A MITEL
PRODUCT
GUIDE

Mitel OpenScape Fault Management

Mitel OpenScape Fault Management V14, IP Manager Plugin

User Guide
10/2026

A31003-F30D0-U107-02-7619

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 Preface . . . 5
1.1 Purpose . . . 5
1.2 Audience . . . 5
1.3 Organization of this Guide . . . 5
1.4 Conventions Used in this Manual . . . 5
1.5 Terminology . . . 6

2 Introduction . . . 7
2.1 Basic Network Management Concepts: Managers and Agents . . . 7

3 First Steps . . . 9
3.1 Installation of the IP Manager Plugin . . . 9
3.2 Initialization of the IP Manager Plugin . . . 9
3.3 Licencing . . . 9

4 Working with the IP Manager . . . 11
4.1 Basic IP Manager Concepts . . . 11
4.2 IP Discovery . . . 12
4.2.1 General Principle of the IP Discovery . . . 12
4.2.2 IP Discovery Filter . . . 13
4.2.3 Difference between ARP Cache Scan and IP Address Range Scan . . . 13
4.3 Adding an IP Network . . . 14
4.3.1 Ignore Address Ranges . . . 15
4.4 Configuration of IP Discovery Filter . . . 16
4.5 Managed and Unmanaged IP Networks . . . 17
4.6 Adding IP Nodes . . . 18
4.6.1 Adding an IP Node . . . 18
4.6.2 Seed File . . . 18
4.6.3 IP Address Range Scan . . . 19
4.7 Deleting an IP Node . . . 20
4.8 Status Handling of IP Nodes . . . 20
4.9 Handling of IP Address Changes . . . 20
4.9.1 IP Node Expiration Time . . . 21
4.10 Configuration of the IP Parameters . . . 22
4.10.1 IP Parameters in the IP Manager . . . 23
4.10.2 IP Parameter Configuration for an IP Network . . . 24
4.10.3 IP Parameter Configuration for an IP Node . . . 25
4.11 Configuration of the Interfaces of IP Nodes . . . 26
4.11.1 List of Interfaces of a Node or Cluster . . . 26
4.11.2 Display of an Individual Interface . . . 27
4.11.3 Virtual Interfaces . . . 27
4.12 Configuration of the SNMP Parameters . . . 28
4.12.1 SNMP Parameters in the IP Manager . . . 28
4.12.2 Changing SNMP Parameters for Several SNMP Agents of an IP Network or IP Node . . . 28
4.12.3 Changing SNMP Parameters for One SNMP Agent . . . 29
4.12.4 Receiving SNMP Traps . . . 29
4.13 Configuration Templates . . . 29
4.13.1 IP Configuration Templates . . . 30

4.13.2 SNMP Configuration Templates . . . 30
4.14 Saving and Loading Configurations . . . 31
4.15 Changing SNMP Port for SNMP Agents. . . . 31
4.16 Adding SNMP Agents Manually . . . 31
4.17 Layer-3 Routes . . . 31
4.18 Interface Up/Down Traps . . . 32
4.19 Monitoring of Ping Results . . . 33
4.20 HTTP and HTTPS Servers . . . 33
4.21 IP Address Mappings. . . . 34
4.22 Cluster . . . 34
4.22.1 Status Determination in Clusters . . . 35
4.22.2 Configuration of Clusters. . . . 36
4.22.2.1 Setting Up Clusters . . . 36
4.22.2.2 Object Configuration in Clusters. . . . 37
4.23 Network Access Control (NAC) . . . 37
4.23.1 Rule Evaluation . . . 37
4.23.2 Allowing/Forbidding an Address Explicitly . . . 39
4.23.3 Extending the Address Lists. . . . 40
4.23.4 Definition of a Filter . . . 40
4.23.5 The NAC Event. . . . 41
4.24 Applications . . . 41
4.24.1 Access Applications. . . . 42
4.24.1.1 Listing Access Applications . . . 43
4.24.1.2 Configuring Access Applications . . . 44
4.24.1.3 Telnet Recognition and Integration. . . . 45
4.24.1.4 SSH Recognition and Integration . . . 45
4.24.2 Application Monitoring. . . . 46
4.24.2.1 Installed Software on a Server. . . . 46
4.24.2.2 Monitoring Programs . . . 46
4.24.2.3 Receiving SNMP Traps from Applications . . . 47
4.25 Control Center Overviews . . . 47

5 Symbols and Overviews . . . 49
5.1 Topology Symbols . . . 49
5.2 IP symbols . . . 49
5.3 Overviews . . . 50

A Access Rights . . . 51

Index. . . . 53

1 Preface

This chapter discusses the following aspects:

- purpose and audience of this guide
- terminology
- organization of this guide
- conventions used in this manual

1.1 Purpose

This user guide describes the IP Manager plugin for OpenScape FM.

1.2 Audience

This guide addresses users who want to learn how to use the IP Manager Plugin. To work with the IP Manager Plugin, it is necessary to know how to use the OpenScape FM. More about this can be found in the *OpenScape FM Desktop User Guide*.

1.3 Organization of this Guide

This guide is organized as follows:

- *Chapter 1, "Preface"* explains the structure of this manual.
- *Chapter 2, "Introduction"* introduces the IP Manager Plugin.
- *Chapter 3, "First Steps"* shows how to start, initialize and license the Plugin.
- *Chapter 4, "Working with the IP Manager"* describes the user interface of the Plugin.
- *Chapter 5, "Symbols and Overviews"* describes the used symbols.

1.4 Conventions Used in this Manual

The following font conventions are used in this document:

Bold Font: Indicates that a word is a new or important term. Bold is also used for Buttons, menu names and item names

Example: **Proxy Agent** or **OK**.

Bold Computer Font: Indicates data to be entered by the user.

Example: **`java`**.

Computer Font: Indicates computer output, including UNIX prompts, an explicit directory or a file name.

Example: `prompt%.`

Italics: Indicates a reference to another manual or to a different section within the current manual.

Example: *see Layer 2 Manager User Guide.*

Italic type is also used for emphasis.

Example: *All* users will be affected.

1.5 Terminology

- **OpenScape FM** means OpenScape Fault Management.
- **Server** means the OpenScape FM Server, i.e. the server where OpenScape FM Desktop has been installed.
- **Client** means the OpenScape FM Client, usually a web browser where OpenScape FM has been started.
- **Desktop** means the OpenScape FM Desktop.

2 Introduction

The IP Manager plugin is a core plugin for the OpenScape FM. It provides basic functionality, like e.g. the discovery of IP networks, status monitoring of IP devices and other devices. For example the IP Manager is used to add new IP components to the system, since only objects that are registered by the IP Manager can be managed.

Though the IP Manager is a separate OpenScape FM plugin, it will be installed automatically during the installation of the OpenScape FM.

After initialization of the IP Manager, the menu item **IP Manager** is added to the main menu bar and the **Network Topology** icon is created on the root submap.

The IP Manager establishes the basis for managing IP networks. It is used to add networks and IP Nodes to the OpenScape FM Desktop.

Note: Since version 10, the name „Host“ is used equivalent to „IP Node“ in the UI, especially in the new Web UI.

2.1 Basic Network Management Concepts: Managers and Agents

Network management is built upon agents and manager systems. The most common protocol for network management is SNMP. An SNMP agent provides information about a managed object. The manager system is responsible for monitoring the agent systems and retrieving information from the specific MIBs of the various agents in a network.

There are SNMP agents that are integrated in their particular devices and proxy agents that run on a different proxy device. Typically, proxy agents obtain the information about “their” device(s) via non standard or proprietary interfaces. A device can be a network element like a router, hub, IP switch or a voice device.

3 First Steps

3.1 Installation of the IP Manager Plugin

The IP Manager Plugin will be installed automatically when the OpenScape FM is installed.

3.2 Initialization of the IP Manager Plugin

The IP Manager Plugin will be initialized automatically during the installation of the OpenScape FM. The menu **IP Manager** will then be added to the main menu. A new object which represents the IP Manager Plugin will be added to the hierarchy. This object has the path **Root->System->Plugins->IP Manager**.

3.3 Licencing

The licencing of the IP Manager is part of the OpenScape FM licence.

4 Working with the IP Manager

4.1 Basic IP Manager Concepts

The IP Manager establishes the basis for managing IP networks. It is used to add networks and IP Nodes to the OpenScape FM Desktop.

Note: Since version 10, the name „Host“ is used equivalent to „IP Node“ in the UI, especially in the new Web UI.

The OpenScape FM can be used in IPv4 or IPv6 environments. It can be used in a mixed IPv4/IPv6 environment when the OpenScape FM itself is running on a dual stack system.

IPv4 and IPv6 networks will be separately created and discovered. IP nodes supporting a dual stack which have IPv4 and IPv6 addresses assigned are displayed in all corresponding networks. As a consequence they appear in more than one network.

The IP Manager offers two methods for detecting IP addresses and IP nodes: the “**auto discovery**” method and the manually started “**IP address range discovery**“. Both discovery methods are activated/started on basis of IP networks. Guided by specific discovery rules, the IP Manager will add discovered IP nodes to the OpenScape FM Desktop. Some of the discovery rules can be defined by the administrator via so called “Discovery Filters“, *Section 4.2.2*. The default rule is, a discovered IP node must have either a running SNMP agent or a running HTTP server.

IP addresses can be added explicitly to the OpenScape FM Desktop by entering a specific address via the **IP Manager->New->Node** dialogue or a set of specific IP address with a **seed file**. The latter two methods allow a network administrator to focus his network representation on a defined set of IP systems.

The IP Manager uses specific IP container objects to manage IP nodes. Such an IP container object is always located below the corresponding IP network. (The IP network should not be mixed up with the networks of the Topology Manager which are used to build up a network hierarchy. The IP network is in Topology Manager context only a node.) All IP nodes discovered for an IP network are stored in the related IP container object. An IP node can contain specific child objects, e.g. network interface(s), HTTP server, SNMP agents etc.

The IP Manager provides additional information about the status of the managed objects by representing an object in a status specific color. Traps sent by the related device can cause status changes. An example for such traps are the UP/Down Traps, see *Section 4.18, “Interface Up/Down Traps”*.

IP nodes can be configured to be displayed in topology networks.

4.2 IP Discovery

4.2.1 General Principle of the IP Discovery

Initially the local IP node will be added to the database. Other IP addresses and the related systems are detected by checking their network connectivity using a “Ping”. The Ping waits for a response from the system related with the IP address. If this connection attempt is either accepted or refused within a certain time out period, it is assumed that the ip address is “used“ and that there is a system representing this address. In this case the discovery process proceeds with this IP address, otherwise the IP address is regarded as not “used“. When a “Ping” was successfully executed, further checks will be performed by the discovery process. In the next step the “IP Discovery Filter“ conditions are checked (*Section 4.2.2*). By default there must be either an SNMP agent or a HTTP Server running on this system. If this condition is fulfilled, an IP node **exists** from the view point of the OpenScape FM Desktop and a node and object respectively will be created in the OpenScape FM database for this system.

Important Note:
If the timeout period is exceeded, for the response time of the scan a value of `-1ms` is written into the history data, the value `NoValue` into the export database and the status is set to *Critical*.
Timeout results will not be used to calculate average values. If not a single valid value can be determined for a calculation period, the average for the period is also displayed with `-1ms` and `NoValue`.

The ICMP-Ping is used by default. TCP-Ping can be used as an alternative.

For the discovery of an SNMP agent the community defined in the dialogue **IP Manager->Configure...** on page **SNMP Parameters** is used. Per default, the existence of specific SNMP agents is checked by testing the ports 161, 2161, 3161, 4161 and 5161. For each discovered SNMP agent an SNMP agent object is added to the submap of the related IP node. Each SNMP agent supporting the MIB II should provide a sysObjectId which is used to determine the type of device. According to the device type the corresponding IP node object is represented by a specific symbol on the views (trees and submaps).

Per default, the existence of specific web servers is checked by testing the ports 80, 280, 8888, 8080 and 8085. This could also be configured via the “IP Discovery Filter“. Some applications are discovered by retrieving specific HTTP/XML responses from the related Web-Server.

If one of the conditions defined via the “IP Discovery Filter“ matches, the technology-specific plugins proceed with the discovery process. These plugins discover their specific devices by checking the existence of device-specific MIBs and HTTP-servers and querying the component found for specific device and technology information on the added nodes. Having initialized multiple plugins, each plugin will discover its related devices. They obtain information about the capabilities of the managed objects from the corresponding MIBs.

Note, an SNMP agent can support different MIBs, e.g. Windows 2000 Servers serve requests for MIB-II, Host Resources MIB and MIBs of other applications.

In order to get the traps (fault events) send by the agent, it is very important to allow the OpenScape FM Server to register itself as a trap target on the SNMP agent of the trap originating device. Per default, OpenScape FM tries to register itself as a trap destination on each discovered node in the trapDestTable of the RMON MIB tree. If this operation cannot be performed, the trap destination has to be entered manually on the agent.

Example:

When an IP address of a Windows Server 2012 is added, its symbol will appear in the corresponding IP network. On its submap appears the network interface and the SNMP icon, which itself contains only one child object: the MIB II entry. There might be additional MIBs available via this SNMP agent, but as long as no specific plugin module has been initialized in the OpenScape FM Desktop, they will not be detected.

IP devices supporting routing (MIB II - IP forwarding = “on”) or switching are added to special locations. If such a device has only one IP interface, the device is - besides its representation in the IP nodes container- also displayed on the same level as the IP nodes container. If there are two or more interfaces (which usually link networks), the device will appear one level higher - on the network topology view - as a link between networks.

4.2.2 IP Discovery Filter

By default the OpenScape FM Desktop creates an IP node for any system where an SNMP agent or HTTP server is running. Additionally, a more fine-grained control for the creation of IP nodes is offered by the OpenScape FM Desktop. The following conditions can be used to control in which cases an IP node object should be created:

- A connection attempt to an IP address was successful (Ping)
- An SNMP agent is running on a specific port of the IP node
  - A specific sysObjectID was found
  - A specific MIB object was found
- A HTTP/HTTPs server is running on a specific port of the IP node.

There are some conditions where the creation of IP nodes is forced by the system, regardless of any discovery filters. Some examples are listed below:

- The system was entered manually by the user or imported via a seed file.
- A HiPath/OpenScape 4000 system which has an IP address assigned was discovered.

Via the “IP Discovery Filter“, the network and subnetwork where the IP node should be initially placed in the hierarchy of the OpenScape FM, can be defined, as well.

How to configure IP Discovery Filters will be described in *Section 4.4*.

4.2.3 Difference between ARP Cache Scan and IP Address Range Scan

The difference between the ARP Cache Scan and IP Address Range Scan lies in the basic mechanism used to determine the IP addresses to be analyzed. As suggested by the name, the ARP cache scan is based on the information stored in the ARP caches of the IP nodes. Generally the ARP cache is used to store the mapping between IP address and MAC-Address (Media Access Control Address). The content of the ARP cache is retrieved from the MIB-II of an SNMP Agent / IP node discovered by the OpenScape FM, by evaluating the MIB-

II's `ipNetToMediaTable`. Only the IP addresses found in the ARP caches of the currently discovered IP nodes take part in the auto discovery process of a network. The content of the ARP caches is checked during the periodically performed configuration polls on IP nodes.

The ARP Cache based discovery method works very well in most cases. But in some cases, where systems with an SNMP Agent could not be discovered or where certain IP systems only very rarely take part in the network communication, this mechanism will not work efficiently and it may take a long time to discover the whole network. In these cases an "IP address range discovery" will be the better method to analyze straight forward a defined address range of a network. This scan will check (Ping) all IP addresses in the defined IP address range. When an IP address is "used", the discovery process for this IP address will continue, otherwise the IP address is discarded. Because an IP address scan uses much more resources than an ARP cache based discovery, it will not be performed automatically.

Important Note:
Range Scans should be avoided within IPv6 networks. Every address within the given interval would be checked. In contrast to IPv4 the number of addresses could be very large.

4.3 Adding an IP Network

When an IP network should be added to the OpenScape FM database, the main menu entry **IP Manager->New->Network...** can be used. This will open the window to configure the IP network.

Within the window the **Network Address** and **Network Mask** must be entered. The definition of a **Network Name** is optional. The name will be used for the label below the network symbol. If no name is entered, the address will be used instead.

The fields **Start Address Scan** and **Auto Discovery** determine the discovery method used to find IP addresses and related nodes for this network. In case the **Start Address Scan** check box is marked, an additional dialogue allows the definition of an IP address range to be scanned. Every single IP address in the defined range will be analyzed according to the methods described in *Section 4.2.1* (more about this can be found in *Section 4.6.3*).

The selected **Auto Discovery** determines, whether the network will be (additionally) analyzed using the ARP Cache discovery and whether found IP nodes will be added to the network or not.

The Auto Discovery **Discover and add new nodes** analyzes the network using the ARP Cache discovery. For every found IP address an IP node object will be created.

If both, the discovery of new nodes and the IP address scan are selected, both IP discovery methods will work in parallel and add existing IP nodes to the network. Both methods are discussed in more detail in *Section 4.2.3*.

Note:
If an ARP Cache discovery gets deactivated, it will not stop immediately. All IP addresses that have already been detected, are waiting in the queues of the discovery process and will still be analyzed. But no additional IP addresses of the network will be added to the queue.

The Auto Discovery **Discover but don't add new nodes** also analyzes the network using the ARP Cache discovery, but no IP nodes will be added to the network container. Instead the discovered IP nodes can be viewed, by selecting the entry **Configure...** from the context menu of the network container. The tab **Discovered IP Addresses** shows a list of all discovered IP nodes. By selecting one or more IP addresses and pressing the button **Add Node...** the corresponding IP nodes will be added to the network.

If the Auto Discovery **Auto discovery off** is selected, no ARP Cache Discovery will be performed. If the address scan is also disabled, all nodes that should be displayed must be added manually (see *Section 4.6, "Adding IP Nodes"*) or by using a seed file (see *Section 4.6.2*).

A selection of the check box **Delete empty network automatically** will delete the network container automatically when the last IP node of the network is deleted.

Pressing the button **Ok** ends the **Add Network** dialogue. A new grey colored IP network symbol is created which is in the status "managed".

Note:
If only IP nodes belonging to a restricted IP address range shall be added to a network, the check box **Start Address Scan** and the Auto Discovery **Auto discovery off** should be selected. Otherwise the Auto Discovery will fill the network with all existing systems.

Note:
If the Auto Discovery **Discover and add new nodes** is activated, an IP network node will be only added to the network, when the system fulfills one of the configured IP discovery filters (see *Section 4.2.2*). To speed up the discovery, one known IP node should manually be added first. This node should support an SNMP agent and the MIB-II and it should be involved intensively in the IP traffic of this network.

After a network has been added, its configuration can be modified. This can be started by selecting the entry **Configure...** from the context menu of the network symbol. The page **Network Parameters** contains the elements known from the creation.

In addition the network can now be filtered out by selecting the Auto Discovery **Ignore address range** (see *Section 4.3.1*).

4.3.1 Ignore Address Ranges

In some cases it is desired to ignore specific networks or sub-networks. Nodes within such networks and their events should be ignored.

This can be done within the OpenScape FM by using one of two methods:

- For a network that is already known by the OpenScape FM, the context menu entry **Configure...** and the page **Network Parameters** can be used. On this page the selection menu **Auto Discovery** has to be set to **Ignore address range**.

  Warning:
  All nodes that are known for the ignored networks will be removed from the database. If such a network will be activated at a later time, a new configuration for the deleted nodes is necessary.

- If a new network should be ignored, it can be created by using the main menu entry **IP Manager->Address Filter->Filter Address Range** and entering the usual network parameters.

In both cases the network will be moved to the submap for ignored address ranges (System->Plugins->IP Manager->Ignored address ranges) and set into the status ‚*unmanaged*‘. For all networks located on this submap no new nodes will be discovered and already assigned nodes will be deleted.

The ignored address ranges can be displayed with the help of the main menu entry **IP Manager->Address Filter->Show Filter...**. This function opens the submap **System->Plugins->IP Manager->Ignored address ranges**, which displays a symbol for every ignored address range.

To activate an ignored network, the entry **Configure...** from the context menu of the respective address range symbol can be used. On the page **Network Parameters** another **Auto Discovery** besides **Ignore address range** has to be selected. The respective network will then be set to ‚*managed*‘ and it will be moved to its normal position within the navigation tree.

4.4 Configuration of IP Discovery Filter

The IP Discovery Filter defines, under which conditions new IP nodes are discovered and in which network/sub network they will be placed by default. This e.g. allows that all objects of a certain type will be placed within the same network container.

The configuration of the discovery filters is started by selecting the entry **Discovery Filter...** within the main menu **IP Manager**. This menu entry is only visible for users with Administrator rights, and opens the configuration window.

On the left hand side the window shows all conditions (column **Discovery**) which can be activated when an IP address is processed by the discovery mechanism. The list of conditions contains all enterprise specific MIBs, sysObjectIDs and HTTP ports known by the OpenScape FM Desktop.

General conditions will be displayed left-most, while more specific conditions are displayed indented below the respective general condition.

If IP nodes that fulfill a condition should be generated, the checkbox in the column **Create IP Node** must be checked to activate the condition. If a general condition gets activated, all specific conditions will also be activated and locked. The other options (“Default Net“, “Default Subnet“, “Network Precedence“) are still changeable. If the checkbox **Create IP Node** gets unchecked for a general condition, the checkboxes for the specific conditions are unlocked.

The column **Default Net** shows in which network the created IP node is initially placed in the hierarchy of the OpenScape FM. The corresponding subnetwork is shown in the column **Default Subnet**. The column **Network Precedence** indicates which priority the network/subnetwork placement has.

The column **Host Type** is used to tag a host with a specific label. These labels are used to group together hosts of the same type to easily find e.g. all discovered routers. The list of all known host types can be accessed via the main menu **IP Manager->Host Types** or in the Web UI below **Categories->Host Types**.

The checkbox in the column **Active** can be unchecked to deactivate the configuration for the respective entry.

The highest **Network Precedence** applicable to an object determines where it is located. If a configuration with a higher precedence applies at a later point in time, the object gets relocated

For example, if a configuration exists where the Network Precedence of the MIB II configuration is “30“ and the Network Precedence of the Hostresources is “50“ an IP node which supports the MIB II *and* the Host Resources MIB will be placed in the network/subnetwork defined for Hostresources.

By selecting **Properties** from the context menu of an IP node object, a window opens on whose page **Topology->Configuration** a position within the network topology can be set manually. This additional configuration has the Network Precedence `100`.

On this page, it is also possible to recalculate the network topology for the individual object by checking **Reset Network Precedence**. If the page is now saved (**OK** or **Apply**), the Network Precedence of the object is set to `0`. The check box is only active if the object has currently an assigned precedence greater than `0`.

Note:
Within the MIB-II or at another location a sysLocation can be defined. This sysLocation will have a precedence of ’40’. Therefore, in order to overwrite a sysLocation, a precedence of more than ’40’ must be selected.

To change the conditions, the respective rows must be selected and the dialogue components on the right hand side must be used.

4.5 Managed and Unmanaged IP Networks

IP networks are created either explicitly by a user action, or implicitly by a discovery (ARP cache scan or IP address range scan).

An IP network which has been added to the system explicitly using the **Add Network** dialogue (see *Section 4.3*) is in the *managed* state. If a certain network should no longer be managed, the state must be manually set to *unmanaged*. This can be done by using the entry **Edit->Unmanage** from the network symbol’s context menu. After setting a network to *unmanaged*, all IP nodes which reside in this network are also set to *unmanaged*.

The menu entry **Edit->Manage** sets the network and all IP nodes residing in this network to the *managed* state.

An IP network can be created implicitly during the auto discovery process. This represents the fact that there are IP nodes which have an interface into this network and which are part of another existing network with activated ARP cache discovery. When a network is created implicitly, it is set to *unmanaged* and it will only contain IP nodes that are also a part of another network.

Note:
New IP network nodes can not be added to an *unmanaged* IP network.

4.6 Adding IP Nodes

4.6.1 Adding an IP Node

After an IP network has been added, it can be proceeded with the configuration of the network.

To manually add a node to a network, the entry **New->Node...** from the main menu **IP Manager** can be used. This will open a window in which the IP address of the new node can be entered. If a DNS server or a host file is defined, a host name can also be entered.

If an IP address is entered, the OpenScape FM tries to determine a suitable host name. If this is successful, this name is displayed in the label of the new IP node.

A node for a specific network can be added by using the menu entry **New->IP Node** within the context menu of the respective network symbol.

If the Auto Discovery **Discover but don't add new nodes** is activated for the network to which the new node belongs, the IP Discovery process as described in *Section 4.2, "IP Discovery"* is performed.

In contrast to the automatic discovery processes, when an IP address is added by an explicit user action, a corresponding IP object will be created when a related network exists. It will not be checked if the IP node really exists and a node does not have to fulfill any "Discovery Filter" conditions.

If the associated network has not yet been added and the IP node offers a readable MIB-II, the IP node and the associated IP network are added to the OpenScape FM database. If no MIB-II is accessible for this IP address and no netmask has been specified for the node, the IP manager cannot determine the associated network and the node is created in the network *Default*.

If a suitable network is set up at a later time, the node is automatically moved to this network at its next discovery.

4.6.2 Seed File

A comfortable solution to add a specific set of IP addresses/IP nodes is the usage of a seed file. A seed file is a simple text (ascii) file which contains a set of IP addresses. Each IP address-entry has to be specified in a separate line. This can be an IP address in dot notation or a hostname with a complete domain address (FQDN).

Examples:

```
#Network Configuration
139.2.48.0:255.255.240.0:my_net

#Ipv6 Network
fda5:a176:e234:1203::|64

#Nodes
139.2.51.74
test_host
fda5:a176:e234:0102:0250:56ff:fe8D:2D6E
```

A seed file is loaded via the menu item **IP Manager**->**Load Configuration**. By opening the Seed File Browser, the opened file manager can be navigated the same way as known from common file navigation programs (e.g. WinNT/Win2k explorer) and a seed file can be selected. Clicking **Open** will load the selected file. The IP Manager adds the IP nodes and displays them in the corresponding views. The process of adding IP addresses (nodes) using a seed file follows the same rules as described in *Section 4.6.1, "Adding an IP Node"*.

Each IP node can be assigned additional properties in the address list. These are separated by a comma. In total, the following 5 properties can be assigned to a node in exactly this order.

IP Address or **Hostname**
Defines the host, that should be added to the OpenScape FM.

Net (optional), **Subnet** (optional) and **Network Precedence** (optional)
These three parameters define how the new object will be integrated into the network topology. They correspond to the **Default Net**, **Default Subnet** and **Network Precedence** for defining discovery filters (see *Section 4.4*), but only apply to the respective object.

Object Comment (optional)
Defines an object comment String (see *Desktop User Guide*), that will be attached to the new object. It will e.g.displayed as a tooltipp for the object's symbols.
Line breaks or tabulator insertions can be inserted with the character strings `\\n` or `\\t`.

If individual properties are not to be considered, only the corresponding commas must be set.

Examples:

```
139.2.57.2,myNetwork,mySubNetwork,10,Main Server
```

Adds an object with the IP address `139.2.57.2` and places it within the network container `myNetwork` and its sub container `mySubNetwork` with the network precedence `10` (if no discovery rule with a higher precedence applies for the object). The object itself gets the tooltipp `Main Server`.

```
139.2.57.3,,,,Backup Server
```

Adds an object with the IP address `139.2.57.3` at an automatically determined network position and assigns the tooltipp `Backup Server` to it.

4.6.3 IP Address Range Scan

When a new IP network has been added, it is possible to check the check box **Start Address Scan**. Pressing the **Ok** button will then open a new window where the IP address range can be entered that should be scanned. The **OK** button in this window opens an info browser showing the progress of the IP address range discovery. For each queried IP address the result will show if there was an answer from a corresponding system and whether an IP node was created for this address.

An IP node is only created when the configured "IP Discovery" conditions match for the system related with this IP address. Pressing the **Stop** button will cancel the scan. Pressing the **Close** button will close the browser and also cancel the scan.

In order to start an IP address range scan for an existing IP network, select the IP network and use the context menu item **Address Scan**. After pressing this menu item, the same dialogue described above will be opened.

Important Note:
Range Scans should be avoided within IPv6 networks. Every address within the given interval would be checked. In contrast to IPv4 the number of addresses could be very large.

4.7 Deleting an IP Node

While working with a large network and with many IP nodes, it is possible that IP nodes are discovered that should not be monitored by the OpenScape FM. These nodes can be easily removed by selecting the entry **Edit->Delete Object** from the context menu of a symbol representing the node. After a positive confirmation, the node will then be removed from the IP network.

When the ARP cache discovery is enabled for the network, the node will be found again on the next query. To avoid the repetitive deletion of unwanted nodes, a discovery behaviour can be defined for each network (see *Section 4.3, “Adding an IP Network”*).

4.8 Status Handling of IP Nodes

The IP node‘s status is usually the most critical status of its child objects, as long as the IP node is reachable (see *Section 4.2.1, “General Principle of the IP Discovery”*). To identify the component that is responsible for the status of the IP node symbol, the submap of the IP node can be opened.

If an IP node is detected not reachable, a critical event is generated for this IP node setting its status to „*critical*“ and the reachability status of the IP node will also be set to „*critical*“. The status of child objects, whose status can only be determined when the IP node is reachable, are set to „*unknown*“. These e.g. are SNMP agents, IP interfaces, or HTTP server. The status of child objects whose status is set via other systems will be left unchanged.

When the IP node is reachable again, the respective event gets acknowledged and the reachability status of the IP node is set to „*normal*“.

4.9 Handling of IP Address Changes

Often IP addresses are assigned dynamically (usually at device startup). Therefor it is not possible to uniquely identify and recognize a particular device by it’s IP address. But previously discovered data should not be lost when an IP change occurs for an object.

To avoid such data losses two mechanisms are used by OpenScape FM to recognize already known systems.

Since the MAC (Media Access Control) address is unique and does usually not change during the life-cycle of a network component, the MAC address is used to detect IP address changes. If the MAC address of a newly discovered IP address is already known by OpenScape FM, it will be assumed, that the interface attached to the MAC address has changed to a new IP address.

MAC addresses, or physical addresses, are used to identify network nodes at the physical layer of the communication protocol. Since this is the lowest level of the protocol stack, MAC addresses are usually assigned to network adapters. The MAC addresses of the network adapters for a particular network node can be obtained

from the MIB II. As long as that node has an SNMP agent running which supports the MIB II. If this is the case, the following table gives information about the network adapters:
`.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable`

For each interface, this table provides the field `ifPhysAddress` which contains it's MAC address. If the node has more than one interface (the loopback device will be ignored) all MAC addresses will be used to identify the IP node.

If an IP node is added to OpenScape FM by the ARP Cache scan discovery process (*Section 4.2.3*), the MAC address is already known from the corresponding ARP cache entry through which the IP node was discovered.

If the ARP Cache scan discovery finds a node which is already known (by its MAC address) but has a different IP address, it can be assumed that an IP address change has occured. Therefore it will be checked whether the old IP address is still accessible. If this is the case, a new object will be added representing the new IP address. If only the new IP address is accessible the following steps are performed:

- The auto discovery will change the IP of the old IP node to the new IP address.
- All events in the Event Browser related to the old IP are updated with the address and object name of the new IP node.

Important Note:
If an IP node is added manually (see *Section 4.6*) or by the IP address range scan discovery (see *Section 4.2.3*), the MAC address can only be obtained if the system has a running MIB-II agent. If this is not the case, the mechanism described above will not work for that particular system, i.e. it can not be recognized if it's IP address changes.

This mapping information for a single IP node can be displayed by using the menu entry **Properties...** from the context menu of the respective IP node. The information can be found on the tab **Topology->Node ID Configuration**.

4.9.1 IP Node Expiration Time

In an environment where MAC addresses can not be reliably determined, duplicate IP nodes (same devices with different IP addresses) can be avoided by expiration dates. That means, if an IP node has not been up for a predetermined amount of time, by default it will be deleted from the OpenScape FM database. In fact, the expiration time is bound to the interface through which the IP node was discovered by OpenScape FM. If no connection can be established to this interface, a configured action will be performed for the IP node object.

By default the expiration time is one week and the default action is that the related IP node object will be deleted. Of course a user with administrator rights can configure the expiration time, and can decide whether the IP node should be deleted, set to unmanaged or that no action should be performed on this IP node when the expiration time is exceeded. These values are configured via the IP Parameter dialogues (*Section 4.10*).

All sub-components (e.g. HTTP server, SNMP agent, etc.) of an IP node are also treated as expirable objects. For the sub-components the same configuration (expiration time and action) will be used as for the related IP node. Therefore IP components which are not reachable for the expiration time can be deleted or set to unmanage automatically. By default, when for example an HTTP server on an IP node is deinstalled, the HTTP object will be deleted automatically from the view of the related IP node, when the expiration time is passed.

The expiration times will be checked during the status poll of the IP node (*Section 4.10*).

4.10 Configuration of the IP Parameters

The IP Manager regularly performs three types of automatic IP pollings. These pollings are repeated automatically in defined time intervals:

1. **Status Poll:**
   The Status Poll controls if the IP Node is responding to a Ping (see *Section 4.2.1*). If this is the case, the child components will be triggered to refresh their status. The ping results are automatically collected for each IP node (see *Section 4.19*).

   By default the automatic Status Poll will be performed once per hour. Via the menu item **Host**->**Status Poll** in the context menu of the IP node or via the menu item **Status Poll** in the main menu **IP Manager** the Status Poll can be started manually.

   The results of the poll are displayed in an summary list.

2. **Configuration Poll:**
   The Configuration Poll triggers the child components of an IP node to refresh their configuration data.

   The default time period for the automatic Configuration Poll is once per day. Like the Status Poll it can also be started manually. This can be performed via the menu item **Host**->**Configuration Poll** in the context menu of the IP node.

   The results of the poll are displayed in an summary list.

3. **Discovery Poll:**
   The Discovery Poll checks the existence of new child components (e.g. a new HTTP server).

   Per default the Discovery Poll will be performed once per day. In order to manually start a Discovery Poll, the menu item **Host**->**Discovery** in the context menu of the IP node has to be selected.

   The results of the poll are displayed in an summary list.

The time intervals for the IP polls can be changed via the IP Parameters.

For each IP node the default values for the automatic IP Polling intervals can be manually overridden using the IP Parameter configuration dialogues. These dialogues allow to define time intervals in which the automatic status poll, configuration poll and discovery poll of an IP node will be started. Additionally the general timeout value can be defined. If the connection cannot be established, within this timeout, the IP node will be treated as not alive. The maximum value for the timeout is 300 seconds. This reachability check will be performed at least once. The number of retries can be changed via the IP Parameters. *Table 1* shows the minimal values which can be set for each parameter:

Parameter	Min.-Value
Timeout	1 second
Status Polling	1 minute
Configuration Polling	1 hour

Table 1 configuration limits

Parameter	Min.-Value
Discovery Polling	1 hour

Table 1 configuration limits

In addition to the configuration of the time intervals of the IP polls the mentioned dialogues are also used to define the expiration time of IP components and the related action that will be performed when the expiration time exceeds (*Section 4.9.1*). By default the expiration time is set to one week and the related component will be deleted. The expiration time has to be set to at least one day.

The handling of topology information of IP nodes where the IP address has been changed (*Section 4.9*) can also be configured in these dialogues. A user can decide via a checkbox whether the topology data should be preserved or discarded. If the topology data should be discarded the discovery filter conditions (*Section 4.2.2*) will be used for the placement in the topology.

By default the manually changed topology configuration and topology data of the related IP node will be preserved.

Note:
Only a user with Administrator rights can change the values in the IP Parameter dialogues.
A user with Operator rights can only view the parameters.

The following sections provide the following information:

- How to set the default IP Parameters (*Section 4.10.1, “IP Parameters in the IP Manager”*).
- How to automatically assign IP Parameters to newly discovered IP nodes, based on their network parameters (*Section 4.13.1, “IP Configuration Templates”*).
- How to define the IP Parameters for a set of IP Nodes of an IP Network (*Section 4.10.2, “IP Parameter Configuration for an IP Network”*).
- How to configure the IP Parameters for one IP Node individually (*Section 4.10.3, “IP Parameter Configuration for an IP Node”*).

4.10.1 IP Parameters in the IP Manager

The menu entries **IP Manager->Configure...** (for “Administrator” users) and **IP Manager->Show Configuration** (for “Operator” users) open the configuration dialogue of the IP Manager. Within the page **Default** of this dialogue (subpage **IP Parameter**), users with „Administrator”-rights can change the following default parameters. Users with „Operator“-rights can only view these parameters.

The selection menu **Ping Engine** defines the general method how availability checks will be performed for IP nodes (*ICMP*, *TCP*, *SNMP*, *HTTP*, *HTTPS*). When the entry *Auto* gets selected, for new nodes the methods are tried in sequence. The first method that works for the new node will be configured for this node. If *Disabled* is selected, each started ping will automatically return `0ms` as its result and no actual ping will be started.

Note:
For *HTTP* and *HTTPS* pings: Connection errors will result a failure and no response time will be logged.
For *TCP* pings: If the host is running but the configured port is not listening, this will nevertheless be counted as a success. This logic enables the TCP method to be used as a fallback if the ICMP ping is not enabled for the network. If the host is not running, the TCP ping will display a failure.

The field **Timeout** defines the time interval in which a response to the check must be received. A check is successful, if a reply from the checked system is received within the given interval. The request is even successful, when the system answers the request with a rejection, since it has proven itself as active.

If a request is not successful, it will be retried as long as fewer retries have been performed than are defined in the field **Retries**. The node will then be set to the reachability status selected in the menu **Offline Severity**.

Regardless whether a timeout has occurred or not, the ping results are collected for each IP node (see *Section 4.19*).

If all possible retries have been performed without getting a reply within the time interval, the system will be marked as not available.

The fields **Status Poll**, **Conf. Poll** and **Disc. Poll** define the time intervals in which automatically performed Status-, Configuration- and Discovery-Polls will be started.

If a node is not available for a longer time than defined in the field **Expiration Time**, the action chosen in the menu **Expired IP Nodes** will be performed for the node. Depending on the selection, the node will be deleted, set to the status '*unmanaged*', or no action will be started.

If **Preserve Topology** is checked, the configured network topology will be preserved, when an IP address change is discovered for a system. This is the case, when a new IP address is discovered for a known MAC address, while the former IP address is in the status '*not active*'.

The selection menu **Offline Status** can be used to determine the status of IP nodes that can no longer be reached.

If **IP Address Adjustment** is checked AND if the current request IP address of the node is no longer reachable AND if more than one interface/IP address is defined for the node, then the node will automatically get a new request IP address from the list of interfaces/IP addresses.

If **Delete empty network automatically** is checked, a network will automatically be removed, when the last object within the network is removed.

The selection menu **Auto Discovery** defines the discovery rule for networks that are generated automatically.

Host Display Name Format defines the structure of the default display names for newly discovered Hosts.

Note:
The values which are configured on this page are the default values which are used for each new discovered IP node. The values of already existing IP nodes will **not** be changed.

4.10.2 IP Parameter Configuration for an IP Network

If a subset or all IP nodes of a specific IP network should be handled simultaneously, this can be started by selecting the entry **Configure...** from the context menu of the IP network.

A list of all IP nodes can be opened by using the entry **Configure...** from the main menu **IP Manager** and using the tab **Node**.

Page **IP Node Parameter** shows a dialogue in which all IP nodes of the IP network are listed. One, multiple or all IP nodes can be selected (Ctrl + click) and the IP parameters can be changed with the dialogue elements on the right hand side. To submit the values, the respective button must be pressed for each parameter. This dialogue also offers the possibility to set the manage/unmanage status of the IP nodes from the IP network. For unmanaged IP nodes no automatic polling will be performed. Next to the general IP Parameters described in *Section 4.2.1*, the port for the reachability check can be set here. By default the check tests for port 7 (ECHO port). The key combination Ctrl+A will select all IP nodes simultaneously.

The selection menu **Template** can be used to assign an IP Configuration Template to individual IP nodes (see *Section 4.13.1*). When a template is selected, the template configuration will be used for the node.

Important Note:
The submap of an IP node may contain objects which are not managed by the IP Manager plugin (for example a HiPath/OpenScape 4000 system with IP address). These objects will not be influenced by an unmanage/manage action.

4.10.3 IP Parameter Configuration for an IP Node

To configure the IP parameters of a single IP node, the entry **Configure...** can be used by an “Administrator” within the IP node’s context menu.

This will open a window in which the tab **IP Parameter** can be used to configure the parameters for the selected network node as described in *Section 4.10.1*.

If more than one IP node is selected, a window that corresponds to the one described in *Section 4.10.2* will be opened instead. In this case the selected nodes are displayed in a list.

In addition, if the ping method **TCP** is selected, the **TCP Port** that should be used for the availability checks can be selected. By default the availability will be checked by using ICMP (Echo Request). If the **Ping Engine** is set to *Default*, the general method (see *Section 4.10.1*) will be used. If *Disabled* is selected, no ping will be started.This fact is indicated in the Status Explanation of the affected IP node.

The fields **Host** and **IP Address** can be used to manually assign a new hostname or a new IP address to the object. If the hostname is changed, the matching IP address will be determined automatically. If the IP address is changed without changing the hostname, the matching hostname for the new IP address will be determined automatically.

The selection menu **Template** can be used to assign an IP Configuration Template to individual IP nodes (see *Section 4.13.1*). When a template is selected, the template configuration will be used for the node.

The selection menu **Cluster** is used to determine whether the current IP node should be part of a cluster (see *Section 4.22*). The respective cluster can be selected in the menu, or the blank line can be selected to not assign the node to a cluster. The **+** button can be used to create a new cluster.

On the right hand side of the dialogue it can be manually configured, whether the IP node is an IP V4/V6 router or a network switch. By default these values are detected via SNMP. If this is not possible, or if the gathered values should be changed, the following values can be configured:

- **IP V4 Router Displaying:** If IP V4 Forwarding is set to *ON* (per SNMP or manually) the IP node is treated as an IP V4 Router. The IP node will additionally be shown inside the *Network Topology* container and is connected to each network it belongs to.
- **IP V6 Router Displaying:** If IP V6 Forwarding is set to *ON* (per SNMP or manually) the IP node is treated as an IP V6 Router. The IP node will additionally be shown inside the *Network Topology* container and is connected to each network it belongs to.
- **MAC Switch Displaying:** If MAC Forwarding is set to *ON* (per SNMP or manually) the IP node is treated as a network switch.

Note:
By setting the IP V4/V6 Forwarding by hand, routers can be integrated, without having access to their SNMP agent (e.g. if the SNMP communities are unknown). In this case, the corresponding network interfaces of the router have to be added manually.

Note:
If Status Poll relevant settings are modified, a Status Poll will be automatically started (see *Section 4.10*).

4.11 Configuration of the Interfaces of IP Nodes

The following sections describe how to display the interfaces of an IP node or cluster (see *Section 4.11.1*) or the values of an individual interface (see *Section 4.11.2*).

Section 4.11.3 explains the concept of interfaces defined as virtual in OpenScape FM

4.11.1 List of Interfaces of a Node or Cluster

A list of all interfaces assigned to an IP node can be opened via the context menu of the IP node object using the entry **Interfaces->Info**.

For clusters (see *Section 4.22*) it is possible to open such a list covering all IP nodes contained in the cluster. This can be done via the context menu of the cluster object using the entry **Configure**. The **Interfaces** page then contains the corresponding list.

The structure of the list is identical in both cases and contains a number of parameters recognized for the interfaces.

In addition, it is possible to define individual nodes as **Virtual** (see *Section 4.11.3*) or to remove this definition using the corresponding button.

4.11.2 Display of an Individual Interface

The configuration page of an individual interface can be opened via the context menu of the corresponding interface object by using the entry **Configure**. These can be found in the navigation tree within the container `Interfaces` of the corresponding IP node, or in the form of the Interface Lists described above (see *Section 4.11.1*).

A number of values are displayed on the page, such as the **IP Address**, **MAC Address** or Interface **Type**.

In addition, parameters such as the **Administrative Status** can also be set manually here.

For interfaces with an assigned IP address, two check marks can be set:

- If the check mark in front of **Check IP** is set, the IP address of the interface is additionally tested when the reachability of the IP node is checked. Otherwise, the check is only performed using the main IP address of the node. If the check fails, a corresponding internal event is generated
- The check mark in front of **Virtual** defines the corresponding IP address as virtual for the node (see *Section 4.11.3*).

4.11.3 Virtual Interfaces

Virtual interfaces in OpenScape FM are IP addresses that are not permanently assigned to a specific IP node object, but can dynamically switch to one or more other IP nodes under certain circumstances.

In a cluster, for example, this can be an address that is always assigned to the IP node of the cluster that currently provides a particular service. If the service on this node fails or is congested with requests, the address can be temporarily assigned by the cluster management to another node, that now performs the task.

If the corresponding service should be monitored, it may make sense to monitor the object with the virtual address.

However, if the individual elements of a cluster are to be monitored, it is not helpful to look at the virtual address, since it is not always known to which system the address.is currently assigned. This would prevent a problem from being reliably assigned to the affected component.

To check the availability of systems in the OpenScape FM, the OpenScape FM Server tests the reachability of the primary IP address of the system. If this cannot be reached, all other non-virtual addresses of the system are also checked. Virtual addresses are therefore ignored when determining reachability.

For some technologies, the OpenScape FM is able to automatically recognize the virtual addresses and mark them accordingly (see corresponding technology manuals). In other cases, this attribute has to be set manually (see *Section 4.11.1* and *Section 4.11.2*).

Hint:
The OpenScape FM often only detects with the next discovery whether and on which system a particular virtual address is currently valid. A virtual address can therefore be assigned to the wrong system or even to several systems simultaneously at specific times.

4.12 Configuration of the SNMP Parameters

The IP Manager plugin uses SNMP to communicate with the devices and agent systems.

This chapter describes how the SNMP Parameters necessary for the communication can be configured.

If the SNMP agent of an IP node supports the RMON MIB, the OpenScape FM Server can automatically configure itself as a trap recipient. If this is not the case, the OpenScape FM Server must manually be added as a trap recipient on the agent's system.

4.12.1 SNMP Parameters in the IP Manager

With the menu item **Configure...** in the main menu **IP Manager** an "Administrator" can modify the default SNMP polling parameters by selecting the tab **Default** (subpage **SNMP Parameter**). The **Show configuration** dialogue merely displays the current variables for "Operators". The values set in this dialogue are the default values which will be used for each newly discovered IP node, the values of already existing IP nodes are not changed.

Important Note:
If a new host is added to the OpenScape FM, a corresponding entry for this host is automatically created in the Password Manager (see *OpenScape FMDesktop User Guide*).
Changing the default setting has no effect on hosts that are already known.

The values defined for SNMP Port 161 for an IP node will also be used by the IP Discovery to check if SNMP agents are responding (*Section 4.2, "IP Discovery"*). For each IP node an entry for SNMP port 161 exists, no matter if an SNMP agent is running on this SNMP port or not.

The checkbox **Display unknown traps** is used to define whether traps that are not defined in any loaded MIB should be displayed within the Event Browser. The same setting can also be made under **Server->Administration->Server Properties** on the page **Event Browser**.

4.12.2 Changing SNMP Parameters for Several SNMP Agents of an IP Network or IP Node

If a number of SNMP agents should be configured for a single network or node at the same time, the entry **Configure...** (network) or **IP->Configure** (node) can be used within the context menu of the respective object.

A list of all IP nodes can be opened by using the entry **Configure...** from the main menu **IP Manager** and using the tab **Node**.

The page **SNMP Parameter** of the opened configuration window contains a list of the discovered SNMP agents.

Values defined for SNMP port 161 are also used by the IP discovery, to check whether SNMP agents reply (*Section 4.2, "IP Discovery"*). Independent from the fact that an agent is running, for each IP node an entry exists for port 161. For IP nodes, for which no SNMP agent was discovered on port 161, the SNMP port number 161 will not be displayed with a respective entry.

For each entry the **SNMP Version**, the number of **Retries** and the SNMP **Timeout** value can be set. The **Port** can additionally be set for entries of actually discovered agents where a port number is displayed.

Pressing an attached button will set the entered value for the selected nodes.

The settings for e.g. communities or security levels can be defined separately for **SNMP V1/V2c** and **SNMP V3** on the respective pages. Depending on the SNMP version selected for a node, the matching configuration will be used for the node.

The selection menu **Template** can be used to assign an SNMP Configuration Template to individual IP nodes (see *Section 4.13.2*). When a template is selected, the template configuration will be used for the node.

4.12.3 Changing SNMP Parameters for One SNMP Agent

To configure the SNMP parameters of a single SNMP agent, the entry **Configure...** can be used by an “Administrator” within the IP node’s context menu.

The three SNMP pages can be used to configure the parameters as described above.

On the first page, the selection menu **Template** can be used to assign an SNMP Configuration Template to individual IP nodes (see *Section 4.13.2*). When a template is selected, the template configuration will be used for the node.

If more than one IP node is selected, a window that corresponds to the one described in *Section 4.12.2* will be opened instead. In this case the selected nodes are displayed in a list.

4.12.4 Receiving SNMP Traps

The methods described above define how the SNMP parameters, that are used by the OpenScape FM to actively access other systems, can be configured.

The OpenScape FM receives SNMP traps from various devices. To receive SNMP V3 traps, it is necessary to define which coding parameters should be used.

The configuration of the method and parameters to receive the traps is handled centrally through the main menu entry **IP Manager->Configure...** on the page **SNMP V3 Trap**.

On this page the **Security Level**, the **Authentification Protocol**, the **Privacy Protocol** and their respective passwords that are used by the OpenScape FM to receive traps, can be defined.

4.13 Configuration Templates

Configuration Templates can be used to avoid the need to define the IP- and SNMP-configuration separately for each node. Each template represents a dedicated IP or SNMP configuration that can be manually or automatically assigned to a special type (group) of IP nodes.

A configuration template can be automatically assigned to IP nodes by defining assignment rules, based on the node’s IP address / subnet. By changing a setting in a configuration template, all IP nodes which are assigned to this template will be adjusted automatically.

Templates can e.g. be created for specific networks or for specific types of objects (routers, printers).

Example:
The availability of servers can be checked via different kinds of ping types. If ICMP is blocked for servers located in a distinct subnet, these nodes can automatically be assigned to a configuration template, which checks the availability of servers via TCP-Ping.

The general dialog to define configuration templates can be opened by using the entry **Configure...** from the main menu **IP Manager** and selecting the tab **Templates**.

The following subsections describe the definition of IP and SNMP configuration templates.

4.13.1 IP Configuration Templates

IP Configuration Templates can be defined by using the entry **Configure...** from the main menu **IP Manager** and selecting the tab **Templates** and subtab **IP Parameter**.

New templates can be created by pressing the button **+** at the bottom of the list. The button **-** can be used to delete selected templates. The **up** and **down arrow** buttons can be used to change the order position of a selected template.

The configuration uses the same parameters as the ones used for individual node configurations (see *Section 4.10.1*).

In addition the parameter **Template** is used to assign a name to the template. This name will be used to select the template for individual nodes and therefore should be meaningful and unique within the list of templates.

The parameters **Network** and **Mask** are used to define a network range that is assigned to the template. Whenever a new IP node is discovered, the list of templates will be checked in order. The first template with a matching network will be assigned to the new node as its initial configuration.

Note:
The **Network** and **Mask** parameters are ignored, if a template is manually assigned to a node. Every template can be assigned to every IP node. These parameters are only used for the initial automatic assignment.

When an existing IP Configuration Template is modified, the modification will affect all IP nodes to which the template is assigned to at this moment.

4.13.2 SNMP Configuration Templates

SNMP Configuration Templates can be defined by using the entry **Configure...** from the main menu **IP Manager** and selecting the tab **Templates**.

SNMP Configuration Templates are handled in the same fashion as the IP Configuration Templates described in the previous subsection (see *Section 4.13.1*).

In this case the **Network** and **Mask** parameters that are used for the default assignment of newly discovered nodes can be found on the subtab **SNMP Templates**. On this tab some base parameters can also be entered. The pages **SNMP V1/V2c** and **SNMP V3** are used to enter parameters based on the selected **SNMP Version**.

The configuration uses the same parameters as the ones used for individual node configurations (see *Section 4.12.1*).

When an existing SNMP Configuration Template is modified, the modification will affect all IP nodes to which the template is assigned to at this moment.

4.14 Saving and Loading Configurations

The current network configuration can be stored as an XML-file and loaded at a later time. For this the main menu entries **IP Manager->Save Configuration...** and **IP Manager->Load Configuration...** can be used.

Important Note:
Since the backup file may contain passwords in plain text, it should be kept in a safe place.
Before saving, the action must be confirmed by entering the user password.

When the functions are called, a file browser is displayed to define the name and position of the file or to select a file.

The currently included IP nodes, networks and SNMP configurations will be stored.

Via the menu item **IP Manager->Load Configuration...** a seed file can be loaded (see *Section 4.6.2*).

4.15 Changing SNMP Port for SNMP Agents

Port numbers for SNMP agents are variable within the OpenScape FM and can be changed via the various dialogues for configuring SNMP agents. This enables the access to the MIB content of already discovered SNMP agents, even if their port changes. These SNMP agents will not be considered incorrectly as new agents.

4.16 Adding SNMP Agents Manually

SNMP agents running on different ports than the standard ports can be added and configured manually by selecting the entry **New->SNMP Agent...** from the context menu of the IP node.

4.17 Layer-3 Routes

The OSI (Open Systems Interconnection Model) Layer-3 describes the Network Layer of an IT infrastructure.

Layer-3 is responsible for the forwarding of data packages between nodes that cannot directly communicate with each other. Usually these are nodes that are not located within the same network.

Besides the start nodes and end nodes, the objects relevant on this layer are devices that transfer data packages between different networks, like routers and Layer-3 switches.

Layer-3 routes are the possible paths that data packages can take within an IT infrastructure to travel between the networks from a selected sender (start node) to a selected receiver (end node).

Within the OpenScape FM, Layer-3 routes between two selected nodes can be displayed by using the entry **Show Layer-3 Route** within the main menu **IP Manager**.

This entry opens a window in which a start node (**Source**) and an end node (**Target**) can be entered with their hostname or IP address.

Pressing **OK** opens a window that contains a list with the possible Layer-3 routes between the selected nodes.

The list includes the Source and Target node and the routers and Layer-3 switches on the possible routes.

All list entries that are part of one possible path have the same entry in the column **Path No**. The column **Distance** displays the number of hops that are necessary to reach the respective node with the respective path. The combination of these two columns provides the information about the individual routes.

When other intermediate nodes, like Layer-2 switches located within a network, should be displayed, the Layer-2 plugin has to be used (see separate *Layer-2 Manager Plugin User Guide*).

4.18 Interface Up/Down Traps

When an SNMP Agent on an IP node recognizes that an interface has changed the status (from up to down or vice versa) or a warm or cold start has been executed, the SNMP Agent sends a trap to the OpenScape FM server. Depending on the trap a new event is generated which is displayed in the OpenScape FM Event Browser. The OpenScape FM will also update the status of the IP interface object, if the interface changes its status. A warm or cold start will update the whole IP node object.

The following table lists the four different trap types and the reaction performed by the OpenScape FM:

Trap Name	OID	Reaction
SNMP_Cold_Start	.1.3.6.1.6.3.1.1.5.1	start Discovery-Poll for this node
SNMP_Warm_Start	.1.3.6.1.6.3.1.1.5.2	start Discovery-Poll for this node
SNMP_Link_Down	.1.3.6.1.6.3.1.1.5.3	interface icon color will be set to the status “critical“
SNMP_Link_Up	.1.3.6.1.6.3.1.1.5.4	interface icon color will be set to the status “normal“

Table 2 IP node traps and reactions

Note:
If the SNMP Agent of the IP Node supports the RMON MIB, the OpenScape FM server can register itself automatically as a trap receiver. If this is not the case, the OpenScape FM has to be manually configured on the IP node as an additional trap destination.

If the OpenScape FM is not registered as a trap destination on an IP node, it will not receive traps from the IP node and the status of this node can only be determined by performing a Status Poll. Depending on the result of the Status Poll the interface status is set to up (green) or down (red). For more information about the Status Poll see *Section 4.10, “Configuration of the IP Parameters”*.

4.19 Monitoring of Ping Results

The OpenScape FM is checking the status of an IP node or a specific service on the IP node by using different reachability checks (“pings”). For a wide range of object types (SNMP, HTTP, Telnet, SSH, Web Service etc.), the reachability status is determined by performing such pings (see *Section 4.10.1*). The status is modified by a respective new event.

If the pings are not answered within a configured timeout for a configured number of successive retries, the OpenScape FM considers the tested IP node as not reachable and therefore in a *critical* status.

But even if the pings are answered within the timeout interval, growing ping times might indicate a problem.

For example, if a web server is running on a host where a process/service is constantly consuming too much cpu time, the response time of this web server is likely to increase. Another example, which may result in the increase of the response time or retry count, would be a router/switch that is handling a high traffic volume.

To detect such problems, the OpenScape FM automatically collects the determined response times of the different ping operations for all IP nodes. The collected data is exported to the database defined in the Online Data Export Configuration (e.g. MySQL). The response times are tagged, so that their values can be selected in the reports. The values are collected with the help of the System Management Monitor `ResponseTimes.Delay`.

To display the results (in milli seconds), the IP node objects provide the entry **Host->Response Time** within their context menu. This entry opens a standard System Management result page that contains the collected data for the respective host.

The page **Thresholds** of the result window can be used to define additional value thresholds that trigger status changes and corresponding events when they are exceeded.

4.20 HTTP and HTTPS Servers

Every HTTP server which has been found on port 80, 280, 8080, 8085 or 8888 during the IP discovery process, i.e. every HTTP server which has answered the request before the timeout point, is displayed on the submap of the corresponding IP device symbol (see *Section 5.2*). Every HTTP server that has been found in the same fashion on port 443, which is generally used by HTTPS servers, will be displayed as an HTTPS icon on the submap of the corresponding IP device symbol.

HTTP server running on different ports than the standard ports could be added and configured manually by selecting the entry **New->Web Server...** from the context menu of the IP node.

Both symbol types offer an HTTP context menu with the entries **Configure** and **Home Page** or the entries themselves:

- With the help of the entry **Home Page** the starting URL of the respective HTTP/HTTPS Server can be accessed.

  In case of an HTTPS server, the URL of the Home Page starts with "`https://`".

- Using **Configure** opens a window that consists of two pages:

  - On the page **HTTP Connection Parameter** the necessary login data for the HTTP access can be entered.

- The page **Certificate** displays the current certificate, which can be accepted by marking the check box **Accept certificate**.

It has to be kept in mind, that deleted symbols will be displayed again when they are discovered during a scan.

4.21 IP Address Mappings

Since the number of IP addresses in the internet is limited, a lot of intranets use non-routable internal addresses within the private IP address scope. NAT (Network Address Translation) enables a device, like a router, which is located between the internet and the intranet, to translate external into internal addresses and vice versa. There are different forms of NAT, static and dynamic NAT. OpenScape FM supports static NAT, i.e. the static mapping of one defined external (i.e. unique in the internet and routable) to one defined internal (i.e. routable only in its specific intranet) IP address.

The mapping data is stored on the respective routing devices as NAT mapping tables, and all devices which are managed by one such device are called a NAT domain.

OpenScape FM supports static NAT, and since the IP Manager is the module which manages everything concerning IP addresses, the management of NAT tables is done by the IP Manager. Every time OpenScape FM discovers a device which hosts NAT mapping tables (and for which NAT mapping is supported by OpenScape FM!), it registers the corresponding mappings and uses them to manage the IP nodes. NAT routers or devices cannot be configured via OpenScape FM, but the OpenScape FM client GUI provides comfortable access to NAT mapping policies which have been registered in the OpenScape FM database.

The NAT mappings registered within the OpenScape FM can be displayed by using the entry **IP Address Mappings...** from the main menu **IP Manager**. The entry will only be displayed when at least one NAT entry has been discovered by the OpenScape FM. The shown table contains the following columns:

External: the external IP address

Internal: the corresponding internal IP address

Netmask: the subnet mask used in the indicated network

Node: the node (i.e. device) where the table is stored on.

All rows that contain the same node define the rules for a NAT domain.

IP objects with NAT addresses

IP objects which have two IP addresses, an internal and an external one, display both addresses on their label and in the “Info” of their interface. The „Info“ can be opened via the context menu **Info** of the interfaces container of the respective IP node. Here all interfaces found for this IP node are listed.

4.22 Cluster

A cluster is generally a number of interconnected computers that can be viewed from the outside as a single system.

For example, clusters are used for hot or cold standby systems or for load balancing across several systems.

Although the tasks within the cluster are performed alternatively or simultaneously by several systems of the cluster, this is usually not transparent for external systems. They always communicate with the same IP address of the cluster and it usually is irrelevant from which of the cluster systems e.g. a requested web service is performed.

From the OpenScape FM perspective, a special approach to clusters makes sense, since alleged errors that occur on individual systems of a cluster do not represent a real malfunction for an monitoring technician.

For example, if a service runs only on one system of the cluster and is inactive on all other systems, this can be a deliberate behavior. In a cold standby system it is even always intentional that the systems in the waiting status are not active.

In these cases it is reasonable for the OpenScape FM not to report supposedly critical status (service or system not available) as long as the corresponding task is still fulfilled by the cluster in order to hide the 'wrong' critical status from the monitoring technician.

This chapter describes how clusters are generally handled in OpenScape FM and how they can be configured.

Working with clusters in the OpenScape FM Web is described in the OpenScape FM Web user guide.

4.22.1 Status Determination in Clusters

In OpenScape FM clusters are represented by one cluster container object each. This container holds the IP node objects of the systems that are part of the cluster.

The systems contained in a cluster are not handled differently by most OpenScape FM functions than systems not contained in a cluster. However, the determination of their status is changed significantly:

The status of an object within a cluster is determined not only by the usual methods of status determination, but also by the status of similar objects in the other systems of the cluster. In this respect similar means that the object names differ only by the IP address of the affected systems.

For example, if two IP nodes A and B both have an HTTPS Web service on port 3080, the object names of these services are `IPhttps:<IP_of_A>:3080` and `IPhttps:<IP_of_B>:3080` and they are therefore similar. The IP nodes themselves are also similar, since in this case they have the object names `IPNode:<IP_of_A>` and `IPNode:<IP_of_B>`.

So that individual IP nodes that are completely failing can still be recognized easily, the IP nodes of a cluster are automatically placed on the Ignore List (see *Section 4.22.2.2*) and are not included in the cluster calculation.

If the status Critical is directly assigned to an object in a cluster and not propagated by a child object, the OpenScape FM checks whether a similar object currently does not have the status *Critical* within the cluster. If this is the case, the OpenScape FM assumes that the cluster can still fulfill the function of the affected object, and the object is therefore not set to the status Critical but to the status *Disabled* (dark brown). Objects in a cluster only become *Critical* by direct status assignment if all similar objects are also *Critical*.

The same method is also used for the reachability status of the affected objects. If applicable, this is also only set to *Disabled* instead of *Critical*.

4.22.2 Configuration of Clusters

The configuration of clusters consists of two steps. The setup of the clusters themselves (see *Section 4.22.2.1*) and the configuration of the relevant objects for the status determination (see *Section 4.22.2.2*).

4.22.2.1 Setting Up Clusters

A list of all clusters and their systems can be opened by selecting the entry **IP Manager->Cluster** from the main menu. The displayed view contains the central **cluster container** and all clusters and their systems as child objects.

Defining New Clusters and New Cluster Systems

A variety of clusters and their systems are automatically created for different technologies by the OpenScape FM. More details can be found in the user manuals of the corresponding technologies.

In addition, new clusters can be created manually using two methods:

- By selecting the menu entry **New->Cluster** from the context menu of the central cluster container or of a topology container.

  Individual systems can be added into the displayed container using Drag&Drop or using **Edit->Copy** and **Edit->Paste**

- By using the IP parameter configuration of an IP node (see *Section 4.10.3*) and using the **+** button next to the **Cluster** selection menu or by using the context menu entry **New->Cluster** of an IP node. This additionally assigns the current IP node to the new cluster.

  If an existing cluster is selected in the **Cluster** selection menu, the current IP node is assigned to the cluster.

If an IP node is added to a cluster, at this moment all events assigned to this IP node are examined once. Events that describe a problem covered by a similar object (see *Section 4.22.1*) within the cluster are automatically acknowledged during this examination.

Important Note:
An IP node can only be assigned to one cluster. If it gets assigned to another cluster, any previously existing assignment is removed.

Network Topology for Clusters

Clusters are located in the same position within the Network Topology as the IP node with the highest Network Precedence contained within them (see *Section 4.4*).

Deletion of Existing Clusters and existing Cluster Systems

Existing clusters can be deleted and cluster systems removed from clusters by deleting their symbol below the central cluster container.

Cluster systems can also be deleted from a cluster by selecting the **blank entry** in the **Cluster** selection menu in their IP parameter configuration.

4.22.2.2 Object Configuration in Clusters

The central cluster container contains a respective container for each defined cluster.

Using the entry **Configure** from the context menu of these containers, the detailed configuration of the corresponding cluster can be called, which consists of two configuration pages:

- On the page **Interfaces** it can be determined which of the interfaces of the IP nodes contained in the cluster are to be considered virtual. This corresponds to the function of virtual interfaces described in *Section 4.11*. Since virtual interfaces and their IP address are not allocated to a fixed IP node over time, they are not taken into account when determining the reachability of an IP node.
- On the page **Ignore List** it can be defined which child objects of the IP nodes contained in the cluster should not be affected by the cluster function.

  For this purpose, individual objects can be moved from the subtree of the cluster to the list **Selected Objects** on the right. These objects are then not part of the special status calculation of the cluster.

  Selected objects are neither set to *Disabled* status or reachability status nor is their status used to determine the status of similar objects.

  The IP nodes of the cluster are automatically placed on the Ignore List. For example, in a cold standby system, these can be removed from the list so that they are not always recognized as unavailable and set to *Critical*.

4.23 Network Access Control (NAC)

The Network Access Control (NAC) monitors whether unwanted systems get connected to the monitored network. Which systems are wanted or not wanted is configured with a rule set. This rule set defines which IP or MAC addresses are allowed or should be prohibited.

If the access of an unwanted system is detected, the NAC informs about it by generating an event which contains the IP/MAC address of the unwanted system.

A rule set defines which IP and MAC addresses are allowed and which are forbidden.

The rule sets can be separately build for IP addresses and MAC addresses. The rule sets consist of two components:

1. A list of addresses which are explicitly allowed, forbidden or have to be checked.
2. Filter definitions that, based on MAC address patterns or IP ranges, determine which address ranges/patterns are forbidden or allowed.

The two components make it possible to create a list of allowed addresses and to use the definition of a general filter to deny all other addresses.

4.23.1 Rule Evaluation

The check against the rule set will be performed whenever an address (IP or MAC) is detected.

Detections are e.g. made when:

- An IP node is added.
- During the Status Poll of an IP node.
- During a Configuration Poll of a switch/router.
- When a Link Up or Link Down Trap is received from a switch or router.

This should be considered when the polling intervals for the respective devices are configured.

When a new address (IP or MAC) is detected, the rule set for the IP or MAC address will be independently checked in the following sequence:

1. Initially it will be checked whether an entry for the address exists within the explicit address list.

   If this is not the case, the check continues with the second step.

   Else the procedure follows according to the definition of the respective address within the list. There are three possible definitions:

   - The address is *Allowed*: The address is wanted and the check is canceled.
   - The address is *Forbidden*: In this case, an event is generated that informs about the unwanted access. The check will be canceled.
   - The address is entered as to *Prove*: The second step of the check will be performed.

2. It will be checked whether an object with the respective address exists within the OpenScape FM.

   If this is the case, the address will be allowed and it will be entered into the explicit list as allowed. The check will be canceled.

   If no matching object exists within the OpenScape FM, the third step will be performed.

   Hint:
   This leads to the fact that NAC filters will not be used on IP nodes already added to the OpenScape FM. They will be checked only once during the adding process.

3. The last step checks, whether a matching filter definition exists for the address. The filter definitions will be checked in order depending on the list entries, and the first matching filter will be used for the evaluation.

   If no filter matches or the first matching filter has the value *Prove*, the address will be allowed. The address will be added to the explicit list as to *Prove*. No event will be generated.

   If the first matching filter has the value *Allowed*, the address will be allowed and it will be entered into the explicit list with value *Allowed*.

   If the first matching filter has the value *Forbidden*, the address will be forbidden and it will be entered into the explicit list with value *Forbidden*. In addition an event will be generated that informs about the unwanted system.

The configuration of the NAC rules is done via the general configuration panels of the IP Manager. It can be opened by selecting the menu item **IP Manager**->**Configure**. The NAC configuration is handled on the tab **NAC Rules** which consists of four additional tabs:

- **MAC List**: Here all discovered MAC addresses are displayed. The list can be extended manually (see *Section 4.23.3*).
  It can be explicitly defined, if the discovered MAC address is wanted or not. Further details can be found in *Section 4.23.2*.
- **MAC Filter**: Here filters for MAC addresses are defined. MAC address patterns are added and it is declared, whether MAC addresses matching this pattern are wanted or not. A description how general NAC-Filters are defined can be found in *Section 4.23.4*.
- **IP List**: Here all discovered IP addresses are listed. IP addresses are e.g. discovered via the ARP cache or the interface tables of SNMP agents. All network addresses of added IP nodes are in this list. The list can be manually extended (see *Section 4.23.3*).
  It can be defined in this list whether an IP address is wanted or not. Further details can be found in *Section 4.23.2*.
- **IP Filter**: Here filter for network ranges can be configured. Network addresses and their subnet masks are added for this, and it is defined if addresses according to this range are wanted or not. A description how general NAC-Filter are defined can be found in *Section 4.23.4*.

4.23.2 Allowing/Forbidding an Address Explicitly

An IP address or MAC can be explicitly allowed or forbidden by using the tab **IP List** or **MAC List.**

The lists provide the following information:

- **IP** / **MAC**: Here the discovered IP / MAC address is shown.
- **Node**: If an IP node for this address already exists within the OpenScape FM, it is displayed here.
- **Detection**: Shows by which mechanism this address was detected. The following values are possible:
  - *arpcachev4* and *arpcachev6*: The address was read from the ARP cache of an SNMP agent.
  - *iftable*: The address was read from the interface table of an SNMP agent.
  - *user*: The address belongs to an IP node which was added to the OpenScape FM or the address was added manually.
  - *imported*: This address has been imported via the import function (see *Section 4.23.3*).
  - *layer2*: The address was discovered by the Layer 2 Plugin.
- **Source**: The source of the address.
- **Type**: Defines the handling of this address, if it is discovered again:
  - *Allowed:* The address is allowed and no further checks of filters will be performed for this address.
  - *Forbidden:* An event will be generated informing that an unwanted address was detected. To avoid unnecessary duplicates of events, the generation of an event is subject to conditions which are described in *Section 4.23.5*.
  - *Prove Filter*: The address is allowed but the filters will be checked for this address in the future.

- **Date**: The last detection date for this address.
- **Acknowledged**: If an unwanted access event was generated for the address, this states whether the event has been acknowledged.
- **Comment**: A comment that can be manually defined or that is set by a matching filter when the address is detected (see *Section 4.23.4*). Matching filters only add comments, if the field is empty.

The **Type** can be set directly in the table by double clicking the type and selecting the according value.

If more than one entry should be changed at the same time, these entries can be selected and then be changed via the field **Type** and the button **Save** on the right side.

4.23.3 Extending the Address Lists

The lists in the tabs **IP List** and **MAC List** can be extended manually. Two options exist:

1. Directly adding a single address: An individual entry can be created by using the button **+**. It can be edited in the table itself or via the text fields and **Save** button on the right side.
2. Importing a list of IP or MAC addresses: Via the button **Import** a list of IP addresses or MAC addresses can be added. Existing entries for the same address will be overwritten. The file has to be consistent with the following format:

```
nac.IP;ipmanager.label.ipid.Node;nac.Detection;nac.Source;nac.Type;nac.Date;nac
.Acknowledge
<IP Address>;;;;<Type>;;
<IP Address>;;;;<Type>;;
```

Individual IP and MAC addresses can be deleted from the lists by using the button **-**.

To save lists, the export function can be used. The export function creates a semicolon separated list of all detected IP or MAC addresses. The button **Export** on the respective tab opens a file chooser. In this file chooser the directory can be selected, where the list will be saved.

4.23.4 Definition of a Filter

General filters can be defined via the tabs **IP Filter** and **MAC Filter**.

In both cases the button **+** can be pressed within the respective tab to define a new filter. This generates a new entry within the table. The entry can be edited directly in the table or via the text fields and the **Save** button on the right side.

The **Index** specifies the order in which the filters will be applied on the detected address. When a filter matches all following filters will be ignored.

For IP addresses, IP network ranges (**Network**) and their masks (**Mask**) are defined.

For MAC addresses, a MAC address pattern can be defined in the field **MAC Pattern**. Regular expressions can be used for this.

Regular Expression	*Description*
`.*`	any alpha numeric pattern
`^03.*`	any alpha numeric pattern, which starts with the numbers 03
`.*03$`	any alpha numeric pattern, which ends with the numbers 03
`^[03].*`	any alpha numeric pattern, which starts either with the numbers 0 or 3

Table 3 Regular Expressions: Examples for search patterns

Type specifies how an address that matches the pattern should be handled. Type can be „Allowed“, „Forbidden“ or „Inactive“.

- *Allowed*: The matching address is added to the respective list as *Allowed*. No further filter checks will be done for this address in the future.
- *Forbidden*: The matching address is added to the respective list as *Forbidden* and no further filter checks will be done for this address in the future. Additionally, an event is generated, showing that a forbidden address was detected. The generation of an event is subject to conditions which are described in *Section 4.23.5*.
- *Inactive*: This filter is not used and will be skipped.

Comment defines a comment that will be automatically added to newly detected addresses that match the respective filter.

4.23.5 The NAC Event

If an IP or MAC address is detected as forbidden for the first time, an event is generated.

If the address is discovered again and the former event has not yet been acknowledged, no further event will be generated. Instead it will be extended by an annotation. If the event has already been acknowledged, a new event will be generated.

The event contains the discovered address and the interface where the address has been detected.

4.24 Applications

The OpenScape FM allows the execution of applications, as so-called Access Applications, for selected IP nodes directly from their context menu (see *Section 4.24.1*).

It is also possible to monitor the execution status of individual applications (see *Section 4.24.2*).

4.24.1 Access Applications

Access Applications are local applications which are defined for some or all IP nodes and can be executed directly from the context menu of the different IP node objects.

If a user has **Administrator Rights**, the context menu of the IP node objects contain the submenu **Access Applications**. This menu contains one entry per defined access application which can be used to call them. In addition, it encloses the entry **Configure...** which can be used to add new applications, or to configure or delete old ones. If this entry is selected, the configuration opens.

Figure 1 shows the mechanism that is used by the server to connect to an access application.

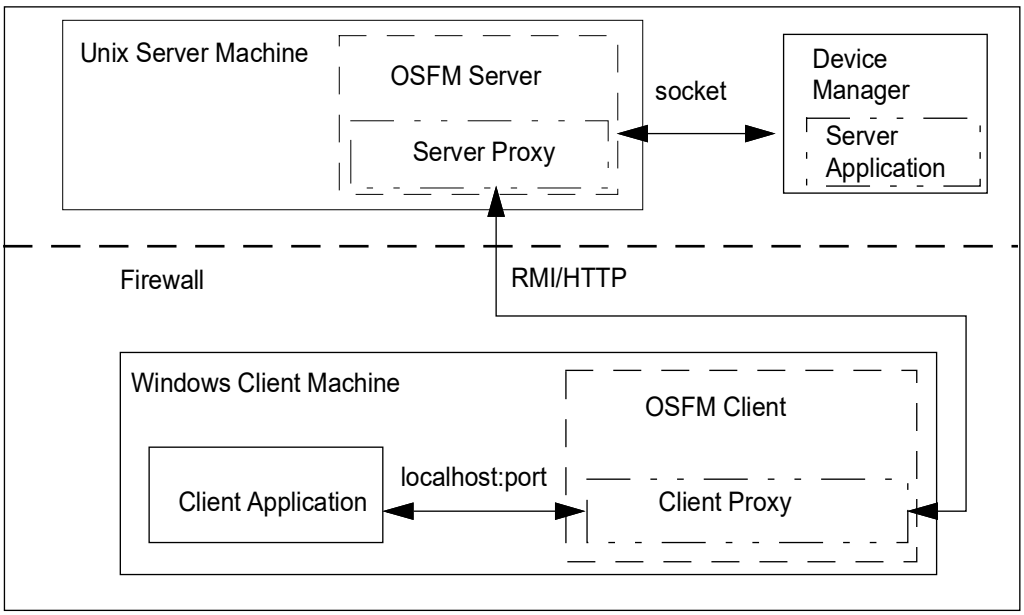


Figure 1 Overview of the Proxy Functionality

The example displayed in *Figure 1* consists of an OpenScape FM Client system, an OpenScape FM Server system and a Device Manager system on which the server application is running.

The last two systems are behind a firewall, which is configured in a way that only the access to the OpenScape FM Server is allowed. This prevents the client system from directly connecting to the server application.

To allow the access from an OpenScape FM client to a server application, the following conditions have to be met:

- The local Client Proxy has to be started. In case of an activation, this will be done automatically. The Client Proxy connects itself to the OpenScape FM Server, transmits the target IP address and respective port, and requests a session id. This id will be used in step two, to create an HTTP tunnel to the OpenScape FM Server.

- The local (configurable) access application will be started and connects itself to the local proxy. This proxy acts like the server of the access application, but the whole input and output datastream will be send through the OpenScape FM Server to the application server. This is done by an HTTP connection to the web server of the OpenScape FM Server. The used URL contains the session id (requested in step one) to identify and authentify the client.
- The Proxy Module on the OpenScape FM Server accepts the incoming HTTP connection, identifies the target system through the session id contained in the URL, and opens a socket on the target system. The HTTP connection (TCP socket) will be kept open and the application's data traffic will be handled through this connection.

The proxy functionality will only work for access applications that only use one port for the communication. If more than one port is used, a direct connection has to be established. In this case no proxy may be used. The access application will be started and the OpenScape FM takes no further part of the communication management.

To start an access application using a Client Proxy, first a menu entry for the respective IP node has to be created (see *Section 4.24.1.1, "Listing Access Applications"*). If the menu entry is selected, the access application will be started and a session to the target system will be established. The access application itself has to be installed on the machine on which the OpenScape FM Client is running. Since the access application will be started on the OpenScape FM Client's machine, the defined menu entry is only available for OpenScape FM Clients running on the machine on which the definition was made.

Since Telnet is a generally available application for remote access, Telnet will be setup by the OpenScape FM by default (see *Section 4.24.1.3, "Telnet Recognition and Integration"*). Additional Access Applications can be manually configured. An example for an application that is located behind a firewall can be found in *Section 4.24.1.2, "Configuring Access Applications"*.

4.24.1.1 Listing Access Applications

Selecting an IP node's menu entry **Access Applications... -> Configure...** , will open a configuration window.

Note:
Administrator rights are required for this action.

The window contains a list of all access applications already configured on the IP node. These can be reconfigured or deleted. The window is also used to add new applications to an IP node.

The window consists of the following elements:

The list contains one entry per already defined application. The column **Application Name** shows the name of the application. This name will be displayed within the IP node's context menu to start the application. The column **Local Definition** shows whether the application was only defined for one IP node (checked) or for all IP nodes (unchecked).

- The button **Add...** opens a configuration window for access applications, in which new access applications for IP nodes can be defined.
- The button **Edit...** also opens the configuration window for access applications. This can be used to change the configuration for the application selected within the list.

- The button **Delete...** deletes the applications for the IP nodes selected in the list. The respective applications will be removed from the list and the corresponding menu entries will be removed from the IP nodes‘ context menu.
- The button **Delete Globally...** will remove the selected application from all IP nodes for which the application was defined as a global access application.
- The button **Close** closes the configuration window.

4.24.1.2 Configuring Access Applications

With the help of the configuration window for access applications the various access applications can be configured. This window can be used to define a new access application as well as to reconfigure already existing definitions.

The window consists of the following elements:

- The field **Application Name** shows the name of the application. It is used within the IP nodes’ context menu of the affected IP nodes. If a new application is defined, the name can be defined in this field.
- The field **Command** contains the path which is used to call the application. The path can be entered manually, or it can be selected within a file system browser which can be opened with the button **Browse...** .
- The field **Parameters** is used to define the parameters with which the application will be called. Besides ’fixed’ entries, two macros can be used. `$HOST` and `$PORT` will be replaced with the respective values depending on the selected **Connection Method** (see below).
- The field **Timeout (sec.)** defines the maximum time the Client Proxy will wait to create a connection to the Client Application. This time will be exceeded e.g. if the application could not be started successfully.
- The field **Target Port** defines the port which is used by the Server to connect the application in Proxy mode.
- The field **Local Port** is only editable if ’Proxy’ is selected as a **Connection Method**. The field defines the local port on which the proxy will be started. The Client Application has to connect itself to this port. If the entry is ’0’, a dynamic port will be used. In both cases the actually used port number will replace the macro `$PORT`.
- In the menu **Connection Method** one of two methods can be selected:

  Proxy means that a local proxy will be started when the application’s entry will be selected within an IP nodes context menu. In this case the macro `$HOST` will be set to ’localhost’. The macro `$PORT` will be set to the local proxy port number. The connection to the target server will be tunneled by the proxy and the OpenScape FM Server. Applications which use more than one port for their communication can’t use this method.

  Direct means that the access application will be started without the proxy. The macro `$HOST` will be set to the IP address which was identified for the IP node. The macro `$PORT` will be set to the configured target port number. If this method fails, a connection with the help of the proxy will be tried. The direct method will only work if the target server can be reached from the OpenScape FM Client.
- If the button **Ok** is pressed, the entered configuration gets active. If a new access application was entered, an entry for the new application will be added to the context menu of the affected IP note.

- If the button **Apply Globally...** is pressed, the configuration will be used for all IP nodes which are known to the system at this moment. Access applications that are registered with the same name will be overwritten by this action. For all IP nodes an entry for the application will be added to the context menu.

4.24.1.3 Telnet Recognition and Integration

Telnet is a generally available application which allows remote access to an arbitrary computer within a network. The OpenScape FM sets this remote access up as a standard access application for all identified IP nodes.

For every IP node it will be checked whether a running Telnet service exists. The check is considered successful, if a scan for port 23 is successful. In this case the menu **Telnet** will be added to the IP node's context menu.

In addition to the automatic setup of the access application a symbol that represents the Telnet function will be added to the submap of the IP symbol. The status of the Telnet symbol depends of the reachability of the Telnet service installed on the IP node.

If the Telnet service is not reachable using port 23, the status will change to 'critical', else the status will be 'normal'. The context menu of the symbol contains the entry **Telnet**, that can be used to start a Telnet session on the target system. For this, the OpenScape FM Client uses a locally installed Telnet application.

When the menu entry gets selected, e.g. on Windows systems only the command `cmd /c start telnet` without a path will be executed. This will only work if the telnet application is located within the standard path.

The Telnet application can be configured or deleted with the menu entry **Access Applications->Configure...** . If a Telnet entry has been deleted, but a Telnet is still running on the system, it will be discovered and added again during a new IP discovery.

It has to be considered that changes on the configuration will only be done for the OpenScape FM client machine on which the modification was performed.

4.24.1.4 SSH Recognition and Integration

SSH (or Secure Shell) is a generally available application which allows secure encrypted remote access to an arbitrary computer within a network. The OpenScape FM sets this remote access up as a standard access application for all identified IP nodes.

For every IP node it will be checked whether a running SSH service exists. The check is considered successful, if a scan for port 22 is successful. In this case the menu **SSH** will be added to the IP node's context menu.

In addition to the automatic setup of the access application a symbol that represents the SSH function will be added to the submap of the IP symbol. The status of the SSH symbol depends of the reachability of the SSH service installed on the IP node.

If the SSH service is not reachable using port 22, the status will change to 'critical', else the status will be 'normal'. The context menu of the symbol contains the entry **Start SSH Application**, that can be used to start a SSH session on the target system. For this, the OpenScape FM Client uses a locally installed SSH application.

The context menu of the SSH symbol is transferred to the context menu of the IP node. In addition to starting the application, commands and scripts can be executed here, and files can be uploaded or downloaded.

When the menu entry gets selected, e.g. on Windows systems only the command `cmd /c start ssh` without a path will be executed. This will only work if the SSH application is located within the standard path.

The SSH application can be configured or deleted with the menu entry **Access Applications->Configure...** . If a SSH entry has been deleted, but a SSH is still running on the system, it will be discovered and added again during a new IP discovery.

It has to be considered that changes on the configuration will only be done for the OpenScape FM client machine on which the modification was performed.

4.24.2 Application Monitoring

The application monitoring shows the status of programs running on a server. The SNMP agent of the respective server must support the hostresources MIB, like e.g. Windows 2000 machines.

Important Note:
The Hostresources Plugin module has to be initialized in order to enable the OpenScape FM Server to monitor applications. The plugin gets initialized by using the main menu entry **Server->Plugins->Initialize Hostresources Plugin**.

There are two states for the programs: *running* and *not running*.

To activate the application monitoring, the **Server** symbol and the **SNMP** symbol on the next level have to be opened with a double click. This level shows a MIB II symbol called *Host Ressources*.

To start the monitoring the menu item **Activate/Deactivate** has to be selected from the context menu of this symbol. A new symbol appears one level above with the name Applications. This symbol provides two context menu entries **Running Software** and **Installed Software** described in the next sections.

4.24.2.1 Installed Software on a Server

To display the software installed on a server, the entry **Installed Software** has to be selected from the context menu of the *Applications* object. The next window shows a five-column list with all applications which have entries in the hostresources MIB. An *Index*, the *Software Name*, the *Software ID*, *Software Type* and *Installation Date* are displayed.

4.24.2.2 Monitoring Programs

To display the programs running on servers that support the host-ressources MIB, the entry **Running Software** has to be selected from the context menu of the *Applications* object.

An eight-column list is displayed which indicates several parameters for each application: an *Index*, the *Software Name*, the *Software ID*, the *Path* to the binary, *Run Parameters*, the *Software Type*, the *Status* [*running*|*not running*], and the *Monitored Status* [*monitored*|*ignored*].

The *Monitor Status* defines, whether a server process gets monitored or not. This can be set for the selected processes by using the selection menu **Monitor Status** [*monitored*|*ignored*] and the button **Set**.

The button **Reload** has to be used to refresh the display after a change.

There are two ways a server can obtain information concerning the status of a monitored program: polling and traps. If a monitored program stops running, the status of the object and therefor the color of the corresponding symbol will change with the next poll. Nothing has to be configured to use polling. More about receiving SNMP traps from applications can be found in *Section 4.24.2.3*.

To see on which hosts the application monitoring has been activated, the entry **SNMP->Hostresources->List Application Groups** can be selected from the main menu. A list with the *Agent Name* and *IP Address* of each host, where application monitoring has been started, is displayed and the current *Status* is indicated.

4.24.2.3 Receiving SNMP Traps from Applications

If an application should send traps, the respective system has to be configured manually.

The trap generation on a machine running a Windows operating system is based on events that are sent to the Windows Eventlog. It can be configured, which of these events should result in SNMP traps. Therefor, this mechanism can only be used for programs which are capable of generating entries in the Windows Eventlog. In order to configure SNMP trap generation, the following steps have to be accomplished:

- It has to be checked, if an SNMP agent is installed on the server. On Windows 2000 machines, an SNMP agent should be installed after the installation of the operating system.
- SNMP service must be up and running.
- SNMP trap service must be up and running.
- `evntwin.exe` can be used to define the events that should produce traps for the applications that should be monitored. Only applications that offer this mechanism can be configured to send traps.

4.25 Control Center Overviews

If the Control Center plugin has been initialized, a number of Control Center overviews are provided for IP Manager objects. They can be displayed by using the main menu entry **IP Manager->ControlCenter Overview...**. The following chart windows are available:

- **Recent 10 Non-normal Routers**: This window lists up to ten routers whose status is not normal.
- **Recent 10 Non-normal Switches**: This window lists up to ten switches whose status is not normal.
- **Recent 10 IP Nodes Gone Critical**: This window lists up to ten IP nodes whose status most recently changed to critical.
- **Recent 10 IP Interfaces Gone Critical**: This window lists up to ten IP interfaces whose status most recently changed to critical.
- **IP Events Over Time:** This window shows the distribution of events within category ’IP Manager’ by time.

More about the Control Center can be found in the respective user guide.

5 Symbols and Overviews

All objects are represented on views (i.e. submaps and/or trees) by symbols. The Desktop assigns specific symbols to each type of object. This chapter contains a short overview over the IP Manager symbols.

The appearance of each symbol can be changed (**Properties**, **Symbol->Symbol Properties**), but this is not recommended for system symbols.

5.1 Topology Symbols

- Topology Network symbol

- Topology Subnetwork symbol

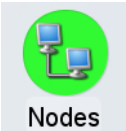
- Meta edge symbol (submap view)

- Meta edge symbol (tree view)

5.2 IP symbols

- IP network symbol

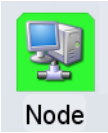
- IP node container symbol



- IP node symbols:
  - Router symbol

- Switch symbol

- IP node symbol



- Remote Desktop Protocol symbol

- Telnet symbol

- IP Interface symbol

5.3 Overviews

If the ControlCenter plugin has been initialized, a number of ControlCenter overviews are provided for IP node objects.

The following overviews are provided:

- The last ten IP Nodes that changed to the status '*critical*' and that are still in that status.
- The last ten IP Interfaces that changed to the status '*critical*' and that are still in that status.
- The last ten Routers that changed to a status worse than '*normal*' and that are still in that status.
- The last ten Switches that changed to a status worse than '*normal*' and that are still in that status.
- The distribution of events within category '*IP Manager*' by time.

The overviews can be displayed by selecting the entry **ControlCenter - Overview** within the main menu **IP Manager**.

More about the ControlCenter can be found in the respective user guide.

A Access Rights

The IP Manager access rights are integrated into the general access management (*see OpenScape FM Desktop User Guide*).

The description of the individual rights can be found within the tooltips for the corresponding right symbols (tree or submap).

The names of the rights for the IP Manager Plugin begin with the designation *IP Manager*.

Index

A
Access Applications 42
Add
    IP Network 14
    IP Nodes 18
    SNMP Agent 31
Address
    NAC 39
Address List
    NAC 40
Address Range
    Display 16
    Ignore 15
Application group 47
Applications 41
    Execution 42
    Monitoring 46
ARP Cache Scan 13

B
Basic Concepts 7

C
Change
    SNMP Agent Port 31
Cluster 34
    Configuration 36
    Creation and Deletion 36
    Object Configuration 37
    Status 35
Configuration
    Access Applications 44
    Cluster 36
    Interface 26
    IP Node IP Parameters 25
    IP Parameters 22
    IP Templates 30
    Load and Save 31
    Network IP Parameters 24
    SNMP Parameters 28
    SNMP Templates 30
    Templates 29
Configuration Poll 22
Control Center 50
Control Center Overviews 47

D
Default
    Network 18
Delete
    IP Node 20
Discovery Poll 22

E
Event
    NAC 41
Expiration Time 21

F
Filter
    NAC 40

H
Host-Resources-MIB 46
HTTP and HTTPS Servers 33

I
Initialization 9
Installation 9
Interface
    Configuration 26
    Individual 27
    List 26
    Virtual 27
Interface Up/Down Traps 32
IP
    Configuration Templates 30
IP Address
    Changes 20
    Mapping 34
    Range Scan 13, 19
IP Discovery 12
    Filter 13
IP-Discovery-Filter
    Konfiguration 16
IP Interface symbol 50
IP Manager
    Concepts 11
IP Network
    Adding 14
    Manage 17
    Unmanage 17
IP network symbol 49

IP Node
Add 18
Deletion 20
Expiration Time 21
Status Handling 20
IP node container symbol 49
IP Node symbol 50
IP Parameters 23
Configuration 22
IP Node Configuration 25
Network Configuration 24
IP symbols 49

K

Konfiguration
IP-Discovery-Filter 16

L

Layer-3 Routes 31
License 9
Logging symbols 49

M

Manage 17
Meta edge symbol 49

N

NAC 37
Address 39
Address List 40
Event 41
Filter 40
Rule Evaluation 37
Network
Default 18
Network Access Control 37

O

Overview 50
Control Center 47

P

Ping
Method 23
Monitoring 33
Poll
Configuration 22
Discovery 22
Status 22

R

RDP symbol 50
Rights 51
Router symbol 49
Rules
NAC 37

S

Saving and Loading Configurations 31
Scan
ARP Cache 13
IP Address Range 13
Seed File 18
SNMP 7
Configuration Templates 30
Receive Traps 29
Traps 47
SNMP Agents
Adding 31
SNMP Parameters 28
Configuration 28
SNMP Port
Change 31
SSH Recognition 45
Status
Cluster 35
Status Handling
IP Nodes 20
Status Poll 22
Switch symbol 50
Symbol
IP Interface 50
IP Network 49
IP Node 50
IP node container 49
Meta edge 49
RDP 50
Router 49
Switch 50
Telnet 50
Topologie Subnetwork 49
Topology Network 49
Symbols 49
System symbols 49

T

Telnet Recognition 45
Telnet symbol 50
Templates 29
IP Configuration 30
SNMP Configuration 30
Topology Network symbol 49
Topology Subnetwork symbol 49
Topology Symbols 49

U

Unmanage 17

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.