HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

BACHELORARBEIT

Herr
Marcus Schiefer

Vergleichende Analyse von verschiedenen Produkten für das Management und Monitoring von HP- und Cisco-basierten Netzwerken in mittelständischen Unternehmen

2014

Fakultät Mathematik/Naturwissenschaften/Informatik

BACHELORARBEIT

Vergleichende Analyse von verschiedenen Produkten für das Management und Monitoring von HP- und Cisco-basierten Netzwerken in mittelständischen Unternehmen

Autor:
Herr

Marcus Schiefer

Studiengang:
Wirtschaftsinformatik

Seminargruppe:
WF07w1-B

Erstprüfer:
Prof. Dr. J. Mario Geißler

Zweitprüfer:
Prof. Dr. Thomas Horn

Einreichung:
Mittweida, 06.01.2014

Verteidigung/Bewertung:
Dresden, 2014

Faculty Mathematics / Sciences / Computer Science

BACHELOR THESIS

Comparative analysis of various management and monitoring products for HP and Cisco-based networks in medium-sized companies.

author:
Mr.

Marcus Schiefer

course of studies:
business information technology

seminar group:
WF07w1-B

first examiner:
Prof. Dr. J. Mario Geißler

second examiner:
Prof. Dr. Thomas Horn

submission:
Mittweida, 06.01.2014

defence/ evaluation:
Dresden, 2014

Bibliografische Beschreibung:

Schiefer, Marcus:
Vergleichende Analyse von verschiedenen Produkten für das Management und Monitoring von HP- und Cisco-basierten Netzwerken in mittelständischen Unternehmen. - 2014. - VII, 46, 3 S.
Mittweida, Hochschule Mittweida, Fakultät Mathematik/Naturwissenschaften/ Informatik, Bachelorarbeit, 2014

Referat:

In der vorliegenden Arbeit wird eine umfangreiche Lösung für das Management und Monitoring der grundlegenden Netzwerktechnik in einem mittelständischen Unternehmen gesucht. Den IT-Administratoren soll mit diesen Programmen eine einfache und zeitsparende Möglichkeit zum Betrieb und Wartung des Firmennetzwerkes bereitgestellt werden. Dazu werden die Softwarelösungen von HP und Cisco mit Anwendungen anderer Entwickler verglichen.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACL	Access Control List
Cisco	Cisco Systems
CLI	Command Line Interface
CPI	Cisco Prime Infrastructure
FCAPS	Fault / Configuration / Accounting / Performance / Security
HP	Hewlett-Packard Company
http/https	Hypertext Transfer Protocol / Secure
IBH	IBH IT-Service GmbH
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IMC	Intelligent Management Center
IOS	Internetwork Operating System
IPFIX	Internet Protocol Flow Information Export
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LMS	LAN Management Solution
MIB	Management Information Base
NCM	Network Configuration Manager
NCS	Network Control System
NNMi	Network Node Manager i
NPM	Network Performance Monitor

NTA	NetFlow Traffic Analyzer
OID	Object identifier
OSI	Open Systems Interconnection
OVA	Open Virtual Appliance
PCM+	ProCurve Manager Plus
RFC	Request for Comments
RMON	Remote Monitoring
SCP	Secure Copy
SCTP	Stream Control Transmission Protocol
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
TMN	Telecommunications-Management-Network
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

1 Einleitung

Im Laufe der vergangenen Jahrzehnte entwickelten sich Computer und Computernetzwerke zu einem unverzichtbaren Bestandteil innerhalb eines Unternehmens. In solchen Netzwerken, die ohne genaue Planung gewachsen sind, nimmt das Risiko von Performance-Problemen oder sogar Netzwerkausfällen stark zu. Ein Problem mit dem IT-Netzwerk kann die meisten Arbeitsabläufe negativ beeinflussen oder sogar unmöglich machen. Daher wird immer häufiger von der Unternehmensführung erkannt, dass die IT-Abteilung nicht nur eine Kostenstelle für die Aufrechterhaltung des täglichen Betriebes ist, sondern auch die Betriebsprozesse verbessern kann und so indirekt zu einem wertschöpfenden Teil des Unternehmens wird.

Wird in Folge dieses Umdenkens das Netzwerkkonzept überarbeitet, geschieht das in der Hoffnung, dass Störungswahrscheinlichkeiten im Netzwerk eliminiert bzw. stark minimiert werden. Aufgrund der Investition in ein modernes, gut durchdachtes Netzwerk wird von den Mitarbeitern der IT-Abteilung erwartet, dass diese jetzt erheblich weniger Zeit für Management, Wartung und Fehlersuche in Verbindung mit dem Netzwerk aufwenden. Allerdings ist anzunehmen, dass diese Erwartung nicht vollständig eintritt. Da Netzwerkprobleme seltener auftreten und die Mitarbeiter in der Regel nicht intensiv mit grundlegenden Netzwerkfunktionsweisen vertraut sind, wird im Fehlerfall trotzdem mehr Zeit als erwartet für die Lösung des Problems investiert.

Um auf einen Ausfall im Netzwerk vorbereitet zu sein, kann das Unternehmensmanagement wie folgt reagieren:

- regelmäßige Schulung der IT-Mitarbeiter für Management- und Wartungsaufgaben am Netzwerk,
- Beauftragung eines externen Dienstleisters, der sich im Fehlerfall um die schnelle Behebung bemühen muss.

In beiden Fällen ist der Einsatz von speziellen Netzwerkmanagementlösungen notwendig, um die schnelle Fehlersuche und Problembeseitigung zu ermöglichen.

Als Teil des Portfolios bietet die *IBH IT-Service* GmbH (im Folgenden *IBH* genannt) Umstrukturierungen von komplexen Unternehmensnetzwerken an. Im Rahmen solcher Projekte wird die Einrichtung von passenden Netzwerkmanagementlösungen empfohlen und durchgeführt. Darüber hinaus werden der Support bei Netzwerkproblemen und die Wartung von Kundennetzwerken angeboten.

1.1 Problemstellung

Als Dienstleister im Netzwerkbereich verfügt die IBH über viele Kunden mit sehr unterschiedlichen Netzwerksituationen. Bei der eingesetzten Switch- und Router-Technik handelt es sich meist um Geräte von *Cisco Systems* (Cisco) oder *Hewlett-Packard Company* (HP). Das Management und Monitoring dieser Netzwerke wurde in den meisten Fällen durch die Softwarelösung des jeweiligen Herstellers realisiert. Beide Unternehmen haben die angebotenen Programme abgelöst und durch Neuentwicklungen ersetzt. Diese Nachfolgeprogramme wurden bereits einem ersten Test durch einen Mitarbeiter der IBH unterzogen. Es fehlt allerdings eine umfangreiche Testserie, bei der eine größere Anzahl von Funktionen geprüft wird und die dabei noch alternative Softwarelösungen in den Vergleich mit einbezieht.

1.2 Zielsetzung

Im Rahmen dieser Arbeit sollen die Vor- und Nachteile sowie die Praxistauglichkeit verschiedener Management- und Monitoring-Lösungen gezeigt werden. Die dabei gewonnenen Erkenntnisse sollen in Zukunft als Entscheidungshilfen dienen, anhand derer für jedes individuelle Kundennetzwerk die bestmögliche Softwarelösung ausgewählt werden kann.

Außerdem wird erhofft, dass sich ein universell einsetzbares Programm herauskristallisiert. Der Einsatz eines einzigen Programmes für alle Anwendungsszenarien würde den Schulungs- und Weiterbildungsaufwand für die IBH-Mitarbeiter reduzieren.

Weiterhin besteht ein starkes Interesse an einer Softwarelösung, welche trotz ihrer Komplexität einfach zu handhaben und übersichtlich bzw. leicht verständlich aufgebaut ist. Dieses Programm würde sich für die lokalen Administratoren von Kundennetzwerken eignen.

1.3 Methodisches Vorgehen

Diese Arbeit beginnt im *Kapitel 2* mit der allgemeinen Beschreibung von Netzwerken und stellt eine mögliche Umsetzung für mittelständische Unternehmen vor. Unter Zuhilfenahme von zwei standardisierten Modellen wird die Einführung in die Thematik des Managements von Netzwerken durchgeführt (*Kapitel 3*). Im letzten Kapitel des theoretischen Teiles (*Kapitel 4*) werden Mechanismen beschrieben, die für das Management und Monitoring von Netzwerken genutzt werden.

Anhand der Erkenntnisse aus den Beschreibungen von Netzwerken, den Bestandteilen des Netzwerkmanagements sowie den Techniken, die das Netzwerkmanagement ermöglichen, werden in *Kapitel 5* die Rahmenbedingungen für die Analyse und Programmauswahl festgelegt. Außerdem werden auch die Erwartungen an die Leistungen eines Netzwerkmanagementsystems formuliert.

Das *Kapitel 6* beschreibt die Vorabbetrachtung und Auswahl einzelner Managementlösungen auf Basis der Festlegungen im *Kapitel 5*. Dabei werden die Gründe für oder gegen die weitere Betrachtung einer Lösung aufgezeigt.

Die ausgewählten Managementlösungen werden anhand der in *Kapitel 5* beschriebenen Erwartungen untersucht. Die daraus resultierenden Erkenntnisse und Beobachtungen beschreibt das *Kapitel 7*. Dabei werden wichtige Erkenntnisse aus jedem Abschnitt in einem Resümee zusammengefasst.

Die Arbeit wird im *Kapitel 8* mit einer Auswertung und Empfehlung für unterschiedliche Anwendungsfälle abgeschlossen.

2 Netzwerke

Dieses Kapitel beschreibt IT-Netzwerke und wie diese in einem mittelständischen Unternehmen aufgebaut sein können.

2.1 Allgemeine Beschreibung

Die einfachste Umsetzung eines IT-Netzwerks besteht aus zwei direkt miteinander verbundenen Computersystemen. Neben den Computersystemen, bei denen es sich sowohl um Client-Geräte als auch um Server handeln kann, sind auch aktive und passive Netzwerkkomponenten Bestandteil eines Netzwerks. Dabei ermöglichen die aktiven Komponenten, wie Switches und Router, ein Netzwerk zu vergrößern. Zum Verbinden von mehreren Computersystemen werden Switches genutzt. Für das Verbinden von Netzwerken kommen Router zum Einsatz. Als passive Komponente eines Netzwerks gilt die zwischen den verschiedenen Geräten im Netzwerk eingesetzte Verkabelung.

Ziel eines Netzwerks ist es, die Kommunikation zwischen den verbundenen Systemen zu ermöglichen. Dabei sollen Dienste und Ressourcen durch Server für viele Client-Systeme zugänglich gemacht werden. Die Weiterentwicklung von Geschäftsprozessen in Unternehmen sorgt für eine verstärkte Nutzung des Netzwerks und der so bereitgestellten Dienste.

2.2 Netzwerke im Unternehmen

Da sich das Netzwerk zu einer unverzichtbaren Grundlage für viele Arbeitsprozesse in Unternehmen entwickelt hat, stellen diese Unternehmen mitunter hohe Anforderungen an ihr Netzwerk. Die Anforderungen beziehen sich in der Regel auf die Leistungsfähigkeit, Zuverlässigkeit, Sicherheit und Flexibilität des Netzwerks.

Um diese Anforderungen an das Netzwerk zu erfüllen, hat der Netzwerkkomponentenhersteller Cisco anhand seiner Erfahrungen ein entsprechendes Netzwerkdesign-Modell entwickelt[1]. Dieses als *hierarchisches Netzwerkmodell* bekannte

[1] Vgl. (2)

Modell besitzt einen modularen Charakter und kann dementsprechend flexibel auf die Besonderheiten von Netzwerken unterschiedlicher Größe angepasst werden.

Für das Design eines Netzwerks mittlerer Größe mit einer geringen räumlichen Ausdehnung bietet sich die in *Abbildung 1* dargestellte Lösung an. Dieses für mittelständische Unternehmen geeignete Design stellt einen Kompromiss aus dem Aufwand der Umsetzung und den Anforderungen an das Netzwerk dar.

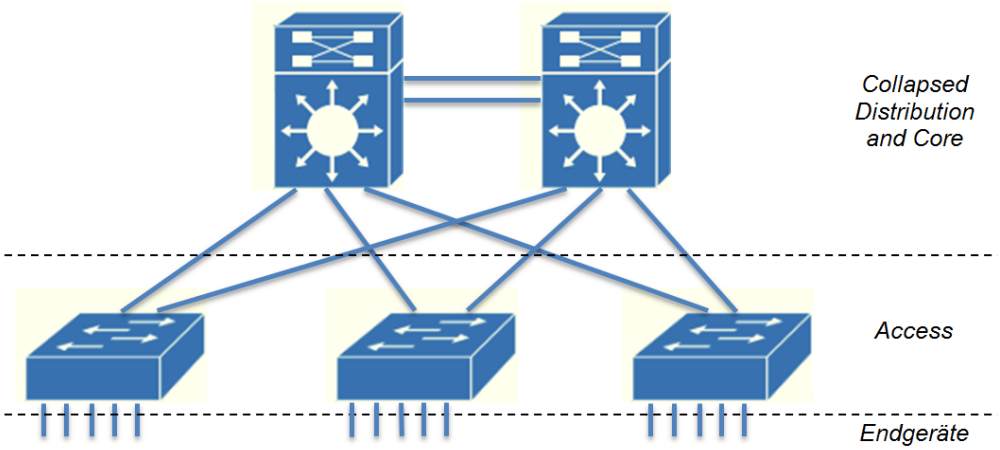

Abbildung 1: Netzwerkdesign mit *Collapsed Distribution and Core*

Das *Netzwerkmodell* sieht normalerweise eine hierarchische Einteilung der aktiven Netzwerkkomponenten in die Ebenen *Core*, *Distribution* und *Access* vor. Dabei bilden die Switches auf der Core-Ebene das Zentrum des Netzwerks, während die Switches der Access-Ebene die Anbindung von Endgeräten an das Netzwerk ermöglichen. Auf der Distribution-Ebene wird eine Bündelung durchgeführt. Jeder Switch dieser Ebene verbindet mehrere angeschlossene Switches der Access-Ebene mit der Core-Ebene. Der dargestellte Vorschlag ändert die Anzahl der Ebenen ab, indem die Ebenen *Core* und *Distribution* zum *Collapsed Distribution and Core* vereint werden. Aus der Darstellung ist außerdem erkennbar, dass die Switches der Core-Ebene redundant eingesetzt werden und somit zusätzliche Verbindungen zwischen beiden Ebenen bestehen. Dieser Aufbau erhöht die Ausfallsicherheit bzw. Verfügbarkeit des Netzwerks. Je nach technischer Umsetzung befinden sich die redundanten Verbindungen zwischen Core- und Access-Ebene in einem Wartezustand oder in aktiver Nutzung. Aus dem zweiten Fall ergibt sich zusätzlich eine gesteigerte Leistungsfähigkeit des Netzwerks.

Da die Aufgabe der Switches der Access-Ebene hauptsächlich in der Anbindung der Endgeräte an das Netzwerk besteht, können dafür Geräte mit einem darauf spezialisierten Funktionsumfang eingesetzt werden. Bei dem Einsatz eines *Collapsed Distribution and Core* werden die Aufgaben beider Ebenen zusammengeführt. Dementsprechend muss das eingesetzte Gerät die hohen Performance der Core-Ebene und den Funktionsumfang der Distribution-Ebene in sich vereinen.

3 Netzwerkmanagement

Das Netzwerkmanagement soll den Administratoren geeignete Methoden, Prozeduren und Werkzeuge zur Verwaltung, Wartung und zum Betrieb des Netzwerks zur Verfügung stellen[2]. Um die Entwicklung von Lösungen für das Management von komplexen heterogenen Netzwerken zu erleichtern, wurde das Netzwerkmanagement mit seinen Bestandteilen durch verschiedene Organisationen definiert.

3.1 Beschreibung durch die ISO

Aus der raschen Entwicklung von vernetzten Computersystemen in den 1970er Jahren ergab sich die Situation, dass die einzelnen Hersteller für ihre Geräte proprietäre Netzwerkprotokolle entwickelten. In der Hoffnung, dass die eigene Lösung einen möglichst hohen Marktanteil erreicht und sich so als Standard durchsetzt, wurden kaum Anstrengungen zur Entwicklung von herstellerübergreifenden Lösungen unternommen. Das Management dieser Systeme war dementsprechend auch nur durch die jeweilige Herstellerlösung möglich. Um diesen Entwicklungen entgegenzuwirken, wurde gegen Ende der 1970er Jahre versucht, die Kommunikation in Computernetzwerken mit Hilfe von Modellen und offenen Protokollen zu standardisieren. Dafür erarbeitete die *International Organization for Standardization* (*ISO*) zusammen mit der *International Telecommunication Union* (*ITU*), bzw. deren Komitee *ITU Telecommunication Standardization Sector* (*ITU-T*), das *Open Systems Interconnection* (*OSI*) Basisreferenzmodell. Dieses Modell wird in der aktuellen Version von 1994 durch den ISO Standard 7498 bzw. die ITU-T Empfehlung[3] X.200 beschrieben. Weitere nationale und internationale Organisationen haben diesen Standard übernommen. Ergänzend zu diesem Modell wurden in dem ISO Standard 7498-4 (1989) bzw. der ITU-T Empfehlung X.700 (1992) erste Konzepte des Netzwerkmanagements beschrieben.

In erster Linie soll dieses Management-Modell bei der Erfüllung der nachfolgenden Aufgaben im Rahmen des Netzwerkmanagements helfen:

- Planung, Organisation, Überwachung, Kontrolle und Abrechnung von Verbindungsdiensten,

[2] Vgl. (3) S.8

[3] Diese Empfehlungen sind auf der ITU Webseite einsehbar (9)

- Reagieren auf veränderte Anforderungen,
- zuverlässige Vorhersage des Kommunikationsverhaltens,
- Schutz von Informationen und Authentifizierung von Quellen und Zielen übertragener Daten.

Darüber hinaus werden diese Aufgaben in fünf Funktionsbereiche untergliedert:

- Fehlermanagement (Fault Management),
- Konfigurationsmanagement (Configuration Management),
- Abrechnungsmanagement (Accounting Management),
- Leistungsmanagement (Performance Management),
- Sicherheitsmanagement (Security Management).

Als Zusammenfassung dieser fünf Funktionsbereiche hat sich inzwischen die Bezeichnung *FCAPS*-Modell etabliert.

Das OSI-Management-Modell beschreibt außerdem verwaltete Objekte (managed objects), die zur abstrakten Darstellung der Eigenschaften einer Netzwerkressource dienen. Ein solches Objekt definiert sich durch seine Eigenschaften, die Änderungsmöglichkeiten an dem Objekt, die Nachrichten die das Objekt ausgibt sowie die Beziehungen zu anderen verwalteten Objekten. Die Summe der Objekte einer Ressource, zusammen mit deren Eigenschaften, ergeben dessen *Management Information Base* (MIB).

3.2 Erweiterte Beschreibung durch ITU

Parallel zu den Arbeiten am OSI-Modell begann die ITU mit der Entwicklung einer sehr umfangreichen Spezifikationssammlung für die Verwaltung großer Telekommunikationsnetzwerke von Service Providern. Das aus diesen Bemühungen entstandene *Telecommunications Management Network* (*TMN*) Modell wurde im Jahr 2000 veröffentlicht. Das TMN wird durch die ITU-T Empfehlungen M.3000 bis M.3499 definiert.

Das TMN basiert auf dem OSI-Basisreferenzmodell, erweitert daher dessen Umfang und beschreibt viele Punkte genauer. So befasst sich beispielsweise die ITU-T Empfehlung M.3400 mit den fünf Bereichen des FCAPS Modells. Die grundlegende Struktur für ein TMN wird im ITU-T M.3010 durch verschiedene Architekturkonzepte beschrieben. Für ein besseres Verständnis des Zusammenwirkens aller Aspekte im Netzwerkmanagement soll die *Logical Layered Architecture* näher betrachtet werden. Dieses Modell teilt die Managementfunktionen in die folgenden Ebenen auf:

- Business Management Layer,
- Service Management Layer,

- Network Management Layer,
- Element Management Layer.

Die zu mangenden Geräte des Netzwerks bilden den Network Element Layer. Wie in *Abbildung 2* dargestellt, bildet diese Ebene die Grundlage, auf der die vier Managementebenen aufbauen.

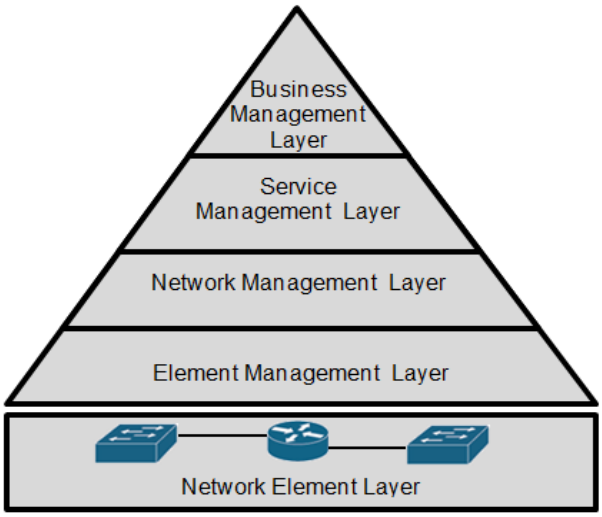

Abbildung 2: Logische Ebenen des TMN

Die Kommunikation der Managementebenen untereinander bzw. mit den Netzwerk-Elementen wird mittels Manager und Agenten umgesetzt. Einem Agent sind dabei die technischen Details zum Abfragen von Informationen auf seiner Ebene bekannt. Er ruft diese Informationen nach Aufforderung ab und bereitet diese für den Manager einer höheren Ebene auf. Ein Manager verwaltet meist mehrere Agenten und stellt an diese Anfragen, um Informationen über das Netzwerk zu erhalten. Dem Manager muss dafür nicht bekannt sein, welche Methoden ein Agent anwendet, um die geforderten Informationen zu sammeln. Es ist jedoch erforderlich, dass die direkt miteinander kommunizierenden Agenten und Manager über einen gemeinsamen Wissensstand auf Basis der MIB-Objekte verfügen.

3.3 Logische Ebenen eines TMN

Auf jeder Schicht, die weiter von den verwalteten Netzwerkgeräten entfernt ist, ergibt sich eine abstraktere Sicht auf das Netzwerk. Dabei kann man die Arbeitsweise der vier logischen Schichten in zwei Gruppen einordnen. Die unteren zwei Schichten, die Element- und Netzwerk Management Layer, können durch ihre Nähe zu den Netzwerkgeräten als technische Managementebene bezeichnet werden. Demgegenüber sind die oberen zwei Ebenen eher durch Verwaltungsaufgaben geprägt und lassen sich deshalb als verwaltende Managementebenen zusammenfassen.

3.3.1 Element Management Layer

Diese Ebene verwaltet die Netzwerkelemente und arbeitet mit den vom Hersteller implementierten MIB-Objekten und Managementprotokollen zusammen. Die so gesammelten Daten werden aufbereitet und der nächsthöheren Ebene durch hardware- und herstellerunabhängige Schnittstellen zur Verfügung gestellt. Neben der getrennten Verwaltung von Netzwerkelementen können diese auch in Gruppen organisiert, kontrolliert und koordiniert werden. Im Rahmen der Kontrollfunktion werden alle gesammelten statistischen Daten und Informationen über das jeweilige Netzwerkelement aufbewahrt.

3.3.2 Network Management Layer

Diese Ebene betrachtet und verwaltet das Netzwerk unabhängig von dessen räumlicher Ausdehnung als Ganzes. Dabei erlauben die durch den Element Management Layer bereitgestellten Daten die abstraktere Darstellung und Handhabung der einzelnen Netzwerkelemente. Außerdem ist dadurch dieser Ebene bekannt, welche Ressourcen im Netzwerk existieren, wie sie zusammenhängen und wie sie zu kontrollieren bzw. zu konfigurieren sind. Für das umfassende Monitoring und Management stehen dieser Ebene Funktionen zur Koordination von Aktivitäten über das gesamte Netzwerk zur Verfügung. Außerdem können damit die abstrakt formulierten Anforderungen umgesetzt werden, die der Service Management Layer an das Netzwerk stellt. Dieser übergeordneten Ebene wird eine von der technischen Implementierung unabhängige Sicht auf das Netzwerk bereitgestellt.

3.3.3 Service Management Layer

Diese Ebene ist in erster Linie für die Zusammenarbeit mit den Kunden (Nutzern) verantwortlich, die das Netzwerk bzw. die darüber angebotenen Dienste verwenden. Zu den Serviceaufgaben dieser Ebene gehören unter anderem die Kundendaten-Verwaltung, die Buchhaltung und die Verwaltung statistischer Daten zur Analyse der Dienstgüte. Diese Ebene arbeitet zwar mit den Daten aus dem Network Management Layer, die Struktur des Netzwerks ist hier jedoch nicht mehr bekannt. Daraus resultieren sehr abstrakt abgebildete Prozesse. Aufgrund dieser Abstraktion wird der Network Management Layer zur Durchführung von Änderungen am Netzwerk und zum Abfragen von Informationen über das Netzwerk benötigt.

3.3.4 Business Management Layer

Der Business Management Layer verwaltet das gesamte Unternehmen. Dabei stellt das Netzwerk nur einen Teilbereich dar. Die Aufgabe in dieser Ebene liegt

hauptsächlich in der strategischen Zielstellung für die Weiterentwicklung des Unternehmens. Die detaillierte Umsetzung der gesteckten Ziele erfolgt dann durch die untergeordneten Ebenen der jeweiligen Teilbereiche des Unternehmens. Um fundierte Entscheidungen über die weitere Entwicklung des Netzwerks zu ermöglichen, müssen dieser Ebene aussagekräftige Informationen über den Zustand des Netzwerks geliefert werden.

3.4 Funktionsbereiche von FCAPS

Der logische Aufbau eines Netzwerks anhand der TMN Empfehlungen kann gut mit den Bestandteilen des FCAPS-Modells verknüpft werden (*Abbildung 3*). Die Funktionsbereiche von FCAPS können dabei unterschiedlich stark auf den einzelnen Ebenen ausgeprägt sein. Gemeinsam vermitteln diese zwei Ansätze einen guten Überblick über das Thema des Netzwerkmanagements.

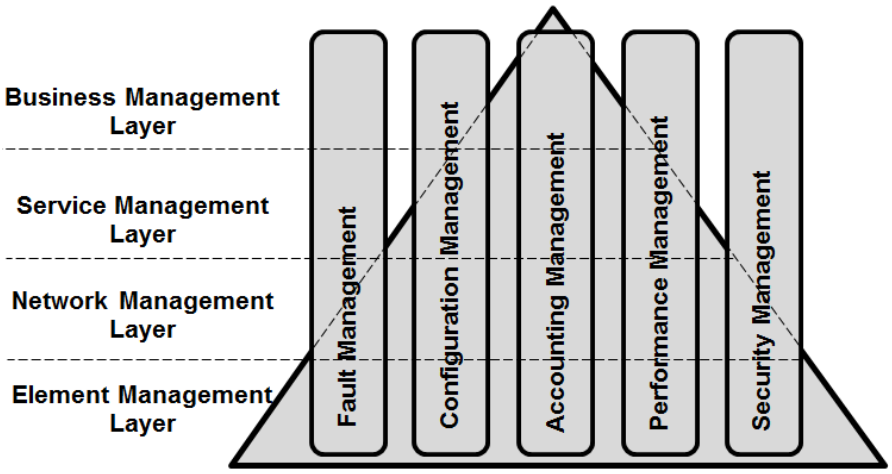

Abbildung 3: Logische Ebenen und FCAPS

3.4.1 Fehlermanagement (Fault Management)

Das Fehlermanagement beschreibt den Umgang mit Problemen im Netzwerk. Dabei wird ein unerwünschter Betriebszustand erkannt, isoliert, behoben und protokolliert. Das Erkennen eines Fehlers erfolgt in der Regel durch die Mitteilung des betroffenen Gerätes an das Managementsystem. Der Administrator reagiert auf diese Meldung, indem er sie analysiert und dabei den Fehler isoliert. Sobald die Ursache bekannt ist, kann der Administrator Gegenmaßnahmen einleiten und den Fehler beheben. Die Dokumentation aller Ereignisse, die das Netzwerk und seine Elemente betreffen, ist für eine statistische Auswertung mittels Reporting von Bedeutung.

3.4.2 Konfigurationsmanagement (Configuration Management)

Diese Funktionssammlung befasst sich mit den detaillierten Einstellungen der Geräte des Netzwerks. Dafür werden alle Netzwerkkomponenten im Managementsystem inventarisiert, ihre Konfiguration gesichert und stetig auf Veränderungen überprüft. Die Überwachung und Speicherung der Konfiguration ist eine wichtige Analysequelle für das Fehlermanagement. Viele Fehler die im Netzwerk auftreten, können so auf Probleme in der Gerätekonfiguration zurückgeführt werden. Neben der passiven Überwachung und Sicherung der Geräte werden auch Möglichkeiten zum Ändern von Konfigurationen sowie das einfache Hinzufügen, Tauschen oder Löschen von Geräten geboten.

3.4.3 Abrechnungsmanagement (Accounting Management)

Die Funktionen des Abrechnungsmanagements haben die Erstellung von Nutzungsstatistiken für Netzwerkdienste, Netzwerkressourcen oder Nutzer zum Ziel. Auf Basis dieser Daten kann für jeden Nutzer eine Kostenzuordnung und somit eine Rechnungsstellung durchgeführt werden. Um die korrekte Verknüpfung zwischen verbrauchter Ressource und dem verursachenden Anwender erstellen zu können, ist eine Benutzerverwaltung notwendig. Ein weiterer wichtiger Punkt ist die Möglichkeit der Limitierung einer Ressource wenn ein Nutzer diese unangemessen verwendet hat.

Bei der Erstellung des OSI- und TMN-Modells wurde von Telekommunikationsnetzwerken ausgegangen, bei denen eine solche Zuordnung und Abrechnung von Kostenstellen notwendig ist. Für kleinere Netze, die nicht solche Anforderungen haben, kann dieser Funktionsbereich auch als Administrationsmanagement bezeichnet werden. Dann besteht die Hauptaufgabe nur noch in der Nutzer-, Zugangsdaten- und Zugriffsrechte-Verwaltung.

3.4.4 Leistungsmanagement (Performance Management)

Hierbei werden alle Netzwerkelemente überwacht, um so die Leistungsfähigkeit des gesamten Netzwerks einschätzen zu können. Dafür werden statistische Daten von den Geräten gesammelt, analysiert und bewertet. Zusätzlich stehen Funktionen zur Berichterstattung bereit, die das Verhalten und die Effektivität eines Elements bzw. des gesamten Netzwerks aufzeigen können. Ist eine Schwachstelle im Netzwerk gefunden, muss diese umgangen, entschärft bzw. behoben werden.

3.4.5 Sicherheitsmanagement (Security Management)

Das Sicherheitsmanagement beschreibt die Umsetzung von Sicherheitsrichtlinien für den Zugriff auf das Netzwerk bzw. dessen Ressourcen ausschließlich durch

autorisierte Nutzer. Für diese Richtlinien werden Sicherheitsmechanismen generiert, verteilt und gespeichert sowie gegebenenfalls wieder entfernt. Entscheidend ist auch die Erkennung von Verletzungen der festgelegten Sicherheitsrichtlinien und eine daraus resultierende Alarmmeldung an das Managementsystem.

4 Techniken für das Netzwerkmanagement

Das OSI-Basisreferenzmodell beschreibt und standardisiert ein theoretisches Modell für die Kommunikation in Netzwerken. Entsprechend diesem Modell wurden Protokolle entwickelt, um es so auch in der Praxis zu etablieren. Allerdings konnten sich diese kaum durchsetzen. Ihre Entwicklung dauerte zu lange und die so entstanden Protokolle waren zumeist sehr komplex. Parallel zur Entwicklung des OSI-Modells ist die Internetprotokollsammlung (TCP/IP) entstanden. Diese Protokolle waren eher verfügbar, einfacher zu realisieren und erlangten durch erfolgreiche Förderung seitens der Politik eine weite Verbreitung. Inzwischen wird die Netzwerkkommunikation fast ausschließlich mit Protokollen der Internetprotokollsammlung realisiert[4].

Auf dieser Protokollsammlung basieren die nachfolgenden Techniken für das Management und Monitoring von Netzwerkgeräten.

4.1 Konfiguration und Datentransfer

Für die Grundkonfiguration von aktiven Netzwerkkomponenten steht dem Administrator auf diesen Geräten häufig eine Kommandozeile (*CLI*[5]) zur Verfügung. Um diese auch über das Netzwerk zu erreichen wurde *Telnet* entwickelt. Dieses Protokoll ist in der aktuellen Version von 1983 durch den RFC[6] 854 definiert. Telnet ist ein Client-Server-Protokoll, wobei die Netzwerkkomponente der Server ist. Ein Telnet Client verbindet sich mit dem Server und übermittelt diesem eine Anfrage. Der Server übergibt diese an die CLI und sendet deren Antwort zurück an den Client. Diese Kommunikation erfolgt über ein TCP[7]-Verbindung auf Port 23. Ein großer Nachteil von Telnet besteht im Fehlen von Sicherheitsmechanismen zum Schutz der übertragenen Informationen. Für die Authentifizierung des Nutzers auf dem Gerät werden Passwörter unverschlüsselt über das Netzwerk transportiert und können so von potentiellen Angreifern abgefangen werden.

---

[4] Vgl. (1) Kapitel 1.4.4

[5] command line interface – textbasierter Eingabebereich zur Steuerung von Geräten

[6] Requests for Comments – von der *Internet Engineering Task Force (IETF)* veröffentlichte Dokumente Vgl. (10), einige dieser Dokumente beschreiben Netzwerkprotokolle und anerkannte Internet Standards.

[7] Transmission Control Protocol

Um dieses Sicherheitsrisiko zu verringern, ist auf den heutigen Geräten zusätzlich *Secure Shell* (SSH) implementiert. SSH der aktuellen Version 2 wird durch die RFC 4250 bis 4254 aus dem Jahr 2006 sowie zahlreiche erweiternde Dokumente definiert. Im Vergleich zu Telnet erfolgt bei SSH die Kommunikation zwischen Server und Client verschlüsselt. Dabei wird eine TCP-Verbindung auf Port 22 verwendet. Da SSH dem Nutzer die gleichen Funktionen wie Telnet bereitstellt und dabei ein hohes Maß an Sicherheit bietet, sollte in der Praxis vorrangig SSH eingesetzt werden.

Neben der Kommandozeile stellen die Netzwerkkomponenten auch Protokolle zum Übertragen von Dateien bereit. Bei diesen Daten handelt es sich hauptsächlich um neue Software für das Gerät und die Möglichkeit, die Gerätekonfiguration schnell zu sichern. Am weitesten verbreitet ist dabei das *Trivial File Transfer Protocol* (TFTP). Es wird im RFC 1350 von 1992 definiert und nutzt für die Kommunikation eine UDP[8]-Verbindung auf Port 69. Dieses Protokoll ist sehr einfach aufgebaut und erlaubt nur das Lesen und Schreiben von Daten. Zwischen dem Sender und Empfänger findet keine Authentifizierung statt. Welche Alternativen außerdem noch auf den Geräten zur Verfügung stehen, ist von dem jeweiligen Hersteller bzw. Gerätemodell abhängig.

4.2 Erreichbarkeitsüberwachung

Die Überwachung der Erreichbarkeit von Netzwerkkomponenten kann am einfachsten mit dem Diagnose-Programm *Ping* erreicht werden. Dieses Programm nutzt das ICMP-Protokoll (RFC 792 von 1981) und seine verschiedenen Pakettypen. Dabei wird ein ICMP-Paket vom Typ *Echo-Request* über das Netzwerk vom Sender an das Zielgerät verschickt. Das Zielgerät antwortet darauf mit einem Paket vom Typ *Echo-Reply*. Erhält der Sender diese Antwort, ist das Ziel für ihn erreichbar. Bleibt die Antwort aus oder wird eine Fehlermeldung empfangen, liegt ein Fehler vor. Die Ursache für diesen Fall kann sowohl ein Fehler in der Netzwerkverbindung, als auch ein Problem des Ziels selber sein. Aus der Zeitspanne bis zum Erhalten einer Antwort ergibt sich die für das Monitoring interessante Antwortzeit des Ziels. Eine solche wiederkehrende Anfrage an Geräte im Netzwerk, zur Ermittlung von deren Statusinformationen, wird als *Polling* bezeichnet.

4.3 Ereignisprotokollierung

Viele Netzwerkkomponenten speichern die Ereignisse, die während des Betriebs auftreten, in einer internen Logdatei. Um ein Managementsystem über diese Mel-

[8] User Datagram Protocol

dungen zu informieren, wird das Syslog-Protokoll verwendet. Es wurde erst 2009 im RFC 5424 definiert und hat noch keinen Status als offizieller Standard. Allerdings gilt Syslog aufgrund seiner weiten Verbreitung bereits als quasi Standard für die Übertragung von Log-Nachrichten über das Netzwerk. Die Übertragung erfolgt mittels UDP auf den Port 514 an den Syslog-Server. Das Protokoll erlaubt dem Syslog-Client des Netzwerkgeräts ohne Aufforderung neue Meldungen an den Server zu senden. Bei der Kommunikation mittels UDP ist es nicht notwendig, dass der Server den Erhalt einer Meldung dem Client bestätigt. Die daraus resultierende Ungewissheit, ob die Meldungen ankommen, ist ein Nachteil des Syslog-Protokolls. Auf Netzwerkgeräten einiger Hersteller wurde Syslog deshalb erweitert und bietet dann Möglichkeiten zum Einsatz von TCP für die Kommunikation mit dem Server oder zumindest eine Nummerierung der übertragenen Meldungen.

Eine Syslog-Meldung beinhaltet neben der Beschreibung des Ereignisses noch Informationen über dessen Herkunft und Priorität. Anhand der Priorität kann eine erste Filterung der Meldungen durch den Administrator bzw. ein Managementsystem durchgeführt werden.

4.4 Überwachung und Steuerungen

Das OSI-Management-Modell (Abschnitt 3.1) sieht den Einsatz von MIBs für die Beschreibung von Netzwerkgeräten und deren Eigenschaften vor. Dabei existieren allgemeine und herstellerspezifische MIBs[9] in denen die verwertbaren Objekte beschrieben sind. Die so für ein Gerät definierten Objekte ermöglichen das Auslesen von System- und Status-Informationen. Durch Objekte mit entsprechenden Schreibrechten ist es außerdem möglich, Änderungen an der Gerätekonfiguration durchzuführen.

MIBs und die darin enthaltenen Objekte sind hierarchisch in einer Baumstruktur organisiert. Wie in *Abbildung 4* dargestellt, sind alle Elemente auf jeder Ebene des Baumes nummeriert. Aus diesen Nummern ergibt sich eine eindeutige Zahlenfolge, die den Weg von der Wurzel des Baumes bis zum gewünschten Objekt beschreibt. Sie dient der Identifizierung eines Objekts und wird als *Object Identifier* (OID) bezeichnet.

Für das Netzwerkmanagement werden hauptsächlich Objekte des Knotens *internet* (OID 1.3.6.1.) verwendet. Im Knoten *enterprise* können Gerätehersteller private MIBs einbinden, die spezielle Objekte für deren Geräte beschreiben. Zum Beispiel sind die MIBs von Cisco unter der OID 1.3.6.1.4.1.9. und von HP unter der OID 1.3.6.1.4.1.11. zu finden.

[9] MIBs werden in verschieden RFC-Dokumenten beschreiben

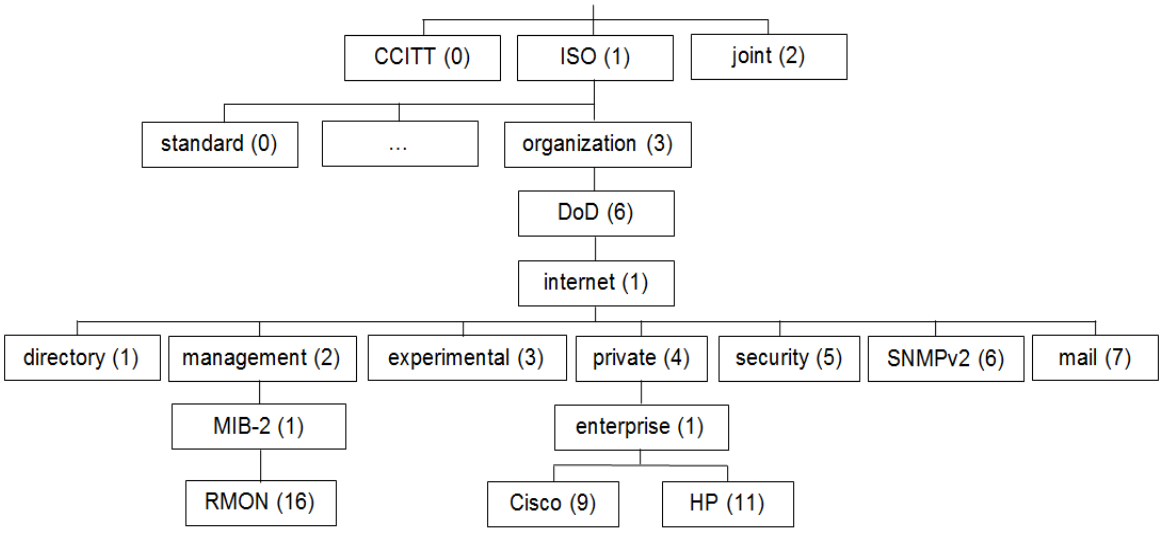

Abbildung 4: MIB-Hierarchie mit den wichtigsten Knoten

Der Zugriff auf Objekte der MIB durch ein Managementsystem bzw. einen Administrator kann mit Hilfe des *Simple Network Management Protocol* (SNMP) erfolgen. Das SNMP wurde erstmals 1988 im RFC 1067 beschrieben und seitdem mehrfach angepasst und erweitert. Die heute häufig eingesetzte *Community-Based SNMP Version 2* (SNMPv2c) wurde 1996 im RFC 1901 veröffentlicht. Diese beiden SNMP Versionen verfügen über unzureichende Schutzmechanismen, die es einem Angreifer erlauben, aus der Kommunikation die verwendeten Passwörter zu extrahieren. Die neueste Version SNMPv3 (RFC 3411) beseitigt dieses Risiko und verschlüsselt die Kommunikation.

SNMP setzt auf Netzwerkgeräten einen Agenten ein, der den Zugriff auf die MIB-Objekte verwaltet. Der Agent kann auf zwei Arten mit SNMP-Managern kommunizieren. Der überwiegende Teil der Kommunikation zwischen den beiden SNMP-Komponenten besteht aus Anfragen des Managers und den Antworten des Agenten (Polling). Auf diese Weise können Objekte ausgelesen oder verändert werden. Die so periodisch ausgelesen Statistikdaten von Netzwerkgeräten sind eine wichtige Datenquelle für das Netzwerkmonitoring. Diese Art SNMP-Kommunikation findet auf dem UDP Port 161 statt. Darüber hinaus kann der Agent den Manager unaufgefordert über Veränderungen eines Objektes informieren. Dadurch ist eine schnelle Fehlererkennung möglich. Diese, als Traps bezeichneten Meldungen, werden mittels UDP auf Port 162 übertragen.

Für die optimale Zusammenarbeit und Kommunikation zwischen dem Managementsystem und einem Gerät muss das Managementsystem wissen, welche MIB-Objekte vom Gerät bereitgestellt werden.

Aufgrund seiner Vielseitigkeit unterstützt SNMP, in Verbindung mit den MIBs, das Netzwerkmanagement bei der Überwachung, Fehlererkennung und Konfiguration

von Netzwerkkomponenten. SNMP gilt deshalb als das wichtigste und mächtigste Netzwerkmanagementwerkzeug.

Remote Monitoring (RMON) erweitert die durch SNMP genutzte MIBs um wichtige Objekte für das Monitoring des Netzwerks. Der *RMON*-Knoten wird innerhalb des *MIB-2* Knotens eingebunden und ist durch die OID 1.3.6.1.2.1.16. erreichbar. Die Objekte des RMON-Knotens werden in den RFC 2819 und 4502 definiert und darin in 19 Gruppen untergliedert. Obwohl diese Objekte eine sehr umfangreiche Basis zum geräteunabhängigen Monitoring des Netzwerks bilden, werden von vielen Hardwareherstellern meist nur die Gruppen *Statistics, History, Alarm* und *Event* implementiert. Die nicht implementierten Gruppen erlauben theoretisch die Analyse von Datenströmen im Netzwerk. Aufgrund dieser geringen Verbreitung kommt RMON eher selten zum Einsatz und spielt für das Netzwerkmanagement nur eine untergeordnete Rolle.

4.5 Datenstrom-Monitoring

Für ein umfassendes Netzwerkmanagement benötigt der Administrator zusammengefasste Informationen über die im Netzwerk fließenden Datenströme. Dafür analysiert ein entsprechend konfigurierter *Exporter* auf der Netzwerkkomponente die Datenpakete, welche vom Gerät empfangen bzw. versendet werden. Die Informationen über Quelle, Ziel, genutztes Netzwerkprotokoll und Datenvolumen eines Datenstromes werden in Tabellen zusammengefasst und in regelmäßigen Abständen an ein Netzwerkmanagementsystem (*Collector*) geschickt. Der Netzwerkadministrator kann aus diesen Daten erkennen, welche Netzwerkkomponenten zu einem bestimmten Zeitpunkt, wie viel Traffic, durch welche Anwendung verursacht haben. Diese Informationen sind wichtig für die Suche nach Ursachen von Performanceproblemen im Netzwerk oder zur Überwachung von Restriktionen für einzelne Anwendungen, Geräte oder Nutzer.

Cisco hat für diesen Zweck 1996 Netflow[10] veröffentlicht. Das Protokoll versendet die zusammengefassten Informationen mittels UDP oder SCTP[11] und erlaubt die freie Wahl des Netzwerkports. Netflow wird heute überwiegend in Version 5 eingesetzt. Die aktuelle Version 9 ist im RFC 3954 dokumentiert und stellt die neueste von Cisco entwickelte Version dar. Auch auf Geräten anderer Hersteller ist dieses Protokoll, mit verschiedenen Bezeichnungen, stark verbreitet. Aufgrund seines proprietären Ursprungs erhielt Netflow nicht den Status eines offiziellen

[10] Vgl. (4) S. 2

[11] Stream Control Transmission Protocol (RFC 4960)

Standards. Die IETF entwickelte deshalb aus Netflow v9 das *IPFIX*-Protokoll[12], um diese Technik offiziell zu standardisieren.

Im Jahr 2001 wurde sFlow als Alternative zu Netflow vorgestellt. Das im RFC 3176 beschriebene Protokoll verwendet zur Übertragung UDP mit dem Port 6343. Netflow und sFlow sind nicht miteinander kompatibel und erzeugen aufgrund ihrer verschiedenen Funktionsweisen teilweise unterschiedliche Ergebnisse für identische Datenströme[13].

[12] Internet Protocol Flow Information Export (RFC 5655).

[13] Vgl. (5)

5 Anforderungen an die Analyse

Für die umfangreiche und aussagekräftige Analyse der Netzwerkmanagementlösungen werden im Folgenden die Rahmenbedingungen festgelegt. Auf dieser Basis werden die Erwartungen an die Lösungen formuliert.

5.1 Vorgaben

Die Netzwerkmanagementlösung soll in einem von Windows-Systemen dominierten Netzwerk eines mittelständischen Unternehmens eingesetzt werden. Die Größe des Netzwerks umfasst typischerweise etwa 20 Switches für bis zu 500 Endgeräte und verfügt nur über eine geringe räumliche Ausdehnung. Aus diesem Grund wird ein *Collapsed Distribution and Core* als Zentrum des Netzwerks gebildet. Angesichts des geeigneten Funktionsumfangs und der hohen Leistungsfähigkeit eignen sich *Cisco Catalyst 3560-E* oder *HP ProCurve 5406zl* für den Einsatz in der Core-Ebene. Für die Aufgaben der Access-Ebene verfügen *HP ProCurve 2626* oder *Cisco Catalyst 2950* über einen entsprechenden Funktionsumfang.

Für die Analyse stehen *Cisco Catalyst 3560-E* und *HP ProCurve 2626* zur Verfügung. Dadurch kann die Unterstützung von verschiedenen Geräteherstellern durch die Managementlösungen untersucht werden.

Der für das Netzwerkmanagement notwendige Funktionsumfang dieser Geräte wird in Tabelle 1 zusammengefasst.

Features	Cisco Catalyst 3560-E	HP ProCurve 2626
Zugriff: **Telnet / SSHv2**	X / X	X / X
Datenübertragung: **TFTP / SFTP / SCP**	X / X / x	X / X / X
Logging: **Syslog**	X	X
SNMP: **v2c / v3** **MIBs**	X / X	X / X
RMON:	X (eingeschränkt)	X (eingeschränkt)
Datenstrom-Analyse: **Netflow / sflow**	- / -	- / -

Tabelle 1: Funktionsumfang der Netzwerkgeräte (Auswahl)

Keines der Geräte beherrscht Funktionen zur Analyse der Datenströme im Netzwerk. Um diese Funktion der Managementlösungen trotzdem analysieren zu können, kommt für diesen Test zusätzlich ein *Cisco 1841 Integrated Services Router* zum Einsatz. Dieser unterstützt die Netflow Versionen 1, 5 und 9.

5.2 Erwartungen

Im Fokus dieser Arbeit steht ausschließlich die Zusammenarbeit der Netzwerkmanagementlösungen mit der Switch-Technik eines Netzwerks. Das gesuchte Managementsystem sollte nach Möglichkeit Geräte verschiedener Hersteller unterstützen, um so einen universellen Einsatz zu ermöglichen. Die Unterstützung von Servern, Firewalls und anderen Netzwerkkomponenten ist wünschenswert, aber für diese Analyse kein relevantes Kriterium.

Des Weiteren soll die Netzwerkmanagementlösung in erster Linie die Ebene des *Element Management Layer* betrachten. Stellt sich während der Analyse heraus, dass eine Managementlösung zusätzliche Funktionen für eine der anderen Ebenen anbietet, soll eine auf dieser Arbeit aufbauende eigenständige Analyse durchgeführt werden. Die detaillierten Anforderungen an den Funktionsumfang der Managementlösungen werden im Abschnitt 5.3 näher beschrieben.

Außerdem soll eine überschaubare Managementlösung gefunden werden, die in ihrem Funktionsumfang zu den Anforderungen eines Netzwerks mittlerer Größe passt.

Weiterhin soll sich das Netzwerkmanagementsystem einfach in die Windows-basierte Server- und Client-Umgebung des Unternehmens eingliedern lassen. So kann der zusätzliche Aufwand für Wartung des Servers und die Schulung der Administratoren reduziert werden. Unter Windows installierbare Lösungen sind deshalb zu bevorzugen.

5.3 Detaillierte Anforderungen

Die in der Analyse zu untersuchenden Anforderungen orientieren sich überwiegend an den Bereichen des FCAPS-Modells.

Im Vorfeld der eigentlichen Analyse der Netzwerkmanagementfunktionen soll der Installationsprozess, die Benutzeroberfläche und die Dokumentation der Lösungen betrachtet werden. Außerdem ist die Einrichtungsmöglichkeit für ein regelmäßiges Backup die erste wichtige zu untersuchende Funktion.

Für das weitere Vorgehen werden die allgemeinen Einstellungen des Servers, insbesondere die Möglichkeiten zum Festlegen globaler Vorlagen für die SSH-

und SNMP-Authentifizierung an den Netzwerkkomponenten, untersucht. Der Einsatz dieser Vorlagen kann die weiteren Arbeitsschritte vereinfachen.

Um Netzwerkgeräte in eine Managementsoftware einzubinden, findet in der Regel ein Discovery-Prozess statt. Dieser durchsucht anhand zuvor festgelegter Bedingungen das Netzwerk nach Geräten, die verwaltet werden können. Es wird dabei erwartet, dass die Konfigurationsmöglichkeiten eine individuelle Anpassung an die Anforderungen verschiedener Netzwerke erlauben. Das umfasst neben den Discovery-Techniken auch die Zugriffsmöglichkeiten auf die Geräte sowie die Konfiguration einer individuellen, zeitgesteuerten Durchführung.

Im Anschluss an die Integration der Geräte soll deren Betriebssoftware und Gerätekonfiguration durch den Server gesichert werden. Für die Gerätekonfiguration muss eine planbare, regelmäßige Wiederholung dieses Vorgangs möglich sein. Außerdem muss auch die Wiederherstellung einer gesicherten Konfiguration auf ein beliebiges Gerät ermöglicht werden. Zusätzlich wäre ein automatischer Hinweis durch das Managementsystem hilfreich, wenn eine Veränderung in der Konfiguration eines Gerätes erkannt wurde.

Damit ein umfassendes Monitoring und Management für die Geräte ermöglicht werden kann, müssen verschiedene Dienste auf dem Gerät entsprechend konfiguriert werden. Dazu zählen beispielweise die Einrichtung des Managementsystems als Ziel für SNMP-Traps, Syslog-Meldungen und Netflow-Daten. Es ist anzunehmen, dass während des Netzwerkbetriebs weitere individuelle Konfigurationsänderungen an den Geräten durchgeführt werden müssen. Deshalb ist die Möglichkeit unverzichtbar, mittels individueller Befehle uneingeschränkt die Gerätekonfigurationen zu verändern. Darüber hinaus sind Vorlagen oder Konfigurations-Wizards für einzelne Anwendungsfälle wünschenswert.

Bei der Überwachung von sehr vielen Netzwerkgeräten kann der Überblick schnell verloren gehen. Deshalb werden Funktionen erwartet, die ein Organisieren der Geräte in individuellen Gruppen ermöglichen. Weiterhin sollte eine grafische Darstellung der Geräte und ihrer Verbindungen untereinander einen schnellen Überblick ermöglichen.

Für das Monitoring werden Attribute der Geräte regelmäßig abgerufen, statistisch aufbereitet und in geeigneter Form dargestellt, um dem Administrator einen Überblick über den Zustand des Netzwerks zu ermöglichen. Diese Attribute sollen hauptsächlich mittels SNMP abgefragt werden. Außerdem soll es möglich sein die Darstellung anzupassen, für jedes Gerät individuelle Attribute abzufragen und für jedes Attribut Grenzwerte festzulegen. Mit dem Überschreiten eines dieser festgelegten Grenzwerte soll der Administrator durch eine Alarmmeldung informiert werden.

Ein weiterer Bestandteil des Monitoring ist die Analyse der Datenströme im Netzwerk mittels Netflow. Mit dieser Technik können die Verursacher von Performance-Problemen ausfindig gemacht werden. Das Managementsystem muss dafür umfangreiche Filtermöglichkeiten anbieten. So soll genau erkannt werden, wie viel Datenverkehr über welches Netzwerkprotokoll ein bestimmtes Netzwerkgerät zu einem Ziel versendet hat. Für größere Netzwerkumgebungen ist es von Vorteil, wenn diese Filtereinstellungen abgespeichert werden können.

Im Laufe des Betriebs eines Netzwerks werden für unterschiedlichste Ereignisse Mitteilungen generiert. Diese stammen häufig von Syslog, SNMP oder dem Managementsystem selbst. Diese Meldungen können einen vergleichsweise unwichtigen Hinweis oder auch eine wichtige Fehlermeldung enthalten. Die Managementlösung muss eine zentrale Sammelstelle für alle Mitteilungen anbieten. Entsprechend individuell festlegbarer Regeln sollen diese Mitteilungen gefiltert werden. Besonders wichtige Meldungen müssen umgehend dem Administrator mitgeteilt werden.

Das Reporting soll zusammengefasste Informationen über den Status des Netzwerks oder ein bestimmtes Ereignis abspeichern. Diese Berichte unterstützen die höheren Managementebenen bei Ihren Entscheidungen über die Entwicklung des Netzwerks. Für diesen Zweck muss das Managementsystem in der Lage sein, aussagekräftige Berichte regelmäßig zu erzeugen. Nur mit einer umfangreichen Auswahl an Vorlagen sowie der Möglichkeit zum Erstellen von individuellen Berichten ist dies möglich.

Die Managementaufgaben aus dem *Accouting*-Bereich des FCAPS-Modells werden in dieser Arbeit nicht mit betrachtet. In diesem Anwendungsfall ist keine Abrechnung von Servicekosten für einzelne Netzwerknutzer vorgesehen. Auch die Nutzer und deren Zugriffsrechte sollen nicht durch das Managementsystem verwaltet werden. In Windows-Umgebungen wird diese Aufgabe meist durch entsprechende *Domain Controller* realisiert.

6 Programmauswahl

In diesem Kapitel wird anhand der im *Kapitel 5* beschriebenen Anforderungen an das Netzwerkmanagementsystem die Programmauswahl getroffen. Die Eignung einer Lösung ergibt sich aus der Analyse der Produktbeschreibungen auf den Webseiten der Hersteller.

Die am Markt vorhandenen Lösungen können grob in folgende drei Kategorien aufgeteilt werden:

- kommerzielle Lösungen von Hardwareherstellern,
- sonstige kommerzielle Lösungen und
- kostenfreie Lösungen.

Der Auswahlprozess soll nach Möglichkeit für jede Kategorie wenigstens eine Lösung aufzeigen, welche alle geforderten Aufgabenbereiche bedienen kann.

6.1 Kommerzielle Lösungen von Hardwareherstellern

Wie in *Abschnitt 5.1* beschrieben, kommen Geräte der Hersteller Cisco und HP für die Analyse der Programme zum Einsatz. Daher sollen vor allem deren Managementlösungen auf ihre Eignung geprüft werden.

6.1.1 HP

Mit der Übernahme des Hardwareherstellers *3Com Corporation* im Jahr 2010[14] wurde das Portfolio auch um deren Managementsoftware *Intelligent Management Center* (IMC) erweitert. Die Weiterentwicklung des bis dahin für das Management von HP-Geräten angeboten *ProCurve Manager Plus* (PCM+) wurde daraufhin zugunsten von IMC im Juli 2013 aufgegeben[15]. HP selber sieht das IMC als Lösung für den Element Management Layer und den *Network Node Manager i* (NNMi) als Lösung des darüber liegenden Network Management Layer an[16]. NNMI ist ein Bestandteil der von HP als *Network Management Center* bezeichneten Software-

[14] Vgl. (7)

[15] Vgl. (6)

[16] Vgl. (8) S.6

sammlung. Damit wird IMC als die geeignete Softwarelösung für das grundlegende Netzwerkmanagement angesehen und für die Analyse ausgewählt.

HP IMC der aktuellen Version 7 ist eine modular aufgebaute Managementlösung und wird als Basic-, Standard- oder Enterprise-Edition angeboten. Diese Editionen unterscheiden sich anhand der integrierten Module und der enthalten Lizenzen für die Anzahl der unterstützten Netzwerkkomponenten. Allerdings können sowohl fehlende Module als auch die Lizenzen nachträglich ergänzt werden. Da die Module in der Enterprise-Edition alle gestellten Anforderungen abdecken, wird diese Edition für die nachfolgende Analyse eingesetzt

IMC ist für den Betrieb auf *Red Hat Enterprise Linux* 5 und *Windows Server* 2003 Betriebssystemen, sowie deren Nachfolger, ausgelegt. Aufgrund der im *Abschnitt 5.2* festgelegten Anforderung wird IMC auf einem Windows Server getestet.

Für die Informationen, die das IMC während des Betriebes sammelt, wird eine Datenbank benötigt. Dabei unterstützt IMC einen *Microsoft SQL Server* ab Version *2005 SP4* für den Betrieb unter Windows und einen *Oracle 11g*-Datenbankserver für den Betrieb unter Linux. Alternativ kann für beide Betriebssysteme auch ein *MySQL Enterprise Server* ab Version *5.1* eingesetzt werden.

HP empfiehlt für die Nutzung von IMC mit bis zu 50 Endgeräten folgende Mindestanforderungen an die Hardware[17]:

- Zweikern-Prozessor mit 3GHz,
- 4 GB Arbeitsspeicher,
- 100 GB Festplattenspeicher.

Die Arbeit mit dem IMC erfolgt über einen Webbrowser. Um Darstellungsfehler bei Diagrammen und Grafiken zu vermeiden, ist mindestens der *Internet Explorer 9* oder ein gleichwertiger Browser notwendig. Es kommen HTML5 und Java-Plugins zum Einsatz.

6.1.2 Cisco

Cisco Prime Infrastructure (CPI) ist die aktuelle Lösung die Cisco für das Netzwerkmanagement seiner Geräte anbietet. Diese Lösung ist das Ergebnis des Integrationsprozesses von *Cisco Prime LAN Management Solution* (LMS) in *Cisco Prime Network Control System* (NCS)[18]. Das Einsatzgebiet von Prime LMS war

[17] Vgl. (11)

[18] Vgl. (14) S. 6

das Management und Monitoring von kabelgebunden Netzwerken und deren Geräte. Prime NCS hingegen bot umfangreiche Möglichkeiten für das Management von drahtlosen Netzwerken. Mit CPI 2.0 ist diese Integration zum größten Teil abgeschlossen[19] und damit die Unterstützung für kabelgebundene Netzwerktechnik offiziell gegeben. Cisco sieht CPI als Komplettpaket für ein umfassendes Lifecycle-Management von kabelgebundenen und drahtlosen Netzwerken[20].

Von den drei durch Cisco angeboten CPI-Editionen kommt die Express-Edition für die Analyse zum Einsatz. Die Editionen unterscheiden sich nur in der Anzahl der unterstützten Netzwerkkomponenten. Dabei bildet die Express-Edition mit bis zu 300 Komponenten den Einstieg[21].

Für den Betrieb in einer virtualisierten Serverumgebung steht CPI als OVA[22] bereit. Dabei handelt es sich um das Abbild (Image) eines fertig installierten und konfigurierten Servers, das sofort einsatzbereit ist. Zusätzlich wird auch eine Installation für physische Computer angeboten. Als Betriebssystem nutzt CPI ein *Red Hat Enterprise Linux*, was den festgelegten Anforderungen widerspricht. Allerdings kommt der Administrator weder während der Installation des OVAs noch während des Betriebs von CPI mit dem Linux in Kontakt. Deshalb ist in diesem Fall eine Ausnahmeregelung zulässig.

CPI speichert die während des Betriebes gesammelten Informationen in einer Oracle Datenbank, die bereits im OVA integriert ist.

Cisco stellt für den Betrieb seiner CPI-Lösung die umfangreichsten Hardwareanforderungen an den Server. Für die genutzte Express Edition werden folgende Mindestanforderung benötigt:

- virtueller Vierkern-Prozessor,
- 12 GB Arbeitsspeicher,
- 300 GB Festplattenspeicher.

Auch bei CPI erfolgt die administrative Arbeit über den Webbrowser. Für die korrekte Darstellung wird ein Browser mit *Flash Player* Plug-In benötigt.

---

[19] Vgl. (12)

[20] Vgl. (13)

[21] Vgl. (15)

[22] Open Virtual Appliances (entsprechend dem *Open Virtualization Format*)

6.2 Sonstige kommerzielle Lösungen

Als alternative kommerzielle Lösungen sollten vorrangig Produkte betrachtet werden, die sich bereits bei Kunden der IBH im Einsatz befinden oder mit denen Mitarbeiter der IBH bereits erste Erfahrungen gesammelt haben. Zu diesen Lösungen zählen unter anderem *InterMapper (Help/Systems, LLC)* und *PRTG Network Monitor (Paessler AG)*. Die Vorbetrachtung ergab jedoch, dass diese Programme hauptsächlich nur Monitoringaufgaben erfüllen. Ein umfassendes Konfigurationsmanagement ist nicht enthalten[23].

Auch unter den anderen mehr oder weniger weit verbreiteten Managementlösungen ist kaum eine für diese Analyse geeignete Lösung zu finden. Einige wenige Lösungen, wie z.B. *IBM Tivoli Management Framework*, richten sich aufgrund ihres Aufbaus und ihrer Funktionsweise an Unternehmen mit sehr großen Netzwerken und komplexen Management-Prozessen. Die meisten Lösungen ähneln allerdings den bereits erwähnten Intermapper bzw. PRTG und bieten hauptsächlich Funktionen zur Überwachung der unterschiedlichsten Netzwerkkomponenten an. Der Grund für die fehlende Funktion des Konfigurationsmanagements besteht in der individuellen Kommandosammlung der verschiedenen Geräte.

Mit Solarwinds konnte ein Anbieter gefunden werden, der das Konfigurationsmanagement trotz des hohen Aufwandes in seine Lösung integriert hat. Die *Orion* genannte Managementlösung ist modular aufgebaut, so dass für jeden Aufgabenbereich ein eigenständiges Produkt zur Verfügung steht. Anhand der Anforderungen, die ein Unternehmen an das Netzwerkmanagement stellt, kann eine individuelle Lösung zusammengestellt werden.

Für die Analyse werden folgende Produkte eingesetzt:

- Orion *Network Performance Monitor* v10.6.0 (NPM),
- Orion *Network Configuration Manager* v7.2.2 (NCM),
- Orion *NetFlow Traffic Analyzer* v4.0.0 (NTA).

Diese Programme sind nur für Microsoft Windows Server 2003 (und neuer) verfügbar. Die im laufenden Betrieb gesammelten Daten werden in einem Microsoft SQL Server 2005 SP1 (oder neuer) gespeichert. Als Webserver kommt das IIS[24] Feature des Windows Server zum Einsatz.

---

[23] Vgl. (17) und Vgl. (16)

[24] Microsoft Internet Information Services – Webserver von Microsoft für Windows Server Systeme

Von Solarwinds werden nur die minimalen Hardwareanforderungen veröffentlicht:

- Zweikern-Prozessor mit 3GHz,
- 3 GB Arbeitsspeicher,
- 20 GB Festplattenspeicher.

Hinweise auf die Entwicklung der benötigten Ressourcen bei einer größeren Anzahl verwalteter Geräte gibt es nicht.

Wie bereits CPI und IMC werden auch die Orion-Module durch eine gemeinsame Weboberfläche bedient.

6.3 Kostenfreie Lösungen

Im Bereich der freien und kostenlosen Netzwerkmanagementlösungen sind *Nagios Core 4* und *OpenNMS 1.12* die bekanntesten Vertreter. Allerdings entsprechen beide Lösungen in mehreren wichtigen Punkten nicht den Kriterien, um an der Analyse teilnehmen zu können.

Das Hauptproblem dieser beiden Systeme liegt darin begründet, dass sie nur Aufgaben des Netzwerkmonitorings abdecken. Das Konfigurationsmanagement der verwalteten Netzwerkgeräte ist nicht vorgesehen[25].

Bei Nagios kommt hinzu, dass es für den Betrieb auf Linux Plattformen entwickelt wurde und die Einrichtung des Managementsystems überwiegend durch manuelles Anpassen von Textdateien durch den Netzwerkadministrator erfolgt. Da Nagios eine sehr flexible und individuell optimierbare Plattform ist, besteht ein vielseitiges Angebot an Plugins zur Erweiterung des Funktionsumfanges. Es ist anzunehmen, dass auch Plugins für eine webbasierte Konfiguration des Nagios-Systems existieren. Allerdings soll die Suche nach einer die Anforderungen erfüllenden Plugin-Sammlung nicht Inhalt der Analyse sein.

Im Gegensatz zu Nagios ist OpenNMS auch für den Betrieb auf einem Windows System geeignet. Die Entwickler von OpenNMS sind außerdem bemüht, die schnelle Konfiguration und Inbetriebnahme über das Webinterface zu ermöglichen. Leider sind noch viele Funktionen genauso wie bei Nagios nur durch manuelles Eingreifen in die Konfigurationsdateien möglich.

[25] Vgl. (18) und Vgl. (19)

Auch unter den anderen kostenfreien Netzwerkmanagement-Werkzeugen konnte keine Lösung gefunden werden, die alle benötigten Funktionen in einem System vereint. Sehr viele dieser Werkzeuge bedienen nur punktuell einzelne Aufgaben des Netzwerkmanagements.

7 Erkenntnisse der Analyse

Dieses Kapitel befasst sich mit Erkenntnissen und Beobachtungen, die während der Analyse der gewählten Netzwerkmanagementlösungen erlangt wurden. Dabei sollen diese Ergebnisse entsprechend ihrer inhaltlichen Nähe zueinander, in gemeinsamen Abschnitten aufgeführt werden.

7.1 Installation und allgemeine Inbetriebnahme

Für diesen Teil der Analyse wurden die Managementlösungen installiert und anschließend das Userinterface sowie die Dokumentation der Software betrachtet. Im Vorfeld der eigentlichen Analyse der Managementfunktionen erfolgte eine Untersuchung der Backup-Funktionalität.

7.1.1 IMC

Für die Installation von IMC wurde ein Windows Server 2008 R2 verwendet. Der Installationsprozess wird durch das Skript *install.bat* gestartet. An gleicher Stelle befindet sich ein weiteres Skript zum Installieren eines sekundären Servers für den hochverfügbaren Einsatz von IMC. Die Installation findet in zwei Schritten statt. Zu Beginn werden der *Intelligent Deployment Monitoring Agent* installiert und die IMC-Module im Programmordner bereitgestellt. Im zweiten Schritt wird vom Administrator im installierten *Agent* die Auswahl getroffen, welche Module für den IMC-Server installiert werden.

Für die weitere Analyse wurden anhand der Beschreibung folgende Management-Module ausgewählt:

- Resource Management,
- Alarm Management,
- Syslog Management,
- Report Management,
- Performance Management,
- Network Asset Management,
- Network Traffic Analyser (NTA),
- Intelligent Configuration Center,
- NE Management,
- VLAN Management,
- ACL Management.

Während des Installationsprozesses muss ausgewählt werden, welcher Datenbank-Server durch IMC verwendet werden soll. Sollte lokal keine Datenbanksoftware existieren, bietet IMC die Installation eines *Microsoft SQL Server 2008 R2 (Express)* an und ermöglicht so eine unkomplizierte Inbetriebnahme des IMC-Servers. Allerdings ist zu beachten, dass der nachträgliche Wechsel auf eine neue oder andere Datenbank mit einem sehr hohen Aufwand verbunden ist. Genauso wie die enthaltene Datenbankserver-Installation ist auch eine Java-Laufzeitumgebung Bestandteil der Installation. Allerdings werden diese Java-Komponenten nicht im System installiert, sondern nur in den IMC-Programmordner verschoben. Außerdem kann der http/https[26] Port des Webservers während der Installation individuell festgelegt werden. Diese Auswahl lässt sich nachträglich nur durch das Skript *setwebport.bat* ändern ([Programmordner]\client\bin). Nach dem Abschluss der Installation und dem Start des IMC-Servers, kann IMC über einen Webbrowser erreicht werden.

Anhand der installierten Module wird die IMC-Weboberfläche in Gruppen eingeteilt. Dabei sind unter *Resource* die Geräteverwaltungs- und Monitoring-Funktionen zusammengefasst. Die Gerätekonfigurations- und Sicherungsfunktionen sowie das NTA-Modul sind im Bereich *Service* angesiedelt. Die Funktionen der übrigen Gruppen *Alarm, Report* und *Administration* sind selbsterklärend. Am unteren Rand der Weboberfläche befindet sich eine Informationsleiste, die stets angezeigt wird und über die Anzahl der erkannten Probleme informiert.

Die Dokumentation ist vergleichsweise sparsam mit zusätzlichen Informationen über bestimmte Einstellungsmöglichkeiten versehen. Daher ist es teilweise schwer herauszufinden, welche Konfiguration die richtige für eine bestimmte Situation ist. Hilfreich ist jedoch, dass die Dokumentation in Form einer Hilfefunktion auf der gesamten Weboberfläche zur Verfügung steht.

Das einfache Backup des Datenbank-Inhaltes und der im Dateisystem gesicherten Informationen über die Netzwerkkomponenten erfolgt durch den *Intelligent Deployment Monitoring Agent.* Dieser bietet alle Funktionen für das einmalige oder regelmäßige Backup sowie zur Wiederherstellung an. Außerdem kann vom IMC-Server ein vollständiges Backup angelegt werden. Dafür muss das in dem Installationsordner enthaltene Skript *backup.bat* ausgeführt *werden*. Dieser Backup-Assistent verpackt den gesamten IMC-Programmordner in ein Dateiarchiv (*.zip). Zum Wiederherstellen reicht das Entpacken des Archives.

[26] Hypertext Transfer Protocol (Secure)

7.1.2 CPI

Für die Installation von CPI muss aus der bereitgestellten OVA-Vorlage eine virtuelle Maschine erzeugt werden[27]. Der erste Start des so installierten CPI-Servers führt den Administrator zum Konfigurationssetup, das die Netzwerkeinstellungen abfragt und einen ersten Benutzer anlegt. Außerdem besteht noch die Möglichkeit der Konfiguration eines sekundären Servers für den hochverfügbaren Einsatz. Der die Konfiguration abschließende Neustart des Servers dauerte über 30 Minuten. Allerdings dauert auch ein normaler Neustart des Servers bereits 20 Minuten. Auf den fertig konfigurierten Server kann ab diesem Zeitpunkt über SSH zugegriffen werden. Die so erreichbare Kommandozeile ähnelt der eines Cisco IOS[28] Gerätes. Auf das eigentliche Linux, welches die Basis des Servers bildet, ist im laufenden Betrieb kein Zugriff möglich. Das gilt ebenfalls für die meisten Dateien, die sich auf dem Server befinden. Eine Ausnahme bilden dabei die lokal gesicherten Backups und andere Repositories. Die Weboberfläche des CPI ist nach dem Abschluss der Konfiguration ebenfalls verfügbar.

Cisco bietet dem Nutzer des CPI die Möglichkeit, zwischen zwei Ansichten der Weboberfläche zu wählen. Im standardmäßig ausgewählt *Lifecycle Theme* werden die Funktionen in den fünf Gruppen *Design, Deploy, Operate, Report* und *Administration* organisiert. Wie an der Bezeichnung dieser Ansicht erkennbar, orientiert sich die Aufteilung an den aufeinander aufbauenden Managementprozessen. Dementsprechend können unter *Design* die Konfigurationsvorlagen erstellt und unter *Deploy* angewendet werden. Die Gruppe *Operate* bietet alle Funktionen für die Organisation und Überwachung des Netzwerks. Die Funktionen der Gruppen *Report* und *Administration* erklären sich von selbst. Alternativ zum *Lifecycle Theme* existiert das *Classic Theme,* welches auf die Cisco Prime NCS Ursprünge zurückgeht. Diese Ansicht ist darauf ausgelegt, ein drahtloses Netzwerk zu managen. Aus diesem Grund sind viele Funktionen, die im *Lifecycle Theme* angeboten werden, hier nicht verfügbar. Deshalb wird das *Lifecycle Theme* für die Analyse der CPI-Funktionalität verwendet. Gemeinsamkeiten dieser beiden Ansichten sind die sehr umfangreichen, allgemeinen Einstellungsmöglichkeiten für den Server sowie die am unteren Rand der Website angedockte Informationsleiste. Diese Leiste ist permanent eingeblendet und informiert über die erkannten Probleme des Netzwerks.

Für jede der beiden Ansichten wird eine eigenständige Dokumentation angeboten. Die Dokumentation des *Classic Theme* entspricht dabei dem Dreifachen der Lifecycle Theme Dokumentation. Die Dokumentationen selbst sind meist sehr aus-

[27] Mit Hilfe von VMware vSphere

[28] Verbreitetes Betriebssystem für Router und Switches von Cisco

führlich und erlauben so ein schnelleres Verständnis für eine beschriebene Funktion und deren Arbeitsweise. Zusätzlich ist die Dokumentation in der Weboberfläche eingebunden.

In der Standardkonfiguration ist das Erstellen von Backups bereits aktiviert und wird einmal pro Woche durchgeführt. Von den lokal auf dem Server abgelegten Backups werden nur die zwei neuesten Versionen aufbewahrt. Zwar kann dieser Wert erweitert werden, aber das birgt das Risiko, dass nach einer gewissen Laufzeit die gesamte Festplattenkapazität mit Backups belegt ist. Um die Backups für längere Zeiträume zu sichern, kann ein FTP-Server als Ziel eingerichtet werden. Der Backup-Vorgang wird in der Weboberfläche als *Background Task* angelegt. Alternativ kann diese Konfiguration auch über die Kommandozeile durchgeführt werden. Das Wiederherstellen eines Backups ist in jedem Fall nur über die Kommandozeile möglich.

7.1.3 Orion

Auch die Komponenten der Managementlösung Orion werden auf einem Windows Server 2008 R2 installiert. Da der NPM das Kernmodul des Systems enthält, wird mit der Installation dieser Komponente begonnen. Darauf aufbauend werden das NCM- und das NTA-Modul installiert. Während der Installation wird geprüft, ob das *.NET Framework* (3.5SP1 und 4.0) sowie *Visual C++ Redistributable* (2008 und 2010) vorhanden sind. Trifft dies nicht zu, werden diese Komponenten automatisch installiert. Außerdem installiert jede der drei Komponenten auch eine Reihe von Werkzeugen, die das Verwalten des Servers unterstützen. Die Installation von NPM beinhaltet zusätzlich noch die Installation der Datenbank und des Webservers. Dabei kann der mitgelieferte *Microsoft SQL Servers 2008 R2 (Express)* installiert oder ein bereits existierender Datenbankserver ausgewählt werden. Für die Installation des Webservers greift NPM auf das *IIS*-Modul des Windows Servers zurück. Dabei wird der http Port 8787 vorgegeben. Allerdings erlaubt der mitgelieferte Konfigurations-Assistent nachträgliche Änderungen an den Datenbank-, Webserver- und Service-Einstellungen. Unter den analysierten Programmen bietet NPM als einziges die Installation einer deutschsprachigen Benutzeroberfläche an.

Nach der Installation der einzelnen Komponenten sind die entsprechenden Funktionen in vier Kategorien erreichbar. Die *Startseite* bildet dabei den zentralen Punkt für die Ereignis-Überwachung. In der Kategorie *Netzwerk* werden alle statistischen Informationen der Netzwerkkomponenten zusammengefasst. Die Funktionen der restlichen beiden Gruppen *Konfiguration* und *Netflow* ergeben sich aus der Gruppenbezeichnung. Im Vergleich zu den anderen Managementlösungen bietet Orion nur wenige Punkte innerhalb dieser Kategorien an. Allerdings scheinen alle für die Funktionsanalyse benötigten Punkte vorhanden zu sein.

Die mitgelieferte Dokumentation beschreibt das Programm ausführlich. Ergänzend dazu kann über die Orion-Weboberfläche auf einen Schulungsbereich zugegriffen werden. Dieser enthält eine große Auswahl an Dokumenten und Video-Tutorials, die den Umgang mit Orion ausführlich erklären. Neben dem Schulungsbereich ist auch ein entsprechendes Forum über die Weboberfläche erreichbar.

Eine umfassende Backup-Funktionalität bietet Orion nicht an. Es wird lediglich das Werkzeug *Datenbank-Manager* bereitgestellt. Dieses gibt dem Nutzer einen direkten Zugriff auf die Datenbank und ermöglicht so das Erstellen und Wiederherstellen von Backups. Allerdings verfügt der installierte Datenbank-Manager nicht über die in der Dokumentation aufgeführten und in Video-Tutorials gezeigten Funktionen. Dabei ist es unklar, ob dieser Unterschied nur eine Einschränkung der genutzten Test-Lizenz ist oder ob ein Fehler im Programm vorliegt. Alternativ wird in der Dokumentation auch das Vorgehen mithilfe des *Microsoft SQL Server Management Studio* beschrieben. Ein regelmäßiges automatisches Backup der Datenbank ist mit beiden Programmen nicht möglich.

7.1.4 Resümee

Bei keiner Managementlösung bereitete der Installationsprozess Schwierigkeiten. Dank der eingesetzten Wizards ist der gesamte Installationsprozess selbsterklärend. Lediglich für die Einrichtung des Datenbankservers bei IMC und Orion sind Kenntnisse über die Funktionsweise von *Microsoft SQL Datenbanken* hilfreich.

CPI konnte aufgrund des speziellen Installationsvorgangs am einfachsten in Betrieb genommen werden. Durch das abgeschottete Betriebssystem dieser Lösung ist kaum Wartungsaufwand zu erwarten.

Aufgrund der Komplexität der Systeme wird viel Zeit benötigt, um sich in der jeweiligen Weboberfläche zurechtzufinden. Während bei CPI die ungewohnte Struktur in Verbindung mit unzähligen Funktionen zu Schwierigkeiten führt, liegt das Problem der Orion-Oberfläche in einem nicht durchdachten Aufbau.

Es ist zu befürchten, dass aufgrund des fehlenden automatischen Backup-Prozesses die Sicherung des Orion-Servers mit der Zeit vernachlässigt wird. Mit den planbaren Backups zeigen HP und Cisco, dass solch eine hilfreiche Funktion einfach umgesetzt werden kann.

7.2 Grundeinstellungen und Discovery

In diesem Abschnitt wird betrachtet, wie die Managementlösungen die Discovery-Funktion umsetzen. Im Vorfeld sollen globale Einstellungen für SNMP, SSH und Mail untersucht werden.

7.2.1 IMC

Das IMC bietet in den Systemeinstellungen an, Vorlagen für SSH, Telnet und SNMP Authentifizierungen anzulegen. Unter anderem kann hier der Nutzerzugriff auf das IMC-System geregelt und ein Mail-Server eingestellt werden.

Für das Einbinden von Netzwerkkomponenten in das IMC stehen mehrere Auto-Discovery Optionen bereit. In der Grundeinstellung wird ein IP-Adressbereich festgelegt, in dem nach Netzwerkkomponenten gesucht wird. Je nach Größe des gewählten Bereiches dauert dieser Vorgang entsprechend lang. Bei diesem Verfahren erlaubt IMC lediglich das Festlegen von SNMPv2 Communities und Telnet Login Daten. Erst der erweiterte Discovery-Modus bietet mit SNMPv3 und SSH mehr Flexibilität. Dabei können die global angelegten SSH- und SNMP-Vorlagen eingesetzt werden. Auf den Einsatz von Telnet sollte prinzipiell verzichtet werden. Der erweitertet Discovery-Modus ermöglicht außerdem, das Netzwerk anhand von Routing-, ARP-, VPN- oder PPP-Informationen[29] nach neuen Geräten zu durchsuchen. Dafür muss anstelle eines IP-Bereichs nur die IP eines Netzwerkgeräts angegeben werden. Sobald der Discovery-Prozess Zugriff auf dieses Gerät (Seed-Device) erlangt hat, können die Informationen über andere vorhandene Geräte ausgelesen werden. Über den sogenannten Hop-Counter kann festgelegt werden, wie oft dieser Vorgang mit den neu gefunden Geräten wiederholt werden soll.

Die Cisco- und HP-Geräte konnten ohne Probleme erkannt und in das IMC eingebunden werden. Für beide Gerätetypen werden umfangreiche Statusinformationen und Konfigurationsmöglichkeiten bereitgestellt. Insgesamt kann IMC mehr als 6.300 unterschiedliche Gerätetypen erkennen. Es kann allerdings nicht abgeschätzt werden, in welchem Umfang das IMC deren Funktionen unterstützt.

7.2.2 CPI

Cisco hat konsequent alle administrativen Einstellungen für CPI an einem Punkt im System vereint. Allerdings ermöglicht keine Einstellung das Erzeugen einer Authentifizierungsvorlage, die im Discovery-Prozess verwendet werden kann. Unter den sonstigen Einstellungen sind beispielsweise Mail- und Alarm/Event-Optionen zu finden.

Die Auto-Discovery Funktion im CPI bietet die umfangreichsten Einstellungsmöglichkeiten. Neben den von IMC bekannten Optionen kann noch das *Cisco Discovery Protocol* (CDP) und das *Link Layer Discovery Protocol* (LLDP) verwendet

[29] Address Resolution Protocol / Virtual Private Network / Point-to-Point Protocol

werden. Beide Protokolle kommen auf Netzwerkgeräten zum Einsatz, um benachbarte Geräte zu erkennen.

Durch den Discovery-Prozess wurden nur die Cisco Switches erfolgreich vom CPI erkannt. Entsprechend der offiziellen Geräteunterstützung sollten auch Nicht-Cisco-Geräte minimal verwaltet werden können. Dazu zählt das Sichern von Konfiguration und Gerätesoftware sowie das Monitoring der Geräteverfügbarkeit. Das gelang allerdings nicht mit den verwendeten HP-Geräten. Von den Geräten wurde nur der Hostname korrekt ausgelesen. Als Ursache wird eine falsche SNMP-Konfiguration genannt. Dieser Fehler konnte auch nicht durch das manuelle Hinzufügen der Geräte behoben werden. Daraus resultiert der Ausschluss der HP-Geräte von der weiteren CPI-Analyse.

7.2.3 Orion

Da die Orion-Lösung aus drei Programmen besteht, sind die Systemeinstellungen auch auf mehreren getrennten Seiten aufgeführt. Die Präsentation dieser Einstellungen ist zudem recht überladen, so dass die Orientierung unnötig erschwert wird. Die Einrichtung einer globalen SSH-Authentifikation ist möglich, wird jedoch für den Discovery-Prozess nicht benötigt.

Orion bietet für das Auto-Discovery nur die Suche in IP-Bereichen an. Für den Zugriff auf die gefunden Switches steht nur SNMP zur Verfügung. Die anderen Optionen sind nur für das Discovery von Server-Umgebungen gedacht.

Ähnlich wie IMC wirbt Orion mit der herstellerübergreifenden Geräteunterstützung. Mit den HP- und Cisco-Geräten konnten keine Probleme oder Einschränkungen festgestellt werden.

7.2.4 Resümee

Die von HP und Cisco angebotenen Konfigurationsmöglichkeiten des Discovery-Prozesses sind sehr umfangreich und ermöglichen dadurch ein für jedes Netzwerk optimales Discovery. Die Implementation von Solarwinds dürfte hingegen überwiegend in einfach aufgebauten Netzwerken Anwendung finden. Gemeinsam haben alle drei Umsetzungen, dass eine automatisierte regelmäßige Durchführung des Discovery eingerichtet werden kann.

7.3 Konfiguration der Geräte

Für die vollständige Zusammenarbeit zwischen den Netzwerkgeräten und den Managementlösungen müssen Syslog, SNMP Traps und Netflow durch die Pro-

gramme konfiguriert werden. Außerdem ist das Backup der Gerätesoftware und der Gerätekonfiguration ein zu betrachtender Punkt.

7.3.1 IMC

Das Sichern der aktuellen Gerätesoftware auf dem IMC-Server war mit allen Geräten erfolgreich. Auch das Kopieren einer neueren Software auf die Geräte gelang ohne erkennbare Zwischenfälle. Allerdings musste später festgestellt werden, dass bei den Cisco-Switches der Inhalt des internen Speichers vor dem Kopieren gelöscht wurde. Dort abgelegte Konfigurationsdateien gingen dabei verloren. Das IMC bietet die Möglichkeit, die passende Gerätesoftware für HP-Geräte direkt von einem HP-Server herunterzuladen.

Probleme entstanden ebenfalls bei dem Backup der Gerätekonfiguration von den HP-Switches. Obwohl für diese Geräte der Login-Typ auf SSH eingestellt war, versuchte das IMC manchmal eine Verbindung mit Telnet aufzubauen, um den Kopiervorgang zu starten. Da keine Login-Daten für Telnet hinterlegt waren, scheiterten diese Versuche. Ein ähnlicher Effekt entstand, als der Datentransfer-Modus von TFTP auf SCP umgestellt wurde. Das gleiche Vorgehen auf einem anderen IMC-Server erzeugte hingegen keine Fehler. Das Backup der Gerätekonfiguration kann als regelmäßiger Vorgang eingerichtet werden.

IMC bietet eine Reihe von Templates und Vorlagen für die Konfiguration an, allerdings sind diese nicht mit den getesteten Cisco- und HP- Geräten kompatibel. Deshalb wurden die benötigten Funktionen in einem neuen Skript angelegt. Für das Anwenden der Skripte stellt das IMC einen *Deployment Guide* bereit. Dieser bietet zusätzliche Funktionen, wie z.B. das Speichern der Gerätekonfiguration nach erfolgreichem Deploy eines Skripts. Diese Funktion wurde für Cisco-Geräte mittels SSH und für HP-Geräte mit Telnet durchgeführt. Die Ursache für diesen Effekt ist unklar. Eine manuelle Beeinflussung dieser Einstellungen ist über das Webinterface nicht möglich.

Neben der direkten Gerätekonfiguration anhand von Vorlagen stehen für die Konfiguration von VLAN (Virtual Local Area Network) und ACL (Access Control List) entsprechende Module bereit. Diese bieten detaillierte Vorgehensweisen für die Konfiguration dieser Funktionen an und vermitteln den Eindruck, dass deren Funktionsumfang bereits den Ansprüchen des *Network Management Layer* entspricht.

7.3.2 CPI

Das Lifecycle Theme von CPI ist optimal für diese Konfigurationsaufgaben geschaffen. Unter *Feature Design* wird von Cisco eine Vielzahl an Konfigurationsvorlagen angeboten. Das Anpassen dieser Vorlagen gestaltet sich als schwierig, da

diese in der Regel aus dem eigentlichen Skript und einem Formular für die Benutzereingaben bestehen. Für Funktionen, die nicht durch eine Vorlage konfiguriert werden können, kann eine leere CLI-Vorlage für die individuelle Konfiguration genutzt werden. Anhand der Vorlagen wird unter *Configuration Tasks* der Deploy-Vorgang durchgeführt.

Die Sicherung und Wiederherstellung der Gerätekonfiguration und der Gerätesoftware findet im *Device Work Center* statt. Außerdem können an dieser Stelle auch die Gerätekonfigurationen verglichen werden. Im Rahmen der Softwareverwaltung kann CPI von der Cisco-Website verfügbare Versionen der Gerätesoftware herunterladen.

Während dieser Analysen sind keine Probleme oder Fehler aufgetreten.

7.3.3 Orion

Das NCM-Modul stellt in erster Linie eine Reihe von Grundfunktionen für das Sichern und Vergleichen von Konfigurationen bereit. Außerdem können damit einfache Konfigurationen ausgeführt und regelmäßiges automatisches Backup der Gerätekonfigurationen eingerichtet werden.

Weiterhin wird eine Sammlung von Vorlagen bereitgestellt. Weniger als zehn dieser Vorlagen sind bereits verfügbar, weitere etwa 67 Vorlagen können durch Orion direkt aus einem Forum heruntergeladen[30] werden. Der überwiegende Teil der verfügbaren Vorlagen beschreibt Funktionen für Cisco-Geräte. Die Änderung oder Erstellung einer Vorlage erfordert einen hohen Aufwand. Die Vorlagen enthalten nicht nur die einfachen Befehle, sondern ein umfangreiches Skript, aus dem ein Wizard zum Abfragen von Variablen entsteht. Keines der mitinstallierten Werkzeuge kann diese Aufgabe automatisieren.

Orion bietet keine Funktionen zum Download und Archivieren der Gerätesoftware an.

7.3.4 Resümee

Die Eigenheiten von IMC im Umgang mit HP-Geräten sind überraschend. Nach drei Jahren Entwicklung durch HP müsste die fehlerfreie und umfassende Unterstützung der eigenen Hardware sichergestellt sein. Im direkten Vergleich dazu, hat CPI keine Probleme bei der Kommunikation mit Cisco-Geräten.

---

[30] Login erforderlich (http://thwack.solarwinds.com/)

Im Vergleich zu CPI und IMC bietet Orion den schlechtesten Leistungsumfang. Die fehlende Funktion zum Sichern und Archivieren der Gerätesoftware, sowie der aufwendige Erstellvorgang für individuelle Vorlagen, schmälern den Nutzwert des NCM-Moduls beträchtlich. Selbst die Einbeziehung eines Forums, um weitere Vorlagen bereitzustellen, ändert an dem Resultat nichts.

7.4 Monitoring und Datenstromanalyse

Dieser Abschnitt betrachtet die Einstellungsmöglichkeiten für Monitoring-Attribute sowie die Darstellung der daraus gewonnenen Informationen. Weiterhin werden die Möglichkeiten zur Datenstromanalyse unter der Verwendung von Netflow betrachtet.

7.4.1 IMC

Die verwalteten Geräte organisiert das IMC wahlweise anhand der Gerätekategorie, dem IP-Adressbereich oder einer individuell angelegten Struktur. Außerdem kann mit Hilfe der Topologie-Ansicht der Aufbau des Netzwerks und die Verkabelung zwischen den einzelnen Geräten sehr gut verdeutlicht werden. Diese Darstellung ist flexibel anpassbar und zeigt die wichtigsten Statusinformationen für Geräte und Verbindungen an.

Das IMC bietet eine sehr umfangreiche Auswahl an überwachbaren Attributen, deren Abfrage für jedes Gerät individuell eingerichtet werden kann. Außerdem sind für jedes Attribut zwei individuelle Grenzwerte einstellbar. Anhand dieser Werte werden Alarm-Meldungen generiert.

Für die übersichtliche Darstellung der wichtigsten Informationen stehen im IMC Dashboards sowie individuelle Ansichten zur Verfügung. Die darauf angezeigten Diagramme und Darstellungen können beliebig angeordnet und skaliert werden.

Das für die Datenstromanalyse genutzte NTA-Modul erlaubt die Analyse von Netflow- und sflow-Daten. Der Port auf dem der Server Netflow-Daten erwartet, kann individuell gewählt werden. Nach der entsprechenden Konfiguration des Servers stehen die aufbereiteten Datenströme zur Verfügung. Dabei werden diese Daten in den Ansichten *Source, Destination, Application* oder *Session* dargestellt. Durch die Verknüpfungen zwischen den einzelnen Ansichten wird die Analyse und Suche nach einem bestimmten Verursacher erleichtert. Alternativ ist das manuelle Festlegen von Filtern möglich. Eine solche Auswahl lässt sich nicht für eine spätere Wiederholung der Suche abspeichern. Zu Darstellungen auf einem Dashboard bietet das NTA-Modul eine Reihe von TopN Statistik-Ansichten an.

7.4.2 CPI

Das CPI ermöglicht das Organisieren der Geräte entsprechend ihres Gerätetyps oder anhand einer benutzerdefinierten Ordnerstruktur. Eine Topologie-Ansicht, wie von IMC bekannt, ist nicht verfügbar. Lediglich für die Darstellung von Wireless Access-Point und deren Sendeleistung kommt eine vergleichbare Lösung zum Einsatz.

Im Vergleich zum IMC können im CPI weniger Monitoring-Attribute eingerichtet und überwacht werden. Die Darstellung aller Monitoring- und Netflow-Daten erfolgt in der gemeinsamen Gruppe *Monitoring Dashboards*. Diese Dashboards können variabel auf die individuellen Anforderungen des Netzwerks angepasst und erweitert werden. CPI ermöglicht das Festlegen von Grenzwerten für die Generierung von Alarm-Meldungen. Die zur Verfügung stehenden Optionen sind jedoch nicht sehr umfangreich.

Der CPI-Server erfordert keine Vorabkonfiguration für den Empfang von Netflow-Daten. Diese Daten werden von CPI auf dem UDP Port 9991 erwartet. Sobald die ersten Informationen empfangen werden, beginnt die Aufbereitung und visuelle Darstellung. Die Such- und Filter-Möglichkeiten bieten ausreichende Funktionen, um eine zuverlässige Analyse zu ermöglichen. Allerdings konnte auch ein Schwachpunkt in der Darstellung entdeckt werden. Für die Zuordnung eines Datenstromes zu einer Anwendung wird die genutzte Portnummer verwendet. Verbindungen, die einen Port verwenden, für den das CPI keine Anwendung kennt, werden als *unknown* in der Auswertung angezeigt. Im CPI ist es zwar möglich für Ports neue Anwendungen zu referenzieren, aber die Netflow-Statistiken auf den Dashboards geben keine Auskunft über die Portnummer eines solchen Datenstromes.

7.4.3 Orion

Im NPM-Modul ist auch *Orion Network Atlas* enthalten. Dabei handelt es sich um ein eigenständiges Windows-Programm zum Erstellen von Topologie-Karten. Der *Network Atlas* verbindet sich mit der Datenbank des Managementsystems und erhält so den Zugriff auf alle verwalteten Geräte. Auf einem beliebigem Hintergrund (z.B. Gebäudegrundriss) können die einzelnen Geräte platziert werden. Die Verbindungen zwischen den Geräten können manuell eingezeichnet oder durch die „*ConnectNow*“-Funktion automatisch generiert werden. Die fertige Zeichnung kann auf der Weboberfläche integriert werden. Das Bild informiert durch eine Tooltip-Funktion über Name, IP-Adresse, Typ und Betriebszustand der einzelnen Geräte.

Für die Darstellungen von Informationen auf der Weboberfläche setzt Orion vollständig auf den Einsatz von Dashboards. Dementsprechend befinden sich auf je-

der Seite ausschließlich Infoboxen, die als Objektressourcen bezeichnet werden. Jede dieser Infoboxen ist beliebig veränderbar oder auch entfernbar. Die für das Monitoring relevanten Informationen werden in Form von Top-10-Listen zusammengefasst. Das Einrichten von Grenzwerten für die Alarm-Generierung ist nur für Interfaceauslastung, Interfacefehler und zwei weitere Attribute möglich.

Auch für Orion muss Netflow nicht erst eingerichtet werden. Standardmäßig werden die Netflow-Informationen auf UDP Port 2055 erwartet. Die Daten werden durch das Netflow-Modul aufbereitet und durch eine erste Filterung in sechs Ansichten bereitgestellt. Auch die Inhalte des Netflow-Moduls können beliebig verändert werden. Die bereitgestellten Filter-Optionen ermöglichen eine zielführende Analyse der Daten.

7.4.4 Resümee

Die voreingestellten Übersichten zur Darstellungen der Monitoring-Informationen sind im CPI und IMC aussagekräftiger als bei Orion. Allerdings kann dieser Umstand, aufgrund der sehr flexiblen Änderungsmöglichkeiten an der Weboberfläche, wieder ausgeglichen werden.

Der Umfang der konfigurierbaren Grenzwerte in Orion ist kaum erwähnenswert. Die Möglichkeiten des CPI sind im Vergleich bereits wesentlich umfangreicher. Die Leistungsfähigkeit des IMC erreicht das CPI aber nicht.

Von allen Lösungen wurde die Netflow-Analyse gut umgesetzt. Die zur Verfügung gestellten Filter arbeiten zuverlässig und erlauben eine zielführende Arbeit. Lediglich das im CPI erkannte Problem der *unknown* Daten trübt den positiven Gesamteindruck.

7.5 Event-Meldungen und Reporting

Dieser Abschnitt betrachtet die Möglichkeiten im Umgang mit Event-Meldungen sowie die Optionen zum Erstellen von Berichten.

7.5.1 IMC

In der Gruppe *Alarm* bündelt das IMC alle Funktionen für den Umgang mit Meldungen und Events, die das Netzwerk betreffen. Neben den Syslog-Meldungen und SNMP-Traps werden hier auch vom IMC erstellte Meldungen gesammelt. Anhand vorgegebener oder manuell erstellter Filter werden die Events weiterverarbeitet. Die Filtermöglichkeiten erlauben sowohl das Löschen von Events als auch das Erzeugen eines Alarms mit einstellbarer Dringlichkeit. Weiterhin bietet das IMC die Einrichtung von SMS- und E-Mail-Benachrichtigungen, um die Administra-

toren über Events zu informieren. Dabei sind individuelle Einstellungen möglich, die eine Benachrichtigung anhand der Dringlichkeit des Alarms für einzelne Geräte oder für bestimmte Zeiten konfigurieren. Während der Arbeit im IMC ist die Informationsleiste am unteren Rand der Webseite eine hilfreiche Quelle, um stets aktuelle Informationen über die Probleme im Netzwerk zu erhalten. Um die Aufmerksamkeit des Administrators zu erlangen, wird zusätzlich akustisch auf neue Fehler hingewiesen.

Das Reporting-Modul des IMC bietet 23 Vorlagen an. Darüber hinaus ist es möglich, weitere Vorlagen in das System einzubinden. Für das Erstellen neuer Vorlagen stellt HP mit *Intelligent Analysis Reporter* ein entsprechendes Werkzeug zur Verfügung. Grundsätzlich scheint dieses auf *SAP Crystal Reports* zu basieren.

7.5.2 CPI

Im *Lifecycle Theme* ist die Ansicht der Events und Meldungen ein Teil der *Operate*-Kategorie. In dieser Ansicht stehen die Gruppen *Alarms*, *Events* und *Syslogs* bereit. Dabei zeigt die Gruppe *Events* die erhaltenen Meldungen an. Lediglich die empfangen Syslog-Meldungen werden getrennt aufgelistet. Anhand von mehreren hundert vorgegebenen Filtern generiert CPI aus Event-Meldungen entsprechende Alarme. Dabei kann der Administrator die Dringlichkeit eines Alarms im jeweiligen Filter anpassen. Darüber hinaus filtert CPI auch die empfangenen Syslog-Meldungen. Eine Änderung dieser Filtereinstellungen ist über die Weboberfläche nicht möglich. Allerdings zeigte das System auch die Meldungen nicht an, die diesen Filterregeln entsprachen[31]. Für die Benachrichtigung des Administrators über einen Alarm steht nur der E-Mail-Versand zur Verfügung. Der überwiegende Teil der möglichen Einstellungen betrifft lediglich den Inhalt und Umfang der Mail. CPI erlaubt den Versand nur für Alarme mit der höchsten Dringlichkeit. Eine einschränkende Filterung ist nur auf Basis der Gerätekategorien möglich. Die auf der Weboberfläche von CPI stets vorhandene Informationsleiste ermöglicht ein schnelles Erkennen von neuen Fehlern.

Das Reporting erhält im *Lifecycle Theme* eine eigene Kategorie. Cisco stellt eine umfangreiche Sammlung - mit mehr als hundert Vorlagen - zur Verfügung. Für das Entwickeln und Anwenden von weiteren Vorlagen stehen dem Nutzer keine Optionen zur Verfügung.

[31] Syslog Anzeige Problem ist ein seit CPI Version 1.2 bekannter Fehler (Bug-ID CSCud66666)

7.5.3 Orion

Orion bietet keinen zentralen Punkt zur Darstellung von Events und Meldungen an. Die für diese Analyse relevanten Informationen sind in den Ansichten *Ereignisse, Alarme, Syslog, Traps* und *Meldungszentrale* innerhalb der Kategorie *Startseite* untergebracht. Die Meldungszentrale fasst dabei alle Events der einzelnen Quellen zusammen. In allen Ansichten ist es möglich, anhand umfangreicher Filterkriterien, nach Events zu suchen. Für Änderungen an den Bedingungen für die Alarm-Generierung kann der *Alert Manager* eingesetzt werden. Dabei handelt es sich um eines der mitinstallierten Werkzeuge. Über dieses Programm ist es außerdem möglich, eine E-Mail Benachrichtigung zu konfigurieren. Allerdings ist diese Einstellung für jeden Alarm einzeln durchzuführen. Außerdem ist zu beachten, dass auch der Inhalt der E-Mail festgelegt werden muss. Geschieht dies nicht, enthält jede Mail nur den Hinweis, dass Anpassungen erforderlich sind.

Als Bestandteil der Reporting-Funktion ist es möglich, den Inhalt jeder dargestellten Webseite als ein PDF-Dokument zu exportieren. Darüber hinaus lassen sich einzelne Ansichten, wie beispielsweise Netflow-Diagramme, einzeln auswählen und als PDF-Dokument abspeichern. Für das eigentliche Reporting werden 150 Vorlagen mitgeliefert. Diese erstellen ebenfalls eine Website, die anschließend als ein PDF-Dokument exportiert werden kann. Weiterhin enthält die Webseite einen leicht bedienbaren Wizard zum Entwickeln neuer Vorlagen. Für ein geplantes oder wiederholtes Erzeugen eines Reports kommt mit *Orion Report Scheduler* wiederum ein eigenständiges Werkzeug zum Einsatz.

7.5.4 Resümee

Das IMC bietet die umfangreichste und variabelste Lösung für den Umgang mit Event-Meldungen an. Trotz der mitunter eingeschränkten Konfigurationsmöglichkeiten und der anscheinend fehlerhaften Syslog-Komponente bietet das CPI eine funktionale Lösung. Mit der fragwürdigen Einbindung in die Webseite und der sehr umständlichen Konfiguration der E-Mail Benachrichtigung hinterlässt Orion den schlechtesten Eindruck bei dieser Analyse.

Die von Orion erzeugten Reporte sind in vielen Fällen nicht professionell genug. Die dafür erstellten PDF-Dokumente entsprachen meist einem Ausdruck der vollständigen Website inklusive deren Menüleiste. Lediglich der webbasierte Wizard für das Erzeugen neuer Vorlagen ist hier positiv zu bewerten. Die Umsetzung im CPI und IMC sind dagegen funktionell und liefern professionelle Ergebnisse. Durch die große Auswahl an verfügbaren Vorlagen bietet das CPI insgesamt die besten Möglichkeiten.

8 Zusammenfassung

Dieses Kapitel dient der Darstellung der erzielten Analyseergebnisse. Neben dem Fazit wird eine subjektive Bewertung der untersuchten Netzwerkmanagementlösungen vorgenommen. Den Abschluss der Arbeit bildet ein Ausblick auf weiterhin zu analysierende Themengebiete.

8.1 Fazit

Diese Arbeit hatte das Ziel eine Netzwerkmanagementlösung zu finden, welche mit Geräten verschiedener Hersteller zusammenarbeiten und ein breites Spektrum von Managementaufgaben bedienen kann. Eine Managementlösung die kompromisslos alle gestellten Anforderungen erfüllt, konnte unter den analysierten Programmen nicht gefunden werden.

Das aus einzelnen Produkten verbundene Orion System von Solarwinds konnte im direkten Vergleich zu CPI und IMC nicht überzeugen. Die fehlende allumfassende Struktur der Benutzeroberfläche und die unzureichende Unterstützung verschiedener Anforderungen führten zu einem lediglich befriedigenden Gesamteindruck.

Cisco hat mit CPI eine sehr umfassende Lösung geschaffen, die optimal für die Zusammenarbeit mit Cisco-Geräten geeignet ist. Diese Komplexität führt jedoch zu einer überdurchschnittlichen Einarbeitungszeit. Der Einsatz der ungewohnten *Lifecycle*-Ansicht erschwert diesen Umstand weiter. Allerdings ist die alleinige Unterstützung für Cisco-Hardware das Hauptargument gegen den universellen Einsatz von CPI in verschiedenen Netzwerken.

Die beste Gesamtleistung unter den betrachteten Netzwerkmanagementlösungen erbrachte das *HP Intelligent Management Center*. Lediglich die Probleme bei der Konfiguration von HP-Netzwerkkomponenten und das in einigen Fällen nicht optimal umgesetzte modulare Konzept können als Kritikpunkte aufgeführt werden.

8.2 Ausblicke

Ein wichtiger Aspekt, welcher in dieser Arbeit nicht betrachtet wurde, umfasst den finanziellen Aufwand, den die Beschaffung eines Netzwerkmanagementsystems bedeutet. Die Lösungen sollten daher anhand ihres Funktionsumfanges im Verhältnis zu den Kosten erneut untersucht werden. Möglicherweise stellt sich dabei

heraus, dass die Lösung von Solarwinds für einfache Szenarien die beste Wahl ist.

Weiterhin hat die Produktauswahl gezeigt, dass nur wenige Programme in der Lage sind, einen so umfangreichen Anforderungskatalog abzudecken. In einer weiteren Analyse könnte auf die Forderung nach dem Konfigurationsmanagement verzichtet werden, um dadurch ein breiteres Spektrum an Programmen untersuchen zu können.

Aufbauend auf den Ergebnissen dieser Arbeit können Managementlösungen untersucht werden, deren Funktionen für den *Network Management* oder *Service Mangement Layer* geeignet sind. In diesem Zusammenhang bietet sich die Analyse des Zusammenspiels zwischen HP IMC und HP NNMi an.

Literatur

1. **Tanenbaum, Andrew S.** *Computernetzwerke.* [Übers.] Angelika Shafir. München : Prentice Hall, 1997.

2. **Cisco Systems.** *Enterprise Campus 3.0 Architecture.* [PDF] San Jose, USA : Cisco Systems, Inc., 2008. OL-15716-01.

3. **Clemm, Alexander.** *Network Management Fundamentals.* [PDF] Indianapolis, USA : Cisco Systems, Inc., 2007.

4. **Cisco Systems.** Cisco IOS NetFlow Overview. *www.cisco.com.* [Online] 2004. https://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_presentation0900aecd80311f57.pdf.

5. **Reese, Brad.** Closer look: sFlow better than NetFlow? *www.networkworld.com.* [Online] 2008. http://www.networkworld.com/community/node/29117.

6. **Hewlett-Packard Development Company.** End of Sale Announcement. *www.1.hp.com.* [Online] 2013. http://h17007.www1.hp.com/docs/products/eos/PCM_Plus_End_of_Sale_Announcement.pdf.

7. —. HP Completes Acquisition of 3Com Corporation. *www8.hp.com.* [Online] 2010. http://www8.hp.com/us/en/hp-news/press-release.html?id=342187&jumpid=reg_r1002_usen_c-001_title_r0001#.Ur91sOFYTkU.

8. **Kiwic, Anton.** Intelligent Management Center. *www.hp.com.* [Online] 2012. http://www8.hp.com/h41112/ch/de/campaign/techcircle/pdf/Tech-Circle-Introduction-IMC-March-2012.pdf.

9. **ITU.** ITU-T Recommendations. [Online] 2013. http://www.itu.int/pub/T-REC.

10. **IETF.** Search Internet-Drafts and RFCs. [Online] 2013. http://datatracker.ietf.org/doc/search/.

11. **Hewlett-Packard Development Company.** HP IMC Enterprise Edition - QuickSpec. [Online] 2013. http://h18000.www1.hp.com/products/quickspecs/productbulletin.html#!spectype=worldwide&type=html&docid=13832.

12. **Cisco Systems.** Cisco Prime Infrastructure-LMS Functional Comparison with Prime Infrastructure 2.0. [Online] 2013. http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/guide_c07-729089.html.

13. —. Cisco Prime-Infrastruktur. [Online] 2013. http://www.cisco.com/web/DE/products/networkmgmt/cisco_prime_infrastructure.html.

14. —. *Managing an Enterprise WLAN with Cisco Prime Infrastructure.* [PDF] 2013.

15. —. Cisco Prime Infrastructure 2.0 Data Sheet. [Online] 2013. http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/data_sheet_c78-729088.html.

16. **Paessler AG.** Funktionsumfang PRTG Network Monitor. [Online] 2013. http://www.de.paessler.com/prtg/features.

17. **Help/Systems, LLC.** InterMapper Network Monitoring, Mapping and Alerting Software. [Online] 2013. http://www.intermapper.com/products/intermapper/feature/default.aspx.

18. **Nagios Enterprises.** Nagios Features. [Online] 2013. http://www.nagios.org/about/features.

19. **The OpenNMS Group.** Features List. [Online] 2012. http://www.opennms.org/wiki/Features_List.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Dresden, den 06.01.2014

Marcus Schiefer