A MITEL
PRODUCT
GUIDE

Unify OpenScape Fault Management

Unify OpenScape Fault Management V12, IP Manager Plugin

Bedienungsanleitung
10/2021

A31003-F30C0-U107-01-0019

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.

Inhalt

1 Vorwort

In diesem Kapitel werden folgende Aspekte behandelt:

- Zweck und Adressatenkreis dieses Handbuchs
- Terminologie
- Aufbau dieses Handbuchs
- In diesem Handbuch verwendete Konventionen

1.1 Zweck

In dem vorliegenden Anwenderhandbuch wird das IP Manager Plugin für das OpenScape FM beschrieben.

1.2 Adressatenkreis

Dieses Handbuch ist an die Benutzer gerichtet, welche die Bedienung des IP Manager Plugins erlernen möchten. Um mit dem IP Manager Plugin zu arbeiten ist es notwendig zu wissen, wie das OpenScape FM bedient wird. Mehr dazu findet sich in der OpenScape FM *Desktop Bedienungsanleitung*.

1.3 Aufbau dieses Handbuchs

Dieses Handbuch ist folgendermaßen aufgebaut:

- *Kapitel 1, „Vorwort“* zur Erläuterung der Gliederung dieses Handbuchs.
- *Kapitel 2, „Einleitung“* führt das IP Manager Plugin ein.
- *Kapitel 3, „Erste Schritte“* zeigt wie das Plugin installiert, initialisiert und lizenziert wird.
- *Kapitel 4, „Arbeiten mit dem IP Manager“* beschreibt die Benutzeroberfläche des Plugins.
- *Kapitel 5, „Symbole und Übersichten“* beschreibt die verwendeten Symbole.

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. Fettgedruckte Schrift wird außerdem für Schaltflächen, Menünamen und Menüeinträge verwendet.

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 Layer 2 Manager Bedienungsanleitung.*

Kursiv gedruckte Schrift dient auch der Betonung.

Beispiel: *Alle* Anwender sind davon betroffen.

1.5 Terminologie

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

2 Einleitung

Das IP Manager Plugin ist ein zentrales Plugin des OpenScape FM. Es bietet grundlegende Funktionen, wie beispielsweise das Discovery von IP-Netzwerken, Statusüberwachung von IP-Geräten und anderer Geräte. Der IP Manager dient beispielsweise zum Hinzufügen neuer IP-Komponenten zum System, denn es können nur Objekte verwaltet werden, die vom IP Manager registriert sind.

Zwar stellt der IP Manager ein separates Plugin für das OpenScape FM Desktop dar, er wird aber automatisch während der Installation des OpenScape FM initialisiert,

Nachdem der IP Manager initialisiert wurde, wird im Hauptmenü der Eintrag **IP Manager** hinzugefügt und das **Netzwerk Topologie** Symbol auf der Root-Submap erstellt.

Der IP Manager bildet die Grundlage für das Verwalten von IP-Netzwerken. Er dient dazu Netzwerke und IP-Knoten zum OpenScape FM Desktop hinzuzufügen.

2.1 Grundlagen des Netzwerk-Managements: Manager und Agenten

Ein Netzwerk-Management basiert auf Agenten und Manager-Systemen. Das geläufigste Protokoll beim Netzwerk-Management ist das SNMP (Simple Network Messaging Protocol). Ein SNMP-Agent liefert Statusinformationen über ein verwaltetes Objekt. Das Managementsystem ist verantwortlich für die Überwachung der Agenten-Systeme und Beschaffung von Informationen von den spezifischen MIBs der verschiedenen Agenten im Netzwerk.

Es gibt SNMP Agenten, die in speziellen Geräten integriert sind, und Proxy Agenten, die auf einem anderen Proxy Gerät laufen. Üblicherweise erhalten Proxy Agenten die Informationen über „ihr(e)“ Gerät(e) über eine nicht standardisierte oder eigene Schnittstelle. Ein Gerät kann eine Hardware-Netzwerk-Komponente sein, wie beispielsweise ein Router, Hub oder IP-Switch oder ein TK-Gerät.

3 Erste Schritte

3.1 Installation des IP Manager Plugins

Das IP Manager Plugin wird bei der Installation des OpenScape FM automatisch installiert.

3.2 Initialisierung des IP Manager Plugins

Das IP Manager Plugin wird bei der Installation des OpenScape FM automatisch initialisiert. Der Hauptmenüeintrag **IP Manager** wird ergänzt. In die Hierarchie wird ein Objekt eingefügt, das das IP Manager Plugin repräsentiert. Dieses hat den Pfad **Root->System->Plugins->IP Manager**.

3.3 Lizenzierung

Die Lizenzierung des IP Managers ist Teil der OpenScape FM Lizenz.

4 Arbeiten mit dem IP Manager

4.1 Grundlagen des IP Managers

Der IP Manager bildet die Grundlage für das Verwalten von IP-Netzwerken. Er dient dazu Netzwerke und IP-Knoten zum OpenScape FM Desktop hinzuzufügen.

*Hinweis: Ab der Version 10 wird an vielen Stellen in der Oberfläche der Begriff „**Host**“ synonym zum Begriff „**IP-noten**“ verwendet, insbesondere in der neuen Web-Oberfläche.*

Das OpenScape FM kann in IPv4- oder IPv6-Umgebungen eingesetzt werden. Der Einsatz in gemischten IPv4/IPv6-Umgebungen ist möglich, wenn das OpenScape FM selbst auf einem Dual-Stack-System läuft.

IPv4- und IPv6-Netzwerke werden separat erstellt und dargestellt. IP-Knoten, die Dual-Stack unterstützen und denen IPv4- und IPv6-Adressen zugewiesen sind, werden in allen entsprechenden Netzwerken dargestellt. Als Konsequenz erscheinen sie daher in mehr als einem Netzwerk.

Der IP Manager bietet zwei Methoden an mit denen IP-Adressen und IP-Knoten entdeckt werden können: Das „Auto-Discovery“ und das manuell zu startende „IP-Adressbereich-Discovery“. Beide Discovery Methoden werden auf der Grundlage von IP-Netzwerken aktiviert und gestartet. Gefundene IP-Knoten fügt der IP Manager anhand von spezifischen Discovery-Regeln zum OpenScape FM Desktop hinzu. Einige der Discovery-Regeln können vom Administrator über so genannte Discovery-Filter definiert werden, siehe auch *Abschnitt 4.2.2*. Die Standard-Regel ist, dass nur IP-Knoten hinzugefügt werden, auf denen entweder ein SNMP-Agent oder ein HTTP-Server läuft.

IP-Adressen können explizit zum OpenScape FM Desktop hinzugefügt werden. Dies kann über Eingabe einer bestimmten IP-Adresse über den **IP Manager->Neu->Netzknoten** Dialog oder eine Menge von IP-Adressen über eine „**Adressliste**“ erfolgen. Die letzten beiden Methoden erlauben es einem Netzwerk-Administrator die Netzwerk-Darstellung nur auf eine definierte Menge von IP-Systemen zu beschränken.

Der IP Manager benutzt spezielle IP-Container-Objekte für die Verwaltung von IP-Knoten. Ein IP-Container-Objekt befindet sich immer unterhalb des zugehörigen IP-Netzwerks. (Das IP-Netzwerk sollte nicht mit dem Topologie-Netzwerk, das für die Darstellung von Netzwerk-Hierarchien benutzt wird, verwechselt werden. Das IP-Netzwerk ist im Topologie Manager Kontext nur ein Knoten.) Die IP-Knoten, die für ein IP-Netzwerk entdeckt worden sind, werden in dem zugehörigen IP-Container-Objekt abgelegt. Ein IP-Knoten kann spezielle Kind-Objekte enthalten, wie beispielsweise Netzwerk-Interfaces, HTTP-Server oder SNMP-Agenten usw.

Der IP Manager bietet zusätzliche Informationen über den Status der verwalteten Objekte an. Dieser Status wird durch die Anzeige eines Objektes in einer Status-spezifischen Farbe realisiert, (weitere Informationen hierzu sind in der *OpenScape FM Desktop Bedienungsanleitung* zu finden). Ein Statuswechsel kann über Traps geschehen, die von dem zugehörigen Gerät verschickt werden. Ein Beispiel für solche Traps sind die Link UP/Down Traps.

IP-Knoten können für die Darstellung in Topologie-Netzwerken konfiguriert werden.

4.2 IP-Discovery

4.2.1 Allgemeines Prinzip des IP-Discovery

Der lokale IP-Knoten wird initial der Datenbasis hinzugefügt. Andere IP-Adressen und die dazugehörigen Systeme werden entdeckt, indem über ein Ping überprüft wird, ob sie über das Netzwerk erreichbar sind. Der Ping versucht eine Antwort von dem Systems mit der jeweiligen IP-Adresse zu erhalten. Wird dieser Verbindungsversuch innerhalb einer Timeout-Periode akzeptiert oder abgelehnt, wird davon ausgegangen, dass diese IP-Adresse „benutzt“ wird und ein System mit dieser IP-Adresse existiert. In diesem Fall wird der Discovery-Prozess mit dieser IP-Adresse fortgesetzt, andernfalls wird davon ausgegangen, dass diese IP-Adresse nicht „benutzt“ wird. Wenn ein „Ping“ erfolgreich ausgeführt worden ist, werden weitere Überprüfungen durch den Discovery-Prozess vorgenommen. Als nächstes werden die IP-Discovery-Regeln überprüft. Per Default wird überprüft, ob ein SNMP-Agent oder ein HTTP-Server auf diesem System läuft. Ist diese Bedingung erfüllt, geht das OpenScape FM Desktop davon aus, dass dieser IP-Knoten **existiert.** Für dieses System wird dann ein Knoten und ein entsprechendes Objekt in der OpenScape FM Datenbank erzeugt.

Wichtiger Hinweis:
Wird die Timeout-Periode überschritten, wird für die Antwortzeit der Messung ein Wert von `-1ms` in die History Daten bzw. `NoValue` in die Export Datenbank geschrieben und der Status auf *Critical* gesetzt.
Timeout-Ergebnisse werden nicht für die Berechnung von Durchschnittswerten berücksichtigt. Kann für einen Berechungszeitraum kein einziger gültiger Wert ermittelt werden, wird auch der Durchschnitt für den Zeitraum mit `-1ms` bzw. `NoValue` angezeigt.

Als Voreinstellung wird ein ICMP-Ping versucht. Alternativ kann auch ein TCP-Ping verwendet werden.

Für das Discovery von SNMP-Agenten wird die Community benutzt, die über den Dialog **IP Manager->Konfigurieren...** im Reiter **SNMP Parameter** konfiguriert worden ist. Es werden standardmäßig die Ports 161, 2161, 3161, 4161 und 5161 überprüft. Für jeden SNMP-Agenten, der erkannt wird, wird ein SNMP-Agenten-Objekt auf der Submap des zugehörigen IP-Knotens abgelegt. Jeder SNMP-Agent, der die MIB II unterstützt sollte eine sysObjectId unterstützten. Diese wird benutzt, um den Geräte-Typ zu ermitteln. Das entsprechende IP-Knoten-Objekt wird durch ein spezifisches Symbol, das abhängig vom Geräte-Typ ist, auf den verschiedenen Sichten (Navigationsbaum und Submaps) dargestellt.

Durch das Austesten der Ports 80, 280, 8888, 8080 und 8085, wird standardmäßig überprüft, ob spezifische Webserver existieren. Diese können auch über die „IP-Discovery-Filter“ konfiguriert werden. Einige Anwendungen werden durch das Abrufen spezifischer HTTP/XML Antworten des entsprechenden Webservers entdeckt.

Wenn für einen gefundenen IP-Knoten eine der über die „IP-Discovery-Filter“ definierten Bedingungen zutrifft, führen die Technologie-spezifischen Plugins den Discovery-Prozess fort. Diese Plugins entdecken ihre spezifischen Geräte, indem sie überprüfen ob Geräte-spezifische MIBs und HTTP-Server existieren und durch das Abfragen der gefundenen Komponenten nach spezifischen Geräte- und Technologie-Informationen. Wurden mehrere Plugins initialisiert, entdeckt jedes Plugin die zugehörigen Geräte. Über die entsprechenden MIBs erhalten sie Informationen über die Leistungsmerkmale der verwalteten Objekte.

Es ist zu beachten, dass ein SNMP-Agent verschiedene MIBs unterstützen kann, z.B. ein Windows 2000 Server kann Anfragen für MIB II, Host Resources MIBs und MIBs anderer Anwendungen beantworten.

Um Traps (Störungs-Ereignisse) zu erhalten, die durch einen Agenten gesendet worden sind, ist es wichtig dem OpenScape FM Server zu erlauben, sich als Trap-Empfänger auf dem Trap-sendenden SNMP-Agenten einzutragen. Standardmäßig versucht OpenScape FM sich auf jedem gefundenen IP-Knoten als Trap-Empfänger in der *trapDestTable* des RMON MIB Baums einzutragen. Kann diese Aktion nicht durchgeführt werden, muss der Trap-Empfänger manuell auf dem Agenten eingetragen werden.

Beispiel:

Wenn die IP-Adresse eines Windows Server 2012 hinzugefügt wird, erscheint sein Symbol in dem zugehörigen Netzwerk. Auf der Submap des Server-Symbols erscheint das Netzwerk-Interface und das SNMP-Symbol, welches den MIB II-Eintrag als Kind-Objekt enthält. Möglicherweise sind über diesen SNMP-Agenten weitere MIBs verfügbar, solange aber keine spezifischen Plugins im OpenScape FM Desktop initialisiert sind, werden diese nicht erkannt.

IP-Geräte, die das Routing (MIB II - IP forwarding = „on“) oder Switching unterstützen, werden sowohl im IP-Nodes-Container als auch eine Ebene höher, neben dem IP-Nodes-Container angezeigt.

4.2.2 IP-Discovery-Filter

Standardmäßig erzeugt der OpenScape FM Desktop für jedes System auf dem ein SNMP-Agent oder ein HTTP-Server läuft einen IP-Knoten. Zusätzlich wird vom OpenScape FM Desktop eine feinkörnigere Kontrolle bezüglich der Erzeugung von IP-Knoten angeboten. Die folgenden Bedingungen können benutzt werden um zu kontrollieren in welchen Fällen ein IP-Knoten erzeugt werden soll:

- Ein Verbindungversuch zu einer IP-Adresse war erfolgreich (Ping).
- Ein SNMP-Agent läuft auf einem spezifischen Port des IP-Knotens
- Eine spezifische sysObjectID wurde gefunden
- Ein spezifisches MIB-Objekt wurde gefunden
- Ein HTTP/HTTPS-Server läuft auf einem spezifischen Port des IP-Knotens.

Es gibt einige Bedingungen bei denen die Erzeugung eines IP-Knotens vom System erzwungen wird, unabhängig von den definierten IP-Discovery-Filtern. Nachfolgend werden einige Beispiele aufgelistet:

- Das System wurde manuell von einem Anwender eingegeben oder über eine Adressliste importiert.
- Ein HiPath/OpenScape 4000 System mit einer IP-Adresse wurde entdeckt.

Über die IP-Discovery-Filter können außerdem sowohl das Netzwerk als auch das Teilnetzwerk, in denen der IP-Knoten initial hinzugefügt werden soll, definiert werden.

Wie die IP-Discovery-Filter definiert werden, kann in *Abschnitt 4.4* nachgelesen werden.

4.2.3 Unterschied zwischen ARP-Cache-Discovery und IP-Adressbereich-Scan

Der Unterschied zwischen ARP-Cache-Discovery und IP-Adressbereich-Scan liegt im grundlegenden Mechanismus, der benutzt wird, um die zu analysierenden IP-Adressen zu ermitteln. Das ARP-Cache-Discovery basiert auf Informationen, die im ARP-Cache der IP-Knoten abgelegt sind. Üblicherweise wird der ARP-Cache verwendet, um die Zuordnungen von IP-Adressen und MAC-Adressen (Media Access Control Adresse) abzubilden. Der Inhalt des ARP-Caches wird von der MIB II eines vom OpenScape FM entdeckten SNMP-Agenten/IP-Knoten abgefragt, indem die `ipNetToMediaTable` der MIB-II ausgewertet wird. Im ARP-Cache-Discovery Prozess eines Netzwerks gehen nur IP-Knoten ein, deren IP-Adresse im ARP-Cache eines entdeckten IP-Knotens gefunden worden sind. Der Inhalt des ARP-Caches wird während des periodisch durchgeführten Konfigurations-Polls eines IP-Knotens überprüft.

Die auf das ARP-Cache basierende Discovery-Methode ist in den meisten Fällen ausreichend. In seltenen Fällen, in denen Systeme mit SNMP-Agenten nicht entdeckt werden konnten, oder einige IP-Systeme nur selten an der Netzwerk-Kommunikation teilnehmen, arbeitet dieser Mechanismus nicht effizient genug und es kann sehr lange dauern bis das ganze Netzwerk entdeckt wird. In diesen Fällen wäre eine direkte Analyse eines definierten IP-Adressbereichs eines Netzwerks über den „IP-Adressbereich-Scan“ die bessere Methode. Dieser Scan überprüft (per Ping) alle IP-Adressen innerhalb des definierten IP-Adressbereichs. Wenn eine IP-Adresse „benutzt“ wird, wird der Discovery-Prozess fortgeführt, andernfalls wird diese IP-Adresse verworfen. Da ein „IP-Adressbereich-Scan“ viel mehr Ressourcen benötigt als ein auf dem ARP-Cache basierendes Discovery, wird dieser nicht automatisch durchgeführt.

Wichtiger Hinweis:
Für IPv6-Netzwerke sollten Adressbereichs-Scans vermieden werden. Jede Adresse im angegebene Bereich wird überprüft. Im Gegensatz zu IPv4 wird hier sehr schnell eine sehr große Anzahl möglicher Adressen erreicht.

4.3 Hinzufügen eines neuen IP-Netzwerks

Um der OpenScape FM Datenbank ein IP-Netzwerk hinzuzufügen, kann der Eintrag **IP Manager->Neu->Netzwerk...** aus der Hauptmenüleiste ausgewählt werden. Dies öffnet das Konfigurationsfenster für IP-Netzwerke.

In dem Fenster müssen die **Netzwerk Adresse** und die **Netzwerk Maske** eingegeben werden. Die Festlegung eines **Netzwerk Name**ns ist optional. Dieser wird als Kennzeichen unter dem Netzwerksymbol angezeigt. Wird kein Name festgelegt, wird stattdessen die Adresse angezeigt.

Die Felder **Adressbereich scannen** und **Auto Discovery** bestimmen die Discovery-Methoden, die benutzt werden um IP-Adressen und zugehörige Knoten für dieses Netzwerk zu entdecken. Wird das Statusfeld **Adressbereich scannen** ausgewählt, öffnet sich beim Bestätigen ein zusätzlicher Dialog. Dieser Dialog ermöglicht die Definition eines zu scannenden IP-Adressbereichs. Jede einzelne IP-Adresse innerhalb des definierten Bereichs wird mit den in *Abschnitt 4.2.1* beschriebenen Methoden analysiert (nähere Erläuterung in *Abschnitt 4.6.3*).

Das Auswählen des **Auto Discovery** legt fest, ob IP-Adressen (zusätzlich) über das ARP-Cache-Discovery erkannt werden sollen und ob gefundene IP-Knoten zum neu definierten Netzwerk hinzugefügt werden sollen.

Mit dem Auto Discovery **Netzelemente erkennen und anlegen** wird das Netzwerk über das ARP-Cache-Discovery analysiert. Außerdem wird für jede gefundene IP-Adresse ein IP-Knoten-Objekt erzeugt.

Wird sowohl das Erkennen neuer Knoten und der IP Adressbereichs-Scan ausgewählt, so werden beide Methoden parallel ausgeführt, um existierende IP-Knoten dem Netzwerk hinzuzufügen. Beide Methoden werden ausführlicher in *Abschnitt 4.2.3* behandelt.

Hinweis:
Wird ein ARP-Cache-Discovery deaktiviert, so wird es nicht sofort gestoppt. Alle IP-Adressen, die bis zu diesem Moment bereits entdeckt worden sind, befinden sich in einer Warteschlange des Discovery-Prozesses und werden weiter analysiert. Es werden jedoch keine zusätzlichen IP-Adressen aus diesem Netzwerk in die Warteschlange eingereiht.

Beim Auto Discovery **Netzelemente erkennen aber nicht anlegen** wird das Netzwerk ebenfalls über das ARP-Cache-Discovery analysiert, es werden jedoch keine IP-Knoten unter dem Netzwerk-Container angelegt. Stattdessen können in diesem Fall die erkannten IP-Knoten über das Kontextmenü des Netzwerk-Containers über den Menüpunkt **Konfigurieren...** im Reiter **Erkannte IP-Adressen** in einer Tabelle eingesehen werden. Die Tabelle zeigt an, welche der definierten Discovery-Filter zu welchem Zeitpunkt auf den IP-Knoten gefunden wurden. Über die Funktion **Netzknoten hinzufügen...** kann dann für zuvor ausgewählte IP-Adressen ein IP-Knoten im Netzwerk-Container erzeugt werden.

Wird das Auto Discovery **Knoten nicht erkennen** ausgewählt, wird kein ARP-Cache-Discovery durchgeführt. Falls außerdem kein Adressbereichscan durchgeführt wird, müssen alle IP-Knoten, die in diesem Netzwerk angezeigt werden sollen entweder manuell (*Abschnitt 4.6.1*) oder durch die Benutzung einer Adressliste (*Abschnitt 4.6.2*) hinzugefügt werden.

Über das Statusfeld **Leeres Netz automatisch löschen** wird konfiguriert, ob der IP-Netzwerk-Container automatisch gelöscht werden soll, sobald der letzte IP-Knoten des Netzwerks gelöscht wird.

Durch das Betätigen der **Ok**-Schaltfläche wird der **Netzwerk hinzufügen** Dialog beendet. Ein neues, grau gefärbtes, IP Netzwerk-Symbol wird im Status ’verwaltet’ erstellt.

Hinweis:
Wenn nur IP-Knoten, die zu einem beschränkten IP-Adressbereich gehören, hinzugefügt werden sollen, sollte das Statusfeld **Adressbereich Scannen** und gleichzeitig das Auto Discovery **Knoten nicht erkennen** auswählen. Andernfalls füllt das Auto-Discovery das Netzwerk mit allen existierenden Systemen.

Hinweis:
Wenn das Auto Discovery **Netzelemente erkennen und anlegen** aktiviert ist, wird ein IP-Knoten nur zum Netzwerk hinzugefügt, wenn das System einen der konfigurierten IP-Discovery-Filter erfüllt (siehe *Abschnitt 4.2.2*). Um den Discovery-Prozess zu beschleunigen, sollte als erstes ein bekannter IP-Knoten manuell hinzugefügt werden. Dieser IP-Knoten sollte einen SNMP-Agenten mit MIB II unterstützen und intensiv im Netzwerk-Verkehr involviert sein.

Nach dem Hinzufügen eines Netzwerkes kann dessen Konfiguration modifiziert werden. Dies kann durch Auswahl des Punktes **Konfigurieren...** aus dem Kontextmenü des Netzwerkes geschehen. Der Reiter **Netzwerkparameter** enthält die aus der Erstellung bekannten Elemente.

Zusätzlich kann hier das Netzwerk mit dem Auto Discovery **Adressbereich ausblenden** ausgeblendet werden (siehe *Abschnitt 4.3.1*).

4.3.1 Adressbereiche ausblenden

Gelegentlich ist es erwünscht, dass bestimmte Netze oder Teilnetze aus der Überwachung ausgeblendet werden sollen. Knoten aus derartigen Netzen und ihre Ereignisse sollen ignoriert werden.

Dies kann im OpenScape FM mit zwei Methoden erreicht werden:

- Für ein dem OpenScape FM bereits bekanntes Netzwerk kann aus dem Kontextmenü der Eintrag **Konfigurieren...** und anschließend die Karteikarte **Netzwerkparameter** aufgerufen werden. Auf dieser Karte muss im Auswahlmenü **Auto Discovery** die Auswahl **Adressbereich ausblenden** eingestellt werden.

  Warnung:
  Alle Knoten, die für ausgeblendete Netzwerke bekannt sind, werden aus der Datenbasis entfernt. Soll ein entsprechender Bereich zu einem späteren Zeitpunkt wieder aktiviert werden, ist eine Neukonfiguration der gelöschten Knoten notwendig.

- Soll ein neues Netzwerk ausgeblendet werden, kann dieses über den Hauptmenüeintrag **IP Manager->Adressfilter->Adressbereich filtern** angelegt und wie gewohnt definiert werden.

In beiden Fällen wird das Netzwerk auf die Submap für ausgeblendete Adressbereiche (System->Plugins->IP Manager->Ausgeblendete Adressbreiche) verschoben und in den Status ‚*nicht verwaltet*' gesetzt. Für alle auf dieser Submap befindlichen Netzwerke werden keine neuen Knoten mehr erkannt, bereits zugewiesene Knoten werden gelöscht.

Die ausgeblendeten Adressbereiche können mit Hilfe des Hauptmenüeintrages **IP Manager->Adressfilter->Gefilterte Bereiche anzeigen...** angezeigt werden. Diese Funktion öffnet die Submap **System->Plugins->IP Manager->Ausgeblendete Adressbreiche**, auf der sich Symbole für alle ausgeblendeten Adressbereiche befinden.

Um einen ausgeblendeten Bereich wieder einzublenden, kann der Eintrag **Konfigurieren...** aus dem Kontextmenü des entsprechenden Adressbreich-Symbols ausgewählt werden. Anschließend muss auf der Karteikarte **Netzwerkparameter** lediglich ein anderes **Auto Discovery** als **Adressbereich ausblenden** eingestellt werden. Das betroffene Netzwerk wird dadurch auf ‚*verwaltet*' gesetzt und an seine normale Position innerhalb des Navigationsbaumes verschoben.

4.4 Konfiguration von IP-Discovery-Filtern

IP-Discovery-Filter legen fest, unter welchen Bedingungen neue IP-Knoten erkannt werden, und in welches Netzwerk/Teilnetzwerk sie standardmäßig eingetragen werden sollen. Dies ermöglicht es z.B. alle Objekte eines Typs unter einem Netzwerk-Container zusammenzufassen.

Die Konfiguration der Discovery-Filter wird über den Menüpunkt **Discovery Filter...** im Hauptmenü **IP Manager** gestartet. Dieser öffnet das Konfigurationsfenster, und ist nur für Anwender mit Administrator-Rechten sichtbar.

Das Fenster zeigt auf der linken Seite alle Bedingungen (Spalte **Discovery**) an, die aktiviert werden können, wenn eine IP-Adresse vom Discovery-Mechanismus abgearbeitet wird. Die Liste der Bedingungen setzt sich aus allen Enterprise spezifischen MIBs, sysObjectIDs und HTTP-Ports zusammen, die dem OpenScape FM Desktop bekannt sind.

Übergeordnete Bedingungen werden linksbündig angezeigt, jeweils spezifischere Bedingungen eingerückt unter der entsprechenden übergeordneten Bedingung.

Wenn IP-Knoten, die eine Bedingung erfüllen, erzeugt werden sollen, muss das zugehörige Auswahlfeld in der Spalte **IP-Knoten erzeugen** gesetzt werden, um die Bedingung zu aktivieren. Wird eine übergeordnete Bedingung aktiviert, werden alle untergeordneten Bedingungen ebenfalls aktiviert und gesperrt. Alle anderen Optionen („Standard Netzwerk“, “Standard Teilnetzwerk“, “Priorität“) bleiben weiterhin änderbar. Wenn das Auswahlfeld **IP-Knoten erzeugen** für die allgemeine Bedingung deaktiviert wird, werden die Auswahlfelder für die spezifischeren Bedingungen wieder entsperrt.

Die Spalte **Standard Netzwerk** gibt an, in welches Netzwerk in der Hierarchie des OpenScape FM der IP-Knoten initial hinzugefügt werden soll. Das entsprechende Teilnetzwerk wird in der Spalte **Standard Teilnetzwerk** angezeigt. Die Spalte **Netzpriorität** gibt an welche Priorität die Netzwerk/Teilnetzwerk-Zuweisung hat.

Die Spalte **Host-Type** markiert einen Host (IP-Knoten) mit dem dort eingetragenen Label. Dieser Label dient zur Markierung und Einordnung der Hosts.. Die Hosts können pro Typ aufgelistet werden über den Menüpunkt **IP Manager->Host Typen** oder in der Web-Oberfläche unter **Kategorien->Host Typen**.

In der Spalte **Aktiv** kann der Haken entfernt werden, um die Konfiguration des entsprechenden Eintrages zu deaktivieren.

Die höchste für ein Objekt zutreffende Netzpriorität legt fest, wo es angeordnet wird. Ist zu einem späteren Zeitpunkt eine Konfiguration mit höherer Priorität zutreffend, erfolgt eine neue Einsortierung des Objektes.

Wenn beispielsweise eine Konfiguration existiert, in der die Netzpriorität der MIB II Konfiguration „30“ beträgt und die von Hostresources „50“, so wird ein IP-Knoten der die MIB II *und* die Hostresources MIB unterstützt in das Netzwerk/Teilnetzwerk abgelegt, welches für Hostresources definiert worden ist.

Über den Eintrag **Eigenschaften** aus dem Kontextmenü eines IP-Knoten-Objektes öffnet sich ein Fenster auf dessen Seite **Topologie->Konfiguration** eine Position innerhalb der Netzwerk-Topologie manuell festgelegt werden kann. Diese zusätzliche Konfiguration besitzt die Netzpriorität `100`.

Auf dieser Seite kann zusätzlich für das einzelne Objekt eine Neuberechnung der Netzwerk-Topologie angestoßen werden, indem der Haken vor **Netzpriorität zurücksetzen** gesetzt wird. Wird die Seite nun gespeichert (**OK** oder **Übernehmen**) so setzt dies die Netzpriorität des Objektes auf 0. Der Haken ist nur aktiv, wenn dem Objekt aktuell eine Priorität größer `0` zugeordnet ist.

Hinweis:
In der MIB-II oder an anderer Stelle könnte eine sysLocation definiert sein. Diese sysLocation besitzt eine Priorität von ’40’. Um eine sysLocation zu überschreiben, muss daher eine Priorität größer als ’40’ gewählt werden.

Um die Bedingungen zu ändern, müssen die entsprechenden Zeilen selektiert und die Dialog-Komponenten auf der rechten Seite verwendet werden.

4.5 Verwaltete und nicht Verwaltete IP-Netzwerke

IP-Netzwerke können entweder explizit durch eine Anwender-Aktion oder implizit durch ein Discovery (ARP-Cache-Discovery oder IP-Adressbereich-Scan) hinzugefügt werden.

Ein IP-Netzwerk das explizit über den **Netzwerk hinzufügen** Dialog (siehe *Abschnitt 4.3*) hinzugefügt worden ist, hat den Status *Verwaltet*. Wenn ein bestimmtes Netzwerk nicht mehr verwaltet werden soll, muss sein Status von Hand auf *Nicht verwaltet* gesetzt werden. Dies erfolgt über seinen Menüpunkt **Bearbeiten->Nicht verwalten**. Wird der Status eines Netzwerkes auf *Nicht verwaltet* gesetzt, werden alle in diesem enthaltenen IP-Knoten ebenfalls auf *Nicht verwaltet* gesetzt.

Der Menüpunkt **Bearbeiten->Verwalten** setzt das Netzwerk und alle in ihm enthaltenen IP-Knoten in den Status *Verwaltet*.

Ein IP-Netzwerk kann implizit durch einen automatischen Discovery-Prozess erzeugt werden. Dies ist dann der Fall, wenn es IP-Knoten gibt, die ein Interface zu diesem Netzwerk besitzen und die bereits in einem existierenden Netzwerk mit eingeschaltetem ARP-Cache Discovery enthalten sind. Wenn ein Netzwerk implizit hinzugefügt worden ist, hat es den Status „nicht verwaltet“. Es enthält außerdem keine IP-Knoten, die ausschließlich in diesem Netzwerk enthalten sind.

Hinweis:
Es können keine neuen IP-Knoten zu „nicht verwalteten“ IP-Netzwerken hinzugefügt werden.

4.6 Hinzufügen von IP-Knoten

4.6.1 Hinzufügen eines IP-Knotens

Nachdem ein IP-Netzwerk hinzugefügt worden ist, kann mit der Konfiguration des Netzwerkes fortgefahren werden.

Um einem Netzwerk manuell einen Knoten hinzuzufügen, kann der Eintrag **Neu->Netzknoten...** aus dem Hauptmenü **IP Manager** aktiviert werden. In dem sich öffnenden Fenster kann die IP-Adresse eines neuen Knotens eingegeben werden. Wurde der DNS-Server oder eine Host-Datei eingerichtet, kann auch ein Host-Name eingegeben werden.

Wird eine IP-Adresse eingegeben, versucht das OpenScape FM einen passenden Host-Namen zu ermitteln. Ist dies erfolgreich, wird dieser Name im Bezeichner des neuen IP-Knotens angezeigt.

Ein Knoten für ein spezifisches Netzwerk kann über den Menüeintrag **Neu->Netzknoten** aus dem Kontextmenü des entsprechenden Netzwerk-Symbols hinzugefügt werden.

Wurde für das Netzwerk, zu dem dieser Knoten gehört, das Auto Discovery **Netzelemente erkennen aber nicht anlegen** ausgewählt, wird der Discovery-Prozess wie in *Abschnitt 4.2, „IP-Discovery“* beschrieben ausgeführt.

Im Gegensatz zu den automatischen Discovery-Prozessen wird für ein IP-Knoten, der durch eine explizite Anwender-Aktion hinzugefügt worden ist, ein entsprechendes Objekt erstellt, sobald ein zugehöriges IP-Netzwerk existiert. Es wird nicht überprüft, ob es diesen IP-Knoten tatsächlich gibt und ob dieses System einen der Discovery-Filter erfüllt.

Falls das zugehörige Netzwerk noch nicht hinzugefügt worden ist und der IP-Knoten eine lesbare MIB-II anbietet, werden der IP-Knoten und das zugehörige IP-Netzwerk zur OpenScape FM Datenbank hinzugefügt. Ist für diese IP-Adresse keine MIB-II zugänglich und wurde für den Knoten keine Netzmaske angegeben, kann der IP Manager das zugehörige Netzwerk nicht bestimmen, und der Knoten wird im Netzwerk *Default* angelegt.

Wird zu einem späteren Zeitpunkt ein passendes Netzwerk eingerichtet, wird der Knoten bei seinem nächsten Discovery automatisch in dieses verschoben.

4.6.2 Adressliste (Seed File)

Eine komfortable Lösung zum Hinzufügen einer bestimmten Menge von IP-Adressen/IP-Knoten, ist die Benutzung einer Adressliste. Eine Adressliste ist eine einfache Text-Datei im ASCII-Format (Seed File). Sie enthält eine Menge von IP-Adressen. Jeder IP-Adressen-Eintrag muss in einer separaten Zeile angegeben werden. Dies können entweder IP-Adressen in Punkt-Notation oder ein Hostname mit der kompletten Domain-Adresse (FQDN) sein.

Beispiele:

```
#Netzwerk Konfiguration
139.2.48.0:255.255.240.0:my_net

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

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

Eine Adressliste wird über den Menüpunkt **IP Manager->Konfiguration laden...** eingespielt. Durch das Öffnen des „Adressliste laden“-Browser kann durch den Datei-Manager auf die gleiche Weise wie in anderen gängigen Dateiverwaltungsanwendungen (z. B. WinNT/Win2000 Explorer) eine Adressliste auswählen. Durch das Betätigen der Schaltfläche **Öffnen** wird die ausgewählte Datei geladen. Der IP Manager fügt die (neuen) IP-Knoten umgehend hinzu und zeigt sie in den entsprechenden Ansichten an. Das Hinzufügen von IP-Adressen (Knoten) erfolgt nach den Selben Regeln wie in *Abschnitt 4.6.1, „Hinzufügen eines IP-Knotens“* beschrieben.

Jedem IP-Knoten können in der Adressliste weitere Eigenschaften zugewiesen. Diese werden jeweils durch ein Komma separiert. Insgesamt können einem Knoten die folgenden 5 Eigenschaften in genau dieser Reihenfolge zugewiesen werden.

- **IP-Adresse** oder **Hostname**
  Definiert den Host, der dem OpenScape FM hinzugefügt werden soll.
- **Netzwerk** (optional), **Teilnetzwerk** (optional) und **Netzpriorität** (optional)
  Diese drei Angaben definieren, wie das neue Objekt in die Netzwerk-Topologie eingegliedert werden soll. Sie entsprechen den Feldern **Standard Netzwerk**, **Standard Teilnetzwerk** und **Netzpriorität** für die Definition von Discovery-Filtern (siehe *Abschnitt 4.4*), gelten jedoch nur für das jeweilige Objekt.

- **Objekt-Kommentar** (optional)
  Definiert einen Objektkommentar-String (siehe *Desktop Bedienungsanleitung*), der dem neuen Objekt hinzugefügt wird. Er wird z.B. als Tooltipp für die Objektsymbole angezeigt.
  Zeilenumbrüche bzw. Tabulatoreinschübe können durch die Zeichenfolge `\\n` bzw. `\\t` eingebunden werden.

Sollen einzelne Eigenschaften nicht berücksichtigt werden, müssen lediglich die entsprechenden Kommata gesetzt werden.

Beispiele:

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

Fügt ein Objekt mit der IP-Adresse `139.2.57.2` hinzu und richtet es im Netzwerk-Container `myNetwork` und dessen Unter-Container `mySubNetwork` mit der Netzwerkpriorität `10` ein (falls für das Objekt keine Discovery Regel mit einer höheren Priorität zutrifft). Das Objekt selbst erhält den Tooltipp `Main Server`.

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

Fügt ein Objekt mit der IP-Adresse `139.2.57.3` an einer automatisch ermittelten Netzwerk-Position hinzu und versieht es mit dem Tooltipp `Backup Server`.

4.6.3 IP-Adressbereich-Scan

Wenn ein neues Netzwerk hinzugefügt worden ist, besteht die Möglichkeit das Statusfeld **Adressbereich Scannen** auszuwählen. Nach dem Betätigen der Schaltfläche **OK**, öffnet sich dann ein neues Fenster, in dem der zu scannende Adressbereich eingeben wird. Die **OK**-Schaltfläche in diesem Fenster öffnet einen Info-Browser, in dem der Status des IP-Adressbereich-Scans angezeigt wird. Für jede angefragte IP-Adresse zeigt das Ergebnis, ob eine Rückmeldung von diesem System kam und ob ein IP-Knoten für diese IP-Adresse erzeugt wurde.

Ein IP-Knoten wird nur erzeugt, wenn für das System mit der entsprechenden IP-Adresse einer der konfigurierten IP-Discovery-Filter zutrifft. Das Betätigen der **Stopp**-Schaltfläche beendet den Scan. Das Betätigen der **Abbrechen**-Schaltfläche schließt das Fenster und beendet ebenfalls den Scan.

Um einen IP-Adressbereich für ein bereits existierendes IP-Netzwerk zu starten, kann das IP-Netzwerk selektiert und der Kontextmenü-Eintrag **Adressbereich scannen...** ausgewählt werden. Anschließend öffnet sich der gleiche oben beschriebenen Dialog.

Wichtiger Hinweis:
Für IPv6-Netzwerke sollten Adressbereichs-Scans vermieden werden. Jede Adresse im angegebene Bereich wird überprüft. Im Gegensatz zu IPv4 wird hier sehr schnell eine sehr große Anzahl möglicher Adressen erreicht.

4.7 Löschen eines IP-Knotens

Bei der Arbeit mit einem großen Netzwerk mit vielen IP-Knoten werden möglicherweise IP-Knoten erkannt, die nicht vom OpenScape FM überwacht werden sollen. Diese Knoten können einfach entfernt werden, indem im Kontextmenü eines Symbol, das den Knoten repräsentiert, der Eintrag **Bearbeiten->Objekt Löschen** ausgewählt wird. Nach einer Bestätigung des Löschwunsches wird der IP-Knoten entfernt.

Wenn das ARP-Cache-Discovery für das Netzwerk eingeschaltet ist, wird dieser IP-Knoten jedoch bei der nächsten Abfrage wieder erkannt. Damit bestimmte Knoten nicht ständig von Neuem gelöscht werden müssen, kann für jedes Netzwerk das „Discovery-Verhalten“ konfiguriert werden (siehe *Abschnitt 4.3, „Hinzufügen eines neuen IP-Netzwerks“*).

4.8 Ermittlung des IP-Knoten-Status

So lange ein IP-Knoten erreichbar ist wird sein Status in der Regel über das kritischste Kind-Objekt ermittelt (siehe *Abschnitt 4.2.1*). Um die Komponente zu ermitteln, die für den jeweiligen Zustand des IP-Knotensymbols verantwortlich ist, kann die Submap des IP-Knotens geöffnet werden.

Falls ein IP-Knoten als nicht erreichbar erkannt wird, wird ein kritisches Ereignis für diesen Knoten erzeugt, welches dessen Status auf „*kritisch*“ setzt. Der Erreichbarkeitsstatus des Knotens wird ebenfalls auf „*kritisch*“ gesetzt. Der Status seiner Kind-Objekte, deren Status nur bei Erreichbarkeit des IP-Knotens ermittelt werden kann, werden auf „*unbekannt*“ gesetzt. Dies sind z.B. SNMP-Agenten, IP-Interfaces oder HTTP-Server. Die Status seiner Kind-Objekte, deren Status durch die Daten anderer Systeme berechnet und gesetzt werden, werden nicht verändert.

Ist ein IP-Knoten wieder erreichbar, wird das entsprechende Ereignis bestätigt und der Erreichbarkeitsstatus des IP-Knotens wird auf „*normal*“ gesetzt.

4.9 Behandlung von IP-Adressen-Änderungen

Häufig werden IP-Adressen dynamisch zugewiesen (gewöhnlich beim Start des Gerätes). Daher ist es nicht möglich ein Gerät eindeutig anhand seiner IP-Adresse zu identifizieren bzw. zu erkennen. Trotzdem sollten zuvor ermittelte Daten nicht verloren gehen, wenn für ein Objekt eine IP-Adress-Änderung vorkommt.

Um derartige Datenverluste zu vermeiden, werden im OpenScape FM zwei Mechanismen verwendet, um bereits bekannte Systeme zu erkennen.

Da die MAC-Adresse (Media Access Control) eindeutig ist und sich normalerweise während des Lebens-Zyklus einer Netzwerkkarte nicht ändert, wird die MAC-Adresse benutzt, um IP-Adressen-Änderungen zu entdecken. Ist die MAC-Adresse einer neu erkannten IP-Adresse dem OpenScape FM bereits bekannt, so wird davon ausgegangen, dass dem der MAC-Adresse zugehörigen Interface eine neue IP-Adresse zugeteilt wurde.

MAC-Adressen oder physikalische Adressen werden benutzt, um einen Netzwerk-Knoten auf der physikalischen Ebene des Kommunikations-Protokolls zu identifizieren. Da dieses die niedrigste Ebene des Protokoll-Stapels ist, werden MAC-Adressen üblicherweise einem Netzwerk-Adapter zugewiesen. Die MAC-Adresse eines Netzwerk-Adapters eines einzelnen IP-Knotens kann über die MIB II ausgelesen werden:
`.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable`.

Für jedes Interface enthält diese Tabelle den Eintrag `ifPhysAddress`, welcher die MAC-Adresse des Interfaces enthält. Wenn ein IP-Knoten mehr als ein Interface hat (das Loopback-Gerät wird ignoriert), werden alle MAC-Adressen verwendet um den IP-Knoten zu identifizieren.

Wenn ein IP-Knoten über den ARP-Cache Discovery-Prozess zum OpenScape FM hinzugefügt worden ist (siehe *Abschnitt 4.2.3*), ist die MAC-Adresse bereits über den ARP-Cache-Eintrag bekannt geworden, mit dem der IP-Knoten entdeckt worden ist.

Wenn das ARP-Cache-Scan-Discovery einen IP-Knoten entdeckt, der bereits bekannt ist (über die MAC-Adresse), der aber eine andere IP-Adresse hat, kann angenommen werden, dass sich die IP-Adresse geändert hat. Daher wird überprüft, ob die alte IP-Adresse immer noch erreichbar ist. Wenn dem so ist, wird ein neues Objekt für die neue IP-Adresse erzeugt. Wenn nur die neue IP-Adresse erreichbar ist, werden die folgenden Schritte durchgeführt:

- Das Auto-Discovery ändert die IP-Adresse des alten IP-Knotens auf die neue IP-Adresse.
- Alle Ereignisse im Ereignis-Browser, die zu der alten IP gehören, werden entsprechend der neuen IP-Adresse aktualisiert.

Wichtige Information:
Falls ein IP-Knoten manuell (*Abschnitt 4.6*) oder über einen IP-Adressbereich-Scan Discovery (*Abschnitt 4.6.3*) hinzugefügt worden ist, können die MAC-Adressen nur über einen MIB II-Agenten herausgefunden werden. Wenn dies nicht der Fall ist, findet der oben beschriebenen Mechanismus bei diesen einzelnen Systemen keine Anwendung, d.h. es kann nicht erkannt werden, dass eine IP-Adressen-Änderung stattgefunden hat.

Die Mapping-Informationen für einzelne IP-Knoten können über den Menüeintrag **Eigenschaften...** aus dem Kontextmenü des jeweiligen IP-Knoten aufgelistet werden. Die Information befindet sich auf der Seite **Topologie->Knoten ID Konfiguration**.

4.9.1 IP-Knoten Verfallszeit

In einer Umgebung, in der MAC-Adressen nicht zuverlässig bestimmt werden können, können doppelte IP-Knoten (selbes Gerät mit verschiedenen IP-Adressen) durch Verfallszeiten vermieden werden. Das bedeutet, dass IP-Knoten die innerhalb einer vorgegebenen Zeitspanne nicht laufen, standardmäßig aus der OpenScape FM Datenbank gelöscht werden. Genaugenommen ist die Verfallszeit an das Interface gebunden, über das der IP-Knoten im OpenScape FM entdeckt worden ist. Wenn keine Verbindung zu diesem Interface zustande kommt, erfolgt eine konfigurierte Aktion auf das IP-Knoten-Objekt.

Standardmäßig beträgt die Verfallszeit eine Woche und das zugehörige IP-Knoten-Objekt wird gelöscht, sobald die Verfallszeit abgelaufen ist. Ein Anwender mit Administrator-Rechten kann die Verfallszeit konfigurieren und entscheiden, ob der IP-Knoten gelöscht, oder nicht verwaltet werden soll oder ob keine Aktion auf diesem IP-Knoten ausgeführt werden soll. Diese Werte werden über die IP Parameter Dialoge konfiguriert (*Abschnitt 4.10*).

Alle Teilkomponenten eines IP-Knotens (z.B. HTTP-Server, SNMP-Agenten usw.) werden ebenfalls als Objekte angesehen, die ungültig werden können. Für die Teilkomponente wird die Konfiguration (Verfallszeit und auszuführende Aktion) benutzt, die für den zugehörigen IP-Knoten definiert worden ist. Aus diesem Grund können Teilkomponenten, die für den Zeitraum der Verfallszeit nicht erreichbar sind, automatisch gelöscht oder auf „nicht verwaltet“ gesetzt werden. Standardmäßig wird, wenn beispielsweise ein HTTP-Server eines IP-Knotens deinstalliert wird, das HTTP-Objekt automatisch von der Sicht des IP-Knotens gelöscht, sobald die Verfallszeit verstrichen ist.

Die Verfallszeiten werden während des Status-Polls eines IP-Knotens überprüft (*Abschnitt 4.10*).

4.10 Konfiguration der IP Parameter

Der IP Manager führt regelmäßig drei verschiedene Arten automatischer IP-Pollings durch. Diese Abfragen werden automatisch wiederholt:

1. **Status-Poll:**
   Ein Status-Poll überprüft, ob der IP-Knoten auf einen Ping reagiert (*Abschnitt 4.2.1*). Ist dies der Fall, werden die untergeordneten Komponenten aufgefordert ihren Status zu aktualisieren. Die Ping-Ergebnisse werden automatisch für jeden IP-Knoten gesammelt (siehe *Abschnitt 4.19*).

   Die Standardeinstellung für das automatische Status-Poll ist einmal pro Stunde. Über den Menüeintrag **Host->Status aktualisieren** im Kontextmenü des IP-Knotens oder den Menüeintrag **Status aktualisieren** im Hauptmenü **IP Manager** kann ein Status-Poll manuell gestartet werden.

   Die Ergebnisse des Polls werden in einer Übersichtsliste angezeigt.

2. **Konfigurations-Poll:**
   Das Konfigurations-Poll fordert die untergeordneten Komponenten eines IP-Knotens auf ihre Konfigurationsdaten zu aktualisieren.

   Standardmäßig erfolgt das automatische Konfigurations-Poll einmal täglich. Wie das Status-Poll kann auch das Konfigurations-Poll manuell gestartet werden. In diesem Fall über den Menüeintrag **Host->Konfiguration aktualisieren** im Kontextmenü des IP-Knotens.

   Die Ergebnisse des Polls werden in einer Übersichtsliste angezeigt.

3. **Discovery-Poll:**
   Das Discovery-Poll führt eine Überprüfung nach neuen untergeordneten Komponenten, wie z.B. einem neuen HTTP-Server, durch.

   Standardmäßig wird das Discovery-Poll einmal täglich ausgeführt. Um das Discovery-Poll manuell zu starten, muss der Menüeintrag **Host->Discovery** im Kontextmenü des IP-Knotens ausgewählt werden.

   Die Ergebnisse des Polls werden in einer Übersichtsliste angezeigt.

Die Zeitintervalle für das IP-Polling können über die IP-Parameter geändert werden.

Für jeden IP-Knoten können die Werte für die automatischen IP-Polling-Intervalle manuell verändert werden. Dies ist über die IP-Parameter-Konfigurationsdialoge möglich. In diesen Dialogfeldern ist es möglich, die Zeitintervalle festzulegen, nach denen Status-Poll, Konfigurations-Poll und Discovery-Poll eines IP-Knotens gestartet werden. Darüber hinaus kann ein allgemeiner Zeitüberschreitungswert definiert werden. Kann eine Verbindung innerhalb dieser Zeit nicht aufgebaut werden, so gilt der IP-Knoten als nicht verfügbar. Der Höchstwert für die Zeitüberschreitung beträgt 300 Sekunden. Diese Verfügbarkeitsprüfung erfolgt mindestens einmal. Die Anzahl der Versuche kann jedoch über die IP-Parameter verändert werden. *Tabelle 1* zeigt die Mindestwert der einzelnen Parameter:

Parameter	**Mindestwert**
Zeitüberschreitung	1 Sekunde
Status aktualisieren	1 Minute
Konfiguration aktualisieren	1 Stunde
Discovery Polling	1 Stunde

Tabelle 1 Konfigurationsgrenzen

Neben den Zeitintervallen der einzelnen IP-Polls werden die erwähnten Dialoge auch dazu verwendet, die Verfallszeit der IP-Komponenten und die dazugehörige Aktion die ausgeführt werden soll, wenn die Verfallszeit verstrichen ist, zu definieren (*Abschnitt 4.9.1*). Standardmäßig beträgt die Verfallszeit eine Woche bis die jeweilige Komponente gelöscht wird. Die Ablaufzeit muss mindestens einen Tag betragen.

Was mit den Topologie-Informationen von IP-Knoten passieren soll, wenn sich die IP-Adresse eines IP-Knotens geändert hat, wird ebenfalls in diesen Dialogen konfiguriert (*Abschnitt 4.9*). Ein Anwender kann über ein Auswahlmenü entscheiden, ob die Topologie-Informationen beibehalten oder ignoriert werden sollen. Wenn die Topologie-Informationen ignoriert werden sollen, werden die Discovery-Filter-Regeln verwendet (*Abschnitt 4.2.2*) um die Position innerhalb der Topologie festzulegen.

Die manuell geänderten Topologie-Konfigurationen und Topologie-Daten des jeweiligen IP-Knotens werden standardmäßig beibehalten.

Hinweis:
Nur ein Anwender mit Administratorrechten kann diese Werte verändern.

Die folgenden Abschnitte enthalten folgende Informationen:

- Wie stellt man die standardmäßigen IP-Parameter ein (*Abschnitt 4.10.1, „IP-Parameter im IP Manager“*).
- Wie können IP-Parameter automatisch und basierend auf den Netzwerk-Parametern, neu discoverten IP-Knoten hinzugefügt werden (*Abschnitt 4.13.1, „IP Konfigurationsvorlagen“*).
- Wie definiert man die IP-Parameter für eine Reihe von IP-Knoten in einem IP-Netzwerk (*Abschnitt 4.10.2, „Konfiguration der IP-Parameter für ein IP-Netzwerk“*).
- Wie konfiguriert man die IP-Parameter gesondert für die einzelnen IP-Knoten (*Abschnitt 4.10.3, „Konfiguration der IP-Parameter für einen IP-Knoten“*).

4.10.1 IP-Parameter im IP Manager

Die Menüeinträge **IP Manager->Konfigurieren** (für Anwender mit „Administrator“-Rechten) bzw. **IP Manager->Konfiguration anzeigen** (für Anwender mit „Operator“-Rechten) öffnen den Konfigurationsdialog des IP Managers. Auf der Seite **Default** dieses Dialogs (Unterseite **IP Parameter**) können Anwender mit „Administrator“-Rechten die folgenden Standardparameter ändern. Anwender mit „Operator“-Rechten können diese Parameter lediglich betrachten.

Im Auswahl-Menü **Ping-Methode** wird die allgemeine Methode festgelegt, mit der die Verfügbarkeitsüberprüfung für IP-Knoten durchgeführt werden soll (*ICMP*, *TCP*, *SNMP*, *HTTP*, *HTTPS*). Wird als Methode *Auto* ausgewählt, werden für neue Knoten die Methoden der Reihe nach ausprobiert. Die erste Methode, die für den neuen Knoten funktioniert, wird für diesen Knoten konfiguriert. Ist *Deaktiviert* ausgewählt, gibt jeder gestartete Ping automatisch `0ms` als Ergebniswert zurück und es wird kein echter Ping gestartet.

Hinweis:
Für *HTTP*- und *HTTPS*-Pings: Verbindungsfehler führen zu einem Fehler und es wird keine Antwortzeit protokolliert.

Für *TCP*-Pings: Läuft der Host, aber der konfigurierte Port lauscht nicht, wird dies dennoch als Erfolg gewertet. Diese Logik ermöglicht es, die TCP-Methode als Fallback zu verwenden, falls der ICMP-Ping für das Netzwerk nicht aktiviert ist. Läuft der Host nicht, zeigt der TCP-Ping einen Fehler an.

Unter **Zeitüberschreitung** wird festgelegt, in welcher Zeit eine Antwort auf die Überprüfung erfolgen muss. Eine Überprüfung ist dann erfolgreich, wenn in der vorgegeben Zeit eine Antwort durch das überprüfte System erfolgt. Die Anfrage ist also auch dann erfolgreich, wenn das System mit einer Abweisung der Anfrage antwortet, und damit zeigt, dass es aktiv ist.

Ist eine Anfrage nicht erfolgreich, wird sie wiederholt, falls noch nicht so viele Wiederholungen erfolgt sind, wie unter **Wiederholungen** festgelegt wurde.

Unabhängig davon, ob eine Zeitüberschreitung aufgetreten ist, werden die Ping-Ergebnisse für jeden IP-Knoten gesammelt (siehe *Abschnitt 4.19*).

Sind alle Wiederholungen ausgeschöpft, ohne dass eine Antwort innerhalb des Zeitintervalls erfolgte, wird das System als nicht erreichbar markiert. Der Knoten erhält dann den in der Auswahl **Offline Status** ausgewählten Erreichbarkeitsstatus.

Die Felder **Status aktualisieren**, **Konf. aktualisieren** und **Discovery-Abfrage** definieren die Zeitabstände zwischen den regelmäßig automatisch durchgeführten Status-, Konfigurations- und Discovery-Pollings.

Ist ein Knoten länger als die unter **Verfallszeit** definierte Frist nicht erreichbar, so wird für den Knoten die im Menü **Abgelaufene IP Knoten** gewählte Aktion ausgeführt. Das heißt, je nach Auswahl wird der Knoten entweder gelöscht, in den Status '*nicht verwaltet*' gesetzt, oder es wird keine Aktion durchgeführt.

Ist der Haken vor **Topologie erhalten** gesetzt, so bleibt die konfigurierte Netzwerk-Topologie erhalten, wenn für ein System eine IP-Adressänderung erkannt wird. Dies ist der Fall, wenn für eine bekannte MAC-Adresse eine neue IP-Adresse erkannt wird, und sich die vorherige IP-Adresse im Zustand '*nicht aktiv*' befindet.

Mit Hilfe des Auswahlmenüs **Offline Status** kann festgelegt werden, in welchen Status IP-Knoten wechseln, die nicht länger erreichbar sind.

Ist der Haken vor **IP-Adressanpassung** gesetzt UND die Abfrage-IP-Adresse des Knotens ist nicht erreichbar UND es sind mehrere Interfaces/IP-Adressen für den Knoten definiert, so wird die Abfrage-IP-Adresse automatisch auf eine andere IP-Adresse aus der Liste der Interfaces/IP-Adressen gesetzt.

Ist der Haken vor **Leeres Netz automatisch löschen** gesetzt, so wird ein Netzwerk automatisch entfernt, wenn das letzte Objekt aus dem Netz entfernt wird.

Das Auswahlmenü **Auto Discovery** legt fest, welche Discovery-Regel für automatisch generierte neue Netzwerke ausgewählt wird.

Hinweis:
Die auf dieser Seite konfigurierten Werte werden als Standardwerte für alle künftig neu erkannten IP-Knoten verwendet. Die Werte bereits bestehender IP-Knoten werden **nicht** verändert.

4.10.2 Konfiguration der IP-Parameter für ein IP-Netzwerk

Sollen die IP-Parameter für eine Teilmenge oder alle IP-Knoten eines bestimmten IP-Netzwerks in einem Arbeitsgang bearbeitet werden, kann dies durch die Auswahl des Menüeintrages **Konfigurieren...** im Kontextmenü eines IP-Netzwerks eingeleitet werden.

Die Liste aller IP-Knoten kann über den Eintrag **Konfigurieren...** aus dem Hauptmenü **IP Manager** auf der Seite **Knoten** angezeigt werden.

Unter dem Reiter **IP Knoten-Parameter** findet sich nun ein Dialogfeld, in dem alle IP-Knoten des IP-Netzwerks aufgeführt sind. Hier können beliebig viele IP-Knoten ausgewählt werden (Strg + klicken) und die IP-Parameter mit den Dialogelementen auf der rechten Seite eingestellt werden. Zur Übernahme der Werte muss die Auswahl für jeden Parameter durch Klicken auf die Schaltfläche  bestätigt werden. In diesem Dialogfeld kann außerdem der Status „Verwaltet/Nicht Verwaltet“ der IP-Knoten eines IP-Netzwerks eingestellt werden. Für „nicht verwaltete“ IP-Knoten findet kein automatisches Polling statt. Neben den allgemeinen in *Abschnitt 4.10.1* beschriebenen IP-Parametern kann hier auch der Port für die Verfügbarkeitsprüfung gesetzt werden. Standardmäßig testet die Verfügbarkeitsprüfung den Port 7 (ECHO Port). Die Tastenkombination Strg+A wählt alle IP-Knoten gleichzeitig aus.

Das Auswahlmenü **Vorlage** kann verwendet werden, um eine IP-Konfigurationsvorlage einem individuellen IP-Knoten zuzuweisen (siehe *Abschnitt 4.13.1*). Wurde eine Vorlage ausgewählt, so wird die Vorlagen-Konfiguration für den Knoten verwendet.

Wichtiger Hinweis:
Die Submap eines IP-Knotens kann auch Objekte enthalten, die nicht vom IP-Manager Plugin verwaltet werden (z.B. ein HiPath/OpenScape 4000-System mit IP-Adresse). Diese Objekte sind vom Vorgang Verwalten/Nicht verwalten nicht betroffen.

4.10.3 Konfiguration der IP-Parameter für einen IP-Knoten

Um die IP-Parameter eines einzelnen IP-Knotens zu konfigurieren, kann ein „Administrator“ aus dem Kontextmenü des betroffenen Objektes den Menüpunkt **Konfigurieren** auswählen.

Im sich öffnenden Fenster können im Reiter **IP Parameter** die in *Abschnitt 4.10.1* beschriebenen Parameter für den ausgewählten Knoten eingestellt werden.

Wurden mehrere IP-Knoten selektiert, öffnet sich stattdessen ein Fenster, welches dem in *Abschnitt 4.10.2* beschriebenen entspricht. In diesem Fall werden die selektierten Knoten in der Liste angezeigt.

Zusätzlich kann hier der **TCP-Port** für die Verfügbarkeitsprüfung verändert werden, falls die Methode **TCP** ausgewählt wurde. Standardmäßig testet die Verfügbarkeitsprüfung mittels ICMP (Echo Request). Wird als **Ping-Methode** die Auswahl *Default* gewählt, wird die allgemeine Methode (siehe *Abschnitt 4.10.1*) verwendet. Ist *Deaktiviert* ausgewählt, wird kein Ping ausgeführt, und dies in der Statuserklärung des betroffenen IP-Knotens angezeigt.

Die beiden Felder **Host** und **IP Adresse** können verwendet werden, um dem Objekt manuell einen neuen Hostnamen bzw. eine neue IP-Adresse zuzuweisen. Wird der Hostname verändert, so wird für diesen die evtl. ebenfalls veränderte IP-Adresse automatisch ermittelt. Wird die IP-Adresse verändert, ohne dass der Hostname geändert wurde, wird für die neue IP-Adresse automatisch der ihr zugewiesene Hostname ermittelt.

Das Auswahlmenü **Vorlage** kann verwendet werden, um eine IP-Konfigurationsvorlage einem individuellen IP-Knoten zuzuweisen (siehe *Abschnitt 4.13.1*). Wurde eine Vorlage ausgewählt, so wird die Vorlagen-Konfiguration für den Knoten verwendet.

Das Auswahlmenü **Cluster** dient dazu festzulegen, ob der aktuelle IP-Knoten Teil eines Clusters sein soll (siehe *Abschnitt 4.22*). In den Menü kann der jeweilige Cluster ausgewählt werden, bzw. es kann die Leerzeile gewählt werden, um den Knoten keinem Cluster zuzuweisen. Mit der **+** Schaltfläche kann ein neuer Cluster erstellt werden.

Im rechten Teil des Dialogs kann manuell konfiguriert werden, ob es sich bei dem Knoten um einen IP V4/V6 Router oder einen Switch handelt. Standardmäßig wird versucht, dies per SNMP zu ermitteln. Ist das nicht möglich oder sollen die ermittelten Werte überschrieben werden, können folgende Werte angepasst werden:

- **IP V4 Router Darstellung:** Wird dieser Wert per SNMP oder manuell auf AN gesetzt, wird der IP-Knoten als IP V4 Router behandelt. Im OpenScape FM Desktop wird der IP-Knoten dann zusätzlich im Netzwerk-Topologie Container dargestellt und erhält eine Verbindung zu jedem Netzwerk, in dem er eine IP-Adresse besitzt.
- **IP V6 Router Darstellung:** Wird dieser Wert per SNMP oder manuell auf AN gesetzt, wird der IP-Knoten als IP V6 Router behandelt. Im OpenScape FM Desktop wird der IP-Knoten dann zusätzlich im Netzwerk-Topologie Container dargestellt und erhält eine Verbindung zu jedem Netzwerk, in dem er eine IP-Adresse besitzt.
- **MAC Switch Darstellung:** Wird dieser Wert per SNMP oder manuell auf AN gesetzt, wird der IP-Knoten als Switch behandelt.

Hinweis:
Durch das manuelle Anpassen des IP V4/V6 Forwarding können Router, auf deren SNMP-Agent nicht zugegriffen werden (z.B. wenn die SNMP Community nicht bekannt ist) trotzdem als Router eingebunden werden. Die entsprechenden Netzwerk-Interfaces des Routers müssen dann ggf. ebenfalls manuell hinzugefügt werden.

Hinweis:
Werden Status-Poll relevante Einstellungen verändert, wird automatisch ein Status-Poll (siehe *Abschnitt 4.10*) ausgeführt.

4.11 Konfiguration der Interfaces eines IP-Knotens

Die folgenden Abschnitte beschreiben, wie die Interfaces eines IP-Knotens oder Clusters (siehe *Abschnitt 4.11.1*) bzw. die Werte eines einzelnen Interfaces (siehe *Abschnitt 4.11.2*) angezeigt werden können.

Abschnitt 4.11.3 erklärt das Konzept von als virtuell definierten Interfaces im OpenScape FM.

4.11.1 Liste der Interfaces eines Knotens oder Clusters

Eine Liste aller Interfaces, die einem IP-Knoten zugewiesen sind, kann über das Kontextmenü des IP-Knoten-Objektes mittels des Eintrages **Interfaces->Info** geöffnet werden.

Für Cluster (siehe *Abschnitt 4.22*) ist es möglich, eine derartige Liste übergreifend für alle im Cluster enthaltenen IP-Knoten zu öffnen. Dies kann über das Kontextmenü des Cluster-Objektes über den Eintrag **Konfigurieren** geschehen. Die Seite **Interfaces** enthält dann die entsprechende Auflistung.

Die Struktur der Liste ist in beiden Fällen identisch und enthält eine Reihe von für die Interfaces erkannten Parameter.

Zusätzlich ist es möglich einzelne Knoten mit Hilfe der entsprechenden Schaltfläche als **Virtuell** (siehe *Abschnitt 4.11.3*) zu definieren, bzw. diese Definition zu entfernen.

4.11.2 Anzeige eines einzelnen Interfaces

Die Konfigurationsseite eines einzelnen Interfaces kann über das Kontextmenü des entsprechenden Interface-Objektes über den Eintrag **Konfigurieren** geöffnet werden. Diese finden sich im Navigationsbaum im Container `Interfaces` des entsprechenden IP-Knotens, oder in Form der oben beschriebenen Interface-Listen (siehe *Abschnitt 4.11.1*).

Auf der Seite werden eine Reihe von ermittelten Werten, wie z.B. die **IP-Adresse**, die **MAC-Adresse** oder der Interface-**Typ** angezeigt.

Zusätzlich können Parameter wie z.B. der **Verwaltungsstatus** hier auch manuell gesetzt werden.

Für Interfaces mit einer zugewiesenen IP-Adresse können zwei Haken gesetzt werden:

- Ist der Haken vor **Prüfe IP** gesetzt, wird die IP-Adresse des Interfaces zusätzlich getestet, wenn die Erreichbarkeit des IP-Knotens überprüft wird. Ansonsten erfolgt die Überprüfung nur über die Haupt-IP-Adresse des Knotens. Schlägt die Überprüfung fehl, wird ein entsprechendes internes Ereignis generiert.
- Der Haken vor **Virtuell** definiert die entsprechende IP-Adresse für den Knoten als virtuell (siehe *Abschnitt 4.11.3*).

4.11.3 Virtuelle Interfaces

Virtuelle Interfaces sind im OpenScape FM IP-Adressen, die nicht fest einem bestimmten IP-Knoten-Objekt zugewiesen sind, sondern unter gewissen Umständen dynamisch zu einem oder mehreren anderen IP-Knoten wechseln können.

In einem Cluster beispielsweise kann dies eine Adresse sein, die stets dem IP-Knoten des Clusters zugewiesen ist, der aktuell einen bestimmten Dienst zu Verfügung stellt. Fällt der Dienst auf diesem Knoten aus, oder ist er mit Anfragen überlastet, kann die Adresse durch das Cluster-Management temporär einem anderen Knoten zugewiesen werden, der nun die Aufgabe übernimmt.

Soll der entsprechende Dienst überwacht werden, kann es Sinn machen, das Objekt mit der virtuellen Adresse zu überwachen.

Will man jedoch konkret die einzelnen Elemente eines Clusters überwachen, ist die Betrachtung der virtuellen Adresse nicht hilfreich, da nicht zu jedem Zeitpunkt bekannt ist, welches System gerade mit der Adresse belegt ist. Ein gefundenes Problem könnte also nicht sicher der betroffenen Komponente zugeordnet werden.

Um die Erreichbarkeit von Systemen im OpenScape FM zu überprüfen, testet der OpenScape FM Server die Erreichbarkeit der primären IP-Adresse des Systems. Ist diese nicht erreichbar, werden in Folge auch alle weiteren nicht virtuellen Adressen des Systems überprüft. Virtuelle Adressen werden also bei der Bestimmung der Erreichbarkeit ignoriert.

Bei einigen Technologien ist das OpenScape FM selbstständig in der Lage, die virtuellen Adressen zu erkennen und entsprechend zu markieren (siehe entsprechende Technologie-Handbücher). In anderen Fällen muss diese Eigenschaft manuell gesetzt werden (siehe dazu *Abschnitt 4.11.1* und *Abschnitt 4.11.2*).

Hinweis:
Das OpenScape FM erfährt häufig erst mit dem nächsten Discovery, ob und auf welchem System eine bestimmte virtuelle Adresse aktuell gültig ist. Eine virtuelle Adresse kann daher zu konkreten Zeitpunkten dem falschen System oder sogar mehreren Systemen gleichzeitig zugewiesen sein.

4.12 Konfiguration der SNMP-Parameter

Das IP-Manager-Plugin verwendet SNMP, um mit einzelnen Geräten bzw. Agenten-Systemen zu kommunizieren.

Im Folgenden wird beschrieben, wie die für die Kommunikation notwendigen SNMP-Parameter konfiguriert werden können.

Falls der SNMP-Agent eines IP-Knotens die RMON MIB unterstützt, kann sich der OpenScape FM-Server automatisch als Trap-Empfänger konfigurieren. Ist dies nicht der Fall, so sollte der OpenScape FM-Server manuell als zusätzlicher Trap-Empfänger auf dem Agentensystem hinzugefügt werden.

4.12.1 SNMP-Parameter im IP-Manager

Mit Hilfe des Menüeintrags **Konfigurieren...** im Hauptmenü **IP Manager** kann ein “Administrator” über den Reiter **Default** (Unterseite **SNMP Parameter**) die standardmäßigen SNMP Polling-Parameter verändern. **Konfiguration anzeigen...** zeigt lediglich die aktuellen Variablen für Anwender mit „Operator“-Rechten an. Die in diesem Dialogfeld eingestellten Werte werden als Standardwerte für alle neu erkannten IP-Knoten verwendet. Die Werte bereits bestehender IP-Knoten werden nicht verändert.

Die definierten Werte für den SNMP-Port 161 eines IP-Knotens werden auch für das IP-Discovery verwendet, um festzustellen, ob SNMP-Agenten antworten (*Abschnitt 4.2, „IP-Discovery“*). Für jeden IP-Knoten existiert ein Eintrag für Port 161, unabhängig davon, ob auf diesem SNMP-Port ein Agent läuft.

Mit dem Haken **Unbekannte Traps anzeigen** kann festgelegt werden, ob Traps, die in keiner geladenen MIB definiert werden, im Ereignis-Browser angezeigt werden sollen.

4.12.2 Ändern der SNMP-Parameter für mehrere SNMP-Agenten eines IP-Netzwerkes oder IP-Knotens

Sollen eine Reihe von SNMP-Agenten für ein IP-Netzwerk oder einen IP-Knoten in einem Arbeitsgang konfiguriert werden, so kann dies durch den Eintrag **Konfigurieren...** (Netzwerk) bzw. **IP->Konfigurieren** (Knoten) aus dem Kontextmenü des IP-Netzwerk- bzw. IP-Knoten-Objektes eingeleitet werden.

Eine Liste aller IP-Knoten kann über den Eintrag **Konfigurieren...** aus dem Hauptmenü **IP Manager** auf der Seite **Knoten** angezeigt werden.

Die Seite **SNMP Parameter** des sich öffnenden Konfigurationsfensters enthält eine Liste der erkannten SNMP-Agenten.

Die definierten Werte für den SNMP-Port 161 eines IP-Knotens werden auch für das IP-Discovery verwendet, um festzustellen, ob SNMP-Agenten antworten (*Abschnitt 4.2, „IP-Discovery“*). Für jeden IP-Knoten existiert ein Eintrag für Port 161, unabhängig davon, ob auf diesem SNMP-Port ein Agent läuft. Für IP-Knoten, auf denen auf Port 161 kein SNMP-Agent erkannt wurde, wird die SNMP-Portnummer 161 in dem entsprechenden Eintrag nicht angezeigt.

Für jeden Eintrag kann die **SNMP Version**, die Anzahl der **Wiederholungen** und der Wert für die **Zeitüberschreitung** eingestellt werden. Der **Port** kann nur dann geändert werden, wenn es sich um einen tatsächlich erkannten Agenten handelt und somit eine Portnummer angezeigt wird.

Die jeweilige Schaltfläche  , übernimmt den eingetragenen Wert für die selektierten Knoten.

Die Einstellungen für z.B. die Communities oder die Sicherheitsstufen können getrennt für **SNMP V1/V2c** und **SNMP V3** auf den entsprechenden Seiten konfiguriert werden. Je nach der für einen Knoten gewählten SNMP Version, wird die passende Konfiguration für den Knoten berücksichtigt.

Das Auswahlmenü **Vorlage** kann verwendet werden, um eine SNMP-Konfigurationsvorlage einem individuellen IP-Knoten zuzuweisen (siehe *Abschnitt 4.13.2*). Wurde eine Vorlage ausgewählt, so wird die Vorlagen-Konfiguration für den Knoten verwendet.

4.12.3 Ändern der SNMP-Parameter für einen SNMP-Agenten

Um die SNMP-Parameter eines einzelnen Agenten zu konfigurieren, kann ein „Administrator“ aus dem Kontextmenü des betroffenen Objektes den Menüpunkt **Konfigurieren** auswählen.

Auf den drei SNMP Seiten können die Parameter, wie zuvor beschieben, konfiguriert werden.

Auf der ersten Seite kann das Auswahlmenü **Vorlage** verwendet werden, um eine SNMP-Konfigurationsvorlage einem individuellen IP-Knoten zuzuweisen (siehe *Abschnitt 4.13.2*). Wurde eine Vorlage ausgewählt, so wird die Vorlagen-Konfiguration für den Knoten verwendet.

Wurden mehrere IP-Knoten selektiert, öffnet sich stattdessen ein Fenster, welches dem in *Abschnitt 4.12.2* beschriebenen entspricht. In diesem Fall werden die selektierten Knoten in der Liste angezeigt.

4.12.4 Empfang von SNMP Traps

Die zuvor beschriebenen Verfahren definieren, wie SNMP-Parameter konfiguriert werden können, mit denen das OpenScape FM auf andere Systeme aktiv zugreift.

Das OpenScape FM empfängt aber auch SNMP-Traps unterschiedlichster Geräte. Für den Empfang von SNMP V3 Traps ist es dabei notwendig festzulegen, ob und welche Kodierungsparameter verwendet werden sollen.

Die Konfiguration der Empfangsmethode und -Parameter geschieht zentral über den Hauptmenü-Eintrag **IP Manager->Konfigurieren...** auf der Seite **SNMP V3 Trap**.

Auf dieser Seite können die **Sicherheitsstufe**, das **Authentisierungsprotokoll**, das **Verschlüsselungsprotokoll** und die zugehörigen Kennworte definiert werden, unter denen das OpenScape FM die eingehenden Traps empfängt.

4.13 Konfigurationsvorlagen

Konfigurationsvorlagen können verwendet werden, um zu vermeiden, dass für jeden Knoten eine separate IP- und SNMP-Konfiguration durchgeführt werden muss. Jede Vorlage repräsentiert eine dedizierte IP- oder SNMP-Konfiguration, welche manuell oder automatisch einem speziellen Typ (Gruppe) von IP-Knoten zugewiesen werden kann.

Eine Konfigurationsvorlage kann manuell zugewiesen werden, oder es kann automatisch IP-Knoten zugewiesen werden, indem Zuordnungsregeln festgelegt werden, die auf der IP-Adresse oder dem Teilnetz des IP-Knotens basieren. Werden die Einstellungen einer Konfigurationsvorlage verändert, werden alle IP-Knoten, denen diese Vorlage zugewiesen wurde, automatisch angepasst.

Vorlagen können zum Beispiel für spezifische Netzwerke oder spezifische Objekttypen (Router, Drucker) erstellt werden.

Beispiel:
Die Verfügbarkeit eines Servers kann mit verschiedenen Ping-Methoden überprüft werden. Ist ICMP für die Server eines bestimmten Teilnetzes gesperrt, kann diesen Knoten automatisch eine Konfigurationsvorlage zugewiesen werden, welches die Verfügbarkeit mittels TCP-Ping bestimmt.

Der allgemeine Dialog für die Definition von Konfigurationsvorlagen kann geöffnet werden, indem der Eintrag **Konfigurieren...** aus dem Hauptmenü **IP Manager** ausgewählt, und die Seite **Vorlagen** geöffnet wird.

Die folgenden Unterabschnitte beschreiben die Definition von IP- und SNMP-Konfigurationsvorlagen.

4.13.1 IP Konfigurationsvorlagen

IP-Konfigurationsvorlagen können definiert werden, indem der Eintrag **Konfigurieren...** aus dem Hauptmenü **IP Manager** ausgewählt, und die Seite **Vorlagen** und Unterseite **IP Parameter** geöffnet wird.

Neue Vorlagen können über die unterhalb der Liste befindlichen Schaltfläche **+** erstellt werden. Die Schaltfläche **-** kann verwendet werden, um ausgewählte Vorlagen zu löschen. Die **Pfeil hoch** und **runter** Schaltflächen können verwendet werden, um die Ordnungsposition des ausgewählten Vorlagen zu verändern.

Die Konfiguration verwendet die gleichen Parameter, die auch für die Konfiguration einzelner Knoten benutzt werden (siehe *Abschnitt 4.10.1*).

Der zusätzliche Parameter **Vorlage** dient dazu, der Vorlage einen Namen zuzuweisen. Dieser Name wird verwendet, um die Vorlage für einzelne Knoten auszuwählen und sollte daher sinnvoll und, innerhalb der Vorlagen-Liste, eindeutig sein.

Die Parameter **Netzwerk** und **Maske** werden verwendet, um der Vorlage einen Netzwerkbereich zuzuordnen. Immer wenn ein neuer IP-Knoten discovered wird, wird die Liste der Vorlagen in der angegebenen Reihenfolge überprüft. Die erste Vorlage mit einem passenden Netzwerk wird dem neuen Knoten als initiale Konfiguration zugewiesen.

Hinweis:
Die Parameter **Netzwerk** und **Maske** werden ignoriert, wenn eine Vorlage einem Knoten manuell zugewiesen wird. Jede Vorlage kann jedem IP-Knoten zugewiesen werden. Diese Parameter werden nur für die initiale automatische Zuweisung verwendet.

Wird eine existierende IP Konfigurationsvorlage modifiziert, betrifft die Modifikation alle IP-Knoten, denen die Vorlage in diesem Moment zugewiesen ist.

4.13.2 SNMP Konfigurationsvorlagen

SNMP Konfigurationsvorlagen können definiert werden, indem der Eintrag **Konfigurieren...** aus dem Hauptmenü **IP Manager** ausgewählt, und die Seite **Vorlagen** geöffnet wird.

SNMP Konfigurationsvorlagen werden ähnlich behandelt, wie die im vorherigen Unterabschnitt beschriebenen IP Konfigurationsvorlagen (siehe *Abschnitt 4.13.1*).

In diesem Fall können die Parameter **Netzwerk** und **Maske**, die für die Zuweisung an neu discoverte Knoten zuständig sind, auf der Unterseite **SNMP-Parameter** gefunden werden. Auf dieser Seite können auch einige allgemeine Parameter eingegeben werden. Die Seiten **SNMP V1/V2c** und **SNMP V3** dienen dazu, Parameter einzugeben, die spezifisch für die ausgewählte **SNMP Version** sind.

Die Konfiguration verwendet die gleichen Parameter, die auch für die Konfiguration einzelner Knoten benutzt werden (siehe *Abschnitt 4.12.1*).

Wird eine existierendes SNMP Konfigurationsvorlage modifiziert, betrifft die Modifikation alle IP-Knoten, denen die Vorlage in diesem Moment zugewiesen ist.

4.14 Konfigurationen Sichern und Laden

Die aktuelle Netzwerk-Konfiguration kann in eine XML-Datei gesichert und zu einem späteren Zeitpunkt geladen werden. Dies kann über die Hauptmenü-Einträge **IP Manager->Konfiguration Speichern...** bzw. **IP Manager->Konfiguration Laden...** geschehen.

Bei Aufruf der Funktionen kann über einen Datei-Browser der Name und die Position der Datei festgelegt bzw. eine Datei ausgewählt werden.

Gespeichert werden die aktuell enthaltenen IP-Knoten, Netzwerke und SNMP-Konfigurationen.

Über den Menüpunkt **IP Manager->Konfiguration Laden...** kann auch eine Adressliste geladen werden, siehe auch *Abschnitt 4.6.2, „Adressliste (Seed File)“*.

4.15 Port-Wechsel eines Agenten

Port-Nummern für SNMP-Agenten sind im OpenScape FM variabel und können über die unterschiedlichen Dialoge zur Konfiguration von SNMP-Agenten umgestellt werden. Hierdurch ist ein Zugriff auf die MIB-Inhalte eines bereits erkannten SNMP-Agenten weiterhin möglich, auch wenn sich dessen Port ändert. Der Agent wird nicht fälschlicherweise als neu betrachtet.

4.16 Manuelles Hinzufügen neuer SNMP-Agenten

SNMP-Agenten, die auf anderen Ports als den Standardports laufen, können im Kontextmenü des IP-Knotens über **Neu->SNMP-Agent...** hinzugefügt und konfiguriert werden.

4.17 Layer-3 Routen

Das OSI (Open Systems Interconnection Model) Layer-3 beschreibt die Netzwerkschicht einer IT-Infrastruktur.

Layer-3 ist für das Weiterleiten von Datenpaketen zwischen Knoten verantwortlich, die nicht unmittelbar miteinander kommunizieren können. Gewöhnlich sind dies Knoten, die sich nicht innerhalb des gleichen Netzwerkes befinden.

Neben dem Start- und Zielknoten sind auf diesem Layer die Geräte relevant, welche die Datenpakete zwischen den verschiedenen Netzwerken übertragen, wie Router und Layer-3-Switche.

Layer-3-Routen sind die möglichen Pfade, die von Datenpaketen innerhalb der IT-Infrastuktur genommen werden können, um vom ausgewählten Sender (Startknoten) zum ausgewählten Empfänger (Endknoten) zu reisen.

Im OpenScape FM können Layer-3-Routen zwischen zwei ausgewählten Knoten angezeigt werden, indem der Eintrag **Layer-3 Route anzeigen** aus dem Hauptmenü **IP Manager** ausgewählt wird.

Dieser Eintrag öffnet ein Fenster, in dem ein Startknoten (**Start**) und ein Endknoten (**Ziel**) als Hostname oder IP-Adresse eingegeben werden können.

Die Schaltfläche **OK** öffnet ein Fenster, das eine Liste mit den möglichen Layer-3-Routen zwischen den ausgewählten Knoten enthält.

Die Liste enthält den Start- und Zielknoten und die Router und Layer-3-Switche auf den möglichen Routen.

Alle Listeneinträge, die Teil eines möglichen Pfades sind, besitzen den gleichen Eintrag in der Spalte **Pfad Nr**. Die Spalte **Entfernung** zeigt die Zahl der Hops an, die nötig sind, um den entsprechenden Knoten über den jeweiligen Pfad zu erreichen. In Kombination liefern diese beiden Spalten die Information über die individuellen möglichen Routen.

Sollen weitere Zwischenknoten, wie Layer-2-Switche, die sich innerhalb eines Netzwerkes befinden, angezeigt werden, muss das Layer-2 Plugin verwendet werden (siehe separate *Layer-2 Manager Plugin Bedienungsanleitung*).

4.18 Interface UP/Down Traps

Wenn ein SNMP-Agent auf einem IP-Knoten entdeckt, dass ein Interface seinen Status gewechselt hat (von aktiv zu inaktiv oder umgekehrt) oder ein Warm- bzw. Kalt-Start ausgeführt worden ist, sendet der SNMP-Agent einen Trap zum OpenScape FM Server. Abhängig vom gesendeten Trap wird ein Ereignis erzeugt und im Ereignis-Browser angezeigt. Außerdem aktualisiert das OpenScape FM den Status des IP-Interface, wenn es seinen Status wechselt. Ein Warm- oder Kalt-Start aktualisiert das komplette IP-Knoten-Objekt.

In der folgenden Tabelle sind die vier verschiedenen Trap-Arten und die vom OpenScape FM ausgeführten Reaktionen aufgelistet:

Trap Name	OID	Reaction
SNMP_Cold_Start	.1.3.6.1.6.3.1.1.5.1	Start eines Discovery-Poll für den IP-Knoten
SNMP_Warm_Start	.1.3.6.1.6.3.1.1.5.2	Start eines Discovery-Poll für den IP-Knoten
SNMP_Link_Down	.1.3.6.1.6.3.1.1.5.3	Der Status des Interface-Symbols wird auf „kritisch“ gesetzt
SNMP_Link_Up	.1.3.6.1.6.3.1.1.5.4	Der Status des Interface-Symbols wird auf „normal“ gesetzt

Tabelle 2 IP-Knoten-Traps und die Reaktionen

Hinweis:
Wenn der SNMP-Agent die RMON MIB unterstützt, kann der OpenScape FM Server sich automatisch als Trap-Empfänger anmelden. Ist dies nicht der Fall, muss auf diesem IP-Knoten der OpenScape FM Server manuell als zusäztlichen Trap-Empfänger eingetragen werden.

Wenn auf einem IP-Knoten der OpenScape FM Server nicht als Trap-Empfänger eingetragen wurde, erhält das OpenScape FM keine Traps von diesem IP-Knoten und der Status des IP-Knotens kann nur durch einen Status-Poll ermittelt werden. Abhängig vom Ergebnis des Status-Polls wird der Status des Interfaces auf „aktiv“ (grün) oder „inaktiv“ (rot) gesetzt. Weitere Informationen über den Status-Poll erhalten sie im *Abschnitt 4.10*.

4.19 Überwachung der Ping-Ergebnisse

Die OpenScape FM überprüft den Status eines IP-Knotens oder eines bestimmten Dienstes auf dem IP-Knoten anhand verschiedener Erreichbarkeitsprüfungen ("Pings"). Für eine Vielzahl von Objekttypen (SNMP, HTTP, Telnet, SSH, Web Service etc.) wird der Erreichbarkeitsstatus durch die Ausführung solcher Pings bestimmt (siehe *Abschnitt 4.10.1*). Der Status wird über ein entsprechendes neues Ereignis verändert.

Wenn die Pings innerhalb eines konfigurierten Timeout für eine konfigurierte Anzahl aufeinanderfolgender Wiederholungen nicht beantwortet werden, betrachtet das OpenScape FM den getesteten IP-Knoten als nicht erreichbar und damit in einem kritischen Zustand.

Aber selbst wenn die Pings innerhalb des Timeout-Intervalls beantwortet werden, können wachsende Ping-Zeiten auf ein Problem hinweisen.

Wenn beispielsweise ein Webserver auf einem Host läuft, auf dem ein Prozess/Dienst ständig zu viel Rechenzeit verbraucht, wird sich die Antwortzeit dieses Webservers wahrscheinlich erhöhen. Ein weiteres Beispiel, das zu einer Erhöhung der Antwortzeit oder der Anzahl der Wiederholungsversuche führen kann, wäre ein Router/ Switch, der ein hohes Datenvolumen bewältigt.

Um solche Probleme zu erkennen, sammelt das OpenScape FM automatisch die ermittelten Antwortzeiten der verschiedenen Ping-Operationen für alle IP-Knoten. Die gesammelten Daten werden in die in der Online Data Export Konfiguration festgelegten Datenbank (z.B. MySQL) exportiert. Die Antwortzeiten sind getaggt, so dass ihre Werte in den Berichten ausgewählt werden können. Die Werte werden mit Hilfe des System Management Monitors `ResponseTimes.Delay` ermittelt.

Um die Ergebnisse (in Millisekunden) anzuzeigen, stellen die IP-Knoten-Objekte in ihrem Kontextmenü den Eintrag **Host->Antwortzeit** zur Verfügung. Dieser Eintrag öffnet eine Standard-Ergebnisseite des System-Managements, welche die gesammelten Daten für den jeweiligen Host enthält.

Auf der Seite **Schwellwert** des Ergebnisfensters können zusätzliche Schwellenwerte definiert werden, die Statusänderungen und entsprechende Ereignisse auslösen, wenn sie überschritten werden.

4.20 HTTP- und HTTPS-Servers

Jeder beim IP-Discovery an den Ports 80, 280, 8080, 8085 oder 8888 erkannte HTTP-Server (d. h. jeder Server, der innerhalb der vorgegebenen Zeit auf die Anfrage reagiert hat) wird auf der Submap des entsprechenden IP-Gerätesymbols angezeigt (siehe *Abschnitt 5.2*). Jeder mit der gleichen Methode auf Port 443 erkannte HTTP-Server wird, da HTTPS-Server in der Regel diesen Port benutzen, als HTTPS-Symbol auf der Submap des entsprechenden IP-Gerätesymbols angezeigt.

HTTP-Server, die nicht auf einem Standard-Port laufen, können manuell angelegt und konfiguriert werden, hierfür muss der Menüpunkt **Neu**-> **Web-Server** aus dem Kontextmenü des IP-Knotens aufgerufen werden.

Beide Symboltypen bieten ein HTTP-Kontextmenü mit den Einträgen **Konfigurieren** und **Startseite** bzw. die Einträge selbst an.

- Mit Hilfe des Befehls **Startseite** kann auf die Start-URL des entsprechenden HTTP/HTTPS-Servers zugegriffen werden.

  Im Falle eines HTTPS-Servers beginnt die URL der entsprechenden Startseite mit dem Kürzel „`https://`“

- Über **Konfigurieren** öffnet sich ein Fenster, dass zwei Seiten enthält:

  - Auf der Seite **HTTP-Verbindungsparameter** können ggfs benötigte Login-Daten für den HTTP-Zugriff angegeben werden.

  - Die Seite **Zertifikate** zeigt das aktuelle Zertifikat an, und dieses kann durch markieren von **Zertifikat akzeptieren** akzeptiert werden.

Es ist zu beachten, dass gelöschte Symbole wieder angezeigt werden, wenn sie bei einem Scan erneut erkannt werden.

4.21 IP-Adressen Mapping

Da die Anzahl der IP-Adressen im Internet begrenzt ist, arbeiten zahlreiche Intranets innerhalb des privaten IP-Adressbereichs mit nicht-routbaren internen Adressen. Mit Hilfe der NAT (Network Address Translation) kann ein Gerät wie beispielsweise ein Router, der zwischen Internet und Intranet eingefügt wird, externe in interne Adressen umsetzen und umgekehrt. Generell wird nach statischer und dynamischer NAT unterschieden. OpenScape FM unterstützt die statische NAT, d.h. die statische Zuordnung einer bestimmten externen (im Internet eindeutig definiert und routbar) zu einer bestimmten internen (routbar nur innerhalb dieses konkreten Intranets) IP-Adresse.

Die Zuordnungsdaten werden als NAT-Zuordnungstabellen auf den entsprechenden Routing-Geräten gespeichert und die Gesamtheit der Geräte, die von einem derartigen NAT-Gerät verwaltet wird, werden als NAT-Domain bezeichnet.

Da der IP-Manager für die gesamte Verwaltung der IP-Adressen zuständig ist, übernimmt er auch das Management der NAT-Tabellen. Jedes Mal, wenn OpenScape FM ein Gerät mit NAT-Zuordnungstabellen erkennt (und wenn OpenScape FM für dieses Gerät die NAT-Zuordnung unterstützt!), werden die entsprechenden Zuordnungen registriert und bei der Verwaltung der IP-Knoten verwendet. NAT-Router oder -Geräte können nicht über OpenScape FM konfiguriert werden. Allerdings können die in der OpenScape FM-Datenbank registrierten NAT-Zuordnungsrichtlinien über die Bedienoberfläche des OpenScape-Clients komfortabel einsehen werden.

Die im OpenScape FM registrierten NAT-Zuordnungen können mit Hilfe des Eintrages **IP Adressen Mapping...** aus dem Hauptmenü **IP Manager** aufgerufen werden. Der Eintrag wird nur dann angezeigt, wenn mindestens ein NAT-Eintrag vom OpenScape FM erkannt wurde. Die angezeigte Tabelle enthält die folgenden Spalten:

External: Die externe IP-Adresse

Internal: Die entsprechende interne IP-Adresse

Netmask: Die in dem angegebenen Netzwerk verwendete Subnetzmaske

Node: Der Knoten (das Gerät), auf dem die Tabelle gespeichert ist.

Die Zeilen, in denen ein und derselbe Knoten ausgewiesen ist, bilde die Regeln für eine NAT-Domain.

IP-Objekte mit NAT-Adressen

Wenn ein IP-Objekt zwei IP-Adressen hat, eine interne und eine externe, werden beide Adressen im Label und in der „Info” der Interface angezeigt (aufrufbar über das Kontextmenü des Interfaces Container mit dem Eintrag **Info...**). In diesem Info Browser werden alle Interfaces aufgelistet, die zu diesem IP-Knoten gefunden worden sind.

4.22 Cluster

Ein Cluster ist im Allgemeinen eine Anzahl miteinander verbundener Computer, die von außen gesehen wie ein einzelnes System betrachtet werden können.

Cluster werden z.B. für Hot- oder Cold-Standby Systeme oder für das Load Balancing über mehrere Systeme eingesetzt.

Obwohl die Aufgaben innerhalb des Clusters alternativ oder gleichzeitig von mehreren Systemen des Clusters durchgeführt werden, ist dies in der Regel für außenstehende Systeme intransparent. Diese kommunizieren stets mit der gleichen IP-Adresse des Clusters und es ist ihnen in der Regel auch egal, von welchem der Cluster Systeme z.B. ein angeforderter Web-Dienst durchgeführt wird.

Aus Sicht des OpenScape FM ist eine besondere Betrachtung von Clustern sinnvoll, da vermeintliche Fehler, die auf einzelnen Systemen eines Clusters auftreten, für einen beobachtenden Techniker keine echte Störung darstellen.

Läuft ein Dienst z.B. nur auf einem System des Clusters und ist auf allen anderen Systemen inaktiv, so kann dies ein gewolltes Verhalten sein. In einem Cold-Standby System ist es sogar immer gewollt, dass die im Wartezustand befindlichen Systeme nicht aktiv sind.

In diesen Fällen ist es für das OpenScape FM daher sinnvoll, vermeintlich kritische Zustände (Dienst- bzw. System nicht verfügbar) solange nicht zu melden, wie die entsprechende Aufgabe durch den Cluster noch erfüllt wird, um die ‚falschen' kritischen Zustände für den überwachenden Techniker auszublenden.

Dieses Kapitel beschreibt, wie im OpenScape FM Cluster generell behandelt werden und wie diese konfiguriert werden können.

Das Arbeiten mit Clustern im OpenScape FM Web ist in der OpenScape FM Web Bedienungsanleitung beschrieben.

4.22.1 Statusermittlung in Clustern

Im OpenScape FM werden Cluster durch jeweils ein Cluster-Container-Objekt repräsentiert. Dieser Container enthält die IP-Knoten-Objekte der Systeme, die in dem Cluster enthalten sind.

Die in einem Cluster enthaltenen Systeme werden von den meisten Funktionen des OpenScape FM nicht anders behandelt als Systeme, die nicht in einem Cluster enthalten sind. Die Ermittlung ihres Status verändert sich allerdings wesentlich:

Der Status eines Objektes innerhalb eines Clusters bestimmt sich neben den üblichen Methoden der Statusfeststellung auch vom Status ähnlicher Objekte der anderen Systeme des Clusters. Dabei bedeutet ähnlich, dass sich ihre Objektnamen lediglich durch die IP-Adresse der betroffenen Systeme unterscheiden.

Besitzen beispielsweise zwei IP-Knoten `A` und `B` beide einen HTTPS-Web-Dienst auf Port `3080`, so lauten die Objektnamen dieser Dienste `IPhttps:<IP_von_A>:3080` und `IPhttps:<IP_von_B>:3080` und sie sind somit ähnlich. Ähnlich sind aber auch die IP-Knoten selbst, da sie in diesem Fall die Objektnamen `IPNode:<IP_von_A>` und IPNode:<IP_von_B> besitzen.

Damit einzelne komplett ausfallende IP-Knoten trotzdem schnell erkannt werden können, werden die IP-Knoten eines Clusters automatisch auf eine Ausnahmeliste gesetzt (siehe *Abschnitt 4.22.2.2*) und von der Cluster-Berechnung nicht berücksichtigt.

Ist in einem Cluster einem Objekt unmittelbar, und nicht durch ein Kindobjekt propagiert, der Status *Critical* zugewiesen, so überprüft das OpenScape FM, ob innerhalb des Clusters ein ähnliches Objekt existiert, das sich aktuell nicht im Status *Critical* befindet. Ist dies der Fall, so geht das OpenScape FM davon aus, dass der Cluster

die Funktion des betroffenen Objektes noch erfüllen kann, und das Objekt wird daher nicht auf den Status *Critical* sondern auf den Status *Disabled* (dunkelbraun) gesetzt. Objekte in einem Cluster werden also durch unmittelbare Statuszuweisung nur dann *Critical*, wenn auch alle ähnlichen Objekte *Critical* sind.

Die gleiche Vorgehensweise gilt auch für den Erreichbarkeitsstatus der betroffenen Objekte. Auch dieser wird entsprechend gegebenenfalls nur auf *Disabled* statt auf *Critical* gesetzt.

4.22.2 Konfiguration von Clustern

Die Konfiguration von Clustern besteht aus zwei Schritten. Der Einrichtung der Cluster selbst (siehe *Abschnitt 4.22.2.1*) und der Konfiguration der relevanten Objekte für die Statusermittlung (siehe *Abschnitt 4.22.2.2*).

4.22.2.1 Einrichten von Clustern

Eine Auflistung aller Cluster und deren Systeme kann über den Eintrag **IP Manager->Cluster** aus dem Hauptmenü aufgerufen werden. Die angezeigte Sicht enthält den zentralen **Cluster Container** und als Kindobjekte alle Cluster und deren Systeme.

Anlage neuer Cluster und neuer Cluster-Systeme

Eine Vielzahl von Clustern und ihrer Systeme werden für verschiedene Technologien automatisch durch das OpenScape FM angelegt. Näheres dazu findet sich in den Bedienungsanleitungen der entsprechenden Technologien.

Zusätzlich können neue Cluster manuell über zwei Methoden angelegt werden:

- Durch die Auswahl des Menüeintrages **Neu->Cluster** aus dem Kontextmenü des zentralen Cluster Containers oder eines Topologie-Containers.

  Einzelne Systeme können durch Drag&Drop oder durch **Bearbeiten->Kopieren** und **Bearbeiten->Einfügen** in den angezeigten Container hinzugefügt werden.

- Über die **IP-Parameter**-Konfiguration eines IP-Knotens (siehe *Abschnitt 4.10.3*) und der Verwendung der **+** Schaltfläche neben dem **Cluster** Auswahlmenü oder über den Kontextmenüeintrag **Neu->Cluster** eines IP-Knotens. Dies ordnet zusätzlich den aktuellen IP-Knoten dem neuen Cluster zu.

  Wird im **Cluster** Auswahlmenü ein bestehender Cluster ausgewählt, wird der aktuelle IP-Knoten dem Cluster zugewiesen.

Wird ein IP-Knoten einem Cluster hinzugefügt, so werden in diesem Augenblick einmalig alle Ereignisse, die diesem IP-Knoten zugewiesen sind, untersucht. Ereignisse, die ein Problem beschreiben, das durch ein ähnliches Objekt (siehe *Abschnitt 4.22.1*) innerhalb des Clusters abgedeckt werden, werden bei dieser Untersuchung automatisch bestätigt.

Wichtiger Hinweis:
Ein IP-Knoten kann nur einem Cluster zugewiesen sein. Wird er einem anderen Cluster zugeordnet, wird eine eventuell vorher bestehende Zuordnung aufgelöst.

Netzwerk Topologie für Cluster

Cluster werden an der gleichen Position innerhalb der Netzwerk-Topologie angeordnet, wie der in ihnen enthaltene IP-Knoten mit der höchsten Netzpriorität (siehe *Abschnitt 4.4*).

Löschen bestehender Cluster und bestehender Cluster-Systeme

Bestehende Cluster können gelöscht und Cluster-Systeme aus Clustern entfernt werden, indem ihr Symbol unterhalb des zentralen Cluster Containers gelöscht wird.

Cluster-Systeme können ebenfalls aus einem Cluster gelöscht werden, indem in ihrer IP-Parameter-Konfiguration im Auswahlmenü **Cluster** die **Leerzeile** ausgewählt wird.

4.22.2.2 Objektkonfiguration in Clustern

Der zentralen Cluster-Container enthält für jeden definierten Cluster einen entsprechenden Container.

Über den Eintrag **Konfigurieren** aus dem Kontext-Menü dieser Container kann die Detail-Konfiguration des entsprechenden Clusters aufgerufen werden, die aus zwei Konfigurationsseiten besteht:

- Aus der Seite **Interfaces** kann festgelegt werden, welche der Interfaces der im Cluster enthaltenen IP-Knoten als virtuell betrachtet werden sollen. Dies entspricht der in *Abschnitt 4.11* beschriebenen Funktion virtueller Interfaces. Da virtuelle Interfaces und ihre IP-Adresse über die Zeit nicht eindeutig einem IP-Knoten zugewiesen sind, werden sie bei der Ermittlung der Erreichbarkeit eines IP-Knotens nicht berücksichtigt.
- Auf der Seite **Ausnahmeliste** kann festgelegt werden, welche Kindobjekte der im Cluster enthaltenen IP-Knoten nicht von der Cluster-Funktion betroffen sein sollen.

  Dazu können einzelne Objekte aus dem Teilbaum des Clusters nach rechts in die Auflistung **Selektierte Objekte** verschoben werden. Diese Objekte sind dann nicht Bestandteil der speziellen Status-Berechnung des Clusters.

  Selektierte Objekte werden weder in den Status bzw. Erreichbarkeitsstatus *Disabled* versetzt, noch wird ihr Status für die Bestimmung des Status ähnlicher Objekte verwendet.

  Die IP-Knoten des Clusters werden automatisch auf die Ausnahmeliste gesetzt. Damit diese z.B. in einem Cold Stand-By System nicht ständig als nicht erreichbar erkannt und auf *Critical* gesetzt werden, können sie hier von Ausnahmeliste entfernt werden.

4.23 Netzwerkzugriffskontrolle (NAC)

Die Netzwerkzugriffskontrolle (Network Access Control - NAC) überwacht, ob unbekannte oder nicht erwünschte Systeme mit dem überwachten Netzwerk verbunden werden. Welche Systeme erwünscht bzw. nicht erwünscht sind, kann über ein Regelwerk definiert werden, das festlegt, welche IP- und MAC-Adressen erlaubt bzw. verboten werden sollen.

Wird der Zugriff eines nicht erlaubten Systems erkannt, informiert die NAC darüber, indem sie ein entsprechendes Ereignis generiert, welches die IP-Adresse bzw. MAC-Adresse des unerwünschten Systems beinhaltet.

Das Regelwerk kann für IP-Adressen und MAC-Adressen separat aufgebaut werden und besteht jeweils aus zwei Bausteinen:

1. Eine Liste von Adressen, die explizit erlaubt, verboten oder zu prüfen sind.
2. Filter-Definitionen, die anhand von MAC-Adress-Strukturen bzw. IP-Bereichen allgemein festlegen, welche Adress-Bereiche/-Muster verboten bzw. erlaubt werden sollen.

Diese Zweiteilung ermöglicht es zum Beispiel, eine Liste aller erlaubten Adressen aufzubauen und über die allgemeinen Filter-Definitionen alle übrigen Adressen zu verbieten.

4.23.1 Regelauswertung

Die Überprüfung entsprechend des Regelwerks erfolgt immer dann, wenn eine Adresse (IP oder MAC) erkannt wird.

Eine Erkennung erfolgt beispielsweise in den folgenden Fällen:

- Hinzufügen eines IP-Knotens
- Status-Poll eines IP-Knotens
- Konfigurations-Poll eines Switches/Routers
- Empfang eines Up/Down-Traps von einem Switch/Router.

Bei der Konfiguration der Polling-Intervalle für die entsprechenden Geräte sollte dies berücksichtigt werden.

Wird eine neue Adresse (IP oder MAC) erkannt, erfolgt für die IP-bzw. MAC-Adresse eine unabhängige Überprüfung des Regelwerks in der folgenden Reihenfolge:

1. Zunächst wird überprüft, ob für die Adresse ein Eintrag in der expliziten Adressliste existiert.

   Ist dies nicht der Fall, wird der zweite Schritt der Überprüfung durchgeführt.

   Ansonsten erfolgt das weitere Vorgehen entsprechend der Definition für die entsprechende Adresse innerhalb der Liste. Es gibt die folgenden drei Möglichkeiten:

   - Die Adresse ist *Erlaubt*: Die Adresse ist erwünscht und die Überprüfung wird abgebrochen.
   - Die Adresse ist *Verboten*: In diesem Fall wird ein Ereignis generiert, welches auf den unerwünschten Zugriff hinweist, und die Überprüfung wird abgebrochen.

- Die Adresse ist als zu *Prüfen* eingetragen: Es wird der zweite Schritt der Überprüfung durchgeführt.

2. Es wird überprüft, ob ein Objekt mit der entsprechenden Adresse im OpenScape FM existiert.

   Ist dies der Fall**,** wird diese Adresse erlaubt und als erlaubt in die explizite Liste eingetragen. Die Überprüfung wird abgebrochen.

   Existiert kein passendes Objekt im OpenScape FM, wird der dritte Schritt der Überprüfung ausgeführt.

   Hinweis:
   Dieses Verhalten führt dazu, dass für im OpenScape FM hinzugefügte IP-Knoten die NAC-Filter nicht angewendet werden. Nur beim Hinzufügen selbst findet eine einmalige Überprüfung statt.

3. Im letzten Schritt wird überprüft, ob eine passende aktive Filter-Definition für diese Adresse vorhanden ist. Die Filter-Definitionen werden in der Reihenfolge der Filter-Liste überprüft, und es wird der erste passende Filter für die Auswertung verwendet.

   Passt kein Filter, oder besitzt der erste passende Filter den Wert *Prüfen*, so wird die Adresse erlaubt. Die Adresse wird in der expliziten Liste als zu *Prüfen* eingetragen, und es wird kein Ereignis generiert.

   Besitzt der erste passende Filter den Wert *Erlaubt*, wird die Adresse erlaubt und sie wird in der expliziten Liste mit dem Wert *Erlaubt* eingetragen.

   Besitzt der erste passende Filter den Wert *Verboten*, wird die Adresse verboten und sie wird in der expliziten Liste mit dem Wert *Verboten* eingetragen. Außerdem wird ein Ereignis generiert, welches auf das unerwünschte System hinweist.

Die Konfiguration der NAC-Regeln findet sich in der allgemeinen Konfigurationsoberfläche des IP Managers. Diese öffnet sich über den Menüpunkt **IP Manager**->**Konfigurieren**. Die NAC-Konfiguration wird auf dem Reiter **NAC Regeln** behandelt, welcher aus vier weiteren Reitern besteht:

- **MAC-Liste**: Hier werden alle MAC-Adressen angezeigt, die erkannt worden sind. Die Liste kann manuell erweitert werden (siehe *Abschnitt 4.23.3*).
  Es kann explizit definiert werden, ob eine MAC-Adresse erwünscht oder nicht erwünscht ist. Weitere Details finden sich in *Abschnitt 4.23.2*.

- **MAC-Filter**: Hier können Filter für MAC-Adressen definiert werden. Dafür werden Muster von MAC-Adressen angelegt und es wird definiert, ob eine MAC-Adresse, die zu diesem Muster passt, erwünscht oder nicht erwünscht ist. Eine Beschreibung zur Definition von allgemeinen NAC-Filtern findet sich in *Abschnitt 4.23.4*.

- **IP-Liste**: Hier werden alle IP-Adressen angezeigt, die erkannt worden sind. Erkannt werden IP-Adressen z.B. über den ARP-Cache und die Interface-Tabellen der einzelnen SNMP-Agenten. Alle Netzwerkadressen hinzugefügter IP-Knoten werden ebenfalls in der Liste aufgeführt. Die Liste kann manuell erweitert werden (siehe *Abschnitt 4.23.3*).
  In der Liste kann angegeben werden, ob die IP-Adresse erwünscht oder nicht erwünscht ist. Weitere Details finden sich in *Abschnitt 4.23.2*.

- **IP-Filter**: Hier können Filter für Netzwerkbereiche definiert werden. Dafür werden Netzwerk-Adressen und deren Subnetzmasken angelegt und es wird definiert, ob die Adressen, die in diesem Netzwerkbereich enthalten sind, erwünscht oder nicht erwünscht sind. Eine Beschreibung zur Definition von allgemeinen NAC-Filtern findet sich in *Abschnitt 4.23.4*.

4.23.2 Explizites Erlauben/Verbieten einer Adresse

Das explizite Erlauben oder Verbieten einer IP-Adresse oder MAC erfolgt über die Reiter **IP-Liste** bzw. **MAC-Liste**.

Diese Listen bieten folgende Informationen an:

- **IP** bzw. **MAC**: Hier wird die erkannte IP- bzw. MAC-Adresse aufgelistet.
- **Knoten**: Gibt es zu dieser Adresse bereits einen IP-Knoten im OpenScape FM, so wird dieser hier angezeigt.
- **Erkennung**: Hier wird angezeigt, über welchen Mechanismus diese Adresse erkannt worden ist. Es kann folgende Werte geben:
  - *arpcachev4* und *arpcachev6*: Die Adresse wurde über den ARP-Cache eines SNMP-Agenten ausgelesen.
  - *iftable*: Die Adresse wurde aus der Interface-Tabelle eines SNMP-Agenten ausgelesen.
  - *user*: Die Adresse gehört zu einem IP-Knoten, der manuell hinzugefügt worden ist, oder die Adresse wurde manuell der expliziten Liste hinzugefügt.
  - *imported*: Die Adresse wurde über die Import-Funktion importiert, siehe auch *Abschnitt 4.23.3*.
  - *layer2*: Die Adresse wurde durch das Layer 2 Plugin erkannt.
- **Quelle**: Die Quelle der Adresse.
- **Typ**: Der Typ legt die Behandlung dieser Adresse fest, falls diese erneut erkannt wird:
  - *Erlaubt:* Die Adresse wird erlaubt, und es findet keine weitere Überprüfung der Filter für diese Adresse statt,
  - *Verboten:* Es wird ein Ereignis generiert, welches darauf hinweist, dass eine verbotene Adresse entdeckt worden ist. Die Generierung erfolgt gemäß der Beschreibung in *Abschnitt 4.23.5* um unnötige Duplikatereignisse zu vermeiden.
  - *Prüfe Filter:* Die Adresse wird erlaubt, und es findet auch zukünftig eine weitere Überprüfung der Filter für diese Adresse statt.
- **Datum**: Das Datum, wann diese Adresse zuletzt erkannt worden ist.
- **Bestätigt**: Wurde ein Verboten-Ereignis generiert, so steht hier, ob dieses Ereignis bereits bestätigt wurde.
- **Kommentar**: Ein Kommentar, der manuell definiert werden kann, oder der durch einen passenden Filter gesetzt wird, wenn die Adresse erkannt wird (siehe *Abschnitt 4.23.4*). Passende Filter fügen nur dann Kommentare hinzu, wenn das Feld leer ist.

Der **Typ** kann für einen einzelnen Eintrag über einen Doppelklick direkt in der Tabelle ausgewählt und gesetzt werden.

Sollen mehrere Einträge verändert werden, kann dies durch deren gemeinsame Auswahl und Verwendung des Textfeldes **Typ** und der Schaltfläche **Speichern** auf der rechten Seite erfolgen.

4.23.3 Erweitern der Adresslisten

Die Listen auf den Reitern **IP-Liste** und **MAC-Liste** können manuell erweitert werden. Hier gibt es zwei Möglichkeiten:

1. Direktes Hinzufügen einzelner Adressen: Ein einzelner Eintrag kann über die **+** Schaltfläche angelegt werden. Dieser kann direkt in der Tabelle oder über die Textfelder und der Schaltfläche **Speichern** auf der rechten Seite bearbeitet werden.
2. Importieren einer Liste von IP- bzw. MAC-Adressen: Über die Schaltfläche **Import** kann eine Liste von IP- bzw MAC-Adressen ergänzt werden. Bestehende Einträge werden überschrieben. Die Datei muss folgendem Format entsprechen:

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

Einzelne IP- bzw. MAC-Adressen können aus den Listen über die Schaltfläche **-** entfernt werden.

Zum Sichern der einzelnen Listen steht eine Export-Funktion zur Verfügung. Die Export-Funktion erzeugt eine Semikolon separierte Liste aller erkannten IP- bzw. MAC-Adressen. Durch Betätigen der Schaltfläche **Export** auf dem jeweiligen Listen-Reiter öffnet sich ein Dateibrowser. In diesem Dateibrowser kann ein Ablageort für die anzulegende Datei ausgewählt werden.

4.23.4 Definition eines Filters

Allgemeine Filter können über die Reiter **IP-Filter** und **MAC-Filter** definiert werden.

Um einen neuen Filter zu definieren, wird in beiden Fällen innerhalb des jeweiligen Reiters die Schaltfläche **+** betätigt. Dies erzeugt einen neuen Eintrag in der Tabelle, der entweder direkt in der Tabelle oder über die Textfelder und Schaltflächen auf der rechten Seite editiert werden kann.

Der **Index** gibt an, in welcher Reihenfolge die einzelnen Filter auf die erkannte Adresse angewendet werden. Sobald ein Filter zutrifft, werden nachfolgende Filter nicht mehr geprüft.

Für IP-Adressen werden IP-Netzwerk-Bereiche (**Netzwerk**) mit ihren Masken (**Maske**) definiert.

Für MAC-Adressen werden in dem Feld **MAC_NAC** Muster von MAC-Adressen definiert. Hier können Reguläre Ausdrücke angewendet werden. Die nachfolgende Tabelle enthält einige häufig vorkommende Beispiele.

Regulärer Ausdruck	*Beschreibung*
`.*`	Beliebiges alphanumerisches Muster
`^03.*`	Beliebiges alphanumerisches Muster, das mit den Ziffern 03 beginnt.
`.*03$`	Beliebiges alphanumerisches Muster, das mit den Ziffern 03 endet.
`^[03].*`	Beliebiges alphanumerisches Muster, das entweder mit der Ziffer 0 oder 3 beginnt.

Tabelle 3 Regulare Ausdrücke: Beispiele für Suchmuster

Typ gibt an, wie eine Adresse, die zu einem Filter passt, behandelt werden soll. Der **Typ** kann „Erlaubt“, „Verboten“ oder „Inaktiv“ sein.

- *Erlaubt:* Die passende Adresse wird in der entsprechenden Liste als *Erlaubt* aufgenommen und es findet in Zukunft keine weitere Überprüfung der Filter für diese Adresse statt.
- *Verboten:* Die entdeckte Adresse wird in der entsprechenden Liste als *Verboten* aufgenommen und es findet in Zukunft keine weitere Überprüfung der Filter für diese Adresse statt. Zusätzlich wird ein Ereignis generiert, welches darauf hinweist, dass eine verbotene Adresse entdeckt worden ist. Die Ereignis-Generierung unterliegt den Regeln die in *Abschnitt 4.23.5* näher erläutert werden.
- *Inaktiv*: Dieser Filter wird nicht angewendet und wird übersprungen.

Kommentar definiert einen Kommentar, der automatisch den neu erkannten Adressen hinzugefügt wird, die zum entsprechenden Filter passen.

4.23.5 Das NAC-Ereignis

Wird eine IP- bzw. MAC-Adresse erstmalig als verboten erkannt, wird ein Ereignis erzeugt.

Wird die Adresse erneut erkannt, und wurde das Ereignis bisher nicht bestätigt, so wird kein neues Ereignis erzeugt, sondern das bestehende Ereignis um einen Kommentar erweitert. Wurde das Ereignis bereits bestätigt, so wird ein neues Ereignis generiert.

Das Ereignis beinhaltet die erkannte Adresse und das Interface, an dem diese Adresse erkannt worden ist.

4.24 Applikationen

Das OpenScape FM erlaubt es Applikationen, als sogenannte Zugriffsapplikationen, für ausgewählte IP-Knoten unmittelbar aus deren Kontextmenü heraus auszuführen (siehe *Abschnitt 4.24.1*).

Außerdem ist es möglich den Ausführungsstatus einzelner Applikationen zu überwachen (siehe *Abschnitt 4.24.2*).

4.24.1 Zugriffsapplikationen

Zugriffsapplikationen sind lokale Applikationen, die für einzelne oder alle IP-Knoten definiert sind und die über das Kontextmenü der IP-Knoten-Objekte ausgeführt werden können.

Besitzt ein Anwender **Administrator-Rechte**, so befindet sich in den Kontextmenüs der einzelnen IP-Knoten-Objekte das Untermenü **Zugriffsapplikationen**. Dieses Menü enthält pro definierter Zugriffsapplikation einen Eintrag um diese aufzurufen. Außerdem ist der Eintrag **Konfigurieren...** enthalten, mit dem neue Applikationen hinzugefügt oder alte neu konfiguriert bzw. gelöscht werden können. Wird dieser Eintrag betätigt, so öffnet sich das Konfigurationsfenster.

Bild 1 veranschaulicht den Mechanismus, mit dem die Server-Verbindung für eine Zugriffsapplikation hergestellt wird.

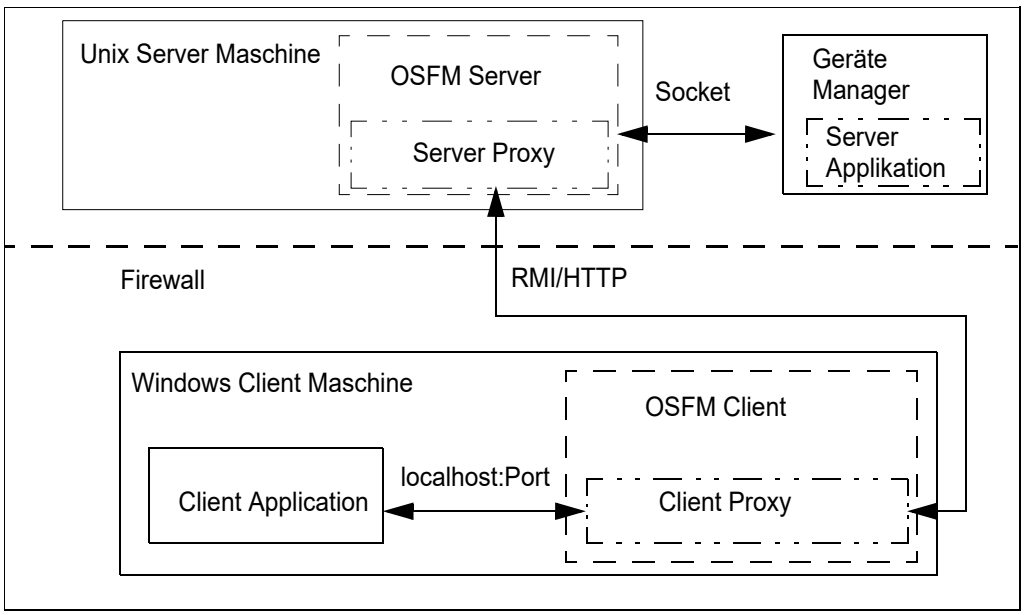


Bild 1 Zugriffsapplikationen - Verbindungsstruktur

Das in *Bild 1* veranschaulichte Beispiel besteht aus den folgenden Komponenten: ein OpenScape FM-Client-System, ein OpenScape FM-Server-System und ein Geräte-Manager-System, auf dem die Server-Applikation läuft.

Die beiden letztgenannten Systeme befinden sich hinter einer Firewall, die so konfiguriert ist, dass sie nur den Zugriff auf den OpenScape FM-Server erlaubt. Dadurch bedingt kann die Server-Applikation nicht direkt vom Client-System angesprochen werden.

Um den Zugriff von einem OpenScape FM-Client aus auf eine Server-Applikation zu ermöglichen, müssen die folgenden Bedingungen erfüllt sein:

- Der lokale Client-Proxy muss gestartet sein. Dies geschieht im Falle einer Aktivierung automatisch. Der Client-Proxy verbindet sich mit dem OpenScape FM-Server, übergibt die Ziel-IP-Adresse und den zugehörigen Port, und beantragt eine Sitzungs-Id. Diese Id wird im zweiten Schritt verwendet, um einen HTTP-Tunnel zum OpenScape FM-Server aufzubauen.
- Die lokale (konfigurierbare) Zugriffsapplikation wird gestartet und verbindet sich mit dem lokalen Proxy. Dieser Proxy handelt wie der Server der Zugriffsapplikation. Allerdings wird der gesamte Ein- und Ausgabe-Datenstrom über den OpenScape FM-Server zum Applikations-Server geleitet. Dies geschieht über eine HTTP-Verbindung zum Web-Server des OpenScape FM-Servers. Die verwendete URL enthält die Sitzungs-Id (ermittelt in Schritt 1), um den Client zu identifizieren und zu authentifizieren.
- Das Proxy-Modul auf dem OpenScape FM-Server akzeptiert die eingehende HTTP-Verbindung, identifiziert das Zielsystem anhand der in der URL enthaltenen Sitzungs-Id und öffnet einen Socket auf dem Zielsystem. Die HTTP-Verbindung (TCP-Socket) wird geöffnet gehalten und der Datenverkehr der Applikation wird durch diese übertragen.

Es muss bei diesen Verfahren beachtet werden, dass die Proxy-Funktionalität nur für Zugriffsapplikationen funktioniert, die für die Kommunikation einen einzigen Port verwenden. Wird mehr als ein Port verwendet, so muss mit einer direkten Verbindung gearbeitet werden. Es darf dann also kein Proxy eingesetzt werden. In diesem Fall wird die Zugriffsapplikation gestartet und das OpenScape FM übernimmt kein weiteres Kommunikations-Management.

Um eine Zugriffsapplikation über einen Client-Proxy starten zu können, muss zunächst ein Kontextmenü-Eintrag für den entsprechenden IP-Knoten erstellt werden (siehe dazu *Abschnitt 4.24.1.1, „Zugriffsapplikationen auflisten“*). Wird der Menüeintrag ausgewählt, wird die Zugriffsapplikation gestartet und eine Sitzung zum Zielsystem etabliert. Zu diesem Zweck muss die Zugriffsapplikation selbst lokal auf der Maschine installiert sein, auf der der OpenScape FM-Client läuft. Da die Zugriffsapplikation auf der OpenScape FM-Client-Maschine gestartet wird, ist auch der definierte Menüeintrag nur verfügbar für OpenScape FM-Clients, die auf der Maschine laufen, auf der die Definition stattfand.

Da Telnet eine allgemeinverfügbare Anwendung für den Fernzugriff ist, wird Telnet standardmäßig vom OpenScape FM eingerichtet (siehe *Abschnitt 4.24.1.3, „Telnet-Erkennung und -Einbindung“*). Weitere Zugriffsapplikationen können manuell konfiguriert werden. Ein Beispiel für eine solche Applikation, die sich hinter einer Firewall befindet, findet sich in *Abschnitt 4.24.1.2, „Zugriffsapplikationen konfigurieren“*.

4.24.1.1 Zugriffsapplikationen auflisten

Wird aus dem Kontextmenü eines IP-Knotens der Menüeintrag **Zugriffsapplikationen -> Konfigurieren...** ausgewählt, so öffnet sich das Konfigurationsfenster.

Hinweis:
Für diese Aktion werden Administrator-Rechte benötigt.

Dieses Fenster enthält eine Auflistung aller bereits für den IP-Knoten konfigurierten Zusatzapplikationen. Diese können neu konfiguriert bzw. entfernt werden. Das Fenster wird ebenfalls benötigt, um neue Applikationen zu einen IP-Knoten hinzuzufügen.

Das Fenster besteht aus den folgenden Elementen:

Die **Liste** enthält einen Eintrag pro bereits definierter Applikation. Dabei enthält die Spalte **Applikationsname** den Namen der Applikation. Unter diesem Namen wird die Applikation auch in den Kontextmenüs des IP-Knotens angezeigt. Die Spalte **Lokal Definiert** gibt an, ob die Applikation nur für den einen IP-Knoten (der Haken ist gesetzt) oder für alle IP-Knoten definiert wurde (der Haken ist nicht gesetzt).

- Die Schaltfläche **Hinzufügen...** öffnet ein Konfigurationsfenster für Zugriffsapplikationen, in dem eine neue Zugriffsapplikation für den IP-Knoten definiert werden kann.
- Die Schaltfläche **Editieren...** öffnet ebenfalls das Konfigurationsfenster für Zugriffsapplikationen. In diesem kann die Konfiguration für die in der Liste selektierte Applikation verändert werden.
- Die Schaltfläche **Löschen...** löscht die in der Liste selektierten Applikationen für den IP-Knoten. Die entsprechenden Applikationen werden aus der Liste entfernt und die ihnen zugehörigen Menüeinträge werden aus dem Kontextmenü des IP-Knotens entfernt.
- Die Schaltfläche **Global Löschen...** löscht die in der Liste selektierten Applikationen für alle IP-Knoten, für die die entsprechende Applikation als globale Zugriffsapplikation definiert ist.

- Die Schaltfläche **Schließen** schließt das Konfigurationsfenster.

4.24.1.2 Zugriffsapplikationen konfigurieren

Mit Hilfe des Konfigurationsfensters für Zugriffsapplikationen können die einzelnen Zugriffsapplikationen konfiguriert werden. Dies gilt sowohl für die Neuanlage von Zugriffsapplikationen wie auch für spätere Anpassungen der Konfiguration.

Das Fenster besteht aus den folgenden Elementen:

- Im Eingabefeld **Applikationsname** kann der Name festgelegt werden, unter dem die Applikation in den Kontextmenüs der betroffenen IP-Knoten angezeigt werden soll.
- Das Feld **Kommando** enthält den Pfad, über den die Applikation aufgerufen werden kann. Der Pfad kann entweder manuell in das Feld eingetragen werden, oder es kann mittels der Schaltfläche **Auswählen...** eine Applikation mit Hilfe eines Dateisystem-Browsers ausgewählt werden.
- Das Feld **Parameter** dient zur Angabe der Parameter, mit denen die Applikation aufgerufen werden soll. Dabei können neben 'festen' Eingaben zwei Makros verwendet werden. `$HOST` und `$PORT` werden abhängig von der gewählten **Verbindungsmethode** durch die entsprechenden Werte ersetzt (siehe unten).
- Das Feld **Zeitüberschreitung (Sek.)** gibt an, wie lange der Client-Proxy maximal auf den Verbindungsaufbau der Client-Applikation wartet. Diese Zeit wird z. B. dann überschritten, wenn die Applikation nicht erfolgreich gestartet werden konnte.
- Im Feld **Ziel-Port** wird angegeben, über welchen Port der Server im Proxy-Modus der Applikation den Service anbietet.
- Das Feld **Lokaler Port** ist nur editierbar, wenn als **Verbindungsmethode** 'Proxy' ausgewählt wurde. Das Feld gibt an, auf welchem lokalen Port der Proxy gestartet wird. Die Client-Applikation muss sich zu diesem Port verbinden. Enthält das Feld eine '0', so wird ein dynamischer Port verwendet. In beiden Fällen wird die tatsächlich verwendete Port-Nummer für das Makro `$PORT` eingesetzt.
- Das Auswahlmenü **Verbindungsmethode** kann über eine von zwei Methoden festgelegt werden:

  Proxy bedeutet, das der lokale Proxy gestartet wird, wenn der Eintrag der Applikation im Kontextmenü des IP-Knotens ausgewählt wird. Das Makro `$HOST` wird in diesem Fall durch 'localhost' ersetzt. Das Makro `$PORT` wird durch die Portnummer ersetzt, die der lokale Proxy verwendet. Die Verbindung zum Ziel-Server wird dann durch den Proxy und den OpenScape FM-Server getunnelt. Applikationen, die mehr als einen Port für ihre Kommunikation verwenden, können dieses Verfahren nicht verwenden.

  Direkt bedeutet, dass die lokale Zugriffsapplikation ohne den Proxy gestartet wird. Das Makro `$HOST` wird in diesem Fall durch die IP-Adresse ersetzt, die für den IP-Knoten erkannt wurde. Das Makro `$PORT` wird durch die konfigurierte Ziel-Portnummer ersetzt. Schlägt eine Verbindung mit diesem Verfahren fehl, so wird versucht, die Verbindung mit Hilfe des Proxys aufzubauen. Das direkte Verfahren funktioniert nur dann, wenn der Ziel-Server vom OpenScape FM-Client aus erreichbar ist.
- Wird die Schaltfläche **Ok** betätigt, so wird die eingegebene Konfiguration in das System übernommen und das Kontextmenü des betroffenen IP-Knotens wird ggfls. um einen Menüeintrag für die konfigurierte Zusatzapplikation erweitert.

- Wird die Schaltfläche **Global Zuweisen...** betätigt, so wird die Konfiguration für alle IP-Knoten übernommen, die zu diesem Zeitpunkt dem System bekannt sind. Zugriffsapplikationen, die bereits unter dem aktuellen Namen registriert sind, werden durch diese Aktion überschrieben. Für alle IP-Knoten wird ein Eintrag für die Applikation in das Kontextmenü eingetragen.

4.24.1.3 Telnet-Erkennung und -Einbindung

Telnet ist eine allgemein verfügbare Anwendung, die den Fernzugriff auf beliebige Computer in einem Netzwerk ermöglicht. Das OpenScape FM richtet diesen Fernzugriff für erkannte IP-Knoten als Standard-Zugriffsapplikation ein.

Dabei wird für jeden IP-Knoten überprüft, ob ein laufender Telnet-Service existiert. Eine derartige Überprüfung ist dann erfolgreich, wenn ein Scan auf Port 23 erfolgreich ist. In diesem Fall wird das Menü **Telnet** dem Kontextmenü des IP-Knotens hinzugefügt.

Zusätzlich zur automatischen Einrichtung der Zugriffsapplikation wird der Submap des IP-Knoten-Symbols ein Symbol hinzugefügt, das die Telnet-Funktionalität repräsentiert. Der Status des Telnet-Symbols hängt von der Erreichbarkeit des auf dem IP-Knoten installierten Telnet-Services ab.

Ist der Telnet-Service nicht mehr über Port 23 verfügbar, so ändert sich der Status des Telnet-Symbols auf 'kritisch', ansonsten ist der Status des Symbols 'normal'. Das Kontextmenü des Symbols enthält den Eintrag **Telnet**, über den eine Telnet-Sitzung auf dem Zielsystem angestoßen werden kann. Dazu verwendet der OpenScape FM-Client eine lokal installierte Telnet-Applikation.

Wird der Menüpunkt ausgewählt, so wird auf Windows-Systemen z. B. das Kommando `cmd /c start telnet` ohne die Angabe eines Pfades ausgeführt. Dies funktioniert wenn die Telnet-Applikation im Standard-Pfad enthalten ist.

Die Telnet-Applikation kann über den Menüpunkt **Zugriffsapplikationen->Konfigurieren...** konfiguriert oder entfernt werden. Wurde der Telnet-Eintrag entfernt, aber es läuft weiterhin ein Telnet auf dem System, so wird es bei einem erneuten IP-Discovery erneut erkannt und hinzugefügt.

Es muss beachtet werden, dass Veränderungen, die an der Konfiguration vorgenommen werden, sich stets nur für die OpenScape FM-Client-Maschine auswirken, auf der die Modifikationen vorgenommen wurden.

4.24.1.4 SSH-Erkennung und -Einbindung

SSH (oder Secure Shell) ist eine allgemein verfügbare Anwendung, die einen sicheren verschlüsselten Fernzugriff auf beliebige Computer in einem Netzwerk ermöglicht. Das OpenScape FM richtet diesen Fernzugriff für erkannte IP-Knoten als Standard-Zugriffsapplikation ein.

Dabei wird für jeden IP-Knoten überprüft, ob ein laufender SSH-Service existiert. Eine derartige Überprüfung ist dann erfolgreich, wenn ein Scan auf Port 22 erfolgreich ist. In diesem Fall wird das Menü **SSH** dem Kontextmenü des IP-Knotens hinzugefügt.

Zusätzlich zur automatischen Einrichtung der Zugriffsapplikation wird der Submap des IP-Knoten-Symbols ein Symbol hinzugefügt, das die SSH-Funktionalität repräsentiert. Der Status des SSH-Symbols hängt von der Erreichbarkeit des auf dem IP-Knoten installierten SSH-Services ab.

Ist der SSH-Service nicht mehr über Port 22 verfügbar, so ändert sich der Status des SSH-Symbols auf 'kritisch', ansonsten ist der Status des Symbols 'normal'. Das Kontextmenü des Symbols enthält den Eintrag **SSH-Applikation starten**, über den eine SSH-Sitzung auf dem Zielsystem angestoßen werden kann. Dazu verwendet der OpenScape FM-Client eine lokal installierte SSH-Applikation.

Wird der Menüpunkt ausgewählt, so wird auf Windows-Systemen z. B. das Kommando `cmd /c start ssh` ohne die Angabe eines Pfades ausgeführt. Dies funktioniert wenn die SSH-Applikation im Standard-Pfad enthalten ist.

Das Kontextmenü des SSH-Symbols wird auf das Kontextmenü des IP-Knotens übertragen. Neben dem Start der Applikation können hier auch Befehle und Skripte ausgeführt oder Datein hoch- bzw. heruntergeladen werden.

Die SSH-Applikation kann über den Menüpunkt **Zugriffsapplikationen->Konfigurieren...** konfiguriert oder entfernt werden. Wurde der SSH-Eintrag entfernt, aber es läuft weiterhin ein SSH auf dem System, so wird es bei einem erneuten IP-Discovery erneut erkannt und hinzugefügt.

Es muss beachtet werden, dass Veränderungen, die an der Konfiguration vorgenommen werden, sich stets nur für die OpenScape FM-Client-Maschine auswirken, auf der die Modifikationen vorgenommen wurden.

4.24.2 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.

4.24.2.1 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.

4.24.2.2 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 4.24.2.3*.

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*.

4.24.2.3 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.

4.25 Control Center Übersichten

Wurde das Control Center Plugin initialisiert, so werden für IP Manager Objekte eine Reihe von Control Center Übersichten bereitgestellt. Sie können angezeigt werden, indem der Hauptmenü-Eintrag **IP Manager->ControlCenter Übersicht...** ausgewählt wird. Es stehen die folgenden Fenster zur Verfügung:

- **Aktuelle 10 nicht normale Router**: In diesem Fenster werden bis zu zehn Router dargestellt, deren Status zuletzt nicht den Wert „Normal“ angenommen hat.
- **Aktuelle 10 nicht normale Switches**: In diesem Fenster werden bis zu zehn Switches dargestellt, deren Status zuletzt nicht den Wert „Normal“ angenommen hat.
- **Aktuelle 10 kritische IP-Knoten**: In diesem Fenster werden bis zu zehn IP-Knoten dargestellt, deren Status zuletzt den Wert kritisch angenommen hat.
- **Aktuelle 10 kritische IP Interfaces**: In diesem Fenster werden bis zu zehn IP Interfaces dargestellt, deren Status zuletzt den Wert kritisch angenommen hat.
- **IP Ereignisse über Zeit**: In diesem Fenster wird die Verteilung der Ereignisse der Kategorie ’IP Manager’ über die Zeit angezeigt.

Mehr über das Control Center findet sich in der entsprechenden Bedienungsanleitung.

5 Symbole und Übersichten

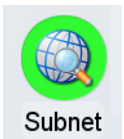
Die Objekte werden in den Ansichten (Submaps und/oder Bäume) durch Symbole dargestellt. Hierbei weist der Desktop jedem Objekttyp ein bestimmtes Symbol zu. Dieses Kapitel bietet einen kurzen Überblick über die im IP Manager verwendeten Symbole.

Das Erscheinungsbild jedes Symbols kann frei ausgewählt werden (**Eigenschaften**, **Symbol->Symbol Eigenschaften**). Bei Systemsymbolen ist dies jedoch nicht empfehlenswert.

5.1 Topologiesymbole

- Netzwerksymbol

- Teilnetzwerksymbol



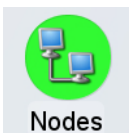
- Meta-Kanten-Symbol (Submap-Ansicht)

- Meta-Kanten-Symbol (Baumansicht)

5.2 IP-Symbole

- IP-Netzwerksymbol

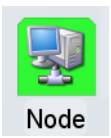
- IP-Knoten-Container-Symbol



- IP-Knoten:
  - Router-Symbol

- Switch-Symbol

- IP-Knoten-Symbol



- Remote Desktop Protocol-Symbol

- Telnet-Symbol

- IP-Interface-Symbol

5.3 Übersichten

Wurde das IP Manager Plugin initialisiert, so wird für IP-Knoten-Objekte eine Reihe von ControlCenter-Übersichten bereitgestellt.

Es werden die folgenden Übersichten angeboten:

- Die letzten zehn IP-Knoten, die in den Zustand ’*kritisch*’ gewechselt haben, und die sich noch in diesem Zustand befinden.
- Die letzten zehn IP-Interfaces, die in den Zustand ’*kritisch*’ gewechselt haben, und die sich noch in diesem Zustand befinden.
- Die letzten zehn Router, die in einen Zustand schlechter als ’*normal*’ gewechselt haben, und die sich noch in diesem Zustand befinden.
- Die letzten zehn Switches, die in einen Zustand schlechter als ’*normal*’ gewechselt haben, und die sich noch in diesem Zustand befinden.
- Die Verteilung der Ereignisse der Kategorie ’*IP Manager*’ über die Zeit.

Die Übersichten können angezeigt werden, indem im **IP Manager** Menü in der Hauptmenüleiste der Eintrag **ControlCenter - Übersicht** ausgewählt wird.

Mehr über das ControlCenter findet sich in der entsprechenden Anwender-Dokumentation.

A Rechteverwaltung

Die Zugriffsrechte des IP Managers 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 IP Manager Plugins beginnen mit der Kennzeichnung *IP Manager*.

Stichwörter