Bull. Nov. Comp. Center, Comp. Science, 21 (2004), 33–56
© 2004 NCC Publisher

Network monitoring and analysis systems. Review and operational experience

S.V. Bredikhin, V.M. Lyapunov, N.G. Scherbakova

Abstract. This paper presents the review of the network monitoring technologies that now are widely used. The main attention is given to MRTG, NETMON and NFC&NDA systems. The paper describes their advantages, configuring parameters and a necessary programming base. The experience of using these systems for monitoring the NSCnet network is discussed. A special attention is given to the issues of measurement and analysis of the traffic that concerns certain groups of users and control points of the network. Also, this paper describes how the monitoring, the data collecting and the traffic analyzing systems are used in the SB RAS (Siberian Branch, the Russian Academy of Sciences) Internet.

1. Introduction

The currently existing systems of the network management are complex software products that provide a general strategy of management. One of important aspects of the network management is the network monitoring. The network monitoring is the accumulation of various statistical data about a network and its further presentation to network administrators in the form most appropriate for them. These data include the hardware status, the hardware performance, the number of packets, changes in topology, etc. If topology and configuration become more complex, then the information is required for having an adequate picture of the network. And in this case it becomes much harder to make this information available. Often, network administrators have to combine several systems of network monitoring for managing their network effectively.

The fast development of Internet and corporate networks resulted in an increase in the carrying capacity of data transfer channels, an increase in routers and network commutator capacity. Also it became necessary to continuously control the use of network resources. The network users and administrators permanently need the objective information about the quality of provided services, network reliability and predictability of the network behavior. The network analysis, which allows the network administrator to control the use of network resources and to predict the network behavior should be conducted in order that such data (estimations) be obtained.

Along with statistics about the state of network links, the network administrators also need the necessary information about the volume of traffic and tools for recognizing the data transfer protocols used. The key elements of this analysis are the IP level aggregated data, for example, an application protocol, a port or a set of IP addresses.

2. Overview

The basic types of monitoring include: SNMP monitoring, RMON monitoring, monitoring of commutated networks, IP Accounting, monitoring, which provides information about the upper Layers of the OSI model.

The SNMP monitoring is monitoring of Layer 2 information of the OSI model. It relies on the hierarchical library of parameters, SNMP MIB [1, 2] and on the ability of network devices to provide information about these parameters upon special requests (according to the SNMP protocol, [3]). In addition, this devices can send to the control station SNMP traps and the SNMP alarms about critical events. The SNMP monitoring is most useful for collecting the key parameters of central routers, errors on interfaces, CPU and memory usage statistics and other parameters, necessary for the real time monitoring. It should be noted that currently the SNMP tools are implemented almost in all network hardware, used for the IP networks.

The RMON monitoring. This type of the network monitoring gives a wider understanding of the network dynamics on the level the network hardware interaction. In fact, it is the SNMP monitoring expansion. The RMON (RemteMONitoring) specification [4–6] determines statistics parameters and rules, characterizing the network behavior. Information (for Ethernet) is divided into nine groups: Statistics group, History group, Alarm group, Host group, HostTopN Matrix group, Filter group, Packet Capture group, and Event group. The RMON does not require the active polling of the SNMP variables. A device accumulates all the necessary information and then periodically sends it out to a RMON station, which exhibits the information received. At present, the RMON II [7] standard is accepted, where monitoring functions provide information of a network and application Layers. One of disadvantages of the RMON technology is that it is poorly adapted to switched networks, as it was developed for the networks with the sharing transfer environment.

The switched network monitoring. It is not necessary that the switched networks transfer broadcasts. Commutation can occur at the 2nd, 3rd, and 4th Layers of the OSI model. These networks are characterized by the virtual LANs (VLANs) and the packet prioritization. The RMON monitoring is poorly performed with such networks. The SMON and SMON II [8] recommendations were designed especially for these networks. The SMON defines special tools for deep monitoring of switched networks, providing a detailed information about the capacity of all the network VLANs and enabling the information filtering according to the type of ports, used in the virtual LAN. The SMON II allows us to analyze information of network, transport and application Layers. But SMON and SMON II recommendations have not been supported by all the types of commutators yet.

The IP Accounting [9, 10] provides information about the traffic, going through network devices. Its key parameters are a source port, destination port, the number of IP packets and bytes, and the type of service, ToS. Usually, the IP Accounting provides accessibility via the SNMP, which allows checkpoints and retrieval of accounting data. The IP Accounting is deployed in Cisco-routers, for example. One of weak points of the IP Accounting is that it accounts only for the egress traffic and does not give sufficient information for analyzing.

Monitoring of the Upper Layers of the OSI Model provides a large scale of detalization enabling to conduct not only the quantitative analysis of the traffic, but qualitative as well. It provides the administrator with necessary tools for the network analysis and planning along with tools for accounting, billing and data mining. In order to implement such a type of monitoring the workstation, where the system is launched, it is either possible to receive all the necessary information about the IP packets and events from the observed network devices or can capture the packets themselves, using special adapters installed in the workstation. The HP OpenView [11] can be an example of such a system. It includes both the Manager modules for managing critical environments and the SMART Plug-In for managing Internet servers or databases. It should be noted that such systems of monitoring require large volumes of RAM and hard disk memory, especially, in the cases of a high speed data transfer environment.

The traffic analysis methods. The main problem of getting the objective information about the traffic is that all measurements are done in the network environment, where the techniques of data transfer and network topology is always changing. There are no standards in the sphere of measurement and analysis of network traffic. There are only recommendations. Currently, there are series of RFCs that are of recommended nature and concern the accounting.

Policies of resource sharing on the level of administrative domains is discussed in RFC1125 [12]. The RFC1346 [13] deals with mechanisms of allocation and accounting of shared network resources. In RFC1272 [14], the architecture of traffic accounting systems is discussed. The model defines three basic entities: METER, which measures and aggregates the results, COLLECTOR, which provides integrity, security and storage of data, and APPLICATION, which processes data.

The traffic load on network links, supported by SNMP MIBs, is the starting point of the network monitoring. Traffic, measured in bites or packets per second, is usually represented by graphs, based on the WEB technology. The MRTG [15] can be shown as an example. This system provides tools for monitoring and visualization of changes in investigated parameters. The methods of an independent analysis of the network productivity are studied in the RIPE-NCC [16] project. Delays, occurring during the information transfer from one Internet provider to another, are measured. Traffic generators/receivers are placed in the close proximity to the border routers. Then the active testing is conducted. As a result, the matrices are compiled at the measurement points, the time of the packet transfer from the source s to the destination d is put at the intersection of the line s and the column d.

In order to investigate high-speed networks, based on the ATM technology, first of all, highly productive measurement tools and large volumes of hard disk memory for storage of results are required. In addition, specific parameters such as, for example, the number of "cells", received or sent by the ATM interface or the number of deleted "cells" are of interest here. The methodology of such measurements is discussed, for example, in [17].

The external METERS that are placed outside of the routers, are usually developed on the basis of "capture cards" adapted to the particular physical environment. But from the Internet service provider's point of view, the gathering information inside the router has obvious advantages, since the routers reside at the critical points of the net. There are two possibilities: COLLECTOR reads SNMP data from the router or the router itself exports these data. Moreover, there is a difference between active and passive measurements. In the case of passive measurements, naturally, traffic originated by real network devices is collected. Active measurements require traffic generators and requests for the required parameters.

From the beginning of the 90s, the research team [18] deals with issues of methodology of measurements in Internet. This group has developed CoralReef [19] software packet for passive analysis of Internet traffic. This software provides access to data, gathered with the use of capture cards, developed by different manufacturers. Here, a special attention is given to passing the IP over ATM. The data are captured by special DAG cards. First of all, CoralReef [19] provides the common interface to passive data used for analysis applications, starting with data collecting systems to report generation systems. The packet consists of hardware drivers, libraries, classes and modules, which can be called from different programming languages. Data aggregation tools are provided on the basis of a wide variety of features, such as a protocol or an autonomous system.

The most interesting thing for us is the information collecting tools that reside inside the routers. The term "traffic flow" is put in vanguard. The main characteristics are the specification of its end points and the traffic volume. The subject of the research is the one way flow. As a rule, the flow contains IP addresses of the sender and the receiver and a number of packets and bytes. The discussions go on about the issues of what other information should these flows contain, when this flow can be considered to be completed and when it should be exported.

By the present, the Realtime Traffic Flow Measurement Working Group has developed a series of recommendations RFC2720–RFC2724 [20], concerning measurements made on the basis of the "traffic flow" concept. Parameters for management of METER are defined here in the terms of Management Information Base (MIB).

3. MRTG

The Multi-Router Traffic Grapher (MRTG, [22]) is a system of the SNMP monitoring of network devices. The MRTG gathers statistics information about the work of objects of research and generates the HTML pages, which give the visual presentation of changes of SNMP variables for a particular period of time. The MRTG generates graphs in the PNG (Portable Network Graphics, [23]) format. The PNG was developed to replace the GIF (Graphic Interchange Format) format and has a series of advantages specifically for presenting images on Web pages. Moreover, effective methods of data compression were developed especially for this format. Table 1 shows the main features of the MRTG.

The main objective of the MRTG is building the graph of changes of values in question per current day. In addition, it can provide graphic representation of changes for the last seven days, for the last four weeks and for the last 12 months depending on its configuration. It is possible because the MRTG stores all the information, received from the network objects for the last two years, on disk. Log file is automatically consolidated and it does not grow, but still contains all the relevant data. The monitoring of 200 and more network links is possible because of the effective method of data storage. This monitoring system can be installed at the UNIX station with minimum features.

Even though the MRTG is more often used for monitoring of the network links utilization, the system provides the opportunity to research changes of any SNMP variables such as: System Load, Login Sessions, Modem Availability. Also, there is an opportunity of data collection by any external program (for example, in the case when the device does not support SNMP) and then a graphical representation of these data using MRTG. The MRTG allows us to accumulate two or more data sources in a single graph.

The MRTG graphical representation can be customized, but usually, the daily statistics is presented as a graph, with one axis showing the time of the day and another one showing the traffic range.

Table 1. MRTG facilities

Facility	Comments
Portability	MRTG works on most UNIX platforms and Windows NT
Source Code Availability	MRTG is written in Perl and delivered in source codes
Portable SNMP	MRTG uses the portable SNMP implementation, and it is no need to install SNMP packet
SNMPv2c Support	MRTG can read new 64 bit SNMPv2c counters
Reliable	Router interfaces can be identified by IP address, Ethernet address, Description field or interface number
Constant Size Log-files	Log-files don't grow because of the unique consolidation algorithm
Automatic Configuration	MRTG is delivered together with the set of configuring tools, that simplify the process of configuring
Performance	Critical time routines are written in C
Shareware Library of Graphic Programs	Graphs are generated in PNG format using the shareware library of graphic programs (GD library, [15])
Customizability	Web page presentation can be easily configured
RRDTool	RRDTool [16], in which effective graphic and data storage tools were realized, can be used with MRTG

The MRTG configuration and software base. The MRTG configuration file contains a lot of setting parameters. The main parameters are: the description of objects of research, the description of the SNMP variables, polling intervals, the SNMP options, the log-file format, the scale and the size of the image, directories, where data are stored, frequency of Web page refreshment, the language, in which the text is written, the Web page headings.

From the operational system point of view, the MRTG is a utility, launched by the user or by the system itself. It works in Solaris and HP-UX operational environments. The Perl interpreter is required for MRTG to work. For MRTG installation, the following are required: GNU C translator, GD (Graph Drawing) library, which use LIBPNG library for realization of PNG, and ZLIB library for data compression.

4. NETMON

NETMON (Network Monitoring [25]) is a system for monitoring of network devices. The NETMON allows one to manage the network in real time and to receive information about network devices and their services. Like MRTG, the NETMON generates HTML pages that show the status of the network. The main NETMON features are shown in Table 2.

Table 2. NETMON facilities

Facility	Comments
Simple and quick configuration	Examined variables are fixed in NETMON. They are the main variables that show status of objects. Here there is no need to make cumbersome SNMP definitions. Besides graphic representation is also fixed
Lack of large number of temporary iterations	Data collecting and processing, setting of object dependence, alarm identifying and corresponding procedure calls are executed within one program
Flexibility	User friendly method of alert signal setting with option of external program call, method of data storage and flexible methods of network device polling
Logging	Gathered data can be either saved on disk for further processing by external programs or transferred online to the external program (Unix pipe)
Access to variables	NETMON contains the wide set of internal variables, which show status of objects, which can be referred to using special mechanism

And as MRTG, the NETMON generates graphs in the PNG formats, using a GD library. But in the NETMON, the method of investigated object polling depends on the object type: routers are examined by the SNMP polling, hosts are inquired by ICMP Echo, and host services – by TCP or UDP chat scripts, developed by users.

On the HTML page, the graphic data are represented as the table that shows the current status of all objects and services, interface load and errors on interfaces in percentage and color view. Also the HTML page, showing only problem objects, is available.

The main problems solved by the NETMON are:

- Monitoring of routers status, status of their interfaces and BGP sessions;
- Collecting and storage of router interface counters;
- Monitoring of host status and their services;
- Logging the network performance;
- Dynamic discovery of the network topology;
- Alerting about the network problems;
- Presenting all the above data on web pages.

The NETMON configuration and software base. The system configuration includes the following parameter settings: the program, launched, when the alarm signal occurs with its parameters; defining objects of research, depending on their types; defining intervals and methods of data storage; defining intervals of object polling; defining working directories.

From the system point of view, the NETMON is utility of the Unix operation system, launched either by the user or by the system itself. Starting parameters are: path to the configuration file, the UDP port number for receiving traps and demand for configuration file check up. In order the NETMON be installed the following is required: the GNU C translator, the GD library, which uses the LIBPNG library for the PNG implementation, and the ZLIB library for data compression. Moreover, Perl UCD-SNMP module is required to access to SNMP variables.

The program NETMOND of data collecting and storage consists of the following main units:

- Asynchronous-parallel object poller;
- Autonomous SNMP trapper, which recognizes Cold/Warm Start, Link Up/Down signals;
- Events correlator;
- Planner, which optimally distributes load on the network;
- Background dumper of the network status;
- Subsystem of status and values accounting that saves data in database;
- Analyzer of alarm signals for launching external servicing procedures.

5. NFC & NDA

The work of Cisco NetFlow FlowCollector (NFC) and Network Data Analyzer (NDA) [26, 27] systems is based on NetFlow Services, built in Cisco IOS. NetFlow Services are capturing and data export tools providing a full picture of traffic flowing within the network device. They enable to:

- Gather and export detailed information about traffic flows between the source and the recipient;
- Effectively use access lists (ACLs), enabling applications, which analyze and filter information, to base their functions on the IP addresses of the source and the destination, the IP protocols and device interfaces;
- Filter and aggregate data by the exporting device for reducing volumes of data and presenting data in the required format.

The Information, provided by Cisco IOS NetFlow Services, can be used not only for network monitoring and planning, but also for the development of analysis and data accounting systems.

Table 3. NFC facilities

Facility	Comments
Large scale of data detailing	Statistic data contains the following fields: the source and the destination IP addresses, source and destination port numbers, IP protocol, type of service (ToS), input and output interfaces, autonomous system numbers, and also counters of bytes, packets and timing characteristics
Precise timing characteristics	Each record is characterized by the absolute time of first packet summarized and last packet summarized
Data filtration and aggregation	The use of filters allows not to save odd data, and aggregation schemes provide the required data format and additional optimization of disk space
Hierarchical data storing	Provides easy access by client applications
Disk space management	Besides filtration and aggregation tools, there is the feature of data compression and data storing in the special binary format
Management tools	Includes the set of utilities, presenting information about the status of system components

Table 4. NDA facilities

Facility	Comments
To view the received data by external workstations	Display module is the independent program module, which can be installed separately from other Analyzer modules on external workstations with different platforms, including PC Windows
To manage data presented on the screen	User is provided with tools to view data in the form most appropriate for him. In particular, he can sort data by fields of records, request conversion of IP addresses into names, create histogram and sector diagrams by numeric fields. Also he is provided with the searching tools and tools of data saving
Graphic interface for configuring NFC&NDA component	Display module provides the graphic interface to system components for visual and easy-to-use parameter setting. Even network devices can be configured to export NetFlow data
Controlling tools	User is provided with the set of utilities which inform him about the status of system components

The NFC system collects data received from network devices that are configured for the NetFlow data export. The main features of the NFC are shown in Table 3. And the main features of the NDA are shown in Table 4.

The NFC configuring and software base. It is rather difficult to configure the collector. There are eight configurations files of various purposes: nf.resources file sets the collector's environment; nfcd.config file contains parameters necessary for an automatic start and restart of program components; nfknown.protocols contains definitions of recognized Application Layer protocols; nfknown.srcports and nfknown.dstports files limit recognized TCP/UDP ports, and nfknown.srcasns and nfknown.dstasns limit recognized autonomous system numbers. And the most important file is nfconfig.file. It contains the description of aggregation schemes with data formats, filters and other parameters of data collecting.

The NFC system consists of four subsystems. The Collector is the heart of the system. This subsystem is used for receiving data from export devices and its processing with consideration of setup parameters. The Gateway subsystem organizes interface with client applications. The Daemon subsystem monitors the operational status of other subsystems. The User Interface subsystem is used to perform the configuration tasks and to query NFCollector for runtime statistics. The system operates with Solaris 2.5.1/2.6 (128 MB RAM, 512 MB swap space, 4 GB disk space) or HP-UX 11.0 (with the same characteristics) platforms. The NDA system provides the presentation of data collected by NFC and their analysis.

The NDA configuring and software base. Analyzer is the client/server application that runs on Solaris or Windows NT platforms. It consists of three modules. The DisplayServer module is used for retrieving data from the storage and sending to the Display module. The UtilityServer module provides conversion of the IP addresses to names, and it also manages configuring of system components. The Display module is a stand alone Java application, which provides data visualization and conversion and the user interface. This module can work on PC Windows platform. It is recommended to install NDA on a special workstation separately from NFC. The workstation requirements: Sun Ultra 5 and higher, 256 MB of physical memory (RAM), 400 MB of free logical memory (if the DisplayServer module runs) and 50 MB for the installed Analyzer executable.

Display module is the separate program and it is configured by its own configuration file. The following parameters should be set: the workstation IP addresses, on which the rest of the components are launched, the port numbers of these modules, and the size of the data display window. UtilityServer module settings mostly concern the information about network devices in order to configure them for NetFlow data export. DisplayServer main settings are: the port number, on which this module listens for network commands, and the size of dynamic memory pool.

6. The object of analysis

The object of our analysis is Internet of Novosibirsk Scientific Center (NSC) of SB RAS [21]. The core of the network consists of the central Cisco-routers (IOS 12.2) and net servers, physically connected by Fast Ethernet. In most cases, local user (scientific, culture, health, and educational organizations) networks are connected to the central network devices via peripheral routers. Some of the peripheral routers are connected to the central network node by Frame Relay links.

The telephone channels of various capacity provide the connection with the external segment of Internet. The regional scale of the network is represented by the ground communication links to scientific centers of SB RAS, located in the city of Tyumen, Irkutsk, Tomsk and others. In addition, there is the peering with some Novosibirsk networks.

The objective of the traffic accounting between the users of the NSC network and organizations that are not registered users of this network stands out among the objectives of statistics information analysis. Let us call this traffic "external".

The current paper investigates two following issues:

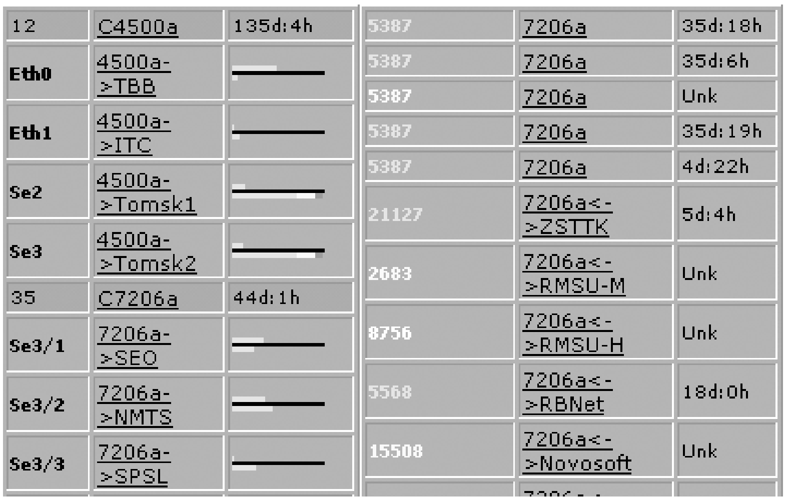
- The volume of the external traffic, received and sent by each NSC network user per particular period of time;
- The structure of traffic, received and sent by users, i.e., how it is distributed among data transfer protocols.

Traffic is measured in the control points of the network, that are corresponded to the physical or virtual router interfaces. The formal description of the control points of the network is applied to automate the process of collecting and analysis. These control points are represented by multitude of fours: $\{(N_1, R_1, I_1, F_1), \ldots, (N_n, R_n, I_n, F_n)\}$, where N_i is the control point identifier, R_i is the router address, I_i is the router interface name, F_i is the path to the processing script file. These data are used to generate daily files for further tasks starting by the system cron process.

7. NSCnet monitoring

The NSCnet status analysis uses the combination of tools, which compliment each other. The NetFlow system collects data of the Upper Layers of the OSI model, and the NETMON and the MRTG systems are used for monitoring in real time and collecting information about device status, interface status, CPU and other parameters not associated with the qualitative information about data flow.

The NETMON system (see http://monitor.nsc.ru/cgi-bin/netmon/netmon.cgi) is used for network monitoring and it is the main tool for real time visualization of the network status. All parameters that we observe are shown in the table on one HTML page. In our case, they are: status of core and boundary routers, their interfaces and the BGP sessions, and also status of the following services: proxy, http, dns and pop3 (Figure 1). The most useful feature of this system is the ability to call the html page, containing only the problem network elements.



12	C4500a	135d:4h
Eth0	4500a->TBB	
Eth1	4500a->ITC	
Se2	4500a->Tomsk1	
Se3	4500a->Tomsk2	
35	C7206a	44d:1h
Se3/1	7206a->SEO	
Se3/2	7206a->NMTS	
Se3/3	7206a->SPSL	

5387	7206a	35d:18h
5387	7206a	35d:6h
5387	7206a	Unk
5387	7206a	35d:19h
5387	7206a	4d:22h
21127	7206a<->ZSTTK	5d:4h
2683	7206a<->RMSU-M	Unk
8756	7206a<->RMSU-H	Unk
5568	7206a<->RBNet	18d:0h
15508	7206a<->Novosoft	Unk

Figure 1. NETMON: State diagram of channels

The table shown in Figure 1 is divided in three columns. First two columns identify an object. The third column shows the status of the object. The router status is represented by color and corresponding comment. Green color is UP, light-green means that it changed its status to UP, red color is DOWN, lilac color means error. Moreover, the time period, during which the object has the current status, is also indicated in the same column. The color of the first column, that contains autonomous system number, indicates the status of the BGP session, and the time is shown in the third column. For interfaces, communication links utilization is graphically represented in the third column if the status is UP and there are no INPUT/OUTPUT errors. Green line is less than 70%, yellow $\sim$ 70%, red $\sim$ 90%.

There are four columns in the table showing only the problem objects. Fourth column contains information about errors. The pictures are renewed when the following occurs: as soon as polling results are received (the interval is specified), upon the change of the status of one of the objects, and upon the user request.

The MRTG system (see http://monitor.nsc.ru/mrtg/index.html), as applied to NSCnet, is used for dynamic evaluation of the network control points utilization, including utilization of the external communication links. The system ability to provide the live visual representation of the traffic load on communication links and, also, the ability to provide the history of links utilization are the powerful tools for monitoring of bottle neck places of the net (Figure 2). Unlike NETMON, the MRTG offers ready solutions.

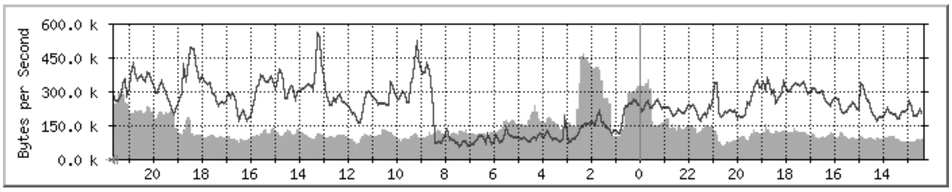


Figure 2. MRTG: Channel daily traffic

8. Network traffic analysis tool

Cisco-routers and commutators are able to accumulate various statistics data and export it to the special workstation for further processing. This is the function of NetFlow Services, supported by the latest versions of Cisco IOS. Here, METER is located inside a router. Exported data consists of traffic flows, which are unidirectional sequences of packets between a particular source device and destination device that share the same protocol and transport-layer information.

For example, HTTP packets from the source to the destination are collected separately from the FTP packets from the same source to the same destination. As a whole, routers and commutators identify flows, taking into account the following fields within IP packets: source IP address, destination IP address, source port number, destination port number, type of protocol, type of service (ToS), and input interface.

Statistics data of each active flow is accumulated in the memory of METER. Summary statistics is exported periodically to a user-specified destination by means of User Datagram Protocol (UDP) datagrams. The flow expires when one of the following conditions occurs: the transport protocol indicates that the connection is completed (TCP FIN), the delay for the completion of the FIN acknowledgment handshaking is taken into account, or there was not any traffic exchange during 15 minutes. For continuously active links, a forced expiration occurs every 30 minutes.

Data is exported to receiving workstation either every second or if the number of recently expired flows reaches a predetermined maximum – whichever occurs first. For example, in a single UDP datagram of approximately 1500 bytes up to 30 flows can be sent.

Detailed statistics contains the following information: source and destination IP addresses, IP address of next hop device, input and output interface numbers, number of packets, number of octets, time of the beginning and the end of the flow, source and destination port numbers, protocol, type of service (ToS), source and destination autonomous system numbers, source and destination IP address prefix mask bits.

Cisco Systems Inc. distributes NetFlow FlowCollector (NFC) [27] software that provides data collection and aggregation from multiple export devices exporting NetFlow data records. Thus NFC, following RFC1272 terminology, plays the role of COLLECTOR. Exporting devices are configured for NetFlow data export. The configuration information includes the IP address and the UDP port number that identify FlowCollector as the receiver of flows. The UDP port number is a user-configurable parameter, one can configure FlowCollector to listen for flows on a number of different UDP ports.

The NFC functions are: data collection from multiple exporters, data filtration and aggregation, hierarchical data storage, file system space management. The NFC collects and summarizes data into files based on user-defined criteria. The data file directory structure created by FlowCollector 3.0 contains the information about the aggregation schemes, the day of year and the export devices. A long form filename contains the following information: export-resource-name, date and time of file generating.

FlowCollector consists of four subsystems: the Collector (NFCollector), the Gateway (NFCGW), the Daemon (NFCD), the User Interface (NFUI). The NFC architecture is shown in Figure 3.

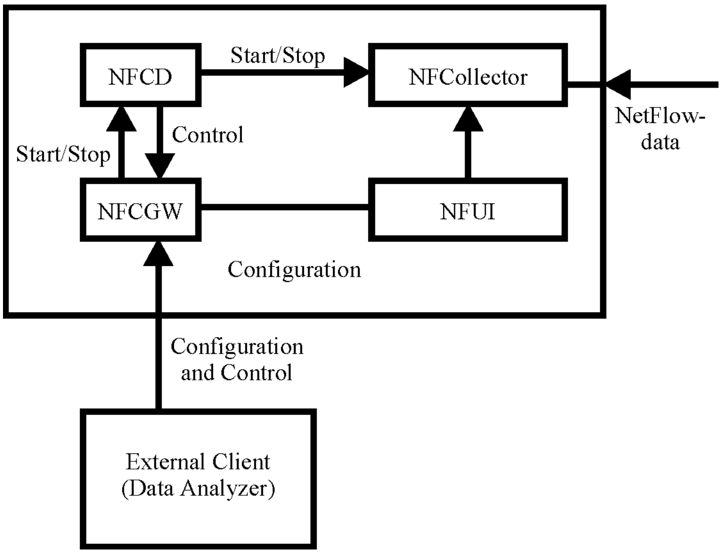


Figure 3. FlowCollector System Architecture

The Collector is the main part of the system. Among its objectives are: data collection, its aggregation and filtration, and data saving in files with the user-defined frequency. Each file consists of the header and records containing key fields and value fields according to the aggregation scheme. *The Gateway* provides the interaction between the Collector and external client applications, for example, Data Analyzer, installed on another workstation. *The Daemon* monitors the operational status of both Collector and Gateway. It executes and restarts these subsystems. *The User Interface* is used to query NFCollector for runtime statistics and to perform configuration tasks.

In our case, NFC works in the SunOS 5.6 operation environment. Each 15 minutes data, received from the central routers, are written into output files. Since the size of files is rather big, all daily information is compressed, using tar and gzip utilities, and stored into day-file.

During last two years NFC&NDA systems are used for analyzing of the traffic structure. At the present, we use NFCollector 3.0. The large volume of disk memory is required to store data, daily received from export devices. NFC provides tools to reduce the amount of disk space: data compression (gzip utility) and binary format data files. Unfortunately, Analyzer 3.0 cannot display the compressed data. That is why, at the present, the current day data, which is analyzed by NDA, is written in ASCII format. Previous data is compressed and available for analysis, using traffic analysis system, developed in our Institute. This system saves the results of analysis in database for further access to this data with the help of Web technology.

NFC is configured to use DetailASMatrix aggregation schemes. This aggregation scheme returns data for fields, represented in Table 5.

NDA provides the opportunity to view data on external workstation or on multiple stations. In our case, the Display module is running as the stand-

Table 5. DetailASMatrix fields

Field	Content
Srcaddr	Source IP address
Dstaddr	Destination IP address
src-as	Autonomous system number of the source
dst-as	Autonomous system number of the destination
input interface	SNMP index of input interface
output interface	SNMP index of output interface
srcport	TCP/UDP source port number or equivalent
dstport	TCP/UDP destination port number or equivalent
protocol	IP protocol type (for example, TCP=6, UDP=17)
packets count	Number of packets, counted as part of this record
byte count	Total number of Layer 3 bytes counted as part of this record
flow count	Total number of flows aggregated into this record

alone Java application working in the PC Windows operation environment. After startup, data set path can be defined and then data can be requested. Time interval is represented in the mode, most appropriate for user, not in UTC seconds, used by Collector. From 10 to 10000 flows (bytes or packets) can be selected. But there is a bug in the current version: a request for 10000 cause “Out of Memory” exception. The data, displayed on the screen, can be sorted by value and key fields. This, for example, allows a network manager to effectively detect attacks from the network devices (sorted by source address), to analyze the means being used (srcport, dstport, protocol fields) and determine the interface packets are coming from. Sector diagrams and bar charts, together with tools for address to name conversion, facilitate the monitoring of users’ activity.

At the present, we plan to install NFC&NDA system version 3.6(1). This version has several advantages over previous versions. For us, the most important things in this version are the expanded Analyzer features: compressed and binary files displaying, support of a large number of aggregation schemes, expanded search, and graphic representation.

9. Traffic analyzing system

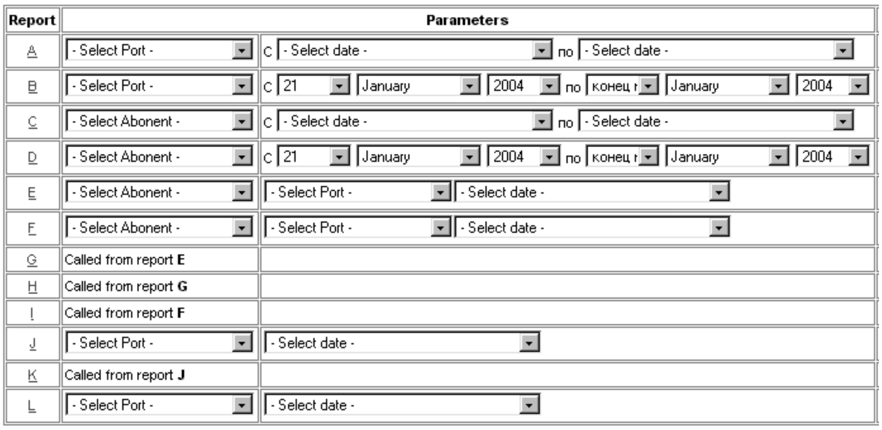
In RFC1272 [10] terminology, our system of traffic analysis, STAT (see http://monitor.nsc.ru/stat/index.php), is APPLICATION. It provides a user with the following daily information (for the last 10 days): the volume of external traffic for each abonent, protocols, used by network abonents within external traffic, devices, which provide maximum traffic for each abonent. Moreover, aggregated information (with precision to 10 days) about traffic of each abonent, from the begging of statistics data collection to the present moment, is available.

Web browser provides access to this information. As an answer to the request to Web server, user receives the page displaying management elements (Figure 4). After parameters are entered, one of the reports, mentioned below, is displayed. These reports contain data, generated according to the selected parameters. The report use the terminology explained in Appendix.

Parameters and the resulting report description are listed in Table 6.

Report A provides for each abonent the information about the traffic passed through the selected channel for the particular time period. The information for only ten previous days is available. Accuracy of definition of the time period makes one day.

Report B provides for each abonent the aggregated information about the traffic passed through the selected channel for the particular time period. The information for the whole period of statistics data collection is available. Accuracy of definition of the time period makes ten days.



Report	Parameters	
A	- Select Port -	c - Select date - по - Select date -
B	- Select Port -	c 21 January 2004 по конец г January 2004
C	- Select Abonent -	c - Select date - по - Select date -
D	- Select Abonent -	c 21 January 2004 по конец г January 2004
E	- Select Abonent -	- Select Port - - Select date -
F	- Select Abonent -	- Select Port - - Select date -
G	Called from report **E**	
H	Called from report **G**	
I	Called from report **F**	
J	- Select Port -	- Select date -
K	Called from report **J**	
L	- Select Port -	- Select date -

Figure 4. STAT: User interface

Report C provides the information about the traffic of the selected abonent for all channels for the particular time period. The information for only ten previous days is available. Accuracy of definition of the time period makes one day.

Report D provides the information about the traffic of the selected abonent for all channels for the particular time period. The information for the whole period of statistics data collection is available. Accuracy of definition of the time period makes ten days.

Report E provides the information about devices of the selected abonent with maximum traffic for the indicated channel per one day. The information is provided only for devices, making up more than 1% of all traffic of the selected abonent. Maximum number of devices is twenty. The information for only ten previous days is available.

Report F provides the information about protocols, used during the selected day by the selected abonent for the indicated channel. The information is provided only about protocols, making up maximum traffic and more than 1% of all the traffic of this abonent. The information for only ten previous days is available. The current list of protocols, recognized by STAT, can be found at http://monitor.nsc.ru/stat/prot.html.

Report G provides the information about protocols, used during the selected day by the selected device of the abonent for the selected channel. The information is provided only about protocols, making up maximum traffic and more than 1% of all the traffic of this device. Maximum number of protocols is twenty. The information for only ten previous days is available.

Table 6. Reports: parameters and results

Report	Parameters	Result
A	Channel, Time interval	1. If time interval equals 1 day (from = to), then summary table contains the following fields: Organization, InExtern, OutExtern, External, InExt%%, OutExt%%, Hosts, Activ 2. If time interval is more than 1 day (from < to), then summary table contains the following fields: Organization, InExtern, OutExtern, External, InExt%%, OutExt%%
B	Channel, Time interval	Summary table contains the following fields: Organization, InExtern, OutExtern, External, InExt%%, OutExt%%
C	Abonent, Time interval	1. If time interval equals 1 day (from = to), then summary table contains the following fields: Channel, InExtern, OutExtern, External, InExt%%, OutExt%, Hosts, Activ 2. If time interval is more than 1 day (from < to), then summary table contains the following fields: Channel, InExtern, OutExtern, External, InExt%%, OutExt%%
D	Abonent, Time interval	Summary table contains the following fields: Channel, InExtern, OutExtern, External, InExt%%, OutExt%%
E	Abonent, Channel, Date	Summary table contains the following fields: Device, DExt%%, DIn%%, DOut%%
F	Abonent, Channel, Date	Summary table contains the following fields: Protocol, PExt%%, PIn%%, POut%%
G	Device[1], (Abonent, Channel, Date)[2]	Summary table contains the following fields: Protocol, DPExt%%, DPIn%%, DPOut%%
H	Device[3], (Abonent, Channel, Date)[4], TCP/UDP-Other[5]	Summary table contains the following fields: Port, DPortExt%%, DPortIn%%, DPortOut%%
I	(Abonent, Channel, Date)[6], TCP/UDP-Other[7]	Summary table contains the following fields: Port, PortExt%%, PortIn%%, PortOut%%
J	Channel, Date	Summary table contains the following fields: Protocol, AllPExt%%, AllPIn%%, AllPOut%%
K	(Channel, Date)[8], TCP/UDP-Other[9]	Summary table contains the following fields: Port, AllPortExt%%, AllPortIn%%, AllPortOut%%
L	Channel, Date	Summary table contains the following fields: Host, AllHExt%%, AllHIn%%, AllHOut%%

[1] A device is selected from the list of devices included in the summary table of Report E or L. [2] Parameters of Report E or L. [3] A device is selected from the list of devices included in the summary table of Report E. [4] Parameters of Report E. [5] Type is selected from the summary table of E. [6] Parameters of Report F. [7] Type is selected from the summary table of F. [8] Parameters of Report J. [9] Type is selected from the summary table of J.

Report H provides the information about TCP/UDP ports used by devices mentioned in Report G. It concerns the protocols marked as TCP/UDP-Other. Information is provided only about ports, making up maximum traffic and more than 1% of TCP/UDP-Other. Maximum number of ports is twenty.

Report I provides the information about TCP/UDP ports used by devices mentioned in Report F. It concerns the protocols marked as TCP/UDP-Other. Information is provided only about ports, making up maximum traffic and more than 1% of TCP/UDP-Other. Maximum number of ports is twenty.

Report J provides the information about protocols, used during the selected day by all abonents for the indicated channel. The information is provided only about protocols, making up maximum traffic and more than 1% of all the traffic of the selected channel. The information for only ten previous days is available.

Report K is similar to Report I but it concerns protocols mentioned in Report J.

Report L provides the information about devices with maximum traffic for the indicated channel per one day. The information is provided only for devices, making up more than 1% of all traffic of the selected channel. Maximum number of devices is twenty. The information for only ten previous days is available. The information about protocols used by these devices can be obtained with Report G.

10. Implementation

STAT consists of the following subsystems: Data Analysis Subsystem, MySQL database, Data Display Subsystem.

Data Analysis Subsystem is implemented as the set of Perl scripts [28], started by cron daemon in SunOS 5.5.1 environment.

The file, consisting of specified fours of (N_i, R_i, I_i, F_i) type, is passed to the script generator as a parameter. Generator finds out SNMP index of R_i router interface for each i and organizes crontab file. UCD SNMP packet [29] is used for receiving the SNMP information from the remote routers.

In case of failure (when the router is unavailable, when the source data is unavailable, or when it is impossible to put the data in the database table) operator receives e-mail message and generator continuously tries to complete his work.

When generator completes its work, the processing scripts are started. They analyze previous day data files, provided by NFC, and then place the results into the database tables.

In addition, the script, that aggregates data for the previous ten days and cleans database tables, is executed once in ten days. Collection process and analysis process are running on separate workstations within one Backbone.

DBI (DataBase Interface) and DBD (DataBase Driver) packets from CPAN [30] are used to gain access from Perl scripts to MySQL Data Base Management System. DBI provides the interface between the program and driver, used for work with the particular DBMS, in our case it is DBD::mysql.

Perl scripts are parameterized. The parameters of daily script are: routers address, SNMP interface index, channel identifier, and the table of abonents and their network addresses. Aggregating script uses number of ten-day period as parameter.

MySQL [31] was selected as a shareware effective database server. Database STAT consists of eleven tables, five of them containing statistics information. Day_stat table contains daily statistics and each day it is expanded by 300 records. The record is 62 bytes long. Host_stat table contains information about abonent devices, which generate and receive traffic, and it is expanded by 1700-1800 records per day. The record in this table is 48 bytes long. Prots-stat table contains information about protocols, used by the abonents, and it is expanded by 1050 records per day. The record is 52 bytes long. Hostprots-stat table contains information about protocols, used by abonent devices and it is expanded by 3600 records per day. The record is 68 bytes long. These tables contain information for 10 previous days. Stat table contains all statistics from the beginning of information collection, with precision to 10 days, and it is expanded by 300 records per 10 days. The record is 88 bytes long. All other tables contain the auxiliary information and all of them have the constant length.

Data Display Subsystem is implemented using PHP v.4 [32]. It provides the user interface to the statistics data, generating the reports mentioned above. Upon user request to Web server he receives a Web page displaying management elements. After he enters all the necessary parameters he receives one of the reports.

References

[1] RFC 1156. Management Information Base for Network Management of TCP/IP-based internets. – http://www.ietf.org/rfc/rfc1156.txt.

[2] RFC 1158. Management Information Base for Network Management of TCP/IP-based internets: MIB-II – http://www.ietf.org/rfc/rfc1158.txt.

[3] RFC 1157. A Simple Network Management Protocol (SNMP). – http://www.ietf.org/rfc/rfc1157.txt.

[4] RFC 1271. Remote Network Monitoring Management Information Base. – http://www.ietf.org/rfc/rfc1271.txt.

[5] RFC 1513. Token Ring Extensions to the Remote Network Monitoring MIB. – http://www.ietf.org/rfc/rfc1513.txt.

[6] RFC 1757. Remote Network Monitoring Management Information Base. – http://www.ietf.org/rfc/rfc1757.txt.

[7] RFC 2021. Remote Network Monitoring Management Information Base Version 2 using SMIv2. – http://www.ietf.org/rfc/rfc2021.txt.

[8] RFC 2613. Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0. – http://www.ietf.org/rfc/rfc2613.txt.

[9] RFC 1346. Resource Allocation, Control, and Accounting for the Use of Network Resources. – http://www.ietf.org/rfc/rfc1346.txt.

[10] RFC 1272. Internet Accounting: Background. – http://www.ietf.org/rfc/rfc1272.txt.

[11] HP OpenView. – http://openview.hp.ru/.

[12] RFC 1125. Policy Requirements for Inter Administrative Domain Routing. – http://www.ietf.org/rfc/rfc1125.txt.

[13] RFC 1346. Resource Allocation, Control, and Accounting for the Use of Network Resources. – http://www.ietf.org/rfc/rfc1346.txt.

[14] RFC 1272. Internet Accounting: Background. – http://www.ietf.org/rfc/rfc1272.txt.

[15] Multi Router Traffic Grapher. – http://people.ee.ethz.ch/ oetiker/webtools/mrtg/.

[16] Uijterwaal H. Providing Test Traffic Measurements (TTM) as a Membership Service. – http://www.ripe.net/ripe/docs/ripe-209.html.

[17] Jerkins J.L., Neidhardt A.L., Wang J.L., Erramilli A. Operations Measurements for Engineering Support of High-Speed Networks with Self-Similar Traffic. – http://www.caida.org/outreach/isma/9901/slides/wang/jwang_itc16.pdf.

[18] CAIDA/NLANR Group. – http://www.caida.org/.

[19] CoralReef. – http://www.caida.org/tools/measurement/coralreef/.

[20] Realtime Traffic Flow Measurement. – http://www2.auckland.ac.nz/net/Internet/rtfm/.

[21] NSC Network. – Novosibirsk, 2002. – (Preprint; 1155) (in Russian).

[22] MRTG. MultiRouter Traffic Grapher. – http://people.ee.ethz.ch/˜oetiker/webtools/mrtg/.

[23] Portable Network Graphics. – http://www.design.ru/png/png.html.

[24] Graphical Interchange Format Specification. – http://www.nist.ru/hr/doc/spec/gif87.htm.

[25] NETMON – Network Monitoring System. – Rinet Software, 1999.

[26] Cisco NetFlow FlowCollector with Network Data Analyzer. – http://www.cisco.com/univercd/cc/td/doc/pcat/nefl__s1.htm.

[27] NetFlow FlowCollector. Release 3.0. – Cisco Systems, Inc., 2000.

[28] Practical Extraction and Report Language. – http://www.perl.com/.

[29] UCD-SNMP Package. – http://www.ece.ucdavis.edu/ucd-snmp/.

[30] Comprehensive Perl Archive Network. – http://www.perl.com/CPAN/CPAN.html.

[31] MySQL. – http://www.mysql.com/.

[32] PHP. – http://www.php.net/.

Appendix. The terminology

Abonent – organization, connected to NSCnet

External traffic – traffic between user and organizations, which are not registered as NSCnet users

Channel – identifier of the point of interaction with the external provider

Protocol – Internet protocol identifier recognized by Cisco NetFlow FlowCollector. The list of known protocol names is defined by the collector administrator according to RFC 1700 and placed into the configuration file nfknown.protocols

Port – TCP/UDP port number

Network device – abonent network device generating and receiving traffic

InExtern – external traffic sent to abonent, which passes through the indicated channel for particular time period

OutExtern – external traffic sent by abonent, which passes through the indicated channel for particular time period

External = InExtern + OutExtern

InExt%% = (InExtern*100)/External

OutExt%% = (OutExtern*100)/External

InLocal – local traffic sent to abonent, which passes through the indicated channel for particular time period

OutLocal – local traffic sent by abonent, which passes through the indicated channel for particular time period

In = InExtern + InLocal

Out = OutExtern + OutLocal

Total = In + Out

In%% = (In*100)/Total

Out%% = (Out*100)/Total

Hosts – total number of abonent's device IP addresses, registered during External traffic accounting

Activ – number of abonent's device IP addresses, registered during OutExternal traffic accounting

DInExt – external traffic sent to the device

DOutExt – external traffic sent by the device

DExternal = DInExt + DOutExt

DExt%% = (DExternal*100)/External

DIn%% = (DInExt*100)/DExternal

DOut%% = (DOutExt*100)/DExternal

PInExt – external traffic sent to abonent, using indicated protocol

POutExt – external traffic sent by abonent, using indicated protocol

PExternal = PInExt + POutExt

PExt%% = (PExternal*100)/External

PIn%% = (PInExt*100)/PExternal

POut%% = (POutExt*100)/PExternal

DPInExt – external traffic sent to device, using indicated protocol

DPOutExt – external traffic sent by device, using indicated protocol

PExternal = DPInExt + DPOutExt

DPExt%% = (DPExternal*100)/DExternal

DPIn%% = (DPInExt*100)/DPExternal

DPOut%% = (DPOutExt*100)/DPExternal

DOtherExternal – external traffic of abonent's device marked as TCP/UDP-Other

DPortInExt – external traffic sent to abonent's device marked as TCP/UDP-Other and using indicated destination port

DPortOutExt – external traffic sent by abonent's device marked as TCP/UDP-Other and using indicated destination port

DPortExternal = DPortInExt+DPortOutExt

DPortExt%% = (DPortExternal*100)/DOtherExternal

DPortIn%% = (DPortInExt*100)/DPortExternal

DPortOut%% = (DPortOutExt*100)/DPortExternal

OtherExternal – external traffic of abonent marked as TCP/UDP-Other

PortInExt – external traffic sent to abonent marked as TCP/UDP-Other and using indicated destination port

PortOutExt – external traffic sent by abonent marked as TCP/UDP-Other and using indicated destination port

PortExternal = PortInExt + PortOutExt

PortExt%% = (PortExternal*100)/OtherExternal

PortIn%% = (PortInExt*100)/PortExternal

PortOut%% = (PortOutExt*100)/PortExternal

AllExternal – all external traffic fixed on the channel

AllPInExt – external traffic to NSCnet fixed on the channel and using indicated protocol

AllPOutExt – external traffic from NSCnet fixed on the channel and using indicated protocol

AllPExternal = AllPInExt + AllPOutExt

AllPExt%% = (AllPExternal*100)/AllExternal

AllPIn%% = (AllPInExt*100)/AllPExternal

AllPOut%% = (AllPOutExt*100)/AllPExternal

AllOtherExternal – all external traffic fixed on the channel and marked as TCP/UDP-Other

AllPortInExt – external traffic to NSCnet marked as TCP/UDP-Other and using indicated destination port

AllPortOutExt – external traffic from NSCnet marked as TCP/UDP-Other and using indicated destination port

AllPortExternal = AllPortInExt+AllPortOutExt

AllPortExt%% = (AllPortExternal*100)/AllOtherExternal

AllPortIn%% = (AllPortInExt*100)/AllPortExternal

AllPortOut%% = (AllPortOutExt*100)/AllPortExternal

AllHInExt – external traffic to NSCnet devices marked as TCP/UDP-Other and using indicated destination port

AllHOutExt – external traffic from NSCnet device marked as TCP/UDP-Other and using indicated destination port

AllHExternal = AllHInExt + AllHOutExt

AllHExt%% = (AllHExternal*100)/AllOtherExternal

AllHIn%% = (AllHInExt*100)/AllHExternal

AllHOut%% = (AllHOutExt*100)/AllHExternal