A MITEL
PRODUCT
GUIDE

Unify OpenScape Fault Management

Unify OpenScape Fault Management V12, OpenScape Business/H3K Plugin

User Guide

10/2021

A31003-F30C0-U112-01-7619

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 2024, Mitel Networks Corporation

All rights reserved

Contents

1 Preface

This chapter discusses the following aspects:

- purpose and audience of this manual
- structure of this manual
- conventions used in this manual
- terminology

1.1 Purpose

This User Guide introduces the **OpenScape Business/H3K Plugin for the OpenScape Fault Management**, a platform independent tool that allows web-based management of voice and data networks. The manual covers the key concepts used and the components necessary to run the **OpenScape Business/H3K Plugin.** Basic knowledge about network management and about the OpenScape FM is needed. More about this can be found in the *OpenScape FM Desktop User Guide* and the *IP Manager Plugin User Guide*.

This OpenScape Business/H3K Plugin User Guide also includes the features for application monitoring (host resources), and the monitoring of applications on an OpenScape Business/H3K RSM server.

1.2 Audience

This guide is addressed to users who want to learn how to use the OpenScape Business/H3K Plugin for the OpenScape FM.

1.3 Structure of this Manual

This OpenScape Business/H3K manual covers the following topics:

- *Chapter 1, "Preface"* describes the concepts of the manual.
- *Chapter 2, "Overview"* describes the basic concepts used by the OpenScape Business/H3K Plugin and shows the fault management with OpenScape Business/H3K networks.
- *Chapter 3, "OpenScape Business/H3K Management"* shows how to start the OpenScape Business/H3K Plugin and describes its basic functionalities.
- *Chapter 4, "Symbols and Overviews"* gives a detailed description of the symbols and explains the submap hierarchy.
- *Chapter 5, "OpenScape Business/H3K Specific Information"* explains how to monitor an OpenScape Business/H3K environment.

- *Chapter 6, "Port-Specific Information"* shows how to monitor ports
- *Chapter 7, "OpenScape Business/H3K Gateway Specific Information"* explains how to obtain specific information about the OpenScape Business/H3K Gateway device
- *Chapter 8, "IVM Specific Information"* gives a description how to obtain specific information about IVM devices
- *Chapter 9, "NAT in OpenScape FM"* explains the role of NAT in OpenScape Fault Management
- *Chapter 10, "Voice Over IP (VoIP) Monitoring in OpenScape FM"* gives a description of how to monitor VoIP functionality of an OpenScape Business/H3K Gateway
- *Chapter 11, "OptiPoint 400/600 Devices"* explains the visualization of OptiPoint 400/600 devices in OpenScape FM
- *Chapter 12, "OpenScape Application Monitoring"* describes the monitoring of running programs on OpenScape Business/H3K RSM servers.

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.

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 this manual.

Example: *see IP 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 the OpenScape FM with the OpenScape Business/H3K Plugin has been installed.
- **Client** means the OpenScape FM Client, usually a web browser where the OpenScape FM client has been started.

- **Desktop** means the OpenScape FM Desktop.

2 Overview

This chapter discusses the following aspects:

- introduction into the OpenScape FM architecture
- basic introduction to OpenScape Business/H3K system management
- the management platform OpenScape FM: the graphical user interface

2.1 Introduction

The OpenScape Business/H3K Plugin is a fault management application which integrates the management of OpenScape Business/H3K systems into the OpenScape FM. The OpenScape FM consists of a server and a client part which are written in Java(TM). Since its client part can be executed as an applet in a web browser, it can be integrated easily in standard intranet/internet environments. The OpenScape Business/H3K Plugin is a plugin for the OpenScape FM and cannot run as a standalone application.

Additionally the OpenScape Business/H3K Plugin supports the earlier technologies HiPath 2000/3000/5000, OpenScape Office and ComServer PC. These technologies, though supported by the OpenScape Business/H3K Plugin, will not be explained in any detail in the OpenScape Business/H3K manual.

OpenScape Business/H3K systems are connected to a LAN or intranet and have an SNMP agent which supports MIB II and a private OpenScape Business/H3K Controller MIB. The OpenScape Business/H3K Manager, therefore, uses SNMP (Simple Network Management Protocol) to gather management information from OpenScape Business/H3K systems (see *Figure 1*). Today, nearly every vendor of network components for open networks supports SNMP.

Besides OpenScape Business/H3K systems, other IP network nodes are discovered if they have an SNMP agent supporting MIB II or other known private MIB extensions. These discovery operations are performed by the IP Manager Plugin, which is a prerequisite for the OpenScape Business/H3K Manager and is automatically installed during the OpenScape Business/H3K Plugin installation. A detailed introduction to the IP Manager can be found in the *IP Manager Plugin User Guide*. The discovered IP nodes can represent PCs, workstations, servers or specific OpenScape access devices. Additionally, specific OpenScape applications like CAP/Telas Web and TeleWorking/mWorks V1.0 applications are recognized by performing specific checks (MIBs, web servers) on each discovered IP node.

The OpenScape FM supports client/server architectures, so the OpenScape Business/H3K Plugin comprises a server- and a client-component.The server component is responsible for all management-specific tasks like network discovery, data acquisition from the OpenScape Business/H3K systems and building up the network topology. The client’s graphical interface gives access to the data maintained by the server.

Figure 1 shows a typical scenario for the use of the OpenScape Business/H3K Manager. The server runs the OpenScape FM server process, including the server component of the OpenScape Business/H3K Plugin. The server process communicates with the OpenScape Business/H3K SNMP Agent to get access to the management information base (MIB). The management data is analyzed and processed by the OpenScape Business/H3K Plugin. A web browser (e.g. Firefox, MS Internet Explorer) can be used as an interface for the OpenScape Business/H3K Plugin.

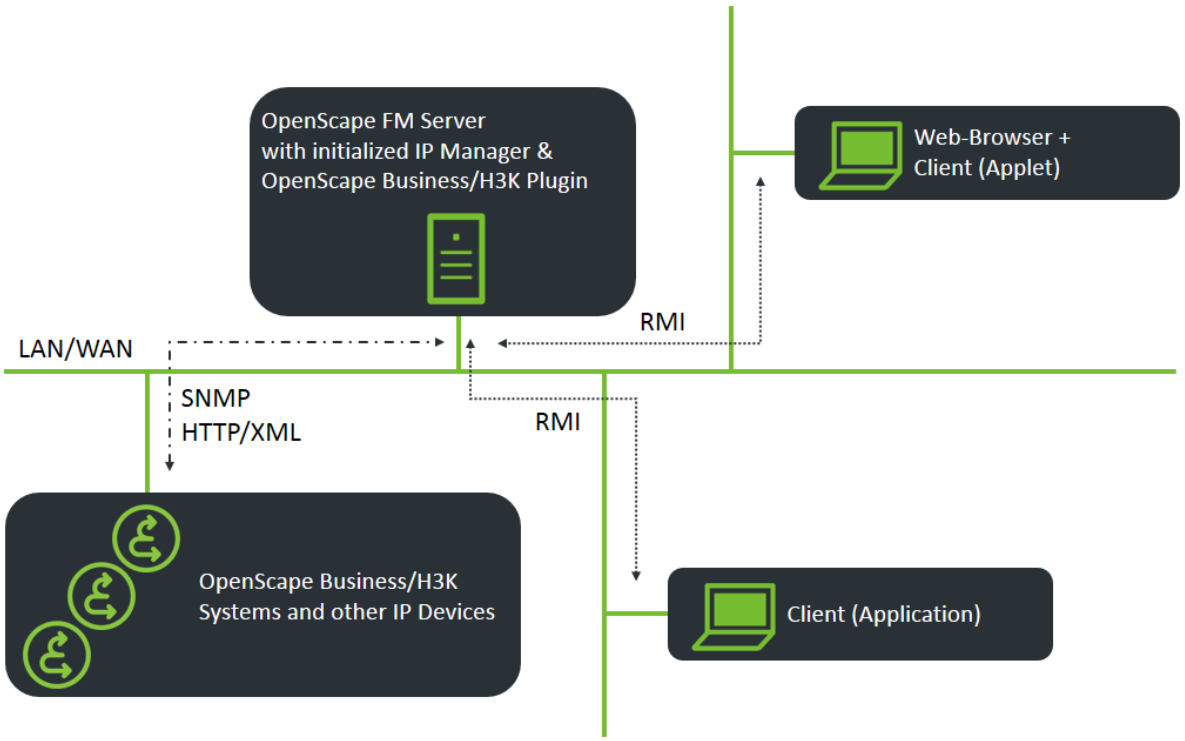

Figure 1 SNMP Management for OpenScape Business/H3K networks

In the current release, the OpenScape Business/H3K Plugin supports the following management areas for OpenScape Business/H3K systems:

- Fault management
- Management of the OpenScape Business/H3K network topology.
- Hardware inventory information.

2.2 OpenScape Business/H3K System Management

An OpenScape Business/H3K network consists of one or more OpenScape Business/H3K systems. Each OpenScape Business/H3K system has an SNMP agent giving access to a variety of system data, stored in its Management Information Base (MIB). The MIB provides basic system information, status data, event related data and data related to installed hardware (slots) and configured connections (ports).

The OpenScape Business/H3K Plugin server-component reads the agent's MIB via SNMP requests. This information is visualized by the client applet (within a web browser) or client application. The communication between OpenScape Business/H3K Plugin server-component and client is done by means of RMI (Remote Method Invocation), which is a part of the Java(TM) standard.

The network components of the OpenScape Business/H3K Management are shown in *Figure 1*.

2.3 The Management Platform OpenScape FM

The network management station, the OpenScape FM server, is a central component for network administration. One of its main functions is to permanently monitor the status of network components and to inform the network administrator in case of status changes. Network management tools have graphical user interfaces and a graphical network map in order to show the topology and the current status of network components. These features are also supported by the OpenScape FM and the OpenScape Business/H3K Manager.

OpenScape FM with OpenScape Business/H3K Plugin provides:

- Hierarchical mapping of the network topology, presented in different abstraction levels (OpenScape Business/H3K network view, subnet view, etc.).
- Possibility to fine-tune the network view by grouping OpenScape Business/H3K systems together and put them into different networks and subnetworks.
- Representation of OpenScape Business/H3K events by graphical status change of OpenScape Business/H3K system icons (color change).
- Representation of connected external systems – including graphical status change of the specific icons.
- Detailed event description in form of textual Browser Windows.
- Detailed OpenScape Business/H3K network topology description.
- Detailed description of installed hardware.

These general features will be described in more detail in the following chapters.

3 OpenScape Business/H3K Management

This chapter provides the first steps for the work with the OpenScape Business/H3K Manager Plugin.

It discusses the following aspects:

- initializing the OpenScape Business/H3K Plugin
- licensing
- topology concept for OpenScape Business/H3K networks
- adding an OpenScape Business/H3K SNMP agent
- presentation of events

It is assumed that the OpenScape FM server software has already been properly installed. Details about the installation process can be found in the *OpenScape FM Desktop User Guide.*

3.1 Initializing the OpenScape Business/H3K Plugin

The OpenScape Business/H3K Plugin is installed as a part of the OpenScape FM installation. More about the installation of the OpenScape FM can be found in the *OpenScape FM Desktop User Guide*.

The plugin can be initialized by using the entry **Server->Plugins->Init OpenScape Business/H3K Plugin** from the main menu of the OpenScape FM.

After the initialization the menu item **Init OpenScape Business/H3K Plugin** will be removed. A new menu item **Technologies->OpenScape Business/H3K** will appear in the main menu. Additionally an object representing the OpenScape Business/H3K Plugin is added to the hierarchy with the path **Root->System->Plugins->Technologies**. The new object offers the same menu entries as the OpenScape Business/H3K menu.

3.2 Licensing

To use the OpenScape Business/H3K Plugin a valid license has to be available. How the OpenScape FM system is licensed is explained in the *OpenScape FM Desktop User Guide*.

Important Note:
The licensing mechanism for the OpenScape Business/H3K Plugin will be changed after this version of the User Guide has been delivered.
The current licensing mechanism can be found in the Release Notes for the plugin.
The following describes the licensing as it was handled when this version of the User Guide was written.

The size of the needed license is based on the number of active ports. The number will be determined differently for HiPath 3000 and OpenScape Business systems:

HiPath 3000

For HiPath 3000, the number of active ports will be gathered by evaluating the `h150ePortTable` of the HiPath 3000 systems. All ports from the MIB table that are in the state (`portState`) '`active(2)`' and whose type (`portType`) does not include the substring '`trunk`' will be counted.

OpenScape Business

OpenScape Business is based on boxes where each box supports a maximum number of ports. For licensing NOT the actual number of used ports will be considered but the number of ports that could be used for each system.

3.3 Adding Nodes to the System

The OpenScape FM automatically starts discoveries for IP nodes that are added. It also performs discoveries for all known IP nodes in defined regular intervals. During these discoveries, IP nodes are identified as OpenScape Business/H3K systems, if the MIB object `h150eErrorHistoryGroup` exists within their local OpenScape Business/H3K MIB.

3.4 Topology Concept for OpenScape Business/H3K Networks

3.4.1 Autodiscovery of Partner Systems

The private MIB of an OpenScape Business/H3K system contains the MIB table "`h150ePortTable`" (`h150eSystemInfoGroup`) which is read during the discovery of a system. Besides other information, the port table contains the field `port type`. For a configured port, this field indicates the type of the port, e.g. a `CoreNetTrunk`, and it may provide a direction information specifying a partner (neighbor) system connected to this port. The type and the direction information are separated by a colon "`:`". This direction information, if specified, is used to auto connect the currently discovered system to a partner system. The direction must correspond to a known hostname/IP address or a MIB II system name (`sysName` in system group). Based on this information, the OpenScape Business/H3K Plugin can draw the topology of an OpenScape Business/H3K voice network automatically.

An OpenScape Business/H3K object is represented by an OpenScape Business/H3K system symbol. The submap of the respective component contains the standard components of OpenScape FM for IP Nodes, e.g. Events and Interfaces. Besides the submap of the OpenScape Business/H3K component contains additional OpenScape Business/H3K specific components, e.g. for discovered partner systems, discovered IVM devices or a router symbol when an OpenScape Business/H3K Gateway with the IP forwarding option set to "*yes*" in its MIB II is detected.

3.4.2 Port/Trunk Status

Besides the information concerning single devices/IP nodes, the OpenScape FM shows the connections (trunks) between them.

The status information of a trunk (port) is derived from the port table fields `portState` and `portLock`. For example, if `portState` is active, the related connection has the state NORMAL (green), if it is inactive it changes to the status WARNING (light blue). *Table 1* shows the possible states.

		portState	
		active	**inactive**
portLock	unlocked	NORMAL	WARNING
	locked	DISABLED	WARNING

Table 1 Rules for setting Port/Trunk Status

All the trunk groups that have been registered for this connection can be found in views (i.e. submaps and trees) of a connection symbol.

3.5 Adding an OpenScape Business/H3K SNMP Agent

The OpenScape Business/H3K Plugin communicates with one or more OpenScape Business/H3K SNMP agents to obtain management information about the related OpenSape Business/H3K networks.

To add a new OpenScape Business/H3K system, it is sufficient to add the system node to the IP Manager. OpenScape FM needs the IP address of the OpenScape Business/H3K SNMP agent or a hostname, which can be resolved via Domain Name Service (DNS) or the hosts file on the management server (see *"IP Manager Plugin User Guide")*

OpenScape FM tries to reach the system via TCP connection. If this is successful, the SNMP discovery starts.

3.6 Tracking Events: the Event Browser

The OpenScape Business/H3K Plugin displays events within the Event Browser (see *OpenScape FM Desktop User Guide*).

Each event is associated with a managed object, e.g. an OpenScape Business/H3K system or an SNMP Agent.

The events shown in the Event Browser are internal events and external SNMP traps which have been sent by the SNMP agents (here the OpenScape Business/H3K systems) to the SNMP Manager (here the Server). For OpenScape Business/H3K specific traps no trap destinations have to be set on the OpenScape Business/H3K systems, since the Server automatically registers itself as trap destination during IP discoveries.

When SNMP traps should be received from applications on a system supporting the Hostresources MIB, this system has to be configured appropriately. See for details. *Chapter 12, “OpenScape Application Monitoring”*

4 Symbols and Overviews

The OpenScape Business/H3K Plugin introduces some new object types, which are represented by new symbol types. A single managed object (MO) can be represented by many symbols on different views (i.e. submaps and/or trees). The managed object itself is the software-representation of a real resource to be managed, e.g. an OpenScape Business/H3K system or a trunk group. Views are used to group related managed objects together as a representation of the object hierarchy. In addition to the default views, customized submap hierarchies can be created.

The *"OpenScape FM Desktop User Guide"* gives a detailed introduction into the work with maps and views (i.e. submaps and trees). Each symbol on a view provides an object-specific context menu that can be invoked by a right-click on the symbol. A submap's context menu is opened by a right-click into the submap's background, respectively.

The following chapters describe the different objects and their symbols created by the Topology Manager and OpenScape Business/H3K Plugin. *Chapter 5, "OpenScape Business/H3K Specific Information"* covers the object-specific context menus and their functionalities.

4.1 Symbols

4.1.1 OpenScape Business/H3K specific Symbols

The following symbols are added to the basic OpenScape symbols by the OpenScape Business/H3K Plugin:

- **IP Node** Symbol, **H3K agent**

The H3K symbol represents a single H3K system, i.e. an IP node with a running SNMP agent with an H3K MIB. It offers a number of functions that can be performed on the system. They can be used to get detailed information about it or to perform administrative tasks.

Next to the H3K symbol is the Compound Status Indicator. More about the indicator can be found in the *OpenScape FM Desktop User Guide*.

- **H3K component** symbol

- **H3K Gateway** Symbol

- **Router** Symbol (Topology Manager specific symbol)

An OpenScape Business/H3K Gateway is an IP device that is integrated into an OpenScape Business/H3K, i.e. it has its own IP address. Since these devices have the default option "IP forwarding = yes" the OpenScape Business/H3K Gateway symbols can appear as routers in the IP view as well as in the network view.

- **Connection Monitoring** Symbol (former VoIP)

- **NAT** Symbol (Network Address Translation)

- **IP phone** Container Symbol

- **IP phone (e.g. OpenStage phone)** Symbol

- **IVM device** Symbol

- **OpenScape Business** Symbol

- **OpenScape Business Call Control** Symbol

- **OpenScape Business Gateway** Symbol

- **OpenScape Business S** Symbol

- **OpenScape Business S Call Control** Symbol

- **OpenScape Business S Gateway** Symbol

4.2 Overviews

If the ControlCenter Plugin has been initialized, a number of ControlCenter overviews are provided for OpenScape Business/H3K objects. These object types are aggregated since they all use identical trap types and hence their events can all be found in category ’OpenScape Business/H3K’.

The following overviews are provided:

- The last ten OpenScape Business/H3K systems that changed to the status ’critical’ and that are still in that status.
- The ten OpenScape Business/H3K systems with the most unacknowledged events.
- The ten most recent events from category ’OpenScape Business/H3K’ that have a status worse than ’normal’.
- The distribution of the unacknowledged events within category ’OpenScape Business/H3K’ by status.
- The distribution of events within category ’OpenScape Business/H3K’ by time.

The overviews can be displayed by selecting the entry **ControlCenter - Overview** within the main menu **Technologies->OpenScape Business/H3K**.

More about the ControlCenter can be found in the *Control Center Plugin User Guide*.

5 OpenScape Business/H3K Specific Information

OpenScape FM provides various OpenScape Business/H3K specific information. It can be accessed via the context menu of an OpenScape Business/H3K system symbol or an OpenScape Business/H3K IP node symbol.

A list of the OpenScape Business/H3K IP nodes can be accessed by selecting the main menu entry **Technologies->OpenScape Business/H3K->Show Hosts**. This list provides a convenient and central access to the context menus of the individual objects.

5.1 OpenScape Business/H3K IP Node

The context menu, of OpenScape Business/H3K IP node symbols, contains the OpenScape Business/H3K specific menu **OpenScape Business/H3K**.

This menu contains the same entries as the context menu of the OpenScape Business/H3K component described in the next section.

5.2 OpenScape Business/H3K Component

The context menu of an OpenScape Business/H3K Component symbol contains the OpenScape Business/H3K specific entries listed below.

Additionally, the entries **Manager E Start** and **Manager E Dialog** appear in the context menu, if the *Manager E for OpenScape Business/H3K* is installed on the same machine as the used OpenScape FM client. When the Client is started it checks automatically if this application has been installed on the client host. These entries are also available in the web browser, if the Manager is installed on the client host (see *Section 5.3, "Access to Manager E via OpenScape FM"*).

The following OpenScape Business/H3K specific entries are located in the submenu **OpenScape Business/H3K**:

- **System Info...** shows the hardware version, software version, code number and software location of the OpenScape Business/H3K system.
- **Events->Event Config...** (only available for H3K systems) can be used to set the event types. It can be chosen between **log** and **log-and-trap**. *log* writes the event to the event log of the OpenScape Business/H3K system. *log-and-trap* writes it to the event log and sends an SNMP trap to the management station.
- **Events->Event Log...** (only available for H3K systems) shows the entries of the event log.
- **Events->Error History...** presents the error history for the OpenScape Business/H3K system.
- **Slots...** offers information about the system slots (card number, the box number, slot number, card type, card description, card code number and the state of the card).
- **Ports...** shows information about the system ports (port number, assigned card, type, general state, lock state and target node id).

- **Features...** offers information about the usage of the specific OpenScape Business/H3K system features (feature no., description and counter).
- **Subscribers...** the entry displays a table that contains the subscriber contacts for OpenScape Business systems. Since the SNMP table with the respective data does not exist for older OpenScape Business/H3K models, in that case, the entry displays an empty table.

5.3 Access to Manager E via OpenScape FM

When the OpenScape FM client is running on a machine where the Manager E has been installed, the Manager can be started via the OpenScape Business/H3K system symbol. In that case, its context menu provides the menu items **Manager E Start** and **Manager E Dialog**.

The entry **Manager E Dialog** opens a window which can be used to configure the **Username** and **Password** that are used to start the Manager E on this machine. By selecting the **Default** option, a Username/Password pair can be configured that will be used as the default option for all Manager E.

When the Username/Password pair has been configured correctly, the Manager E can be started with the **Manager E Start** menu entry.

5.4 Status of OpenScape Business/H3K Systems

The MIB for OpenScape Business/H3K defines a trap called `sendAlarm`. OpenScape Business/H3K systems are sending this trap to the OpenScape FM where it will be displayed as an event within the Event Browser. Based on the content (variable binding) of these traps a specific status will be assigned to the event. The events in the Event Browser can be acknowledged by the user.

The status of the OpenScape Business/H3K objects will be defined by the highest severity of all not acknowledged events within the Event Browser which are connected to the object.

5.5 List of all OpenScape Business/H3K Systems

An overview over all currently managed OpenScape Business/H3K systems can be displayed by using the entry **List Systems** from the main menu **Technologies->OpenScape Business/H3K**. In the resulting Info Browser, each line represents one OpenScape Business/H3K system and offers the respective object-specific context menu.

The **Reload** button starts a new query.

The **Stop** button stops a running query.

6 Port-Specific Information

When a connection symbol is opened, all ports are shown that are defined for one of the end points of the connection. For each port, the source and the destination system are displayed.

As for all symbols, the color of the connection represents the status.

A port symbol offers an object-specific context menu which allows to lock/unlock a port (entry: **Lock Port** or **Unlock Port**).The lock/unlock operation results in an SNMP SET operation on the corresponding OpenScape Business/H3K system, i.e. the port is locked ON this system. A locked port is displayed by a brown port symbol that gets green again when it has been unlocked.

7 OpenScape Business/H3K Gateway Specific Information

When an IP node has been discovered on which an OpenScape Business/H3K Gateway MIB has been identified, an IP node object is created with an OpenScape Business/H3K Gateway object as its child object. The IP node is displayed in the IP network it belongs to, and additionally the OpenScape Business/H3K Gateway object is displayed on the submap of the OpenScape Business/H3K device where it is installed. If no `sysLocation` has been set in the MIB II `systemGroup` of the OpenScape Business/H3K Gateway, OpenScape FM sets the Network Id to "OpenScape Business/H3K Gateway" – thus all OpenScape Business/H3K Gateway devices will be located in the network named "OpenScape Business/H3K Gateway" after the initial discovery.

7.1 OpenScape Business/H3K Gateway Context Menu

The OpenScape Business/H3K Gateway offers a specific context menu which provides access to OpenScape Business/H3K Gateway data. Its menu entries provide access to several Info Browsers which list OpenScape Business/H3K Gateway specific information and will be explained in detail in the following sections. The information is retrieved via SNMP.

7.1.1 Events

The **Events** menu entries provide access to all errors and all trap events which have occurred on the OpenScape Business/H3K Gateway.

7.1.1.1 Error History

The menu entry **Events->Error History...** opens an Info Browser which lists all errors of the OpenScape Business/H3K Gateway.

It contains the following columns:

Class: the class of the error. An error class characterizes the component which caused the error.

Date/Time: Timestamp; point of time when the error occurred.

Description: short description of the error.

7.1.1.2 Traps

The menu entry **Events->Traps...** opens an Info Browser which lists all trap events which have been generated by the OpenScape Business/H3K Gateway.

It contains the following columns:

Severity: Each trap contains information about its severity level; possible levels are "*normal*", "*warning*", "*minor*", "*major*", or "*critical*".

ErrorClass: class of the error which caused the trap; possible classes are "*general*", "*security*", "*data*", and "*voice*".

ErrorCode: internal code of the error which caused the trap.

Date/Time: Timestamp; point of time when the trap was generated.

Handling: It can be configured for each event type, if an SNMP trap should be sent when the event occurs or if the event should only be stored locally at the OpenScape Business/H3K Gateway. Those parameters cannot be configured within the OpenScape FM, but at the OpenScape Business/H3K Gateway itself (e.g. with the Manager I). If the entry is *stored,* the corresponding event was only stored locally. If the entry is *forwarded*, the event was stored locally AND an SNMP trap was generated and sent to all trap destinations.

Description: detailed description of the trap-causing error.

7.1.2 Statistics

The menu entries in the **Statistics** menu provide access to statistic tables with information about data exchange. The information is retrieved using the technologies described in *Section 7.1.4, "Used Technologies"*.

All menu entries of the **Statistics** menu, with detailed information on how OpenScape Business/H3K Gateway statistic data can be retrieved and what the displayed values mean, will be explained in the following paragraphs.

7.1.2.1 Global Data vCAPI Client (only for H3K systems)

The OpenScape Business/H3K Gateway is a virtual CAPI (vCAPI) server where several vCAPI clients, usually installed on PCs, can log in. Thus, these PCs do not need an ISDN hardware device but use a virtual CAPI interface – the vCAPI client. When the PC needs to establish a connection via the ISDN interface, it logs in to its vCAPI server, the OpenScape Business/H3K Gateway, which in turn provides the real ISDN connection.

The menu entry **Statistics->Global Data vCAPI Clients...** opens a browser that shows information about the vCAPI clients. It contains the following information:

No. vCAPI Clients installed: the number of vCAPI Clients which can be managed by this server.

No. vCAPI Clients Logged in: the number of vCAPI clients which currently have a valid connection to this server.

No. vCAPI Clients Active: the number of vCAPI clients which are currently working on this server.

7.1.2.2 Global Data Workpoint Clients

The menu entry **Statistics->Global Data Workpoint Clients...** opens an Info Browser with general information about all TFA Clients of the OpenScape Business/H3K Gateway. An explanation of TFA can be found in *Section 7.1.4, "Used Technologies"*.

The OpenScape Business/H3K Gateway can bridge TFA calls like H.323 calls, but for TFA connections, a client has to log in to the OpenScape Business/H3K Gateway with a valid user/password pair.

The browser contains the following information:

No. TFA Clients Installed: number of installed TFA clients.

No. TFA Clients Active: number of active TFA clients.

No. TFA Clients Registered: number of registered TFA clients.

No. Successful TFA Clients Logins: number of successful logins from TFA clients.

No. Failed TFA Clients Logins: number of failed logins from TFA clients.

7.1.3 General Information

The menu item **General Information...** opens an Info Browser which provides general information about the corresponding OpenScape Business/H3K Gateway device. The following information is displayed:

Idx. of Last Trap: index of the last trap which has been sent by the OpenScape Business/H3K Gateway. The trap index is a number which is increased by one for every new trap.

Error Events Signaled As Traps: the integer value of a bit-encoded trap definition.

Error State: current error state of the OpenScape Business/H3K Gateway.

Connection State: the state of the connection between the OpenScape Business/H3K Gateway and the OpenScape Business/H3K device where it is installed.

MAC Address: the hardware address of the OpenScape Business/H3K Gateway.

Software Version: version of the currently installed and running OpenScape Business/H3K Gateway software.

Agent Version: SNMP agent version of the OpenScape Business/H3K Gateway.

7.1.4 Used Technologies

The technologies used to retrieve the information about data exchange (*Section 7.1.2, "Statistics"*) are described in this section.

H.323

The H.323 standard provides a basis for audio, video, and data communications across IP-based networks, including the Internet. H.323 is an umbrella recommendation from the ITU (International Telecommunications Union) that defines standards for multimedia communications over LANs (Local Area Networks) that do not provide a guaranteed Quality of Service.

Media streams are transported on RTP/RTCP. RTP carries the actual media and RTCP carries status and control information.

RTP

The term "RTP" is explained in the following paragraph which is an excerpt from RFC 1889 that specifies this standard.

RTP means real-time transport protocol, which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, timestamping and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols.
Note that RTP itself does not provide any mechanism to ensure timely delivery or provide other quality-of-service guarantees, but relies on lower-layer services to do so. It does not guarantee delivery or prevent out-of-order delivery, nor does it assume that the underlying network is reliable and delivers packets in sequence. The sequence numbers included in RTP allow the receiver to reconstruct the sender's packet sequence, but sequence numbers might also be used to determine the proper location of a packet, for example in video decoding, without necessarily decoding packets in sequence. While RTP is primarily designed to satisfy the needs of multi- participant multimedia conferences, it is not limited to that particular application. Storage of continuous data, interactive distributed simulation, active badge, and control and measurement applications may also find RTP applicable.
(end of RFC 1889 excerpt).

RTCP

The statistic data cannot be provided by RTP itself but is based on information which is retrieved by the help of RTCP, the RTP control protocol. The following lines are a short excerpt from the RFC 1889.

The RTP control protocol (RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. The underlying protocol must provide multiplexing of the data and control packets, for example using separate port numbers with UDP. RTCP performs four functions:

1. The primary function is to provide feedback on the quality of the data distribution. This is an integral part of the RTP's role as a transport protocol and is related to the flow and congestion control functions of other transport protocols.
   (...)
2. RTCP carries a persistent transport-level identifier for an RTP source
3. The first two functions require that all participants send RTCP packets, therefore the rate must be controlled in order for RTP to scale up to a large number of participants. By having each participant send its control packets to all the others, each can independently observe the number of participants. This number is used to calculate the rate at which the packets are sent.
4. A fourth, optional function is to convey minimal session control information, for example participant identification to be displayed in the user interface.
   (...)
   (end of RFC 1889 excerpt).

TFA

TFA (Telephony Feature Access) is a proprietary Unify protocol. Today, the synonymous term "HFA" (Hicom Feature Access) is often used.

TFA (HFA) is an extended standard for IP telephony: voice data is transmitted via H.323, whereas feature signalization is transmitted via CorNet, a Unify standard. TFA (HFA) therefore can provide all Hicom features even for end devices.

7.2 OpenScape Business/H3K Gateway Subcomponents

When the submap of an IP node which is an OpenScape Business/H3K Gateway is opened, all subcomponents are displayed.

All discovered interfaces are displayed on the submap of the *Interfaces* symbol. The OpenScape Business/H3K Gateway symbols represent different OpenScape Business/H3K Gateway functionalities:

- the OpenScape Business/H3K Gateway functionality (described in this chapter),
- the NAT functionality (see *Chapter 9, "NAT in OpenScape FM"*) and
- the Connection Monitoring functionality (former VOIP) (see *Chapter 10, "Voice Over IP (VoIP) Monitoring in OpenScape FM"*),

The SNMP submap contains all supported MIBs.

Additionally possibly an OptiPoint Container and a QoS container exist. The OptiPoint container includes the connected OptiPoint 400/600 devices (see *Chapter 11, "OptiPoint 400/600 Devices"*). The QoS container includes symbols for bad connections, which occurred with IP-phone devices of this OpenScape Business/H3K Gateway, see also *Section 10.2, "Display QoS Status in VoIP Networks"*.

Since the support for the MIB trees providing the data for the OptiPoint- and QoS-Container have never been implemented, these objects have been removed in OpenScape FM V4 R3.

7.3 Web Based Management

For an OpenScape Business/H3K Gateway V3.0 it will be checked if the "Web Based Management Interface" is available. If this is the case the menu items **Web Based Management Dialog...** and **Web Based Management...** will be offered. The menu item **Web Based Management Dialog...** opens the dialogue to configure the username/password pair. Via the menu item **Web Based Management...** the URL of the Web Based Management Interface can be invoked.

8 IVM Specific Information

IVM, also known as Xpression Compact, is an integrated voice mail solution for OpenScape Business/H3K. The IVM device has a separate LAN interface and its own IP address.

When an OpenScape Business/H3K object has been discovered on which an IVM device has been identified, an IP node object is created with an IVM object as its child object. The IP node is displayed in the IP network it belongs to, and additionally the IVM object is displayed on the submap of the OpenScape Business/H3K device where it is installed. Because the OpenScape Business/H3K object provides information about its IVM device, an IVM device will not be identified as such until the appropriate OpenScape Business/H3K object is known by OpenScape FM.

The IVM device does not provide any specific status information. The related IP node symbol will be set according to its IP interface status, like any other IP node.

8.1 IVM Context Menu

The IVM object offers a specific context menu which provides access to IVM data. Its menu items open several Info Browsers which list IVM specific information and will be explained in detail in the following sections. The information is retrieved via FTP.

Hint:
It has to be kept in mind, that a request of the IVM specific information takes at least 10 seconds.

8.1.1 Description

The **Description** menu entry gives a short description about the IVM device, provided by the related OpenScape Business/H3K system.

8.1.2 General Information

Via the menu entry **General Information** an Info Browser can be opened providing general information about the corresponding IVM device. It contains the following information:

Software Version: the version of the installed software.

Hardware Version: the hardware version.

Hard Disk Usage: the percentage of the actual usage of the hard disk.

Installed Mailboxes: the number of installed mailboxes.

Free Mailboxes: the number of free mailboxes.

Free Channels: the number of free channels.

Occupied Channels: the number of occupied channels.

Activated Features: the number of the activated features.

8.1.3 Installed Languages

The menu entry **Installed Languages** opens an info browser showing all languages installed on this device and the respective version numbers.

8.1.4 Mailbox List

The menu entry **Mailbox List** opens an info browser providing a list about all configured mailboxes.

8.1.5 Login Settings

Via the menu entry **Login Settings** a user with Administrator rights can change the settings for the FTP login on the respective IVM device.

The entry opens a window with the following elements:

FTP Hostname: Here the hostname/IP address of the IVM device is shown, this textfield is not writable.

FTP Port: Here the FTP port is shown. Since the FTP Port 21 is the standard FTP port it cannot be altered even by a user with Administrator rights.

Login Name: Here the FTP login name of the configured user has to entered. The default login name is "31994“.

Password: The related password of the configured user has to be entered here. The default login password is "31994“.

XML Configuration File: Here the name of the xml-file, which is located on the IVM device, has to be entered. The xml-file contains the configuration information of the IVM device, which will be read from the OpenScape Business/H3K Plugin, e.g. "Mail Box List“. The default xml-file is "`ivm_sysd.xml`“.

Set As Global Default: If this checkbox is checked the entered values are set as a default for all new discovered IVM devices and will be set for the selected one, after pressing the **OK** button.Already existing IVM devices will not be affected. If the checkbox is unchecked the values will be only set for the selected IVM device.

The **OK** button closes the window and saves the information. The **Cancel** button closes the window without saving any information. The **Reset To Global** button will put the values which were set as default in the respective text fields, to confirm them the **OK** button has to be pressed.

9 NAT in OpenScape FM

OpenScape FM supports NAT (Network Address Translation) for certain OpenScape FM objects. When the OpenScape Business/H3K Common Monitoring MIB has been discovered on an OpenScape FM object, the corresponding NAT tables are integrated into OpenScape FM IP management.

Currently, the OpenScape Business/H3K Gateway supports the OpenScape Business/H3K Common Monitoring MIB and thus is detected as a NAT device in OpenScape FM.

Since the management of the NAT address mapping tables is done by the IP Manager, an introduction to NAT in OpenScape FM is given in the *"IP Manager Plugin User Guide"*.

9.1 NAT with OpenScape Business/H3K Gateway

The OpenScape Business/H3K Gateway component is a NAT capable device, i.e. it can translate internal to external IP addresses and vice versa. It uses unidirectional IP address mapping between ISDN and a LAN. In packets coming from the ISDN side with a target in the LAN, i.e. with an internal address, only the target IP address is changed (i.e. mapped) by the OpenScape Business/H3K Gateway. When the target computer in the LAN sends an answer via the ISDN device, the target address does not have to be changed in the IP packets, since the target device has a unique IP address.
The situation looks complementary for the source addresses: When the ISDN device sends an IP packet, the source address is unique and does not need any mapping, whereas in the other direction, when the LAN computer sends an IP packet, the source address is an internal one. Thus it will be changed (mapped) by the NAT router (OpenScape Business/H3K Gateway).

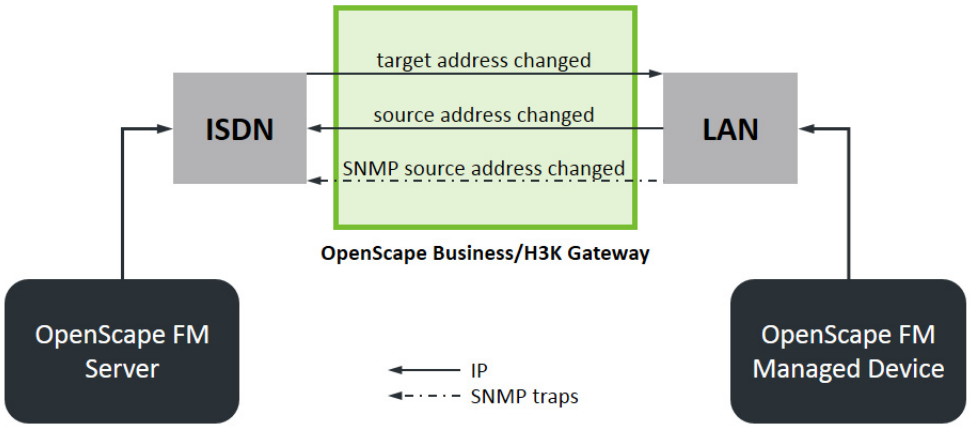

Figure 2 NAT routing with OpenScape Business/H3K Gateway

The NAT functionality of the OpenScape Business/H3K Gateway is managed as a NAT object, a child object of the OpenScape Business/H3K Gateway. The NAT object provides a context menu with one specific menu item: **Rules**.

The menu item **Rules** opens a list where the address mappings of this NAT device are shown. It contains the following columns:

External: the external address.

Internal: the internal address.

Netmask: the netmask.

Rule Valid: OpenScape FM checks if there are any inconsistencies concerning routable/external IP addresses. If there are any, the corresponding rule is invalid. Usually the value should be “valid" for correct internal/external IP address mapping with unique external IP addresses.

The state of the NAT object depends on the definition of NAT rules. The meaning of the colors relating to the status of the objects is handled in the *OpenScape FM Desktop User Guide*).

NAT object state	description
unmanaged	unmanaged
disabled	managed, but no active NAT rules
restricted	managed; NAT rules not used because NAT router lies in mapped IP address range
warning	timeout has occurred while retrieving NAT rules
critical	NAT rules which have been found are not consistent

Table 2 NAT object states and icon colors

10 Voice Over IP (VoIP) Monitoring in OpenScape FM

When IP telephony is used, the quality of the LAN phone connections depend on the quality of the underlying protocol layers. Thus, when there are problems concerning the IP connections between devices in a network, LAN telephony will be affected as well.

In order to monitor whether potential IP connections can be used without interferences like timeouts or other problems, a tool is needed which performs periodic checks of the connection quality.

The OpenScape Business/H3K Common Monitoring MIB allows the monitoring of IP connections. If an SNMP agent which supports this MIB is installed on a system, this system can perform checks concerning the connections to several other IP devices.

OpenScape FM can detect this MIB on an OpenScape FM-monitored device and provides a user interface to configure, for which connections the IP layer should be monitored.

Currently, this MIB has been implemented for OpenScape Business/H3K Gateway devices.

10.1 VoIP in OpenScape Business/H3K Gateway

The Voice over IP functionality of an OpenScape Business/H3K Gateway is represented as a Connection Monitoring object (former VoIP) which is a child object of the corresponding IP node, i.e. of the OpenScape Business/H3K Gateway IP node. The Connection Monitoring object icon provides a context menu. This menu offers the menu item **Configure Connection Table** for users with *Administrator* rights and the menu item **View Connection Table** for users with *Operator* rights. For user with *User* rights, no item will be offered concerning VoIP.

The configuration of the connection table will be explained in the following section.

10.1.1 Configure Connection Table

The entry **Configure Connection Table** opens the VoIP connection GUI for the configuration of the connections which are to be monitored. With this GUI, connections between network devices can be monitored by a "ping" operation.

On the left-hand side, the table lists all connections which are currently monitored.

The right-hand side consists of the configuration panel, where the IP address of the target device can be entered to monitor a new connection.

If this is done, the OpenScape Business/H3K Gateway performs a "ping" operation to this device, using the parameters defined in the three fields: **Timeout**, **Retries** and **Retry Timer**.

In the selection menu at the bottom, the modes for testing can be chosen:

The test is either performed periodically using a ping operation with the defined parameters (**periodical Test**), only once (**singleTest**), or the test is disabled for the selected connection (**noTest**).

In order to modify an already existing connection, the connection has to be selected in the list. Its parameters are then shown in the configuration panel on the right-hand side. Entering the new parameters and pressing **Modify** saves the new values.

The connections which are supervised with **autoTest** cannot be configured manually in then OpenScape FM. They have to be defined on the OpenScape Business/H3K Gateway system itself and are retrieved by OpenScape FM for display only. The parameters of an **autoTest** connection cannot be modified.

As long as a connection can be established without any problems, it will not be displayed on the OpenScape FM GUI. But as soon as problems occur, the related connection will be drawn between the two affected IP devices and it will be colored red which means "critical" state. Additionally the Connection Monitoring symbol gets the fault state "warning", i.e. it will be colored light blue.

For example, if it should be checked whether the connection from the OpenScape Business/H3K Gateway to the LAN phone with IP 139.2.154.2 can be used without problems, the IP address, the Timeout value, the number of Retries, and the Retry Timer value are entered. Then the test mode is selected (in our example periodicalTest) and Add is pressed. A new line appears in the list of monitored connections. At the same time, the OpenScape Business/H3K Gateway starts the periodic "ping" operation to the device 139.2.154.2 and displays the connection in the OpenScape FM topology if a timeout has occurred.

10.2 Display QoS Status in VoIP Networks

The Quality of Service (QoS) in a voice communication network is affected by many factors. These are, for example, network availability, reliability (dropped calls, wrong number), sound quality (loudness, distortion, noise) and end-to-end delay. In this section, QoS focuses mainly on the quality of the phone call itself, also referred to as conversation quality or voice quality (VQ).

Traditional switched telephone networks are optimized for time-sensitive voice applications and provide e.g. constant bandwidth, low delay and low jitter. This is not the case for IP networks, which were designed for non-realtime applications like email or file transfer. Concerning VoIP, the QoS is affected by typical problems that can arise in an IP network like packet loss or delay.

To get accepted by the user, the QoS of a VoIP environment must be comparable to the quality provided by a traditional telephone network. Because of this, monitoring of the QoS status is especially important for network management. OpenScape FM supports the display of QoS status for OpenScape Business/H3K Gateway-based VoIP environments.

10.2.1 Monitoring and Visualization

In an OpenScape Business/H3K Gateway-based VoIP environment, the VoIP clients (OptiPoint 400/600 at the time of this writing) are responsible for the measurement of the conversation quality. For each phone call, parameters like jitter, delay and packet loss are determined and a weighting function calculates the overall-quality of the call. This overall-quality is mapped to a status value (QoS-status) which can have one of the following values:

- normal

- warning
- minor
- major
- critical

On call clearing, the QoS parameters recorded by the VoIP client are transmitted to the OpenScape Business/H3K Gateway and stored in a table (QoS-table). This table contains the QoS parameters of the most recent 200 calls of all VoIP clients of the OpenScape Business/H3K Gateway.

OpenScape FM retrieves the QoS-table via SNMP from the OpenScape Business/H3K Gateway's SNMP agent and visualizes all calls that have a bad overall-quality, i.e. a QoS-status not equal to normal. The visualization is done in two steps:

1. A link will be drawn between the IP node objects, which represent the two affected VoIP clients. If one of the communication partners is not an IP-phone, the link will be created between the VoIP client and the OpenScape Business/H3K Gateway, because the call is routed to an external communication network.
2. A symbol which represents the phone call with the quality problem will be placed below the OpenScape Business/H3K Gateway. All the symbols will be allocated within the container QoS. By that way all bad calls can be associated with the appropriate OpenScape Business/H3K Gateway.

The status of the link and the symbol are set according to the QoS-status of the call. If the QoS-table contains more than one entry for a call with a bad quality between the same pair of communication partners, the QoS-status of the most recent entry will be used to set the status of the link/symbol.

The links and symbols representing a problematic phone call are displayed for a limited time only. They have a decay time which is described in *Section 10.2.2, "Link Decay Time"*.

The QoS-table is evaluated every time OpenScape FM performs a status poll, by default every hour. Additionally the OpenScape Business/H3K Gateway can be configured to send SNMP traps to the OpenScape FM every time a new entry with a QoS-status not equal to normal is added to the QoS-table

Note:
This configuration is performed automatically if the OpenScape FM can enter itself as a trap-target at the rmon-MIB of the OpenScape Business/H3K Gateway's SNMP agent (see *IP Manager Plugin User Guide*).

When the OpenScape FM receives such a QoS-trap, it updates its database and shows problematic phone calls immediately.

For each QoS-trap OpenScape FM receives, a log event is generated and displayed at the OpenScape FM's event browser. The log entry shows the following values, taken from the trap:

- **Conference ID:** The conference id which identifies the affected call.
- **Local IP Address:** The IP address of one communication partner (IP-phone client).
- **Remote IP Address:** The IP address of the other communication partner, or the IP address of the OpenScape Business/H3K Gateway if this is not an IP-phone.
- **Connection Quality:** The quality of the connection.

Note:
If one of the IP node objects representing a link end-point does not exist in the database of OpenScape FM and its IP address lies within a subnetwork which exists and is managed in OpenScape FM, it will be created automatically.

10.2.2 Link Decay Time

Links and symbols representing problematic phone calls are displayed for a limited time and will be removed automatically if no further calls with bad QoS-status are detected for the same pair of communication partners in that time interval. The time interval, called link decay time, is configurable via the OpenScape Business/H3K main menu. The main menu item **Technologies->OpenScape Business/H3K->Link Decay Time** opens a user interface where the decay time can be edited. By default the link decay time is one day.

Changes to the decay time affect only links/symbols that are created after the change was made. For existing links, the decay time will not be updated. If the OpenScape Business/H3K Gateway signals another call with bad QoS-status for a link that already exists, the decay timer for that link will be started anew. Therefore, in case that two communication partners have permanent call-quality problems, it may occur that a link never disappears. The server saves the link decay time for each link. Even when the server gets restarted the decayed links will be correctly removed.

Links can also be deleted manually. However, if another call-quality problem is reported for this pair of communication partners, the link will be created again.

11 OptiPoint 400/600 Devices

The OpenScape Business/H3K Gateway device can be configured to serve as a gatekeeper in an IP-telephony environment. In such an environment, IP-phones (OptiPoint clients) logically belong to a specific OpenScape Business/H3K Gateway, i.e. the OpenScape Business/H3K Gateway is responsible for the connection-establishment for this IP-phones.

The OpenScape FM discovers and displays the IP-phone clients of an OpenScape Business/H3K Gateway device. It monitors the current status of the clients, as well as the quality of service (QoS) of the recent phone calls (the latter is explained in the *Section 10.2, "Display QoS Status in VoIP Networks"*).

All information about the OptiPoint 400/600 devices is retrieved via SNMP from the OpenScape Business/H3K Gateway's SNMP agent. For the discovery and status display of OptiPoint clients, this SNMP agent provides an *OptiPoint-table* (`ipPhoneTable`) which contains all necessary data about the configured clients.

Note:
Not every implementation of an OpenScape Business/H3K Gateway supports the "OptiPoint-table".

11.1 Discovery Process

From the OpenScape FM's point of view, an OptiPoint client is first of all an IP node. If it is newly added to the OpenScape FM's database, OpenScape FM only knows that this IP node is an OptiPoint client, but does not have any further information like its phone number or the related OpenScape Business/H3K Gateway. At this point, only the label of its symbol shows that it is an OptPoint. In addition a basic status monitoring of the client is started which simply tests if the device is reachable through the network or not. By default, this reachability check is done every 60 minutes.

To find out which clients belong to a particular OpenScape Business/H3K Gateway, OpenScape FM reads the OptiPoint-table of every OpenScape Business/H3K Gateway device that is discovered. This table is provided by the OpenScape Business/H3K Gateway's SNMP agent and contains, among other information, the IP address of each OptiPoint belonging to the OpenScape Business/H3K Gateway. Now the OpenScape FM can recognize which OptiPoint clients belong to which OpenScape Business/H3K Gateway and visualize them accordingly (see *Section 11.2, "Visualization and Status Monitoring"*). If the IP node representing an OptiPoint client is not yet contained in the OpenScape FM's database but its corresponding subnetwork exists and is managed, the IP node will be added automatically.

Only operational OptiPoint clients are recognized. Operational means that the client has connected to the OpenScape Business/H3K Gateway at least once since the last reboot of the OpenScape Business/H3K Gateway. If it has not, the IP address is not known to the system and the corresponding IP node can not be determined.

Once an OptiPoint client is identified by OpenScape FM, a more sophisticated status monitoring and visualization of the device can take place, as described below.

11.2 Visualization and Status Monitoring

OptiPoint clients are displayed by IP node objects in the OpenScape FM. To visualize that an IP node is an OptiPoint client, the OpenScape FM uses a special symbol (see *Chapter 4, "Symbols"*) to represent it and additionally places a respective object on the IP node‘s submap.

The status of the OptiPoint object is retrieved via SNMP from the OptiPoint-table of the OpenScape Business/H3K Gateway. This status can be “*normal*“, “*warning*“, “*minor*“, “*major*“, “*critical*“ or “*unknown*“, and the OptiPoint object is colored according to the value of this status. The status of the OptiPoint object is propagated to the IP node object above. The IP node‘s status is always the most critical status of its child objects, as long as the IP node is reachable. To identify the component which actually caused the IP node icon to turn into a specific state, the IP node‘s submap or the status explanation browser (see *OpenScape FM Desktop User Guide*) can be opened.

Important Note:
Status changes at the OptiPoint table of the OpenScape Business/H3K Gateway are signalled by SNMP traps and are shown immediately. Status changes of the network interface are recognized by polling and may appear with a delay of about 60 minutes (default polling cycle, configurable by the user, see *IP Manager Plugin User Guide*). The OpenScape Business/H3K Gateway has to be configured to send SNMP traps to the OpenScape FM. This configuration is performed automatically when the OpenScape FM can enter itself as a trap target at the rmon-MIB via SNMP (see *IP Manager Plugin User Guide*).

To show which OptiPoint clients belong to a particular OpenScape Business/H3K Gateway, the submap of the OpenScape Business/H3K Gateway‘s IP node displays an object labeled **`OptiPoints`**. This object contains all OptiPoint clients that were identified based on the information delivered by the OpenScape Business/H3K Gateway’s SNMP-Agent.

Changes of the OptiPoint-table can be signalled by SNMP-traps if the OpenScape FM is configured as a trap destination at the OpenScape Business/H3K Gateway (see note above). If the OpenScape FM receives such a trap, the addition or removal of clients will change the display in the OpenScape FM almost immediately. An OptiPoint client has to be in operational state to be recognized by the OpenScape FM. A newly configured client has initially no IP address in its OptiPoint-table record and can therefore not be identified by the OpenScape FM.

11.3 OptiPoint-Related Events

If an OpenScape Business/H3K Gateway reports the change of the error state of an OptiPoint client by sending an SNMP trap to the OpenScape FM, the OpenScape FM event browser displays the following information:

- The subscriber number of the IP phone
- The IP address of the IP phone
- The current error state of the IP phone

Additionally, the OpenScape FM monitors the network-connectivity of the IP phone. If the OpenScape FM can not reach it via network, an IP node down event is generated for that OptiPoint client. This does not necessarily mean that there is a problem with the OptiPoint client itself. The connection between the OpenScape Business/H3K Gateway and the OptiPoint may still be fine. An IP node down event just means that OpenScape FM could not reach the OptiPoint client.

11.4 IP Address Change of OptiPoints

In case of an IP address change of a discovered OptiPoint, the OpenScape Business/H3K Plugin updates the IP network topology. Changes of the IP address are signaled by the OpenScape Business/H3K Gateway via an SNMP trap or will be detected after a configuration poll. The configuration poll reads the OptiPoint-table of the OpenScape Business/H3K Gateway which is also used to recognize and display all OptiPoints belonging to an OpenScape Business/H3K Gateway. Among other values, the table contains the subscriber number of an OptiPoint and its current IP address. Both values are used to uniquely identify such an OptiPoint.

If an IP address change of an OptiPoint has been detected, the IP node with the old IP address will be deleted and a new one will be created representing the OptiPoint with the new IP address.

12 OpenScape Application Monitoring

The application monitoring shows the state 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.

12.1 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.

12.2 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 12.2.1, “Receiving SNMP Traps from Applications”*.

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.

12.2.1 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.

13 Installation and Requirements

A detailed description of hardware and software requirements and the installation process can be found in the *OpenScape FM Desktop User Guide*.

A OpenScape Business/H3K rights

The plugin's access rights are integrated into the general access management (*see OpenScape FM Desktop User Guide*).

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

The names of the rights for this plugin begin with the plugin designation *OpenScape Business/H3K*.

Index

O

P

Q

R

S

T

V

© 2024 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.