

InSight

Traffic Analyzer

traffic management by



Highlights

- Top Talkers Statistics for Applications and Application Classes
 - Continuous Monitoring of Service Level Agreements
 - Signature-based Layer-7 Application Classification
 - Device and Path Latency Measurements
 - Interactive Performance Graphs
 - User and Subscriber Accounting
 - 10 Gbit/s Passive Monitoring
 - I-Click Reporting

Visibility for your Network

ipoque's InSight network traffic analyzers provide network operators with a powerful tool to gain maximum visibility in today's high-speed multi-service networks.

A rising number of new Internet services offer chances for innovative business models, but also pose a threat to providers unaware of the traffic carried through their network. Besides the commercial challenge to turn a new service such as VoIP into a profitable business, network monitoring is required to discover and resolve performance problems, to maintain network security, and to obey regulatory and legal requirements.

P2P-based file sharing, for instance, generates more traffic than all other applications combined, thus challenging most flat rate providers' tariff models. Furthermore, its massive bandwidth consumption has a permanent adverse effect on the performance of all other applications.

New VoIP services such as Skype are drawing a huge number of new users. For the first time, subscribers are willing to pay for an Internet service on a large scale making it an attractive premium product for Internet service providers. Detailed knowledge about the subscribers' VoIP usage is indispensable to successfully offer such a product.

Future services such as video on demand and Internet TV will further drive the challenge on infrastructure and tariff models. Hence, application- and user-aware network monitoring and analysis has to be an integral part of any successful network management policy.

ipoque offers powerful and flexible network monitoring solutions to fit the requirements of network operators and Internet service providers. The InSight traffic analyzers combine high-speed network monitoring with application-aware subscriber accounting for optimal network visibility.



Architecture

The InSight traffic analyzer is implemented as a client-server solution. The client captures and analyzes the traffic and sends the results to a database server that stores and aggregates the results. The main processing load rests on the client, while the server needs to be capable of handling large amounts of data. Client and server can be integrated into a single computer. This implementation is particularly suitable for deployments with only a few monitors. If multiple links need to be monitored, several clients can capture and analyze data and send them to a single server that hosts the analysis database for all monitors.

Hardware

Network capacities are growing faster than any other IT technology such as processor speed and memory size. Keeping up with this development requires an extremely powerful and scalable hardware platform.

The InSight traffic analyzer is based on a rack-mountable server platform customized to the performance requirements resulting from the monitored link's bandwidth. Standard systems are equipped with a system disk and a RAID disk array to store the analysis data. The disk array's size is chosen to reflect the time resolution of the data (usually 5 minutes), the amount of historical data to be archived and the number of IP addresses to be monitored individually.



Its central component is a special-purpose network measurement card. The cards are available for the following link technologies:

- DS3/E3
- SONET OC3/12, SDH STM-1/4
- SONET OC48, SDH STM-16
- SONET OC192, SDH STM-64
- 10/100Base-T
- 1000Base-T/SX/LX
- 10GBase-SX

The measurement cards support packet capturing at maximum link rate independent from the host CPU. Captured packets are written into a ring buffer inside the main memory, from where they are read by the analysis software. Reading and writing are independent processes, and as long as the analysis process is able to keep up with the link's packet rate, no single packet will be lost. If the CPU becomes overloaded with traffic analysis, the ring buffer fills up and starts to overwrite unprocessed packets in its tail. Those packets are lost. The card's driver detects such packet losses, and they are reported by the analysis software.

An important component of the measurement cards is a highly accurate internal clock to exactly time-stamp packets at their arrival. Two or more cards can be synchronized to each other by using a GPS or CDMA time receiver. Such a configuration allows one-way delay measurements for network packets traveling through a network device or along a path through the Internet.

For instance, two measurement points on either side of an edge router can be used to permanently monitor the router's packet latency and to generate alarms if a threshold is exceeded. This is particularly useful if many real-time services such as VoIP and Internet TV pass this router.

User Interface

The InSight analyzer is administrated via a Web-based graphical user interface. The Web interface is used to configure all analysis functions and to display the analysis results either graphically or text-based in tables.

The following screenshots illustrate the capabilities of the Web interface. The navigation bar on the left consists of three sections: the upper section lists all subnets as defined by the user; the middle section lists all available graph types; the lower section is used to configure the system. Selecting a subnet from the upper section displays all available statistics graphs for it, and selecting a graph type from the middle section displays the corresponding graphs for all subnets.

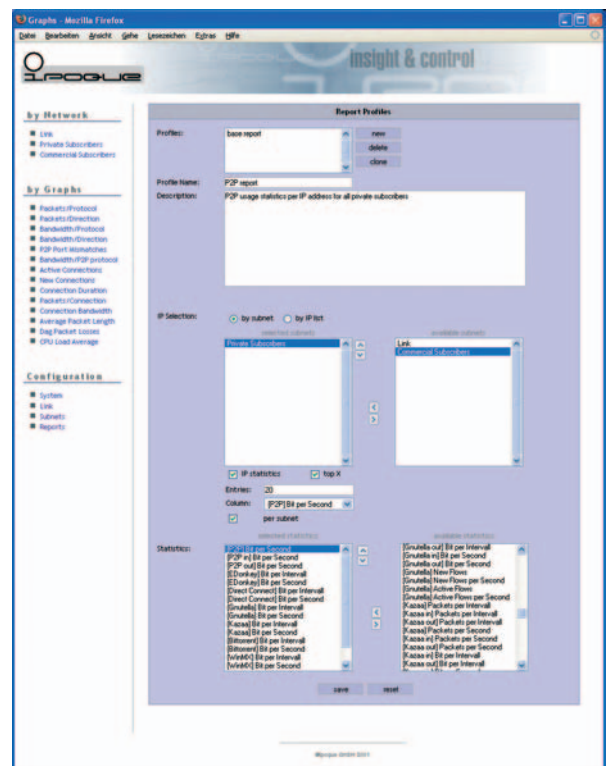
Configuration

The "System" configuration contains the system's IP settings including an NTP server for time synchronization. Depending on the installed network measurement card, various card parameters can be set to match the monitored link's specifications.

The following screenshot shows the "Subnets" dialog, that is used to define the subnets to be monitored. The graphs displayed in the "by Network" and "by Graphs" sections can be selected from a list of available statistics for each subnet and the entire link. Also, their display order can be configured. Individual IP statistics can be selectively enabled for each subnet.



The "Reports" dialog shown in the next screenshot allows to define reports that can be run on the collected data. "IP Selection" determines the IP address scope of the report, which can be the entire link, one or more subnets, or a custom list of IP addresses. By default, aggregated statistics are generated for the selected subnet. Selecting "IP statistics" in "IP Selection" enables full per-IP address statistics generation. Top talker statistics are available by selecting "top X" and providing the number of entries (the "X") and the data source (e.g. P2P bandwidth). Ticking "per subnet" will generate the top talker list for each selected subnet instead of one list for the entire link only.

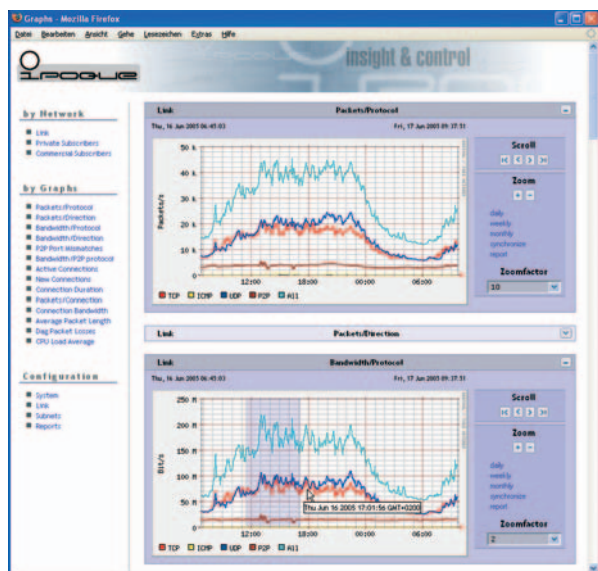


Graph Display

The configured graphs can be displayed either "by Network" – showing each graph type for the selected subnet – or "by Graph" type – showing the selected graph for all defined subnets.

The screenshot below shows the selected graphs for an entire network link. The screenshot shows the packets per protocol and bandwidth per protocol graphs. Each graph has a number of control elements. The

hide/unhide button in the top-right corner can be used to display only selected graphs. The packets/direction graph is currently hidden.



The scroll buttons move the visible window along the time axis. The zoom buttons along with the configurable zoom factor change the visible time interval relative to the middle of the graph. Three predefined shortcuts provide direct access to day, week and month views. In addition to these control elements, the user can select a time interval with the mouse (as depicted in the lower graph of Figure 1) to allow for easy navigation in the graphs. All these operations affect only one graph. By selecting the “synchronize” function, all other graphs will be updated to show the same time interval as the current graph.

Reports

Once an interesting time interval has been determined, the “report” link can be clicked to open a window where a predefined report can be selected for that interval. The report can be generated in HTML format for immediate in-browser presentation, or in CSV (comma-separated values) format for subsequent processing in spreadsheet programs.

Analysis Functions

The InSight traffic analyzer comes pre-configured with a number of statistics. The basic measurement units are:

- bits per second and per report interval
- packets per second and per report interval
- new flows per second and per report interval
- active flows

Counters are maintained for the following traffic classes:

- inbound, outbound
- TCP, UDP, ICMP
- IPv4, IPv6
- layer-7 protocol and protocol class

All applications are classified based on layer-7 protocol signatures. This is particularly important for port hopping protocols with stealth features commonly found in P2P and certain VoIP applications. The following layer-7 protocols are currently implemented:

P2P	VoIP
eDonkey	SIP
DirectConnect	Skype
Gnutella	
KaZaa	IM
BitTorrent	AOL/ICQ
AppleJuice	MSN
SoulSeek	Yahoo
WinMX	IRC
Ares	unencrypted Jabber
MUTE	
Freenet	
XDCC	

This list is subject to ongoing extension. Additional protocols can be easily added on customer request.

If InSight analyzers are installed at different monitoring points with enabled time synchronization, packet latency statistics are available, for instance:

- inbound & outbound delay
- P2P and non-P2P delay
- VoIP and non-VoIP delay

Data Aggregation

By default, the sampling interval for measurement data is 5 minutes, but can be set to any value greater than or equal to 1 second. With IP statistics enabled in a fairly large network, huge amounts of data will be created. Even though the InSight traffic analyzers can be equipped with large disk arrays, storing historical data over extended periods of time will eventually overwhelm the storage capacity. Thus, older data will be gradually aggregated.

The aggregation stages are configurable. For instance, a system could store 5-minute values for one week, 1-hour averages for one month, 6-hour averages for one year and 1-day averages for all older data. This approach allows to store high-resolution data for in-depth analysis of current network events and to retain enough historical data for trend analysis.

Subscriber Accounting

The InSight analyzers support full subscriber accounting for up to 65,536 IP addresses by simply defining one or more subnets and enabling IP statistics for them. It is easily possible to generate top talker lists for certain applications or application classes (e.g. top-100 P2P and VoIP users) in these subnets.

In addition to the subnets, the administrator can supply a list of IP addresses to be monitored separately. Using this function allows, for instance, the temporary observation of selected network nodes, or the permanent monitoring of server machines.

Application Scenarios

The InSight traffic analyzers are deployed both by corporate network operators and Internet service providers. Their comprehensive network monitoring capabilities can replace current NetFlow installations thus relieving routers from statistics data collection. The subscriber statistic feature provides the opportunity to thoroughly monitor every network node.

The following list provides some sample applications for corporate network operators:

- top users by bandwidth usage for protocols or classes of protocols
- how many network users are using a certain application
- how many users are using P2P clients
- average P2P bandwidth utilization
- new connections per network node to detect DoS attacks
- detect illegal services running inside the intranet
- VoIP usage per network node

Possible applications for Internet service providers include:

- top subscribers by bandwidth usage for protocols or classes of protocols
- how many subscribers are using a foreign VoIP service
- most-used online games to provide own servers for these games in future
- top-100 SMTP talkers to locate spammers average P2P bandwidth utilization
- bandwidth trend observation for network capacity planning
- top uploaders

Customization

Every network beyond a certain size is unique and its effective management demands customized solutions. Off-the-shelf products quite often do not cover all individual requirements. ipoque's particular strength is the flexibility when it comes to adapting the InSight traffic analyzers to specific customer requirements.

About ipoque

ipoque, founded in 2005, with headquarter in Leipzig, Germany, specializes in solutions for Internet traffic management. Its comprehensive line of hardware traffic managers provide network operators with effective tools to control undesirable traffic – including peer-to-peer-based file sharing (P2P), instant messaging (IM), Voice over IP (VoIP) and Skype.

A second product line comprises traffic analyzers for collecting and analyzing network data with rates of up to 10 Gbit/s. Comprehensive reports of customizable detail level (overall network, subnets, individual users) are generated in real-time and can be exported in various format for further processing.

Based on its off-the-shelf products, ipoque offers customized implementations of traffic management and analysis solutions.

ipoque GmbH
Karl-Heine-Straße 99
D-04229 Leipzig
Germany

Phone: +49-341-2419607
Fax: +49-341-2419608
Email: info@ipoque.com
www.ipoque.com

