TELCO MANAGER

TRAF$_{ip}$

TECHNICAL DESCRIPTION

Telcomanager is a company specialized in the development of network management tools.

Telcomanager's products are distinguished by the technology used, their friendly features, and especially by their efficiency. Therefore, they reached success in companies representing various market segments, such as telecommunication operators, retail stores, banks, logistic companies, basic industries, content providers, among many others.

Whenever a network is an important part of everyday life, **Telcomanager**'s products will make the difference.

There is no doubt that the network environment is increasingly complex, and that its management is a big challenge. In this scenario, to know what is going through that important infrastructure is a critical point for any network administrator.

TRAFip is a powerful collection and characterization of IP network traffic tool, which comes to solve this problem definitively.

Through data collection, via NetFlow (or equivalent) protocol, TRAFip provides a complete view of its network traffic. It allows the identification of each package and the association to users, applications, servers, workstations, protocols, or several other criteria of your choice.

With the information provided by TRAFip you get answers to perform the correct problem diagnosis that may be affecting your network, besides understanding and clarifying the use each area of the company makes of the network.

Why use it?

Traffic unjustifiably high

TRAFip can easily identify which user and application are generating a specific traffic in your network, also pointing the site and the server used.

Applications not approved

With the TRAFip it is possible to verify if there is any application that has not been approved generating traffic in the network.

Service classes configured correctly

To know if only the applications planned are using a specific type of service is essential to any network manager. With TRAFip it is possible to identify all applications that are using the service classes configured in the network.

Locations that consume more network resources

TRAFip allows viewing which locations, regions, or departments demand more network or datacenter resources. This information is essential when one wants to make some kind of apportionment of cost.

Applications that consume more network resources

TRAFip can view which applications demand more network resources. It can be extremely important for planning of service changes to “Cloud Computing”, for example.

Appliance Solution

TRAFip is an appliance, with hardware and software perfectly integrated. It is a reliable and robust solution, with installation and maintenance low cost.

There is no need to install and optimize the operational system, to install software, viruses risk, lack of memory, database installation, and even less to worry with the maintenance of all those components.

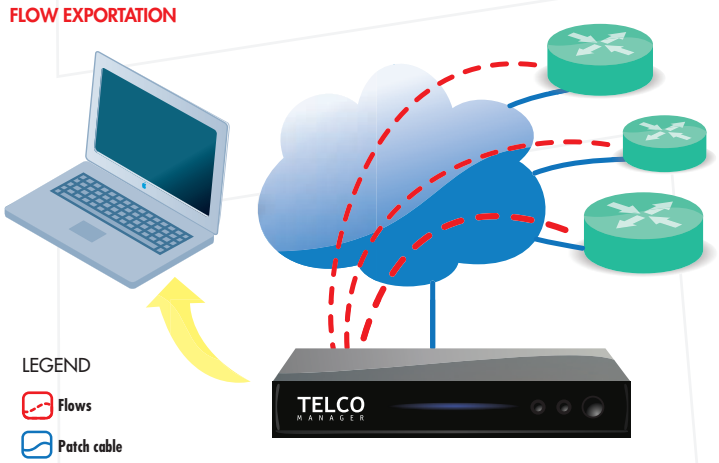
Collection Mechanism

In order to perform its work, TRAFip needs to gather information on the traffic. The most effective way to do it so is by using a technology based on flow exportation.

This technology is available in most level 3 platforms, and in many level 2 platforms present in the market, with a name variation according to the manufacturer (Cisco NetFlow, Juniper JFlow, Huawei Netstream, etc).

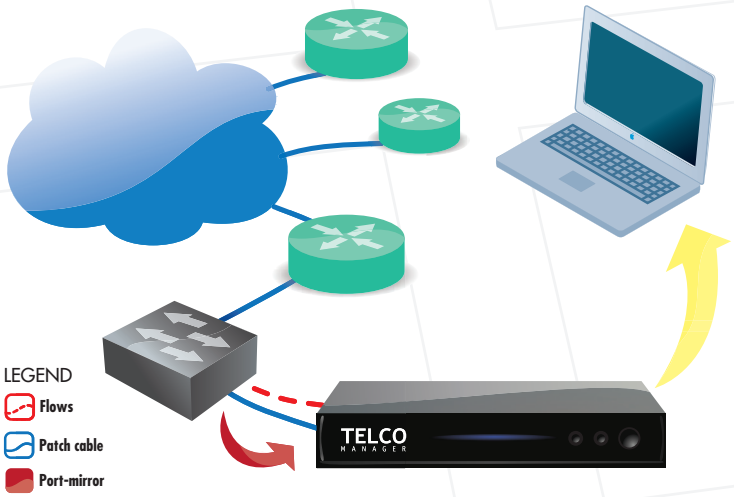
Using the flow exportation technology, information regarding traffic is passed to TRAFip, that will analyze it. The result of this analysis is a classification of this traffic by several parameters such as, e.g.: traffic source, traffic destination, application in use, AS of origin and destination, and many others.

Once the traffic is identified, it becomes easy to know how, when, and who is consuming the bandwidth your network.



Even when there is no available flow technology, TRAFip, through a port-mirror switch or even through a HUB port is capable of performing its analysis. In this case, the appliance must be connected directly in a point of the network where it can have direct access to the traffic to be analyzed.

PORT - MIRROR

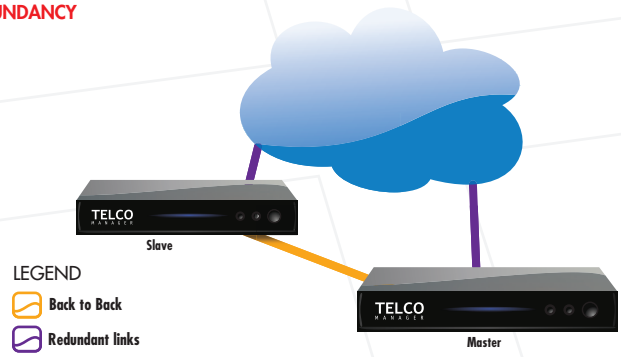


Redundancy

When the monitoring is considered of critical mission and cannot be interrupted, Telcomanager offers an option to activate two appliances in redundancy. In this form of operation, both devices remain synchronized both in their settings and in relation to the collected data and performed analysis.

Telcomanager's redundancy operates under a hot-standby architecture, without the necessity of human intervention. When one of the equipment stops operating, the other takes over all functions automatically.

REDUNDANCY



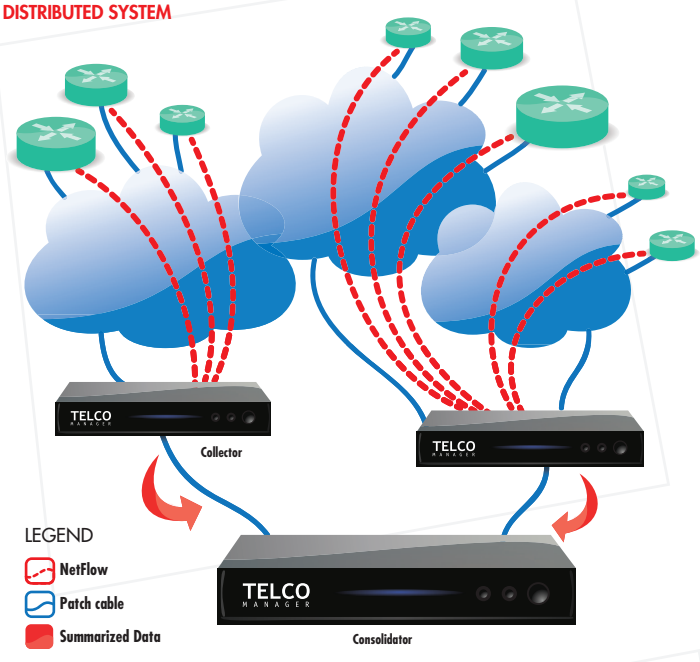
Scalable Architecture

TRAFip can be configured to work with different network sizes. Telcomanager has appliances with the capacity to monitor networks with more than 1000 devices, as well as appliances of small capacity, with effective cost, focused on small networks.

By using a collection cluster and traffic processors that send the collected and treated information to a central consolidator it is possible to expand the installation capacity to, virtually, any network size. Currently, there are cases in operation of network with more than 10,000 devices being monitored by a platform composed of less than 10 appliances, including appliances specific for redundancy.

Telcomanager's collectors are not simple collectors and information conveyors. They perform the processing of much of these data, so that the addition of new collectors won't expand only the collection capacity, but also the general performance of the system.

DISTRIBUTED SYSTEM



Safety, Authentication and Authorization

TRAFip uses a classic model of user/password for the access control. This system may use passwords stored on the appliance itself or may be integrated with an external server of Tacacs or Active Directory authentication.

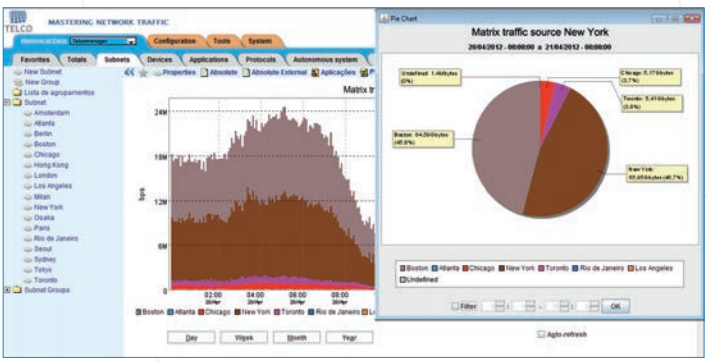
It may be set in the TRAFip the use of the HTTPS protocol to a greater degree of confidentiality and security.

WEB Interface

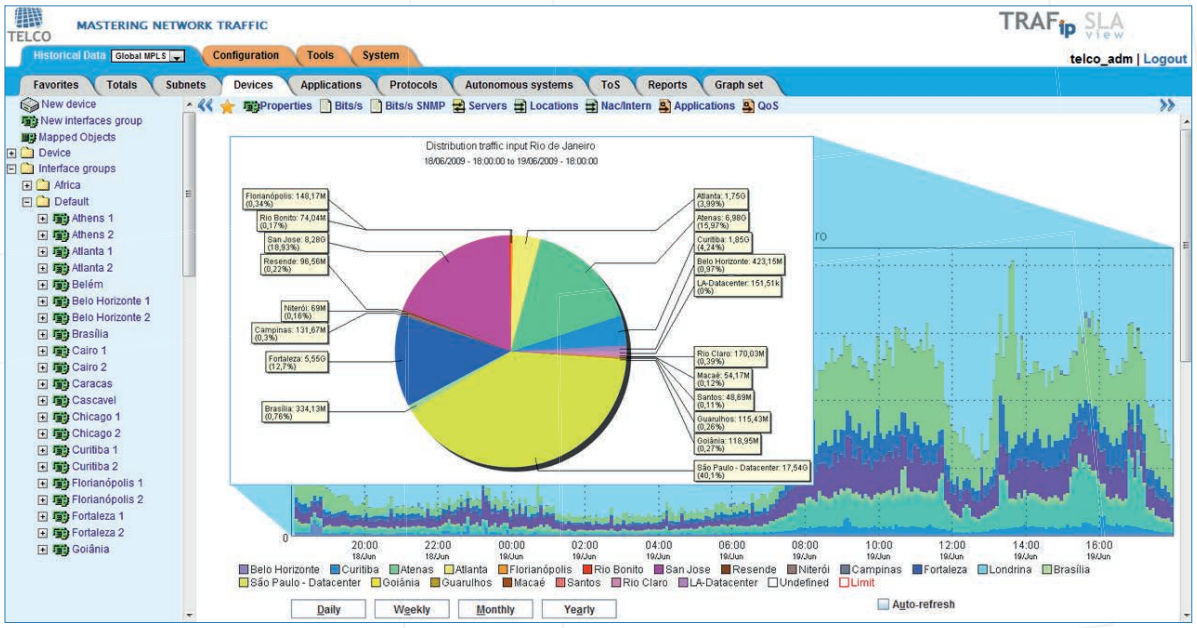
The system features are joined in a WEB interface, which enables quick navigation through the flaps and menus system.

The WEB interface facilitates the requisition and collection of information for the network autonomous management, with the use of resources in HTML, Java Script, and Applet Java to generate graphics and reports.

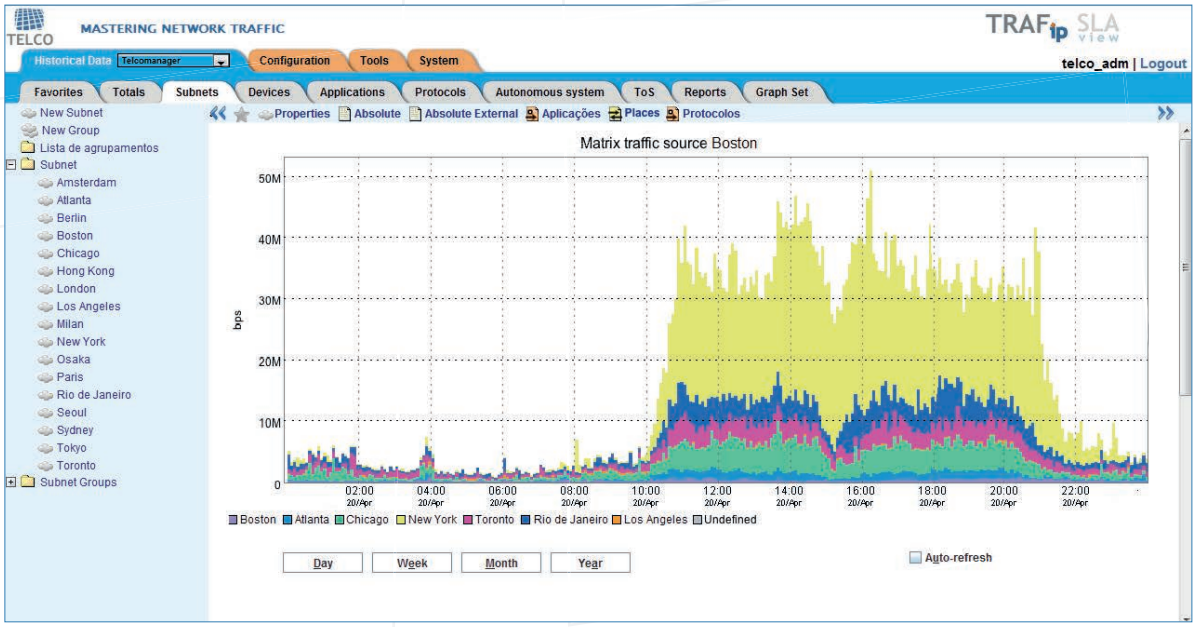
There are several ways to view and analyze the data of the registered devices in the system. In a few clicks, personalized graphics and reports are provided.



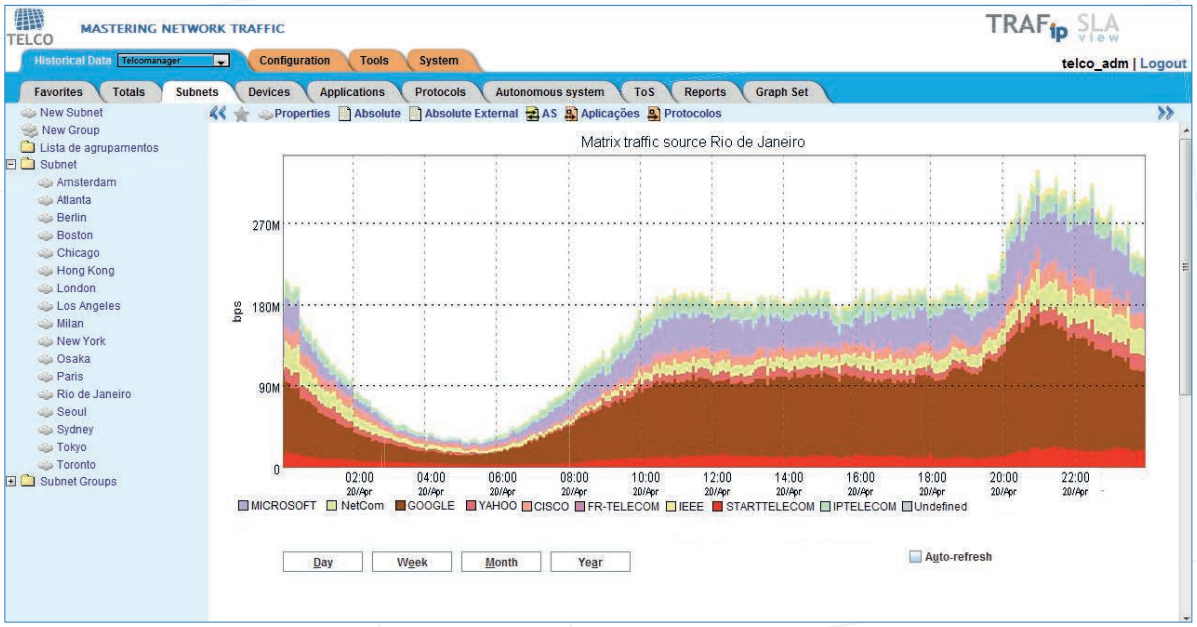
Link x Location



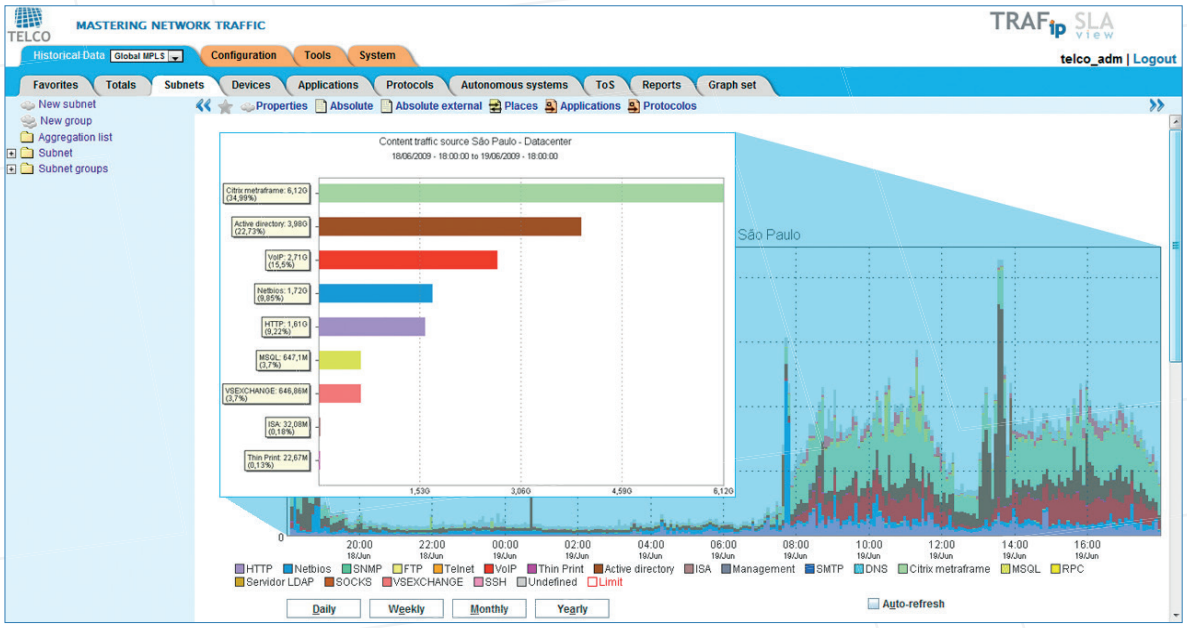
Location x Location



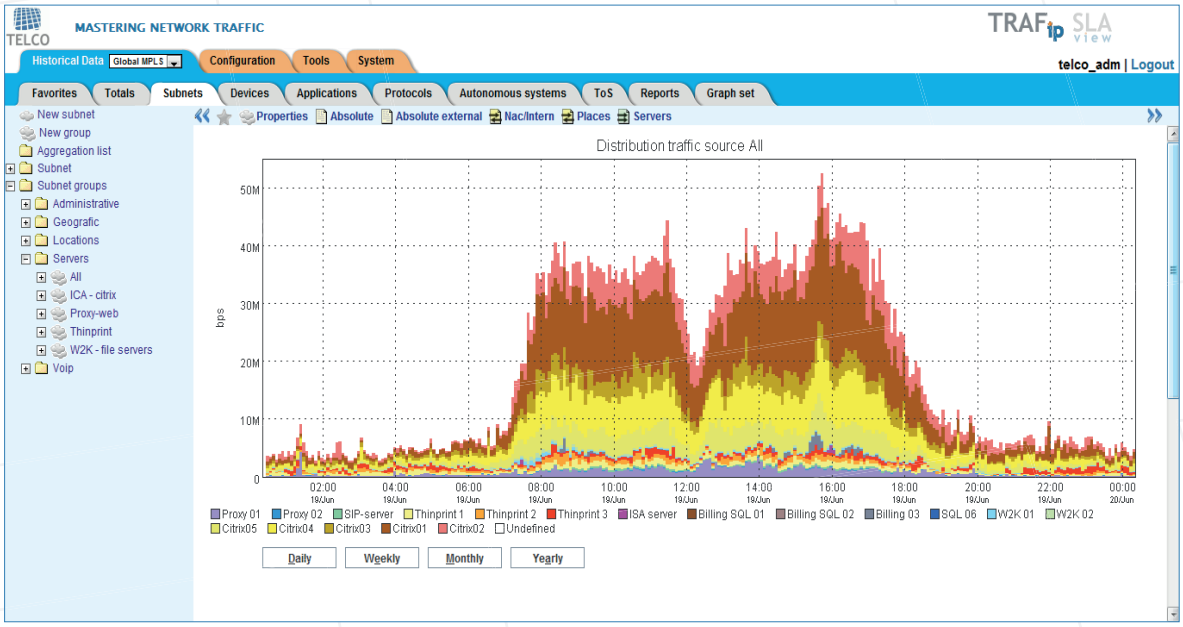
Location x AS



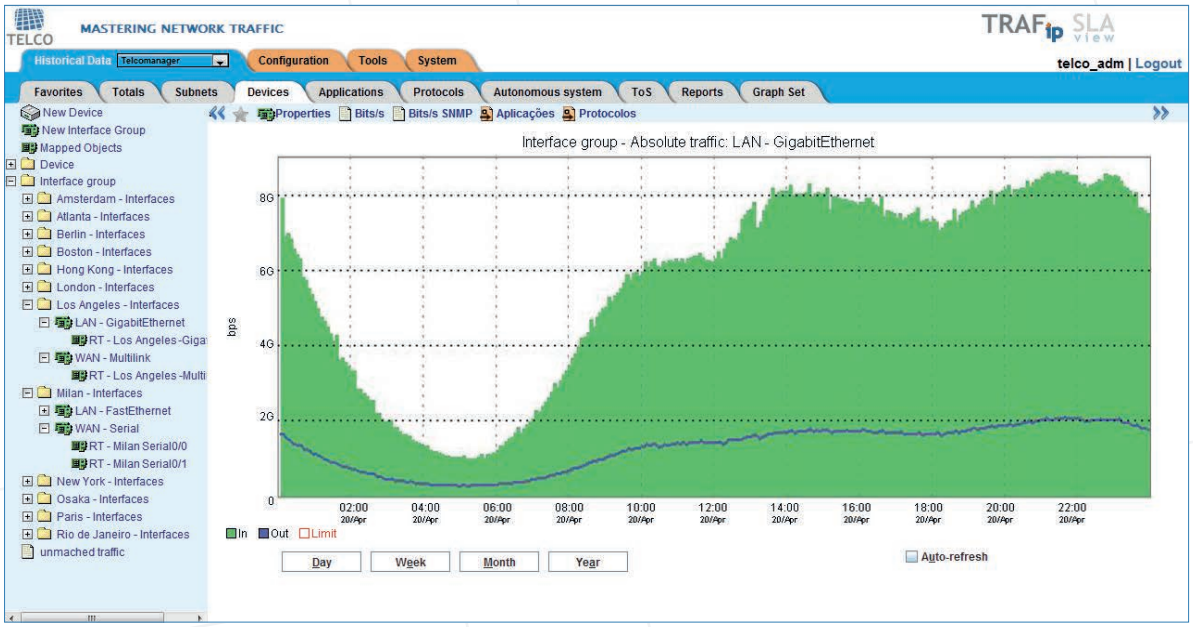
Location x Application



Servers Traffic



Interface Group



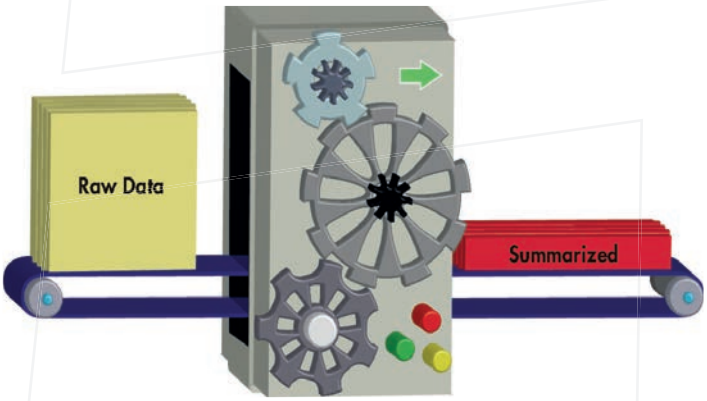
Long Retention Time

TRAFip processes, online, the big volume of received data, aggregates such data, and generates a compact form of storage that was named summarized data.

Due to the great efficiency of the summarizer and of a proprietary method for storing historical sequences, the summarized data occupy much less space than the raw data originally collected. This relationship arrives at the ratio of 1 to 100. With this characteristic it is possible to maintain online long periods of time of summarized data.

Typically, the Telcomanager appliances, in its most basic setting, can retain at least one year of online summarized data for consultation, with frequency, reaching this holding for more than 5 years under ideal conditions of use.

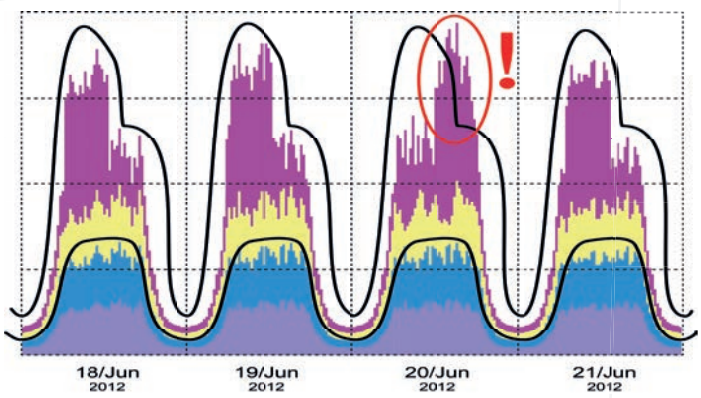
A long retention period does not represent only an increase in the efficiency and comfort for the operator who is now free from having to locate old data for analysis. A long retention period allows more advanced features such as tendency analysis and behavior change analysis, presented later.



Behavior Change

For network traffic that present a wide range of values throughout the day, fixed values are not a proper solution and, frequently, a formula can become quite complex to represent.

For such situations, TRAFip enables the behavior change module, this being a true “help” to the network administrator. This module is capable of analyzing the traffic and to establish adaptable rules that can represent the typical variations of this traffic, generating alarms only when this characteristic behavior is not observed.



Alarms

TRAfip can be set to generate alarms according to criteria established by the network administrator. Those criteria can be defined in a simple way through fixed or percentage limits. More sophisticated criteria can be expressed through formulas, combining several values collected.

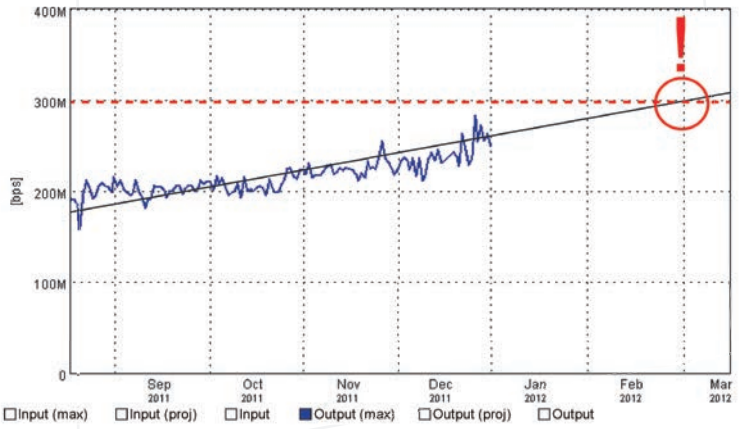
Trend Analysis

Using the data collected and its large capacity of retention, TRAFip can perform previsions on the capacity and limits of its network. For instance, it may warn in advance when a link is going to need upgrade or even which is the estimated traffic to a determined date.

Data networks meet the use dynamic necessities. We know that, unfortunately, it is not enough to scale its capacity a single time and not worry anymore. Networks meet a growing demand of corporate necessities of information traffic, and facing such scenario they are often expanded. And the worst that can happen is the administrator realizing the necessity only when it is already installed and generating problems.

The tendency analysis module was created having in mind the necessities of a network administrator to proactively act in relation to the capacity plan and the network expansion. It helps defining, far ahead, when those expansions will be necessary.

Focus on the expansion strategy or in the partners and new technologies selection, while TRAFip does the hard and repetitive work of calculating and designing data!

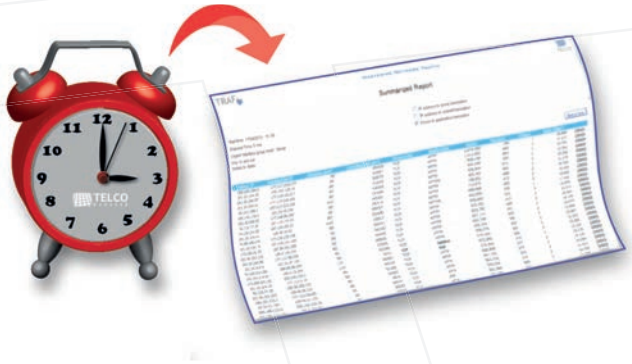


Reports

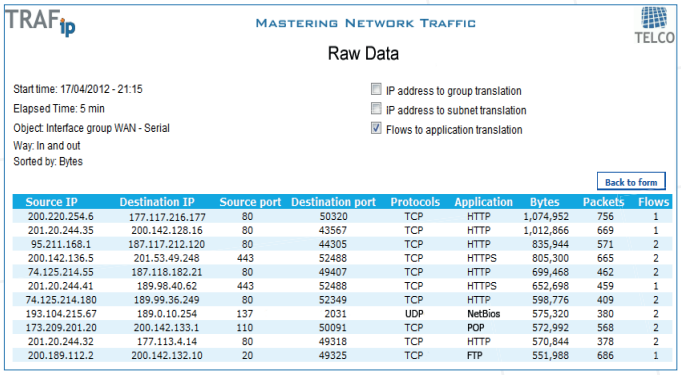
TRAFip allows the generation of several detailed reports, where a rich assembly of information such as source IP address, destination IP address, source port, destination port, among many other information, can be obtained.

The user can customize a report and also schedule a future periodic execution.

TRAFip may generate the HTML, CSV, TSV, and PDF reports.



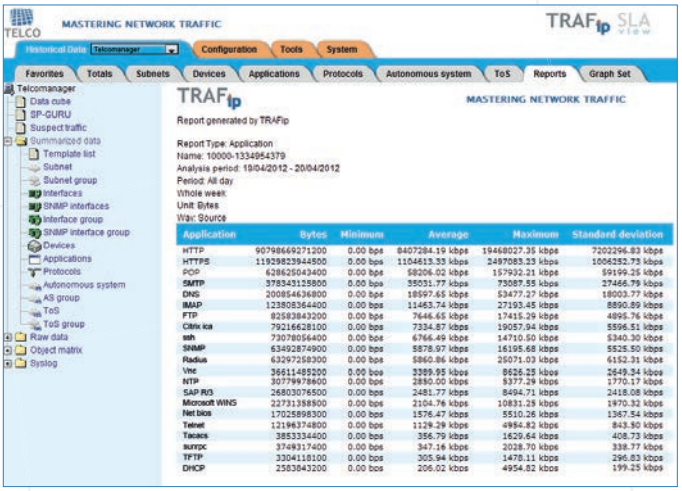
Raw Data



Source IP	Destination IP	Source port	Destination port	Protocols	Application	Bytes	Packets	Flows
200.220.254.6	177.117.216.177	80	50320	TCP	HTTP	1,074,952	756	1
201.20.244.35	200.142.128.16	80	43567	TCP	HTTP	1,012,866	669	1
95.211.168.1	187.117.212.120	80	44305	TCP	HTTP	835,944	571	2
200.142.136.5	201.53.49.248	443	52488	TCP	HTTPS	805,300	665	2
74.125.214.55	187.118.182.21	80	49407	TCP	HTTP	699,468	462	2
201.20.244.41	189.98.40.62	443	52488	TCP	HTTPS	652,698	459	1
74.125.214.180	189.99.36.249	80	52349	TCP	HTTP	598,776	409	2
193.104.215.67	189.0.10.254	137	2031	UDP	NetBios	575,320	380	2
173.209.201.20	200.142.133.1	110	50091	TCP	POP	572,992	568	2
201.20.244.32	177.113.4.14	80	49318	TCP	HTTP	570,844	378	2
200.189.112.2	200.142.132.10	20	49325	TCP	FTP	551,988	686	1

Example of a raw data report. Each line can have several translations, such as: applications, sub-nets, and sub-net groups.

Summarized Data



Application	Bytes	Minimum	Average	Maximum	Standard deviation
HTTP	90798669271200	0.00 bps	8407284.19 kbps	19468027.35 kbps	7202296.83 kbps
HTTPS	11929823944500	0.00 bps	1104613.33 kbps	2497083.33 kbps	1006252.73 kbps
POP	628625043400	0.00 bps	58206.02 kbps	157932.21 kbps	59199.25 kbps
SMTP	378343125800	0.00 bps	35031.77 kbps	75087.55 kbps	27466.79 kbps
DNS	200854636800	0.00 bps	18597.65 kbps	53477.27 kbps	18003.77 kbps
IMAP	123808364400	0.00 bps	11463.74 kbps	27193.45 kbps	8890.89 kbps
FTP	82583843200	0.00 bps	7646.65 kbps	17415.29 kbps	4895.76 kbps
Citrix ica	79216628100	0.00 bps	7334.87 kbps	19057.94 kbps	5596.51 kbps
ssh	73078056400	0.00 bps	6766.49 kbps	14710.50 kbps	5340.30 kbps
SNMP	63492874900	0.00 bps	5878.97 kbps	16195.68 kbps	5525.50 kbps
Radius	63297258300	0.00 bps	5860.86 kbps	25071.03 kbps	6152.31 kbps
Vnc	36611485200	0.00 bps	3389.95 kbps	8626.25 kbps	2649.34 kbps
NTP	30779978600	0.00 bps	2850.00 kbps	5377.29 kbps	1770.17 kbps
SAP R/3	26803076500	0.00 bps	2481.77 kbps	8494.71 kbps	2418.08 kbps
Microsoft WINS	22731388500	0.00 bps	2104.76 kbps	10831.25 kbps	1970.32 kbps
Net bios	17025898300	0.00 bps	1576.47 kbps	5510.26 kbps	1367.54 kbps
Telnet	12196374800	0.00 bps	1129.29 kbps	4964.82 kbps	843.50 kbps
Teams	3853334400	0.00 bps	356.79 kbps	1629.64 kbps	408.73 kbps
sunrpc	3749317400	0.00 bps	347.16 kbps	2028.70 kbps	338.77 kbps
TFTP	3304118100	0.00 bps	305.94 kbps	1478.11 kbps	296.83 kbps
DHCP	2583843200	0.00 bps	206.02 kbps	4954.82 kbps	199.25 kbps

Example of a summarized data report that may be generated by types of objects, interfaces, sub-nets, devices, applications, and so on.

Scheduling Reports

TRAFip allows the scheduling of traffic reports and their automatic sending by e-mail. For this, just save a report template and indicate the time of submission and attendance. Thus, it may be established a process of quality control points.

The scheduling avoids the necessity of an operator's repetitive activity, saving this worker's time and avoiding errors in the reports generation of this quality control point.

QoS Analysis and Audit

TRAFip receives, in each flow, the type of service mark. It allows analyzing how the service classes are being used. It is possible to identify which applications were effectively forwarded to each type, the use of each type' bandwidth, or the use of bandwidth of each application within its own service type.

TRAFip allows a perfect view of how effective is the current QoS configuration and also allows the identification of marking errors and dimension inadequacies of the QoS types.

TRAFip is a powerful ally that allows you to take the most of its network functionalities.

Suspicious Traffic

TRAFip has a specific module for the suspicious traffic analysis. When activated, it performs analysis directly on the collected raw data trying to find traffic patterns that may represent a DDoS, DoS, or also the spread of a virus through the network. Besides those classic traffics, the module can alarm when it detects a traffic excess between two network hosts. The module can be parameterized by the operator in a way to avoid unnecessary alarms and to suit the specific characteristics of the network.

Integration

TRAFip may be integrated in the same appliance with the SLAview. Other information on this product may be found in the technical description of the SLAview.

www.telcomanager.com

phone: +55 21 2203 2222
fax: +55 21 2203 2221
info@telcomanager.com
Presidente Vargas Avenue, 962 - group 1201
20071-002 - Rio de Janeiro - RJ - Brazil