A MITEL
PRODUCT
GUIDE

Mitel OpenScape Fault Management

Mitel OpenScape Fault Management V14, OpenScape Business/H3K Plugin

Bedienungsanleitung

10/2026

A31003-F30D0-U112-02-0019

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

Inhalt

1 Vorwort 5
1.1 Zweck 5
1.2 Zielgruppe 5
1.3 Gliederung dieses Handbuchs 5
1.4 In diesem Handbuch verwendete Konventionen 6
1.5 Terminologie 7

2 Übersicht 9
2.1 Einleitung 9
2.2 OpenScape Business/H3K-Systemmanagement 10
2.3 Die Management-Plattform OpenScape FM 11

3 OpenScape Business/H3K-Management 13
3.1 Initialisieren des OpenScape Business/H3K Plugins 13
3.2 Lizenzieren 13
3.3 Hinzufügen von Knoten zum System 14
3.4 Topologiekonzept für OpenScape Business/H3K-Netzwerke 14
3.4.1 Auto Discovery von Partnersystemen 14
3.4.2 Port-/Leitungsstatus 15
3.5 Hinzufügen eines OpenScape Business/H3K-SNMP-Agenten 15
3.6 Verfolgen von Ereignissen 15

4 Symbole und Übersichten 17
4.1 Symbole 17
4.1.1 Für OpenScape Business/H3K spezifische Symbole 17
4.2 Übersichten 19

5 Spezifische Informationen zu OpenScape Business/H3K 21
5.1 OpenScape Business/H3K-IP-Knoten 21
5.2 OpenScape Business/H3K-Komponente 21
5.3 Aufruf des Manager E über OpenScape FM 22
5.4 Status von OpenScape Business/H3K Systemen 22
5.5 Liste aller OpenScape Business/H3K-Systeme 22

6 Port-spezifische Informationen 23

7 OpenScape Business/H3K Gateway-spezifische Informationen 25
7.1 OpenScape Business/H3K Gateway-Kontextmenü 25
7.1.1 Ereignisse 25
7.1.1.1 Fehlerhistorie 25
7.1.1.2 Traps 25
7.1.2 Statistics 26
7.1.2.1 Globale Daten vCAPI Clients 28
7.1.2.2 Globale Daten H323 Clients 28
7.1.2.3 Globale Daten Workpoint Clients 28
7.1.3 Allgemeine Informationen 29
7.2 OpenScape Business/H3K Gateway-Subkomponenten 29
7.2.1 Web Based Management 30

8 IVM spezifischen Informationen 31
8.1 IVM-Kontextmenü 31

8.1.1 Beschreibung 31
8.1.2 Allgemeine Informationen 31
8.1.3 Installierte Sprachen 32
8.1.4 Mailbox Liste 32
8.1.5 Anmeldeinformationen 32

9 NAT in OpenScape FM 33
9.1 NAT mit dem OpenScape Business/H3K Gateway 33

10 VoIP-Überwachung (Voice over IP) in OpenScape FM 35
10.1 VoIP im OpenScape Business/H3K Gateway 35
10.1.1 Configure Connection Table 35
10.2 Anzeige des QoS-Status in VoIP-Netzen 36
10.2.1 Überwachung und Darstellung 37
10.2.2 Verfallszeit von Verknüpfungen 38

11 OptiPoint 400/600-Geräte 39
11.1 Erkennungsprozess 39
11.2 Darstellung und Statusüberwachung 40
11.3 OptiPoint-bezogene Ereignisse 40
11.4 IP-Adressen-Änderung von OptiPoints 41

12 OpenScape Applikationsüberwachung 43
12.1 Installierte Software auf einem Server 43
12.2 Überwachung von Programmen 43
12.2.1 Empfangen von SNMP-Traps von Applikationen 44

13 Installation und Anforderungen 45

A OpenScape Business/H3K-Rechte 47

Stichwörter 49

1 Vorwort

In diesem Kapitel werden folgende Aspekte behandelt:

- Zweck und Zielgruppe dieses Handbuchs
- Gliederung dieses Handbuchs
- In diesem Handbuch verwendete Konventionen
- Terminologie

1.1 Zweck

Dieses Handbuch stellt das **OpenScape Business/H3K Plugin für das OpenScape Fault Management** vor. Dieses plattformunabhängige Tool ermöglicht das webbasierte Management von Sprachnetzen und Datennetzwerken. Das Handbuch erläutert die grundlegenden Konzepte beim Einsatz des **OpenScape Business/H3K Plugins**. Außerdem werden die notwendigen Komponenten beschrieben. Grundkenntnisse in den Bereichen Netzwerkmanagement und OpenScape FM sollten vorhanden sein. Mehr dazu findet sich in der *OpenScape FM Desktop Bedienungsanleitung* und der *IP Manager Plugin Bedienungsanleitung*.

Dieses Handbuch zum OpenScape Business/H3K Plugin enthält auch Beschreibungen der Funktionen zur Applikationsüberwachung (Host-Ressourcen).

1.2 Zielgruppe

Dieses Handbuch richtet sich an Endanwender, die lernen möchten, wie das OpenScape Business/H3K Plugin für den OpenScape Desktop verwendet wird.

1.3 Gliederung dieses Handbuchs

In diesem OpenScape Business/H3K-Handbuch werden folgende Themen behandelt:

- *Kapitel 1, „Vorwort“* beschreibt die in diesem Handbuch verwendeten Begriffe.
- *Kapitel 2, „Übersicht“* beschreibt die Grundlagen des OpenScape Business/H3K Plugins und verdeutlicht das Fault Management in OpenScape Business/H3K-Netzwerken.
- *Kapitel 3, „OpenScape Business/H3K-Management“* erläutert den Start des OpenScape FM und beschreibt die Grundfunktionen dieses Tools.
- *Kapitel 4, „Symbole und Übersichten“* liefert eine detaillierte Beschreibung der Symbole und erklärt die Map-Hierarchie.

- *Kapitel 5, „Spezifische Informationen zu OpenScape Business/H3K“* erklärt die Überwachung einer OpenScape Business/H3K-Umgebung.
- *Kapitel 6, „Port-spezifische Informationen“* beschreibt die Vorgehensweise zur Überwachung von Ports.
- *Kapitel 7, „OpenScape Business/H3K Gateway-spezifische Informationen“* beschreibt die Beschaffung spezifischer Informationen zum OpenScape Business/H3K Gateway.
- *Kapitel 8, „IVM spezifischen Informationen“* beschreibt wie man spezifische Informationen über IVM-Baugruppen erhält.
- *Kapitel 9, „NAT in OpenScape FM“* erläutert die Umsetzung von Netzwerkadressen (Network Address Translation, NAT) in OpenScape Fault Management.
- *Kapitel 10, „VoIP-Überwachung (Voice over IP) in OpenScape FM“* beschreibt die Überwachung der VoIP-Funktionalität eines OpenScape Business/H3K Gateways.
- *Kapitel 11, „OptiPoint 400/600-Geräte“* erläutert die Darstellung von OptiPoint 400/600-Geräten in OpenScape FM.
- *Kapitel 12, „OpenScape Applikationsüberwachung“* beschreibt die Überwachung von auf OpenScape Business/H3K RSM-Servern laufenden Programmen.

1.4 In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden folgende Schriftkonventionen verwendet:

Fettgedruckte Schrift: Weist darauf hin, dass ein Wort ein wichtiger Begriff ist oder erstmals verwendet wird.

Beispiel: **Proxy-Agent** oder **OK**.

Fettgedruckte Computerschrift: Weist auf Daten hin, die der Anwender eingeben muss.

Beispiel: **`Java`**.

Computerschrift: Weist auf Computerausgaben (einschließlich UNIX-Prompts), einen expliziten Verzeichnis- oder Dateinamen hin.

Beispiel: `Prompt%`**.**

Kursiv gedruckte Schrift: Kennzeichnet einen Hinweis auf ein anderes Handbuch oder einen anderen Abschnitt im vorliegenden Handbuch.

Beispiel: *siehe IP-Manager-Dokumentation*

Kursiv gedruckte Schrift dient auch der Betonung.

Beispiel: *Alle* Benutzer sind davon betroffen

1.5 Terminologie

- **OpenScape FM** bedeutet OpenScape Fault Management.
- **Server** bezeichnet den OpenScape-Server, d. h. den Server, auf dem der OpenScape Desktop mit dem OpenScape Business/H3K Plugin installiert ist.
- **Client** bezeichnet den OpenScape FM-Client; typischerweise einen Web-Browser, in dem das OpenScape FM aufgerufen wurde.
- **Desktop** bezeichnet den OpenScape FM Desktop.

2 Übersicht

In diesem Kapitel werden folgende Aspekte behandelt:

- Einführung in die OpenScape FM-Architektur
- Grundlagen des Managements von OpenScape Business/H3K-Systemen.
- Die grafische Bedienoberfläche der Managementplattform OpenScape FM

2.1 Einleitung

Das OpenScape Business/H3K Plugin ist eine Fault Management-Applikation, die das Management von OpenScape Business/H3K Systemen in das OpenScape FM integriert. Das OpenScape FM teilt sich in einen Server und einen Client auf, die beide in Java(TM) geschrieben sind. Da der Client als Applet in einem Web-Browser ausgeführt werden kann, lässt er sich leicht in gängige Intranet-/Internet-Umgebungen integrieren. Das OpenScape Business/H3K Plugin dient als Erweiterung des OpenScape FM und kann nicht als eigenständige Applikation ausgeführt werden.

Zusätzlich unterstützt das OpenScape Business/H3K Plugin die vorherigen Technologien HiPath 2000/3000/5000, OpenScape Office sowie ComServer PC. Diese Technologien werden, obwohl sie vom OpenScape Business/H3K Plugin unterstützt werden, im OpenScape Business/H3K Handbuch nicht explizit erläutert.

OpenScape Business/H3K-Systeme werden an ein LAN oder Intranet angeschlossen und verfügen über einen eigenen SNMP-Agenten, der MIB II und eine private OpenScape Business/H3K Controller-MIB unterstützt. Der OpenScape Business/H3K-Manager verwendet daher SNMP (Simple Network Management Protocol) zum Sammeln von Informationen von den OpenScape Business/H3K-Systemen (siehe *Bild 1*). Heutzutage unterstützen nahezu alle Anbieter von Komponenten für offene Netzwerke das SNMP-Protokoll.

Neben den OpenScape Business/H3K-Systemen werden auch andere IP-Netzwerkknoten erkannt (Discovery), die über einen eigenen SNMP-Agenten verfügen, der seinerseits MIB II oder andere bekannte private MIB-Erweiterungen unterstützt. Diese Discoveries werden vom OpenScape IP Manager ausgeführt. Dieser bildet die Grundlage für den OpenScape Business/H3K-Manager und wird während der Installation des OpenScape Business/H3K Plugins automatisch installiert. Eine detaillierte Beschreibung des IP Managers findet sich in der *IP Manager Plugin Bedienungsanleitung*. Als IP-Knoten werden PCs, Workstations, Server oder spezifische OpenScape Business/H3K-Zugangsgeräte wie beispielsweise LP 5100-LAN-Telefone oder OpenScape Business/H3K-Adapter wie der AP 1100 erkannt. Zusätzlich erfolgt eine Erkennung spezifischer OpenScape Business/H3K-Applikationen wie CAP/Telas Web und TeleWorking/mWorks V1.0 durch spezielle Prüfungen (MIBs, Web-Server) auf allen erkannten IP-Knoten.

Das OpenScape FM unterstützt Client/Server-Architekturen. Das OpenScape Business/H3K Plugin setzt sich daher aus einer Server- und einer Client-Komponente zusammen. Die Server-Komponente übernimmt Managementaufgaben wie Netzwerk-Discovery, Datenerfassung von den Hicom-Systemen und Aufbau der Netzwerktopologie. Die grafische Bedienoberfläche des Clients bietet Zugriff auf die vom Server verwalteten Daten.

Bild 1 zeigt ein typisches Verwendungsbeispiel für den OpenScape Business/H3K-Manager. Auf dem Server läuft der OpenScape FM-Server-Prozess einschließlich der Server-Komponente des OpenScape Business/H3K Plugins. Der Server-Prozess kommuniziert mit dem SNMP-Agenten der OpenScape Business/H3K-Systeme, um Zugriff auf die Management-Informationsdatenbank (MIB) zu erhalten. Die Managementdaten werden analysiert und vom OpenScape Business/H3K Plugin verarbeitet. Als Bedienoberfläche für das OpenScape Business/H3K Plugin kann ein Web-Browser (z. B. Firefox, MS Internet Explorer) verwendet werden. Alternativ kann auch die eigenständige Client-Applikation installiert werden.

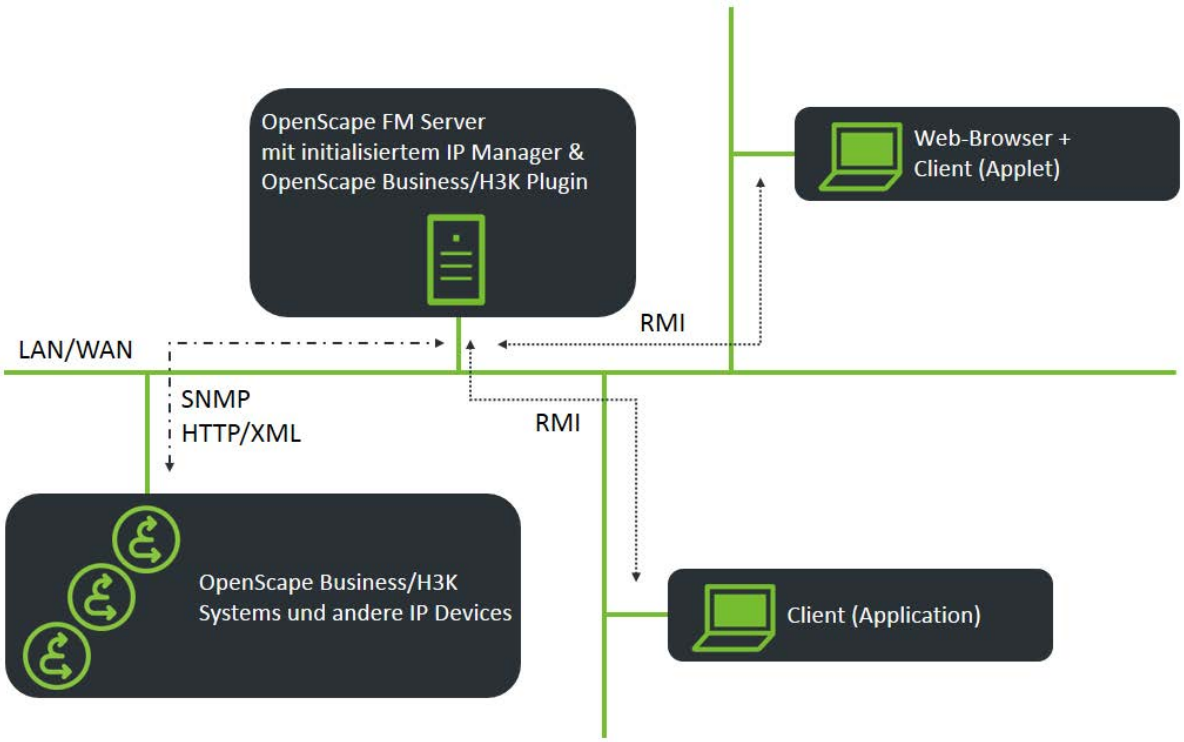

Bild 1 *SNMP-Management für OpenScape Business/H3K-Netzwerke*

In der aktuellen Version bietet das OpenScape Business/H3K Plugin Unterstützung für die folgenden Managementbereiche von OpenScape Business/H3K-Systemen.

- Fault Management
- Management der OpenScape Business/H3K-Netzwerktopologie
- Hardware-Bestandsinformationen

2.2 OpenScape Business/H3K-Systemmanagement

Ein OpenScape Business/H3K-Netzwerk besteht aus einem oder mehreren OpenScape Business/H3K-Systemen. Jedes OpenScape Business/H3K-System verfügt über einen eigenen SNMP-Agenten, der den Zugriff auf eine Reihe von Systemdaten ermöglicht, die in seiner Management-Informationsdatenbank (MIB) gespeichert sind. Die MIB liefert grundlegende Systeminformationen, Statusinformationen, ereignisbezogene Daten sowie Informationen zu installierter Hardware (Einbauplätze) und eingerichteten Verbindungen (Ports).

Die Server-Komponente des OpenScape Business/H3K Plugins kann über SNMP-Anfragen Informationen aus der MIB des Agenten auslesen. Diese Informationen werden vom Client-Applet (in einem Web-Browser) oder der Client-Applikation grafisch dargestellt. Die Kommunikation zwischen der Server-Komponente des OpenScape Business/H3K Plugins und dem Client erfolgt mittels RMI (Remote Method Invocation), die einen Teil des Java(TM)-Standards darstellt.

Die Netzwerkkomponenten des OpenScape Business/H3K-Managements sind in *Bild 1* dargestellt.

2.3 Die Management-Plattform OpenScape FM

Die Netzwerkmanagementstation, der OpenScape FM-Server, ist eine zentrale Komponente für die Netzwerkverwaltung. Eine der Kernfunktionen besteht in der dauerhaften Statusüberwachung der Netzwerkkomponenten und in der Information des Netzwerk-Administrators im Falle von Statusänderungen. Die Dienstprogramme für das Netzwerkmanagement bieten grafische Bedienoberflächen und eine grafisch dargestellte Map des Netzwerks, die die Topologie und den aktuellen Status der Netzwerkkomponenten anzeigt. Diese Funktionen werden ebenfalls von OpenScape FM und dem OpenScape Business/H3K-Manager unterstützt.

OpenScape FM mit OpenScape Business/H3K Plugin bietet:

- Hierarchische Abbildung der Netzwerktopologie in verschiedenen Abstraktionsebenen (OpenScape Business/H3K-Netzwerkansicht, Teilnetzwerkansicht usw.).
- Möglichkeit zur Feinabstimmung der Netzwerkansicht durch Gruppierung von OpenScape Business/H3K-Systemen in verschiedene Netzwerke und Teilnetzwerke.
- Darstellung von OpenScape Business/H3K-Ereignissen durch grafische Statusänderung der OpenScape Business/H3K-Symbole (Farbänderung).
- Darstellung der angeschlossenen externen Systeme – einschließlich grafischer Statusänderung der entsprechenden Symbole.
- Detaillierte Ereignisbeschreibung in Form von Textfenstern im Browser.
- Ausführliche Beschreibung der OpenScape Business/H3K-Netzwerktopologie.
- Detaillierte Beschreibung der installierten Hardware.

Diese allgemeinen Merkmale werden in den folgenden Kapiteln eingehender erläutert.

3 OpenScape Business/H3K-Management

Dieses Kapitel bietet einen Einstieg in die Arbeit mit dem OpenScape Business/H3K-Manager Plugin.

In diesem Kapitel werden die folgenden Aspekte behandelt:

- Initialisieren des OpenScape Business/H3K Plugins
- Lizenzieren
- Topologie-Konzept für OpenScape Business/H3K-Netzwerke
- Hinzufügen eines OpenScape Business/H3K-SNMP-Agenten
- Darstellung von Ereignissen

An dieser Stelle wird davon ausgegangen, dass das OpenScape FM bereits korrekt installiert wurde. Einzelheiten zum Installationsprozess finden sich in der *OpenScape FM Desktop Bedienungsanleitung.*

3.1 Initialisieren des OpenScape Business/H3K Plugins

Das OpenScape Business/H3K Plugin ein Bestandteil der OpenScape FM Installation, und wird zusammen mit diesem installiert. Einzelheiten zur Installation des OpenScape FM finden sich in der *OpenScape FM Desktop Bedienungsanleitung*.

Das Plugin kann über den Eintrag **Server->Plugins->Initialisiere OpenScape Business/H3K Plugin** aus dem Hauptmenü des OpenScape FM initialisiert werden.

Nach der Initialisierung wird der Menüpunkt **Initialisiere OpenScape Business/H3K Plugin** entfernt. Im Hauptmenü befindet sich nun ein neuer Menüpunkt: **Technologien->OpenScape Business/H3K**. Darüber hinaus wird ein Objekt, welches das OpenScape Business/H3K Plugin darstellt, in die Hierarchie eingefügt. Dieses hat den Pfad **Root->System->Plugins->Technologien**. Über das neue Objekt können die selben Menüpunkte aufgerufen werden, wie im OpenScape Business/H3K Menü.

3.2 Lizenzieren

Um mit dem OpenScape Business/H3K Plugin arbeiten zu können, wird eine gültige Lizenz benötigt. Einzelheiten zur Lizenzierung des OpenScape FM-Systems finden sich in der *OpenScape FM Desktop Bedienungsanleitung*.

Wichtiger Hinweis:
Der Lizenzierungsmechanismus des OpenScape Business/H3K Plugins wird sich nach der Auslieferung dieser Bedienungsanleitung ändern.
Der aktuelle Lizenzierungsmechanismus findet sich in den Release Notes für das Plugin.
Das Folgende beschreibt die Lizenzierung, wie zum Zeitpunkt der Erstellung dieser Bedienungsanleitung durchgeführt wurde.

Die Größe der benötigten Lizenz basiert auf der Anzahl der aktiven Ports. Sie wird für OpenScape Business/H3K Systeme unterschiedlich ermittelt:

OpenScape Business/H3K

Für OpenScape Business/H3K wird die Anzahl der aktiven Ports durch eine Auswertung der `h150ePortTable` der OpenScape Business/H3K Systeme ermittelt. Es werden alle Ports aus der MIB-Tabelle gezählt, die sich im Zustand (`portState`) '`active(2)`' befinden, und deren Typbezeichnung (`portType`) nicht den Teilstring '`trunk`' beinhalten.

OpenScape Business

OpenScape Business basiert auf Boxen, die jeweils eine begrenzte maximale Anzahl von Ports unterstützen. Für die Lizenzierung wird NICHT die tatsächliche Anzahl belegter Ports berücksichtigt, sondern die Anzahl der Ports, die für das jeweilige System belegt werden könnten.

3.3 Hinzufügen von Knoten zum System

Das OpenScape FM startet automatische ein Discovery, wenn ein neuer IP-Knoten hinzugefügt wird. Außerdem führt es in definierten regelmäßigen Intervallen Discoveries für alle bekannten IP-Knoten aus. Während dieser Discoveries wird ein IP-Knoten als OpenScape Business/H3K System identifiziert, falls in der lokalen OpenScape Business/H3K MIB das MIB-Objekt `h150eErrorHistoryGroup` existiert.

3.4 Topologiekonzept für OpenScape Business/H3K-Netzwerke

3.4.1 Auto Discovery von Partnersystemen

Die private MIB eines OpenScape Business/H3K-Systems enthält die MIB-Tabelle „`h150ePortTable`“ (`h150eSystemInfoGroup`), die während des Discovery eines Systems gelesen wird. Neben anderen Informationen enthält die Port-Tabelle auch das Feld `Port-Typ`. Dieses Feld gibt für eingerichtete Ports den Port-Typ (z. B. `CoreNetTrunk`) an und liefert ggf. Wegeleitungsinformationen zu einem mit diesem Port verbundenen Partnersystem (Nachbar). Der Port-Typ und die Wegeleitungsinformationen sind durch Doppelpunkte (`:`) getrennt. Die Wegeleitungsinformationen werden, wenn angegeben, verwendet, um das aktuell erkannte System mit einem Partnersystem zu verbinden. Die Richtung muss einer bekannten Host-Namens-/IP-Adressangabe bzw. einem MIB-II-Systemnamen (`sysName` in Systemgruppe) entsprechen. Anhand dieser Informationen kann das OpenScape Business/H3K Plugin die Topologie eines OpenScape Business/H3K-Sprachnetzes automatisch anzeigen.

Ein OpenScape Business/H3K-Objekt wird durch ein OpenScape Business/H3K-Systemsymbol dargestellt. Die Submap der entsprechenden Komponente enthält die für IP-Knoten üblichen Komponenten des OpenScape FM, z.B. Ereignisse und Interfaces. Zusätzlich beinhaltet die Submap der OpenScape Business/H3K Komponente weitere, OpenScape Business/H3K spezifische, Komponenten. Z.B. für erkannte Partnersysteme, erkannte IVM Geräte oder ein Router-Symbol falls es sich um ein OpenScape Business/H3K Gateway handelt, bei dem die IP-Weiterleitungsoption in der MIB II auf „*Ja*“ gestellt ist.

3.4.2 Port-/Leitungsstatus

Neben den Informationen über die einzelnen Geräte/IP-Knoten zeigt das OpenScape FM auch die dazwischen liegenden Verbindungen (Leitungen) an.

Die Statusinformationen für Leitungen (Ports) werden aus den Port-Tabellenfeldern `portState` und `portLock` entnommen. Ist beispielsweise `portStatus` aktiv, wird der zugehörige Verbindung der Status NORMAL (grün) zugewiesen. Ist die Option nicht aktiv, ändert sich der Status auf WARNHINWEIS (hellblau). *Tabelle 1* zeigt die möglichen Zustände.

		portState	
		aktiv	**nicht aktiv**
portLock	entsperrt	NORMAL	WARNHINWEIS
	gesperrt	DEAKTIVIERT	WARNHINWEIS

Tabelle 1 Regeln zum Einstellen des Port-/Leitungsstatus

Alle Leitungsbündel, die für diese Verbindung registriert sind, finden sich in den Ansichten (Submaps und Bäume) eines Verbindungssymbols.

3.5 Hinzufügen eines OpenScape Business/H3K-SNMP-Agenten

Das OpenScape Business/H3K Plugin kommuniziert mit einem oder mehreren OpenScape Business/H3K-SNMP-Agenten und erhält so Managementinformationen zu den zugehörigen OpenScape Business/H3K-Netzwerken.

Um ein neues OpenScape Business/H3K-System hinzuzufügen, ist es ausreichend, den Systemknoten dem IP Manager hinzuzufügen. OpenScape FM benötigt die IP-Adresse des OpenScape Business/H3K-SNMP-Agenten oder einen Hostnamen, der über DNS (Domain Name Service) bzw. die Hosts-Datei auf dem Management-Server aufgelöst werden kann (siehe *„IP Manager Plugin Bedienungsanleitung“).*

OpenScape FM versucht, das System über eine TCP-Verbindung zu erreichen. Ist diese Suche erfolgreich, wird die SNMP-Discovery gestartet.

3.6 Verfolgen von Ereignissen

Das OpenScape Business/H3K Plugin zeigt Ereignisse über den Ereignis-Browser an (siehe *OpenScape FM Desktop Bedienungsanleitung*).

Jedes Ereignis ist mit einem verwalteten Objekt verknüpft, z. B. einem OpenScape Business/H3K-System oder einem SNMP-Agenten.

Die im Ereignis-Browser gezeigten Ereignisse stellen registrierte interne Traps und externe SNMP-Traps dar, die von den SNMP-Agenten (hier die OpenScape Business/H3K-Systeme) an den SNMP-Manager (hier der Server) geschickt wurden. Für die für OpenScape Business/H3K spezifischen Traps müssen keine Trap-Ziele auf den OpenScape Business/H3K-Systemen eingestellt werden, da sich der Server während der IP-Discoveries automatisch als Trap-Ziel registriert.

Sollen SNMP-Traps von Applikationen eines Systems erhalten werden, das die Host-Ressourcen-MIB unterstützt, muss dieses System entsprechend eingerichtet werden. Einzelheiten dazu finden sich im *Kapitel 12, „OpenScape Applikationsüberwachung“*.

4 Symbole und Übersichten

Mit dem OpenScape Business/H3K Plugin gibt es einige neue Objekttypen, die durch neue Symboltypen dargestellt werden. Ein einzelnes verwaltetes Objekt (Managed Object) kann in verschiedenen Ansichten (Submaps und/oder Bäume) durch viele unterschiedliche Symbole dargestellt werden. Das verwaltete Objekt selbst ist die softwareinterne Darstellung einer realen zu verwaltenden Ressource, z. B. ein Hicom-System oder ein Leitungsbündel. Die Ansichten dienen als Gruppierung zusammengehöriger verwalteter Objekte zur Darstellung der Objekt-Hierarchie. Zusätzlich zu den Standardansichten können individuelle Submap-Hierarchien erstellt werden.

Eine ausführliche Einführung zum Umgang mit Maps und Ansichten (Submaps und Bäume) findet sich in der *OpenScape FM Desktop Bedienungsanleitung*. Jedes Symbol in einer Ansicht bietet ein objektspezifisches Kontextmenü, das über einen Rechtsklick auf das Symbol geöffnet werden kann. Das Kontextmenü einer Submap öffnet sich durch einen Rechtsklick auf den Hintergrund der Submap.

In den folgenden Kapiteln werden die verschiedenen Objekte und deren Symbole erläutert, die vom Topologie-Manager und dem OpenScape Business/H3K Plugin erstellt werden. *Kapitel 5, „Spezifische Informationen zu OpenScape Business/H3K“* befasst sich mit den Objekt spezifischen Kontextmenüs und deren Funktionen.

4.1 Symbole

4.1.1 Für OpenScape Business/H3K spezifische Symbole

Die folgenden Symbole werden vom OpenScape Business/H3K Plugin zu den standardmäßigen OpenScape-Symbolen hinzugefügt:

- **IP-Knotensymbol**, **H3K-Agent**

Das H3K-Symbol stellt ein einzelnes H3K-System dar, also einen IP-Knoten mit laufendem SNMP-Agenten mit einer H3K Controller-MIB. Über dieses Symbol können eine Reihe von Operationen am System durchführt werden. Diese Funktionen dienen zum Abrufen detaillierter Informationen oder zum Ausführen von Administrationsaufgaben.

Neben dem H3K-Symbol befindet sich die Gesamtstatusanzeige. Eine detaillierte Beschreibung der Gesamtstatusanzeige findet sich in der *OpenScape FM Desktop Bedienungsanleitung*.

- **/H3K-Komponentensymbol**

- **H3K Gateway-Symbol**

- **Routersymbol** (Topology Manager spezifisches Symbol)

Ein OpenScape Business/H3K Gateway ist ein IP-Gerät, das in ein OpenScape Business/H3K-System integriert ist, also eine eigene IP-Adresse besitzt. Da bei diesen Geräten die IP-Weiterleitung standardmäßig aktiviert ist, erscheinen die OpenScape Business/H3K Gateway-Symbole der IP-Ansicht (als Router) und in der Netzwerkansicht.

- **Verbindungsüberwachungssymbol** (ehemals VoIP)

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

- **OptiPoints-Container-Symbol**

- **ipphone-Symbol**

- **OptiPoint-Symbol**

- **IVM-Baugruppe-Symbol**

- **OpenScape Business Symbol**

- **OpenScape Business Control Symbol**

- **OpenScape Business Gateway Symbol**

- **OpenScape Business S Symbol**

- **OpenScape Business S Control Symbol**

- **OpenScape Business S Gateway Symbol**

4.2 Übersichten

Wurde das ControlCenter Plugin initialisiert, so wird für OpenScape Business/H3K Objekte eine Reihe von ControlCenter-Übersichten bereitgestellt. Die Zusammenfassung der Objekt-Typen erfolgt, da die Ereignisse dieser Objekte die gleichen Trap-Typen verwenden, und die Ereignisse daher alle in der Kategorie ’OpenScape Business/H3K’ zu finden sind.

Es werden die folgenden Übersichten angeboten:

- Die letzten zehn OpenScape Business/H3K Systeme, die in den Zustand ’kritisch’ gewechselt haben, und die sich noch in diesem Zustand befinden.
- Die zehn OpenScape Business/H3K Systeme mit den meisten unbestätigten Ereignissen.
- Die zehn letzten Ereignisse der Kategorie ’OpenScape Business/H3K’, die einen schlechteren Status als ’normal’ hatten.
- Die Verteilung der unbestätigten Ereignisse der Kategorie ’OpenScape Business/H3K’ nach Status.
- Die Verteilung der Ereignisse der Kategorie ’OpenScape Business/H3K’ über die Zeit.

Die Übersichten können angezeigt werden, indem im **Technologien->OpenScape Business/H3K** Menü in der Hauptmenüleiste der Eintrag **ControlCenter - Übersicht** ausgewählt wird.

Mehr über das ControlCenter findet sich in der *Control Center Plugin Bedienungsanleitung*.

5 Spezifische Informationen zu OpenScape Business/H3K

OpenScape FM liefert umfangreiche Informationen zu den OpenScape Business/H3K-Systemen. Diese können über das Kontextmenü von jedem OpenScape Business/H3K-Systemsymbol oder einem OpenScape Business/H3K-IP-Knotensymbol abgerufen werden.

Eine Liste der OpenScape Business/H3K IP-Knoten kann über den Hauptmenüeintrag **Technologien->OpenScape Business/H3K->Zeige Hosts** aufgerufen werden. Diese Liste ermöglicht einen zentralen Zugriff auf die Kontextmenüs der einzelnen Objekte.

5.1 OpenScape Business/H3K-IP-Knoten

Das Kontextmenü eines OpenScape Business/H3K IP-Knoten-Symbols enthält das OpenScape Business/H3K spezifische Menü **OpenScape Business/H3K**.

Dieses Menü enthält die gleichen Einträge wie das Kontextmenü einer OpenScape Business/H3K-Komponente. Diese werden im folgenden Abschnitt näher beschrieben.

5.2 OpenScape Business/H3K-Komponente

Das Kontextmenü eines OpenScape Business/H3K Komponenten-Symbols enthält OpenScape Business/H3K spezifische Einträge, die im folgenden beschrieben werden.

Zusätzlich erscheinen die Einträge **Manager E Start** und **Manager E Dialog** ebenfalls im Kontextmenü, falls der *Manager E für OpenScape Business/H3K* auf der gleichen Maschine installiert wurde, auf welcher der aktuelle OpenScape FM Client läuft. Beim Start des Clients wird automatisch geprüft, ob diese Applikation auf dem Client-System installiert wurde. Diese Einträge sind auch im Web-Browser verfügbar, sofern der Manager auf dem Client-System installiert ist (siehe *Abschnitt 5.3, „Aufruf des Manager E über OpenScape FM“*).

Die folgenden OpenScape Business/H3K spezifischen Einträge befinden sich im Untermenü **OpenScape Business/H3K**.

- **System-Info...** zeigt Hardware-Version, Software-Version, Code-Nummer und Softwareinstallation des OpenScape Business/H3K Systems.
- **Ereignisse->Ereignis-Konfiguration...** kann zum Einstellen des Ereignistyps verwendet werden. Es kann zwischen *log* und *log-and-trap* ausgewählt werden. *log* schreibt das Ereignis in das Ereignisprotokoll des OpenScape Business/H3K-Systems. *log-and-trap* schreibt das Ereignis in das Ereignisprotokoll und sendet eine SNMP-Trap an die Managementstation.
- **Ereignisse->Ereignis Log...** zeigt die Einträge des Ereignisprotokolls.
- **Ereignisse->Fehlerhistorie...** zeigt eine Fehlerhistorie für dieses OpenScape Business/H3K-System.
- **Einbauplätze...** liefert Informationen über die Einbauplätze des Systems (Kartennummer, Boxnummer, Einbauplatznummer, Kartentyp, Kartenbeschreibung, Kartencodenummer und Kartenstatus).

- **Ports...** zeigt Informationen über die Ports des Systems (Port-Nummer, zugeordnete Karte, Typ, allgemeiner Zustand, Verriegelungsstatus und Zielknoten ID).
- **Features...** (Funktionen) liefert Informationen über die Verwendung der für OpenScape Business/H3K spezifischen Funktionen (Funktionsnummer, Beschreibung und Zähler).
- **Teilnehmer**: zeigt eine Tabelle mit den Teilnehmeranschlüssen für OpenScape Business Systeme an. Für ältere OpenScape Business/H3K Modelle wird eine leere Tabelle angezeigt, da für diese die SNMP-Tabelle mit den entsprechenden Daten nicht existiert.

5.3 Aufruf des Manager E über OpenScape FM

Wenn der OpenScape FM-Client auf einem System mit Manager E installiert wurde, kann der Manager über das Symbol des OpenScape Business/H3K-Systemsymbols gestartet werden. In diesem Fall enthält das Kontextmenü die Einträge **Manager E Start** und **Manager E Dialog**.

Der Eintrag **Manager E Dialog** öffnet ein Fenster, das dazu verwendet werden kann, den **Benutzernamen** und das **Passwort** zu konfigurieren, mit dem der Manager E auf der entsprechenden Maschine gestartet werden soll. Wird die **Default**-Option verwendet, kann eine Anwender/Passwort-Kombination konfiguriert werden, die als Default-Option für alle Manager E verwendet wird.

Wurden Benutzername und Passwort korrekt konfiguriert, kann der Manager über den Menüeintrag **Manager E Start** gestartet werden.

5.4 Status von OpenScape Business/H3K Systemen

Die MIB für OpenScape Business/H3K definiert einen Trap mit der Bezeichnung `sendAlarm`. OpenScape Business/H3K Systeme senden den Alarm an das OpenScape FM und dort wird dieser als Ereignis im Ereignis-Browser angezeigt. Basierend auf dem Inhalt dieser Traps (Variablen-Bindung) wird dem jeweiligen Ereignis ein spezifischer Status zugewiesen. Die einzelnen Ereignisse können durch den Anwender im Ereignis-Browser bestätigt werden.

Der Status eines OpenScape Business/H3K Objektes ergibt sich aus dem höchsten Status aller nicht bestätigten Ereignisse im Ereignis-Browser, die dem jeweiligen Objekt zugeordnet sind.

5.5 Liste aller OpenScape Business/H3K-Systeme

Ein Überblick über alle aktuell verwalteten OpenScape Business/H3K Systeme kann über den Eintrag **Zeige Hosts...** angezeigt werden. Dieser befindet sich im Hauptmenü **Technologien->OpenScape Business/H3K**. Im erscheinenden Info-Browser repräsentiert jede Zeile ein OpenScape Business/H3K-System und bietet das jeweilige objektspezifisches Kontextmenü an.

Die Schaltfläche **Aktualisieren** startet eine neue Abfrage.

Die Schaltfläche **Stopp** hält eine laufende Abfrage an.

6 Port-spezifische Informationen

Wenn ein Verbindungssymbol geöffnet wird, werden alle Ports angezeigt, die an einem oder beiden Endpunkten der Verbindung eingestellt sind. Für jeden Port werden Quelle und Zielsystem angezeigt.

Wie bei allen anderen Symbolen, zeigt auch hier die Farbe der Symbole den aktuellen Status an.

Port-Symbole bieten ein objektspezifisches Kontextmenü, über das der Port gesperrt/entsperrt werden kann (Eintrag: **Port sperren** oder **Port entsperren**). Der Sperr-/Entsperrvorgang resultiert in einem SNMP SET-Vorgang auf dem entsprechenden OpenScape Business/H3K-System, d.h., der Port wird auf diesem System gesperrt. Ein gesperrter Port wird mit einem braunen Portsymbol angezeigt, das beim Entsperren wieder grün wird.

7 OpenScape Business/H3K Gateway-spezifische Informationen

Wenn ein IP-Knoten mit einer OpenScape Business/H3K Gateway MIB erkannt wird, wird ein IP-Knotenobjekt mit einem untergeordneten OpenScape Business/H3K Gateway-Objekt angelegt. Der IP-Knoten erscheint in dem IP-Netzwerk, zu dem er gehört. Darüber hinaus erscheint das OpenScape Business/H3K Gateway-Objekt in der Submap des OpenScape Business/H3K-Geräts, in dem es installiert ist. Wenn in der `systemGroup` der MIB II des OpenScape Business/H3K Gateways keine `sysLocation` definiert worden ist, setzt OpenScape FM die Netzwerkkennung auf „OpenScape Business/H3K Gateway" – so dass nach der erstmaligen Discovery alle OpenScape Business/H3K Gateway-Geräte in dem Netzwerk mit der Bezeichnung „OpenScape Business/H3K Gateway" zu finden sind.

7.1 OpenScape Business/H3K Gateway-Kontextmenü

Über das Kontextmenü des OpenScape Business/H3K Gateways können die OpenScape Business/H3K Gateway-Daten abgerufen werden. Bei Anklicken der einzelnen Menüpunkte (in nachfolgenden Abschnitten näher erläutert) öffnen sich verschiedene Info-Browser, die OpenScape Business/H3K Gateway-spezifische Informationen enthalten. Der Abruf der Informationen erfolgt über SNMP.

7.1.1 Ereignisse

Über den Menüeintrag **Ereignisse** können alle für das OpenScape Business/H3K Gateway registrierten Fehler und alle Trap-Ereignisse eingesehen werden.

7.1.1.1 Fehlerhistorie

Über den Menüeintrag **Ereignisse->Fehlerhistorie** öffnet sich ein Info-Browser, in dem alle Fehlerbedingungen des OpenScape Business/H3K Gateways aufgelistet sind.

Der Browser besitzt die folgenden Spalten:

Fehlerklasse: Die Fehlerklasse. Die Fehlerklasse wird durch die Komponente vorgegeben, die den Fehler verursacht hat.

Datum/Zeit: Zeitstempel; Zeitpunkt, zu dem der Fehler aufgetreten ist.

Beschreibung: Kurze Beschreibung des Fehlers.

7.1.1.2 Traps

Über den Menüeintrag **Ereignisse->Traps** öffnet sich ein Info-Browser, in dem alle Trap-Ereignisse aufgelistet sind, die vom OpenScape Business/H3K Gateway erzeugt wurden.

Er enthält die folgenden Spalten:

Status: Für jeden Trap wird die Dringlichkeitsstufe mit „*normal*", „*warning*", „*minor*", „*major*" oder „*critical*" angegeben.

Fehlerklasse: Fehlerklasse, welche den Trap verursacht hat; mögliche Klassen sind „*general*", „*security*", „*data*" und „*voice*".

Fehlercode: Interner Code des Fehlers, der den Trap veranlasst hat.

Datum/Zeit: Zeitpunkt, zu dem der Trap erzeugt wurde.

Bearbeitung: Für jeden Trap-Typ kann vorgeben werden, ob bei Auftreten des Trap-Ereignisses ein SNMP-Trap gesendet oder ob das Trap-Ereignis nur lokal auf dem OpenScape Business/H3K Gateway gespeichert werden soll. Diese Konfiguration kann allerdings nicht über die OpenScape FM Oberfläche geschehen, sondern muss auf dem OpenScape Business/H3K Gateway erfolgen (beispielsweise mit Manager I). Ist der Eintrag *stored*, bedeutet dies, dass das betreffende Ereignis nur lokal gespeichert wurde. Ist der Eintrag *forwarded*, bedeutet dies, dass das Ereignis lokal gespeichert UND ein SNMP-Trap erzeugt und an alle Trap-Ziele gesendet wurde.

Beschreibung: Ausführliche Beschreibung des Fehlers, der den Trap verursacht hat.

7.1.2 Statistics

Über die Einträge im Menü **Statistik** können Tabellen mit Statistiken über den Datenaustausch aufgerufen werden. Die einzelnen Positionen dieses Menüs werden in nachfolgenden Paragraphen ausführlicher beschrieben.

H.323 (nur für H3K-Systeme)

Der H.323-Standard ist die Ausgangsbasis für den Transport von Audio-, Video- und sonstigen Daten über IP-basierende Netze, also auch über das Internet. H.323 ist eine Rahmenempfehlung der ITU (Internationale Fernmeldeunion), in der Standards für die Multimedia-Kommunikation über LANs (Local Area Networks) festgelegt werden, die allerdings keine bestimmte Dienstgüte garantieren.

Die Medienströme werden über das RTP/RTCP transportiert. Das RTP befördert dabei die eigentlichen Mediendaten und das RTCP die Status- und Kontrollinformationen.

RTP

Der Begriff „RTP" wird im folgenden Paragraphen erklärt. Er ist ein Auszug aus dem RFC 1889, in dem dieser Standard publiziert wurde.

RTP steht für Real-Time Transport Protocol (Echtzeit-Transportprotokoll). Es bietet verschiedene Dienste für den Ende-zu-Ende-Transport von Daten mit Echtzeitanforderungen an, beispielsweise für interaktives Audio und Video. Hierzu zählen unter anderem die Identifizierung des transportierten Nutzdatentyps (Payload), die fortlaufende Nummerierung der Pakete (Sequence Numbering), das Hinzufügen von Zeitstempeln (Time Stamping) und das Überwachen des Datentransports (Delivery Monitoring). Anwendungen setzen das RTP in der Regel auf dem UDP auf, um seine Multiplex- und Prüfsummendienste nutzen zu können. Beide Protokolle stellen bestimmte Teile der Funktionalität des Transportprotokolls bereit.
Allerdings kann das RTP auch mit verschiedenen anderen darunterliegenden Netzwerk- oder Transportprotokollen kombiniert werden. Zu beachten ist, dass das RTP selbst keine Mechanismen anbietet, um die pünktliche Auslieferung von Datenpaketen zu gewährleisten oder die Dienstgüte auf sonstige Weise

zu garantieren. Hierfür werden gegebenenfalls Dienste auf unteren Schichten benötigt. Das RTP garantiert darüber hinaus weder die Lieferung eines Pakets an einen Empfänger, noch vermeidet es die Lieferung von verspäteten Datenpaketen. Es geht auch nicht davon aus, dass das zugrundeliegende Netzwerk zuverlässig ist und Pakete in der richtigen Reihenfolge ausliefert. Anhand der fortlaufenden Nummern im RTP kann der Empfänger die Reihenfolge der gesendeten Pakete rekonstruieren. Außerdem kann anhand dieser Nummer jedes Paket exakt platziert werden, beispielsweise bei der Dekodierung von Videodaten, auch wenn die Pakete nicht fortlaufend dekodiert werden. Das RTP ist zwar in erster Linie für Multimedia-Konferenzen mit mehreren Teilnehmern bestimmt, allerdings nicht auf diese spezielle Anwendung beschränkt. Auch bei der Speicherung zeitkritischer (kontinuierlicher) Daten, bei interaktiven, verteilten Simulations-, bei Lokalisierungs- (Active Badge)- sowie bei Steuerungs- und Messanwendungen könnte das RTP eingesetzt werden.
(Ende des RFC 1889-Auszugs).

RTCP

Die Statistikdaten können nicht vom RTP selbst bereitgestellt werden, sondern basieren auf Informationen, die mit Hilfe des RTCP, des RTP-Kontrollprotokolls, abgerufen werden. Die nachfolgenden Zeilen sind ein kurzer Auszug aus dem RFC 1889.

Das RTP-Steuerungsprotokoll (RTCP) basiert auf der periodischen Übertragung von Kontrollpaketen an alle Sitzungsteilnehmer, wobei diese Pakete mit demselben Mechanismus verteilt werden wie die Datenpakete. Das darunterliegende Protokoll muss das Multiplexing der Daten- und Kontrollpakete unterstützen, also beispielsweise, wie beim UDP, separate Port-Nummern benutzen. Das RTCP führt insgesamt vier Funktionen aus:

1. Die wichtigste Funktion ist das Feedback zur Qualität der Datenverteilung. Hierbei handelt es sich um einen integrierten Bestandteil der Aufgabe des RTP als Transportprotokoll, der sich auch auf die Ablaufsteuerung und Überlastungskontrolle anderer Transportprotokolle auswirkt.
   (...)
2. Das RTCP stellt auf der Transportschicht eine persistente Kennung für eine RTP-Quelle bereit.
3. Die ersten beiden Funktionen erfordern, dass alle Teilnehmer RTCP-Pakete senden. Deshalb muss die Übertragungsrate kontrolliert werden, damit das RTP sich auf eine große Anzahl Teilnehmer einstellen kann. Indem jeder Teilnehmer seine Kontrollpakete an alle anderen sendet, kann jeder Teilnehmer für sich die Anzahl der Teilnehmer im Auge behalten. Anhand dieser Zahl wird dann die Rate berechnet, mit der die Pakete übertragen werden.
4. Eine vierte, optionale Funktion ist die Weiterleitung minimaler Informationen für die Sitzungssteuerung, beispielsweise die in der Bedienoberfläche anzuzeigende Teilnehmerkennung.
   (...)
   (Ende des RFC 1889-Auszugs).

TFA

TFA (Telephony Feature Access; Zugriff auf Telefonie-Leistungsmerkmale) ist ein Unify-eigenes Protokoll. Heutzutage wird häufig das Synonym „HFA” (Hicom Feature Access; Zugriff auf Hicom-Leistungsmerkmale) benutzt.

TFA (HFA) ist ein erweiterter Standard für die IP-Telefonie: Sprachdaten werden über H.323 übertragen, während die Signalisierung der Leistungsmerkmale über CorNet, einen Unify-Standard, erfolgt. So kann das TFA (HFA) alle Hicom-Leistungsmerkmale bereitstellen, selbst die für Endgeräte.

In den folgenden Abschnitten wird erklärt, wie OpenScape Business/H3K Gateway-Statistikdaten abgerufen werden können und was die angezeigten Werte bedeuten.

7.1.2.1 Globale Daten vCAPI Clients

Das OpenScape Business/H3K Gateway ist ein virtueller CAPI (VCvCAPI)-Server, bei dem sich verschiedene vCAPI-Clients anmelden können, die im Regelfall auf PCs installiert sind. Deshalb brauchen diese PCs keine ISDN-Hardware, sondern kommunizieren über eine virtuelle CAPI-Schnittstelle – den vCAPI-Client. Wenn der PC eine Verbindung über die ISDN-Schnittstelle herstellen muss, meldet er sich bei seinem vCAPI-Server, dem OpenScape Business/H3K Gateway, an, das wiederum die echte ISDN-Verbindung zur Verfügung stellt.

Der Menüeintrag **Statistik->Globale Daten vCAPI Clients...** öffnet einen Browser, der Information über vCAPI-Clients anzeigt. Er enthält die folgenden Informationen:

Anzahl installierter vCAPI Clients (No. vCAPI Clients Installed): Die Anzahl der vCAPI-Clients, die von diesem Server verwaltet werden können.

Anzahl angemeldeter vCAPI Clients (No. vCAPI Clients Logged In): Die Anzahl der vCAPI-Clients, die zum aktuellen Zeitpunkt eine gültige Verbindung zu diesem Server hergestellt haben.

Anzahl aktiver vCAPI Clients (No. vCAPI Clients Active): Die Anzahl der vCAPI-Clients, die derzeit auf diesem Server arbeiten.

7.1.2.2 Globale Daten H323 Clients

Der Menüeintrag **Statistik->Globale Daten H323 Clients...** öffnet einen Info-Browser mit allgemeinen Informationen über alle H.323-Clients des OpenScape Business/H3K Gateways. Er enthält die folgenden Informationen:

Anzahl aktiver H323 Clients: Anzahl der aktiven H.323-Clients.

Anzahl installierter H323 Clients: Anzahl der auf diesem OpenScape Business/H3K Gateway installierten H.323-Clients, d. h. maximal nutzbare Anzahl H.323-Clients.

7.1.2.3 Globale Daten Workpoint Clients

Der Menüeintrag **Statistik->Globale Daten Workpoint Clients...** öffnet einen Info-Browser mit allgemeinen Informationen über alle TFA-Clients des OpenScape Business/H3K Gateways. Eine Erläuterung des TFA-Standards finden sich in *Abschnitt 7.1.2, „TFA“*.

Über das OpenScape Business/H3K Gateway können sowohl TFA- als auch H.323-Verbindungen laufen. Allerdings muss sich der Client bei einer TFA-Verbindung mit einem gültigen Benutzernamen/Passwort beim OpenScape Business/H3K Gateway anmelden.

Der Browser enthält die folgenden Informationen:

Anzahl installierter TFA Clients: Anzahl der installierten TFA-Clients.

Anzahl aktiver TFA Clients: Anzahl der aktiven TFA-Clients.

Anzahl registrierter TFA Clients: Anzahl der registrierten TFA-Clients.

Anzahl erfolgreicher TFA Client Anmeldungen: Anzahl der erfolgreichen Anmeldungen von TFA-Clients.

Anzahl erfolgloser TFA Client Anmeldungen: Anzahl der fehlgeschlagenen Anmeldungen von TFA-Clients.

7.1.3 Allgemeine Informationen

Der Menüeintrag **Allgemeine Informationen** öffnet einen Info-Browser mit allgemeinen Informationen zu dem betreffenden OpenScape Business/H3K Gateway-Gerät. Es werden die folgenden Informationen angezeigt.

Idx letzter Trap: Index des letzten Traps, der vom OpenScape Business/H3K Gateway übertragen wurde. Bei dem Trap-Index handelt es sich um eine Zahl, die bei jeder neuen Trap um 1 erhöht wird.

Fehlerereignisse als Traps signalisiert: Ganzzahliger Wert einer bit-codierten Trap-Definition.

Fehlerzustand: Aktueller Fehlerzustand des OpenScape Business/H3K Gateways.

Verbindungsstatus: Status der Verbindung zwischen dem OpenScape Business/H3K Gateway und dem OpenScape Business/H3K-Gerät, auf dem er installiert ist.

MAC Adresse: Hardwareadresse des OpenScape Business/H3K Gateways.

Software Version: Version der derzeit installierten und laufenden OpenScape Business/H3K Gateway-Software.

Agentenversion: Version des SNMP-Agenten des OpenScape Business/H3K Gateways.

7.2 OpenScape Business/H3K Gateway-Subkomponenten

Wird die Submap eines IP-Knotens geöffnet, bei dem es sich um ein OpenScape Business/H3K Gateway handelt, werden alle zugehörigen Komponenten angezeigt.

Auf der Submap des Symbols *Interfaces* werden alle erkannten Schnittstellen angezeigt. Die OpenScape Business/H3K Gateway-Symbole stehen für verschiedene Funktionsbereiche des OpenScape Business/H3K Gateways:

- OpenScape Business/H3K Gateway-Funktionalität (beschrieben in diesem Kapitel)
- NAT-Funktionalität (siehe *Kapitel 9, „NAT in OpenScape FM“*)
- Verbindungsüberwachungs-Funktionalität (ehemals VOIP) (siehe *Kapitel 10, „VoIP-Überwachung (Voice over IP) in OpenScape FM“*)

Die SNMP-Submap enthält alle unterstützten MIBs.

Außerdem gibt es u.U.einen OptiPoint-Container und einen QoS-Container. Der OptiPoint-Container enthält die angeschlossenen OptiPoint 400/600-Geräte (siehe *Kapitel 11, „OptiPoint 400/600-Geräte“*). Der QoS-Container enthält Symbole für schlechte Verbindungen, die bei IP-Telefongeräten dieses OpenScape Business/H3K Gateways auftreten (siehe auch *Abschnitt 10.2, „Anzeige des QoS-Status in VoIP-Netzen“)*.

Die Unterstützung der MIB-Trees, welche die Daten für die OptiPoint- und QoS-Container bereitstellen, wurde nie umgesetzt. Daher wurden die entsprechenden Objekte beginnend mit OpenScape FM V4 R3 entfernt.

7.2.1 Web Based Management

Für ein OpenScape Business/H3K Gateway V3.0 wird überprüft, ob das „Web Based Management Interface“ verfügbar ist. In diesem Fall werden die Menüeinträge **Web Based Management...** und **Web Based Management Dialog...** angeboten. Der Menüeintrag **Web Based Management Dialog...** öffnet den Dialog, in dem das Benutzername/Passwort-Paar konfiguriert werden kann. Über den Menüeintrag **Web Based Management...** kann die URL des „Web Based Management Interfaces“ aufgerufen werden.

8 IVM spezifischen Informationen

IVM, auch als Xpression Compact bekannt, ist eine integrierte Voice-Mail Lösung für OpenScape Business/H3K systeme. Die IVM-Baugruppen besitzen ein separates LAN-Interface und haben eine eigene IP-Adresse.

Wenn ein OpenScape Business/H3K-Objekt entdeckt worden ist, auf dem eine IVM-Baugruppe entdeckt wurde, wird ein IP-Knoten für diese IVM-Baugruppe angelegt. Diesem IP Knoten wird ein IVM-Objekt als Kind-Objekt zugewiesen. Der IP-Knoten wird in dem zugehörigen IP-Netzwerk angelegt. Zusätzlich wird der IP-Knoten auf der Submap des OpenScape Business/H3K-Systems angezeigt, auf dem es installiert ist. Die IVM-Baugruppe wird erst als solches erkannt, wenn das OpenScape Business/H3K-System, auf dem die Baugruppe installiert ist, OpenScape FM bekannt ist, da das OpenScape Business/H3K-System die Informationen zu dieser IVM-Baugruppe liefert.

Die IVM-Baugruppe liefert keine spezifischen Status-Informationen. Das zugehörige IP-Knoten Symbol wird abhängig vom Status des IP-Interfaces gesetzt, wie die anderen IP-Knoten auch.

8.1 IVM-Kontextmenü

Das IVM-Objekt bietet ein spezifisches Kontextmenü an, welches Zugang zu den IVM-Daten ermöglicht. Die jeweiligen Menüpunkte öffnen mehrere Info-Browser die IVM-spezifische Informationen auflisten. Die einzelnen Info-Browser werden in den folgenden Abschnitten näher erläutert. Die Information werden über FTP abgefragt.

Hinweis:
Es ist zu beachten, dass eine Abfrage der IVM spezifischen Informationen mindestens zehn Sekunden dauert.

8.1.1 Beschreibung

Der Menüeintrag **Beschreibung** liefert eine kurze Beschreibung über die IVM-Baugruppe. Die Information wird von dem OpenScape Business/H3K-System geliefert.

8.1.2 Allgemeine Informationen

Über den Menüeintrag **Allgemeine Informationen...** kann ein Info-Browser geöffnet werden, der allgemeine Informationen über die entsprechende IVM-Baugruppe liefert. Er enthält die folgenden Informationen:

Software Version: die Version der installierten Software.

Hardware Version: die Hardware-Version.

Festplatten Auslastung: die aktuelle Festplatten-Auslastung in Prozent.

Installierte Postfächer: die Anzahl der installierten Postfächer.

Freie Postfächer: die Anzahl der freien Postfächer.

Freie Leitungen: die Anzahl der freien Leitungen.

Besetzte Leitungen: die Anzahl der besetzten Leitungen.

Aktivierte Features: die Anzahl der aktivierten Feature.

8.1.3 Installierte Sprachen

Der Menüeintrag **Installierte Sprachen** öffnet einen Info-Browser, der alle auf dieser Baugruppe installierten Sprachen und die jeweiligen Versions-Nummern, auflistet.

8.1.4 Mailbox Liste

Der Menüeintrag **Mailbox Liste...** öffnet einen Info-Browser, der eine Liste aller konfigurierten Mailboxen anzeigt.

8.1.5 Anmeldeinformationen

Über den Menüeintrag **Anmeldeinformationen...** kann ein Benutzer mit Administrator-Rechten die Einstellungen für das FTP-Login der entsprechenden IVM-Baugruppe ändern.

Der Eintrag öffnet ein Fenster mit den folgenden Elementen:

FTP Hostname: Hier wird der Hostname/IP-Adresse der IVM-Baugruppe angezeigt. Dieser Wert ist nicht schreibbar.

FTP Port: Hier wird der FTP-Port angezeigt. Da der FTP-Port 21 der Standard-Port für FTP ist, kann dieser Wert auch nicht von einem Benutzer mit Administrator-Rechten verändert werden.

Login Name: Hier wird der FTP-Login-Name des konfigurierten Benutzers eingegeben werden. Der Default-Login-Name ist „31994“.

Passwort: Das dazugehörige Passwort des konfigurierten Benutzers wird hier eingegeben. Das Default-Login-Passwort lautet „31994“.

XML Konfigurationsdatei: Hier wird der Dateiname der xml-Datei, die sich auf der IVM-Baugruppe befindet, eingegeben. Diese Datei beinhaltet die Konfigurationsinformationen der IVM-Baugruppe, diese werden vom OpenScape Business/H3K Plugin ausgelesen, z.B. „Mailbox Liste“. Die Default-xml-Datei heißt „ivm_sysd.xml“.

Als Globalen Standard Verwenden: Wenn diese Checkbox aktiviert ist, werden die eingegebenen Werte nach dem Betätigen der **OK**-Schaltfläche als Default für alle neu entdeckten IVM-Baugruppen und als Werte für die aktuell selektierte gesetzt. De Werte bereits existierender IVM-Baugruppen werden nicht verändert. Ist die Checkbox nicht aktiviert, werden die eingegebenen Werten nach dem Betätigen des Button **OK** nur für die aktuell selektierte IVM-Baugruppe gesetzt.

Die Schaltfläche **OK** schließt das Fenster und speichert die eingegebenen Werte je nach Status der Checkbox **Als Globalen Standard Verwenden** entweder als globalen Default oder nur für die aktuell selektierte IVM-Baugruppe. Die Schaltfläche **Abbrechen** schließt das Fenster ohne die Werte zu speichern. Die Schaltfläche **Auf Global Rücksetzen** trägt die zuletzt als globale Defaults definierten Werte in die entsprechenden Textfelder. Um diese Werte zu übernehmen muss der Button **OK** betätigt werden.

9 NAT in OpenScape FM

OpenScape FM unterstützt für bestimmte Objekte die Umsetzung von Netzwerkadressen (NAT; Network Address Translation). Wenn auf einem OpenScape FM-Objekt eine OpenScape Business/H3K Common Monitoring MIB erkannt wird, werden die entsprechenden NAT-Tabellen in das IP-Management von OpenScape FM integriert.

Derzeit unterstützt das OpenScape Business/H3K Gateway die Common Monitoring MIB und wird somit als NAT-Gerät in OpenScape FM erkannt.

Da der IP Manager generell für das Management der NAT-Adresszuordnungstabellen zuständig ist, finden sich einführende Erläuterungen zur Adressumsetzung mit OpenScape FM in der *IP Manager Plugin Bedienungsanleitung*.

9.1 NAT mit dem OpenScape Business/H3K Gateway

Die OpenScape Business/H3K Gateway-Komponente – ein Router – ist ein NAT-fähiges Gerät, d. h. sie kann interne in externe IP-Adressen umsetzen und umgekehrt. Zwischen ISDN und einem LAN arbeitet dieser Router mit einer unidirektionalen IP-Adresszuordnung. In den von der ISDN-Seite kommenden Paketen mit einem Ziel im LAN, d. h. mit einer internen Adresse, ändert das OpenScape Business/H3K Gateway nur die IP-Zieladresse (er setzt sie um). Wenn der Zielrechner im LAN über das ISDN-Gerät eine Antwort übermittelt, muss die Zieladresse in den IP-Paketen nicht geändert werden, da das Zielgerät eine eindeutige IP-Adresse hat.

Ähnlich sieht die Situation bei den Quelladressen aus. Wenn das ISDN-Gerät ein IP-Paket sendet, ist die Quelladresse eindeutig und muss nicht umgesetzt werden. In der anderen Richtung dagegen, wenn also der LAN-Rechner ein IP-Paket sendet, handelt es sich um eine interne Quelladresse, die der NAT-Router (OpenScape Business/H3K Gateway) ändert (umsetzt).

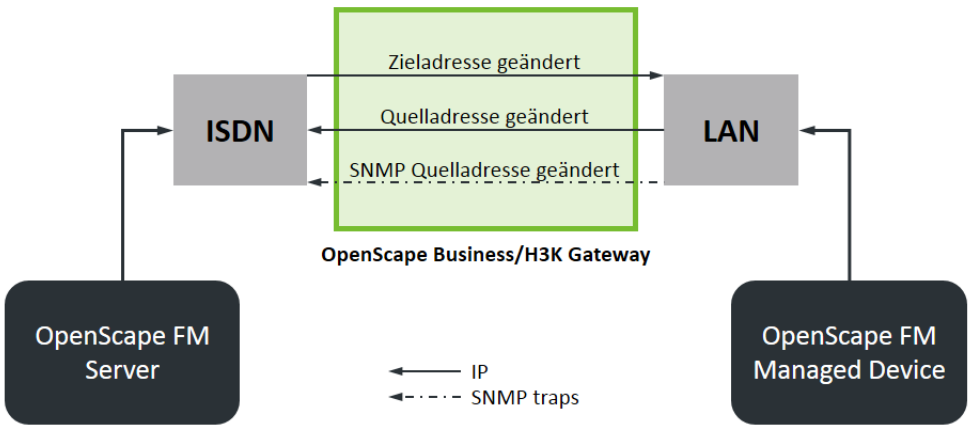

Bild 2 NAT-Routing mit dem OpenScape Business/H3K Gateway

Die NAT-Funktionalität des OpenScape Business/H3K Gateways wird als NAT-Objekt, also ein dem OpenScape Business/H3K Gateway untergeordnetes Objekt, verwaltet. Das Kontextmenü des NAT-Objekts enthält nur eine spezifische Position: **Regeln**.

Über den Menüeintrag **Regeln** öffnet sich eine Liste mit den Adresszuordnungen dieses NAT-Geräts. Es enthält die folgenden Spalten:

Extern: Die externe Adresse.

Intern: Die interne Adresse.

Netzmaske: Die Netzmaske.

Gültige Regel: OpenScape FM prüft, ob Unstimmigkeiten zwischen routbaren/externen IP-Adressen vorliegen. Wenn ja, ist die zugehörige Regel ungültig. Normalerweise wird der Wert bei korrekter Zuordnung von internen/externen IP-Adressen und eindeutigen externen IP-Adressen allerdings „gültig” lauten.

Der Status des NAT-Objekts ist von der Definition der NAT-Regeln abhängig. Die Bedeutung der Farben in Bezug auf den Status der Objekte wird in der *OpenScape FM Desktop-Bedienungsanleitung* behandelt:

NAT-Objektstatus	Beschreibung
Nicht verwaltet	Nicht verwaltet
Deaktiviert	Verwaltet, aber keine aktiven NAT-Regeln
Eingeschränkt	Verwaltet; NAT-Regeln werden nicht benutzt, weil NAT-Router im Bereich der zugeordneten IP-Adressen liegt
Warnung	Zeitüberschreitung beim Abruf von NAT-Regeln
Kritisch	NAT-Regeln sind fehlerhaft

Tabelle 2 Zustände der NAT-Objekte und Symbolfarben

10 VoIP-Überwachung (Voice over IP) in OpenScape FM

Wenn Sprachübertragung über das IP-Protokoll abgewickelt werden soll, hängt die Qualität der Fernsprechverbindungen über das LAN von der Qualität der darunterliegenden Protokollschichten ab. Wenn also Probleme mit den IP-Verbindungen zwischen den Geräten in Ihrem Netzwerk auftreten, ist auch die LAN-Telefonie davon betroffen.

Um festzustellen, ob bestimmte IP-Verbindungen störungsfrei, d. h. ohne Zeitüberschreitungen oder sonstige Probleme, zur Verfügung stehen, wird ein Tool benötigt, das die Verbindungsqualität regelmäßig überprüft.

Die OpenScape Business/H3K Common Monitoring MIB ist für die Überwachung von IP-Verbindungen ausgelegt. Wenn auf einem System ein SNMP-Agent installiert ist, der diese MIB unterstützt, kann das betreffende System die Verbindungen zu verschiedenen anderen IP-Geräten überprüfen.

OpenScape FM ist in der Lage, diese MIB auf einem von OpenScape FM überwachten Gerät zu erkennen. In diesem Fall zeigt OpenScape FM eine Bedienoberfläche an, in der festgelegt werden kann, welche Verbindungen auf der IP-Schicht überwacht werden sollen.

Derzeit ist diese MIB für OpenScape Business/H3K Gateway-Router implementiert.

10.1 VoIP im OpenScape Business/H3K Gateway

Die Voice over IP-Funktionalität eines OpenScape Business/H3K Gateways wird in Form eines Connection Monitoring-Objekts (ehemals VoIP) dargestellt, das dem zugehörigen IP-Knoten, also dem OpenScape Business/H3K Gateway, untergeordnet ist. Bei Anklicken des Connection Monitoring-Objektsymbols öffnet sich ein Kontextmenü mit dem Eintrag **Configure Connection Table** für „Administratoren” bzw. **View Connection Table** für „Operatoren”. Für „Anwender” wird kein VoIP-Eintrag angeboten.

Wie bei Konfiguration der Verbindungstabelle vorgegangen werden kann, wird im nachfolgenden Abschnitt erläutert.

10.1.1 Configure Connection Table

Der Eintrag **Configure Connection Table** öffnet eine Bedienoberfläche, auf der die zu überwachenden VoIP-Verbindungen eingerichtet werden können. Über diese Menüs können Verbindungen zwischen Netzwerkgeräten per „ping“ überwacht werden.

Auf der linken Seite sind in einer Tabelle alle aktuell überwachten Verbindungen aufgelistet.

Die rechte Seite besteht aus einem Konfigurationsfeld, in dem die IP-Adresse eines Zielgerätes eingegeben werden kann, um eine neue Verbindung zu überwachen.

Ist dies geschehen, führt das OpenScape Business/H3K Gateway eine „ping”-Operation auf dieses Gerät aus. Dabei werden die in den drei Feldern **Timeout**, **Retries**, und **Retry Time** konfigurierten Parameter berücksichtigt.

Im unten befindlichen Auswahlmenü kann der Modus für die Testdurchführung ausgewählt werden:

Der Test wird entweder als regelmäßige Ping-Operation unter Verwendung der definierten Parameter durchgeführt (**periodical Test**), er wird nur einmalig durchgeführt (**single test**), oder der Test wird für die ausgewählte Verbindung deaktiviert (**no test**).

Wenn eine bereits bestehende Verbindung geändert werden soll, muss die betreffende Verbindung in der Liste markiert werden. Die zugehörigen Parameter werden dann im Konfigurationsfeld auf der rechten Seite angezeigt. Nun können die neuen Parameter eingegeben und auf **Modify** geklickt werden, um die neuen Werte zu speichern. Die mit **autoTest** überwachten Verbindungen können in OpenScape FM nicht manuell konfiguriert werden. Sie müssen im OpenScape Business/H3K Gateway-System selbst definiert werden und werden durch das OpenScape FM lediglich zur Anzeige abgerufen. Parameter einer **autoTest**-Verbindung können nicht modifiziert werden.

Solange eine Verbindung störungsfrei hergestellt werden kann, werden auf der Bedienoberfläche von OpenScape FM keinerlei Informationen angezeigt. Sobald jedoch ein Problem auftritt, wird die Verbindung zwischen den beiden betroffenen IP-Geräten eingezeichnet und rot dargestellt, um auf den „kritischen" Zustand aufmerksam zu machen. Außerdem erhält das Connection-Monitoring-Symbol den Fehlerstatus „Hinweis", d. h. es erscheint hellblau.

Soll zum Beispiel überprüft werden, ob die Verbindung vom OpenScape Business/H3K Gateway zu dem LAN-Telefon mit der IP-Adresse 139.2.154.2 fehlerfrei zur Verfügung steht, muss die IP-Adresse, der Wert für die Zeitüberschreitung, die Anzahl der Wiederholungen und der Wert für den Wiederholungs-Timer eingegeben werden. Dann muss der Testmodus ausgewählt (im Beispiel: periodical Test) und „Add" angeklickt werden. Daraufhin erscheint in der Liste der überwachten Verbindungen eine neue Zeile. Gleichzeitig beginnt das OpenScape Business/H3K Gateway, wiederholt ein „ping"-Kommando an Gerät 139.2.154.2 zu senden. Tritt eine Zeitüberschreitung auf, zeigt er die Verbindung in der OpenScape FM-Topologie an.

10.2 Anzeige des QoS-Status in VoIP-Netzen

Die Dienstgüte (Quality of Service, QoS) in einem Sprachkommunikationsnetz wird durch viele Faktoren beeinflusst. Dabei handelt es sich beispielsweise um die Verfügbarkeit des Netzes, die Zuverlässigkeit (getrennte Verbindungen, falsche Nummer), Tonqualität (Lautstärke, Verzerrung, Rauschen) und Verzögerung von Ende zu Ende. In diesem Abschnitt bedeutet QoS in erster Linie die Qualität des Gesprächs selbst. Dementsprechend wird sie als Gesprächsqualität oder Sprachqualität (Voice Quality, VQ) bezeichnet.

Traditionelle vermittelte Telefonnetze sind optimiert für zeitkritische Anwendungen und liefern z.B. konstante Bandbreite, geringe Verzögerungen und Verzerrungen (Jitter). Dies gilt nicht für IP-Netze, die entwickelt wurden für Nicht-Echtzeit-Applikationen wie E-Mail oder Dateiübertragungen. Bei VoIP-Verbindungen wird die QoS hauptsächlich durch typische Probleme beeinträchtigt, die in einem IP-Netz auftreten können – beispielsweise Paketverlust oder Verzögerung.

Um vom Anwender akzeptiert zu werden, muss die QoS einer VoIP-Umgebung mit der Qualität eines traditionellen Telefonnetzes vergleichbar sein. Daher ist die Überwachung des QoS-Status eine besonders wichtige Aufgabe im Rahmen des Netzmanagements. OpenScape FM unterstützt die Anzeige des QoS-Status für OpenScape Business/H3K Gateway-basierte VoIP-Umgebungen.

10.2.1 Überwachung und Darstellung

*I*n einer OpenScape Business/H3K Gateway-basierten VoIP-Umgebung sind die VoIP-Clients (zum Zeitpunkt der Erstellung dieses Dokuments OptiPoint 400/600-Geräte) zuständig für die Messung der Gesprächsqualität. Bei jedem Anruf werden Parameter wie Jitter, Verzögerung und Paketverlust überprüft und eine Gewichtungsfunktion ermittelt die Gesamtqualität der Verbindung. Dieser Gesamtqualität wird ein Statuswert (**QoS-Status**) zugeordnet. Dabei handelt es sich um einen der folgenden Werte:

- *Normal*
- *Hinweis*
- *Minor*
- *Major*
- *Kritisch*

Bei Auslösen der Verbindung werden die von VoIP-Client aufgezeichneten QoS-Parameter an das OpenScape Business/H3K Gateway übergeben und in einer speziellen Tabelle (QoS-Tabelle) gespeichert. Diese Tabelle enthält die QoS-Parameter der letzten 200 Verbindungen aller VoIP-Clients des OpenScape Business/H3K Gateways.

OpenScape FM fragt die QoS-Tabelle via SNMP vom SNMP-Agent des OpenScape Business/H3K Gateways ab und zeigt alle Verbindungen an, die eine schlechte Gesamtqualität, d. h. einen anderen QoS-Status als „*Normal*“ aufweisen. Diese Anzeige erfolgt in zwei Schritten:

1. Zwischen den IP-Knotenobjekten, welche die betroffenen VoIP-Clients darstellen, wird eine Verbindungslinie gezogen (eine Verknüpfung hergestellt). Hat einer der an der Kommunikation beteiligten Partner kein IP-Telefon, wird diese Linie zwischen dem VoIP-Client und dem OpenScape Business/H3K Gateway gezogen, da der Anruf an ein externes Kommunikationsnetz weitergleitet wird.
2. Ein Symbol, welches das Gespräch mit dem Qualitätsproblem darstellt, wird unter dem OpenScape Business/H3K Gateway platziert. Die Zuordnung all dieser Symbole erfolgt innerhalb der Container-QoS. Dadurch können alle Gespräche mit schlechter Verbindung dem entsprechenden OpenScape Business/H3K Gateway zugeordnet werden.

Der Status der Verknüpfung und des Symbols werden gemäß des QoS-Status der Verbindung eingestellt. Wenn die QoS-Tabelle mehr als einen Eintrag für einen Anruf mit schlechter Verbindungsqualität zwischen demselben Paar von Kommunikationspartnern enthält, wird der Status der Verknüpfung/des Symbols auf Basis des QoS-Status des letzten Eintrags festgelegt.

Die Verknüpfungen und Symbole, die einen problematischen Anruf darstellen, werden nur für einen begrenzten Zeitraum angezeigt. Sie haben eine Verfallszeit, die in *Abschnitt 10.2.2, „Verfallszeit von Verknüpfungen“* beschrieben wird.

Die QoS-Tabelle wird immer dann analysiert, wenn das OpenScape FM eine Statusabfrage durchführt. Dies geschieht standardmäßig jede Stunde. Zusätzlich kann das OpenScape Business/H3K Gateway so konfiguriert werden, dass immer dann SNMP-Traps an das OpenScape FM gesendet werden, wenn ein neuer Eintrag mit einem anderen QoS-Status als „Normal“ in die QoS-Tabelle eingefügt wird

Hinweis:
Diese Konfiguration erfolgt automatisch, wenn das OpenScape FM sich selbst als Trap-Ziel in die rmon-MIB des SNMP-Agenten des OpenScape Business/H3K Gateways eintragen kann (siehe *IP Manager Plugin Bedienungsanleitung*).

Wenn das OpenScape FM einen derartigen QoS-Trap empfängt, aktualisiert das OpenScape FM die eigene Datenbank und zeigt problematische Gespräche sofort an.

Für jedes QoS-Trap, das OpenScape FM empfängt, wird ein Protokollereignis generiert und im Ereignis-Browser von OpenScape FM angezeigt. Der Protokolleintrag enthält folgende, aus dem Trap übernommene Werte:

- **Conference ID:** Die Konferenz-ID, die den betroffenen Anruf identifiziert.
- **Local IP Address:** Die IP-Adresse eines Kommunikationspartners (IP-Telefon-Client).
- **Remote IP Address:** Die IP-Adresse des zweiten Kommunikationspartners oder die IP-Adresse des OpenScape Business/H3K Gateways, wenn es sich hierbei nicht um ein IP-Telefon handelt.
- **Connection Quality:** Die Qualität der Verbindung.

Hinweis:
Wenn eines der IP-Knotenobjekte, das den Endpunkt einer Verknüpfung darstellt, in der OpenScape FM-Datenbank nicht existiert und dessen IP-Adresse sich in einem Subnetz befindet, das existiert und in OpenScape FM verwaltet wird, wird dieses automatisch erzeugt.

10.2.2 Verfallszeit von Verknüpfungen

Verknüpfungen und Symbole, die problematische Anrufe darstellen, werden für einen begrenzten Zeitraum angezeigt und automatisch entfernt, wenn in dem betreffenden Zeitraum keine weiteren Anrufe mit einem schlechten QoS-Status für dieselben Gesprächspartner ermittelt werden. Dieser Zeitraum, die so genannte Verfallszeit von Verknüpfungen, kann über das Hauptmenü von OpenScape Business/H3K konfiguriert werden. Der Hauptmenüeintrag **Technologien->OpenScape Business/H3K->Verbindungsverfallszeit** öffnet eine Bedienoberfläche, auf der die Verfallszeit eingestellt werden kann. Standardmäßig beträgt dieser Zeitraum einen Tag.

Änderungen der Verfallszeit betreffen nur Verknüpfungen/Symbole, die nach Eingabe der Änderung eingerichtet werden. Für vorhandene Verknüpfungen wird die Verfallszeit nicht aktualisiert. Wenn das OpenScape Business/H3K Gateway eine weitere Verbindung mit einem unbefriedigenden QoS-Status für eine in OpenScape FM bereits vorhandene Verknüpfung signalisiert, wird der Verfalls-Timer für diese Verknüpfung neu gestartet. Wenn zwei Gesprächspartner permanente Probleme mit der Qualität ihrer Verbindung haben, kann es daher vorkommen, dass eine Verknüpfung niemals verschwindet. Der Server speichert die Verfallszeit für jede Verknüpfung ab. Somit werden auch bei einem Neustart des Servers die fälligen Verknüpfungen ordnungsgemäß entfernt.

Verknüpfungen können auch manuell gelöscht werden. Wenn jedoch ein weiteres Qualitätsproblem für dieses Gesprächpartnerpaar gemeldet wird, wird die Verknüpfung wieder hergestellt.

11 OptiPoint 400/600-Geräte

Das OpenScape Business/H3K Gateway-Gerät kann so konfiguriert werden, dass es als Gatekeeper in einer IP-Telefonieumgebung fungiert. Eine derartige Umgebung enthält IP-Telefone (OptiPoint-Clients), die logisch zu einem bestimmten OpenScape Business/H3K Gateway gehören, d. h., das OpenScape Business/H3K Gateway-Gerät ist zuständig für den Verbindungsaufbau für diese IP-Telefone.

Das OpenScape FM entdeckt und zeigt die IP-Telefon-Clients eines OpenScape Business/H3K Gateway-Geräts an. Das OpenScape FM überwacht den aktuellen Status der Clients sowie die Dienstgüte (Quality of Service, QoS) der letzten Anrufe (detaillierte Erläuterungen hierzu enthält *Abschnitt 12.2, „Überwachung von Programmen“*).

Alle Informationen über die OptiPoint 400/600 Geräte werden über SNMP vom SNMP-Agenten des OpenScape Business/H3K Gateways gezogen. Für die Erkennung und die Anzeige des Status von OptiPoint-Clients verfügt dieser SNMP-Agent über eine *OptiPoint-Tabelle* (`ipPhoneTable`), die alle notwendigen Daten über die konfigurierten Clients enthält.

Hinweis:
Nicht jede Implementierung eines OpenScape Business/H3K Gateways unterstützt die “OptiPoint-table“.

11.1 Erkennungsprozess

Aus Sicht des OpenScape FM ist ein OptiPoint-Client in erster Linie ein IP-Knoten. Wenn dieser neu in die Datenbank des OpenScape FM eingefügt wird, besitzt das OpenScape FM nur die Information, dass es sich bei diesem IP-Knoten um einen OptiPoint-Client handelt. Es sind ihr aber keine weiteren Informationen bekannt, wie beispielsweise die Telefonnummer oder das zugehörige OpenScape Business/H3K Gateway. Zu diesem Zeitpunkt zeigt nur das Label des Symbols, dass es sich um einen OptiPoint-Client handelt. Es erfolgt eine allgemeine Statusüberwachung des Clients, wobei lediglich geprüft wird, ob das Gerät über das Netz erreichbar ist oder nicht. Diese Erreichbarkeitsprüfung wird standardmäßig alle 60 Minuten durchgeführt.

Um zu ermitteln, welche Clients zu einem bestimmten OpenScape Business/H3K Gateway gehören, liest das OpenScape FM die OptiPoint-Tabelle jedes OpenScape Business/H3K Gateway-Gerätes, das erkannt wird. Diese Tabelle wird vom SNMP-Agenten des OpenScape Business/H3K Gateways bereitgestellt und enthält unter anderem die IP-Adresse jedes OptiPoint-Gerätes, das zum OpenScape Business/H3K Gateway gehört. Nun kann das OpenScape FM erkennen, welche OptiPoint-Clients zu welchem OpenScape Business/H3K Gateway gehören und diese entsprechend darstellen (siehe *Abschnitt 11.2, „Darstellung und Statusüberwachung“*). Wenn der IP-Knoten, der einen OptiPoint-Client darstellt, noch nicht in der OpenScape FM-Datenbank enthalten ist, das zugehörige Subnetz jedoch existiert und verwaltet wird, wird der IP-Knoten automatisch eingefügt.

Es ist zu beachten, dass nur betriebsbereite OptiPoint-Clients erkannt werden. Betriebsbereit bedeutet hier, dass der Client seit dem letzten Neustart des OpenScape Business/H3K Gateways mindestens einmal eine Verbindung zum OpenScape Business/H3K Gateway hergestellt hat. Ist dies nicht der Fall, ist die IP-Adresse dem System nicht bekannt und der zugehörige IP-Knoten kann nicht ermittelt werden.

Sobald ein OptiPoint-Client durch das OpenScape FM erkannt worden ist, kann eine komplexere Statusüberwachung und Darstellung des Geräts erfolgen. Dies wird nachfolgend beschrieben.

11.2 Darstellung und Statusüberwachung

OptiPoint-Clients werden im OpenScape FM durch IP-Knotenobjekte dargestellt. Um anzuzeigen, dass es sich bei einem IP-Knoten um einen OptiPoint-Client handelt, verwendet das OpenScape FM ein spezielles Symbol (siehe *Kapitel 4, „Symbole“*) und platziert zusätzlich ein entsprechendes Objekt auf die Submap des IP-Knotens.

Der Status des OptiPoint-Objekts wird via SNMP aus der OptiPoint-Tabelle des OpenScape Business/H3K Gateways abgefragt. Das Objekt kann sich in einem der Zustände „*Normal*“, „*Hinweis*“, „*Minor*“, „*Major*“, „*Kritisch*“ oder „*Unbekannt*“ befinden. Das OptiPoint-Objekt erhält die dem Status entsprechende Farbe. Der Status eines OptiPoint-Objekts wird auf das übergeordnete Knoten-Objekt übertragen. Der IP-Knoten befindet sich immer im kritischsten Status, den eines seiner untergeordneten Objekte hat, solange der IP-Knoten selber erreichbar ist. Um die Komponente zu ermitteln, die für den jeweiligen Zustand des IP-Knotensymbols verantwortlich ist, kann die Submap des IP-Knotens oder der Status-Erklärungs-Browser (siehe *OpenScape FM Desktop Bedienungsanleitung*) geöffnet werden.

Wichtiger Hinweis:
Statusänderungen in der OptiPoint-Tabelle des OpenScape Business/H3K Gateways werden durch SNMP-Traps signalisiert und unverzüglich angezeigt. Statusänderungen der Netzwerkschnittstelle werden durch Abfrage erkannt und erscheinen möglicherweise mit einer Verzögerung von etwa 60 Minuten (standardmäßiger Abfragezyklus, vom Anwender konfigurierbar, siehe *IP Manager Plugin Bedienungsanleitung*).
Das OpenScape Business/H3K Gateway muss für die Übertragung von SNMP-Traps an das OpenScape FM konfiguriert sein. Diese Konfiguration erfolgt automatisch, falls das OpenScape FM sich selbst via SNMP als Trap-Ziel in der rmon-MIB eintragen kann (siehe *IP Manager Plugin Bedienungsanleitung*).

Um anzuzeigen, welche OptiPoint-Clients zu einem bestimmten OpenScape Business/H3K Gateway gehören, blendet die Submap des IP-Knotens das OpenScape Business/H3K Gateway als mit `OptiPoints` beschriftetes Objekt ein. Dieses Objekt enthält alle OptiPoint-Clients, die auf Basis der vom SNMP-Agenten des OpenScape Business/H3K Gateways übergebenen Informationen identifiziert wurden.

Änderungen in der OptiPoint-Tabelle können durch SNMP-Traps signalisiert werden, sofern das OpenScape FM als Trap-Ziel am OpenScape Business/H3K Gateway konfiguriert ist (siehe Hinweis weiter oben). Wenn das OpenScape FM einen derartigen Trap empfängt, verändert das Hinzufügen oder Entfernen von Clients die Anzeige im OpenScape FM nahezu unverzüglich. Es ist zu beachten, dass ein OptiPoint-Client betriebsbereit sein muss, um durch das OpenScape FM erkannt zu werden. Ein neu konfigurierter Client hat initial noch keine IP-Adresse in seinem Datensatz der OptiPoint-Tabelle und kann daher nicht durch das OpenScape FM identifiziert werden.

11.3 OptiPoint-bezogene Ereignisse

Wenn ein OpenScape Business/H3K Gateway das OpenScape FM über den Wechsel des Fehlerstatus eines OptiPoint-Clienten mittels SNMP-Trap in Kenntnis setzt, zeigt der Ereignis-Browser des OpenScape FM folgende Informationen an:

- Den Teilnehmernamen des IP-Telefons
- Die IP-Adresse des IP-Telefons
- Den aktuellen Fehlerstatus des IP-Telefons

Zusätzlich überwacht das OpenScape FM die Netzanbindung des IP-Telefons. Wenn das OpenScape FM das Telefon über das Netz nicht erreichen kann, wird für den betreffenden OptiPoint-Client ein Ereignis „IP-Knoten ausgefallen“ generiert. Das bedeutet nicht unbedingt, dass bei dem OptiPoint-Client selbst ein Problem aufgetreten ist. Die Verbindung zwischen OpenScape Business/H3K Gateway und OptiPoint kann weiterhin in Ordnung sein. Ein derartiges Ereignis bedeutet lediglich, dass OpenScape FM den OptiPoint-Client nicht erreichen konnte.

11.4 IP-Adressen-Änderung von OptiPoints

Im Falle einer IP-Adressen-Änderung eines OptiPoints aktualisiert das OpenScape Business/H3K Plugin die IP-Netzwerk-Topologie. IP-Adress-Änderungen werden entweder durch das OpenScape Business/H3K Gateway mittels eines SNMP-Traps signalisiert oder werden beim nächsten Konfigurations-Poll erkannt. Der Konfigurations-Poll liest die OptiPoint-Tabelle des OpenScape Business/H3K Gateways. Die Tabelle wird auch verwendet, um alle OptiPoints, die zu einem OpenScape Business/H3K Gateway gehören, zu erkennen und anzuzeigen. Die Tabelle enthält neben anderen Werten, die „Subscriber“-Nummer eines OptiPoints und seine aktuelle IP-Adresse. Beide Werte werden benutzt, um ein OptiPoint eindeutig zu identifizieren.

Falls eine IP-Adressen-Änderung erkannt worden ist, wird der IP-Knoten mit der alten IP-Adresse gelöscht und ein neuer wird erzeugt, dieser repräsentiert das OptiPoint mit der neuen IP-Adresse.

12 OpenScape Applikationsüberwachung

Mit Hilfe der Applikationsüberwachung kann der Status von auf dem Server laufenden Programmen bestimmt werden. Der SNMP-Agent des Servers muss dazu die Host-Ressourcen-MIB, wie beispielsweise Windows 2000-Systeme, unterstützen.

Wichtiger Hinweis:
Damit der OpenScape FM-Server Applikationen überwachen kann, muss das Plugin-Modul Hostresources initialisiert werden. Das Plugin kann über den Hauptmenüeintrag **Server->Plugins->Initialisiere Hostresources Plugin** initialisiert werden.

Programme können die beiden Zustände *laufend* oder *nicht laufend* aufweisen.

Um die Applikationsüberwachung zu aktivieren, muss das **Server**-Symbol und das **SNMP**-Symbol der nächsten Ebene jeweils mit einem Doppelklick geöffnet werden. Auf dieser Ebene befindet sich ein **MIB-II**-Symbol namens *Host-Ressourcen*.

Um die Überwachung zu starten, muss der Eintrag **Aktivieren/Deaktivieren** aus dem Kontextmenü dieses Symbols ausgewählt werden. Es erscheint ein neues Symbol *Applikationen* auf der übergeordneten Ebene. Dieses Symbol enthält die beiden Einträge Laufende Software und Installierte Software in seinem Kontextmenü, die in den folgenden Abschnitten beschrieben werden.

12.1 Installierte Software auf einem Server

Um die auf einem Server installierte Software anzuzeigen, muss aus dem Kontextmenü des Objekts **Applikationen** der Eintrag **Installierte Software** ausgewählt werden. Im anschließend angezeigten Fenster befindet sich eine fünfspaltige Aufstellung aller Applikationen, die in der Host-Ressourcen-MIB eingetragen sind. Es wird ein *Index*, der *Softwarename*, die *Softwarekennung*, der *Softwaretyp* und das *Installationsdatum* angezeigt.

12.2 Überwachung von Programmen

Um die Programme anzuzeigen, die auf Servern mit Unterstützung für die Host-Ressourcen-MIB laufen, muss aus dem Kontextmenü des Objekts *Applikationen* der Eintrag **Laufende Software** ausgewählt werden.

Anschließend erscheint eine achtspaltige Aufstellung, die verschiedene Parameter für jede Applikation enthält: einen *Index*, den *Softwarenamen*, die *Softwarekennung*, den *Pfad* der Binärdatei, *Ausführungsparameter*, den *Softwaretyp*, den *Status* [*laufend*|*nicht laufend*] und den *Überwachungsstatus* [*überwacht*|*nicht überwacht*].

Der *Überwachungsstatus* legt fest, ob ein Server-Prozess überwacht wird, oder nicht. Dieser kann für die jeweils selektierten Prozesse mit Hilfe des Auswahlmenüs **Überwachungsstatus** [*überwacht*|*nicht überwacht*] und der Schaltfläche **Speichern** gesetzt werden.

Die Schaltfläche **Aktualisieren** muss betätigt werden, um die Anzeige nach einer Anpassung auf den aktuellen Stand zu bringen.

Ein Server kann Statusinformationen zu einem überwachten Programm über Abfragen oder über Traps abrufen. Wenn ein überwachtes Programm anhält, ändert sich bei der folgenden Abfrage der Objektstatus und folglich auch die Farbe des zugehörigen Symbols. Um die Abfragefunktion nutzen zu können, ist also keine besondere Einrichtung erforderlich. Weitere Informationen zum Empfang von SNMP-Traps von Applikationen finden sich in *Abschnitt 12.2.1, „Empfangen von SNMP-Traps von Applikationen“*.

Um zu erfahren, auf welchen Hosts die Applikationsüberwachung aktiviert wurde, kann der Eintrag **SNMP->Host-Resources**–>**Applikations-Gruppen anzeigen...** aus dem Hauptmenü ausgewählt werden. Anschließend wird eine Liste mit den *Namen* und den *IP-Adressen* der Hosts angezeigt, auf denen die Applikationsüberwachung aktiviert ist. Diese Liste enthält auch Informationen zum aktuellen *Status*.

12.2.1 Empfangen von SNMP-Traps von Applikationen

Wenn eine Applikation Traps senden soll, muss das entsprechende System manuell eingerichtet werden.

Die Trap-Generierung auf einem System mit dem Betriebssystem Windows basiert auf Ereignissen, die an das Ereignisprotokoll von Windows gesendet werden. Es kann festgelegt werden, welche dieser Ereignisse einen SNMP-Trap nach sich ziehen sollen. Folglich kann dieser Mechanismus nur für Programme verwendet werden, die Einträge im Ereignisprotokoll von Windows generieren können. Zur Einrichtung der SNMP-Trap-Generierung müssen die folgenden Schritte durchgeführt werden:

- Prüfen, ob auf dem Server ein SNMP-Agent installiert ist. Auf Systemen mit Windows 2000 wird ein SNMP-Agent üblicherweise bereits mit dem Betriebssystem installiert.
- Der SNMP-Dienst muss laufen.
- Der SNMP-Trap-Dienst muss laufen.
- Über das Hilfsprogramm `evntwin.exe` können die Ereignisse definiert werden, die Traps für die zu überwachenden Applikationen generieren sollen. Es können nur Applikationen für das Senden von Traps eingerichtet werden, die diesen Mechanismus unterstützen.

13 Installation und Anforderungen

Eine detaillierte Beschreibung der Hardware- und Software-Anforderungen sowie des Installationsprozesses finden sich in der *OpenScape FM Desktop Bedienungsanleitung*.

A OpenScape Business/H3K-Rechte

Die Zugriffsrechte des Plugins sind in die allgemeine Rechte-Verwaltung eingegliedert (*siehe OpenScape FM Desktop Bedienungsanleitung*).

Die Beschreibung der einzelnen Rechte erfolgt in Form eines Tool-Tipps für das jeweils zugehörige Rechte-Symbol (Baum oder Submap).

Die Namen der Rechte des Plugins beginnen mit der Plugin-Kennzeichnung *OpenScape Business/H3K*.

Stichwörter

A
Agentenversion 29
Anzeige
    QoS-Status 36
Applikationsgruppe 44
Applikationsüberwachung 43

C
Client 7
Configure Connection Table 35
Control Center 19

D
Desktop 7
DNS 15

E
Einbauplätze 10, 21
Ereignis-Konfiguration 21
Ereignistyp 21

F
Features 22
Funktionen 22

G
Gatekeeper 39

H
H.323 26
H3K Gateway-Symbol 18
H3K Komponentensymbol 18
Hosts 21

I
Initialisierung 13
Installation 45
IP Knoten 21
IP Knotensymbol 17
IP Phone-Symbol 18
IVM
    Kontextmenü 31
    Menü Allgemeine Informationen 31
    Menü Anmeldeinformationen 32
    Menü Beschreibung 31
    Menü Installierte Sprachen 32
    Menü Mailbox Liste 32
    Spezifische Informationen 31
IVM-Baugruppe-Symbol 19

K
Knoten
    hinzufügen 14
Komponente 21
Kontextmenü
    IVM 31
    OpenScape Business/H3K Gateway 25

L
Leitungsstatus 15
Lizenzschlüssel 13

M
MAC Adresse 29
Managementdaten 10
Management-Informationsdatenbank 10
Management-Plattform 11
Menü
    Allgemeine Informationen 31
    Anmeldeinformationen 32
    Beschreibung 31
    Installierte Sprachen 32
    Mailbox Liste 32
MIB 10

N
NAT 33
    Netzwerktopologie 34
    Objektstatus 34
    Router 33
    Symbol 18
Netzverkverwaltung 11
Netzwerke 10, 14
Netzwerktopologie 10

O
OpenScape Business/H3K
    IP Knoten 21
    Komponente 21
    Netzwerke 10, 14
    Objekte 14
    Plugin 9, 13
    Rechte 47
    System-Informationen 21
    Übersichtsliste 22
OpenScape Business/H3K Gateway

Darstellung 37
Kontextmenü 25
Menü Events 25
Menü Fehlerhistorie 25
Menü Statistics 26
Menü Traps 25
Spezifische Informationen 25
Überwachung 37
VoIP 35
OpenScape Business Call Control Symbol 19
OpenScape Business Gateway-Symbol 19
OpenScape Business S Call Control Symbol 19
OpenScape Business S Gateway-Symbol 19
OpenScape Business S Symbol 19
OpenScape Business Symbol 19
OpenScape FM 7
Darstellung 40
Netzwerkadressen 33
OptiPoint-Client 39
Statusüberwachung 40
VoIP-Überwachung 35
OptiPoint
Ereignisse 40
IP Adressen ändern 41
OptiPoint-Container-Symbol 18
OptiPoint-Symbol 18

P

Plugin 13
Port-Nummer 22
Ports 10, 22, 23
Port-spezifische Informationen 23
Portstatus 15
Port-Symbol 23
Port-Typ 14

Q

Quality of Service 36

R

Routersymbol 18
RTCP 27
RTP 26

S

Server 7
Server-Komponente 11
SNMP 9
Discovery 15
Management 10
Traps 44
SNMP-Agenten 9
hinzufügen 15
Software Version 29
Spezifische Symbole 17
Statusinformationen 10, 15
Symbol
H3K Gateway 18
H3K Komponenten 18
IP Knoten 17
IP Phone 18
IVM-Baugruppe 19
NAT 18
OpenScape Business 19
OpenScape Business Call Control 19
OpenScape Business Gateway 19
OpenScape Business S 19
OpenScape Business S Call Control 19
OpenScape Business S Gateway 19
OptiPoint 18
OptiPoint-Container 18
Port 23
Router 18
Verbindung 19
Verbindungsüberwachung 18
Symbole 17
System
Knoten hinzufügen 14
System-Information 10, 21
Systemmanagement 10

T

Terminologie 7
TFA 27
Trap-Typen
Severity 26

U

Übersichten 19
Überwachung 43

V

Verbindungssymbol 19
Verbindungsüberwachungssymbol 18
Voice Quality 36

Z

Zeige Hosts 21

© 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.