NetIIS

User manual

CONTENT

1. INTRODUCTION

NetIIS is an advanced, efficient, multi-user, easy to use, web based networking information and monitoring system. NetIIS has been developed at the Belgrade University Computer Centre (RCUB) aiming to discover, collect and provide all relevant networking information and help the network administrators in their everyday technical activities. It performs both passive and active monitoring, giving reliable and up-to-date status information regarding the network infrastructure, services and attached devices. Furthermore, a flexible software framework can also be used as a technical knowledge base with the ability for users to store various texts and information about the target network and networking problems.

The software is developed on the Java platform, running on a Linux web application server with a MySQL database backend. The software is problem-solving oriented, specially adopted to fit user needs and to link networking and monitoring information following the logical troubleshooting process. Typical user access is performed through a standard web interface. It allows browsing the database, having various views on network information, current status and other details. Since an operational multi-domain network requires interaction with the technical staff, web access also supports instant set-up and data configuration.

However, a standalone java client application, with an efficient GUI, is more comfortable for advanced monitoring system configuration. Java web-start technology assures running up-to-date executable code stored on the NetIIS server, which simplifies technical maintenance and support in a multi-domain environment. Both types of access are multi-user oriented, with arbitrary read and write permissions over a database hierarchy.

NetIIS aims to help the users who manage any large scale network. Therefore, intelligent auto discovery functions have been developed. This capability enables complex network topologies to be easily translated into equivalent logical forms, with all relevant technical information: network topology, IP/MAC address, host and port names, SNMP IDs, descriptions etc. Furthermore, in case of network changes, auto-discovery automatically keeps the information up-to-date without the need for manual reconfiguration, always providing consistent monitoring results. Network topology and items from the database can be presented graphically, allowing efficient performance monitoring and information access. Essential indicators, such as link utilization, interface name, router characteristics can be easily obtained by either clicking on an object or by simply placing the cursor on top of a module.

NetIIS is especially built to fit a wide range of user needs in an efficient and effortless way. It combines the best of commonly used free software and commercial tools: a straightforward usage and presentation style, powered by advanced features, such as auto-discovery and its multi-user environment. Additionally, in contrast to all of these toolsets, NetIIS contains a modern networking information system, able to organize necessary technical data and its knowledge base. It complies with EIA/TIE 606 standard, which requires labelling and data recording of all networking elements. While the standard is constrained to passive elements in commercial buildings only, the NetIIS database supports both passive and active elements in LAN and WAN environments.

2. BASIC CONCEPTS

2.1. Objects of the data hierarchy

Computer networks generally contain a large number of devices, links and host computers. Networking information system has a task to present all objects from the external world to the user in the most efficient and easily understood way. Since the tree structure is most suitable for efficient browsing of large amounts of data, objects in the NetIIS information system are hierarchically organised and presented by a tree. The user is best introduced to the system through the description of the tree. He will use it during his work and will often identify with the information system.

There are several general types of objects in data hierarchy: folders, locations, equipments, ports, users, user groups, groups of elements and notes.

Folder presents an object that serves for joining other objects in the purpose of better organisation of the tree structure, in the analogue role of folders in the file system. For example, the user can define equipment in folders organized by type (folder with routers, switches, servers), by their geographical location (folder presenting a region) or by any other criteria.

Location is an object that presents organisational or territorial node in a computer network. Within individual locations other network elements are defined, that can be interpreted as objects physically presented on that location. For example, in the Academic network all faculties and individual buildings as well, are presented as locations. In a corporate network, locations would present each branch office and local office. In the LAN network locations can present rack closets with adhered devices.

Device presents networking equipment, such as routers, switches, computers, but it can also present passive components as well, such as telecommunication connections, cables, outlets etc. Devices are the most important object in the information system since they represent active nodes in the computer network.

Port is the following element of interest in the computer network that presents the physic*al or logical interface of networking equipment. It the data structure ports are attached to devices and are shown as their children.*

User is an object that presents persons in the information system. These objects contain relevant personal information, such as their name, surname, address, telephone and other. Generally, it deals with people that are connected in a business network: contact people, administrator, operator, people on ranks in certain institutes, or even virtual user that can be presented as an email list of users (helpdesk, info etc).

Additionally, if the persons are also users of the NetIIS system, their user names and passwords are added for access to the system. Further on, the users are individually defined with permissions to read and alter (write) particular data in the information system.

A predefined user of the NetIIS system is a *guest*, the user with permission to read public data without password, and *administrator*, the user with all permissions over the NetIIS system.

User group presents an object that has a function to adjoin all users with the same function and/or privileges in the NetIIS system. User groups enable faster and more efficient issuing of privileges to a larger number of users or define user groups that will be informed on certain events in the system. Users can be members in several user groups.

Group is an object that serves for grouping other objects for joint presentation in certain form. This is usually used for grouping objects that contain information on the status of network elements. Objects are grouped by creating shortcuts, and not by physically moving to a group, thus they are located in the primary location in the data hierarchy. Therefore, objects can be assigned to a number of groups. Also, one group can contain other groups.

There are 3 types of groups:

- *Simple Group* (*default*) serves for showing elements in a table format. They are typically used for joining monitoring results, presenting the current status.
- *Graph* serves for graphical presentation of the topological connection of the belonging elements, operational status and recent statistics.
- *Looking Glass* joins devices that enable remote command execution, so-called *Looking Glass* functionality. NetIIS system accesses selected device via telnet sessions, executes the chosen command and output the results to the user (e.g. *show interface Serial 0*).

Note is an object that keeps arbitrary text data. The note is useful for saving certain information connected to the belonging element. For example, for devices it is useful to store history of comments about hardware changes, distributor of the device, period of guarantee, reaction procedure in the case of network problem etc.

2.2. Objects of the monitoring system

Monitor is an object that permanently and periodically monitors the status of the computer network. Types of checking the network status and data that is being returned are defined with the type and monitor parameters. Monitors in the information system are defined within devices or ports and in the data hierarchy are shown as their children. Typical presentation of the monitoring results is adjusted by putting monitors in relational group.

A value that monitors return during a long period of time can be archived and shown via accompanying RRD Charts. Users may also be informed on certain events via the concept of alarm.

RRD Chart (*Round Robin Database*) presents an object of the monitoring system that is defined under the Monitors. RRD chart has a task to store the values of the monitor variables during a period of time and to show them in a graphical form.

Note. RRD Chart object is a generalized paradigm of traditional MRTG charts.

Alarm is an object that is defined under the Monitors and compares values of the monitor within given thresholds. In the case of criteria fulfilment, the alarm becomes active in which case it can execute the given notification action. If the given criterion presents an unwanted event (e.g. connection failure), alarm is a "*Bad*" type, whilst in the opposite case it is of "*Good*" type. The critical levels are defined on the alarm, in the range from -10 to +10. Negative and positive values designate whether the alarm is *Bad* or *Good*, whilst the numerical value defines its acuteness, i.e. importance to the user.

Action is adjoined to certain Alarm and it defines in which way the NetIIS system is going to react in the case of alarm activation. There are 2 types of actions:

- **e-Mail Action** - sends e-mail messages to a selected user or user groups
- **SMS Action** - sends SMS messages to a selected user or user groups.

Both types of actions allow defining messages that are sent with other descriptions connected to the parent Alarm and Monitor. An action always performed when the alarm is activated (turned on) is notification in the *Event Log*, that enables a listing and search of all activated alarms in the system during a time.

Report presents an object that shows on-demand the current status of devices to which it's assigned in the data hierarchy. Report is defined by the list of SNMP variables and form of their presentation. Unlike periodically executed Monitors, reports are performed on user's request (*on-demand*) at which point the up to date values are being read from the devices and shown in an appropriate form.

2.3. General object concepts

Following general concepts can be assigned to the objects in the data hierarchy:

- **Children** present a list of objects associated to the parent object. This relation of "belonging" determines the data hierarchy tree.
- **Attributes** presents specific information that define an object and depend on type of objects. For example, device attributes are manufacturer, the device model and the serial number, whilst ports have text description and SNMP identifiers as attributes etc. Attributions of locations are full name, acronym, address, telephone, fax etc.
- **Properties** present arbitrary data assigned to the object. Properties have their own name, values, description, time of instalment and information on whether it is public. Certain properties have their own pre-defined meaning and are used by the system. For example, if a certain device has a property named "snmp.community", then access to this device will be allowed by a value of this property and not by the global value.
- **Addresses** present IP addresses of objects and can be in a dotted-decimal form with or without a mask, or in a FQDN form (Fully Qualified Domain Name). Addresses can refer to Devices, Ports or Locations. Addresses defined under Location present a part of the address space assigned to this Location.
- **Links** present connections between objects that reflect the computer network topology. Links are shown in the form of a tree with a chosen object on the root of the tree. Its children nodes are directly connected objects and each one can be further expanded in order to view next links and subsequent nodes.

2.4. Other concepts

Repository is a part of the data hierarchy that contains pre-defined objects. Objects in the repository are not active and serve for the purpose of copying and setting up in a part of the hierarchy where they want to be defined. This enables a user to define specific objects in one place that will be uniformly used in the data hierarchy. Repository typically contains various defined Monitors and Reports, with belonging RRD Charts, Alarms and Actions.

Repository initially contains a pre-defined, mostly used Monitors and reports, but the user has a possibility to define new objects in the Repository.

Recycle Bin presents a part of the system where all deleted data are placed. If needed, objects may be restored to the same place from which they were deleted. Once erased from the Recycle Bin, objects are permanently erased from the system. This concept offers the possibility of correcting user's mistakes, such as accidental erasure of a part of object hierarchy.

Tools present a part of the NetIIS system that defines pages which user can directly access, independent of the position in the data hierarchy.

Pre-defined Tools are:

- **Login** – presents a page for login to the NetIIS system via username and password
- **Alerts** – presents a page with all currently active bad alarms in the system. This page is refreshed in given time intervals and presents the most efficient way of current overview of critical events in the network.
- **Search** – presents a page for search of the data hierarchy. Search is possible with any object in the information system with reference of its name, address or properties.
- **Event log** – presents a page for an overview of all good and bad Alarms activated in the system and time when they became active. It is possible to search events by acuteness, by text in the Alarm message or by objects to which the Alarm and Monitor are defined (Ports or Devices).
- **Download Application** – presents a page from where the stand-alone application can be downloaded, following short installation instructions.
- **Syslog search** – presents a page for an overview and search of *Syslog* messages that NetIIS system received from networking devices. Search can be based on originated devices that sent the message or to the text of the message

3. USER INTERFACE

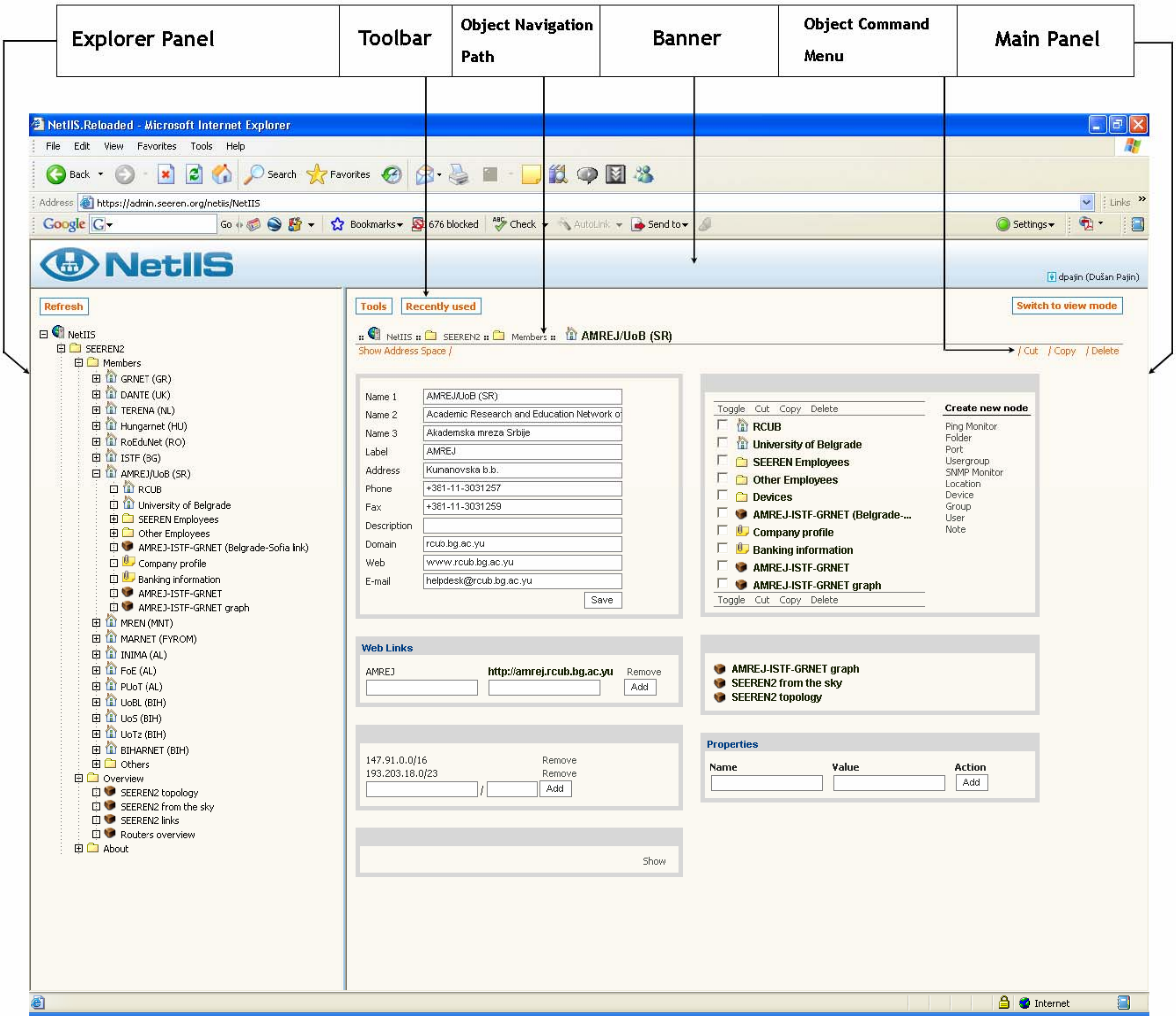
NetIIS web application is accessed via a standard *web browser*, independent of the operating system on the client computer, such as Window Explorer, Mozilla Firefox etc. This chapter will describe elements that form the user interface, principles of efficient overview and data alteration.

3.1. Elements of user interface

User interface of the NetIIS web application contains the following basic elements:

- Banner
- Toolbar
- Explorer panel
- Main panel
- Message panel
- Object Navigation Path
- Object Command Menu

The following picture shows the general appearance of the NetIIS environment with description of functional parts.



Name 1	AMREJ/UoB (SR)
Name 2	Academic Research and Education Network o
Name 3	Akademska mreza Srbije
Label	AMREJ
Address	Kumanovska b.b.
Phone	+381-11-3031257
Fax	+381-11-3031259
Description	
Domain	rcub.bg.ac.yu
Web	www.rcub.bg.ac.yu
E-mail	helpdesk@rcub.bg.ac.yu

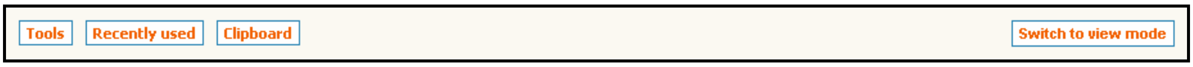
AMREJ http://amrej.rcub.bg.ac.yu

147.91.0.0/16
193.203.18.0/23

3.1.1. Banner

Banner is located on the top of the screen that contains the NetIIS logo on the left side and username of the logged user on the right side.

3.1.2. Toolbar



Toolbar is located on the central part under the banner and contains the following buttons:

- *Tools* – This button opens a menu with tools available to the user, according to configured permission. Predefined tools are: *Login*, *Alerts*, *Event Log*, *Search*, *Download Application*. Since the menu items are in form of HTTP links, new items (tools) can be added by NetIIS administrator using the client application.
- *Recently used* – This button opens a menu with recently used objects (up to ten), that can be directly accessed and reused.
- *Clipboard* – This button opens a menu with one or more objects as the result of previously performed *Cut* or *Copy* command.
- *Switch to view/edit mode* – This button changes current working mode (*View* and *Edit* mode).

3.1.3. Explorer panel

Explorer panel is located on the left side of the screen and contains the data structure presented by a tree. Tree contains data that is visible to the active (logged) user, i.e. objects with the *read* permissions for the user.

As with other similar structures, by clicking the '+' button in front of the object that presents the node in the tree, the belonging sub-tree will expand. A click on an object in the data hierarchy, selects an object and its information details are shown in the Main panel.

Refresh button on top of the panel refreshes the view of the element in the tree. This button is used if certain data is being changed or copied from one place to another, if the changes are not shown immediately.

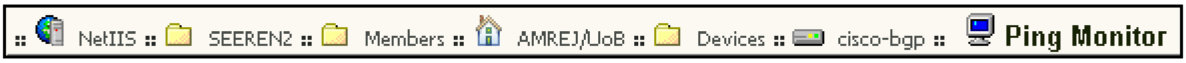
The Repository tree is shown separately below the data hierarchy tree.

3.1.4. Message panel

Message panel is shown below the Toolbar only in the case that NetIIS generates a certain message for the user. Examples of messages are results of some actions, typical for *AutoDiscovery* functions, or when a user is denied access to certain data due to lack of sufficient permissions.

3.1.5. Object Navigation Path

Object Navigation Path contains a path through the information system hierarchy to the current object that is shown. A click to any element in the hierarchy path switches to that element in the Main panel.


:: NetIIS :: SEEREN2 :: Members :: AMREJ/UoB :: Devices :: cisco-bgp :: Ping Monitor

3.1.6. Object Command Menu

Object Command Menu is located below the Object Navigation Path and contains commands that can be performed on that object. The commands are different for a *View* and *Edit* mode as well as for various types of objects.

For majority of objects following commands are available from the *View* mode:

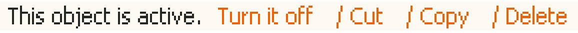
- *Show Address Space* – calls the search page of all IP addresses in the sub-tree of the current object

Especially for monitors following commands are available from the *View* mode:

- Show All Events – calls the Event Log page with selected current monitor, when all attached alarms are shown.
- *Execute* – executes the current monitor on the user request and refreshes the resulted values.

Following actions are available from the *Edit* mode:

- *Enable / Disable* – switching on and off current objects in the monitoring process, which is transmitted to the whole belonging sub-tree. By switching off an object, the entire sub-tree becomes inactive, and the objects within will not be executed by a monitoring process. This is useful if a monitor is to be temporarily aborted, without a need for permanent delete. Also if there is a planned disconnection of a device, switching off in the NetIIS will stop a number of alarm activations.
- *Cut*, *Copy*, *Paste*, *Delete* – usual editing functions on the level of an object. Function *Paste* will show if there is an object on the *Clipboard*.


This object is active. Turn it off / Cut / Copy / Delete

3.1.7. Main panel

Main panel uses a large part of the working space and it shows information on the selected object. Also, this panel shows pages for global tools (e.g. *Alerts*, *Event Log*, *Search*).

The Main panel is commonly used in View mode for viewing data of the current object, whilst the data alteration is performed from the *Edit* mode.

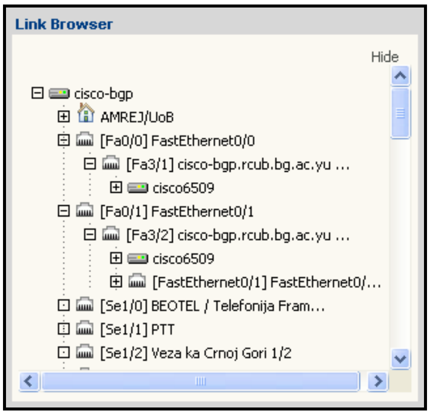
3.1.7.1. View mode

Presentation of object data in the Main panel depends on the type of the object. For majority of objects all relevant data is shown, divided into special boxes.

Boxes that are related to general concepts of objects, are:

- *Attributes box* – contains object attributes, but also general information on the object status, e.g. time of latest monitor execution.
- *Children box* – list of all belonging objects, sorted by type, where the mostly used types are placed on the top (groups, monitors, reports etc.). Content can be scrolled within the box.
- *Properties box* – list of adjoined properties (name and value) if such exists.
- *Addresses box* – list of adjoined IP address and mask, if such exists.

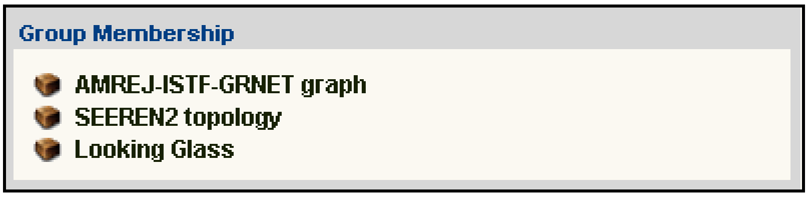
- *Link Browser box* – serves for link hierarchy view that presents the computer network topology. Overview is initially switched off, and it can be switched on by pressing the "Show" button. Links are shown in a tree, with current objects in the root of the tree. Sub-nodes in this tree are objects which are directly linked to the current object. Each node in the tree can be expanded showing other links (previously opened objects /links are not shown). The box can be suppressed by pressing the "*Hide*" button.



Link Browser

```
⊟ cisco-bgp
  ⊞ AMREJ/UoB
  ⊟ [Fa0/0] FastEthernet0/0
    ⊟ [Fa3/1] cisco-bgp.rcub.bg.ac.yu ...
      ⊞ cisco6509
  ⊟ [Fa0/1] FastEthernet0/1
    ⊟ [Fa3/2] cisco-bgp.rcub.bg.ac.yu ...
      ⊞ cisco6509
      ⊞ [FastEthernet0/1] FastEthernet0/...
  □ [Se1/0] BEOTEL / Telefonija Fram...
  □ [Se1/1] PTT
  □ [Se1/2] Veza ka Crnoj Gori 1/2
```

- *Group Membership box* – lists all groups that contain current objects. Click on each group name opens it, which gives a wider information context of the specific element.



Group Membership

- AMREJ-ISTF-GRNET graph
- SEEREN2 topology
- Looking Glass

- **Notes** - Notes attached to the current object are shown on the bottom of the Main panel in formatted text style.

Other boxes depend on the type of objects in the following way.

- Devices and Ports:

  Looking Glass box – The *Execute* button executes the selected command on the current router, while the *Telnet* button initiates a telnet session in a default program on the client working station.

- Ports:

  Trace box – The *Execute* button enlists all objects on the path from the master location to the remote location, followed by topological links.

- Monitors and Alarms:

  Monitor Variables box – shows current values of all Monitor variables. Variables marked with *hide* attribute are shown in a grey colour.

Groups and reports shown from the *View* mode is formatted in a way defined by these objects, either by a table or graph, which is separately described later in this chapter.

3.1.7.2. *Edit mode*

If a user should choose to work in *Edit* mode the main panel boxes will show information related to the current object in a format that is suitable for editing.

The user must have write permission over the current object in order to edit and change any data. Otherwise, the following message will appear on the message panel: *No write permission*.

Edit mode for individual boxes is described in the following paragraphs.

- *Attributes box, Address box, Properties box*

  Data editing in these boxes is performed in a text editing field. Additionally any line in the *Address box* and *Properties box* can be individually removed by performing the *Remove* command.

  In order to save the changes in the base, it is necessary to click on the *Save* button on the current box.

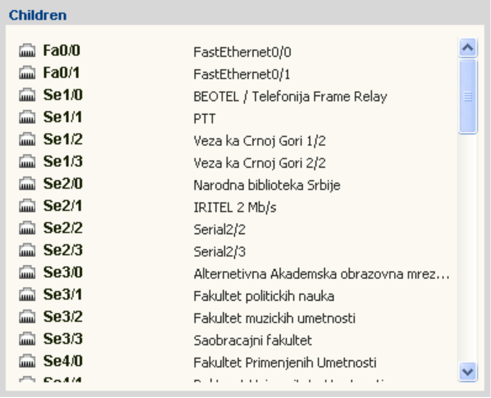
- *Children box*

  For each element of the *Children* box, *Edit* mode will show a *checkbox* for selecting objects and allow commands: *Toggle*, *Cut, Copy, Delete*.

  Toggle alternate selection and de-selection of all belonging objects, whilst *Cut, Copy, Delete* relates to all selected objects. All copied objects are kept in the *Clipboard* which can be viewed from the *Toolbar*. Adding objects to *Children* box is done on the level of current objects, on *Paste* command from the Object Command menu.

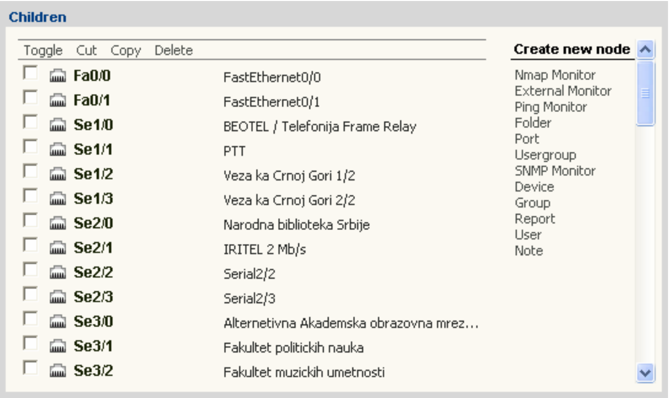
  Generally, combination of *Cut* and *Paste* buttons enables moving of objects, whilst a combination function *Copy* and *Paste* enables copying of objects.

  Apart from these functionalities there is a possibility of creating new objects with buttons located on the "*Create new node*" section. A list of object types that can be added is set in relation to the current object (e.g. for Monitors only Alarms, RRD Charts can be added).



Children

Fa0/0	FastEthernet0/0
Fa0/1	FastEthernet0/1
Se1/0	BEOTEL / Telefonija Frame Relay
Se1/1	PTT
Se1/2	Veza ka Crnoj Gori 1/2
Se1/3	Veza ka Crnoj Gori 2/2
Se2/0	Narodna biblioteka Srbije
Se2/1	IRITEL 2 Mb/s
Se2/2	Serial2/2
Se2/3	Serial2/3
Se3/0	Alternetivna Akademska obrazovna mrez...
Se3/1	Fakultet politickih nauka
Se3/2	Fakultet muzickih umetnosti
Se3/3	Saobracajni fakultet
Se4/0	Fakultet Primenjenih Umetnosti



Children

□	**Fa0/0**	FastEthernet0/0
□	**Fa0/1**	FastEthernet0/1
□	**Se1/0**	BEOTEL / Telefonija Frame Relay
□	**Se1/1**	PTT
□	**Se1/2**	Veza ka Crnoj Gori 1/2
□	**Se1/3**	Veza ka Crnoj Gori 2/2
□	**Se2/0**	Narodna biblioteka Srbije
□	**Se2/1**	IRITEL 2 Mb/s
□	**Se2/2**	Serial2/2
□	**Se2/3**	Serial2/3
□	**Se3/0**	Alternetivna Akademska obrazovna mrez...
□	**Se3/1**	Fakultet politickih nauka
□	**Se3/2**	Fakultet muzickih umetnosti

- *AutoDiscovery box*

  Activation of various types of *AutoDiscovery* functions related to the current object is possible only from the *Edit* mode. Optional properties are entered in the edit fields, whilst the result of the process is written on the Message panel.

- **Note Editor box**

  This box presents a simple text editor with basic formatting tools.

  While notes are shown in the View mode for the parent object, Note Editor box appears only when the Note is selected in the Edit mode.

3.2. Group view

Taking into consideration that basic function of the group is joining chosen objects for the purpose of their view, this chapter describes in detail the group view with the element of user interface that is available.

Groups are shown depending on the type of the group, which can be: *Simple Group*, *Graph* and *Looking Glass*.

3.2.1. Simple Group

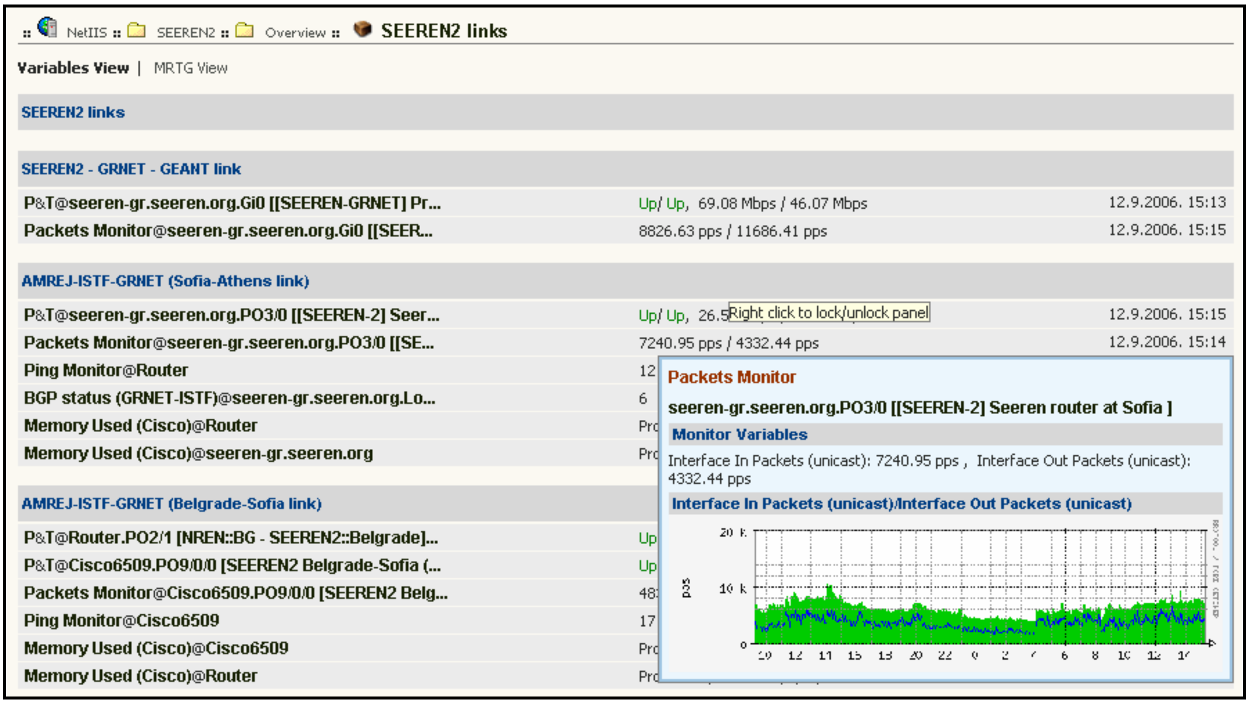
Simple Group serves for showing elements in a table form. They are usually used for joining monitor elements and show current status. Nesting of groups is possible, i.e. one group can have other groups as including elements.

Two outputs are supported for Simple Groups:

- **Variables View** shows textual information of all sub-groups and their individual elements in the order of appearance in table format.

  A click on individual sub-groups gives an overview of this group. Belonging elements are shown in separated rows. An exception is given to Port and Traffic Monitors, which are defined on the same port, and for a simpler overview they are shown in one row, labelled with "P&T".

  Monitors in a group are shown in the first column in the following syntax: "*Monitor@Device.Port [port description]*".



:: NetIIS :: SEEREN2 :: Overview :: SEEREN2 links

Variables View | MRTG View

SEEREN2 links

SEEREN2 - GRNET - GEANT link

P&T@seeren-gr.seeren.org.Gi0 [[SEEREN-GRNET] Pr...	Up/ Up, 69.08 Mbps / 46.07 Mbps	12.9.2006. 15:13
Packets Monitor@seeren-gr.seeren.org.Gi0 [[SEER...	8826.63 pps / 11686.41 pps	12.9.2006. 15:15

AMREJ-ISTF-GRNET (Sofia-Athens link)

P&T@seeren-gr.seeren.org.PO3/0 [[SEEREN-2] Seer...	Up/ Up, 26.5	12.9.2006. 15:15
Packets Monitor@seeren-gr.seeren.org.PO3/0 [[SE...	7240.95 pps / 4332.44 pps	12.9.2006. 15:14
Ping Monitor@Router	12	
BGP status (GRNET-ISTF)@seeren-gr.seeren.org.Lo...	6	
Memory Used (Cisco)@Router	Pro	
Memory Used (Cisco)@seeren-gr.seeren.org	Pro	

AMREJ-ISTF-GRNET (Belgrade-Sofia link)

P&T@Router.PO2/1 [NREN::BG - SEEREN2::Belgrade]...	Up
P&T@Cisco6509.PO9/0/0 [SEEREN2 Belgrade-Sofia (...	Up
Packets Monitor@Cisco6509.PO9/0/0 [SEEREN2 Belg...	48
Ping Monitor@Cisco6509	17
Memory Used (Cisco)@Cisco6509	Pro
Memory Used (Cisco)@Router	Pro

Right click to lock/unlock panel

Packets Monitor

seeren-gr.seeren.org.PO3/0 [[SEEREN-2] Seeren router at Sofia]

Monitor Variables

Interface In Packets (unicast): 7240.95 pps , Interface Out Packets (unicast): 4332.44 pps

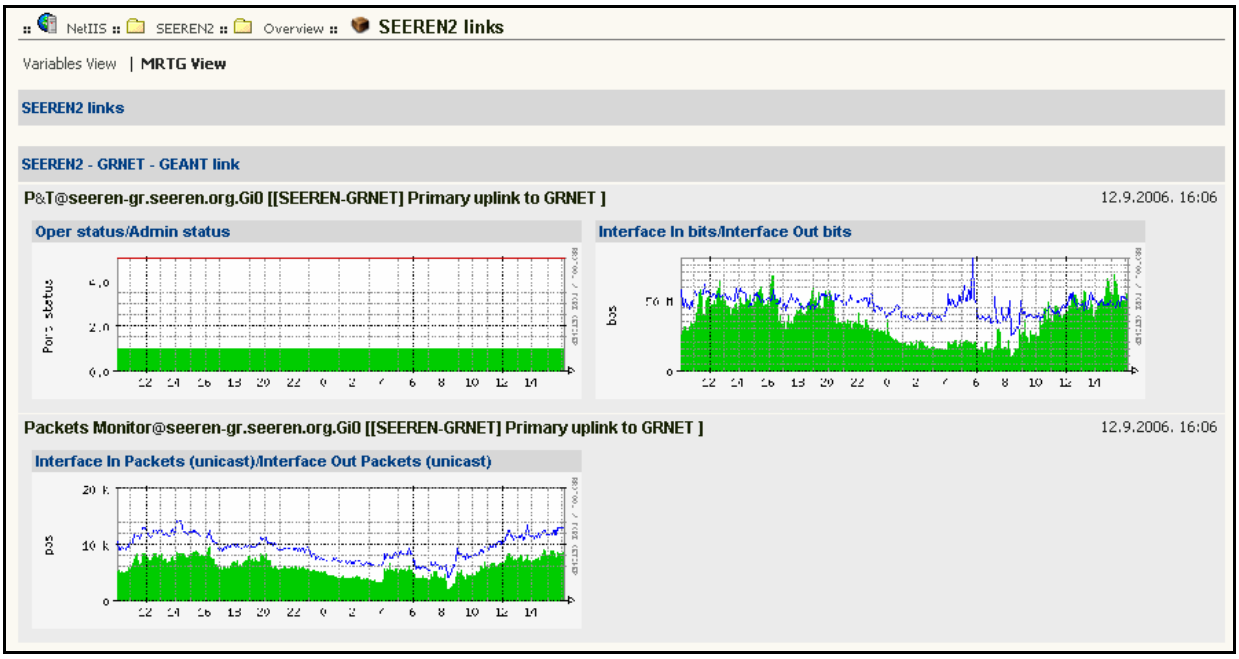
Interface In Packets (unicast)/Interface Out Packets (unicast)

The second column shows current values of the Monitor. Pointing a cursor over this column will automatically open a *pop-up* window, which shows more detailed information with daily RRD Chart, if such are defined by the Monitor.

Pop-up window can be frozen with the right button on the mouse.

Elements in the table and the pop-up windows contain HTTP links to an overview of these objects (Monitors, Devices, Ports, RRD Charts).

- **RRD Charts View** shows daily RRD Charts for the Monitors in the current Group. A click on the charts opens the page with a daily, weekly, monthly and annual chart for selected RRD Chart object.



:: NetIIS :: SEEREN2 :: Overview :: SEEREN2 links

Variables View | **MRTG View**

SEEREN2 links

SEEREN2 - GRNET - GEANT link

P&T@seeren-gr.seeren.org.Gi0 [[SEEREN-GRNET] Primary uplink to GRNET] 12.9.2006. 16:06

Oper status/Admin status

Interface In bits/Interface Out bits

Packets Monitor@seeren-gr.seeren.org.Gi0 [[SEEREN-GRNET] Primary uplink to GRNET] 12.9.2006. 16:06

Interface In Packets (unicast)/Interface Out Packets (unicast)

Variables View is the default mode, while switching from one mode to another is performed from the Object Command menu (*Variables View* or *RRD View*).

In Edit mode, only Children box is shown for the current Group, with an ability to delete, cut, copy or paste objects.

3.2.2. Graphs

Graphs present special type of Group object, which serves for descriptive visual illustration of the topology of belonging elements with clearly marked statuses of individual links and devices.

Presenting graphs as Group objects enables joining of arbitrary objects for a graphical overview. Each type of object has a pre-defined icon, while individual sub-types of objects or individual objects can have a newly assigned icon.

NetIIS system shows direct or indirect links between objects in the group on the basis of link topology. The links are represented as bidirectional arrows. If monitors are added into graphs, their statuses can be marked with red and green colours.

A point with a cursor over a link or object will open a pop-up window with daily RRD Chart of the including monitor, if it is included in the group. For a more detail overview of RRD Chart it is necessary to quickly point over the pop-up window, and then click on the chart that needs to be seen in more detail.

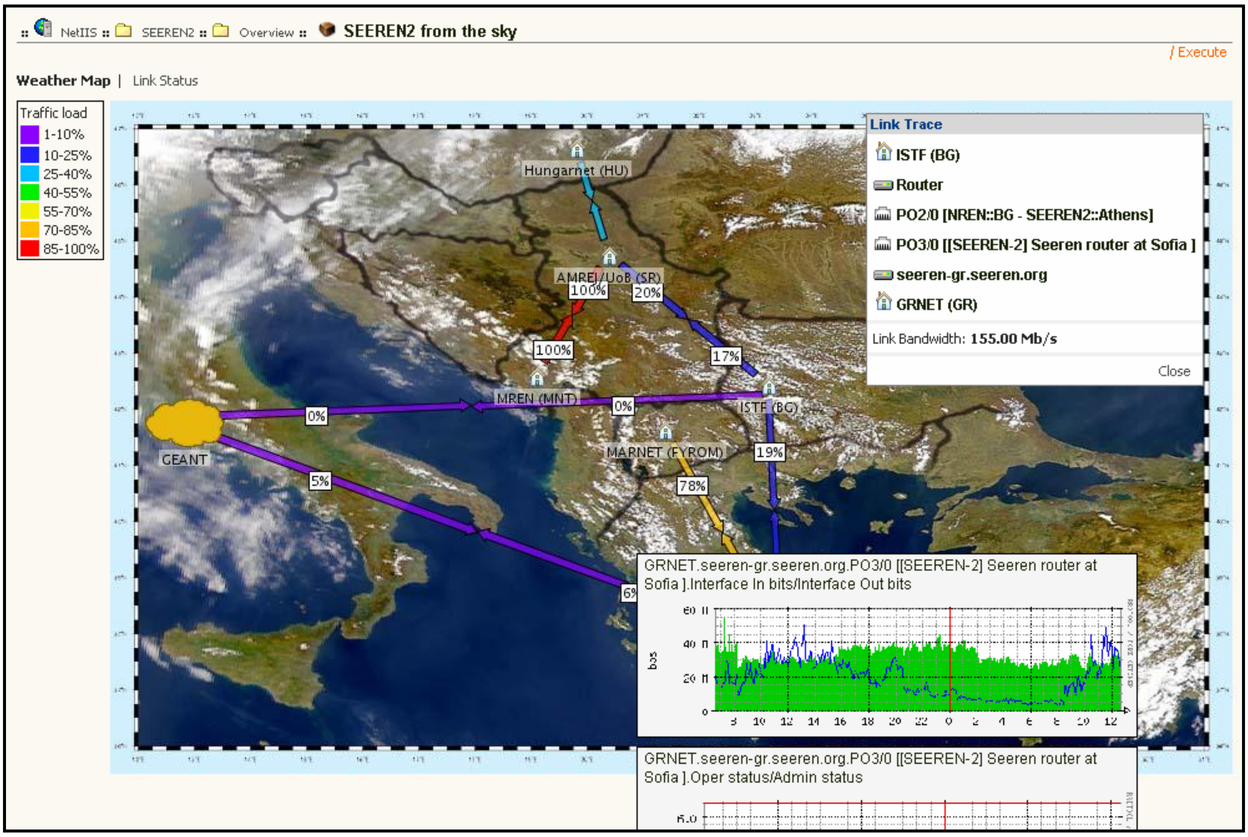
A click on an object, a *pop*-up window appears showing it's basic information, whilst another click opens the Main panel for a chosen object.

A click on a certain link (arrow) opens the *Link Trace* window that shows all objects that are located on this link. This illustration is useful in order to get an overview of all ports and other eventual devices between two connected objects. Pointing a cursor over the object in the *Link Trace* window will show all daily RRD charts defined on a particular object. A click on the object in this window will switch to a detailed overview of the object in the Main panel. The *Link Trace* window will also show the link bandwidth. The window is closed on the *Close* button.

Apart from these general features, the graphs have two output forms: *Weather Map* and *Link Status*.

- *Weather Map* output aims to show current traffic flow on links, which is visually marked with various colours. The system automatically gets and shows Traffic Monitors on the path between two objects. If there are more Traffic monitors on the link or more links between two objects, user can choose which one is taken into consideration by adding the Monitor in the group. The traffic intensity is shown as a capacity occupancy percentage. If an Alarm is active, the associated link will be marked with an "explosion" on the graph.
- *Link Status* output aims to show current link status depending on the alarm status of corresponding port monitors. If the state of the monitor is *Up*, link will be presented with a green colour, and if the state of the monitor is *Down*, link will be presented with a red colour.

  Note. Creating graphs is possible only from the graph editor using the stand-alone client application. Objects position can be setup form this graph editor, as well as special attributes and parameters. This manual describes the way of graph output and their use via Web interface.



Link Trace

ISTF (BG)

Router

PO2/0 [NREN::BG - SEEREN2::Athens]

PO3/0 [[SEEREN-2] Seeren router at Sofia]

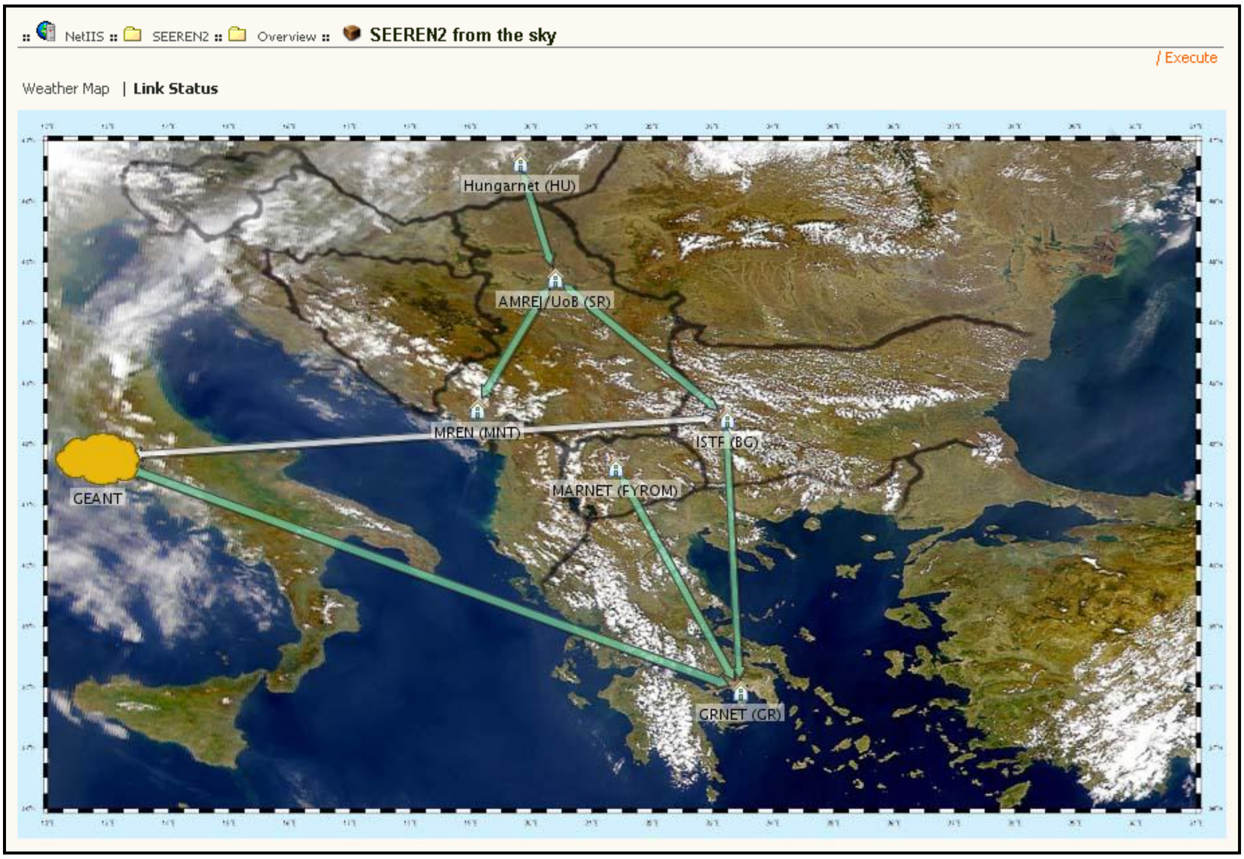
seeren-gr.seeren.org

GRNET (GR)

Link Bandwidth: 155.00 Mb/s

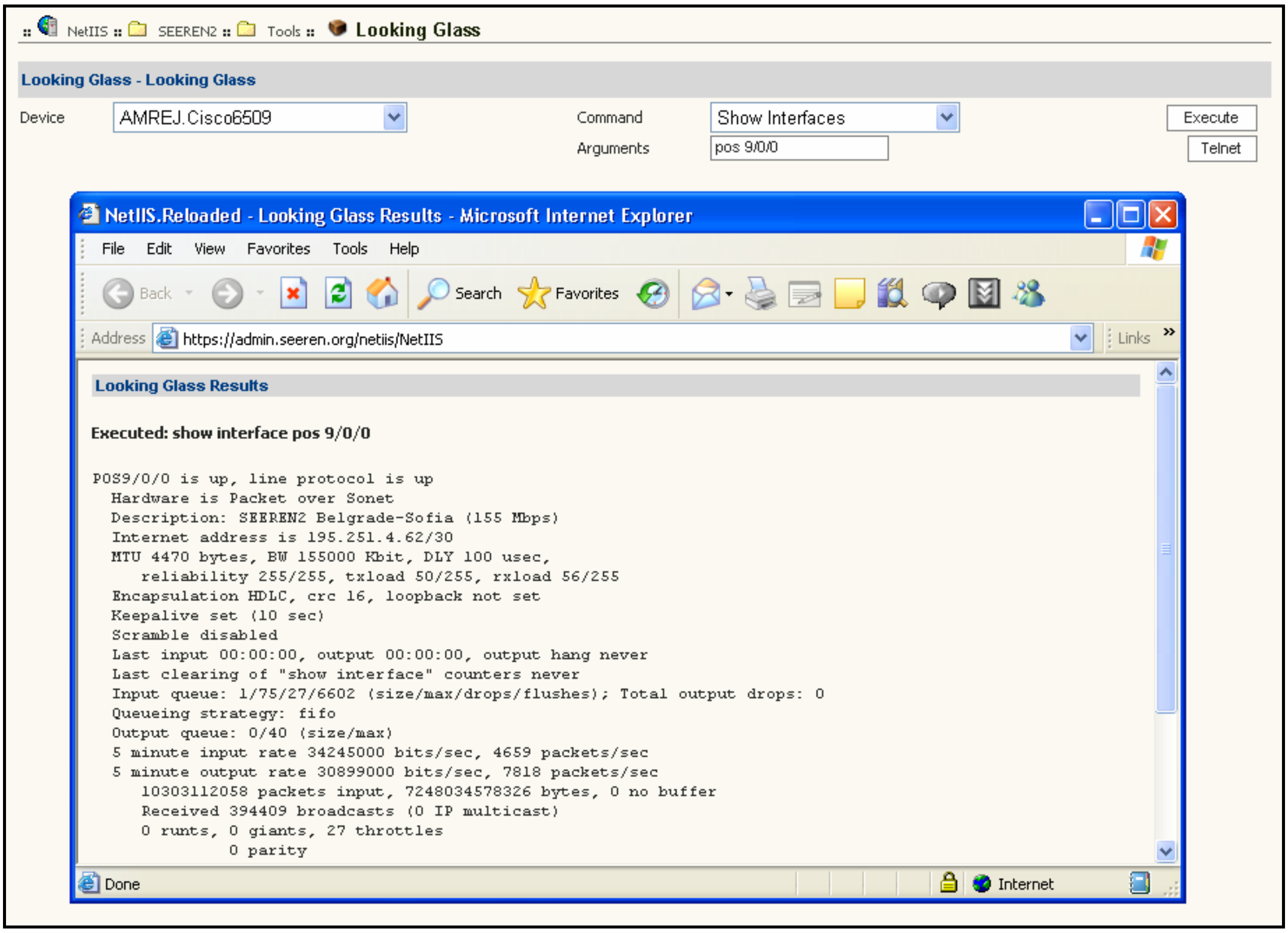
GRNET.seeren-gr.seeren.org.PO3/0 [[SEEREN-2] Seeren router at Sofia].Interface In bits/Interface Out bits

GRNET.seeren-gr.seeren.org.PO3/0 [[SEEREN-2] Seeren router at Sofia].Oper status/Admin status



3.2.3. Looking Glass

Special group of **Looking Glass** type collects all devices which are allowed for a remote command execution, so-called Looking Glass functionality. The only functional difference in relation to the *Looking Glass box* in the Main panel is reflected in a specific choice of devices from the group to which the selected command is to be performed.


:: NetIIS :: SEEREN2 :: Tools :: Looking Glass
Looking Glass - Looking Glass
Execute
Telnet
NetIIS.Reloaded - Looking Glass Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Links
Done
Internet

Device: AMREJ.Cisco6509

Command: Show Interfaces

Arguments: pos 9/0/0

Address: https://admin.seeren.org/netiis/NetIIS

Looking Glass Results

Executed: show interface pos 9/0/0

```
POS9/0/0 is up, line protocol is up
  Hardware is Packet over Sonet
  Description: SEEREN2 Belgrade-Sofia (155 Mbps)
  Internet address is 195.251.4.62/30
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
     reliability 255/255, txload 50/255, rxload 56/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Scramble disabled
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 1/75/27/6602 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 34245000 bits/sec, 4659 packets/sec
  5 minute output rate 30899000 bits/sec, 7818 packets/sec
     10303112058 packets input, 7248034578326 bytes, 0 no buffer
     Received 394409 broadcasts (0 IP multicast)
     0 runts, 0 giants, 27 throttles
              0 parity
```

4. MONITORING SYSTEM

4.1. Basics on Monitors

Monitors present basic elements of the monitoring system that permanently perform measurement in the computer network. This chapter describes basic concepts and typically used predefined Monitors.

Monitors can be configured on Devices or Ports and in that context are executed. In both cases, for device access the monitor will primarily take the IP address of the device, and if such doesn't exist, it will try with the IP address of the Port.

In the View mode the following description is given to Monitors: basic information on their execution and defined variables from the latest read values. Variables are shown with an indexed number, and a specific variable with an indexed zero shows the status of the monitor: status *true* signifies regular performance; whilst the status *false* signifies that the monitor is not being regularly performed (e.g. the device is not available). Variables show current values. Values of minor interest or that serve as mid-value for calculating more complex variables (e.g. occupancy percentage), are marked with a grey colour and they are not shown in the Groups.

Monitors can be executed on the user demand by clicking the command *Execute* on the Object Command menu.

Following actions can be executed in the Edit mode:

- Enabling and disabling Monitors – This serves for temporary abortion of the Monitor performance, with a possibility of reactivation. The current status is marked in Object Command menu in front of the command button ("*This object is enabled*" / "*This object is disabled*").
- Change of time period of monitoring execution and the length of the time-out interval. Time-out interval presents time period in which the monitor waits for the result. If the monitor does not receive a result in the given time interval, it will presume that the result cannot be returned.
- Cut/Copy/Paste/Delete on the level of the current monitor
- Add/Cut/Copy/Paste/Delete on the level of including objects

4.2. Types of monitors

Basic types of monitors are:

- SNMP monitor
- Port monitor
- Traffic monitor
- Ping monitor
- NMAP monitor
- External monitor

Apart from the above mentioned, pre-defined and often used SNMP monitors can also be:

- Packets monitor
- BGP monitor
- CPU Load Monitor
- System Memory Monitor

4.2.1. SNMP Monitor

SNMP Monitor allows measurement of arbitrary SNMP variables (*Simple Network Management Protocol*), so-called OID (*Object Identifier*). If a device supports SNMP, then it is possible to get various information on device functioning and its services. OID databases, so-called MIBs (*Management Information Base*) are either globally standardised or defined by the device manufacturer.

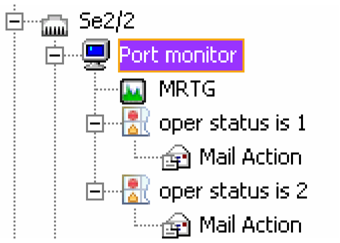
For example, it is possible to overview the network device processor and system memory usage, as well as usage of the storage system.

In the case that the variable refers to the lists of objects, e.g. to all router interfaces or all storage partitions, a list of ID values are added to OID. Adequate values are being accessed via indexes that are joined to all objects in the list. These indexes are called SNMP ID. In the network interface instance this is the most important information, since other data is being accessed and retrieved via this index.

The OIDs which user wants to get are configured as Monitor variables. In the case that the Monitor is defined on an interface, the interface SNMP ID will be automatically added as the suffix to the applied OID. Apart from SNMP ID of the interface, some OID variables require additional specification in the form of suffix to its identifier (OID). For example, it can be an IP address of BPG peer or DLCI identifier of the Frame Relay port. Thus, on the level of monitor variable, it is allowed to insert desirable suffix that will enable access to the correct SNMP data.

> **Note:** SNMP monitor is defined from the client application, while from the web interface, user can copy and paste already configured SNMP Monitors.
>
> **Note:** In the case that only one variable is wrongly defined, SNMP Monitor will return the fault and will not give values for any other variable. This will be marked with a message "*Value not assigned*".

4.2.2. Port Monitor



Port Monitor is a Monitor that overviews administrative and operational status of the network device interfaces to which it is defined. Port Monitor is actually a special SNMP monitor, where the administrative and operational statuses are presented with a standard SNMP OID, that is defined with monitor variables (*var(1)* and *var(2)*).

Administrative status presents the desired status of the interface, i.e. whether it is configured (*Up*) and can have the following values:

Administrative port status		
Value	Status	Description
1	Up	Administratively up port
2	Down	Administratively down port (*shutdown*)
3	Testing	Port is in the test status, packets cannot pass through

Operational status presents the current operative status of the interface and can have the following values:

Operational port status		
Value	Status	Description
1	Up	Port is working properly, traffic can be transmitted
2	Down	Port is not working properly, traffic cannot be transmitted
3	Testing	Port is in the test status, packets cannot pass through
4	Unknown	Unknown status
5	Dormant	Port is waiting for the dial-up connection
6	NotPresent	Modular port is not physically installed
7	LowerLayerDown	Port is *down* due to the status of lower layer logical port

If the administrative status is *Down*, operation status will also be *Down*. If the operational status is *Up*, the link is physically correct and works from end to end on the layer 2 (i.e. port receives a *keepalive* packets from the peer device).

Usual values are *Up/Up* for a properly working line, *Up/Down* for a malfunctioning link.

> **Note:** Administrative and operational statuses are similar, but not entirely equivalent to the status that is returned from the *show interface* command on Cisco devices. Result of this command is textual, which refers to the port status on the first (physical) and second (*data-link*) level and *Up/Down* statuses can have additional information (e.g. *Looped*).

Port Monitor contains predefined RRD Chart that collect time statistics for administrative and operational statuses.

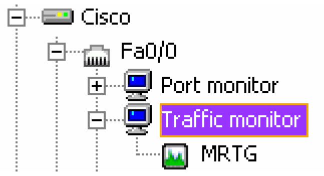
Port Monitor contains two Alarms that are related to the operational status (but does not include the administrative status!):

- *Good Alarm* – checks whether the operational status is equal to the value 1 (*Up*), i.e. the condition for activation is defined with the expression: "**var(2) == 1**". Included message is: "Link is UP". Alarm contains the *Mail action* object with the same message.
- *Bad Alarm* – checks whether the operational status is different from value 2 (*Down*), i.e. the condition for activation is defined with the phrase: "**var(2) != 1**". Included

message is: "Link is DOWN". Alarm contains the *Mail action* object with the same message.

Note: For the Bad Alarm criteria, it is possible to use the comparison with the value 2 ("var(2) == 2"). Still, it has to be taken into consideration that the condition will not be fulfilled if the device is unreachable, which will result to null value. This can be a desirable action for monitoring remote ports, when it can avoid alarming all remote links when the local link is down. Also, criteria "different from 1" is an absolutely inverted statement of Good Alarm, assuring that Alarms are paired.

4.2.3. Traffic Monitor



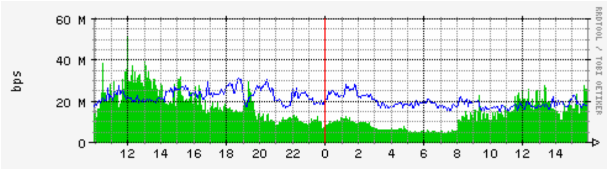
Traffic Monitor is a specifically defined SNMP Monitor that measures data traffic through the network interface on which it is defined.

First two variables, *var(1)* and *var(2)*, are defined with standard, counter type OIDs, which are monitoring the total number of input/output bytes on the interface. Data flow, in bytes per second (Bps) unit, is calculated when the current status of the counter is subtracted from the previously counter status and divided with the time elapsed between the two readings.

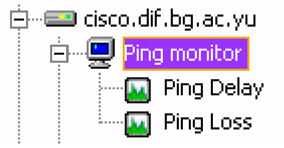
Other two variables, var(3) and var(4), are composite and measure the input and output data flow in bits per second (bps) unit, which is calculated from variables 1 and 2 and multiplying with 8. These are the values of interest to the user and they are shown in groups of monitors in kbps, Mbps or Gbps units.

Belonging RRD Chart refers to variables 3 and 4. The input traffic is shown with a green colour, while the output traffic is shown in a blue colour.

Although, the initial Traffic monitor does not contain alarms, they can be set up to react to certain traffic intensity. In certain cases it is useful to be alarmed for unusually low traffic, which can indicate possible routing problems.



4.2.4. Ping Monitor



Ping Monitor is a Monitor that executes native ICMP *ping* service towards a device on which it is defined and measures the results of this command, i.e. packet delay and percentage of lost packets.

By placing the monitor to a device, NetIIS server sends *ping* packets towards the device, in defined time intervals. Monitor can receive the following values as execution results:

Variables	Description
var(1)	*Minimum RTT* (*Round Trip Time*) – minimum delay
var(2)	*Maximum RTT* (*Round Trip Time*) – maximum delay
var(3)	*Average RTT* (*Round Trip Time*) – average delay
var(4)	*Sent Packets* – number of sent packets
var(5)	*Received Packets* – number of received packets
var(6)	*Packet Loss* – percent of lost packets (100* var(5)/var(4))

Ping Monitor usually includes two RRD Chart objects. One RRD Chart measures the minimum and maximum delay of *ping* packets (var(1) and var(2)), and the second RRD Chart measures the percentage of lost packets (var(6)).

Within the Ping monitor it is possible to adjust the number of packets that are to be sent to the device and their size in bytes. If the time of monitor performance is additionally decreased, it is possible to overload the link with intensive ping messages in the aim of monitoring its quality. It has to be taken into consideration that additional traffic has been added to the network, which can disrupt the normal traffic flow.

4.2.5. NMAP Monitor

NMAP Monitor checks whether certain TCP or UDP ports are available on the network device, measuring the basic statuses of network services. The testing is done via native NMAP command on the NetIIS server. Monitor returns *var(1)*, and when the value is *true* it means that the port is open, while *false* means that the port is closed. RRD Chart draws two values: the value of 1 when the port is open and the value of 0 when the port is closed.

Alarms for events can be created on the Monitor when the port is open or closed, and certain Actions can be added.

4.2.6. External Monitor

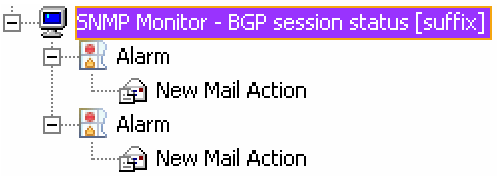
External Monitor is a Monitor that performs an arbitrary external command or a certain program on the operating system and checks the resulting values. It is possible to develop special programs or scripts, so-called *Agents* that take specific measures and actions.

External Monitor, as any other Monitor, can contain Alarms and RRD Charts.

4.2.7. Packet Monitor

Packet Monitor is a Monitor that measures packets flow on the interface in a similar way to Traffic Monitor. Packet Monitor is very useful in the case of detecting anomalies in the network traffic. In the case of *DoS* attack or an attempt of virus expansion on the network, the network traffic (in bps) does not have to rise, but it will increase the number of packets, so it can be easily detected with this type of monitor. RRD can be attached to the monitor.

4.2.8. BGP Monitor



BGP Monitor is a SNMP Monitor defined in the Repository that measures the status of individual BGP sessions via standardised OID variables, when this type of external routing protocol is used in the network.

BGP monitor is defined on the device whose BGP sessions are being monitored.

> **Note:** Although it can be setup on any Port or directly on the Device object, a good practice is a BGP Monitor installed on the Port that is defined as the local *peer* in the BGP session (e.g. *loopback* interface). It is recommended that names of monitors include information on the session that is being observed.

Monitor in variable *var(1)* returns the current status of the session with certain *peer*. BGP session can be in various states during the establishment session and values the OID returns are shown in the following table:

Value	State	Description
1	*Idle*	Session has not been configured
2	*Connect*	Attempt to connect, session still not established
3	*Active*	Attempt to establish session, session still not established
4	*OpenSent*	Request for connection sent, session still not established
5	*OpenConfirm*	Answer for request received, session still not established
6	*Established*	Session successfully established

Only the *Established* state (value 6) means that the BGP session is entirely established with the peer router and the BGP prefixes exchanged.

BGP Monitor contains Bad and Good Alarms that compare variable *var(1)* with the value of 6. Alarms have correspondent *Mail Action* objects for informing user groups via email. Monitor also contains the RRD Chart referred to variable 1.

> **Note**: Copying BGP Monitors to the desired Device or Port is not sufficient. In the Monitor Variables box, in Edit mode it is necessary to insert an IP address of the BGP peer as SNMP OID suffix. This suffix is added to the configured OID, which is jointly used as identifier for accessing the SNMP data on the device.

4.2.9. CPU Load Monitor

CPU Load Monitor measures three variables, the processor utilization in time intervals of 5s, 1min and 5min. Correspondent OID's are not standardised, they are specified exclusively for Cisco devices and belong to the MIB hierarchy of the Cisco Systems. The including RRD Chart refers to the variable *var(2)*, for processor utilization in the time interval of 1min.

> **Note:** For devices of other manufacturers it is possible to define similar monitors if correspondent information is supported by SNMP.

4.2.10. System Memory Monitor

System Memory Monitor measures more variables, specified exclusively for Cisco devices, and requests input of suffixes to the defined OIDs. Namely, Cisco devices return the information of the usage on part of the system memory that is being given to the processor and part that is given to the interfaces for queuing. Processor memory on all Cisco devices has a suffix .1, while interface memory has a suffix .2, .3 or even higher value that varies for every device. This Monitor is made so that it simultaneously measures usage of 2 memory parts. Cisco devices return the information on the used and free memory in bytes, while the NetIIS system calculates the amount of free memory in percentage. The table shows the list of variables.

Variables	Description
var(1)	*Memory Name* - memory name that is being monitored
var(2)	*Used Memory* (*suffix*) – used memory in bytes
var(3)	*Free Memory* (*suffix*) – free memory in bytes
var(4)	*Used Memory* – free memory in percentage 100 * var(2) / (var(2) + var(3))
var(5)	*Memory Name* – memory name that is being monitored
var(6)	*Used Memory* (*suffix*) – used memory in bytes
var(7)	*Free Memory* (*suffix*) – free memory in bytes
var(8)	*Used Memory* – free memory in percentage 100 * var(6) / (var(6) + var(7))

RRD Chart refers to variables var(4) and var(8), i.e. the memory usage in percentage.

> **Note**: In the case that only one OID variable is not correctly defined, all variables will have the undefined values. Typical mistake is un-harmonized suffix with the memory index that the device returns. In this case it is recommended list SNMP data that the device returns in this part of the MIB tree, either using *snmpwalk* command or adequate MIB browser.

4.3. Alarms

Alarms are objects that are optionally defined on Monitors in the aim of observing Monitor values and comparing them with configured thresholds.

State of the alarm signifies that the alarm condition is currently fulfilled or not, and can have a value *On* or *Off*. *Bad* alarm in the *On* status is called **Active Alarm** and it signifies existing failures in the network. The "*Alerts*" page in *Tools* menu shows all Active Alarms. Good alarms are usually not called "active", since they show desired and normal state in the network.

Alarms can be temporarily aborted on *Disable* command from the Object Command menu and re-activation on *Enable* command. The operational status of current Alarm is given in the Attribute box (*Enabled* or *Disabled*).

Alarms have the following attributes that can be configured from the Edit mode:

- **Name**. Although it is possible to choose an arbitrary name for the alarm, it is advised to have a uniform and generic name. Since Alarms are always shown in the context of Monitors over certain Devices or Ports, it is sufficient to distinguish Alarms within the same Monitor. Usual names are "*Good Alarm*" and "*Bad Alarm*", which can be changed if necessary.
- **Condition**. It presents a logical expression with the variables assigned to a Monitor over which the alarms are defined (not other Monitors), in syntax: var(1), var(2) etc.

  The following operations are supported: "==", "!=", "<", "<=", ">",">=", as well as the following logical operations: "OR", "AND", "NOT".

  Example: Conditions for detecting unusually low traffic on the traffic monitor:

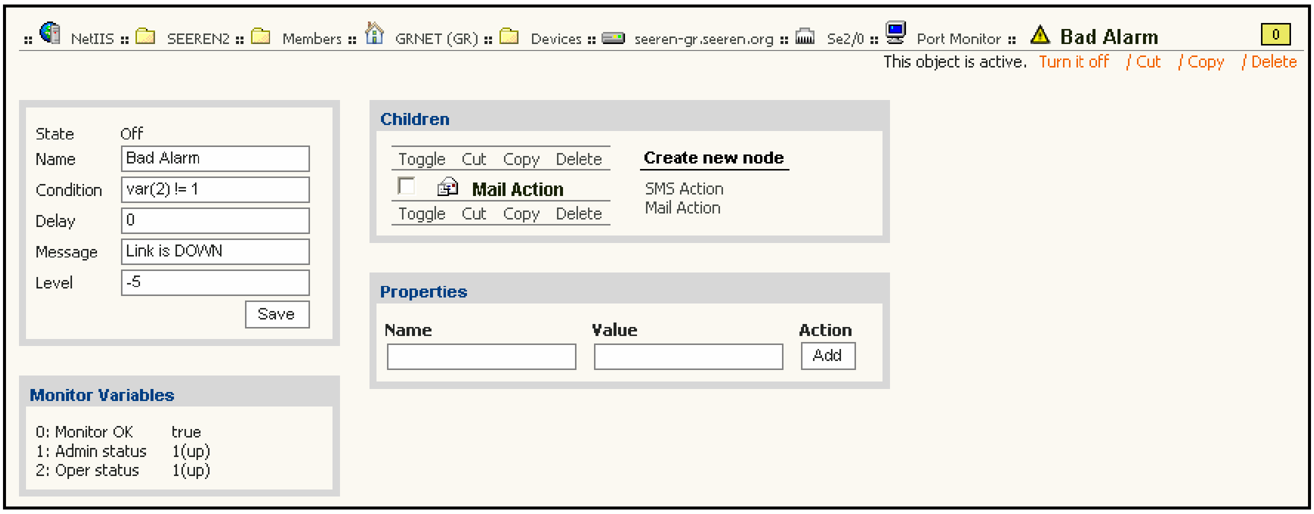
  "var(3) < 100000 OR var(4) < 100000"
- **Delay**. This property presents values in seconds, for what time the Alarm conditions must be true in order to activate the action). This option offers the possibility for the Alarm to return to the "good" state and to avoid alarming and action service for short-term failures that are not of interest. Those short activations will not be registered in the Event Log.
- **Message**. Message that is written in the Event Log. This is not a message sent to the user via email or SMS service.

  Note: It is of particular recommendation that messages should be of uniform and general type, e.g. "*Link is DOWN*". Together with this message a list of referring Monitor and object names are attached – description and name of Ports, Devices and related Locations, this gives enough information for describing the problem. Otherwise, if the message also describes the monitored object, such as "*Telecom link is DOWN*", during Monitor copying for each alarm instance it is necessary to change this message and readjust it. There is a big possibility that the system will, after a certain period of time become inconsistent. The wrong message will only confuse the user and bring distrust in the most significant function of the monitoring system - *failure notification*.
- **Level**. This property presents the critical level of the Alarm in the range from -10 to +10. Negative and positive value is determined whether the Alarm is "bad" or "good", while the numeric value determines its importance to the user. Greater absolute value determines larger acuteness, which is shown in intensive red or green colour, depending whether the Alarm is "bad" or "good". This value and colour is shown on Alarms pages (*Alerts*, *Event Log*, monitor groups etc.).

  Note: Recommendation for this value is to show the real importance of the alarm, not just for sake of notification, but for the possibility of search and event filtering in the *Event Log* page.

Alarms activation event (changing to the state *On*) will be shown in the *Event Log*. This event will also be registered during the first execution of the newly created alarm.

Additional notification of the user on the Alarm activation is performed by Action objects.



:: NetIIS :: SEEREN2 :: Members :: GRNET (GR) :: Devices :: seeren-gr.seeren.org :: Se2/0 :: Port Monitor :: **Bad Alarm** 0

This object is active. Turn it off / Cut / Copy / Delete

State	Off
Name	Bad Alarm
Condition	var(2) != 1
Delay	0
Message	Link is DOWN
Level	-5

Save

Monitor Variables

0: Monitor OK	true
1: Admin status	1(up)
2: Oper status	1(up)

Children

Toggle Cut Copy Delete

□ **Mail Action**

Toggle Cut Copy Delete

Create new node

SMS Action
Mail Action

Properties

Name	Value	Action
		Add

4.4. Action

This object represents an action that can be executed upon the activation of the Alarm. Two types of Action object are supported.

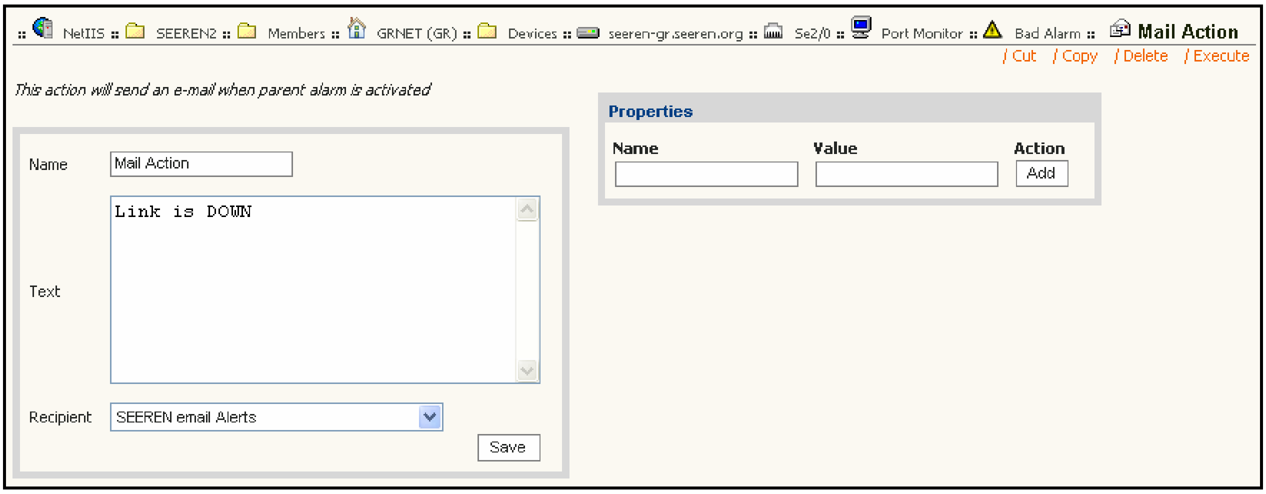
- Mail Action, sending e-mail messages to a selected User of User group
- SMS Action, sending SMS messages to a selected User of User group

Actions have following attributes that can be configured from the Edit mode:

- **Name**. It is possible to enter an arbitrary name of Action.
- **Text**. Arbitrary text that is sent via email or SMS service.
- **Recipient**. Recipient that the message is sent to, chosen from the list of existing users or user groups.

Since Alarm activation is always registered in the *Event Log*, there is no special type of action for this event.

> **Note**: Only one recipient can be chosen for one Action, i.e. individual User or User groups. If the message should be sent to another User, which should not be included to the chosen User group, in this case instead of creating a new User group for this instance, it is recommended to add a new Action to chosen recipient (*copy/paste* in the Children box of the Alarm).



:: NetIIS :: SEEREN2 :: Members :: GRNET (GR) :: Devices :: seeren-gr.seeren.org :: Se2/0 :: Port Monitor :: Bad Alarm :: **Mail Action**

/ Cut / Copy / Delete / Execute

This action will send an e-mail when parent alarm is activated

Name	Mail Action
Text	Link is DOWN
Recipient	SEEREN email Alerts

Save

Properties

Name	Value	Action
		Add

4.5. RRD Chart

RRD Chart is defined within the monitor, with an aim to archive values of monitors' variables during a certain time interval and to draw these values in the chosen time interval.

RRD Charts have up to two variables for measuring. These variables refer to any variables of the parent Monitor and should be distinguished. The first RRD Chart variable is shown in green colour as an area, while the second variable is shown in the blue line.

RRD Chart can be shown in two ways. RRD graphs from the View mode opens the page with 4 graphs with different time periods to the observed moment: daily, weekly, monthly and yearly. Link on the top, opens the page in traditional MRTG format. The page title will be automatically created on the basis of the name and description of the element to which the RRD graph is created. For example, a description and name of the Port will be shown, with the name of the Device and the name of the related Location.

The alternative way of showing RRD chart is performed from many pages, where individual objects are sensitive to the cursor. That is when temporary pop-up windows are opened with current daily RRD Chart.

> **Note**: It is recommended for first RRD Chart variable to address the monitor variable which can have short changes (peaks), since their area output is clearer rather than a line. For this reason, although the operative status is the second variable of the Port Monitor, it is defined as the first variable of the RRD Chart.

Collecting and archiving variable values is executed in 5 minute intervals, while monitors can be executed in a shorter time interval (e.g. 1 minute). Ways in which the system treats various values of executing monitors inside the interval of RRD Chart, and which value will be given to the RRD Chart is defined with the following options of the RRD graph variable:

- *Keep Maximum* - RRD Chart takes the maximum value
- *Keep Minimum* - RRD Chart takes the minimum value
- *Keep none* - RRD Chart takes the latest value.

> **Note**: For Port Monitor variables it is necessary to select the *Keep Maximum* option. RRD Chart will then take the maximum value for all executing monitors in the last 5 minutes and in that way it will register short-term connection failures during this period, i.e. changes in the operational status form 1 to 2 and back to 1.

Attributes that can be setup on RRD Chart type of objects are taken from the traditional MRTG tools.

- **Max Value** – Presents the maximum value of the variable. Larger value than this one will be archived and will not be shown in the graph. This property cannot be 0 or empty. In the case that the graph shows limited values, it is necessary to increase the given value.

  Note: During installation and copying of the Traffic Monitor with RRD graphs to individual port devices, the value of *Max Val* property will be automatically set and the value of the *Bandwidth* property of the related Port in the *bit per second* (bps) unit. In the case that *Bandwidth* properties are changed on the Port, manually or automatically via the *auto-discovery* function, Max Val property will not be automatically updated.

- **Gauge** – option that shows the variable value in the absolute amount. Otherwise the values will be treated as counter values. Example of counters is OID variables that observe the flow in bytes or packets, or the error rate on the interface.
- *No input*, *No Output* – this option is chosen if the first or second variable needs to be hidden.
- *No percent* – This option will not show relative percentage in relation to the Max Val properties. Percents are logical for e.g. Traffic monitors and Packet monitors, while they are useless for other types of monitors, e.g. variables that represent the current state, for Port Monitors and BGP Monitors.
- *With Peak Day, Week, Month, Year* – in the case of selecting this option, RRD Chart will show mid values for corresponding time intervals, aggregated values as well as maximum values.

For other properties and options the user is referred to the configuration manual for MRTG tools (MRTG configuration reference, http://oss.oetiker.ch/mrtg/doc/ mrtg - reference.en.html).

4.6. Reports

Reports will show the current state of the device SNMP variables on the user demand. Configuration of Reports, in which SNMP variables and output forms are chosen, is performed from the client application, while from the web interface it will be possible to see an overview of the Report.

Name of the Report can be arbitrary but it is recommended to carry the basic description of the configured report.

The Report can show simple SNMP variables, as well as a list of variables (e.g. network interface). In this case these retrieved values are shown in table format. It is possible to setup a name for each column (representing different OIDs) which are shown in the table header.

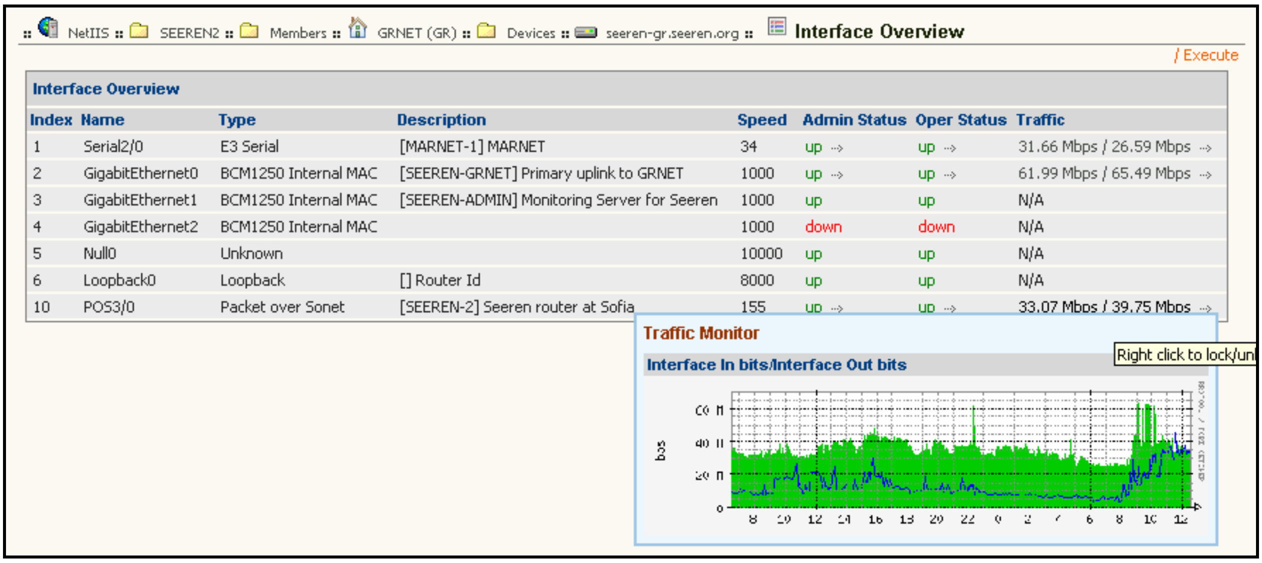
In addition to these general rules, if the administrative and operational port status and the traffic flow are defined in the Report, it is observed whether individual ports have configured Port Monitors and Traffic Monitor. In that case the port status is shown in the form of *Up/Down*, designated with a green and red colour. The current traffic, in bits per second (bps) unit, is shown only if a Port has a Traffic Monitor. Otherwise, the value will be missed, since the original OID is counter variable that is constantly increased and is not in the interest to the user.

In both cases, if there are Port and Traffic monitors, values are connected to corresponding daily RRD Chart which appears in pop-up windows when the cursor is pointed over.

Typically configured Report for routers shows the general status (system uptime, memory usage, processor usage, and temperature) and port details: name, description, status, traffic flow.

For routers with modem dial-up connection, it is possible to show status, telephone number, duration of the connection, connection speed etc.

For servers it is possible to show the status of the running processes or storage partitions.



:: NetIIS :: SEEREN2 :: Members :: GRNET (GR) :: Devices :: seeren-gr.seeren.org :: Interface Overview

/ Execute

Interface Overview

Index	Name	Type	Description	Speed	Admin Status	Oper Status	Traffic
1	Serial2/0	E3 Serial	[MARNET-1] MARNET	34	up	up	31.66 Mbps / 26.59 Mbps
2	GigabitEthernet0	BCM1250 Internal MAC	[SEEREN-GRNET] Primary uplink to GRNET	1000	up	up	61.99 Mbps / 65.49 Mbps
3	GigabitEthernet1	BCM1250 Internal MAC	[SEEREN-ADMIN] Monitoring Server for Seeren	1000	up	up	N/A
4	GigabitEthernet2	BCM1250 Internal MAC		1000	down	down	N/A
5	Null0	Unknown		10000	up	up	N/A
6	Loopback0	Loopback	[] Router Id	8000	up	up	N/A
10	POS3/0	Packet over Sonet	[SEEREN-2] Seeren router at Sofia	155	up	up	33.07 Mbps / 39.75 Mbps

Traffic Monitor

Right click to lock/unl

Interface In bits/Interface Out bits

5. TOOL MENU AND OTHER FUNCTIONS

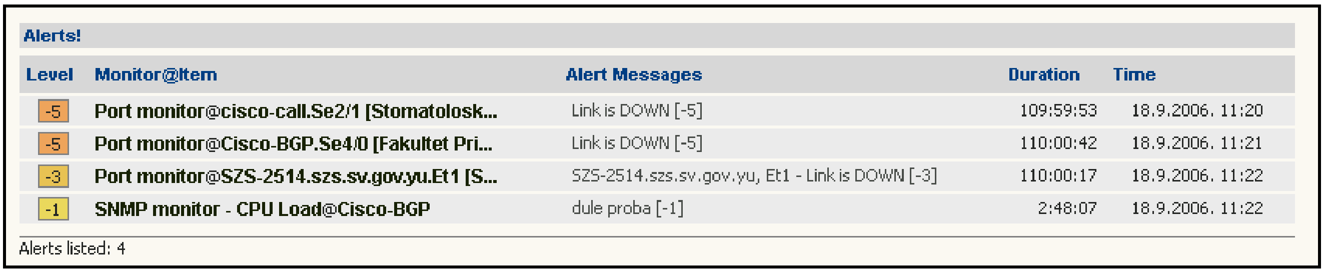
5.1. Alerts

"*Alerts*" presents a page with all currently active Alarms, for which a user have a read permission. Only bad Alarms with an *On* status are considered as active Alarms (alarm conditions met).

The Alerts page is in tabular form with an automatic refresh period and contains following columns:

- **Level** – Level of alarm importance, which presents a negative value from -1 to -10 (since only *bad* alarms are shown), distinctly marked with colours in the range from yellow to red. Rows in the table, i.e. alarms that are shown, are sorted by this value in such a way that the larger absolute value is on the top.
- **Monitor@Item** - HTML link to page of master Monitor and Devices/Ports to which the Alarm is defined, in the form of "*Monitor@[Port description] Port.Device.Location*".
- **Alert Messages** – Message that is defined on the alarm. The text is a HTML link to the page viewing the Alarm. The cursor over it will open a pop-up window with the daily RRD Chart and current values of the master Monitor variables. This pop-up window remains open until the right press button on the mouse is pushed (it closes in the same manner). Otherwise, the pop-up window will disappear when the cursor is moved away from the message.
- **Duration** – Total duration of the active alarm in the format "hours:min:seconds".
- **Time** – date and time of the latest monitor execution.

Overview of this page is useful due to fast observation of current problems (*failure identification*) and navigation of actual object for further analysis of the problem (*failure isolation*).



Alerts!

Level	Monitor@Item	Alert Messages	Duration	Time
-5	Port monitor@cisco-call.Se2/1 [Stomatolosk...	Link is DOWN [-5]	109:59:53	18.9.2006. 11:20
-5	Port monitor@Cisco-BGP.Se4/0 [Fakultet Pri...	Link is DOWN [-5]	110:00:42	18.9.2006. 11:21
-3	Port monitor@SZS-2514.szs.sv.gov.yu.Et1 [S...	SZS-2514.szs.sv.gov.yu, Et1 - Link is DOWN [-3]	110:00:17	18.9.2006. 11:22
-1	SNMP monitor - CPU Load@Cisco-BGP	dule proba [-1]	2:48:07	18.9.2006. 11:22

Alerts listed: 4

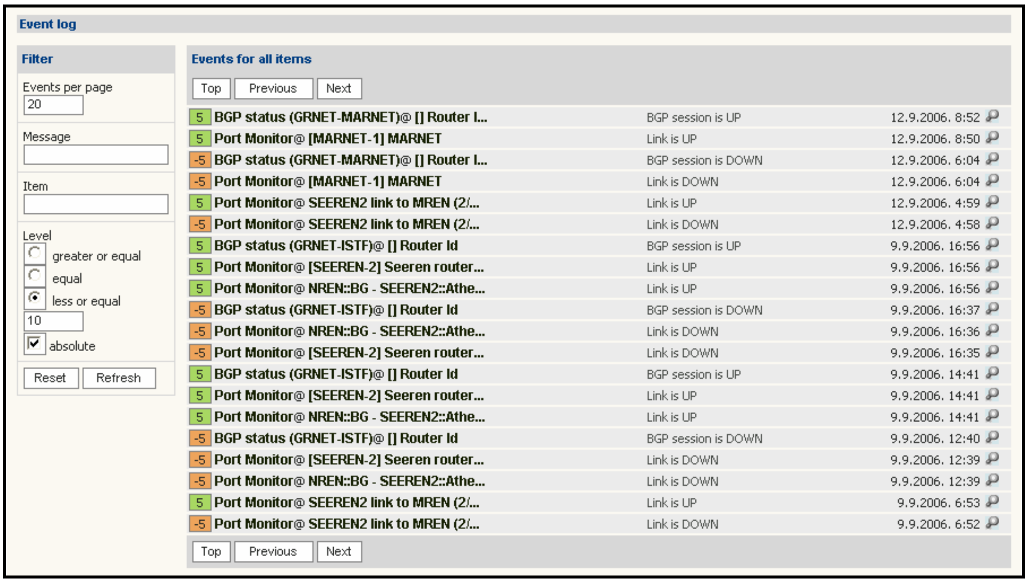
5.2. Event Log

Event Log presents a page with a list of all Alarms activated during a period of time, for which the user has a *read* permission. In this instance, *bad* and *good* alarms are shown and their appearance is in accordance. Events are shown in a table, sorted by time with the latest events at the beginning. Following columns are shown:

- **Level** – Level of Alarm importance, values from -10 to 10, marked in a distinct red or green colour.
- **Item** - HTML links to page that shows the master Monitor and Devices/Ports to which the Alarm is defined, in the form of "*Monitor@[Port description] Port.Device.Location* ".
- **Messages** – Message that is defined on the Alarm. The text is a HTML link to the page showing the Alarm details. Pointing the cursor over it opens a pop-up window with a daily RRD Chart and current values of the master Monitor variables. This pop-up window remains open until the right press button on the mouse is pushed (it closes in the same manner). Otherwise, the pop-up window will disappear that the mouse is scrolled away from the message.
- **Time** – date and time of the event occurring, i.e. alarm activation.
- **Select Icon** – This icon selects the current item (Monitor) and shows only events that are related to this monitor. It is possible to activate the *SLA report* for the selected element in order to view the statistics of the service quality (*SLA management*).
- **Edit Icon** – This icon opens a pop-up window for inserting additional information and comments related to the actual event (for the purpose of bookkeeping and *SLA management*).

Navigation through the active table view is executed with commands *Top*, *Previous* and *Next*, located on top and bottom of the table.

Controls for event filtering are placed on the left side. Fields *Message* and *Item* serve for entering the text that needs to appear in the table (case insensitive). Filtering in relation to the given importance level serves for select certain events categories.



Event log

Filter

Events per page: 20

Message:

Item:

Level
○ greater or equal
○ equal
● less or equal
10
☑ absolute

Events for all items

5	BGP status (GRNET-MARNET)@ [] Router I...	BGP session is UP	12.9.2006. 8:52
5	Port Monitor@ [MARNET-1] MARNET	Link is UP	12.9.2006. 8:50
-5	BGP status (GRNET-MARNET)@ [] Router I...	BGP session is DOWN	12.9.2006. 6:04
-5	Port Monitor@ [MARNET-1] MARNET	Link is DOWN	12.9.2006. 6:04
5	Port Monitor@ SEEREN2 link to MREN (2/...	Link is UP	12.9.2006. 4:59
-5	Port Monitor@ SEEREN2 link to MREN (2/...	Link is DOWN	12.9.2006. 4:58
5	BGP status (GRNET-ISTF)@ [] Router Id	BGP session is UP	9.9.2006. 16:56
5	Port Monitor@ [SEEREN-2] Seeren router...	Link is UP	9.9.2006. 16:56
5	Port Monitor@ NREN::BG - SEEREN2::Athe...	Link is UP	9.9.2006. 16:56
-5	BGP status (GRNET-ISTF)@ [] Router Id	BGP session is DOWN	9.9.2006. 16:37
-5	Port Monitor@ NREN::BG - SEEREN2::Athe...	Link is DOWN	9.9.2006. 16:36
-5	Port Monitor@ [SEEREN-2] Seeren router...	Link is DOWN	9.9.2006. 16:35
5	BGP status (GRNET-ISTF)@ [] Router Id	BGP session is UP	9.9.2006. 14:41
5	Port Monitor@ [SEEREN-2] Seeren router...	Link is UP	9.9.2006. 14:41
5	Port Monitor@ NREN::BG - SEEREN2::Athe...	Link is UP	9.9.2006. 14:41
-5	BGP status (GRNET-ISTF)@ [] Router Id	BGP session is DOWN	9.9.2006. 12:40
-5	Port Monitor@ [SEEREN-2] Seeren router...	Link is DOWN	9.9.2006. 12:39
-5	Port Monitor@ NREN::BG - SEEREN2::Athe...	Link is DOWN	9.9.2006. 12:39
5	Port Monitor@ SEEREN2 link to MREN (2/...	Link is UP	9.9.2006. 6:53
-5	Port Monitor@ SEEREN2 link to MREN (2/...	Link is DOWN	9.9.2006. 6:52

5.3. SLA management

On the basis of individual events from the *Event Log*, which is related to good and bad Alarm activations, it is possible to register all intervals of failure during a larger time period. Calculating the statistics that is related to the service operation and outages during the given time for the purpose of checking the quality that is agreed with the provider is called SLA management (SLA - *Service Level Agreement*).

Click on the Edit icon located in the last column of *Event Log* pages, opens a pop-up window which enables entering the following data:

- *Event Description* - random text that describes the event. This text may represent a comment on the cause of the problem or steps taken in solving the problem.
- *Type* – signifies the general cause of the problem and can be:
  - *Internal* – the problem is internally caused (e.g. power cut, configuration fault etc.)
  - *External* – the problem is externally caused on the service provider premises (e.g. telecommunication link failure) who is obliged to ensure a certain level of service quality to according to contracted SLA.
  - *Unknown* – cause of the problem is unknown.
  - *Ignore* – do not take the failure into the consideration.
- ***Acknowledgement Time** (Provider alerted)* – time when the problem is reported to the service provider.

Pointing cursor over the Edit icon in the View mode opens a pup-up window which shows previously entered data.

Statistics for the service quality for testing SLA, so-called SLA parameters, are related to external problems only from the moment the problem registration and acknowledged from the provider (*Acknowledgement Time*), to the moment of the problem solving.

A page with the summary statistics for the chosen period of time are shown upon activation of the *SLA report* key button (usually for the entire previous month). SLA report also lists all time intervals when the service didn't work with determined type of problem and comments.

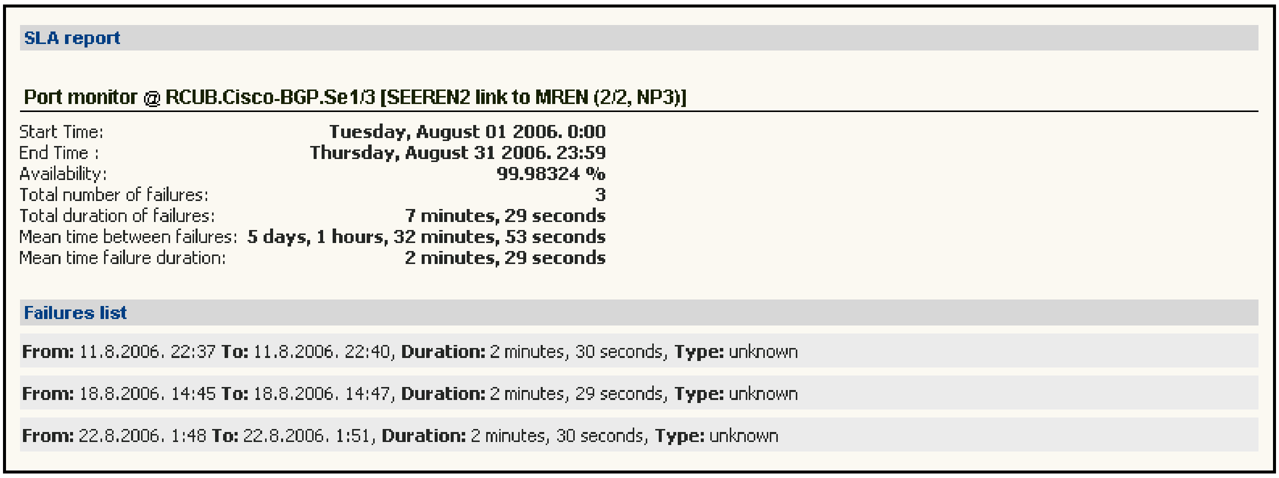
Basic statistic properties that are encountered for the chosen time interval are:

- *Service Availability* – percentage of the service work
- *Mean Time Between Failure* – average time between two problems
- *Mean Service Restoration Time* – average time of problem duration
- *Total Failures Number* – total number of problems

It is also possible to get this statistics for other problem types.

It is also possible to get a chart of the problem of all types during a chosen time period.

Current view of the SLA report can be printed in *PDF* format by selecting the *Print* button.



SLA report

Port monitor @ RCUB.Cisco-BGP.Se1/3 [SEEREN2 link to MREN (2/2, NP3)]

Start Time:	Tuesday, August 01 2006. 0:00
End Time :	Thursday, August 31 2006. 23:59
Availability:	99.98324 %
Total number of failures:	3
Total duration of failures:	7 minutes, 29 seconds
Mean time between failures:	5 days, 1 hours, 32 minutes, 53 seconds
Mean time failure duration:	2 minutes, 29 seconds

Failures list

From: 11.8.2006. 22:37 **To:** 11.8.2006. 22:40, **Duration:** 2 minutes, 30 seconds, **Type:** unknown

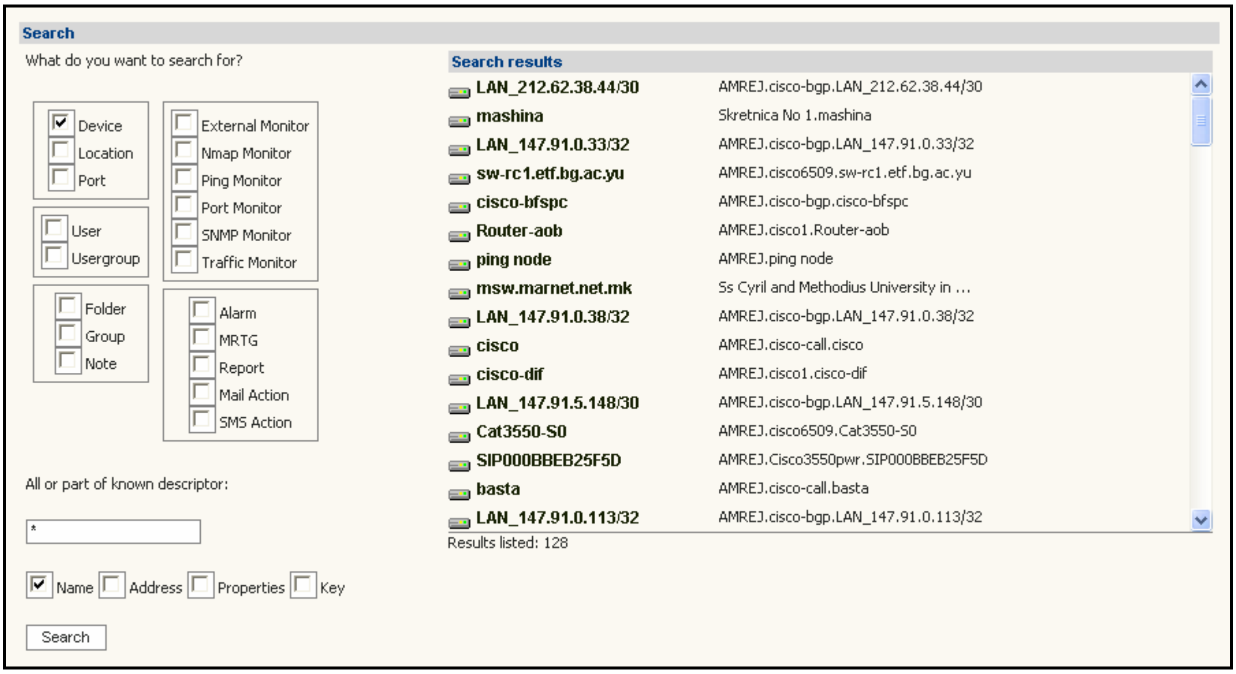
From: 18.8.2006. 14:45 **To:** 18.8.2006. 14:47, **Duration:** 2 minutes, 29 seconds, **Type:** unknown

From: 22.8.2006. 1:48 **To:** 22.8.2006. 1:51, **Duration:** 2 minutes, 30 seconds, **Type:** unknown

5.4. Search

This tool serves for searching the data hierarchy of the information system. The search is performed for selected object types based on the selected attributes (name, address, property or object key).

The search result lists all matched objects. Click on the individual object in the list shows the object details in Main panel.



Search

What do you want to search for?

☑ Device
□ Location
□ Port

□ User
□ Usergroup

□ Folder
□ Group
□ Note

□ External Monitor
□ Nmap Monitor
□ Ping Monitor
□ Port Monitor
□ SNMP Monitor
□ Traffic Monitor

□ Alarm
□ MRTG
□ Report
□ Mail Action
□ SMS Action

All or part of known descriptor:

*

☑ Name □ Address □ Properties □ Key

Search

Search results

LAN_212.62.38.44/30	AMREJ.cisco-bgp.LAN_212.62.38.44/30
mashina	Skretnica No 1.mashina
LAN_147.91.0.33/32	AMREJ.cisco-bgp.LAN_147.91.0.33/32
sw-rc1.etf.bg.ac.yu	AMREJ.cisco6509.sw-rc1.etf.bg.ac.yu
cisco-bfspc	AMREJ.cisco-bgp.cisco-bfspc
Router-aob	AMREJ.cisco1.Router-aob
ping node	AMREJ.ping node
msw.marnet.net.mk	Ss Cyril and Methodius University in ...
LAN_147.91.0.38/32	AMREJ.cisco-bgp.LAN_147.91.0.38/32
cisco	AMREJ.cisco-call.cisco
cisco-dif	AMREJ.cisco1.cisco-dif
LAN_147.91.5.148/30	AMREJ.cisco-bgp.LAN_147.91.5.148/30
Cat3550-S0	AMREJ.cisco6509.Cat3550-S0
SIP000BBEB25F5D	AMREJ.Cisco3550pwr.SIP000BBEB25F5D
basta	AMREJ.cisco-call.basta
LAN_147.91.0.113/32	AMREJ.cisco-bgp.LAN_147.91.0.113/32

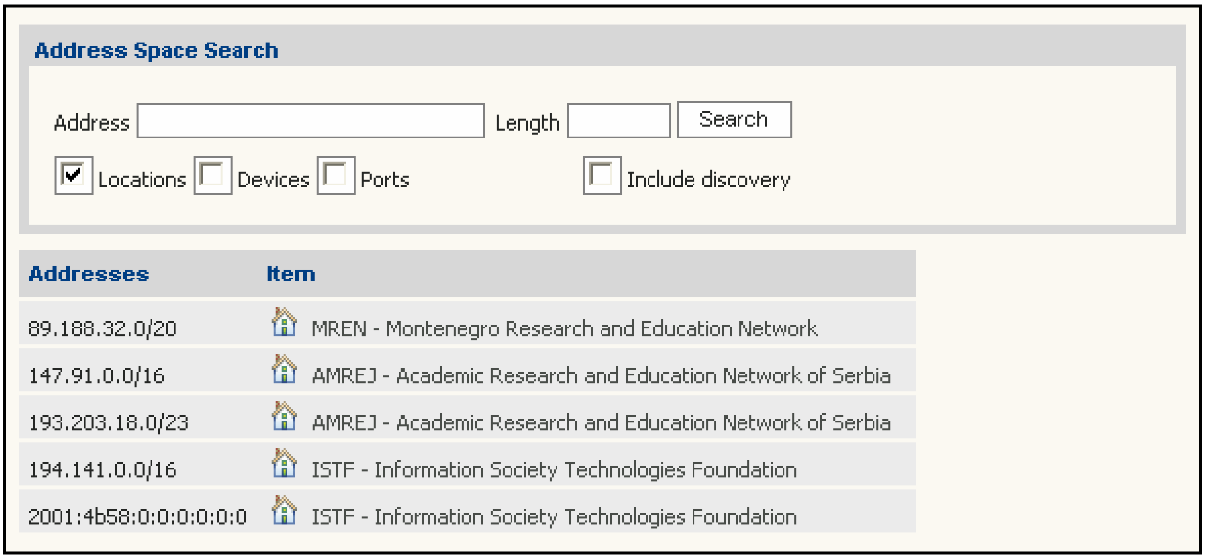
Results listed: 128

5.5. Address Space Search

Address Space Search is available from any part of the NetIIS system hierarchy, by clicking at the "*Show Address Space*" command on the Object Command menu. Address Space Search is applied at the hierarchy below the current object. In the case that is needed to search the whole hierarchy, the Address Space Search should be accessed from the root node.

At the first load, page will generate a list of all Locations and their IP address spaces. Searching the address space can be done by IP address and prefix length, and also by checking the type of object, which should be included in the search (Locations, Devices and Ports). There is also optional checkbox for including a *Discovered* folder into search.

Displayed search results include all matched sub-addresses – longer address prefixes and host addresses of the objects which are included in the searched address space.



Address Space Search

Address □ Length □ Search

☑ Locations □ Devices □ Ports □ Include discovery

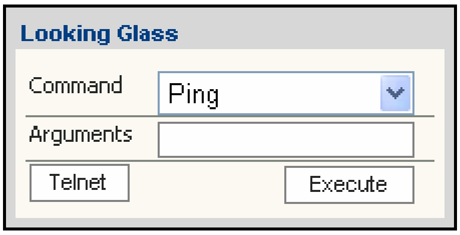
Addresses	Item
89.188.32.0/20	MREN - Montenegro Research and Education Network
147.91.0.0/16	AMREJ - Academic Research and Education Network of Serbia
193.203.18.0/23	AMREJ - Academic Research and Education Network of Serbia
194.141.0.0/16	ISTF - Information Society Technologies Foundation
2001:4b58:0:0:0:0:0:0	ISTF - Information Society Technologies Foundation

5.6. Looking Glass

Main panel contains a special box for performing Looking Glass functions. For current Device (router, switch) one of the globally configured commands are chosen from the drop down menu, and attributes are optionally entered. On the Execute command the chosen command will be executed on the device and the results will show in a new window. This is being executed in a manner that NetIIS server telnets at the router, executes the command, returns the results and closes the telnet session.

Click on the *Telnet* button establishes *telnet* session from user computer in default program for telnet connection.

> **Note:** For Looking Glass functions, it is necessary to setup system properties under the name "looking.glass.username" and "looking.glass.password" with the values of actual usernames and passwords that gives access to devices. If this is defined in the root of the NetIIS data tree, their use will be global for all devices. Configuration of these properties on individual devices will employ over these devices.



Looking Glass

Command: Ping

Arguments:

5.7. AutoDiscovery

Reliable performance monitoring and efficient use of the NetIIS software depends on the accuracy of the data that describe the network and the networking devices. *AutoDiscovery* function aims at easing the initial database population and later data updating, retrieving the relevant data directly from the networking devices.

5.7.1. *AutoDiscovery* principles

AutoDiscovery functions in the NetIIS system are organised in such a way that it executes on the user's request hop-by-hop. This approach, unlike the retrieval of the entire network, allows the user a better overview and control over the process of discovering network elements and offers a possibility of neat data organisation in the information system.

All *AutoDiscovery* functions are executed on the Device objects or their Ports, and data is read via SNMP protocol. Result of executing *AutoDiscovery* functions are shown in the *Message panel*.

AutoDiscovery functions that find new Devices and setup the Links, perform following actions:

- The function attempts to find the discovered Devices in the database, depending on the properties context such as name, IP address and MAC address.
- If the device already exists in the database, only updating of the object properties and Links are being performed.
- If the device doesn't exist in the database, then the device is created in the *Discovered* Folder, which is located underneath the Device on which the *AutoDiscovery* service was initialised.
- Links are being set to the discovered Devices/Ports, depending on the type of initialized *AutoDiscovery* function.

  Note: Manually entered links are not being updated, since it is considered that the user has a reason for manual intervention. If the control should be given to *AutoDiscovery* functions, manually entered links have to be deleted first, which can be done from the client application.

NetIIS system supports following types of *AutoDiscovery* functions:

- *Device Attributes Discovery*
- *Ports Discovery*
- *CDP Neighbours Discovery*
- *Layer 3 Neighbours Discovery*
- *Layer 3 Hosts Discovery*
- *Layer 2 Hosts Discovery*

5.7.2. Ports Discovery

This function is initialized on the networking devices, which discovers all network ports (interfaces) with following attributes: short and full name of the port, description of the port, bandwidth and SNMP ID. These data are standardized and is supported by majority of manufacturers.

When the data are retrieved, the Port objects are updated or created under the Device in the information system hierarchy. Simultaneously, each port is linked to the parent device, which supports the topological device connection over its ports.

In the case of data update, when Ports already exist under the chosen Device, the retrieved data are being paired with existing Ports by their names (and not by SNMP ID). Existing Ports are updated with new data, new ports are created, while the existing Ports that haven't been recognised during this process are being deleted together with included elements (monitors).

> **Note:** Deleted Ports are removed from the parent Device, but still stored in the *Recycle Bin* in the case for eventual recovery. This usual happens when a Port name is changed on the device, but the existing Monitors and RRD Charts have to be reused. Port with a new name will be created; the old name will not be read and will be erased. This is when it is necessary to go to the *Recycle Bin* and restore the old Port, manually relocate the included Monitors to the new Port and delete the old Port again.

SNMP ID Port attribute presents an index in the OIDs list and it is used by the Monitor for access to data of individual ports via SNMP protocol. During time, the devices are given new, added or changed ports, physical modules and logical interfaces such as VLAN, subinterface, *loopbacks*, tunnels etc. **All these changes demand launching of *Ports Discovery*, which reads new ports, but, what is more important, updates existing ports, since their SNMP IDs may be changed.** Otherwise the results will relate to wrong ports, which can bring great confusion: wrong reading, illogical results, false alarms etc.

> **Note:** Certain devices assign first available SNMP ID numbers to new ports, setting them at the end of the list. After a restart of the device, the SNMP ID indexes take the default order, which can bring to inconsistent values in the NetIIS system and wrong monitoring results. It has to be taken into consideration that the restart of communicational devices is rarely executed, and so inconsistent data status can appear after a longer period of time from the device configuration change that brought to it. This can additionally confuse NetIIS users and administrators. Thus it is recommended to use *PortDiscovery* each time after the restart of the device or configuration changes.

Taking into consideration that the reliable communication line is based on accuracy of SNMP ID indexes, *PortDiscovery* presents the most important and frequently used AutoDiscovery function.

> **Note:** In order to keep the data consistent, NetIIS system allows optional selection of automatic *PortDiscovery* function on the devices on daily basis. This option is can be selected from the client application.

5.7.3. *CDP Neighbours Discovery*

This *AutoDiscovery* function is initiated on the device and aims at discovering neighbouring devices and creating links from the information base that sustains CDP (*Cisco Discovery Protocol*). This function is enabled for *Cisco Systems* devices exclusively, with an activated

CDP protocol (*default* option on routers and switches, but is not supported on the PIX *firewall* devices).

Apart from information about neighbouring devices, CDP also offers the information about models of these devices, as well as connected ports. Upon retrieving this information, system checks whether some of the neighbouring devices are already in the database, the test is being done on the basis of devices IP address. For existing devices data is being updated, while new devices are created under the device that has initialised this function, within the *Discovered* folder.

The final result is creating links between two ports of neighbouring devices, which represents the topological connection in this part of the computer network.

> **Note:** Discovered devices that have been created in the Discovered folder need to be moved to corresponding Locations in the data hierarchy, which presents places where the physical devices are located in the computer network. In this instance, the created links between device ports are being kept. It is also recommended to that the new device is linked to its location, directly or indirectly via other devices in the same location, in order to maintain indirect links between locations. This link of devices and locations is manually maintained from the client application.

5.7.4. *Layer 3 Hosts Discovery*

This *AutoDiscovery* function initialises on routers (*Layer 3* device) or router ports, which discovers all IP address of end devices (hosts) on adhering local segments (sub-networks).

Subnet masks and IP addresses are retrieved from the router port during the execution. From this information, NetIIS system gets the address range in the adhering sub-network. This address range is pinged, in order to refresh the ARP router table, from where IP and MAC addresses of end devices are retrieved.

A new object type device is created within the *Discovered* folder, which presents the local sub-network, under a name based on the IP address and length of the mask split with an under score (e.g. 10.1.2.0_24). New and discovered host devices are created in the *Discovered* folder, whose IP addresses are found in the ARP route table. Apart from IP and MAC addresses, NetBIOS and DNS names are requested from host devices, which are set in the device name. MAC addresses are set as device property.

Recognised and created hosts are linked with created logical devices that represent segments of the sub-network. These links present logical Layer 3 connection as part of one segment.

5.7.5. *Layer 2 Hosts Discovery*

This *AutoDiscovery* function is initiated on the switch (Layer 2 device), for which the IP addresses of end devices (hosts) connected to ports are found. It is essential to enter the VLAN number for which the *AutoDiscovery* is executed; IP address of the *default-gateway* router and it is optional to have the address range for pinging in order to refresh the ARP router table and switch *forwarding* table.

AutoDiscovery function takes the *forwarding* table from the switch, from which it gets information of the MAC addresses and the corresponding switch port. Only ports with one accompanying MAC address are analysed, because it is assumed that end computers are linked to these ports. An ARP table is being read from the *default-gateway* router from which IP addresses are paired with previously read MAC addresses. On the basis of IP addresses, NetBIOS and DNS names are searched for, and checked whether the host device already exists in the database, while new devices are installed in the *Discovered* folder.

In this way discovered hosts are linked to adhering switch ports.

5.7.6. Layer 3 Neighbours Discovery

This *AutoDiscovery* function aims at finding neighbouring communication devices on Layer 3 levels (router).

The whole table of routing is being read from the router, where *next-hop* attribute presents IP address of the neighbouring router. These addresses are paired with IP addresses and masks on local ports that show which ports are connected to the neighbouring routers.

Advantage of this *AutoDiscovery* function is that it is not connected to a certain manufacturer of network equipment. Disadvantage of this function in relation to *AutoDiscovery* function that works on the basis of CDP are following:

- Only routers are being found (Layer 3 level), while switches (Layer 2 level) cannot be detected.
- There is no way of getting information about the port of a remote router.
- In the case of large routing tables, executing of this function can be slow, since the reading of the entire table is requested.

5.7.7. Device Attributes Discovery

This function is getting the name information for every SNMP enabled device. For *Cisco Systems* devices, this AutoDiscovery finds serial number and model information.

6. PRINCIPLES OF ORGANISING INFORMATION AND MONITORING SYSTEM

This chapter will deal with the functional principles of NetIIS system, as well as certain experiences and recommendations for organising data in the information system and organising the monitoring system.

6.1. Organising the information system

Organisation of data in the NetIIS system relates to defining the data information system hierarchy. Computer networks generally contain large number of devices, links and locations, as well as various complex services that are being used. Solid data organisation is a precondition for simple and efficient use of the NetIIS system and successful network performance measurement.

Good practice is that the data hierarchy on the highest level should be divided in several basic folders, folders that would define elements of the network and folders for presenting most important monitoring data.

Data hierarchy that describes the computer network can branch by defining folders into a logical division, such as:

- Geographical regions, cities or parts of the network
- Types of locations in the network (e.g. faculties, institutes, libraries etc.)
- Services and technology that are used in some part of the network (LAN, WAN, *dial-up*, *wireless* etc.)

Locations should be configured on lower levels of hierarchy. Within these objects that physically or logically belong to this location are being setup, and these are usually Devices and Users. In a case that a Location contains larger number of various types of objects, e.g. a number of various Devices, a good practice would indicate organising these objects into special Folders within the Locations. For example, special folders can be created: WAN, LAN, Servers, Employees, etc.

Apart from folders that define computer network elements in relation to their belonging, good practice would indicate defining folders at the top of the hierarchy that would contain pages with data overview, such as groups for Monitors, Graphs, *Looking Glass* groups or Reports. This is being done for a faster access to objects of interest for observation which will often be used. For example, this can be groups that represent external links, backbone, most important devices, servers and services etc.

Data organisation in the hierarchy and use of folders is significant and serves for defining different permissions over data for various Users and User groups. Different privileges for reading and writing for users and user groups are being set on a chosen object and relates to the whole sub-tree of data from the same node.

> **Note:** Assigning of user permissions over a data hierarchy is performed via the client application.

6.2. Organising the monitoring system

6.2.1. Communication links monitoring

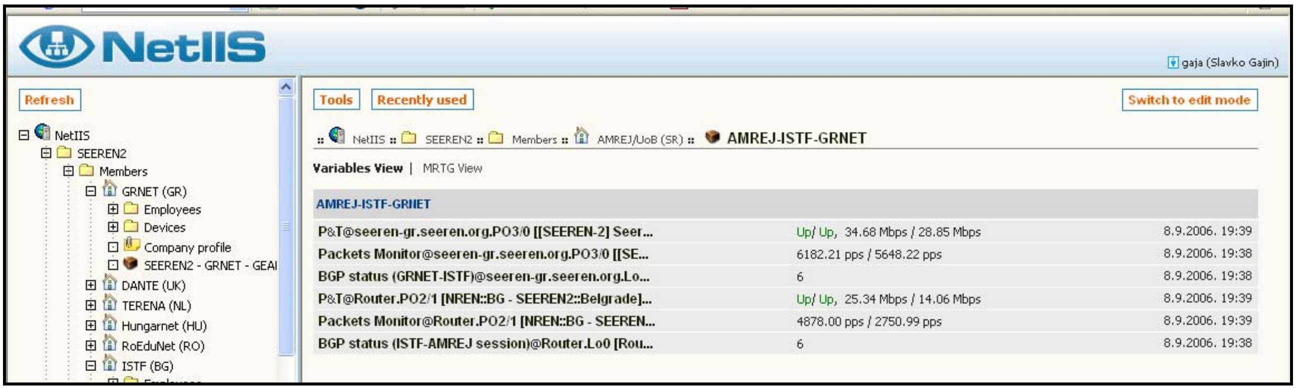
The basic monitoring of the computer network is related to observing the operability and quality of communication links.

In a case of communication line break down, the devices and part of the network on the other side of the line will remain unavailable to the NetIIS server, unless there is an alternative line. For this reason the monitoring that is based on reading properties, should be executed at the nearer end. For this purpose following monitors should be installed on corresponding ports: **Port Monitor**, **Traffic Monitor** and **Packet Monitor**. In the case of BGP routing protocol, it is useful to install **BGP Monitors** as well.

For monitoring the quality of the communication link, a **Ping Monitor** is being used; which is installed on the distant end of the line. Ping monitor can be configured towards any remoute address for the purpose of measuring the quality of the entire communication road from the NetIIS server to the distant point.

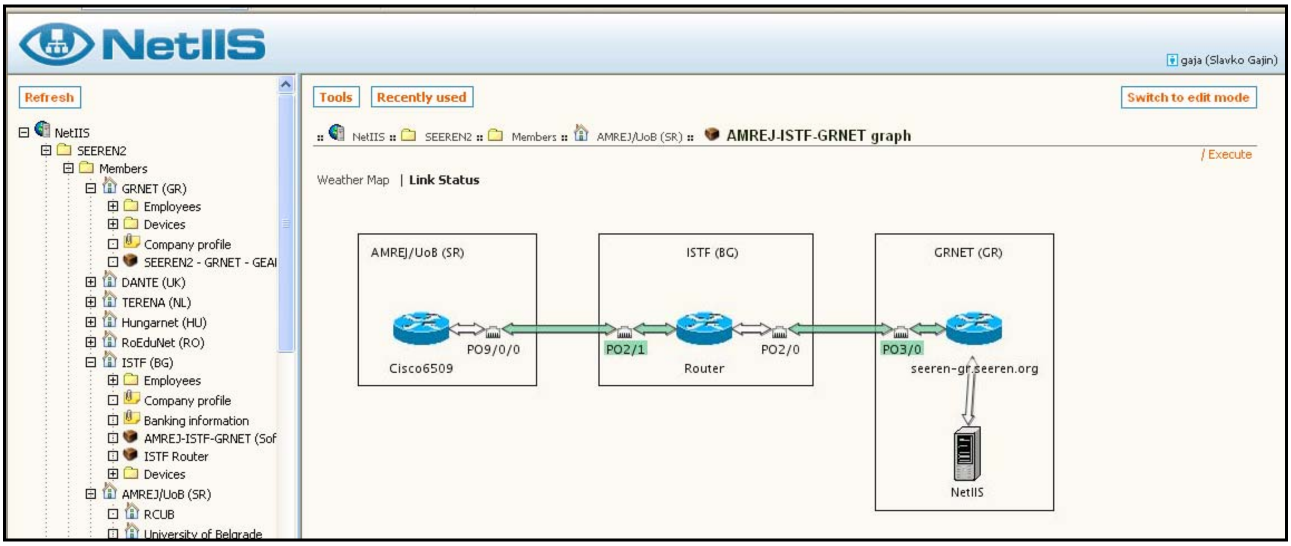
In the case that the link to the distant location has a medium-point or that it has an additional parallel connection, principles of setting the monitor is then being executed to each individual link on the entire road.

Taking into consideration that the status of the connection to the distant location demands an insight into these monitors, for a more efficient overview it is recommended to adjoin them into mutual groups for overview. This group can be set at the data tree directly below the location that it is related to, in order to locate it quickly.



AMREJ-ISTF-GRNET		
P&T@seeren-gr.seeren.org.PO3/0 [[SEEREN-2] Seer...	Up/ Up, 34.68 Mbps / 28.85 Mbps	8.9.2006. 19:39
Packets Monitor@seeren-gr.seeren.org.PO3/0 [[SE...	6182.21 pps / 5648.22 pps	8.9.2006. 19:38
BGP status (GRNET-ISTF)@seeren-gr.seeren.org.Lo...	6	8.9.2006. 19:38
P&T@Router.PO2/1 [NREN::BG - SEEREN2::Belgrade]...	Up/ Up, 25.34 Mbps / 14.06 Mbps	8.9.2006. 19:39
Packets Monitor@Router.PO2/1 [NREN::BG - SEEREN...	4878.00 pps / 2750.99 pps	8.9.2006. 19:39
BGP status (ISTF-AMREJ session)@Router.Lo0 [Rou...	6	8.9.2006. 19:38

Example of group of monitors linked to one complex connection



Example of setting various monitors on a link with a number of locations.

6.2.2. Monitoring of devices

Depending on the type and the manufacturer of the network device, it is possible to define various SNMP monitors. Basic information which shows global performance of network devices are processor and memory usage. Nevertheless, NetIIS surrounding is flexible enough to have various SNMP monitors for observing OID variables. For example, on routers of certain manufacturers the temperature of individual components can be observed, as well as queue size, *frame-relay* interface status, properties on modem lines etc.

It is useful to observe usage of individual disk partitions on the server, or properties and statistics of it’s services. Even network printers can support SNMP and give information about number of pages printed, status of the toner, estimated time for servicing the device etc. This information can be monitored and user can be alarmed for critical values.

For a fast and efficient overview of the current status of a larger number of SNMP variables on the user’s request, it is necessary to define Reports. Typical Report for network devices contains global data and status of all interfaces. For servers it is useful to define Reports that show a list of all executed processes.

User can organise a unique view of wider set of data by joining Reports in one Group.

> **Note:** Monitors are generally assigned for permanent monitoring of numerical variables, whose values are archived in RRD graphs during a certain time interval, and compared with alarm criteria for the purpose of notifying about problems in the network. Although monitors can be linked to text data (information) as well, permanent execution of these monitors is not reasonable. It is recommended to use Reports for this need.

6.2.3. Group of monitors

Similar and related groups of monitors for the links towards single location can be usefully joined to special groups. All groups related to the specific parts of the network can be joined, for example, network backbone, external networks, servers, regional units in the network etc. For an easy access to these groups it is useful to place these groups to folders at the top of the data hierarchy.

6.2.4. Graphs

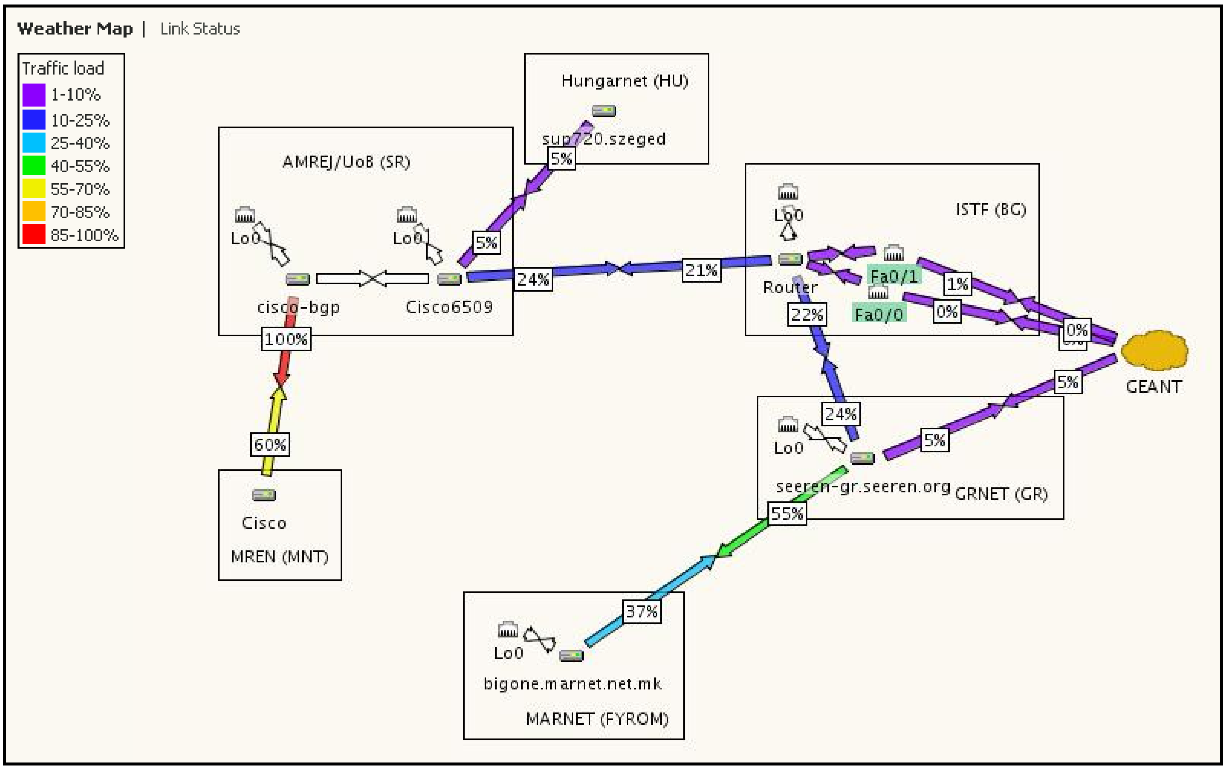
Graphs that represent the network topology offer a best overview of the network elements status.

Graphs are created for most important network parts, such as external links, network backbone, regional centres etc.

On the global view, links between locations can be displayed by adding individual locations into the groups. In a case that we want a more detailed illustration with devices, it is necessary to add chosen devices to groups; locations will be marked to represent a rectangular area that adjoins belonging devices. Individual ports can be added to groups, but they will additional burden the picture, so they should be shown only when multi-links are being sorted amongst devices.

Graphs in the *weather-map* mode automatically shows traffic monitors and they shouldn't be additionally adjoined to groups. If additional graph and alarm overview of certain monitors is needed, these monitors should be added to groups.

> **Note:** For an accurate topology illustration of direct and indirect links between ports, devices or locations, links in the information system should be set accurately. *AutoDiscovery* process can ease the setting and update of links, but sometimes a manual control and intervention is needed, which is executed from the client application. In order to show the indirect link between two locations or devices on the graph, the information system should contain a number of links between all medium-points on the way (devices and ports). Indirect links are requested between two locations, unless the location on the graph isn't selected as *traversable*, when the search is continued to next locations. **For an overview of links between locations, at least one device within the location must be linked to the adhering location.**



7. USE CASES

This chapter will demonstrate the use of the NetIIS system during notification, localisation and problem analysis, as well as assistance in problem solving. For various scenarios a number of problem solving procedure steps are given.

7.1. Navigation

Navigation includes actions of finding specific data in the information system for a more detailed overview and switching to other pages of interest. The user interface of the NetIIS web application is specially designed to support efficient navigation and switching to relevant pages, following the logical analysis and troubleshooting process.

This chapter describes various possibilities of navigation and typical sequences of pages.

Locating individual objects is usually performed for the purpose of a data details and current status overview, as well as for data changes. NetIIS system supports a large spectrum of possibilities for efficient navigation, whose usage primarily depends on the user's needs.

- Browsing of the data hierarchy. This is performed with the successive opening of nodes in the Explorer panel or in the Children box in Main panel. It is necessary to know the organisation of data, in order to find the specific object. This way of browsing needs a number of steps to be taken for finding the objects that are located in the lower hierarchy levels. Also, this is not suitable for devices with a large number of ports since it requires scrolling and an overview of a large data. However, it is usually used to locate groups that are separated on the top of the hierarchy, such as group of significant monitors.
- Search tool can select objects by name, which enables a fast and direct access. This is a useful for objects with known and unique names, e.g. devices or persons, but not for objects with generic names such as ports and monitors. Also, this is the best way for finding the objects whose location within the data hierarchy is unknown.
- Access to objects from the graph. Since graphs usually present the most significant parts of the network, this is most suitable way to navigate to central devices and most significant port links. Those objects that are not shown on the graph but are located on some of the links (e.g. ports) can be accessed by clicking the link and opening the pop-up window with these objects.
- Access to objects from the group for monitor overview (*Simple group*). Groups that are related to the most significant network elements are separated on the top of the hierarchy and are easily accessible. Monitors for observing the status of peripheral links to the final user locations that are not a part of the network backbone, are usually adjoined in groups. Access to devices or ports on these links includes finding individual locations via the *Search* tool or the tree expansion.
- Access from *Alerts* and *Event Log* pages. This is used for navigation to objects that have or had active alarms, usually for the purpose of observing the alarm problem.
- Switching to paired ports or devices on the other side of the link. The use of the main panel *Trace* box port illustration can efficiently bring user to the object on the other

side of the link, including all medium-points. This method is usually used for observing the link status or placing monitors.

- Switching to an object following the network topology. The use of main panel *Links* box can gradually expand the link topology to the chosen device or port.
- Object navigation path is often used for return on higher levels of hierarchy.
- *Recently used* is especially useful for navigation too, since the use of the system often implies the need to return to previous objects for the purpose of overview or properties settings.

7.2. Notification of the problem

Depending on the following ways of problem notification, basic actions are following:

Problem can be noticed on one of the following ways, and for each of them there are corresponding actions**:**

- **email** – look at the RRD graph on the email message HTML link. In the subject of the RRD page is the marked location, device and port with the name of the link that has activated the alarm. Locate problematic elements (e.g. port) via Search tool or direct search.
- **Alerts** - red line – look at the RRD, go to the monitor
- *Monitors Overview Group* - red line – look at the adhering RRD, look at the status of other monitors, go the problematic monitor.
- **Event log**, red line – look at the RRD, check the occurrences of this event (click on the zoom in the last column), go to the monitor.
- **Graph**
  - *weather map* overview, "Explosion" – check the traffic
  - *link status* overview, red arrow – check the status port
  - In a case that a problematic port is marked with a red colour, double click the port
  - click on the communication link which will open all adhering elements, look at other RRD graphs, go to the nearest end port link in relation to the NetIIS server, identify the location, go to the monitor.

7.3. Problem analysis

Problem analysis is demonstrated with following usual situations.

- **"Link failure"**

  Examine the global network status from the topology weather-map. Navigate to the interface details, analyse recent history on the daily chart for all associated monitors and check related events, click and execute Looking Glass command *show interface*. Following the link, go to the remote router page, check the remote interface status if it is accessible through the backup-link (if such exists).

- **"Link is up, BGP is down"**

Navigate to the interface details, analyse recent history for BGP status, execute *Looking Glass* command *show bgp summary*; investigate the link quality by examining the ping monitor, the traffic monitor and the packet monitor;

Execute the ping monitor, check the system uptime on both end routers (for possible reload);

Check the eventual intermediate points between the BGP peers (e.g. connection over MPLS).

- **"BGP session is established but there is no traffic"**

  Navigate to the interface details, investigate the reachability and link quality by checking the ping monitor, and execute a *ping* Looking Glass command;

  Analyse recent history for BGP status, execute command *show bgp summary* and examine the column with the total BGP entries number (number of routes);

  Check the system uptime on both end routers (for possible reload).

- **"Packet loss**

  Navigate to the interface details, investigate the reachability and link quality through cross-checking with the ping monitor, execute the *ping* Looking Glass command;

  Check the traffic monitor and the router utilization monitors for possible link or router congestion;

  Research recent history for BGP status, execute command *show bgp summary* and search for possible BGP flapping;

  Examine the routes using the *show ip route* and *traceroute* Looking Glass commands for the remote address.

- **"Increased packet rate"**

  Navigate to the interface details; investigate packet and traffic monitors;

  Check the link quality using the ping monitor; execute the *ping* Looking Glass command;

  Check the router utilization monitors for possible router congestion;

  If a possible DDoS-attack is in progress, trace the other interfaces investigating the packet/traffic monitors and try to locate the source of traffic;

  Check NetFlow tools, if such are installed.