HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Sirko König

Analyse einer heterogenen Netzwerkinfrastruktur zur Implementierung von systemübergreifendem Monitoring für alle im Netzwerk befindlichen Komponentenklassen unter Einbeziehung von ökonomischen und rechtlichen Aspekten.

Mittweida, 2014

Fakultät MNI

BACHELORARBEIT

Analyse einer heterogenen Netzwerkinfrastruktur zur Implementierung von systemübergreifendem Monitoring für alle im Netzwerk befindlichen Komponentenklassen unter Einbeziehung von ökonomischen und rechtlichen Aspekten.

Autor:
Herr

Sirko König

Studiengang:
Wirtschaftsinformatik

Seminargruppe:
WF10w1-b

Erstprüfer:
Prof. Dr. J. Mario Geißler

Zweitprüfer:
Prof. Dr. Uwe Schneider

Einreichung:
Mittweida, 03.02.2014

Verteidigung/Bewertung:
Mittweida, 2014

Faculty MNI

BACHELORTHESIS

Analysis of a heterogeneous network infrastructure to implement cross-system monitoring for all component classes with economic and legal aspects in mind.

author:
Mr.

Sirko König

course of studies:
business information systems

seminar group:
WF10w1-b

first examiner:
Prof. Dr. J. Mario Geißler

second examiner:
Prof. Dr. Uwe Schneider

submission:
Mittweida, 03.02.2014

defence/ evaluation:
Mittweida, 2014

Bibliografische Beschreibung:

König, Sirko:
Analyse einer heterogenen Netzwerkinfrastruktur zur Implementierung von systemübergreifendem Monitoring für alle im Netzwerk befindlichen Komponentenklassen unter Einbeziehung von ökonomischen und rechtlichen Aspekten. - 2014. – 83 Seiten, 31 Abbildungen, 6 Tabellen

Mittweida, Hochschule Mittweida, Fakultät MNI

Bachelorarbeit, 2014

Referat:

Diese Arbeit befasst sich mit der Implementierung einer systemübergreifenden Monitoring Lösung und beschreibt einige Grundlagen sowie alle wichtigen Schritte von der Analyse bis hin zur Kaufentscheidung. Dabei werden einige Lösungen vorgestellt und zu beachtende Gesetze aufgezeigt.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CLTS	Connection Less Transport Service
CMI	Common Information Model
DDP	Datagram Delivery Protocol
DTMF	Desktop Management Task Force
GGP	Gateway to Gateway Protocol
HP	Hewlett Packard
HP SIM	Hewlett Packard System Insight Manager
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IT	Informationstechnik
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MPI	Max-Planck-Institut
MPI-CPfS	Max-Planck-Institut für chemische Physik fester Stoffe
MTU	Maximum Transmission Unit
OID	Object Identifier
RFC	Request for Comments
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol

SQL	Structured Query Language
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WBEM	Web Based Enterprise Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation

0 Übersicht

In einem einleitenden Kapitel werden die Aufgabenstellung und die Motivation dieser Bachelorarbeit dargestellt. Ein kurzer Überblick zu den einzelnen Kapiteln dieser Arbeit folgt.

0.1 Motivation

In der heutigen Zeit gibt es immer mehr vernetzte Geräte und gerade in größeren Firmen wird der 24h Betrieb sowie die Echtzeitfunktionalität von Anwendungen groß geschrieben. Das betreffende Netzwerk ist meist ein durchdachtes Gesamtkonstrukt aus mehreren Teilkomponenten, teilweise auch herstellerunabhängig und dazu veränderlich. Im Zeitalter von Smartphone[1] und Tablets[2] sowie tragbarer Computer melden sich ständig Geräte am Netzwerk an und andere wieder ab. Meistens funktioniert das Netz und niemand merkt, wenn mal ein unbenutzter Port ausfällt oder ein Drucker durch einen fehlerhaften Auftrag blockiert ist.

Somit ist es unabdingbar eine Gesamtlösung zu besitzen, welche jegliche Komponenten des Netzwerkes überwacht und im Falle eines Problems den zuständigen Dienstleister oder die zuständige Abteilung benachrichtigt. Darüber hinaus unterstützt Monitoring den Dauerbetrieb von Datenverarbeitungstechnik durch Analyse und Status der jeweiligen Komponenten und kann bereits im Voraus Warnungen geben.

0.2 Zielsetzung

Diese Arbeit beschreibt auf Grundlage der Aufgabenstellung den Weg zum systemübergreifenden Netzwerk-Monitoring. Es soll gleichermaßen für Einsteiger, aber auch für erfahrende Anwender oder Administratoren den Weg für die Entscheidung unterstützen. Ebenso wird das nötige technische Wissen geschaffen und die wirtschaftlichen Aspekte angesprochen, indem z.B. auf Open Source eingegangen wird.

[1] Smartphone: Handy, welches weitaus mehr Funktionen als ein herkömmliches Mobiltelefon bietet

[2] Tablet: Tragbarer, flacher Computer, meist ohne Tastatur

Als Beispiel für die Einführung zur Komplettlösung wird von der Analyse bis hin zur fertig konfigurierten Software das Max-Planck-Institut für chemische Physik fester Stoffe genutzt.

0.3 Kapitelübersicht

Die Bachelorarbeit besteht aus 7 Kapiteln.

Das erste Kapitel gibt eine allgemeine Einleitung zur Problemstellung und setzt Grundlagen für das Verstehen der nachfolgenden Kapitel.

Nachfolgend beschreibt das zweite Kapitel den Weg für die Erfassung des IST-Zustandes. Speziell wird auf die Durchführung eingegangen und wie Schwerpunkte zu finden sind.

Kapitel drei beschäftigt sich mit der Analyse der Anforderungen, welche an eine Monitoring Lösung gestellt werden.

Im Kapitel vier werden allgemeine Lösungen vorgestellt und die Vor- und Nachteile aufgegriffen.

Das fünfte Kapitel zeigt die Anforderungen und Softwareauswahl für das Beispiel Max-Planck-Institut. Dabei werden verschiedene Lösungen vorgestellt und auch in der Praxis getestet.

Der Umsetzung des Managementmodells OSI am Beispiel Max-Planck-Institut wird das sechste Kapitel gewidmet.

Welche rechtlichen Aspekte mit dem Monitoring in Berührung kommen, klärt das letzte Kapitel 7.

1 Grundlagen

Der Markt von Monitoring-Lösungen ist sehr breit gefächert und stellt Tools für kleine bis große Unternehmen bereit. Doch was genau steckt eigentlich hinter dem Begriff „Monitoring“? Auf diese Frage gibt dieses Kapitel eine Antwort.

1.1 Monitoring im allgemeinen

Der Begriff „Monitoring“ findet in sehr vielen verschiedenen Bereichen seine Bedeutung. Als Kernpunkt steht dahinter die unmittelbare systematische Erfassung von physischen Objekten oder auch Informationen. Aber auch deren Beobachtung oder Überwachung steht im Vordergrund.

Heutzutage gilt sehr oft eine Protokollierungs- und Dokumentierungspflicht. Dabei kann das Monitoring unterstützend wirken, durch z.B. automatisiertem Überwachen und selbstständigem Erfassen von Werten.

1.2 Netzwerk

Das Netzwerk ist als Gesamtsystem zu verstehen. Eine Teilmenge davon sind Endgeräte. In den meisten Fällen sind das Computer, aber auch mobile Geräte, wie Handys oder Tablets. Server zählen auch in diese Kategorie, sind jedoch als Dienstleister für bestimmte Aufgaben zu verstehen. Zwischen den Endgeräten gibt es zum einen die Transportverbindungen und zum anderen die Übertragungskomponenten. Die Transportverbindungen sind die Übertragungsmedien, wie z.B. optische Leiter, elektrische Leiter oder elektromagnetische Übertragung durch das Medium Luft. Sie dienen dem übermitteln von Daten vom Sender zum Empfänger. Die Übertragungskomponenten stellen die Verteiler- bzw. Vermittlungsgeräte dar. Diese sind Knotenpunkte im Netzwerk und in verschiedenen Größen und Funktionen gegeben. Sie dienen dem Zustellen der Daten an das richtige Übertragungsmedium bzw. in der einfachsten Ausführung der Kopplung der Medien.

1.3 Homogenes Netzwerk

Einleitend zur Erklärung des Begriffes ein kurzer und prägnanter Satz: [TS] S.15

„Unter einem homogenen Netzwerk ist ein Netzwerk zu verstehen, welches sich primär aus Komponenten von nur wenigen Herstellern zusammensetzt.“

Das bedeutet nicht zwangsweise, dass alle Geräte von einem Hersteller stammen müssen. Denn homogen beschreibt im Grunde eine Gruppe von gleichen Objekten. Ein homogenes Netzwerk liegt auch dann vor, wenn z.B. die Geräte der Sicherungsschicht des OSI-Referenzmodells vom selben Hersteller stammen. Die Abgrenzung ist also auf der Herstellerhomogenität auf der jeweiligen Schicht des OSI-Referenzmodells zu beschränken.

Ein Vorteil des homogenen Netzwerkes ist die einfache Administration. Denn die meisten Hersteller liefern bereits angepasst Managementsoftware zu ihren Produkten mit.

1.4 Heterogenes Netzwerk

[TS] S. 17 „Die Vorstellung eines perfekten, homogenen Netzwerkes lässt sich nur in den wenigsten Fällen auch in die Praxis umsetzen."

Ein Netzwerk ist in den meisten Fällen kein homogenes Netzwerk. Allein die Weiterentwicklung oder Umstrukturierung kommt meist mit Neuanschaffungen von Geräten daher. Mitunter kann auch aus wirtschaftlichen oder funktionellen Anforderungen kein herstellergleiches Gerät beschafft werden. Ebenso kann aus einem homogenen Netzwerk auch ein heterogenes entstehen, wenn durch Austausch einiger herstellergleichen Komponenten sich jedoch grundlegende Technologien ändern.

1.5 Netzwerk Monitoring

Unter dem Begriff Netzwerk Monitoring zählen sämtliche Aufgaben der Überwachung und Kontrolle von den im Netzwerk befindlichen Komponenten und deren Dienste (z.B. E-Mail, DNS[3]).

Das Überwachen der Netzwerkkomponenten ist ein Teil des Netzwerkmanagements. Über die Jahre haben sich viele verschiedene Ansätze entwickelt. Im Folgenden wird das OSI-Modell der Internationalen Organisation für Normung (ISO) vorgestellt.

1.6 OSI Managementmodell

Das Managementmodell Open Systems Interconnection (OSI) definiert fünf Bereiche, welche dem Netzwerkmanagement zu Grunde liegen. Dieses Modell beschreibt alle Aufgaben und Inhalte welche für das Management wichtig sind. Darüber hinaus definiert das OSI laut [TS] S. 4 die „verwalteten Objekte und Systeme näher" sowie deren Kommunika-

[3] DNS: Dynamic Name System; Dienst welcher IP-Adresse zu Namen interpretiert und umgekehrt

tionsweg und die dafür benutzen Protokolle. Eine Netzwerküberwachung benötigt ein solides Managementmodell als Grundlage.

1.6.1 Fehlermanagement

Damit ein einwandfreier und ununterbrochener Netzwerkbetrieb gewährleistet ist, muss jederzeit auf das Netzwerk als Ganzes und jeder der einzelnen Komponenten geachtet werden. Das Fehlermanagement beschäftigt sich mit der Verfügbarkeit des Netzes und deren Verbesserung. Dabei werden Mittel zur Fehlererkennung, Fehleranalyse und Fehlerbehebung bereitgestellt. Die Fehlererkennung kann über Auswerten von Protokollen oder der Entgegennahme und Analyse von Fehlermeldungen geschehen. Alles in allem soll dieser Bereich die dauerhafte und durchgängige Erreichbarkeit der Systeme sicherstellen.

Das Fehlermanagement gliedert sich in drei wesentliche Aufgabenbereiche [LE]:

- Erkennen von Fehlern
- Diagnostizieren von Fehlern
- Beheben von Fehlern

Fehlererkennung: Regelmäßig werden Diagnosetests von der Managementstation aus durchgeführt oder das Gerät sendet selbstständig eine Fehlermeldung ab. Tritt ein Fehler auf, sind folgende Punkte zu beachten:

a.) Feststellen, was Ursache für den Fehler ist
b.) Die Störungsstelle vom restlichen Netzwerk isolieren
c.) Umleiten des Netzwerkverkehrs über redundante Leitungen, physisch oder logisch
d.) Reparatur oder Austausch der Komponente

Fehlerdiagnose: Für die Feststellung der Fehlerursache stehen Systemereignisse in der Ereignisanzeige des Gerätes zur Verfügung.

Fehlerbehebung: Hierfür stehen Fehlerbehebungstools zur Verfügung oder der Administrator wird zum aktiven Eingreifen aufgefordert. Nach einer Fehlerbeseitigung ist festzustellen, dass der Fehler tatsächlich behoben wurde und keine neuen Probleme dadurch entstanden sind.

1.6.2 Konfigurationsmanagement

Unter Konfigurationsmanagement wird die allgemeine Verwaltung der Komponenten und Systeme, welche überwacht bzw. konfiguriert werden, verstanden. [TS] S. 5 „Demnach ist es die Aufgabe des Konfigurationsmanagements, die am Management beteiligten Systeme zu identifizieren, Kontrolle über sie auszuüben, Daten von ihnen zu sammeln und ihnen Daten zur Verfügung zu stellen.“ Wichtige Aufgaben sind dabei:

- Eindeutige Bezeichnung der Objekte und Objektgruppen
- Konfiguration der Geräte und Definition der normalen Betriebszustände
- Bedarfsorientierte Abfrage von Informationen der Objekte und Dienste eines Systems
- Empfangen von Informationen über Fehler bzw. den aktuellen Zustand des jeweiligen Objektes
- Konfigurationsänderungen eines verwalteten Systems

1.6.3 Abrechnungsmanagement

Speziell relevant für Dienstleister, wie z.B. Internet Service Provider[4], behandelt dieser Bereich die [TS] S. 5 „Verarbeitung und Verwaltung der anfallenden Abrechnungsdaten“. Dabei geht es vor allem um die Konfiguration der Netzwerkkomponenten hinsichtlich der Datenerfassung, sowie der Überwachung von Kosten- und Ressourcenlimits.

1.6.4 Leistungsmanagement

Die Auslastung eines Systems wird mit Hilfe des Leistungsmanagements ermittelt. Meist reicht die einfache Prüfung der Erreichbarkeit nicht aus, um sagen zu können, ist das System auch verfügbar? Ein System ist dann verfügbar, wenn es „normal“ nutzbar ist. Im Falle einer Überbeanspruchung, z.B. durch eine Vielzahl an Nutzern auf einem Streaming Server[5], ist es sehr wahrscheinlich, dass einige oder gar alle Nutzer den Inhalt nicht mehr in Echtzeit übertragen bekommen. Somit hilft das Leistungsmanagement durch historisierte Erfassung von Leistungsdaten und Nutzungszeiten diesen Problemen vorzubeugen. Dabei stehen Tools zur Ermittlung von Datendurchsätzen im Vordergrund.

1.6.5 Sicherheitsmanagement

Netzwerke besitzen meistens mehrere Ein- und Ausgänge, wie z.B. eine Schnittstelle zum Internet oder den Zugang über einen VPN[6]-Tunnel. Damit nicht jeder beliebige Benutzer diese Schnittstelle passieren kann, müssen Sicherheitsvorkehrungen getroffen und Technologien eingesetzt werden, die das unerlaubte Nutzen verhindern. Selbst das Entdecken von Sicherheitslücken ist die Aufgabe des Sicherheitsmanagement. Dazu gehört aber auch das Sichern des Netzwerkes vor unerlaubten Zugriffen von innerhalb. Zum Beispiel haben viele Unternehmen eine Verwaltungsabteilung welche jedoch vor Fremdzugriffen, z.B. der Mitarbeiter, geschützt werden sollte. Bei Authentifizierungsproblemen oder feh-

[4] Internet Service Provider: Stellt entgeltlich die Nutzung des Internets zur Verfügung

[5] Streaming Server: Server, welche Medieninhalte in Echtzeit überträgt

[6] VPN: Virtuelles Privates Netzwerk, Stellt ein Netzwerk über eine verschlüsselte TCP/IP Verbindung her

lerhaften Authentifizierungsversuchen ist die Protokollierung und gegebenenfalls Benachrichtigung des Administrators zur Analyse sinnvoll.

1.6.6 Management Information Base

Der weitere wichtige Teil im OSI-Modell ist die Management Information Base (MIB). Nach [TS] beschreibt die MIB die überwachbaren und konfigurierbaren Objekte eines zu verwaltenden Systems. Bei der Überwachung fließen die Informationen der Objekte zur Managementstation und bei der Administration in umgekehrter Reihenfolge, also von der Station zum verwalteten Gerät. Um diese Aufgaben zu erfüllen, ist ein entsprechendes Managementprotokoll zu implementieren. Eines der möglichen Protokolle hierfür ist Simple Network Management Protocol (SNMP), welches in einem folgenden Abschnitt beschrieben ist. Die einzelnen Objekte werden auch als Object Identifier (OID) bezeichnet. Die OID werden in der Sprache Structure of Mangement Information (SMI) in den MIBs definiert. Das SMI stellt ein Rahmenwerk über den grundlegenden Aufbau und Syntax der OIDs dar. Die Objekte sind der Übersichtlichkeit wegen hierarchisch angeordnet. Das wird in der Struktur und dem Aufbau der OID gewährleistet. Eine Kette von Zahlen, die durch Punkte getrennt sind steht in jedem Fall für ein eindeutiges Objekt. Das folgende Beispiel beschreibt eine OID, welche den Ort des Gerätes ausgibt:

```
1.3.6.1.2.1.1.6 oder
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-
2(1).system(1).sysLocation(6)
```

In der Standard MIB (MIB-II) sind standardisierte Objekte definiert, welche auf sehr vielen Netzwerkkomponenten Anwendung finden (z.B. sysLocation für den Standort). Für weitere nicht abgedeckte Bereiche, stehen den Herstellern und Administratoren die Bereiche „private“ und „enterprise“ für das Einfügen eigener MIBs zur Verfügung.

Abbildung 1 zeigt die grundlegende Struktur der OID-Hierarchie:

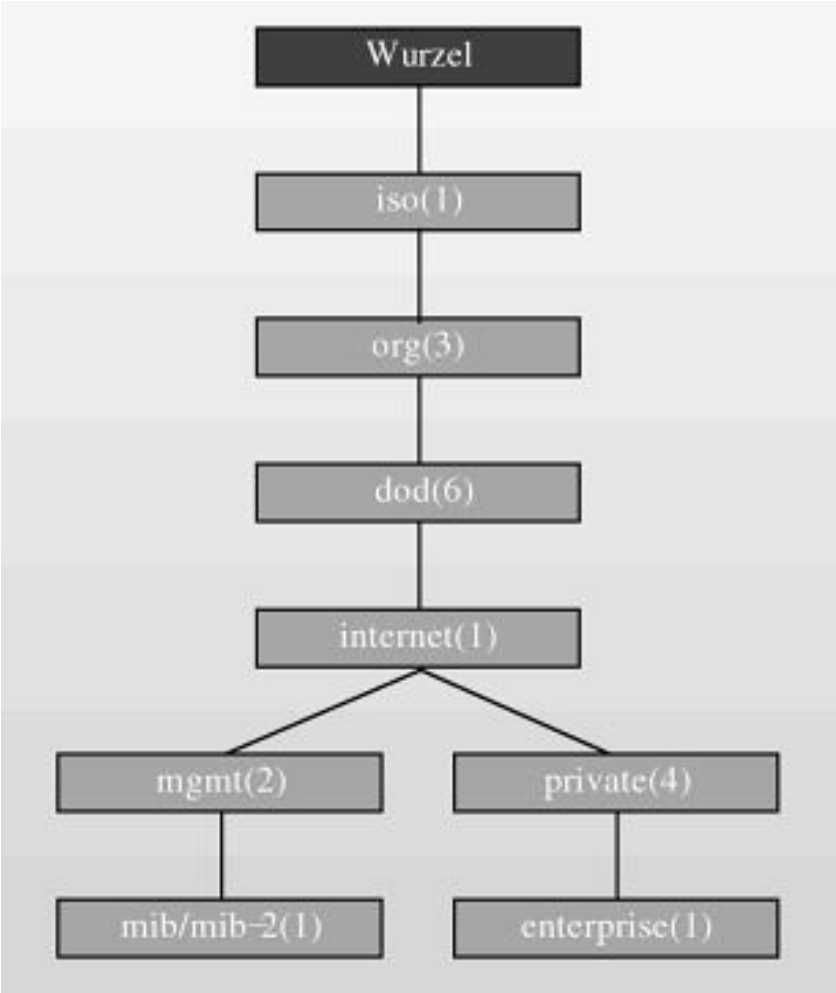

Abbildung 1: Struktur der OID-Hierarchie [TS] S. 110

1.7 Beispiele von Protokollen für das Netzwerkmanagement

Dieser Abschnitt geht auf verschiedene Protokolle welche für das Netzwerkmanagement relevant sind ein. Alle drei hier vorgestellten Protokolle sind in fast jeder Monitoring Software implementiert und deshalb deren Aufbau sowie Funktionsweise wichtig.

1.7.1 Simple Network Management Protocol

Für das Management des Netzwerkes gibt es zweierlei Kommunikationswege. Den Überwachungsweg und den Konfigurationsweg. Eines der Protokolle was diese beiden Wege ermöglicht, ist das sogenannte im Jahr 1988 entwickelte Simple Network Management Protocol (SNMP) [TS] S. 69. Viele Monitoring Lösungen haben das Protokoll implementiert und arbeiten auf dessen Basis. Mittlerweile ist der Entwicklungsstand bereits bei Version 3 angekommen, da bei vorherigen Versionen Sicherheitsmechanismen fehlten.
SNMP basiert in seiner Funktionsweise auf zwei verschiedene Kommunikationsformen.

Die erste Form „verläuft bidirektional und arbeitet nach dem Frage-Antwort-Prinzip“ [TS] S. 70. Bei dieser Kommunikationsart stellt die Überwachungsstation eine Anfrage an eine entsprechende Netzwerkkomponente und diese wiederum schickt eine Antwort zurück. Die Anfrage kann eine Nachricht enthalten über die Anweisung der Informationsrückgabe von Statuswerten oder auch der Bestätigung einer Verwaltungsanfrage.

„Bei der zweiten Kommunikationsform werden Nachrichten[7] unidirektional – und zwar ausschließlich von der überwachten Komponente hin zur Managementstation – gesendet“ [TS] S. 71. Die Bedeutung dieses Kommunikationsweges ist als sehr wichtig anzusehen, denn er sorgt dafür, dass die Netzwerkkomponenten jederzeit bei einem Ereignis eine Nachricht an das Managementsystem schicken kann.

Folgende Grafik zeigt die beiden Kommunikationsformen noch einmal als Übersicht:

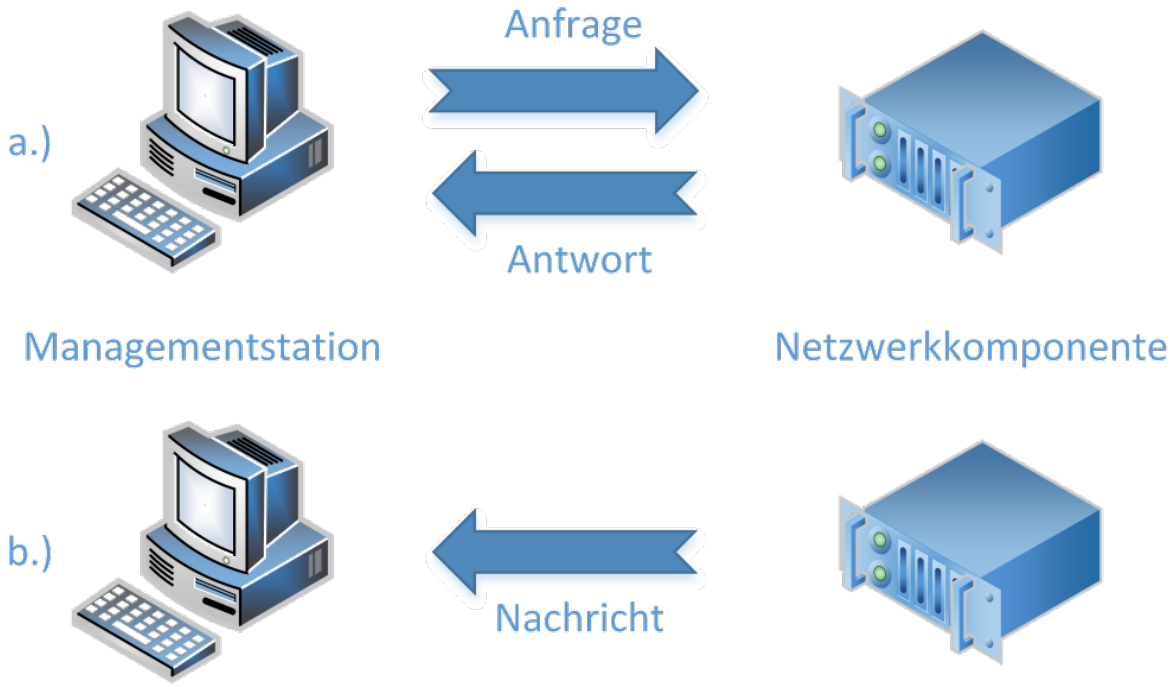

Abbildung 2: Kommunikationswege SNMP

Bei a.) sendet die Station eine Anfrage, z.B. „wie hoch ist die Prozessorauslastung“ oder den Befehl „deaktiviere Port 12“ und bekommt als Antwort, wie hoch die Prozessorauslastung ist oder Port 12 deaktiviert.

Bei b.) schickt die Netzwerkkomponente selbst eine Nachricht an die Station, meistens mit der Information eines Defektes oder Ausfalles.

[7] Diese Nachrichten werden auch als „Traps“ bezeichnet. Laut [TS] stammt diese Bezeichnung aus der Sportart Tontaubenschießen. Denn die Wurfmaschine trägt den Namen „Trap“. Als Parallele sieht [TS] die Unvorhersehbarkeit für das Abschießen der Tontaube bzw. die Versendung eines Traps.

Das SNMP beschreibt im Allgemeinen ein Rahmenwerk von Regeln, auf dessen Basis die Kommunikation der Geräte und Managementzentralen abläuft. Eine Quelle für umfangreiche Informationen darüber bieten die Request for Comments (RFCs) der Internet Engineering Task Force (IETF)[8].

Derzeit üblich ist die Verwendung von SNMPv2c oder SNMPv3. In der Version 3 wurden Sicherheitslücken aus der Version 2c beseitigt. Laut RFC 1906 (SNMPv2c) und RFC 3417 (SNMPv3) können beide Versionen vier verschiedene Protokolle zum Senden von SNMP Nachrichten nutzen: UDP, CLTS, DDP, IPX

Für SNMPv3 ist laut [TS] S. 144 eine Ergänzung um weitere Protokolle nicht ausgeschlossen. Das RFC 3430 beschreibt z.B. die Verwendung von SNMP über TCP.

1.7.1.1 SNMPv2c

Am weitesten verbreitet ist derzeit der Standard SNMPv2c, wohl auch weil viele Geräte den neuen Standard Version 3 noch nicht unterstützen. In manchen Netzen wird auch ein Mischbetrieb von Version 2c und Version 3 genutzt. Deswegen wird an dieser Stelle noch etwas genauer auf die SNMPv2c eingegangen.

Im Jahr 1992 wurde mit der Entwicklung von SNMPv2 als Nachfolger von SNMPv1 begonnen. Ziele dafür waren unter anderem die Verbesserung der unzureichenden Sicherheitsmechanismen, Beheben der teilweise vorhandenen ineffizienten Kommunikation und Erweitern des Informationsmodells. Dabei wurde „im Rahmen der SNMPv2 Spezifikation“ [JH] S.91 das Informationsmodell bearbeitet und als SMIv2 veröffentlicht. Neue Datentypen wie z.B. Counter64 und ein neuer Objekttyp „Makro“ wurden eingeführt. Mit der Einführung zweier weiterer Operationen „GetBulk“ und „Inform“ konnten nun auch SNMP-Manager untereinander kommunizieren und hierarchisch organisiert werden. Dank „GetBulk“ entstand eine Möglichkeit selbst größere Daten effizient abzufragen. Bei SNMPv1 existierten für die Fehlerbehandlung fünf Fehlercodes, diese sind bei SNMPv2 auf 18 Fehlercodes erweitert worden. Weiterhin haben die Entwickler die nutzbaren Protokolle ausgedehnt und die Benachrichtigung durch Traps verbessert. Erste Spezifikationen zum SNMPv2 wurden in den RFC1441 bis RFC1452 [JH] S.91 im Jahr 1993 veröffentlicht. Das in RFC1445 vorgestellte Sicherheitskonzept fand jedoch keine Resonanz durch seine Komplexität. Deshalb stellten die Entwickler im Jahr 1996 das heute noch genutzte Community-based SNMPv2 (SNMPv2c) vor. Dieses ist definiert in den RFCs 1901 bis 1909.

Das wichtigste Merkmal von Version v2c ist, das das Authentifizierungspasswort (die sogenannte „Community“), im Klartext übertragen wird. Somit sollten mit dieser Version,

[8] Die IETF ist ein weltweiter Zusammenschluss aus Administratoren, Netzwerkdesignern, Herstellern und Forschungskonzernen, welche zum Ziel haben, das Internet stetig zu optimieren und die Evolution des Internets voran zu treiben. Sie setzen mit den RFCs Standards und vereinheitlichen die weltweite Kommunikation.

wenn diese noch benutzt werden muss, nur reine Leseabfragen getätigt werden. Die Konfiguration von Netzwerkkomponenten oder anderen Geräten über diese Version sollte möglichst vermieden werden.

1.7.1.2 SNMPv3

Da SNMPv3 stetig weiter an Bedeutung zu nimmt und auch für die später in dieser Arbeit folgenden Softwaretests benötigt wird, wird an dieser Stelle noch etwas genauer auf die Version 3 des Simple Network Management Protocol eingegangen.

Bei der Architektur von SNMPv3 gibt es nicht mehr die Unterscheidung zwischen Manager und Agent, sondern es wird der Begriff SNMP Entität eingeführt. Folgende Grafik zeigt diese Referenzarchitektur:

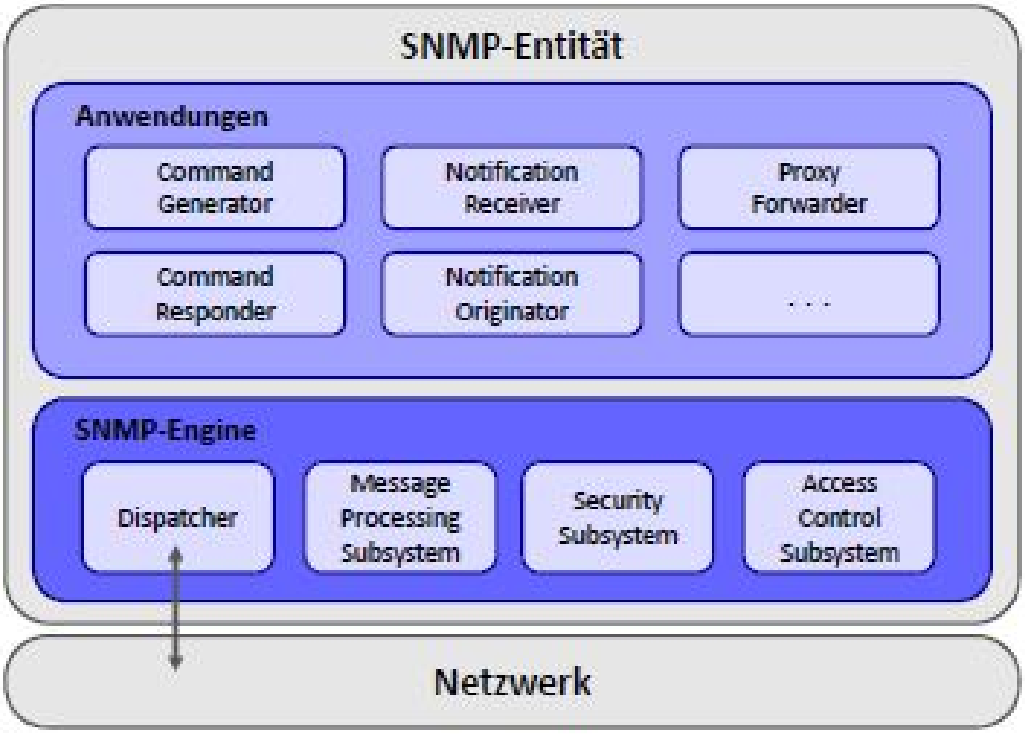

Abbildung 3: SNMPv3 Architektur [JH] S. 93

Abhängig von der jeweiligen Rolle der Entität ist der Implementierungsgrad der einzelnen Module. Diese werden folgend kurz erläutert:

- Dispatcher: Dient der parallelen Verarbeitung mehrerer unterschiedlicher SNMP Versionen, unterteilt sich in folgende 3 Bereiche:
  - Transport Mapping: In diesem Modul werden die SNMP-Nachrichten auf ein entsprechendes Transportprotokoll abgebildet, wie z.B. UDP
  - Message Dispatcher: Verteilt die SNMP Nachrichten an die dafür vorgesehenen Module anhand der Version

  - PDU Dispatcher: Bereitstellung einer generischen Schnittstelle, für das Versenden und Empfangen von SNMP Nachrichten durch Anwendungen
- Message Processing Subsystem: Innerhalb dieses Moduls werden Submodule für die Verarbeitung der unterschiedlichen SNMP Versionen zusammengefasst.
- Security Subsystem: Zuständig für die Authentifizierung und der Ver- sowie Entschlüsselung
- Access Control Subsystem: Regelt die Zugriffskontrolle

In SNMPv3 wird unter Protocol Data Unit (PDU) ein Teil einer SNMP-Nachricht verstanden, nämlich den Teil, der die Nachricht sowie die Variablen enthält.

Die SNMP Anwendungen verarbeiten die PDUs und greifen auf die Dienste zu, welche durch die SNMP Engine (siehe Abbildung 3: SNMPv3 Architektur [JH] S. 93) bereitgestellt werden. Dazu zählen unter anderem:

- Command Generator, Command Responder: Initiierung von Get, GetNext, GetBulk und Set Befehlen und Erzeugung der entsprechenden PDUs. Der Responder hingeben beantwortet die Anfragen auf Basis der MIB.
- Notification Originator, Receiver: Diese beiden Anwendungen erzeugen bzw. verarbeiten Trap- und Inform-Nachrichten.
- Proxy Forwarder: Für die Weiterleitung der SNMP-Nachrichten ist dieses Modul zuständig.

Sicherheitsmodell von SNMPv3: User-based Security Model (USM)

In der RFC3414 wurde das sogenannte User-based Security Modell (USM) definiert. Dabei werden zwei Ziele verfolgt:

- Nachweis der Authentizität, um Maskierungsangriffe zu verhindern
- Schutz der Nachrichten durch Verschlüsselung

Damit die Umsetzung möglich war, musste das Nachrichtenformat geändert werden. Jedoch bleibt der operationsabhängige PDU-Teil dem Format wie in der SNMPv2c Version gleich. Im USM gibt es zwei Schlüssel, den Authentification Key und den Privacy Key. Dabei dient der Authentification Key der Authentifizierung und der Privacy Key der Verschlüsselung der Nachrichten. Beide Schlüssel sind geheim und müssen dem Empfänger sowie Sender bekannt sein. In Abbildung 4 ist der Aufbau einer SNMPv3 Nachricht dargestellt. Dabei ist zu erkennen, dass bei der Verschlüsselung nur die PDU sowie die contextEngineID und der contextName codiert werden.

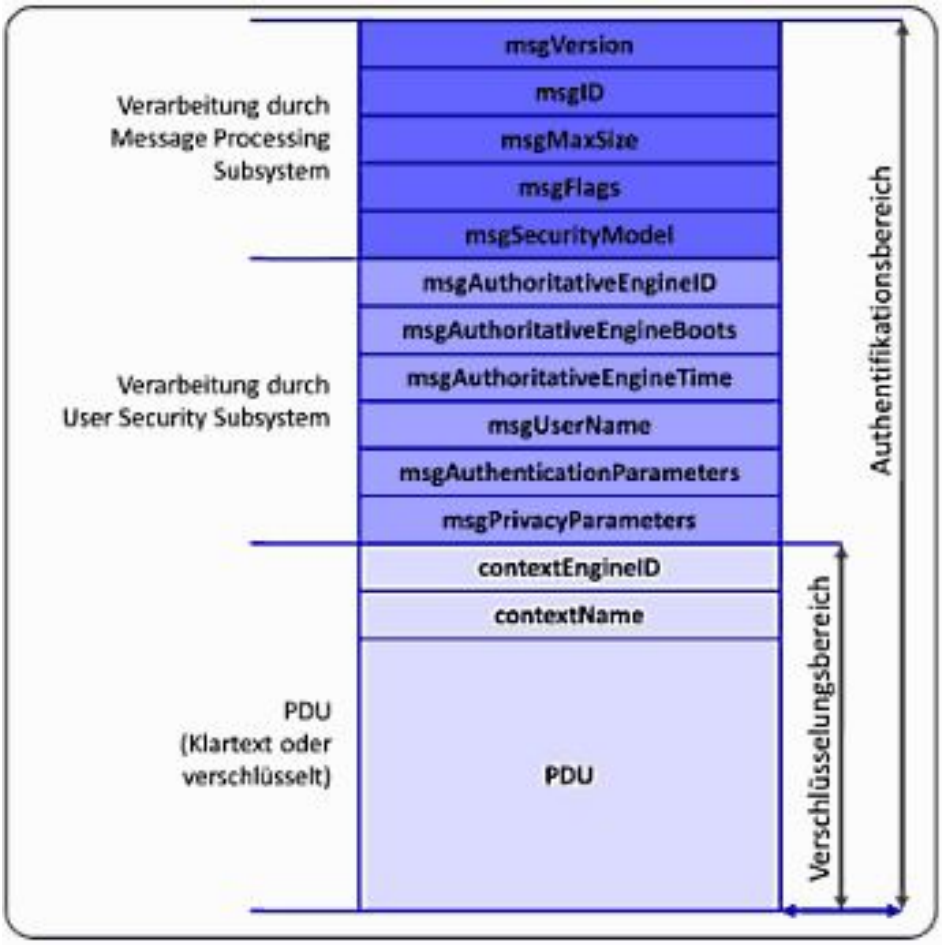

Abbildung 4: Aufbau einer SNMPv3 Nachricht [JH] S. 96

Zugriffskontrolle: View-based Access Control Model (VACM)

Wie auch bereits seit dem Community-Konzept von SNMPv1 kann bei SNMPv3 der Zugriff auf die MIB beschränkt werden. Die Zugriffsrechte sind dabei von folgenden Faktoren abhängig:

- Principal: In Abhängigkeit des Nutzers bzw. seiner Gruppe
- Security Level: In Abhängigkeit der Sicherheitsstufen, sprich der Verschlüsselung der Kommunikation
- Security Model: Wenn der Agent mehrere Security Models implementiert hat, können auch hier die Zugriffsrechte davon abhängig sein
- MIB Context: Beschreibt eine Teilmenge einer MIB, entspricht einem Teil-Baum
- Type of Access: In Abhängigkeit zur Art des Zugriffs (read, write, notify)

Die Zugriffsrichtlinien lassen sich durch die verschiedenen Faktoren sehr feingranular gestalten.

1.7.2 Windows Management Instrument

„Die Windows Management Instrumentation (WMI) ist ein Windows Systembaustein zum Zugriff auf System- und Netzwerkinformationen.“ [HMT] S. 875.

Das WMI ist somit also eine Sammlung von Dateien und Programmen um bestimmte Informationen von Windows Systemen zu erhalten. Ursprung dafür ist das Web Based Enterprise Management System (WBEM) der Desktop Management Task Force (DMTF) welches für System- und Netzwerkmanagementzwecke entwickelt wurde. Microsoft entwickelte aus dem WBEM die WMI Implementierung. Grundlegender Kern von WBEM und somit auch WMI ist das Common Information Model (CMI). Dabei modelliert das CMI die zu verwaltenden Ressourcen mithilfe von objektorientierten Methoden. Bereits seit Windows Millennium (ME) ist das WMI fester Bestandteil von Microsoft Betriebssystemen. Folgende Übersicht zeigt in Anlehnung an die Tabelle 18.1 aus [HMT] S. 876 einen Ausschnitt zum Funktionsumfang von WMI:

Grundkonfiguration	Betriebssystemname, Build-Version Umgebungsvariablen Drucker Datum und Uhrzeit
Hard- und Software	Installierte Software Installierte Updates & Hotfixes Laufende Prozesse Windows Systemdienste Installierte Hardware
Sicherheit	Benutzerkonten (inkl. Ereigniseinträge und Desktopeinstellungen)
Dateisystem und Datenspeicher	Ordner und Dateien des Dateisystems Netzlaufwerksverbindungen Dateisicherheit, Freigabesicherheit Disk Quotas Registrierungsdatenbank
Netzwerk	IP-Routing Netzwerkverbindungen und Sitzungen DNS-Server ASP.NET Terminal Services

Tabelle 1: Übersicht Funktionsumfang WMI

Das WMI wurde mit jeder neuen Version von Windows stetig verbessert. Jedoch gibt es für ältere Windows Versionen keine Update Möglichkeit für das WMI und somit gibt es nur mit den aktuellen WMI Versionen bzw. Windows Versionen vollen Funktionsumfang.

Da WMI ein objektorientiertes Konzept zugrunde liegt, werden alle Informationen als strukturierte Objekte bereitgestellt. Diese strukturierten Objekte sind Instanzen von Klas-

sen und enthalten jeweils das konkrete Vorkommen von Informationen, welche die Klassen beschreiben. Auf dem Dateisystem sind die Objekte und Klassen als DLL[9]-Bibliotheken realisiert.

1.7.3 Internet Control Message Protocol

Das Internet Control Message Protocol (ICMP) stammt aus der Zeit der Entstehung des Internet Protocol (IP). Damals, um 1983, entstand das Internet Protocol für die Kommunikation im „Catanet“, einem für das Militär entwickelte Netzwerk [TS] S. 33. Da das IP jedoch an sich „unzuverlässig und verbindungslos ist“ [TS] S. 33, wurde ein auf das IP aufbauendes Transmission Control Protocol (TCP) entwickelt. Wie früher werden auch noch heute die verschiedenen Netze durch Gateways verbunden. Dafür wurde das Gateway-to-Gateway Protocol (GGP) weitgehend durch das Routing-Information Protocol (RIP), welches die Kommunikation zwischen den Netzknoten regelt, abgelöst. Für die Kommunikation zwischen den Endgeräten wird TCP verwendet. Eine Notwendigkeit zur Kommunikation besteht jetzt noch zwischen den Endgeräten und Gateways. Hierfür kommt ICMP zum Einsatz. Die Aufgaben sind die „Sicherstellung einer reibungslosen und zuverlässigen Kommunikation im Netzwerk“ [TS] S. 34. Somit können in einigen Fällen auch ICMP Nachrichten zwischen Endgeräten zur Sicherstellung des reibungslosen Austausches von Paketen verschickt werden.

Das ICMP umfasst mehrere verschiedene Nachrichtentypen [TS] S. 38-58. Einige für das Verständnis von Monitoring Möglichkeiten relevante werden nachfolgend vorgestellt.

Zwei der wichtigsten sind `echo` und `echo reply`. Einer Echo Nachricht folgt bei erfolgreicher Auswertung der Zielstelle die `echo reply` Nachricht, mit demselben Datenbereich in unveränderter Form.

Als nächsten Typ gibt es `destination unreachable`. Dieser Typ beschreibt sechs verschiedene Gründe für eine Nichterreichbarkeit des angesprochenen Netzwerkgerätes.

net unreachable: Diese Nachricht wird generiert, wenn der Weg zum Ziel Netz, welches durch das Ziel des Paketes definiert ist, nicht bekannt ist bzw. gefunden werden kann.

host unreachable: Tritt ein, wenn das Zielsystem nicht erreichbar ist.

protocol unreachable: Verwenden die Gateways unterschiedliche Protokolle zur Übertragung, wird die Meldung `protocol unreachable` ausgeben.

port unreachable: Gibt es auf dem Zielsystem keinen Prozess der auf dem Ziel Port Pakete entgegennimmt, sendet das Gateway als Fehlermeldung „Port nicht erreichbar“.

---

[9] Dynamik Link Library: Dynamische Programmbibliothek

fragmentation needed: Wenn bei der Übertragung die Nicht-Fragmentierung von Paketen eingestellt ist und ein Paket die Größe der Maximum Transfer Unit (MTU) überschreitet, wird die ICMP Nachricht `fragmentation needed` zurückgegeben.

source route failed: Beim „Source Routing“ ist der Weg zum Zielsystem für die Gateways vorgegeben. Ist nun eine vorgegebene Verbindung zwischen den Gateways nicht mehr verfügbar, wird das Paket verworfen. Das Gateway sendet `source route failed`.

Ein weiterer wichtiger Typ ist `time exceeded`. Bei der Paketübermittlung können verschiedene Ursachen für eine Zeitüberschreitung auftreten. Dabei wird in `time to live exceeded` und `fragment reassembly time exceeded` unterschieden.

time to live exceeded: Das sogenannte Time-to-Live (TTL) Feld im IP Paketkopf enthält die Angabe, über wie viele Gateways das Paket geschickt werden darf, bis es verworfen wird. Jeder Gateway senkt die Zahl um eins ab beim weiterleiten des Paketes. Ist nun das Feld auf den Wert null gesunken, wird der Absender informiert.

fragment reassembly time exceeded: Wenn Pakete zu groß sind, also z.B. die MTU überschreiten, werden diese Fragmentiert und meistens unsortiert und über verschiedenste Routen an den Empfänger geschickt. Die ankommenden Fragmente werden für eine gewisse Zeit gespeichert, um später wieder zusammengesetzt werden zu können. Läuft jedoch diese Zeit ab bevor alle anderen Fragmente des Paketes angekommen sind, so werden die Fragmente mit der Fehlermeldung `fragment reassembly time exceeded verworfen`.

Bei Transportproblemen, welche auf einen Fehler im IP-Kopf zurückzuführen sind, kann ICMP die Nachricht `paramter problem` erzeugen.

parameter problem: Manchmal kann ein Empfänger auf Grund eines syntaktischen Fehlers im IP Paketkopf das Paket nicht korrekt verarbeiten. Dabei kann der Empfänger den Absender mit der `parameter problem` Nachricht mitteilen, das der Paketkopf und welches betroffene Oktett syntaktisch fehlerhaft ist.

Um die Laufzeit von Paketen in Erfahrung zu bringen, gibt es im ICMP Protokoll zwei Nachrichtentypen: `timestamp` und `timestamp replay`.

timestamp: Bei einem `timestamp` Paket wird ein Zeitstempel bei abschicken der Nachricht in das 1. von drei Feldern geschrieben. Die beiden anderen Felder bleiben leer bzw. werden auf null gesetzt.

timestamp reply: Wenn ein System eine `timestamp` Nachricht erhält, wird sofort ein Zeitstempel in das 2. Feld gesetzt. Dabei ist es bereits Möglich, die Zeitspanne wie lange das Paket unterwegs war, zu errechnen. Jedoch ist dann außer acht, wie lange das Paket bearbeitet wird. Dafür wird nach dem Bearbeiten kurz vor dem Absenden ein erneuter Zeitstempel in das 3. Feld geschrieben.

Für die Analyse welchen Weg ein Paket nimmt über mehrere Gateways, wurde der Nachrichtentyp `traceroute` sowie eine Erweiterung im IP-Protokoll um die Option `traceroute` im Paketkopf eingeführt. Das Zusammenspiel zwischen den Konstrukten erlaubt die Verfolgung eines Paketes über mehrere Gateways.

traceroute: Ein `traceroute` Paket signalisiert dem passierendem Gateway, das es eine `traceroute successfully forwarded` Nachricht an den Absender schicken muss. Dabei wird das eigentliche `traceroute` Paket trotzdem weiter an das Ziel bzw. den nächsten Gateway zugestellt.

traceroute successfully forwarded: Diese Nachricht bekommt der Absender nach jedem passierten Gateway. Dabei werden Informationen wie z.B. Anzahl der bisher passierten Gateways mitgegeben.

no route to traceroute target: Kann ein Gateway ein `traceroute` Paket nicht weiterleiten, schickt es die Nachricht `no route to traceroute target` an den Empfänger zurück.

Auf ICMP basierende Werkzeuge sind auf jedem Windows Rechner bereits installiert. Einige Switches bieten ebenfalls eine Reihe dieser nützlichen Tools.

1.7.3.1 PING

Das Programm PING (Abbildung 5) verwendet die beiden ICMP Nachrichten Echo und Echo Reply. Es kann für die Ermittlung der Erreichbarkeit von Geräten im Netzwerk eingesetzt werden. Dieses Tool ist auf fast jedem System, sogar auf Switchen implementiert. Neben dem erfolgreichen Eintreffen der Echo Reply Nachrichten werden auch Paketlaufzeiten ausgegeben. Eine ausführliche Parameterbeschreibung gibt die Anlage 7, „Das Tool PING“.

```
nms$ ping -n -c3 172.17.2.1
PING 172.17.2.1 (172.17.2.1) from 172.17.2.85 : 56(84) bytes.
64 bytes from 172.17.2.1: icmp_seq=1 ttl=64 time=0.492 ms
64 bytes from 172.17.2.1: icmp_seq=2 ttl=64 time=0.307 ms
64 bytes from 172.17.2.1: icmp_seq=3 ttl=64 time=0.302 ms
64 bytes from 172.17.2.1: icmp_seq=2 ttl=64 time=0.313 ms
64 bytes from 172.17.2.1: icmp_seq=3 ttl=64 time=0.301 ms

--- 172.17.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4246ms
rtt min/avg/max/mdev = 0.301/0.343/0.492/0.075 ms
nms$
```

Abbildung 5: Beispiel Verwendung Ping [TS] S. 59

1.7.3.2 Traceroute / Tracert

Traceroute, bzw. Tracert ist ebenfalls auf vielen Systemen bereits implementiert und steht für Diagnosezwecke zur Verfügung. Die Funktionen des Tools gehen weit über die des Ping hinaus. Denn wenn ein Ping Befehl fehlschlägt, lässt sich mittels `traceroute` herausfinden, bis wohin das Paket noch erfolgreich weitergeleitet wurde. Dabei werden mehrere Echo Pakete erzeugt, wobei die maximale Lebensdauer auf ein Minimum gesetzt wird. Das erste Paket besitzt somit immer die Lebensdauer 1. Dann wird beim 2. Gateway das Paket verworfen und die IP-Adresse des Gateways sowie die Laufzeit des Paketes zum Absender zurück geschickt. Folgend wird die Lebensdauer auf 2 erhöht und wieder ein Echo Paket versendet. Diese Prozedur wird solange wiederholt, bis das Paket schließlich entweder am Empfänger angekommen ist oder aber der nicht erreichbare Gateway gefunden wurde. Die folgende Abbildung zeigt ein Beispiel für die Verwendung von `tracert` unter Windows (Abbildung 6).

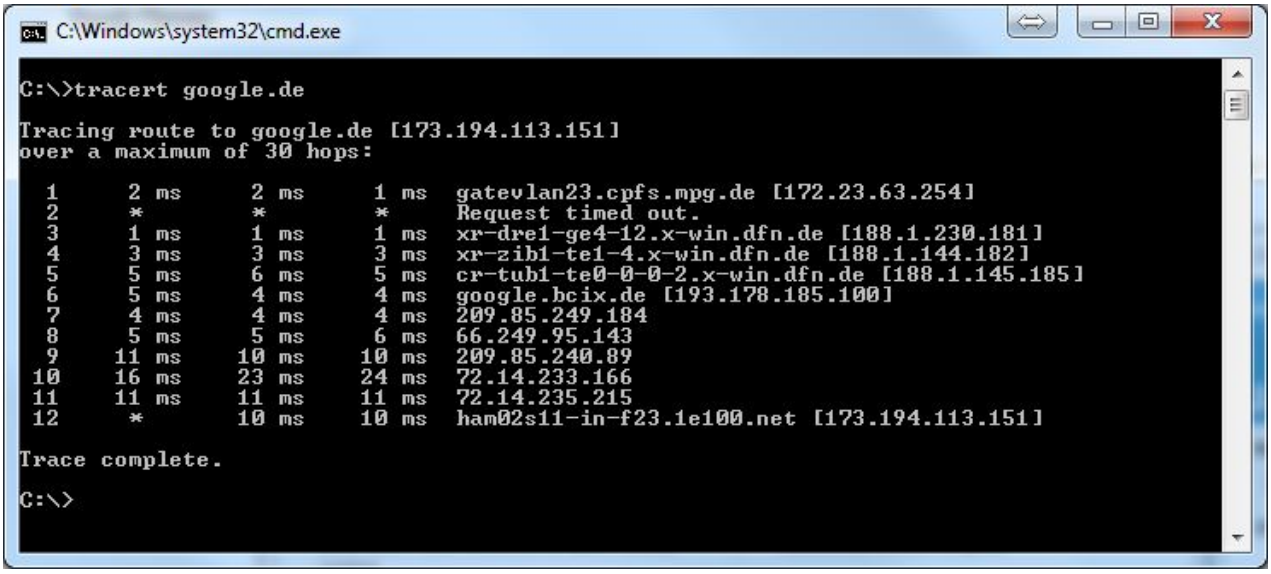

Abbildung 6: Beispiel Verwendung Tracert

1.7.4 Syslog

Jedes Gerät ist in der Lage Ereignisse in einer geeigneten Form zu speichern. Gemeint ist damit das sogenannte Logging. Gibt es im Netzwerk einen entsprechenden Syslog-Server der auf dem Port 514 UDP Nachrichten entgegennimmt, können die von den Netzwerkkomponenten erzeugten Logs direkt an den Syslog-Server geschickt werden.

Die Syslog Architektur umfasst dabei 3 Kernfunktionen: Die Geräte welche die Ereignisse verschicken, die Nachrichtensammler welche die Ereignisse entgegennehmen und die Relaisstationen, welche zur Weiterleitung von Nachrichten dienen.

Die Nachrichten werden mit einer Kritikalität versehen. Somit kann ein Nachrichtensammler mit Hilfe der Kritikalität Entscheidungen über die Bearbeitungspriorität treffen. Folgende Tabelle beschreibt die acht möglichen Kritikalitäten:

Kritikalität	**Beschreibung**
debug(7)	Es werden Debug-Informationen vom System übermittelt
informational(6)	Das angegebene System macht eine unkritische Meldung
notice(5)	Das System arbeitet in der Nähe der definierten Grenzwerte
warning(4)	Es wurde eine Warnung für das System herausgegeben
error(3)	Das angegebene System weist einen Fehler auf
critical(2)	Das System befindet sich in einem kritischen Zustand
alert(1)	Es besteht dringender Handlungsbedarf für das System
emergency(0)	Das angegebene System ist zur Zeit unbrauchbar

Tabelle 2: Kritikalitäten Syslog [TS] S. 153

Viele der Managementplattformen bzw. Softwarelösungen beinhalten einen Syslog Server. Die Konfiguration von Netzwerkkomponenten für die Verwendung von Syslog ist relativ einfach. Für einen HP Switch reicht z.B. der Befehl

```
logging 172.20.1.96 control-descr PCMSRV
```

aus, um das Versenden von Geräteereignissen an die genannte IP-Adresse unter der Bezeichnung „PCMSRV“ zu konfigurieren.

Damit ein System die Herkunft von Syslog Nachrichten erkennt, gibt es noch eine weitere Klassifizierung: die sogenannte Facility (Tabelle 3).

Facility	Beschreibung
kern(0)	Meldungen des Betriebssystemkerns
user(1)	Syslog Nachrichten von Applikationen des Benutzers
mail(2)	Pakete des Mail-Systems
daemon(3)	Meldungen von Systemdiensten
auth(4)	Nachrichten aus dem Bereich Sicherheit und Authentifizierung
syslog(5)	Syslog-eigene Pakete
lpr(6)	Meldungen des Druckersystems
news(7)	Pakete des Nachrichtendienstes
uucp(8)	Nachrichten des Unix-to-Unix Commnications Package (UUCP)
cron(9)	Meldungen des Cron-Dienstes
authpriv(10)	Nachrichten aus dem Bereich Sicherheit und Authentifizierung
ftp(11)	Syslog Pakete von File Transfer Protocol (FTP) Servern
ntp(12)	Syslog Meldungen von Network Time Protocol (NTP) Servern
audit(13)	Meldungen vom Typ “Log Audit”
alert(14)	Meldungen vom Typ “Log Alert”
at(15)	Nachrichten des Automatisierungsdienstes “AT”
local0(16)	Vom Benutzer frei definierbarer Meldungstyp
local1(17)	Vom Benutzer frei definierbarer Meldungstyp
local2(18)	Vom Benutzer frei definierbarer Meldungstyp
local3(19)	Vom Benutzer frei definierbarer Meldungstyp
local4(20)	Vom Benutzer frei definierbarer Meldungstyp
local5(21)	Vom Benutzer frei definierbarer Meldungstyp
local6(22)	Vom Benutzer frei definierbarer Meldungstyp
local7(23)	Vom Benutzer frei definierbarer Meldungstyp

Tabelle 3: Facilities in Syslog [TS] S. 154

Da für Syslog kein einheitlicher Standard existiert, kann es sein das nicht alle Facilities auf allen Geräten existieren.

1.7.5 Weitere Protokolle zum Netzwerkmanagement

Die wichtigsten aller Protokolle für das Verwalten des Netzwerkes wurden bereits in den vorhergehenden 4 Abschnitten beschrieben. Einige weitere werden in diesem Abschnitt kurz erläutert. [JH] S.103-111

RMON: Remote Network Monitoring Management Information Base; Dient dem Erfassen von Netzdaten und dem Sammeln von Messwerten. Diese können zu einem anderen Zeitpunkt abgefragt werden.

SMON: Remote Network Monitoring MIB Extension for Switched Networks Version; Ist eine Erweiterung des RMON mit Objektgruppen, welche das Benutzen von RMON in Netzwerken mit VLANs ermöglichen.

NetFlow: Von der Firma Cisco entwickeltes Protokoll welches dazu genutzt wird, Datenflüsse im Netzwerk nachverfolgen zu können.

IPFIX: Weiterentwicklung von NetFlow durch die IETF.

1.8 Begriffe

Zum besseren Verständnis der Problemstellung und Lösung dieser Arbeit, werden hier zwei weitere Begriffe erklärt und beschrieben.

Protokoll (Netzwerk): Ein Protokoll ist eine Beschreibung, wie 2 oder mehrere Systeme miteinander kommunizieren können. Darin ist geregelt, wie dieser Informationsaustausch vonstattengehen soll.

Script: Bezeichnet eine Abfolge von Befehlen, verpackt als kleines Programm.

2 Erfassung des Ist-Zustandes

Die Erfassung des Ist-Zustandes hilft bei der Ermittlung der Schwerpunkte und zeigt bestehende Schwächen im Monitoring.

2.1 Ablauf der Erfassung

Ein Ist-Zustand beschreibt immer den jetzt vorherrschenden Bestand der Sache. In diesem Fall geht es um die genaue Beschreibung der vorhanden Hardware und Software, welche mit dem Monitoring zusammenhängen. Somit gilt es, die aktiven Netzwerkkomponenten, Server und Computer zu lokalisieren und deren zu überwachende Dienste und Funktionen zu notieren. Dabei erkannte Schwächen im Monitoring sind gesondert zu kennzeichnen. Auf den Systemen sind ebenso die Konfigurationen zu überprüfen. Dabei geht es speziell darum, wie die Geräte sich derzeit von selbst an eine Managementstation bei Fehlern wenden, z.B. ob und wie ein Switch SNMP Nachrichten verschickt.

2.2 Überblick an Hand des Beispiels MPI-CPfS

Im Max-Planck-Institut für chemische Physik fester Stoffe gibt es nahezu alle Arten von netzwerkfähigen Geräten:

Drucker, Computer, IP-Kameras, Handys, Server, Router, Switche u.v.m.

Dazu reicht die Vielfalt der Betriebssysteme von Windows und Linux bis hin zu Mac OS.

Eine Übersicht über die gesamte Technik im MPI zeigt Tabelle 4:

Typen	Anzahl
Windows Rechner	444
Linux Rechner	39
Mac OS Rechner	11
Server	35
Switche	74
IP-Kameras	17
Netzwerkfähige Drucker	45

Tabelle 4: Übersicht Technik (Quelle Active Directory, ProCurve Manager, Jetadmin)

Die Überwachung der aktiven Netzwerkkomponenten, sprich Switches, erfolgt mit der Software ProCurve Manager der Firma Hewlett Packard. Auf dem Server „PCMSRV“ ist

als Betriebssystem Windows 2008 R2 Server Enterprise installiert. Diese Geräte werden nach festgelegten Intervallen auf ihre Erreichbarkeit mittels PING geprüft. Manche Switches sind für SNMPv3 bereits konfiguriert, jedoch nicht für den Versand von Traps. Andere wiederum haben ebenfalls die Einstellungen für SNMPv3, senden aber über SNMPv2c Traps an den Managementserver. Die von den Geräten erzeugten Ereignisse werden derzeit an einen Kiwi Syslog Server geschickt, der ebenfalls auf dem „PCMSRV“ installiert ist.

Die Drucker werden mittels HP Web Jetadmin verwaltet. Die Software ist auf dem „PRNSRV“, einem Windows 2008 R2 Server Standard installiert. Alle relevanten Informationen wie Toner und Papierstand sowie Gesamtzustand der Drucker sind abrufbar. SNMP ist in der Version 1 und 2c aktiviert und das Senden von Traps eingestellt.

Über HP System Insight Manager (HP SIM) erfolgt die aktive Überwachung der Server. Diese Software läuft auf dem „LSERV“, einem Windows 2003 Server Enterprise System. Dabei werden Informationen über das Betriebssystem, Management Protokolle, Firmware und Software Versionen angezeigt.

Ein Monitoring anderer Geräteklassen ist derzeit nicht vorgesehen.

2.3 Schwerpunkte

Beim Sichten des Ist-Zustandes wurden einige Schwachpunkte im Monitoring entdeckt. Seit Anfang des Jahres wurde im Max-Planck-Institut das WLAN-Zugangssystem Eduroam[10] installiert und bereitgestellt. Derzeit können die dafür notwendigen WLAN Access Points[11] (APs) jedoch noch nicht in einer der drei Lösungen hinzugefügt werden. Somit wird bei Ausfall oder Störung eines APs die IT-Abteilung nicht informiert.

Bei der Erfassung und Prüfung der Software zeigt der ProCurve Manager und auch System Insight Manager sehr viele unbekannte Geräte im Netzwerk. Meistens sind es Computer oder Switche, zu denen die entsprechende MIB nicht vorhanden ist.

Im ProCurve Manager sind keine Logs von den Geräten zu sehen. Auch empfängt der ProCurve Manager keine Traps. Somit können Fehler im Netzwerk oder auf den Servern nur in bestimmten Intervallen festgestellt werden, nämlich wenn der ProCurve Manager den routinemäßigen Erreichbarkeitstest durchführt.

[10] Eduroam: Ist ein internationales Projekt zur Bereitstellung eines Internetzuganges für jeden Mitarbeiter oder Gast mit einem gültigen Account

[11] Access Point: Zugangspunkt für drahtlose Endgeräte

2.4 Zusammenfassung IST-Zustand

Insgesamt stehen drei Monitoring Lösungen zur Verfügung, welche grundlegende Überwachungsfunktionen abdecken. Für den Administrativen Aufwand ist diese Konstellation mit der Verteilung des Monitorings über drei Systeme jedoch impraktikabel. Ein Administrator muss somit immer alle drei Überwachungsprogramme im Überblick behalten. Ein als noch kritischer anzusehender Fakt ist, dass zwei der Lösungen keine SNMP Traps empfangen können und somit ein Ausfall von Teilkomponenten, z.B. ein Lüfter in einem Switch, frühestens nach einem intervallbedingten Scan festgestellt werden kann.

Folgende Übersicht (Abbildung 7) fasst den Gesamtzustand noch einmal übersichtlich zusammen:

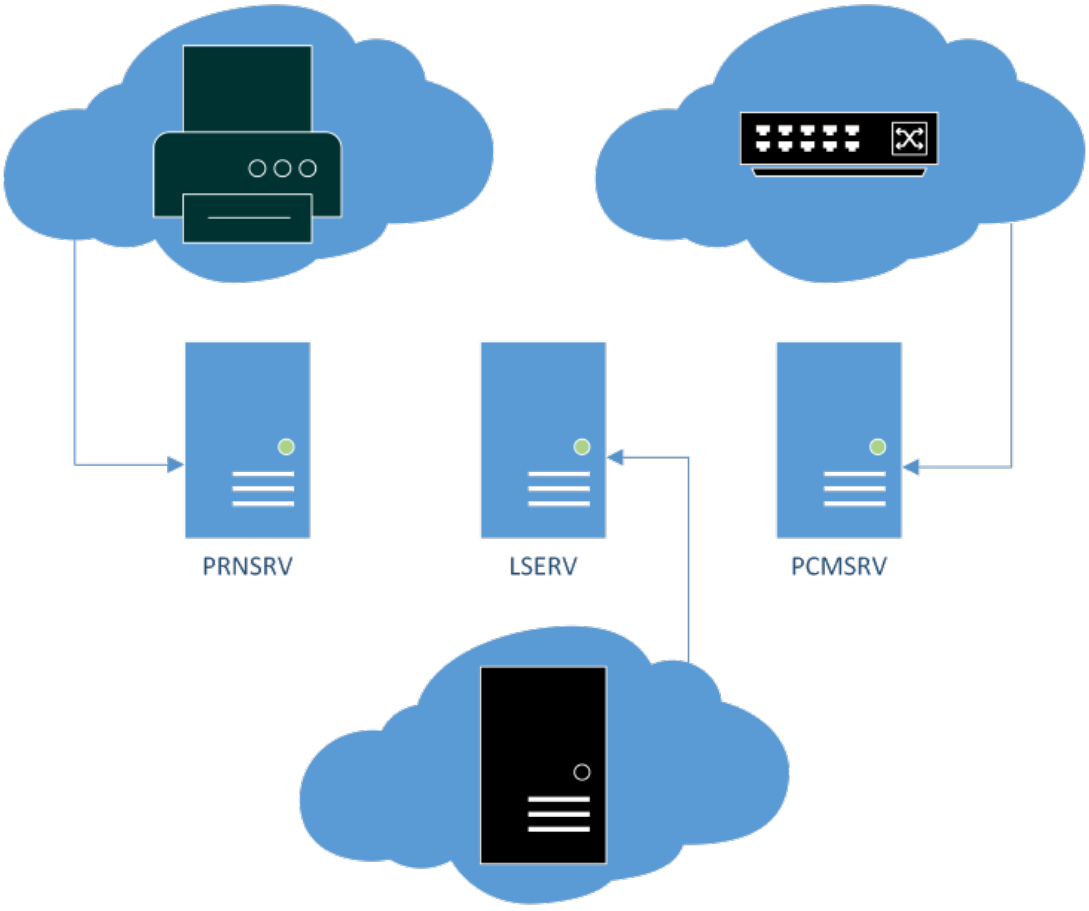

Abbildung 7: Übersicht IST-Zustand

Wenn neue Geräte in das bestehende Netzwerk hinzugefügt werden, fehlt meist die nötige Unterstützung der Software für die diese Geräte.

3 Anforderungsanalyse

Vor dem Kauf einer Software oder der Einführung einer Open Source Lösung gilt es die Anforderungen, welche an das System gestellt werden sollen, herauszufinden. Die allgemein zu beachtenden Punkte zeigt der erste Abschnitt dieses Kapitels.

3.1 Überlegungen zur Anforderungsanalyse

Bei genauer Betrachtung und Überlegung, tauchen viele Fragen auf [TT]:

- Wie viele Geräte sollen überwacht werden?
- Welche Gerätearten und –typen betrifft es?
- Welche zukünftigen Erweiterungen sind im Netzwerk geplant?
- Welche Mittel und Ressourcen stehen zur Verfügung?
- Was genau soll jeweils überwacht werden?
- Wie soll der Zugriff auf die Software erfolgen?
- Welche Präsentation und Aufbereitungsmöglichkeiten der Daten soll es geben?
- Über welchen Weg soll die Alarmierung im Notfall verfügbar sein?
- Welche Möglichkeiten der Erweiterung sollte die Software haben?

Einige dieser Fragen beantwortet bereits die IST-Analyse. Jedoch sind die anderen Fragen mithilfe der IT-Abteilung abzustimmen, um zu einer sinnvollen und wirtschaftlichen Lösung zu gelangen.

Eine Neubeschaffung oder ein Update der aktuellen Monitoring Lösung sollte immer einen Mehrwert besitzen oder eine erhebliche Erleichterung für die Administratoren bedeuten.

Die Anzahl der zu überwachenden Geräte spielt eine wichtige Rolle, da einige Anbieter nur eine gewisse Anzahl an Geräten unterstützten. Ebenso muss die entsprechende Software auch bei einer Vielzahl von Komponenten noch die entsprechende Übersicht gewährleisten. Bei einer stetigen oder geplanten Erweiterung des Netzwerkes sollte dies immer mit in die Anzahl eingerechnet werden.

Verschiedene Gerätetypen müssen auch über verschiedene Wege überwacht werden, sprich über unterschiedlichste Technologien. Nicht jede Softwarelösung beherrscht jede der notwendigen Technologien in einem heterogenen Netzwerk.

Die Frage des Budgets trägt einen wichtigen Faktor bei. Dabei wird Entschieden, ob überhaupt eine kommerzielle oder nicht doch eine Open Source oder Freeware Lösung zu beschaffen ist.

Bei einer reinen Überwachung, im Sinne der Erreichbarkeit, würde ein einfacher Ping Befehl verpackt in einem Script ausreichen. Jedoch reichen die Möglichkeiten bis hin zur Abfrage des Systemzustandes (Festplattenauslastung etc.) oder Überwachung von Tasks[12], bei Switches z.B. der Zustand der einzelnen Ports.

Die einfachste Softwarelösung bietet eine Einzelplatzversion als reine Windows Anwendung. Jedoch gibt es z.B. für größere IT-Abteilungen auch die Möglichkeit eines Client-Server Systems oder einer webbasierten Lösung.

Beim Monitoring werden jederzeit Daten gesammelt und diese zu Informationen verarbeitet. Wichtig ist zu wissen, wie diese Informationen aufbereitet und zur Analyse dargestellt und bereitgestellt werden sollen.

Wenn eine reine Alarmierungsmeldung über E-Mail ausreicht, sollte dies fast jede Lösung beherrschen. Jedoch gibt es Situationen, die einen anderen Informationskanal, wie z.B. die Meldung per SMS oder Telefonanruf, vorsehen kann.

Die Software sollte in jedem Fall die Erweiterung der MIB-Bibliothek vorsehen. Es kann nützlich sein, wenn zusätzliche Module oder Scripte einspielt werden können.

3.2 Anforderungsanalyse am Beispiel MPI-CPfS

Am Beispiel des Max-Planck-Institutes lassen sich folgende Anforderungen und Aufgaben erkennen.

Anforderungen

Benötigt wird eine Monitoring Lösung, welche die bisherigen drei Anwendungen komplett ersetzt. Dabei müssen SNMPv1, SNMPv2c und SNMPv3 beherrscht werden. Ebenso muss das Protokoll WMI für Windows Server Systeme unterstützt werden. Damit die Ereignisprotokolle der Geräte zentral erfasst werden können, muss Syslog integraler Bestandteil sein. Die Softwarearchitektur muss auf Client/Server in Form einer Client Anwendung oder der Management Homepage ausgerichtet sein. Als Kritikalität ist alles zu empfangen und zu protokollieren was nicht den Charakter „informativ“ besitzt. Die Software muss übersichtlich gehalten sein und geeignete Werkzeuge und Ansichten zur Datenaufbereitung vorhalten. Als Benachrichtigungsweg dient der Versand per E-Mail. Die Erweiterungsmöglichkeiten sowie das Customizing müssen durch MIB-Import und großzügigen Einstellungs- und Anpassungsmöglichkeiten durchführbar sein.

[12] Tasks: Nach bestimmten Ereignissen automatisch durchgeführte Anwendungen oder Scripte

Eine Zusammenfassung zeigt folgende Tabelle:

Typ	Anforderung
Architektur	Client/Server, Webinterface
Protokolle	SNMPv1, SNMPv2c, SNMPv3, WMI, Syslog
Customizing, Erweiterung	MIB-Import, sehr gute Einstellungsmöglichkeiten
Benachrichtigung	E-Mail

Tabelle 5: Zusammenfassung Anforderungen MPI-CPfS

Aufgaben

Durch die IST-Analyse sind bereits bestehende Schwächen aufgetaucht. Einige davon sind kein Verschulden der eingesetzten Software, sondern liegen an fehlerhaften oder noch nicht vorgenommenen Einstellungen an den zu überwachenden Geräten.

Vor Inbetriebnahme einer neuen Lösung ist jedes Gerät auf die richtigen Einstellungen von SNMP und Syslog zu prüfen und ggf. anzupassen. Das betrifft in erster Linie die Drucker und Switches.

Zusätzlich ist darauf zu achten das am Managementserver der Windows Dienst SNMP aktiviert ist (wichtig, um die Überwachung per SNMP zu aktivieren). Der Dienst SNMP-Traps muss deaktiviert sein, da dieser sonst den Port für den Empfang von Traps blockiert.

4 Lösungsmöglichkeiten im Allgemeinen

Eine Übersicht über Monitoring-Lösungen gibt dieses Kapitel. Dabei gibt es verschiedene Ansätze um überhaupt ein Monitoring zu realisieren. Diese werden zu Beginn erläutert und anschließend eine Entscheidungshilfe gegeben. Im zweiten Teil des Kapitels wird genauer auf die Möglichkeiten des Monitorings und deren Grenzen eingegangen.

4.1 Auslagerung des Monitoring

Eine Möglichkeit um Monitoring im eigenen Unternehmen einzuführen und bereitzustellen, ist die Auslagerung zu einem externen Dienstleister. Hier spricht man auch von Outsourcing.

Große Vorteile sind meist die Spezialisierung der Firmen auf Monitoring und somit oft der Einsatz der neusten Technologien. Wirtschaftlich gesehen, werden die eigenen Ressourcen geschont und der Administrationsaufwand gering gehalten.

Ist bereits eine IT-Abteilung vorhanden, sollte Outsourcing nicht in Betracht kommen, es sei denn die Auslastung ist bereits auf einem hohen Niveau.

Beispielanbieter für das Outsourcing sind:

- ELAXY Monitoring – www.elaxy.com

4.2 Verwendung von Open Source

Bei dem Einsatz von Open Source wird meist auf eine bereits sehr lang etablierte Software zurückgegriffen, welche von einer großen Community weiterentwickelt und unterstützt wird. Jedoch sind die Installation und vor allem die Einrichtung einer solchen Lösung sehr zeitaufwendig. Eventuell resultiert am Ende eine nicht hundertprozentig zufrieden stellende Lösung.

Kurze Übersicht über Open Source Anbieter:

- Nagios – www.nagios.org
- Icinga – www.icinga.org
- Spiceworks – www.spiceworks.com/app

4.3 Verwendung von kommerzieller Software

Der wichtigste Pluspunkt von kommerzieller Software ist der Support des Herstellers. Dieser hilft beim Einrichten oder bei Problemen meist unkompliziert und kompetent.

Natürlich müssen gewisse Mittel vorgehalten werden und auch eine Erweiterung solcher Software ist in den meisten Fällen kostspielig.

Einige Anbieter sind:

- SHD SM-Box – www.systemmonitoring.de
- Paessler PRTG – www.de.paessler.com
- HP SIM – h18004.www1.hp.com/products/servers/management/hpsim
- HP Operations Manager – http://www8.hp.com/de/de/software-solutions/software.html?compURI=1170678
- DSM Discovery – www.offlimits-it.com/produkte/frontrange/discovery.php
- Microsoft System Center 2013 - Operations Manager - http://technet.microsoft.com/de-de/systemcenter/hh285243.aspx

4.4 Entwicklung einer Lösung durch Unternehmen

Wenn das Aufgabenfeld zu komplex wird kann es erforderlich sein, eine Software neu zu entwickeln um damit die Erfordernisse zu erfüllen. Dies ist jedoch mit sehr hohen Kosten verbunden, dafür entsteht so die passende Lösung für ein bestehendes komplexes Problem.

4.5 Entscheidung

Entscheidend ist also in jedem Falle das vorhandene Budget, die Möglichkeit der Planung einer Konfiguration der Software durch die eigene IT oder auch der Support, welcher zu erwarten ist. Die bestehende Monitoring Lösung, wenn vorhanden, ist ebenso mit in eine Entscheidung einzubeziehen. Eventuell könnte diese sogar, durch ein Update oder eine Erweiterung, auch die Anforderungen erfüllen.

Folgende Tabelle bewertet die einzelnen Lösungen hinsichtlich der eben genannten Punkte von „0“ (nicht vorhanden) bis „10“ (vorhanden):

	Kosten	Support	Konfigurationszeit
Open Source	1	3	10
Kommerzielle Software	9	10	4
Outsourcing	5	8	8
Softwareentwicklung	10	10	4
Update/Erweiterung (wenn möglich)	0-5	10	2

Tabelle 6: Klassifizierung der Lösungsmöglichkeiten

Nach dem die Abwägung zwischen den vier Kriterien entschieden ist, können dann entsprechende Produkte gegen die Anforderungen aus Kapitel drei durch eine Marktanalyse gefunden werden.

4.6 Möglichkeiten des Monitorings

Wie bereits in der Einleitung zur Anforderungsanalyse angedeutet, ist das Überwachen des Netzwerkes sehr komplex und kann sogar bis in das kleinste Detail geschehen. Der Abschnitt soll einige Beispiele erklären und Hinweise auf den Sinn des Einsatzes der Überwachungsmöglichkeiten bieten.

4.6.1 Überwachen von Diensten

Bei der Überwachung von Diensten werden die entsprechenden Ports auf Erreichbarkeit geprüft. Gibt es einen administrativen Zugriff, kann unter Umständen sogar automatisch ein Dienst neugestartet werden um die Erreichbarkeit womöglich wiederherstellen zu können. Ein Beispiel ist ein FTP-Server der über den Port 21 ausgeführt wird. Sobald dieser Port geschlossen bzw. nicht mehr erreichbar ist, kann eine Benachrichtigung an einen Administrator ausgegeben oder ein automatischer Neustart des FTP-Servers ausgelöst werden.

4.6.2 Überwachen von Datenbanken

Die Überwachung von Datenbanken geschieht in erster Linie ähnlich dem Prinzip zur Überwachung von Diensten. Einige Softwarehersteller bieten aber eine detailliertere Möglichkeit des Monitorings. Hierbei wird ebenfalls ein administrativer Zugang geschaffen um auf die Management-Applikation des Datenbankservers zuzugreifen und weitere Informationen zu beschaffen. Darunter können z.B. Informationen über die Speicherauslastung der Datenbank oder Performance-Werte sein.

4.6.3 Überwachen von aktiven Netzwerkkomponenten

Aktive Netzwerkkomponenten sind in der Lage bei Auftreten eines Fehlers selbst Nachrichten, sogenannte Traps, abzuschicken. Werden diese von einer Station richtig ausgewertet, erhält der Administrator sofort eine Information zur Ursache des Problems. Eine weitere Möglichkeit des Monitorings ist das intervallmäßige Pingen der Komponenten um die Erreichbarkeit zu überwachen.

4.6.4 Überwachen von Ordnern

In manchen Fällen erweist sich eine Überwachung von Ordnern als notwendig. Dabei wird regelmäßig geprüft, ob eine Veränderung in dem entsprechenden Ordner auftritt. Dies kann z.B. eine durch einen Virus gelöschte Datei sein. Ein weiterer Anwendungsbereich ist die Sicherstellung der Verfügbarkeit von Netzlaufwerken.

4.6.5 Überwachen der Ressourcenauslastung

Ein Server oder eine Datenbank ist bei erhöhter Auslastung im Regelfall zwar erreichbar, aber sehr langsam. Um solche Probleme sofort beim Auftreten zu erkennen, können die Prozessorauslastung, die Auslastung des Arbeitsspeichers oder sogar die Auslastung der Festplattenkapazität überwacht werden um gegebenenfalls weitere Schritte einzuleiten.

4.6.6 Überwachen von Druckern

Die Überwachung von Druckern geschieht im Regelfall ebenfalls über das SNMP Protocol. Dabei kann u.a. abgefragt werden, wie der aktuelle Tonerstand ist oder auch der Füllstand in den Papierfächern. Eine Fehlermeldung bei einem eventuell aufgetretenen Papierstau sendet der Drucker ebenfalls über SNMP an die Managementstation.

4.7 Grenzen des Monitorings

Die Hersteller von Monitoring Lösungen entwickeln stetig neue Möglichkeiten um das gesamte Portfolio von Komponenten und Diensten abzudecken. Doch auf Grund der Komplexität und Vielfältigkeit, welche von den Möglichkeiten des Monitorings ausgehen, spielt eine gewissenhafte und durchdachte Vorgehensweise und Pflege eines Monitoring Systems eine entscheidende Rolle. Denn das Monitoring ist nur so gut, wie es eingerichtet und gepflegt wird. Regelmäßige Tests über die Genauigkeit, Schnelligkeit und Funktion des Systems sollten durchgeführt werden. Für die administrative Gruppe ist es von hoher Bedeutung sofort nach einem Ausfall benachrichtigt zu werden. Doch könnte auf Grund einer Fehlkonfiguration im SNMP-Modul des Gerätes der Ausfall einer Komponente erst zu spät bemerkt werden.

5 Spezielle Lösung am Beispiel MPI-CPfS

Das Max-Planck-Institut für Chemische Physik fester Stoffe sucht nach einer einheitlichen Gesamtlösung für ihr Netzwerk Monitoring. Eine Software für alle Komponenten auf einem System. Da der Markt sehr breit gefächert ist, wird es trotz genauer Anforderungen schwer ein geeignetes Monitoring System zu finden. Nachfolgend werden einige Lösungen verglichen und in einer realen Umgebung geprüft.

5.1 Software im Vergleich

Vier verschiedene Lösungen werden in der realen Umgebung getestet und somit vorgestellt. Wichtig ist die Erfüllung der Anforderungen, um die Entscheidung für die richtige Software zu finden.

Als Testrechner wurde ein HP Server verwendet. Dieser war früher für das Backup zuständig und wurde nun abgelöst. Damit dieser sich selber auch über SNMP Abfragen kann, muss im Betriebssystem der Dienst SNMP eingerichtet, bzw. erst installiert werden. Für die reale Testumgebung ist die MAC[13]-Adresse der Netzwerkkarte in das entsprechende VLAN[14] (in diesem Fall das VLAN „Server“) einzutragen, damit die Station die Erlaubnis hat mit den Netzwerkkomponenten (z.B. Switches) zu kommunizieren. Diese Vorgehensweisen sind in den Anlagen 1 „Einrichtung von SNMP“ und 2 „Einstellen des VLAN“ beschrieben. Wenn die Managementstation vorbereitet ist, gilt es noch die Switche so zu konfigurieren, das diese ihre SNMP Traps an den Manager schicken. Dies ist in Anlage 3 „SNMP Konfiguration des Switch“ beschrieben.

5.1.1 HP SIM

Die Software, welche bereits vorhanden ist, bietet neben der Unterstützung für alle HP Server und Netzwerkprodukte auch eine grundlegende Funktion für Nicht-HP Server. Die jetzige Version zeigt sehr viele unbekannte und nicht administrierbare Geräte auf (siehe Abbildung 8). Dabei ist zwischen System Type „unknown“ und „unmanaged“ zu unterscheiden. Der Typ „unknown“ kommt vor, wenn ein System nicht klassifiziert werden kann. Der Typ „unmanaged“ hingegen, wenn das System schlichtweg nicht verwaltet wer-

[13] MAC: Media-Access-Control; Hardware Adresse einer Netzwerkkarte, eindeutig und einmalig

[14] VLAN: Virtual Local Area Network; “Bildung von logischen LANs auf einem physischen LAN” [HSB] S. 362

den kann, da kein entsprechendes Management Protokoll unterstützt wird, und somit nur die Überwachung mittels Ping verfügbar ist.

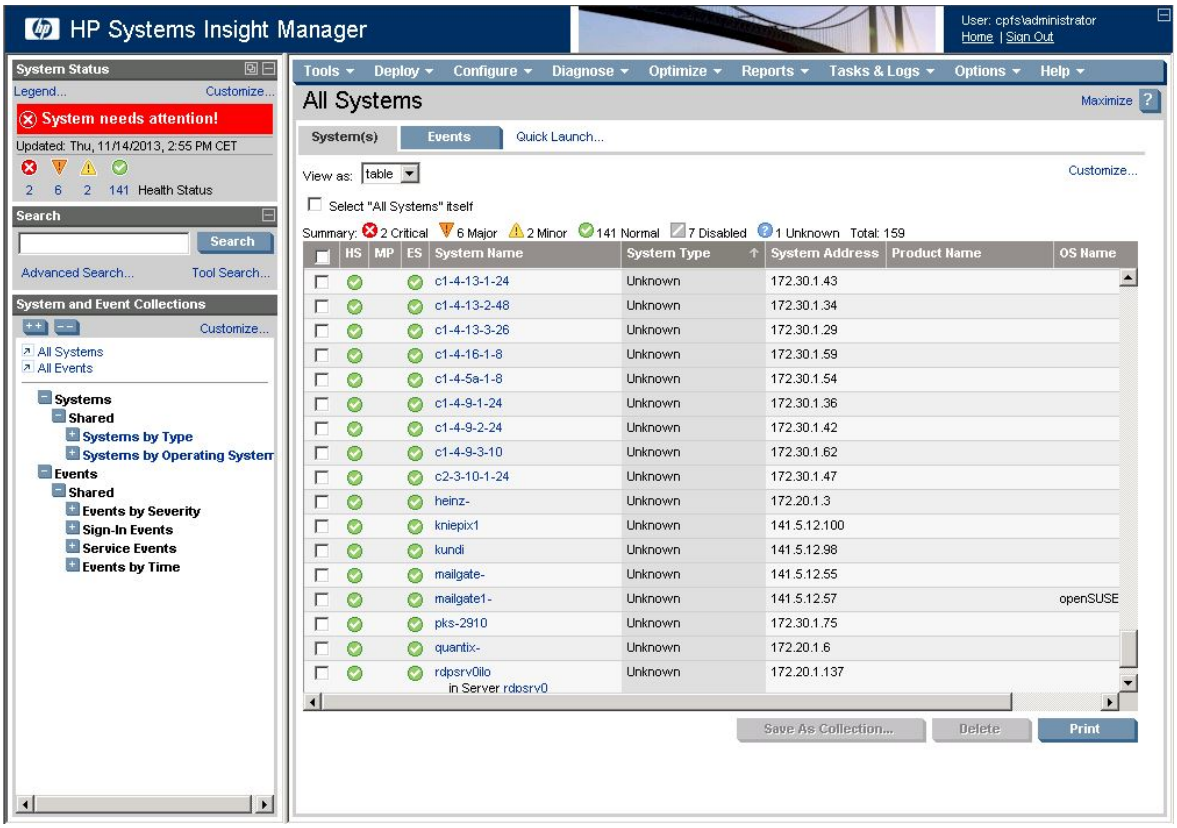

Abbildung 8: Unbekannte Geräte im HP SIM

Die meisten der hier unbekannten Geräte sind Switches. Einige wenige andere Geräte sind Linux Rechner. Ein Update der MIBs und auch der Software ist möglich.

5.1.2 HP-SIM in der Praxis

Derzeit läuft HP-SIM mit der Version 6.2 und es wird ein Update mit der Version 7.2 geprüft. Die Installation läuft selbsterklärend vonstatten. Dabei wird ein Microsoft® SQL Server 2008 Express RS SP1 installiert, es sei denn es gibt bereits einen anderen Datenbankserver. Dann kann dieser ebenfalls als Datenbankinstanz verwendet werden.

Nach dem Start von HP SIM wird eine allgemeine Erstkonfiguration durchgeführt. Dabei müssen unter anderem der SNMP Community String sowie ein Login Account, z.B. für Server, um Zugriff auf das WMI zu haben, angegeben werden. Hier fällt bereits auf, dass es keine Unterstützung für SNMPv3 gibt. Damit das System automatisch nach den Netzwerkkomponenten sucht und zur Überwachung hinzufügt, müssen die IP-Adressen bzw. IP-Bereiche eingegeben werden.

Nach dem der Discovery-Wizard abgeschlossen ist, sind alle im Netzwerk gefundenen Geräte aufgelistet. Dabei tauchen einige „unmanaged“ Geräte auf, dies sind Netzwerk-

komponenten welche z.B. durch Controller verwaltet werden. Anderenfalls sind aber auch Geräte aufgetaucht welche immer noch den Status „unknown“ haben. Um das Problem der falschen Anzeige des Status zu lösen, ist eine Anpassung der MIBs notwendig. Deshalb werden die entsprechenden MIBs durch ein Werkzeug in das Programm integriert.

Dabei müssen alle relevanten MIB Dateien in den „mibs“ Ordner des Programmes gespeichert werden.

Damit HP SIM mit den Dateien arbeiten kann, werden diese nun kompiliert mit Hilfe des Tools „mxcompile“.

```
dir *.mib /b >> mib.list
for /f %A IN (mib.list) DO mcompile %A
```

Der erste Befehl erstellt eine Liste mit allen im Ordner gefundenen MIBs. Anschließend führt der zweite Befehl für jede MIB den Kompilierungsvorgang durch.

Jetzt gilt es die fertigen CFG-Dateien in das HP SIM zu integrieren. Dafür gibt es das Tool „mxmib“.

```
dir *.cfg /b >> cfglist.list
mxmib -f cfglist.list
```

Um wieder eine Liste zu generieren wird der erste Befehl „dir“ verwendet. Danach startet mxmib mit dem Parameter „f“ den Importvorgang aus der vorher generierten Liste.

Jetzt ist die Grundlage geschaffen, damit HP SIM die OIDs der noch nicht erkannten Geräteklassen erkennen kann. Nun fehlt nur noch die Verknüpfung der MIBs mit den Geräten. Dafür benötigt man sämtliche OIDs der noch nicht bekannten Netzwerkkomponenten. Im HP SIM unter „Options“ / „Manage System Types“ müssen neue Produkt Identifizierungsregeln angelegt werden (Abbildung 9).

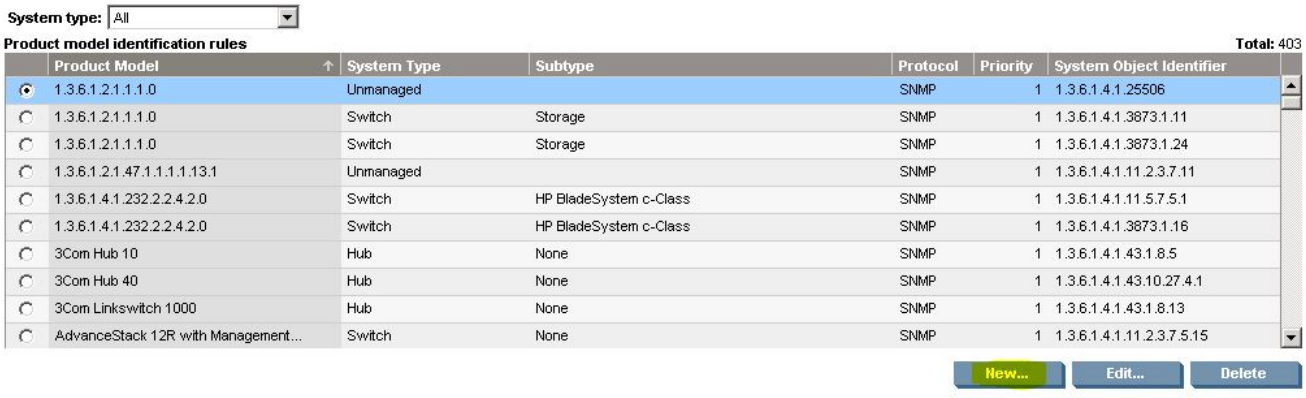

Abbildung 9: Übersicht erkennbare Produkte HP SIM

Bei der Erstellung der neuen Regel müssen `System object identifier` und `product model` eingegeben werden. Zusätzlich aus dem Feld `System type` noch die entsprechende Geräteklasse auswählen (Abbildung 10).

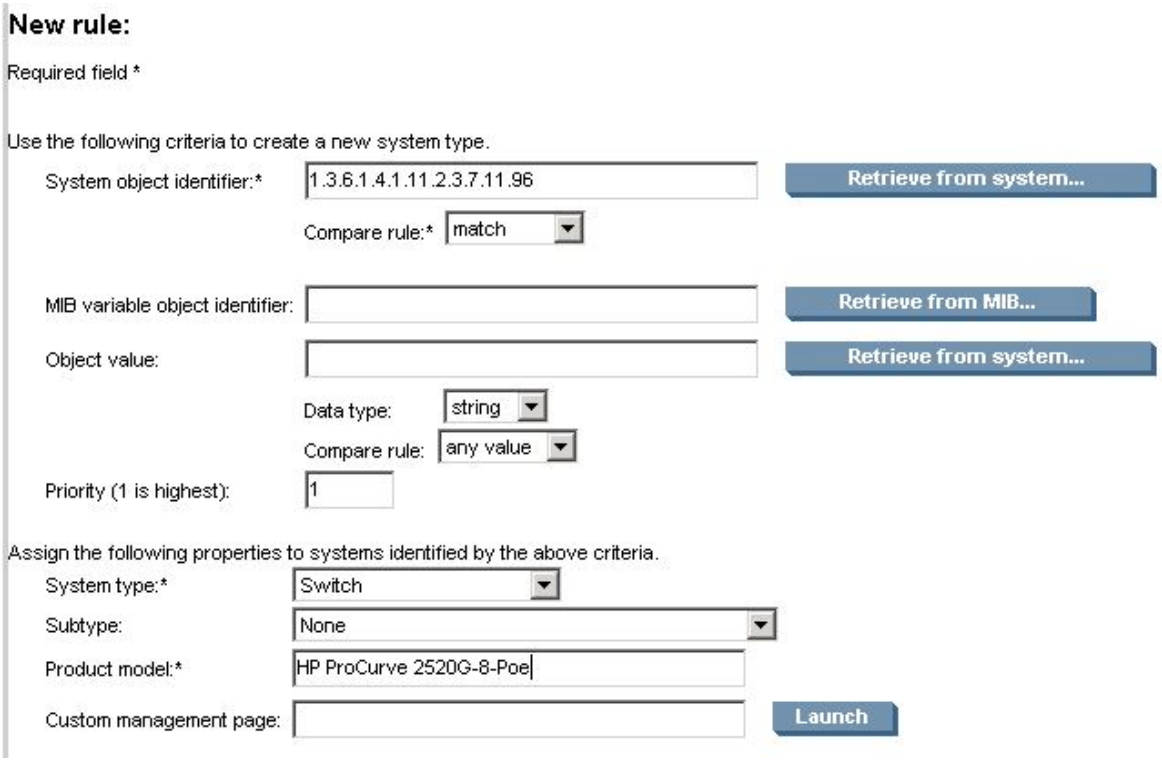

Abbildung 10: Erstellen einer Regel im HP SIM

Nach einem neuen Discovery Durchlauf sind alle Geräte mit ihren Eigenschaften aufgenommen.

Der Systems Insight Manager bietet für Drucker einige grundlegende Informationen sowie die Links zur Management Homepage. Für Server, Switche und Storage hingegen sind weitaus mehr Informationen verfügbar, z.B. Firmware Status und Informationen für den Management Prozessor. Das wichtigste aber fehlt: Eine Unterstützung für den Empfang von SNMP Traps. Im Test konnten keine SNMP Traps empfangen werden. Es wird vom Programm selbst auch nicht an einem Port auf Trapnachrichten gewartet.

5.1.3 ManageEngine OpManager

Der OpManager von ManageEngine bietet eine große Auswahl an Features und unterstützt sämtliche Komponenten. Beworben wird das Produkt mit der Möglichkeit der Überwachung von Switchen, Router, Druckern und Servern bis in das kleinste Detail.

Somit können neben einem Datenbankserver an sich, auch die Datenbank selbst überwacht werden. Weiterhin bietet OpManager sogar das Überwachen der Festplattenauslastung oder Prozessorauslastung von Rechnern an.

Die komplette Liste der Features kann unter der Website http://www.manageengine.com/network-monitoring/features.html eingesehen werden.

Durch die Benutzung von einzelnen Fenstern im Dashboard kann sich jeder Nutzer individuell seine Bedienoberfläche zusammenstellen (Abbildung 11).

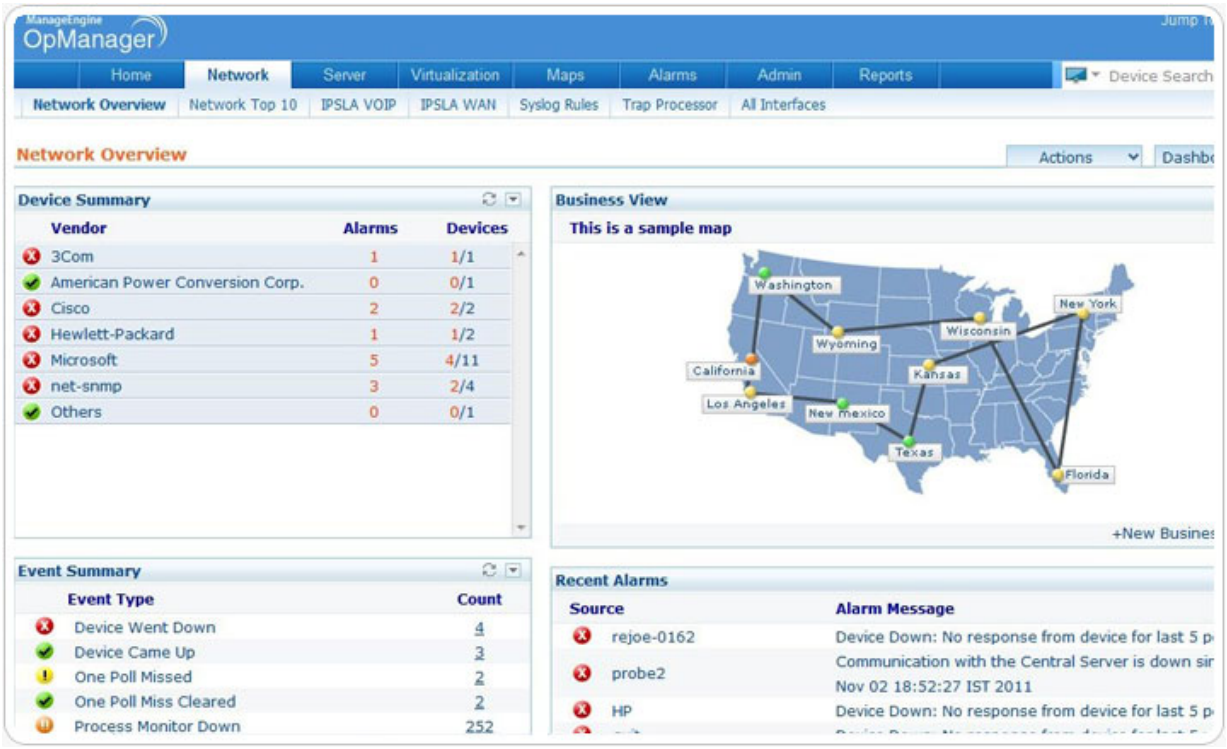

Abbildung 11: Network Monitoring Dashboard [UN11]

Für die Funktionen welche OpManager bereitstellt, belaufen sich allerdings auch die Kosten für die Anschaffung der Enterprise Variante (500 Geräte) auf 16.495$ [UN12].

5.1.4 ManageEngine OpManager in der Praxis

Die Installation verläuft wie auch bei HP SIM selbsterklärend ab. Dabei wird ebenfalls ein Datenbankserver installiert. Bei Beendigung der Installation öffnet sich bereits das Webinterface. Nach der Angabe von Benutzername („admin“) und dem Passwort („admin“) hilft ein Assistent alle nötigen grundlegenden Einstellungen festzulegen. Dabei werden die Zugriffsdaten erfasst, z.B. für SSH, WMI, SNMP Authentifizierungen und anschließend die IP-Bereiche, in dem sich die zu überwachenden Geräte befinden.

OpManager startet mit einer großzügigen informativen Oberfläche, welche jedoch etwas überladen wirkt. Bei der Erstkonfiguration sind die Systeme bereits auf kompatible Sensoren geprüft worden und somit werden schon die Prozessorauslastung und die Speicherplatzbelegung überwacht.

Unter dem Menüpunkt „Alarme“ gibt es einen Unterpunkt „Unangeforderte Traps“. Hier landen alle Traps, welche keiner MIB zugeordnet werden können bzw. deren OID dadurch unbekannt ist. Die Software besitzt für diesen Fall einen eigenen MIB Importer, der jedoch nur eine MIB zur gleichen Zeit importieren kann.

Eine Unterstützung für Syslog ist ebenfalls vorhanden und funktionierte im Test sehr gut.

Das Dashboard wie es in der Abbildung 12 zu sehen ist, wurde schon etwas verändert. Somit ist das Dashboard frei anpassbar und nach dem Login erscheint nur das wichtigste.

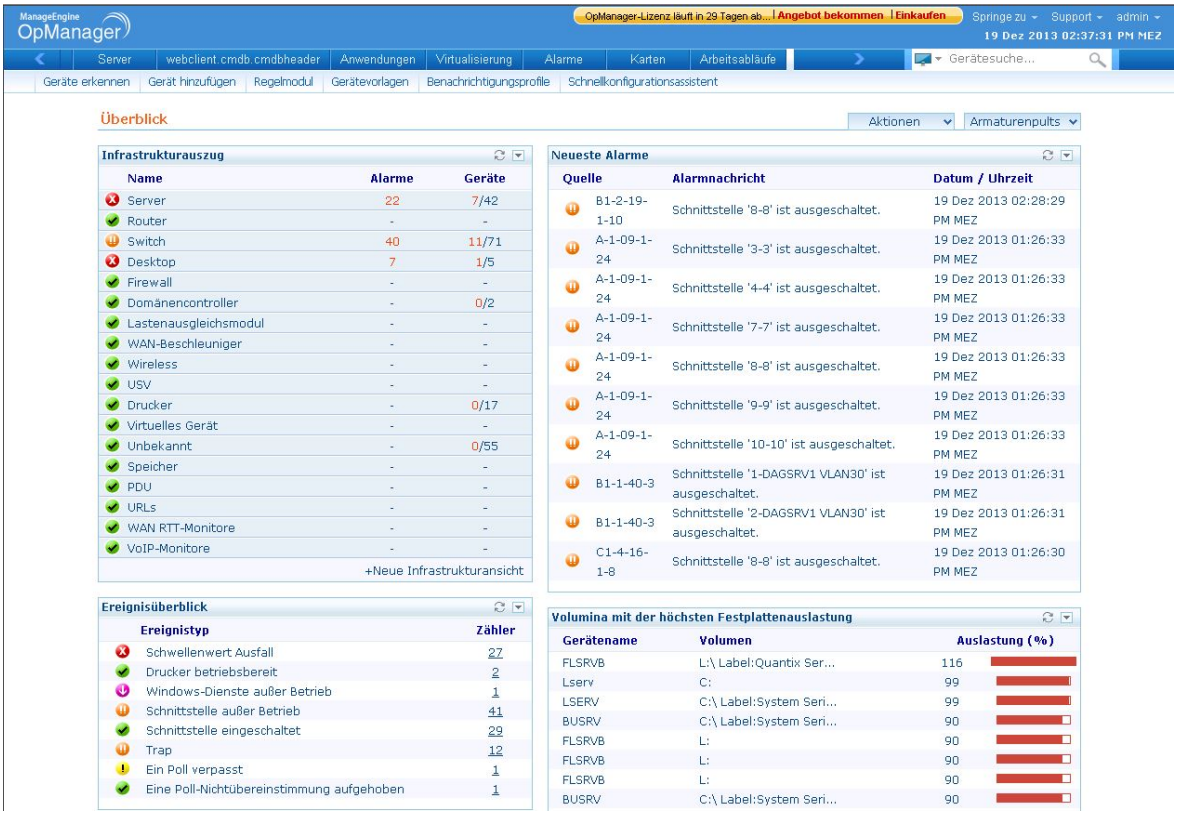

Abbildung 12: OpManager in der Praxis

Die Überwachung von Switchen und Servern funktioniert durch die vielen bereits mitgelieferten Gerätevorlagen und Monitore sehr gut. Jedoch ist für die Überwachung von Druckern nur eine reine Erreichbarkeitsprüfung möglich und die Abfrage der gedruckten Seiten. Damit auch die Tonerstände angezeigt werden, müssen zu den entsprechenden Gerätevorlagen die jeweiligen Monitore hinzugefügt werden. Um die OID herauszufinden, welche die entsprechenden Tonerstände zurück gibt, wird über das Tool snmpwalk aus dem Net-SNMP Paket die MIB der Drucker ausgelesen.

```
snmpwalk.exe –v 2c –c public –O n 172.24.1.47
```

Als Ausgabe erscheinen alle OIDs und Werte welche der Drucker unterstützt. Nun wird anhand der entsprechenden OID die richtige MIB geladen vom Hersteller oder frei verfüg-

baren Quellen. Über das „Monitor hinzufügen“ Fenster kann nun die entsprechende MIB geöffnet und das zu überwachende Attribut ausgewählt werden (Abbildung 13).

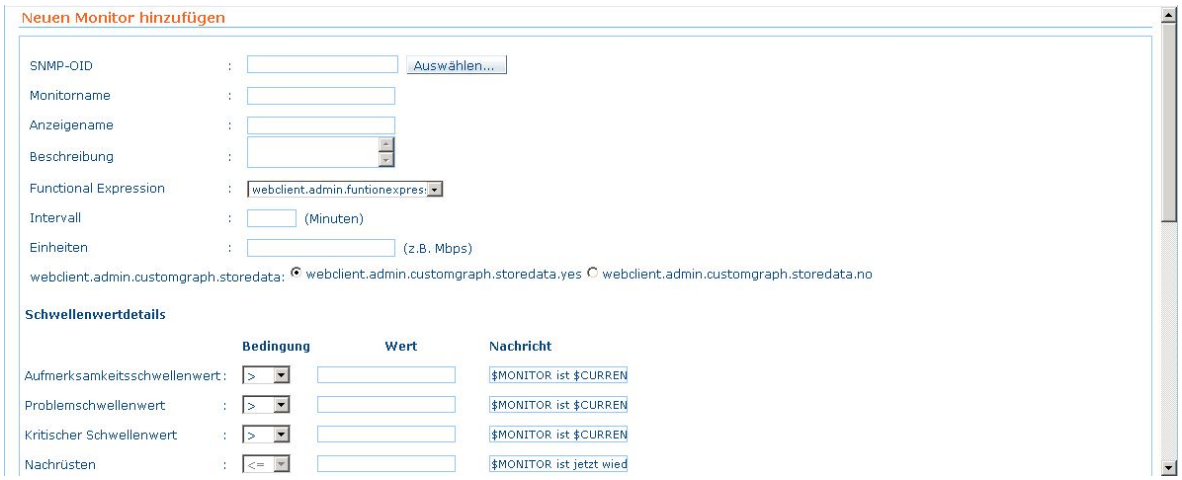

Abbildung 13: OpManager Hinzufügen eines Monitors

Wenn alle Monitore eingerichtet und den Druckern hinzugefügt sind, ist somit eine gute Gesamtlösung entstanden, welche alle wichtigen Parameter überwachen kann.

5.1.5 Icinga

Die Open Source Lösung benötigt eine relativ aufwendige Konfigurationsphase. Jedoch ist die Software kostenlos und frei verfügbar. Ebenso kann sie sehr gut durch Scripte und Module erweitert werden. Für HP Produkte gibt es dank der großen Community bereits mehrere Scripte für das Monitoring. Die Unterstützung für das Empfangen und Verarbeiten von Traps und Syslog-Meldungen ist durch die Verfügbarkeit von Addons ebenfalls gegeben. Aus diesen Gründen wird Icinga auch in der realen Umgebung geprüft.

5.1.6 Icinga in der Praxis

Für die Installation von Icinga wird eine virtuelle Maschine mit dem Betriebssystem OpenSuse[15] 13.1 eingerichtet. Die Installationsprozedur wird auf Grund der Komplexität im Anhang Teil 4 beschrieben. Da wie schon in Punkt 5.1.5 beschrieben Icinga einen komplexen und langen Weg für die Erstkonfiguration benötigt, wird in der Praxis für jede Monitoring Gruppe (Switch, Drucker, Server) je ein Gerät konfiguriert.

Um die drei Beispielkonfigurationen nutzen zu können, muss dies in der Konfigurationsdatei von Icinga freigeschalten werden.

[15] OpenSuse: „ist ein freies und Linux basiertes Betriebssystem“ [UN10]

Dazu die Datei `icinga.cfg` unter `/usr/local/icinga/etc/` mit dem Editor (z.B. VI) aufrufen. Die Zeilen mit den Beispielkonfigurationsdateien sind durch das führende Zeichen „#“ auskommentiert. Somit genügt es das Zeichen vor „cfg_file“ bei den folgenden drei Zeilen zu entfernen:

```
# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/icinga/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/icinga/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/icinga/etc/objects/printer.cfg
```

Abbildung 14: Ausschnitt Icinga Konfigurationsdatei

In `/usr/local/icinga/etc/objects` sind die anzupassenden Beispieldateien zu finden. Generell ist bei allen Dateien der Hostname („host_name“), Systemname („alias“) und die IP-Adresse („address“) zu konfigurieren.

Unterschiede gibt es nun bei den Dienst-Definitionen. Hierfür gibt es sehr viele Möglichkeiten des Monitorings. Für den Praxistest werden die vorgegebenen Dienste verwendet bzw. leicht angepasst.

Für den Drucker wird neben dem voreingestellten PING eine SNMP Abfrage nach dem Füllstand des 1. Toners als Dienst eingestellt:

```
define service{
        use                     generic-service
        host_name               canon5030.cpfs.mpg.de
        service_description     Toner 1 Fuellstand
        check_command           check_snmp!-C public -P 1 -o 1.3.6.1.2.1.43.11.1.1.9.1.1
        normal_check_interval   10
        retry_check_interval    1
        }
```

Abbildung 15: SNMP Abfrage nach Tonerstand in Icinga

Die für die SNMP Abfrage notwendige OID kann aus der PRINTER-MIB entnommen werden.

Der Switch wird zusätzlich zum PING mittels SNMP Abfrage nach der derzeitigen Systemlaufzeit und dem Linkstatus von Port 5 überwacht:

```
define service{
        use                             generic-service
        host_name                       c1-4-9-3-10.cpfs.mpg.de
        service_description             Uptime
        check_command                   check_snmp! -o 1.3.6.1.2.1.1.3.0
 -P 3 -L authPriv -U pcm -a SHA -A ****** -x DES -X ******
        }
```

Abbildung 16: SNMP Abfrage nach der Systemlaufzeit in Icinga

```
define service{
        use                             generic-service
        host_name                       c1-4-9-3-10.cpfs.mpg.de
        service_description             Port 5 Link Status
        check_command                   check_snmp! -o ifOperStatus.5 -r 1 -m RFC1213-MIB
 -P 3 -L authPriv -U pcm -a SHA -A ****** -x DES -X ******
        }
```

Abbildung 17: SNMP Abfrage nach dem Linkstatus des Port 5 in Icinga

Für das Servermonitoring sind die Standardeinstellungen unverändert gelassen. Für die Funktion muss jedoch auf dem Windowssystem eine Clientsoftware namens „nsclient++“ installiert werden (http://nsclient.org/nscp/downloads). Nach dem Start der Software kann Icinga nun auch den Windows Server überwachen. Diese Beispielkonfiguration erscheint im Browser nun wie folgt:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
c1-4-9-3-10.cpfs.mpg.de	PING	OK	01-08-2014 14:02:19	0d 2h 56m 23s	1/3	PING OK - Packet loss = 0%, RTA = 1.32 ms
	Port 5 Link Status	CRITICAL	01-08-2014 13:58:43	0d 0h 54m 59s	3/3	SNMP CRITICAL - *down(2)*
	Uptime	OK	01-08-2014 14:01:32	0d 1h 2m 10s	1/3	SNMP OK - Timeticks: (52874765) 6 days, 2:52:27.65
canon5030.cpfs.mpg.de	PING	OK	01-08-2014 13:54:33	0d 2h 50m 46s	1/3	PING OK - Packet loss = 0%, RTA = 0.68 ms
	Toner 1 Fuellstand	OK	01-08-2014 13:57:23	0d 1h 56m 19s	1/3	SNMP OK - 1944
localhost	Current Load	OK	01-08-2014 14:02:49	0d 2h 55m 53s	1/4	OK - load average: 0.01, 0.06, 0.06
	Current Users	OK	01-08-2014 13:59:13	0d 2h 59m 29s	1/4	USERS OK - 4 users currently logged in
	Icinga Startup Delay	OK	01-08-2014 14:03:29	0d 2h 56m 40s	1/4	OK: Icinga started with 0 seconds delay
	PING	OK	01-08-2014 14:01:30	0d 2h 58m 44s	1/4	PING OK - Packet loss = 0%, RTA = 0.12 ms
	Root Partition	OK	01-08-2014 14:02:43	0d 2h 58m 52s	1/4	DISK OK - free space: / 2622 MB (35% inode=69%):
	SSH	OK	01-08-2014 14:03:10	0d 2h 55m 32s	1/4	SSH OK - OpenSSH_6.2 (protocol 2.0)
	Swap Usage	OK	01-08-2014 13:59:34	0d 2h 59m 8s	1/4	SWAP OK - 99% free (1107 MB out of 1128 MB)
	Total Processes	OK	01-08-2014 13:58:47	0d 2h 57m 43s	1/4	PROCS OK: 56 processes with STATE = RSZDT
w7pc008.cpfs.mpg.de	CPU Load	OK	01-08-2014 14:01:40	0d 0h 42m 2s	1/3	CPU Load 54% (5 min average)
	Drive Space on C	WARNING	01-08-2014 14:03:04	0d 1h 24m 38s	3/3	c: - total: 74.43 Gb - used: 59.61 Gb (80%) - free 14.82 Gb (20%)
	Explorer	OK	01-08-2014 14:00:28	0d 2h 53m 14s	1/3	explorer.exe: Running
	Memory Usage	OK	01-08-2014 14:01:53	0d 2h 51m 49s	1/3	Memory usage: total:14324.29 Mb - used: 3660.18 Mb (26%) - free: 10664.11 Mb (74%)
	NSClient++ Version	OK	01-08-2014 14:03:17	0d 2h 50m 25s	1/3	NSClient++ 0,4,1,102 2013-07-15
	Uptime	OK	01-08-2014 13:54:41	0d 2h 59m 1s	1/3	System Uptime - 5 day(s) 1 hour(s) 56 minute(s)

Abbildung 18: Übersicht Icinga im Praxistest

Durch das Addon Eventdb (http://www.netways.de/de/produkte/nagios_icinga_addons/eventdb/) und den entsprechenden Modulen kann Icinga auch Syslognachrichten und Traps verarbeiten.

5.1.7 Paessler PRTG

Die Netzwerk Monitoring Software von Paessler wird mit großem Funktionsumfang und einfacher Installation beworben. Unterstützt werden als Betriebssystem alle Windows Versionen ab XP. Die Installation soll innerhalb von drei Minuten abgeschlossen sein und somit ist die Software schnell einsatzbereit. Für die Ersteinrichtung steht eine interaktive Benutzerführung bereit, welche auch unerfahrenen Benutzern die Einrichtung ermöglichen soll, ohne ein Handbuch lesen zu müssen.

Fünf verschiedene Varianten für die Bereitstellung der Daten stehen zur Verfügung. Eine Browsergestützte auf AJAX basierende Zugriffsmöglichkeit. Ein reines HTML Interface für ältere Browser mit eingeschränkter Funktionalität. Die Enterprise Console als Windows Applikation, welche sogar das Zusammenfassen von mehreren Monitoring Installationen erlaubt, sowie eine für das Handy optimierte Website und Apps für Android und Iphone.

Die Benachrichtigung kann über 9 verschiedene Möglichkeiten erfolgen: E-Mail, SMS, Syslog, SNMP Trap, http-Aktionen, Ereignisprotokoll, Amazon SNS, Abspielen von Medien oder externe Methoden

Die Überwachungsmöglichkeiten decken derzeit 190 verschiedene Bereiche ab. Darunter das Monitoring von Anwendungen, Up- und Downzeiten, virtuelle Server, Bandbreiten, Prozessorauslastung.

5.1.8 Paessler PRTG in der Praxis

Die Installation läuft, wie auch bei den vorhergehenden Windows Programmen in einfacher weise ab. Dabei gibt es die Wahl zwischen einer freien Version welche auf 10 Sensoren beschränkt ist oder eine unbeschränkte 30 Tage Testversion, die durch einen Trial-Schlüssel[16] aktiviert werden kann.

Nach der Installation werden die Login-Daten für sämtliche Systeme abgefragt welche dann von allen Gruppen übernommen werden. Nach der automatischen Suche von Netzwerkkomponenten fügt PRTG automatisch alle Sensoren hinzu, welche das Programm durch seine Templates findet. Wie später festgestellt werden muss, sollte das bei einer mittleren bis großen Netzwerkinfrastruktur besser nicht benutzt werden. Das manuelle Hinzufügen der Sensoren nach den tatsächlichen Erfordernissen ist hier zu bevorzugen. Der Grund hierfür ist am Ende des Praxistest beschrieben. Für einen genauen Test wurden deswegen nur wenige Geräte zum Monitoring hinzugefügt und die Sensoren manuell ausgewählt.

[16] Trial-Schlüssel: Bezeichnet einen Testcode zum Freischalten einer Software, um diese vor dem eventuellen Kauf testen zu können.

Über den Paessler MIB Importer (http://www.de.paessler.com/tools/mibimporter) werden zuerst die MIBs für die entsprechenden Geräte importiert. Die importierten MIBs werden dann im PRTG Programmverzeichnis als SNMP-Lib abgespeichert. Bei einem Rechtsklick auf das jeweilige Gerät können nun eigene Sensoren auf Basis der eben gespeicherten MIB hinzugefügt werden. Das Anpassen eines einzelnen Sensors, z.B. für das Abfragen und Darstellen des Tonerstandes, dauerte sehr lange und durch Fehlen von Assistenten oder hilfreichen Anleitungen ist es nur schwer möglich die Darstellung, z.B. für den Tonerstand in Prozent der ursprünglichen Gesamttonerkapazität, richtig anzeigen zu lassen. Nach dem aber auch diese Hürde genommen wurde, ist optisch gesehen eine schöne Monitoring Umgebung entstanden (Abbildung 19), wobei die benötigte Rechenleistung bereits bei 3 Geräten mit insgesamt 28 Sensoren relativ hoch liegt.

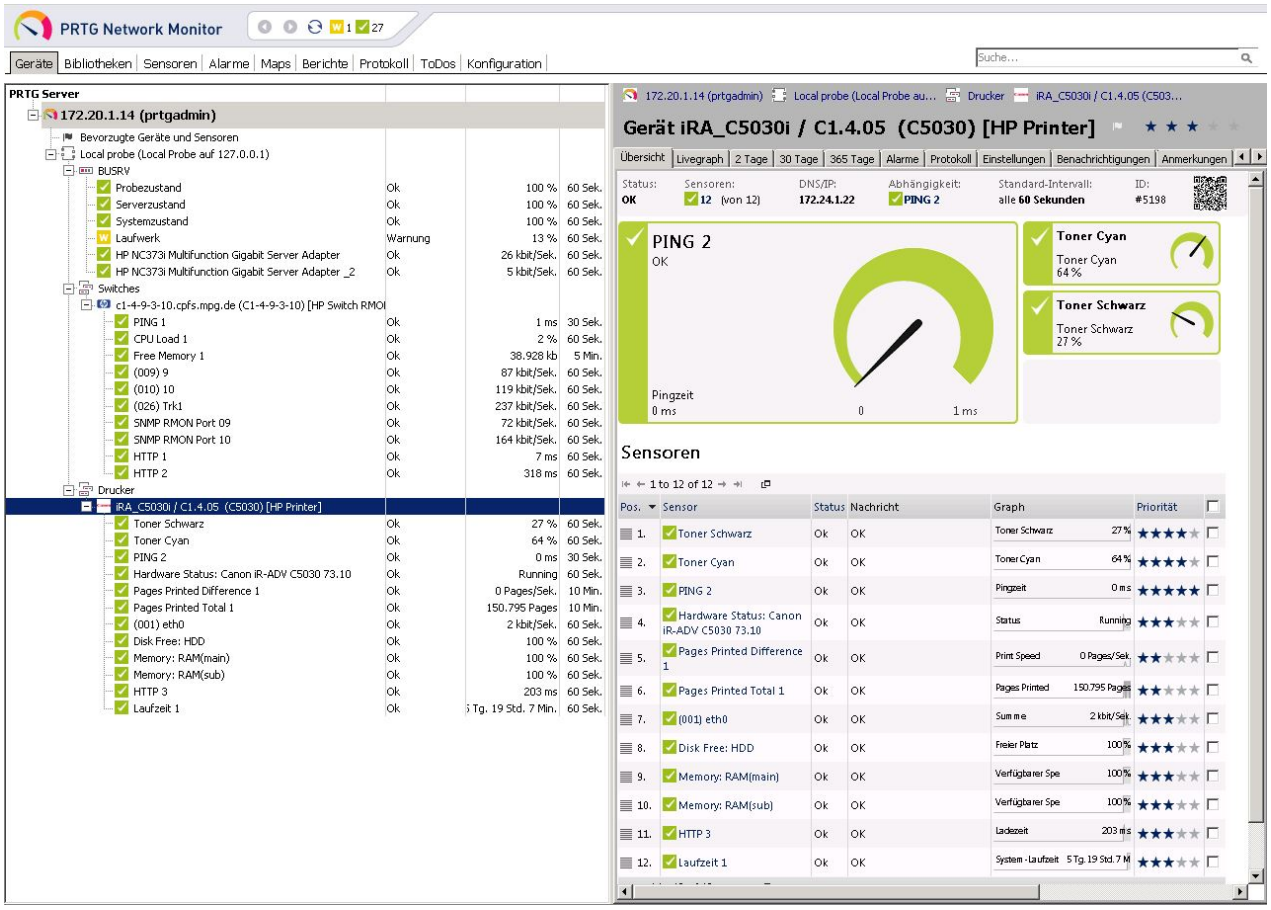

Abbildung 19: PRTG mit 3 Beispielgeräten

Am Anfang des Testes wurden zuerst alle Geräte, welche im Netzwerk existieren, inventarisiert. Danach wurde jedoch festgestellt, dass auf einigen Netzwerkknoten kein Login mehr möglich war. Dabei trat die Fehlermeldung „maximum sessions reached“ auf, was letztlich bedeutet, dass die maximale Anzahl an möglichen Sitzungen bzw. Verbindungen erreicht wurde. Warum es genau dazu kam oder ob es an Fehleinstellungen lag, wurde nicht abschließend geprüft.

Syslog und das Empfangen und Auswerten von Traps kann in PRTG nur über Sensoren geschehen, welche an einen Server gebunden werden. Dabei können bei Traps pro Sensor eine OID angegeben werden, die dann überprüft wird. Sprich: Sobald der entsprechende Trap empfangen wird, gibt es die Fehlermeldung.

5.2 Fazit

Keines der getesteten Lösungen kann die bestehende Software komplett ablösen. Dafür ist die von HP programmierte Software zu speziell auf die eigene Hardware ausgerichtet und an diese Features kann keine vom Hersteller unabhängige Lösung, welche es derzeit auf dem Markt gibt, heran kommen.

Paessler PRTG ist zwar sehr umfangreich und unterstützt sehr viele Monitoring Möglichkeiten, jedoch ist die Performance relativ schlecht und im Test war sogar nach einiger Zeit kein Zugriff mehr auf die Netzwerkknoten möglich.

Hewlett Packard System Insight Manager hilft beim einfachen Inventarisieren des Netzwerkes und überwachen der Erreichbarkeit von allen Komponentenklassen, jedoch gibt es nur die volle Verwaltungsmöglichkeit für die Server von HP. Bei Netzwerkkomponenten können z.B. keine Syslog Nachrichten oder Traps ausgewertet werden.

Der OpManager von ManageEngine punktet in Sachen Automation und Vielfältigkeit der Überwachungsmöglichkeiten. Jedoch ist die Übersichtlichkeit nicht gegeben und die richtigen Menüpunkte lassen sich nur schwer auffinden. Der MIB Import ist zwar möglich, jedoch sehr mühsam, da nur jeweils eine MIB gleichzeitig importiert werden kann.

Die OpenSource Software Icinga benötigt zwar etwas länger bei der Installation und Konfiguration, jedoch ist die Weboberfläche übersichtlich gestaltet und verbraucht relativ wenige Ressourcen. Die Erweiterungsmöglichkeiten sind z.B. durch eventdb gegeben, um an eine vielversprechende Lösung zu gelangen.

Soll es trotzdem eine gesamte Lösung mit den bisherigen Features der HP Software geben, sollte ein Projekt mit einem Systemhaus angebahnt werden. Eine gute Basis dafür ist Icinga oder auch Nagios. Viele Systemhäuser setzen auf die OpenSource Varianten und erstellen durch vor Ort Analysen fertige Lösungen mit den speziellen Anforderungen des Kunden.

6 Umsetzung des Managementmodells OSI

In diesem Kapitel wird noch einmal auf das Managementmodell OSI eingegangen und anhand des Beispiels Max Planck Institut erläutert.

6.1 Konfigurationsmanagement

Die Initialkonfiguration der Netzwerkverteiler am Institut findet manuell mit Hilfe eines Serienbriefes statt. Dieser erstellt durch eine Tabelle die nötige Konfiguration welche über eine Managementkonsole eingegeben werden kann. Bei Notwendigkeit der Änderung einer Konfiguration geschieht dies direkt auf dem betreffenden Switch über die Konsole. Die gesamte Konfiguration der Netzkomponenten wird durch den ProCurve Manager automatisch zu bestimmten Zeiten importiert und mit vorhergehenden verglichen.

Die Router werden ebenfalls komplett manuell konfiguriert. Ebenso wird auch, wie bei den Netzwerkverteilern, die Konfiguration regelmäßig in den ProCurve Manager importiert.

Die physikalische Freischaltung von Netzzugängen geschieht über einen Auftrag per E-Mail. Ein Mitarbeiter der Abteilung EDV patcht anschließend die entsprechende Netzwerkdose im betreffenden Verteilerschrank.

6.2 Leistungsmanagement

Zum Leistungsmanagement werden am Institut verschiedene Parameter der Komponenten überwacht. Hierzu zählen der Datendurchsatz auf den Trunkports[17] und die reine Erreichbarkeit der Geräte.

6.3 Fehlermanagement

Die Managementplattformen HP System Insight Manager, HP ProCurve Manager und HP Jetadmin stellen dem Netzoperator geeignete Oberflächen zur automatischen Fehlererkennung sowie Diagnosewerkzeuge zur Verfügung. Darunter zählen das ICMP basierte Tool PING und eine SSH Konsole.

[17] Gebündelte Ports eines Switch für die Lastverteilung bzw. auch als Failover

Für sofortige Diagnosen stellt der ProCurve Manager die Geräteereignisse durch das Protokoll Syslog und die empfangen Traps unter dem jeweiligen Bereich des Gerätes bereit.

Bei kritischen Fehlern, z.B. eine getrennte Verbindung eines Trunks oder ein abgestürzter Switch, wird eine E-Mail an die Netzoperatoren mit den notwendigen Informationen verschickt.

6.4 Abrechnungsmanagement

Ein Abrechnungsmanagement mithilfe der gewonnen Daten wird zwar nicht praktiziert, die relevanten Datenströme werden im ProCurve Manager jedoch analysiert und für Diagnosezwecke bereitgestellt.

6.5 Sicherheitsmanagement

Das Netzwerk ist in mehrere VLANs unterteilt sodass auch nur aus bestimmten Bereichen auf die kritischen Komponenten, z.B. Netzknoten, zugegriffen werden kann. Die Authentifizierung geschieht über einen zentralen Radius Server.

6.6 Fazit

Sobald am Max-Planck-Institut eine neue Lösung seinen Dienst aufnehmen kann, sollte das Managementkonzept überarbeitet werden. Gerade in den Punkten Leistungsmanagement und Fehlermanagement können Verbesserungen bezüglich der Benachrichtigung bei Problemen bzw. Sammeln von Informationen über Leistungsparameter erzielt werden. Ein hauptverantwortlicher Mitarbeiter ist für das Monitoring ist zu bestellen. Wenn neue Geräte in die Umgebung eingepflegt werden, müssen auch entsprechend der Geräteklasse neue Regeln für die Benachrichtigung und Fehlerbehandlung konfiguriert werden.

7 Rechtliche Aspekte

Dieses Kapitel beschäftigt sich mit den rechtlichen Aspekten und deren Gesetzte mit denen im Netzwerkmanagement umgegangen werden muss.

7.1 Allgemeines

Beim Monitoring von Netzwerkkomponenten und Servern werden viele Informationen abgefragt und abgefangen. Diese Daten sind in Log-Dateien oder Datenbanken abgespeichert und dazu gibt es einige Gesetze, welche dabei beachtet werden müssen. Auf Grund der Gesetze müssen entsprechende Vorkehrungen getroffen oder im Vorfeld beachtet werden um eine Verletzung der Normen zu verhindern. Nachfolgend werden einige Gesetze welche für das Netzwerk Monitoring relevant sind erläutert und Maßnahmen zum Schutz dieser beschrieben.

Da es sehr viele Gesetze um und über den Datenschutz gibt, gilt es für den bestimmten Sachverhalt das richtige Gesetz zu erkennen. Hierfür wurde ein drei-Schichten Modell des Datenschutzes entwickelt (Abbildung 20). Dieses Modell erleichtert die Zuordnung einer Sache zu der richtigen Vorschrift im Telekommunikationsbereich. Dabei ist die genaue Abgrenzung laut [JH] S.283 jedoch in der Rechtswissenschaft nicht ganz geklärt.

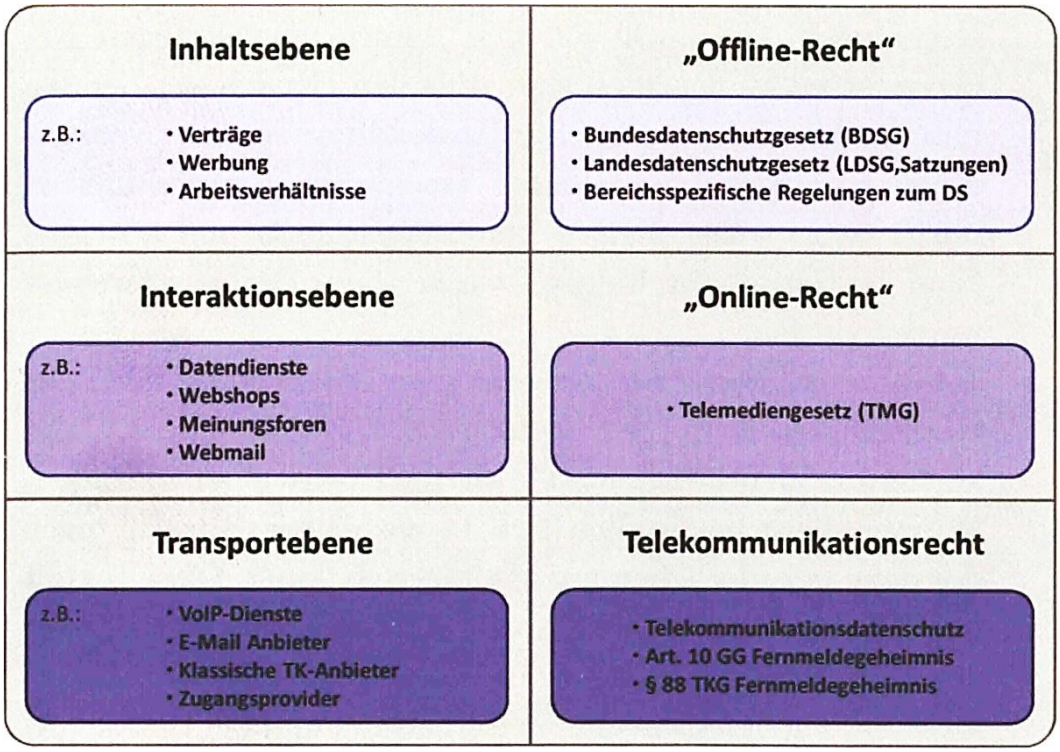

Abbildung 20: Drei-Schichten-Modell für den Datenschutz [JH] S. 283

Dabei gilt es weiterhin zu beachten, das bei öffentlichen Stellen des Bundes oder nicht öffentlichen Stellen generell das Bundesdatenschutzgesetz zu verwenden ist. Wobei bei Stellen des Landes vorrangig das Landesrecht zu beachten ist, es sei denn das jeweilige Institut hat eigene Regelungen getroffen. So ist die rangniedrigste Norm anzuwenden.

Als Basis gilt Artikel 10 des Grundgesetzesbuches welches dem Deutschen Volk ein grundlegendes Recht des Fernmeldegeheimnisses einräumt [RH].

7.2 Fernmeldegeheimnis und Telekommunikationsgesetz

Folgende Regelungen sind im Fernmeldegeheimnis (Grundgesetz Artikel 10) bestimmt:

- *Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.*
- *Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und das an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.*

Somit verbietet das Fernmeldegeheimnis Unbefugten „das Überwachen von Fernmeldeinformationen“ [RH]. Weiterführend ist das Fernmeldegeheimnis genauer im §88 des Telekommunikationsgesetzes (TKG) und §206 des Strafgesetzbuches (StGB) definiert:

Die ersten 3 Absätze des §88 Telekommunikationsgesetz:

- *Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.*
- *Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.*
- *Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.*

Der Paragraph 206 des StGB definiert ab wann eine Verletzung des TKG eintritt (siehe Anlagen, Teil 5).

Aus diesen Gesetzen lässt sich erörtern, das eine Administration und Überwachung in einem bestimmten Rahmen durchaus berechtigt und erlaubt ist [RH]. Dabei ist z.B. speziell die Aufzeichnung von Metainformationen einer Verbindung oder Speichern von Datenpaketen für Performanceanalysen erlaubt, da es sich um den Schutz und die Funktion technischer Systeme handelt. Wie jedoch die gespeicherten Daten behandelt werden müssen, ist im sogenannten Datenschutzgesetz geregelt.

7.3 Datenschutzgesetz

Das Bundesdatenschutzgesetz ist sehr umfangreich. Dabei beschreibt das BDSG genau wie personenbezogenen Daten verarbeitet und gespeichert werden dürfen.

Zu beachten sind dabei folgende Paragraphen des Bundesdatenschutzgesetzes, welche in ausführlicher Fassung im Anhang, Teil 6 zu finden sind:

- §9 Technische und organisatorische Maßnahmen
- §13 Datenerhebung
- §14 Datenspeicherung, -veränderung und –nutzung
- §19 Auskunft an den Betroffenen
- §19a Benachrichtigung

Aus diesen Paragraphen des BDSG können folgende zu beachtende Aspekte für das Netzwerk Monitoring abgeleitet werden:

- Die erhobenen Daten müssen vor dem Zugriff durch Unbefugte geschützt werden.
- Werden Daten von Personen erhoben, so muss das Einverständnis dieser eingeholt werden.
- Welche Daten im Netzwerk erhoben werden, muss auch für Nutzer des Netzes transparent ersichtlich sein.
- Es dürfen nur Daten erhoben werden, welche direkt im Zusammenhang mit dem Schutz des Systems oder der zuverlässigen Funktion des Systems dienen.

Im Zweifel ist die Erklärung jedes neuen Benutzers des Netzes einzuholen und bei Widerspruch der Einwilligung die Nutzung des Netzwerkes zu Verwehren.

Schlusswort

Der Prozess zur Einführung eines systemübergreifenden Monitoring durchläuft viele komplexe Schritte und sollte jederzeit gut überlegt sein. Das wichtigste dabei ist die genaue Analyse des Ist-Zustandes und der daraus resultierenden Anforderungen an die Software. Nichts ist schlimmer als eine nicht hundertprozentig funktionierende und zufriedenstellende Lösung auf Grund fehlerhafter Erforschungen in der Vorbereitungsphase. Weiter geht dieser Prozess auch nach der Einrichtung einer Monitoring Software. Denn regelmäßig müssen Tests durchgeführt werden um die Sicherstellung des Zwecks der Software zu gewährleisten.

Am Beispiel Max-Planck-Institut konnte zwar während der Erstellung dieser Arbeit leider keine fertige Gesamtlösung gefunden werden, jedoch wurden bestehende Mängel im Monitoring behoben. Der Empfang von SNMP-Traps und die entsprechend gute Auswertung sind nun gegeben. Auch das Senden von Geräteereignissen an den ProCurve Manager funktioniert nun.

Ferner ist für die Zukunft auch nach dem Implementieren einer geeigneten Lösung allerdings die Abschaffung von HP ProCurve Manager für die Wartung der Switche nicht zu empfehlen. Ein entscheidender Vorteil, welcher von der Software ausgeht, ist die übersichtliche Darstellung und Erfassung der installierten Firmware. Die Software weiß durch eine Verbindung mit HP welche Firmware derzeit aktuell ist und meldet entsprechend dem vorherrschenden Firmware Stand ob die bevorzugte Version installiert ist. Daneben bietet die Software weitere Analysemöglichkeiten, wie RMON und Trafficmonitoring. Aber auch das bündeln von Traps und Syslog Nachrichten in einer Software ist ein nicht zu unterschätzender Vorteil.

Literatur

[HSB] Heinz-Gerd Hegering, Sebstian Abeck, Bernhard Neumair: Integriertes Management vernetzter Systeme, Heidelberg, dpunkt, 1999

[UN1] Unbekannt; eduroam URL: http://www.cpfs.mpg.de/web/institut/einrichtungen/it/eduroam/; verfügbar am 18.02.2013

[UN2] Unbekannt; Internet Control Message Protocol URL: http://de.wikipedia.org/wiki/Internet_Control_Message_Protocol; verfügbar am 05.11.2013

[UN3] Unbekannt; Windows Management Instrumentation URL: http://de.wikipedia.org/wiki/Windows_Management_Instrumentation; verfügbar am 15.07.2013

[UN4] Unbekannt; Simple Network Management Protocol URL: http://de.wikipedia.org/wiki/Snmp; verfügbar am 06.11.2013

[UN5] Unbekannt; Netzwerkprotokoll URL: http://de.wikipedia.org/wiki/Netzwerkprotokoll; verfügbar am 28.11.2013

[UN6] Unbekannt; Management Information Base URL: http://de.wikipedia.org/wiki/Management_Information_Base, verfügbar am 26.03.2013

[TS] Thomas Schwenkler: Sicheres Netzwerkmanagement, Heidelberg, Springer, 2006

[UN7] Unbekannt; HP SIM Overview URL: http://h18004.www1.hp.com/products/servers/management/hpsim/ , verfügbar am 08.11.2013

[TT] Thomas Timmermann; Kriterien für die Auswahl einer geeigneten Netzwerk-Monitoring-Lösung URL: http://cdn.paessler.com/common/files/pdf/whitepaper/selection-criteria_de.pdf, verfügbar am 06.2012

[UN8] Unbekannt; Monitoring URL: http://www.it-administra-tor.de/themen/netzwerkmanagement/grundlagen/111034.html, verfügbar am 30.01.2012

[UN9] Unbekannt; Integrated Lights-Out URL: http://de.wikipedia.org/wiki/Integrated_Lights-Out, verfügbar am 03.04.2013

[UN10] Unbekannt; opensuse.org URL: http://www.opensuse.org/de/, verfügbar am 26.11.2013

[LE] Ludwig Eckert; Netzwerkmanagement FCAPS URL: http://www.w3service.net/vorlesungen/verteilte-systeme/0062-netzwerkmanagement/Netzwerk-Management-FCAPS-026.pdf, verfügbar am 29.06.2005

[UN11] Unbekannt; Network Monitoring Dashboard URL: http://www.manageengine.com/network-monitoring/images/screenshot/network-monitoring-dashboards.jpg, verfügbar am 04.12.2013

[HMT] Holger Schwichtenberg, Thomas Joos, Manuela Reiss: Windows Vista Business: Das Profihandbuch für den Unternehmenseinatz [Service Pack 1], München, Addison-Wesley Verlag, 2008

[JH] Jochen Dinger, Hannes Hartenstein: Netzwerk- und IT-Sicherheitsmanagement Eine Einführung, Karlsruhe, Universitäts-verlag Karlsruhe, 2008

[UN12] Unbekannt; Editions and Pricing URL: http://www.manageengine.com/network-monitoring/opmanager-editions.html, verfügbar am 18.12.2013

[IDT] Icinga Development Team; Icinga Schnellstart auf Linux URL: http://docs.icinga.org/latest/de/quickstart-icinga.html, verfügbar am 08.01.2014

[RH] Ronny Harbich; Netzwerküberwachung URL: http://www-e.uni-magdeburg.de/harbich/netzwerkueberwachung.php, verfügbar am 10.01.2014

Anlagen

Anlagen, Teil 1 Einrichtung von SNMP

Damit der Server für die Testinstallationen selbst SNMP Anfragen erhalten kann, ist der entsprechende Dienst zu installieren, aktivieren und einzustellen.

Die Vorgehensweise wird nachfolgend in dieser Anlage beschrieben. Als Beispiel dient ein Microsoft® Windows Server® 2008 Standard.

1.) Wenn der SNMP Service noch nicht installiert sein sollte, kann dies über den Server Manager nachgeholt werden. Beschrieben ist dies ausführlich unter der folgenden Adresse: http://blog.skufel.net/2012/09/how-to-adding-snmp-to-windows-server-2008-r2/.
Auf dem hier benutzten Server ist der SNMP Dienst jedoch schon installiert, deswegen wird nicht näher darauf eingegangen.
2.) Der SNMP Dienst „SNMP Service“ (Abbildung 14) muss gestartet sein und konfiguriert werden. Dabei ist zu beachten, dass der Dienst „SNMP Trap“ nicht gestartet ist und der Start auf Deaktiviert gesetzt wird. Sonst können die Monitoring Programme keine Traps empfangen.

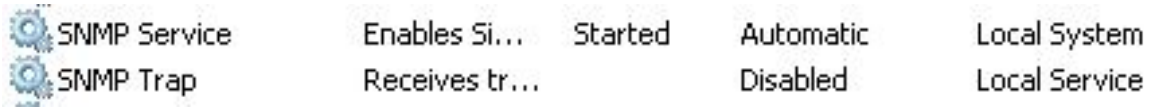

Abbildung 21: SNMP Dienste

Bei Rechtsklick auf „SNMP Service“ und öffnen der Eigenschaften gibt es 2 wesentliche Konfigurationspunkte: Traps und Sicherheit.
In der Konfigurationskarte Traps ist unter „Trap destinations“ einzustellen, wohin die Traps vom Server geschickt werden sollen und unter „Community name“ der entsprechende Name des zu benutzenden Community Namen einzutragen.

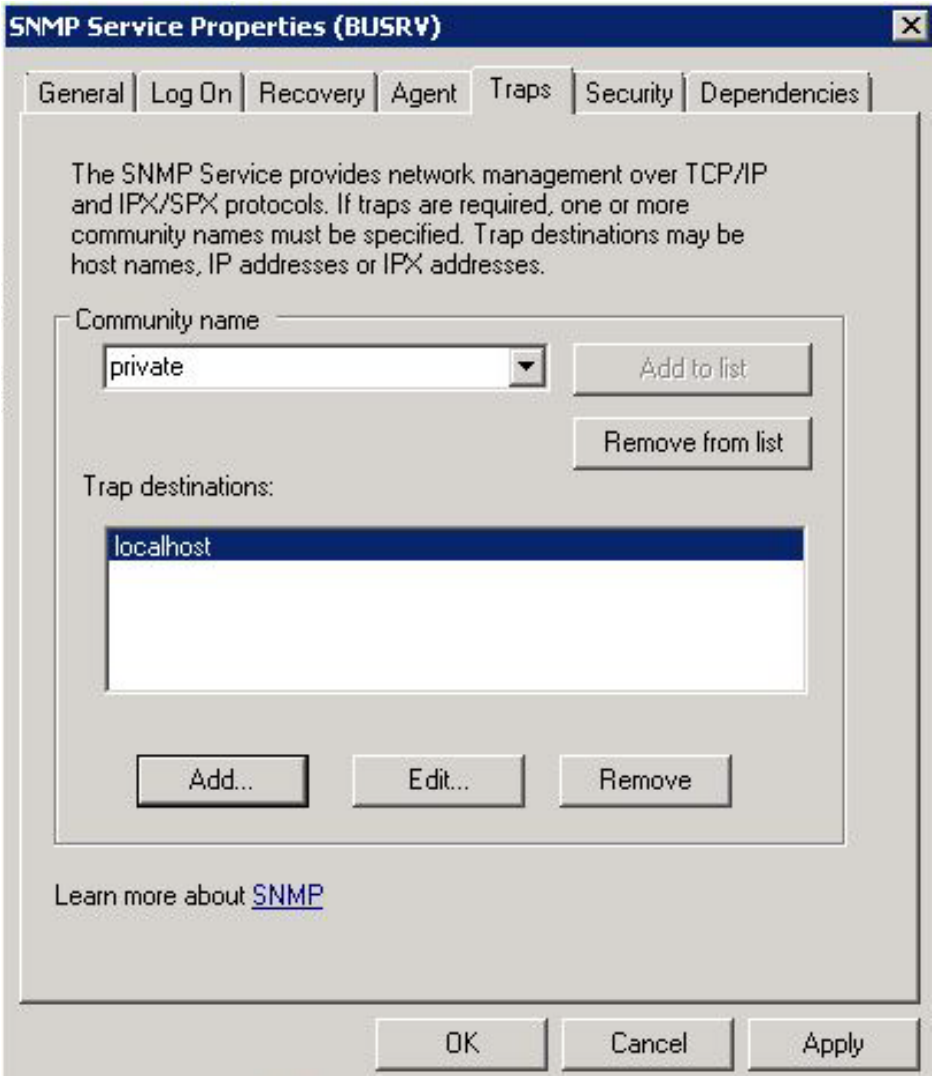

Abbildung 22: Traps in SNMP Einstellungen

Auf der Seite Sicherheit sind die zu akzeptierenden Community Namen einzutragen und anschließend die Server von denen SNMP Pakete akzeptiert werden sollen.

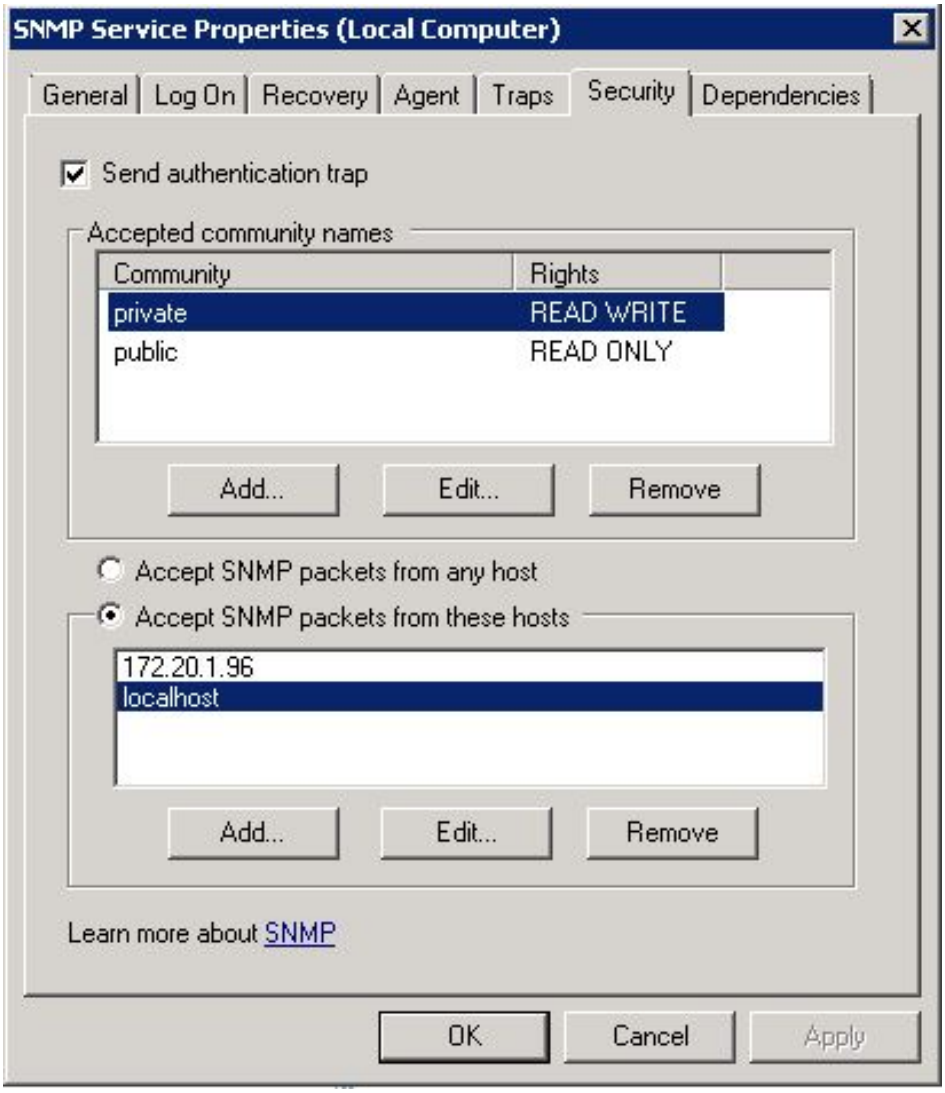

Abbildung 23: Sicherheit in SNMP Einstellungen

Nun ist der Server für den Empfang und Versand von SNMP Nachrichten konfiguriert.

Anlagen, Teil 2 Einstellen des VLAN

Das Institutsnetzwerk besteht aus mehreren virtuellen LANs. Insgesamt sind das 15 verschiedene Netze, welche unterschiedlichste Aufgaben und Zugangsberechtigungen haben.

Damit ein Server bzw. dessen Netzwerkkarte zu einem der Netze dazugehören kann und somit mit den entsprechenden Endgeräten kommunizieren darf, muss die MAC-Adresse im Active Directory einer entsprechenden VLAN Gruppe zugeordnet werden.

Die Vorgehensweise wird nun in dieser Anlage beschrieben. Als Beispiel dient ein Microsoft® Windows Server® 2008 Standard mit 2 Netzwerkkarten als HP Network Team[18].

1.) Notieren der MAC-Adresse der Netzwerkkarte
   Start->Ausführen->cmd.exe
   ipconfig /all

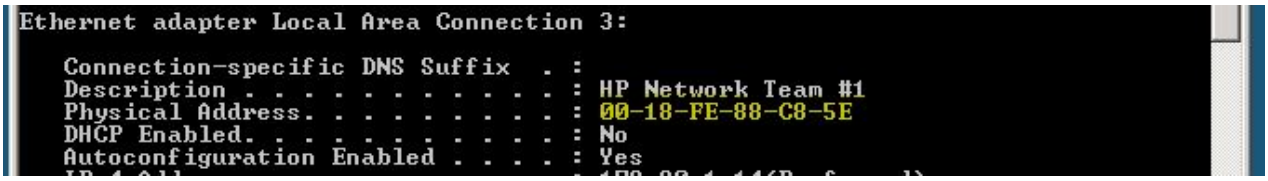

Abbildung 24: Teilausgabe bei ipconfig /all

[18] Beide Netzwerkkarten sind als Verbund zusammengefügt, somit Redundant

2.) Öffnen des Active Directory Managers und auswählen des entsprechenden Baumes bzw. der entsprechenden VLAN Gruppe

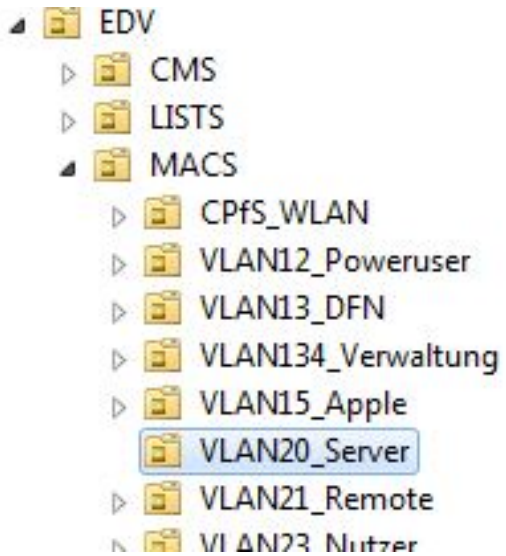

Abbildung 25: Auswahl VLAN Gruppe Server im AD

3.) Erstellen eines neuen Benutzers, Ausfüllen der Felder und Optionen

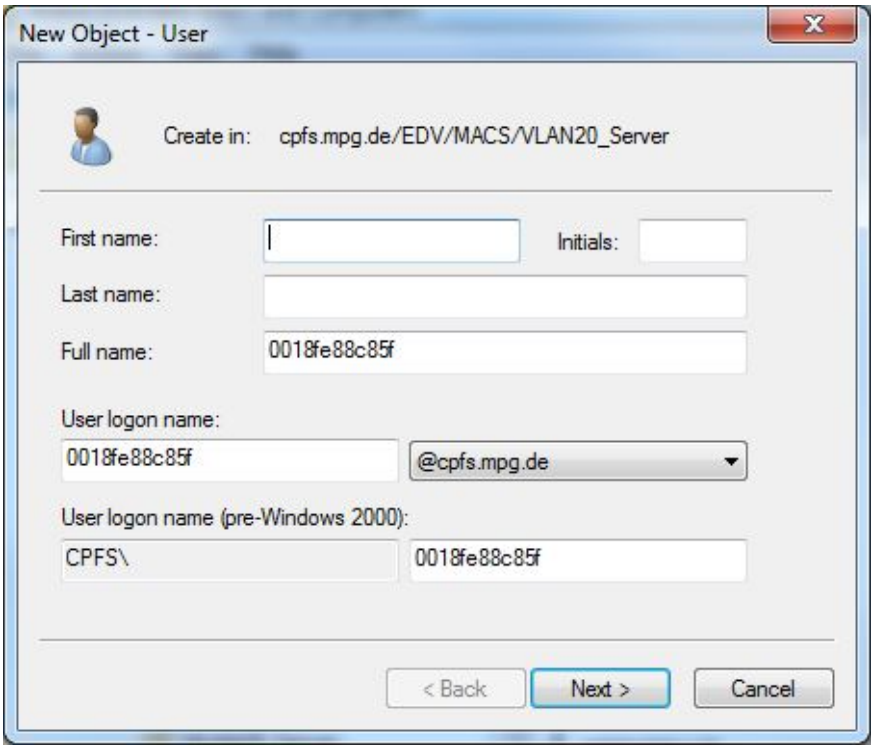

Abbildung 26: Hinzufügen der MAC-Adresse

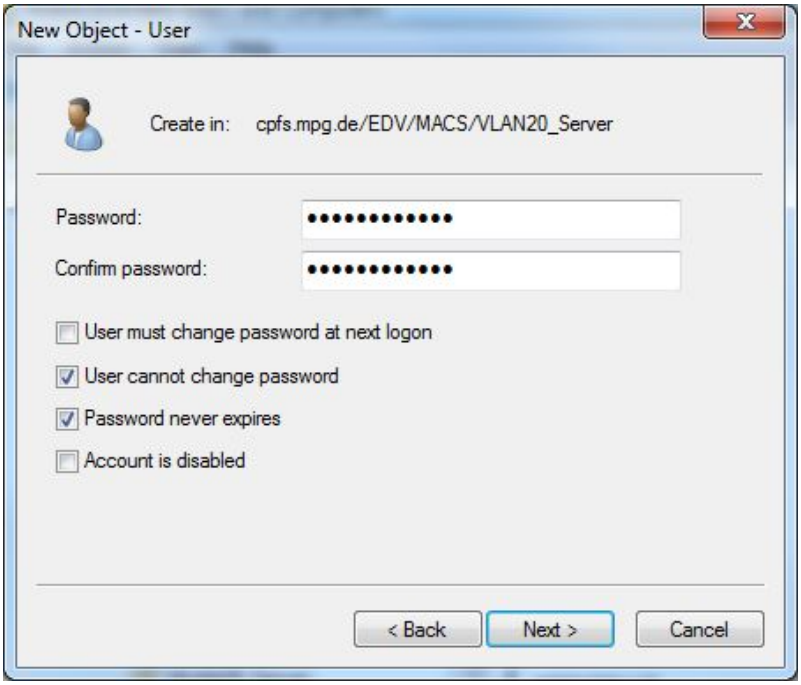

Abbildung 27: Passwort ist gleich dem Benutzernamen

Die Eingaben sind anschließend zu prüfen und zu bestätigen.

4.) Eingeben einer Beschreibung und ändern der Passwortverschlüsselung

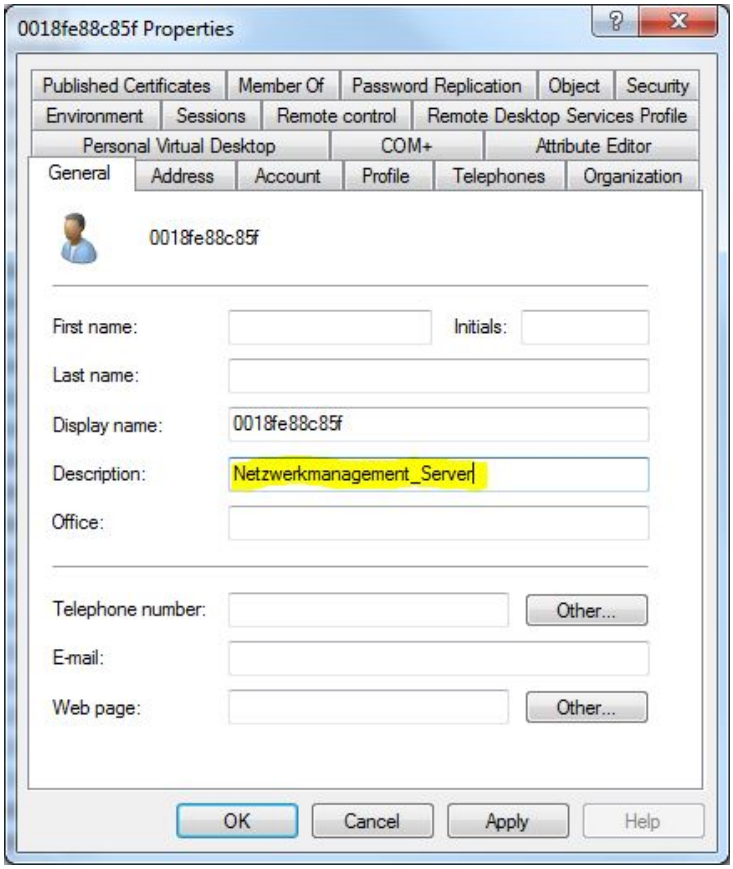

Abbildung 28: Beschreibung AD Benutzer

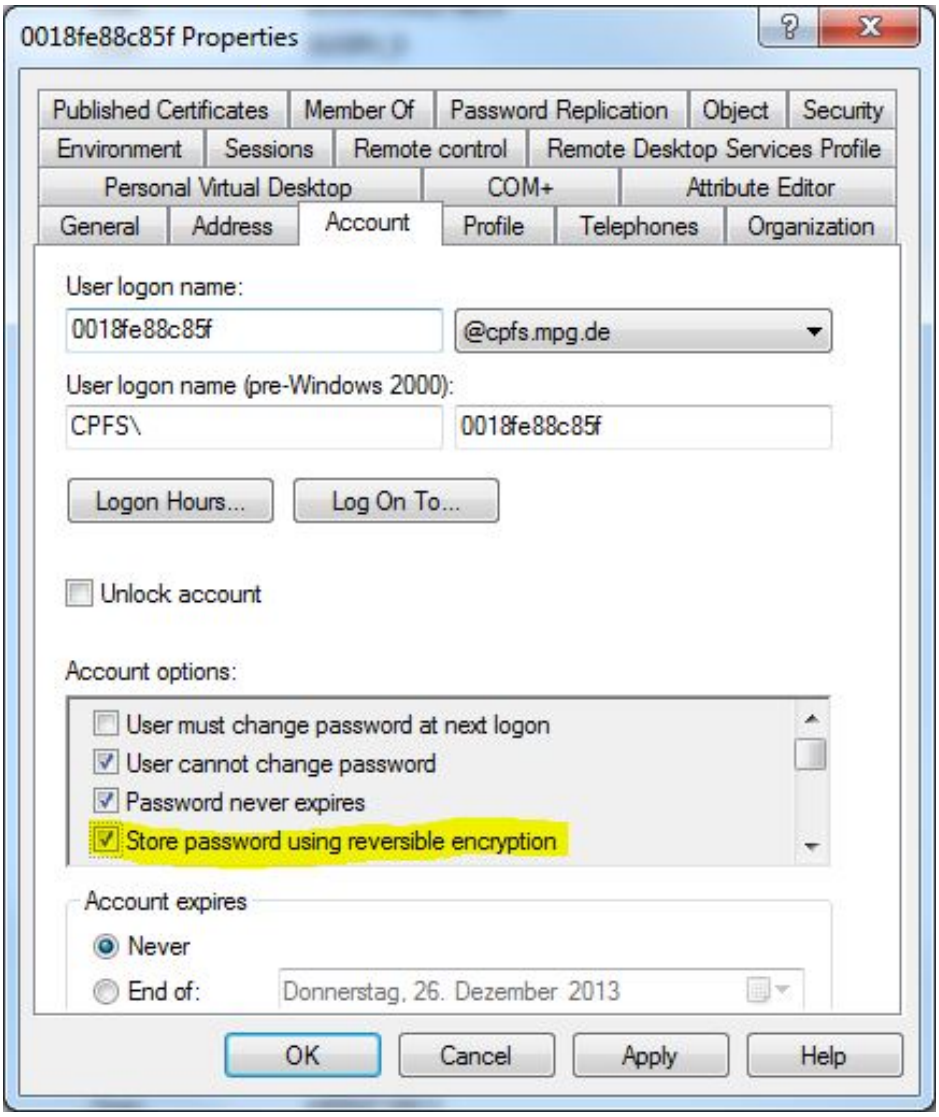

Abbildung 29: Ändern der Passwort Verschlüsselung

5.) Ändern der Gruppe zum VLAN20

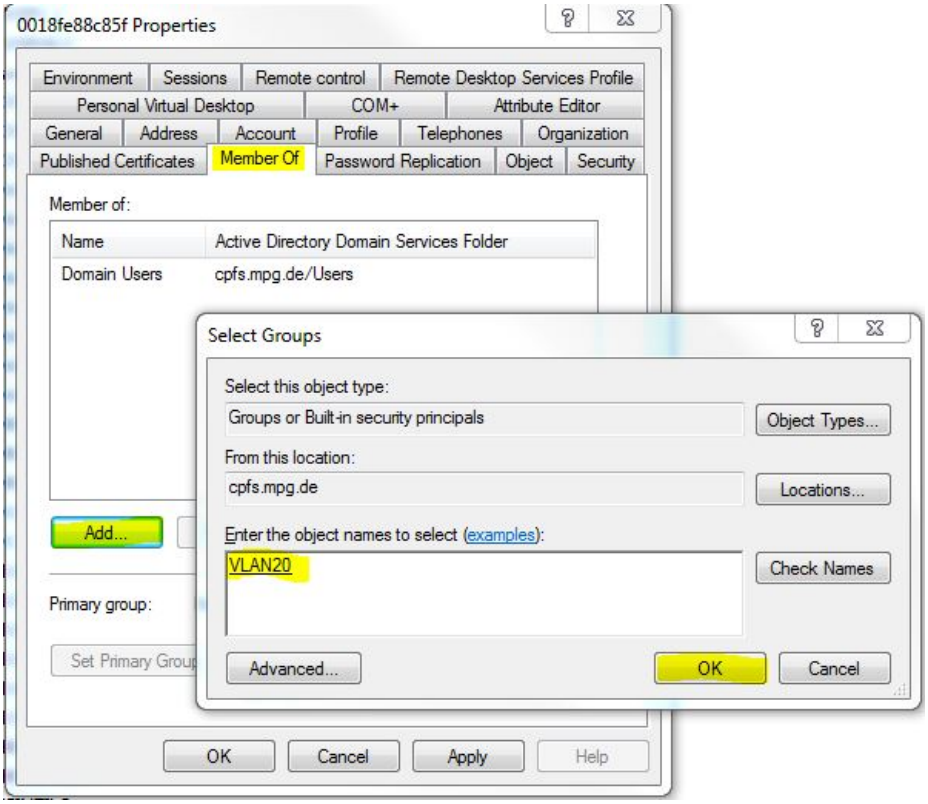

Abbildung 30: Hinzufügen der Gruppe VLAN20

Die Gruppe VLAN20 ist als primäre Gruppe zu setzen und die Gruppe Domain Users zu löschen.

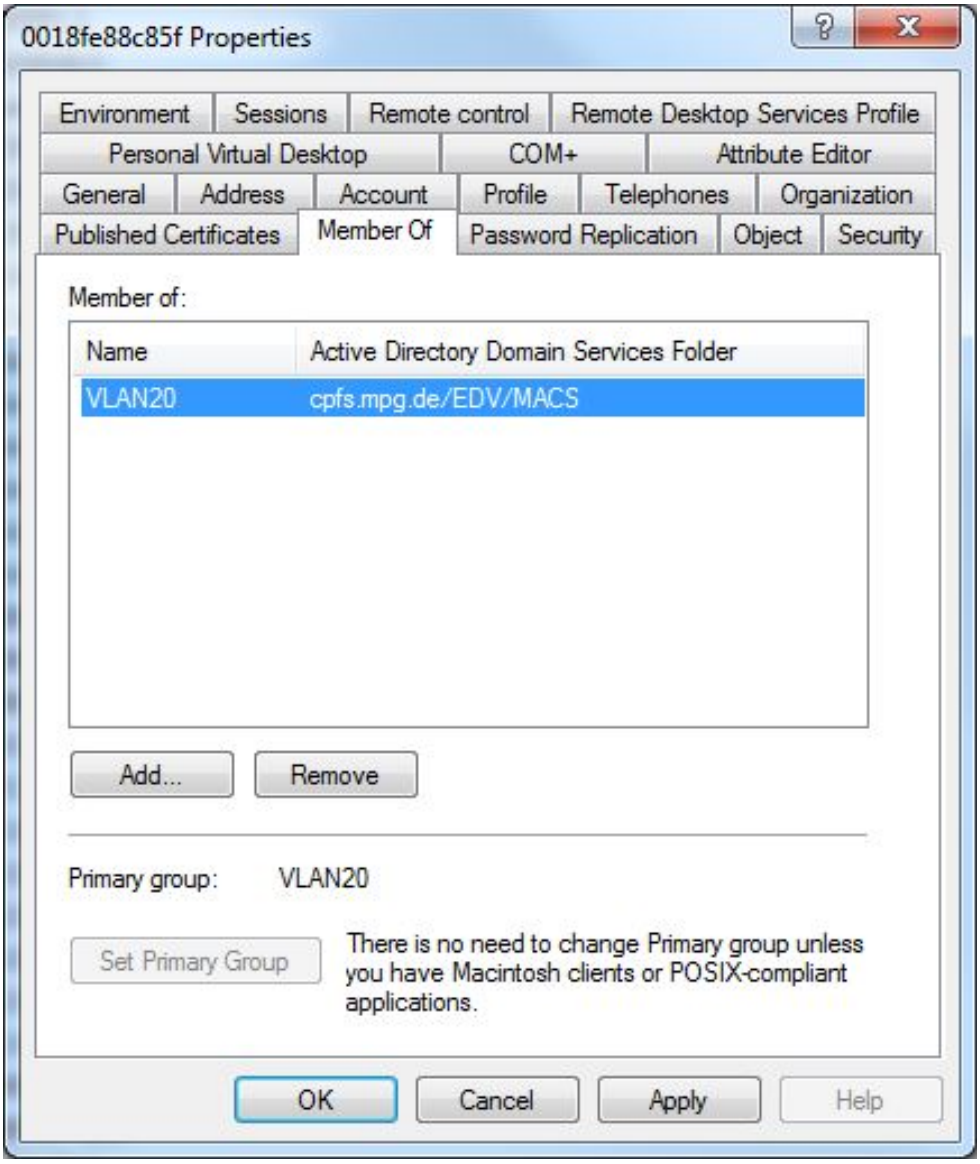

Abbildung 31: Ändern der Gruppe zum VLAN20

Anlagen, Teil 3 SNMP auf Switch einstellen

Für die Konfiguration des Switches (als Beispiel ein HP ProCurve 2520G-8) wird eine SSH Verbindung mithilfe des Tools „putty“ genutzt. Nach erfolgreichem Herstellen der Verbindung und Authentifizierung gilt es zunächst den Konfigurationsmodus zu aktivieren.

```
C1-4-9-3-10# conf
C1-4-9-3-10(config)#
```

Nun konfigurieren wir den Switch (`C1-4-9-3-10`) für das Senden der Traps an den Testserver mit der IP `172.20.1.14`. Dabei Verwenden wir die aktuelle SNMP Version 3.

```
C1-4-9-3-10(config)# snmpv3 enable
C1-4-9-3-10(config)# 123456
C1-4-9-3-10(config)# 123456
C1-4-9-3-10(config)# N
C1-4-9-3-10(config)# y
```

Dabei wird SNMPv3 aktiviert, ein Standardbenutzer „initial“ mit dem Passwort „123456“ eingerichtet und SNMPv1/v2 Nachrichten als nur lesen definiert.

```
C1-4-9-3-10(config)# snmpv3 user pcm auth sha PASSWORD priv des
PASSWORD
C1-4-9-3-10(config)# snmpv3 group managerpriv user pcm sec-model
ver3
```

Der Nutzer „pcm“ wird erstellt mit dem Passwort „PASSWORD“ und den entsprechenden Verschlüsselungsalgorithmen.

```
C1-4-9-3-10(config)# no snmpv3 user initial
C1-4-9-3-10(config)# snmpv3 only
```

Der Nutzer „initial“ wird gelöscht und das SNMP Protokoll auf nur Version 3 gesetzt.

```
C1-4-9-3-10(config)# snmpv3 notify procurve tagvalue procurve
```

Der Parameter „notify“ setzt den Empfängernamen.

```
C1-4-9-3-10(config)# snmpv3 targetaddress procurve params procurve
172.20.1.14 filter all taglist procurve
```

Das Kommando „snmpv3 targetadress“ stellt die Verknüpfung zwischen dem Empfängernamen und der IP der Managementstation her. Zusätzlich wird der Filter auf „all“ gestellt. Dabei sendet der Switch auch informative Traps zur Station.

Zu allerletzt muss dem Empfänger noch der entsprechende Nutzer „pcm“ zugeordnet werden.

```
C1-4-9-3-10(config)# snmpv3 params procurve user pcm sec-model
ver3 message-processing ver3 priv
```

Anlagen, Teil 4 Installation von Icinga

Für die Installation wurde eine virtuelle OpenSuse 13.1 Maschine bereitgestellt. Folgend die Anleitung in Anlehnung an [IDT] mit Kommentaren für die vollständige Installation von Icinga mit den Nagios Plugins mit den Standard Konfigurationsdateien.

Nach dem Login mit SSH oder über das lokale Terminal sind folgende Befehle für die Installation nötig:

```
su –l
```

Gibt dem eingeloggten Nutzer Root-Rechte für die Installation.

```
zypper install gd gd-devel libjpeg libjpeg-devel libpng libpng-
devel
zypper install net-snmp net-snmp-devel perl-Net-SNMP
zypper install apache2 gcc
```

Lädt die angegebenen Programme und Module herunter und installiert diese.

```
/usr/sbin/useradd -m icinga
passwd icinga
/usr/sbin/groupadd icinga
/usr/sbin/groupadd icinga-cmd
/usr/sbin/usermod -a -G icinga-cmd icinga
```

Legt den Nutzer „icinga“ an sowie die Gruppe „icinga“.

```
cd /usr/src
wget http://downloads.sourceforge.net/project/icinga/icinga/1.10.1/icinga-
1.10.1.tar.gz?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Ficinga%2F&ts=1388759264
&use_mirror=freefr
mv icinga-
1.10.1.tar.gz\?r\=http\:%2F%2Fsourceforge.net%2Fprojects%2Ficinga%
2F icinga-1.10.1.tar.gz
tar xvzf icinga-1.10.tar.gz
```

Download des Icinga Paketes und die Extrahierung nach /usr/src/icinga-1.10.1.

```
cd icinga-1.10.1
./configure --with-command-group=icinga-cmd --disable-idoutils
make all
make install
make-install-init
make install-config
make install-eventhandlers
```

```
make install-commandmode
```

Damit werden die Quelldateien kompiliert und installiert.

```
vi /usr/local/icinga/etc/objects/contacts.cfg
```

Konfigurieren einer E-Mail-Adresse für den Empfang von Benachrichtigungen.

```
make cgis
make install-cgis
make install-html
make install-webconf
htpasswd2 -c /usr/local/icinga/etc/htpasswd.users icingaadmin
New Password: ******
Re-type new password: ******
/etc/init.d/apache2 reload
```

Kompiliert und installiert das klassische Webinterface und legt einen Benutzer für den Zugriff auf das Interface an. Anschließend Neustart des Apache Webservers.

```
wget https://www.nagios-plugins.org/download/nagios-plugins-1.5.tar.gz
tar xzf nagios-plugins-1.5.tar.gz
cd nagios-plugins-1.5
./configure --prefix=/usr/local/icinga \
    --with-cgiurl=/icinga/cgi-bin \
    --with-nagios-user=icinga --with-nagios-group=icinga
make
make install
```

Download, Entpacken sowie Installieren der Nagios-Plugins.

```
chkconfig --add icinga
chkconfig icinga on
service icinga start
```

Hinzufügen von Icinga zu den Systemdiensten sowie Start von Icinga.

```
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

Öffnet den TCP Port 80 in der Firewall um von Extern auf den Webserver zugreifen zu können.

Anlagen, Teil 5 §206 Strafgesetzbuch

§206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Anlagen, Teil 6 Auszug aus dem BDSG

§9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der

Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder

9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§14 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle

dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn
   1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder
   2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über
   1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
   2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
   3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.
(4) Die Auskunftserteilung unterbleibt, soweit
   1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
   2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
   3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

   und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.
(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.
(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.
(7) Die Auskunft ist unentgeltlich.

§19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.
(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

Anlagen, Teil 7 Das Tool PING

In dieser Anlage werden die Kommandozeilenoptionen von PING unter der Version 6.1.7600.16385 beschrieben.

Parameter	Beschreibung
-t	Führt den PING solange durch, bis er mit STRG+C abgebrochen wird
-a	Löst den Hostnamen auf
-n count	Festlegen der Anzahl der Echo Anfragen
-l size	Festlegen der Größe des Paketes
-f	Deaktiviert das Fragmentieren von Paketen
-i TTL	Setzt die Lebensdauer des Paketes (Anzahl der zu passierenden Gateways)
-v TOS	Type of Service, VERALTET
-r count	Legt die Anzahl der Hops fest, bis zu dem die Route aufgezeichnet wird
-s count	Legt die Anzahl der Hops fest, bis zu dem der Zeitstempel aufgezeichnet wird
-j hostlist	Benutze die Option „Loose source route“ im IP Header
-k hostlist	Benutze die Option „Strict source route“ im IP Header
-w timeout	Setz das Zeitlimit um auf Rückantwort zu warten
-R	Benutzt den Routing-Header um die Rück-Route zu testen (nur IPv6)
-S srcaddr	Setz die zu benutzende Quelladresse
-4	Zwingt zum Benutzen des IPv4
-6	Zwingt zum Benutzen des IPv6

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 31. Januar 2014

Sirko König