is used only for history alarms. It defines when an alarm occurrence should be generated.

The variables used are weekday and time. There are two other variables that can be used: **everyday**, in order to trigger the alarm every day of the week and **everytime**, in order to trigger the alarm every time of the day.

If you wish to define when an alarm occurrence should be generated you can use the variables weekday and time with the operators defined. The values for weekday should be between 1 (sunday) and 7 (saturday). For the variable time, you should use HH:MM.

Example:

```
weekday > 1  and weekday < 7
```

This alarm will be triggered if the weekday is between sunday and saturday.

History alarms curves

TRAFip measures and divides traffic in three different ways: bps, packets and flows. Each of these is used as metric in a behavior change alarm curve. These metrics can be absolute or can belong to a traffic profile. This way, we can reference metrics in a behavior change alarm curve through the following syntax:

1. **Absolute:** "Domain name".self.<metric>

2. **Traffic profile:** "Domain name".self.<profile type>[<"profile name">.<"profile item name">].<metric>

Profile types can be Matrix, Distribution and Content, represented by **MTX**, **DST** and **CNT**, respectively.

Metrics can be represented according to the following table:

Table 9.9. Metrics representation

Metric	Syntax
Source bps (bits/s)	**bytAb**
Destination bps (bits/s)	**bytBa**
Source packets	**pktAb**
Destination packets	**pktBa**
Source flows	**flwAb**
Destination flows	**flwBa**

Number of consecutive violations

The violated samples will only be considered if they happen consecutively and the number of violations is above the specified parameter, otherwise they will be discarded in the behavior computation.

For example, suppose you have a behavior change alarm for an interface traffic and at some point the expected traffic was 500MB +- 300MB and the detected traffic was 3GB. This sample will not be used in the behavior computation and the expected traffic for the next day will still be 500MB. This sample will only be used if there are N violated samples consecutively, which characterizes a new behavior.

Tolerance factor

TRAFip will perform the following calculation to determine if the observed value represents a behavior change:

```
IF  (AV < (EV - (N * SD)) OR AV > (EV + (N * SD)))
THEN trigger the behavior change alarm.
```

```
Where
N is the tolerance factor
SD is the standard deviation for the curve
AV is the current half hour average value
EV is the current half hour expected average value
```

Alarm period

TRAFip will display a sample every 30 minutes or every 5 minutes.

When the alarm period is set as 5 minutes, the system will show the average value for each 5 minutes and compare with the expected value, but it won't save if there is a behavior change.

When the alarm period is set as 30 minutes, the system will show the average value for each half hour and determine if the observed value represents a behavior change.

Actions

Each time the TRAFip system processes a 5 minute traffic, all alarm formulas are evaluated and if they return true, occurrences are generated. The alarm will fire for an alarm condition only if the number of consecutive occurrences threshold is surpassed.

When you mark an action for an alarm, you have to fill three fields:

Action fields

Consecutive ocurrences to activate	This represents the number of consecutive times a threshold is crossed.
Consecutive non-ocurrences to deactivate	This represents the number of consecutive times a threshold is not crossed.
Urgency level	Define the right alarm urgency level.

Action types

Mail	Email will be sent to users. The SMTP server should be configured and also each user email at the user configuration form. The email will be sent after the number of seconds defined in the field **Mail delay**, starting from the activation time.
Mobile(SMS)	Shorter messages than the ones sent for emails will be sent. This alarm can be sent to an email to SMS gateway if the user SMS field is configured in the following format: 88888888@operator.com. If the SMS is a phone number, the SMPP or http protocol can also be used to send the message. To do that, you need to configure the following item: **System** → **Parameters** → **SMS server** .
Mobile(Telegram)	A message will be sent to a Telegram chat by a bot. To configure this feature, you must create a bot in Telegram, to do it, once you are on Telegram, start a conversation with the user @BotFather. Choose the option /newbot and follow the instructions to finish the bot creation. At the end write down the telegram bot token. Associate the bot to a chat where the messages will be sent. Access

	the user profile form, fill the "Telegram bot token" field and click Validate. If everything goes fine, the "Telegram chat ID" field will be automatically filled. The message will be sent after the number of seconds defined in the field **Mobile delay**, starting from the activation time.
Trap	A trap will be sent for each alarm. The trap should be interpreted using the TELCOMANAGER-ALARMMANAGER-MIB.my MIB, which is available at the MIB list. You should also configure the server to send the traps at **System → Parameters → SNMP → SNMP trap** . The email will be sent after the number of seconds defined in the field **Trap delay**, starting from the activation time.

Alarm suppression management

At this section you will learn how to manage all the alarm/object tuples that your user has access to.

To suppress, follow the procedure below:

1. Go to **ALARMmanager → Alarms** tab and click the Suppressed alarms button.
2. Fill the filter fields at this form to select the desired alarms/objects desired and click the Filter button.
3. Select the alarms/objects on the list
4. Fill the Suppression reason text field, if desired.
5. Click the Save button to suppress the alarms/objects selected.

To unsuppress the alarms, follow the same procedure, but deselect the desired alarms/objects.

Important

Notice that if the alarm is already suppressed, it won't be suppressed again and the same happens for the unsuppression action.

Important

In Mapview, check the option "Consider suppressed" to show their alarm colors on the map. If a suppressed alarm is inactive for a moment and then it becames active again, it is marked as suppressed.

Alarm profile

Profiles are used to tie together alarms and monitored objects.

To configure an alarm profile, select **ALARMmanager → Alarm profile**, click the **New** button and fill out the form.

Table 9.10. Alarm profile form

Field	Description
Name	Define a name for the alarm profile.
Alarm	Select the desired alarms for this profile.

Field	Description
Object selection box	Firstly, select the object type and the available objects will be shown. Then, select the desired objects for this profile.

Service Alarms

Introduction

The Service Alarms feature allows to join alarms from differents objects in a single formula. Now Trafip can alarm under more sophisticated conditions.

You'll be able to create for example the following alarms:

- An alarm that is active when a WAN link has a high latency and also has a low traffic.
- An alarm to tell you when either the primary and backup links of a location will fail.

Formula

In the formulas you can use the OR,AND,NOT and XOR logical operators to build more complex formulas.

Console

Introduction

The ALARMmanager application works integrated to the systems and is capable of generating alarms based on formulas.

It also has the following features:

- HTML5 graphical interface.
- Alarm forwarding through email, mobile and traps.
- Graphical interface to create custom alarms and formulas.
- Alarms can trigger sounds.
- Alarm profiles to ease alarm association to managed objects.
- Alarm acknowledgment and comments.
- Alarm suppression to avoid emails, mobile messages and traps for repeated alarms.

Console operation

To access the operational alarm console, go to **ALARMmanager → Console**.

Authentication

A user must be authenticated to access ALARMmanager.

Console

The ALARMmanager console will display all the alarms that are active and also the inactive alarms that have not yet been inactive for the ALARMmanager storage period parameter. You will be able to visualize only the alarms that you have permissions to see and for the objects that you are allowed to visualize.

You can configure the columns at **System → Users → Alarm console** .

The console has the following columns:

Table 9.11. ALARMmanager console

Column	Description
START TIME	The time of the first occurrence.
END TIME	The time of the last occurrence. Displays ACTIVE if the alarm has not ended.
USER	User that acknowledged the alarm.
TYPE	Object type, can be device of mapped object.
OBJECT	Object name.
DESCRIPTION	If the object is an interface, displays its ifAlias.
PATH	Shows the first path for the object in the SLAview groups.
STATE	Alarm state, can be active or inactive.
ALARM	Alarm name.
LEVEL	The level for the alarm defined at the level configuration.
TRAP	Yes if it was generated by a trap and no otherwise.
COMMENTS	Comments by the operator. To insert a comment, click two times in that cell.

Alarm Acknowledgement

Once an alarm is acknowledged, the alarm line shows the username that performed the operation and this information can also be viewed at the consolidated alarm report. After acknowledging an alarm, you are able to insert comments for the alarm.

To acknowledge an alarm, right click the alarm to be acknowledged and then select the Acknowledge option on the menu. The alarm is then displayed at the acknowledged tab for all operators.

To acknowledge multiple alarms at once, select then with the left mouse button and then right click on the list to display the menu.

The alarm can be released from the operator only by an administrator user. To do it, the administrator should select the acknowledged alarm at the list and select the Unacknowledge alarm option from the menu.

Alarm Suppression

The alarm suppression mechanism allows you to suppress any alarm/object tuple, providing that the alarm is already configured for that object. The suppression will either disable emails, short messages and traps

for that alarm/object or indicate this condition at the emails, short messages and traps. You can set the desired behavior by setting this field at alarm configuration.

To suppress an alarm, follow the procedure below:

1. Select the desired alarms with the left mouse button. To choose more than one alarm, hold CTRL key and select the alarms with left mouse button.
2. Click with the right mouse button to show the popup menu. Click on Suppress alarms option on the popup menu.
3. Fill the suppression reason text box. You can also leave it blank.
4. Click on Confirm button.

You can check the logs for the suppression operations performed by the users at the suppressed alarms report

You can manage the alarm/object suppresssion list globally at **ALARMmanager** → **Alarms** → **Suppressed alarms** .

Alarm Comments

To insert comments for an alarm you first need to acknowledge it.

To insert a comment, follow the procedure below:

1. Click the Acknowledged alarm tab
2. Double click at the COMMENTS column for the alarm.
3. Fill the text box at the Alarm Comments window and click the Confirm button.

Enabling sound for an alarm

The sound alarm will function if there is an active, not acknowledged, critical or major alarm in the ALARMmanager console.

Select **ALARMmanager** → **Console** → **Enable sound warning** option.

Alarm synchronization

The ALARMmanager applet synchronizes its alarms with the system database every 2 minutes. This synchronization can be triggered immediately at **ALARMmanager** → **Console** → **Synchronize Alarms** menu.

Deleting alarms

ALARMmanager deletes automatically the alarms that have finished, but you will be able to visualize then at the console until the maximum inactive alarm storage time has passed. To configure that parameter go to **System** → **Parameters** → **ALARMmanager** menu.

The operator can delete the alarms at any time if they are in the inactive state by selecting the alarms with the right mouse button and clicking the Delete option on the menu.

Opening graphs

Select an alarm line and click the Open graphs button to open the objects graphs.

Alarm filter

This filter can be triggered from any object at any map. It will filter the object's alarms and also from the objects related to it hierarchycally.

Chapter 10. License enabled features

Redundancy

The redundant solution enables you to deploy two **identical** appliances working on HOT-STANDBY mode.

Important

This functionality will only work if both appliances have the same version.

Tip

It's recommended that the appliances have the same hardware configuration. In case it's different, the system will display a warning.

Concepts

- When this feature is enabled, the system works with two identical machines in HOT-STANDBY performing data synchronization and watching each other states at all times.
- A communication protocol runs between the two servers and if a failure is detected in one of the servers, the other will act as the ACTIVE server - if it is not already - and the tmTSRedundancyStateChangeTrap trap will be sent. This trap is documented at TELCOMANAGER-TELCOSYSTEM-MIB mib.
- Both appliances share one IP address, that is used to send flows from the routers. This IP address is active only on the ACTIVE server and when they swith states, the MAC address of that interface will also migrate to the new ACTIVE server.

Enabling the redundancy

1. Using two identical Telcomanager appliances with the redundancy license option enabled, connect them back-to-back using the same interface at each appliance and configure a non-valid IP network between those interface using the CLI (command line interface) on each appliance.
2. At the CLI, configure the IP address that will be shared between the two servers only at the ACTIVE server.
3. Go to **System** → **Parameters** → **Redundancy** menu and fill the form on both appliances.
4. Wait around 20 minutes and verify the state of each server at **System** → **Diagnostics** → **Network information** .

Distributed architecture

Concepts

The distributed architecture should be used to scale in terms of the system capacity to collect ip flows and SNMP data and to process the raw data, since those tasks are delegated to collector appliances.

Prerequisites

- All machines involved must have SNMP access to all devices to be monitored.

- The ip flows should be exported to the collector appliances.
- There should be enough bandwidth to transfer the summarization files between collector appliances and the central appliance. Keep in mind that one collector requires around 64 Kbps of bandwidth to monitor 1000 interfaces with 10 summarization variables in each interface.
- TCP ports 22 and 3306 must be available between collector and central appliances. Port 22 is used to transfer files in the SSH protocol and 3306 is used to issue database queries from collector to central appliance.

Deployment

1. At the central appliance, go to **System** → **Parameters** → **Distributed architecture** and fill the form accordingly.
2. At the collector appliances, go to **System** → **Parameters** → **Distributed architecture** and fill the form accordingly.
3. At the central appliance, go to **Configuration** → **Collectors** and fill the form accordingly.
4. Wait around 20 minutes and go to **Configuration** → **Collectors** menu to check if the collectors are listed in the **ON** status.