

GenieATM™ 2310

An Advanced Network Traffic Management System to Provide Network Security Reinforcement on Locating Problems Instantly, Powerful Traffic Analysis with Flexibility, and Various Traffic Statistics Reports

Along with the explosive growth of Internet, all the networks are encountering more than ever difficult challenges – unpredictable attacks from network worms and DoS/DDoS, and also fast spreading spam-mails, all those are severely impacting the service quality as well as the overall security of your managed network.

Perhaps, you have already deployed some kinds of network security equipments like firewalls, IDSs, and protocol analyzers for protection. In fact, you also know that even firewalls/IDSs are not ensuring your network 100% free from the zero-day attacks which are actually even burning down your security devices. Furthermore, the fast spreading abnormal traffic and/or DoS/DDoS attacks residing in your network will keep downgrading the network service quality dramatically unless you could react instantly and take solid control on it.

Therefore, except the traditional security devices installed, you do also need one more powerful tool for network security reinforcement.

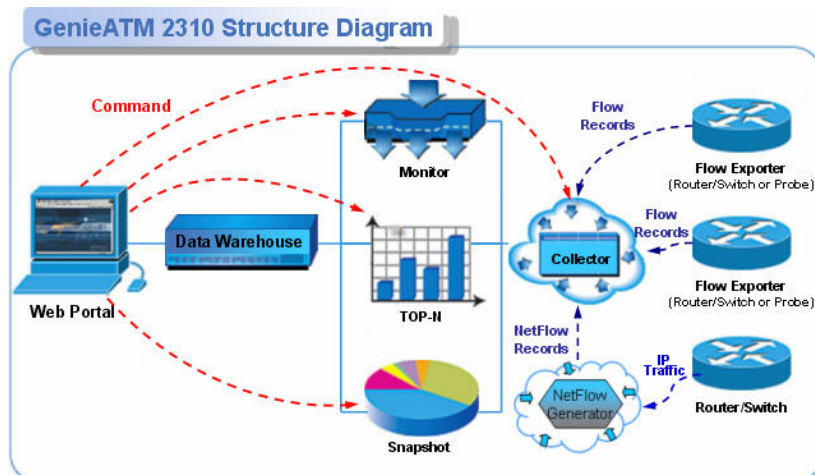
GenieATM 2310 is going to provide you the solution for locating network security problems instantly and better network traffic analysis with network-wide visibility. Through inspecting the collected traffic flow information from core/access routers or backbone switches, it enables the possibility on locating the source/destination of DoS/DDoS attacks,

spam-mails, illegal servers, and also providing user-behaviors, and load balance analysis. With clear visibility on network traffic analysis, both network optimization and expansion works become easier and more efficient

GenieATM 2310 is designed with hardened network appliance architecture, which delivers outstanding performance and ease of deployment. Its friendly operating interface is easy to use. The multilingual GUI support allows you to monitor and analyze your network traffic statistics anytime and anywhere through Web access. It also provides various traffic analysis reporting formats like Standard, Comparison, and Trend reports with selectable time intervals like Daily, Weekly, Monthly, Quarterly, and Yearly.

The embedded database is configured to operate intelligently with self-maintenance capability. The system operation/maintenance cost is remained low by useful system administration functions as well as the support of remote system upgrade.

GenieATM 2310 provides 3 models for users to satisfy all scales of network requirements. Actually, it has been selected and widely deployed as one of the key tools on analyzing network traffic flows in many organizations, such as enterprises, educational campuses, governments, financial services, banking and manufacturers.



Key Features & Benefits

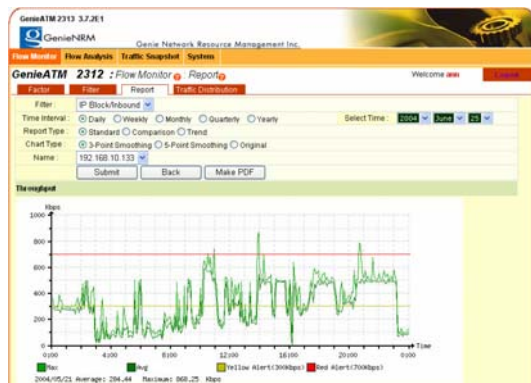
- **Appliance Architecture:** Ease of system set-up and configurations. All modules integrated in one box which could perform all functions independently. No any extra hardware or software is required.
- **Long-term Traffic Monitor:** Network-wide traffic monitor and in-depth analysis are enabled by “rule-based” analysis capability. Except filters figured with various analysis criteria (IP addr., IP blocks, interfaces) to monitor network traffic in longer term, further filter combinations are also available through “And-Or-Not” logic computing.
- **Two-level Threshold Alarm:** Two-level threshold alarms mechanism for real-time display on monitor reports, and could also issue SNMP traps to the Fault Management System of NMS for integration.
- **In-depth Traffic Analysis:** Multi-tiered Top-N ranking reports that being updated at every 5-minute interval and is also available by drag-down functions. The offline analysis on the historical raw data residing in system is also applicable.
- **Instant Traffic Snapshot:** Abnormal traffic, worms, and the source and destination of attacks are easily been identified and located by the unique traffic snapshot function.
- **Web-based Interface:** The system could be accessed from anywhere anytime only with web-client and Internet access. The GUI design would also make the operations friendly to users and quick to learn.
- **Command Line Interface:** In Addition to CLI, the remote Telnet and SSH accesses are also available for operating the system configurations and upgrades securely.
- **Comprehensive Reports:** Various types of the report supported : Line, Bar, and Pie charts ; HTML, PDF, and CSV formats ; Daily, Weekly, Monthly, Quarterly, and Yearly reports ; Standard, Comparison, and Trend reports.
- **Remote Software Upgrade:** The system software upgrade could be easily performed by remote access and/or by replacing the build-in flash card on-site locally.
- **User Account Management:** Four levels of account authority are defined for management of system access, which enables the system suitable for system sharing applications to multi-user environment.
- **Multi-lingual Support:** Per-user language selection for English, Japanese, Traditional Chinese and Simplified Chinese.
- **Flow Record Format:** NetFlow™ V1, V5, V7, and sFlow® flow formats are supported.
- **Built-in Probe:** An alternative by performing packet capture over the Ethernet links to be monitored, either just listening to the links through network taps or connecting to the mirroring/span port on switches.
- **Multiple Exporter Sources:** The system could be configured to collect flow traffic from multiple exporters simultaneously, that makes traffic monitor and analysis applicable to the aggregated network traffic.
- **Ease of Deployment:** The system will work easily in any network with IP connectivity for data collection and management connection, with no impact to user’s existing network environment.
- **Flow Relay:** Forwarding all the received NetFlow/sFlow data to other NetFlow/sFlow collectors.
- **Data Export with ODBC:** Through ODBC links, the DB data of “Traffic Monitor Report” and “Traffic Analysis Report” are available for users to retrieve for further integration with customers’ business support system (BSS).

NetFlow™ is a trademark of Cisco Systems, Inc.
sFlow® is registered as a trademark of InMon Corp.

System Functions

■ Flow Monitor

“Factor” is defined as the basic element for the network targets being analyzed, and then “Filter” is created according to the compound of basic “Factor” for enabling the powerful “rule-based” analysis such as combining factors with “AND”, “OR”, “NOT” logic computing. The system will only retrieve and analyze those NetFlow/ sFlow raw data which have been specified in the “Filter” list, and then store all the conformed statistics data into the embedded database for generating various monitor and analysis reports on-demand.



Besides, two-level threshold alarm indicators are available for real-time traffic monitor, and the system could also be triggered to issue SNMP traps to Network Management Systems for further integration.

Name	Type	Created Date	Created By	Status	Threshold Indicator
R&D Dept.	Multiple	2004-02-05 17:15:11-08	admin	Active	300
Business Dept.	Multiple	2004-02-05 17:17:28-08	admin	Active	300
Marketing Dept.	Multiple	2004-02-05 17:18:15-08	admin	Active	300
MailServer Traffic	Multiple	2004-02-05 17:19:23-08	admin	Active	300
WebServer Input Traffic	Inbound	2004-02-05 17:21:23-08	admin	Active	300
CHG Input Traffic	Inbound	2004-02-05 17:36:44-08	admin	Active	300

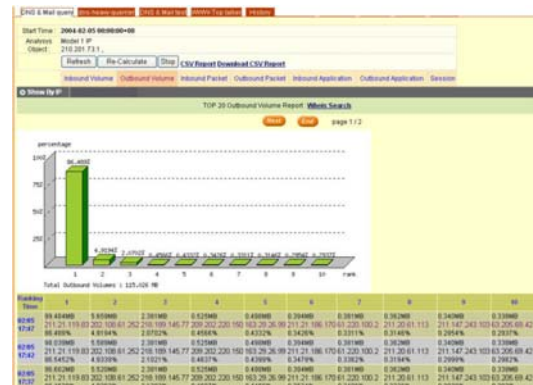
By long-term monitoring onto the entire or some specific network traffic, the system will help users to understand more on the traffic baseline information for better traffic trend analysis. Furthermore, the long-term traffic monitors configured on the specific services, user behaviors, abnormal traffic, and so on are all applicable to users as valuable supporting data.

■ Flow Analysis

Up to 4 or 8 analysis windows, depending on the product model selected, are supported for Top-N ranking analysis. Each analysis window will provide you with one “TOP-N Report” for analyzing either real-time flow data or historical raw data residing in system storage.

The TOP-N report provides you with traffic ranking updated at every 5-minute interval by Traffic Volume, Packet, Application, and Session. The TOP-N report can also be exported for further processing in CSV format.

All Top-N reports will be stored into an embedded database automatically while the analysis windows closed. The directory and storage management functions are making DB maintenance automatically and history records querying more easily.



It's highly recommended to analyze the ranking of all those main traffic within your network periodically; you would have better visibility on the traffic flow directions as well as the application distribution on your network. The system is helping you to understand the important traffic baseline information, and also providing you solid data for network optimization as well as security reinforcement.

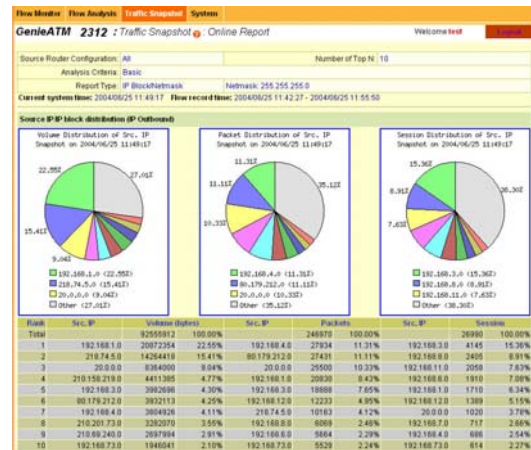
Traffic Snapshot

The unique "Traffic Snapshot" contributes a lot on analyzing the real-time traffic status in specified area; a TOP-N snapshot report is generated instantly with detail information presented in pie-chart as well as table-list data format for timely reference.

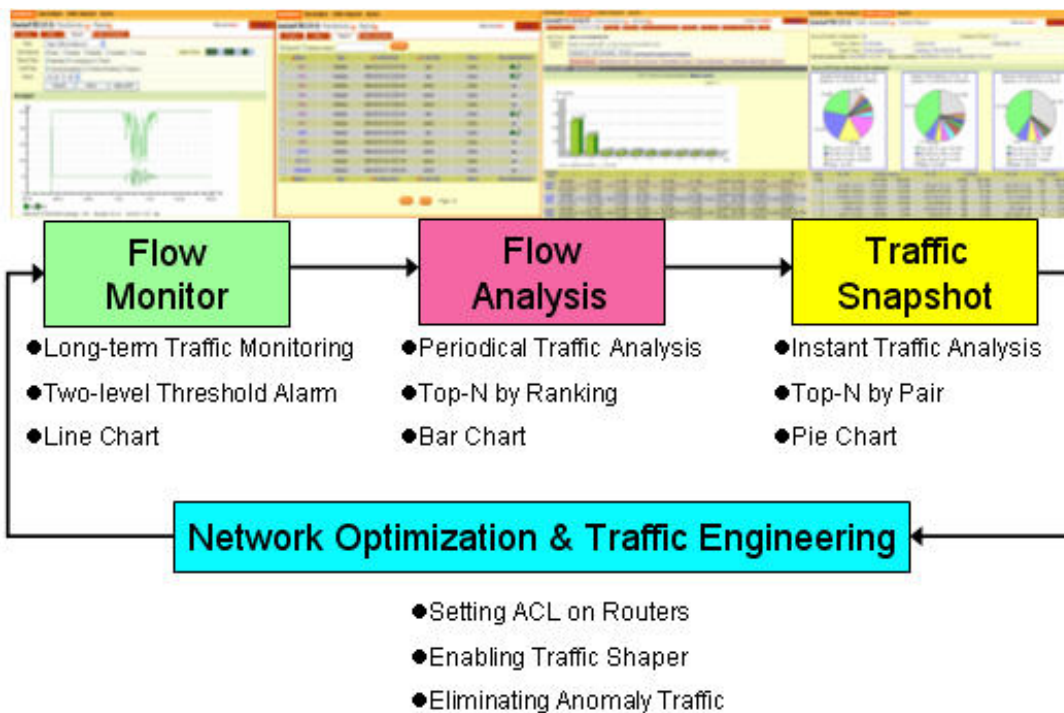
The snapshot could be triggered by analysis criteria defined such as [IP Block], [Interface], [Protocol], [Application], [Factor], and [Filter]. Thereafter, you could define the report types for better presenting the traffic distributions instantly, according to [IP Block], [Paired IP Block] (source or destination),

[Interface], [Paired Interface], and [Application].

The traffic snapshot reports will be independently ranked by instant traffic of Traffic Volume, Packet Count, and Session Number simultaneously.



By utilizing the ranking analysis of your instant network traffic, you will be able to identify and locate out most of abnormal traffic timely with source and destination information, which would enable you to respond to the problems promptly with necessary recovery actions and then to take full control on it.



Product Specifications

Dimensions

Height: 44mm **Depth:** 330mm **Width:** 426mm **Weight:** 4.5kg *suitable for 19" rack (standard)

Power

Voltage: 90-264 VAC **Power Consumptions:** 250W

Status Indicators

Power, HDD (Hard Disk), LAN Activity

Operating Environment

Temperature: 0 to 40°C (32 to 104°F) **Humidity:** 0 to 90% @40°C, non-condensing

Factor Configuration

IP Block, Host, Application, TOS, TCP Flag, Next Hop, Interface

Filter Configuration

Single Filter: Inbound / Outbound / Bi-direction

Multiple Filter: Source IP address / Destination IP address / Source Port / Destination Port

Tow-level Threshold Alarm: Yellow / Red

Flow Monitor Report

Report Type: Standard / Comparison / Trend **Content:** Throughput / Volume / Packet / Session

Time Interval: Daily / Weekly / Monthly / Quarterly / Yearly **Report Format:** Line Chart, HTML / PDF

Flow Analysis

Model 1 : Top-N Analysis among what connecting to the selected objects by ranking

Criteria : IP Block / Host / Single Factor

Model 2 : Top-N Analysis among the selected objects by ranking

Criteria : IP Block / Host / Subnet of IP Block / Factor (comparison between factors) / Factor Break Down (comparison IP addresses inside the factors)

Model 3 : Top-N Analysis based on filters by ranking

Criteria : Filter

Ranking by: Inbound (Volume/Packet/Application) / Outbound (Volume/Packet/Application) / Session

Report Format: Bar Chart + Table List, HTML, CSV (exportable)

Traffic Snapshot

Analysis Criteria: IP Block / Interface / Protocol / Well-known Application / Factor / Filter

Report Type: IP Block/Interface/Application (Single); IP Block/Interface (Paired)

Ranking by: Volume/Packet/Session (Source); Volume/Packet/Session (Destination)

Report Format: Pie Chart +Table List, HTML

System Administration

User Account Management: Account with different level of privilege/ Administration access & user access

Storage Management: Configuring the storage duration of rawdata & automatic deletion of overdue data

Flow Export Management: Flow Exporter information setup

Configuration Backup Management: System configuration backup & restoration

Data Export Interface

ODBC: Open Database Connection



Product Model	GenieATM 2311	GenieATM 2312	GenieATM 2313
Capacity (session/per minute)	50,000	100,000	200,000
No. of Supported Router	2	5	No-limitation
No. of Supported Filter	50	No-limitation	No-limitation
Flow Analysis/ No. of Windows	4	4	8
Storage Capacity	80GB	80GB	80GB
Ethernet Port	10/100/1000 *2	10/100/1000 *2	10/100/1000 *2
Probe Port	10/100/1000*2	10/100/1000 *2	10/100/1000 *2
Console Port	RS-232(DB9)	RS-232(DB9)	RS-232(DB9)
Embedded CF Card	128MB	128MB	128MB

Corporate Headquarters

WILMINGTON DE

GenieNRM INC.
2711
CENTERVILLE RD.
STE 400
WILMINGTON, DE 19808 USA
Tel
(302) 351-2111 Ext. 2041

Asia Pacific

TAIPEI

GenieNRM INC.
5F, No.15, Lane360,
Sec.1, Neihu Road,
Neihu Dist, Taipei
114, Taiwan.
Tel:
886 2 2659 6600
Fax:
886 2 2659 6622

BEIJING

GenieNRM INC.
Unit 2728, China
World Tower 1, No.1,
Jian Guo Men Wai
Avenue, Beijing
100001, China.
Tel:
86 10 6505 0601
86 10 6505 0608
Fax:
86 10 6505 2412

SHANGHAI

GenieNRM INC.
Room 1003, No.8
Middle Huaihai Road
<Lansheng Building>
Shanghai 200021,
China
Tel:
86 21 63191433-4
Fax:
86 21 6319 09