Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Jan Nissen

Auswahl und Konzeptionierung eines Videokonferenzsystems zur Unterstützung der Globalisierung eines mittelständischen Unternehmens

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Jan Nissen

Auswahl und Konzeptionierung eines Videokonferenzsystems zur Unterstützung der Globalisierung eines mittelständischen Unternehmens

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr.-Ing. Martin Hübner
Zweitgutachter : Prof. Dr. Olaf Zukunft

Abgegeben am 04.10.2012

Jan Nissen

Thema der Bachelorarbeit

Auswahl und Konzeptionierung eines Videokonferenzsystems zur Unterstützung der Globalisierung eines mittelständischen Unternehmens

Stichworte

Videokonferenzsystem, Netzwerkanalyse, Schulungssystem, SNMP, RMON, sFlow, NetFlow

Kurzzusammenfassung

Die Verbreitung von Videokonferenzsystemen ist in den letzten Jahren stark gestiegen. Diese Systeme erweitern den örtlichen Konferenzraum um eine virtuelle Komponente. Entfernte Konferenzteilnehmer werden dabei über Bildschirme, Kameras und Mikrofone in Echtzeit in das vorhandene Gespräch eingegliedert.

Diese Arbeit beschäftigt sich mit Auswahl und Konzeptionierung eines solchen Videokonferenzsystems. Dabei wird die bereits vorhandene IT-Infrastruktur eines mittelständischen Unternehmens analysiert um Engpässe bezüglich der Datenübertragungsrate bei der Einführung zu erkennen und zu umgehen. Die Systemempfehlung basiert auf einer Markt-, einer Kosten-Nutzen-Analyse sowie einer Kostenaufstellung.

Jan Nissen

Title of the paper

Selection and conceptual design of a videoconferencing system to support the globalization of a medium-sized company

Keywords

videoconferencing system, network analysis, video training system, SNMP, RMON, sFlow, NetFlow

Abstract

The use of video conferencing systems has increased significantly over the last years. These systems expand the local conference room by a virtual component. Remote conference participants are integrated into the existing conversation in real time via screens, cameras and microphones.

This dissertation deals with the selection and the conceptual design of such a video conferencing system. The existing IT infrastructure of a medium-sized company has to be analyzed in order to detect bottlenecks in bandwidth before the system can be introduced. The recommendation of a system is based on a market, a cost-benefit analysis as well as a financial report.

Inhaltsverzeichnis

1 Einleitung

In den nächsten Kapiteln werden die Themenbeschreibung, das Ziel sowie die Struktur der Arbeit beschrieben.

1.1 Themenbeschreibung und Motivation

Das Unternehmen LESER GmbH & Co. KG besteht seit 1818 und hat sich 1970 auf die Herstellung von Sicherheitsventilen für den Industrieeinsatz spezialisiert. Es beschäftigt mehr als 600 Mitarbeiter und hat in den letzten Jahren mehrere neue weltweite Standorte gegründet, um seine Marktposition zu verbessern. Dabei befindet sich das Unternehmen im Umbruch von der Internationalisierung zur Globalisierung.

Es wurden im Ausland neben reinen Vertriebsbüros auch Standorte gegründet, die sämtliche Prozesse von der Materialbeschaffung über die Produktion bis hin zur Werkstattmontage von Ventilen durchführen.

Durch das schnelle und starke Wachstum muss die IT-Infrastruktur hinsichtlich Performanz, Skalierbarkeit und Ausfallsicherheit überprüft und neu bewertet werden, um eine geringe Latenz und hohe Verfügbarkeit zu gewährleisten.

Im Zuge dessen sollen die Standorte mit Videokonferenzsystemen ausgestattet werden, um das Wissen zwischen Standorten zu verteilen, die Schulung von Mitarbeitern sowie Kunden in neuen Standorten zu ermöglichen und um Reisekosten und Ausfallzeiten der Mitarbeiter zu senken.

1.2 Ziel der Arbeit

Das Ziel der Arbeit ist es eine Strategie zur Einführung eines Videokonferenzsystems im Unternehmen zu erstellen, die mit einem Vertriebspartner zeitnah umgesetzt werden kann, um Unternehmensstandorte im audiovisuellen Bereich miteinander zu verbinden.

Durch eine Analyse des bestehenden Netzwerkes werden Engstellen und Datentransfer ermittelt und bewertet.

Mit Hilfe einer Kosten- sowie einer Kosten-Nutzen-Analyse werden auf dem Markt befindliche Systeme bewertet. Basierend auf dieser Bewertung und der Analyse der bestehenden Netzwerkinfrastruktur wird eine Empfehlung für das einzusetzende Videokonferenzsystem gegeben.

Über die gegebenen Empfehlungen soll es möglich sein, das Netzwerk, falls notwendig, hinsichtlich der Datenübertragungsrate und Protokolle umzustrukturieren und das System zum Einsatz zu bringen.

1.3 Aufbau der Arbeit

Die Grundlagen zur Netzwerkanalyse sowie zur Videokonferenztechnik werden in Kapitel 2 erörtert.

Die Anforderungen des Unternehmens an ein Videokonferenzsystem werden in Kapitel 3 definiert, dort sind auch verschiedene Anwendungsszenarien beschrieben.

Kapitel 4 umfasst die Netzwerkanalyse der bestehenden Infrastruktur des Unternehmens LESER GmbH & Co. KG. Daten werden zu diesem Zweck ausgewertet und visualisiert. Aus dieser Auswertung resultiert letztendlich die Empfehlung zur Verbesserung des Netzwerkes in Hinblick auf Performanz und Ausfallsicherheit.

In Kapitel 5 wird auf Basis einer Marktanalyse, einer Kostenaufstellung und einer Kosten-Nutzen-Analyse eine Systemempfehlung gegeben.

Kapitel 6 beschreibt die spätere Integration dieser getroffenen Empfehlung in das bestehende Netzwerk sowie die notwendigen Maßnahmen, die für einen effizienten Betrieb getroffen werden müssen.

Die Arbeit wird dann mit einer Zusammenfassung der Ergebnisse und einem Ausblick auf zukünftige Technologien in Kapitel 7 abgeschlossen.

2 Grundlagen

Dieses Kapitel beschreibt in Abschnitt 2.1 die Grundlagen der Netzwerktechnik und in Abschnitt 2.2 die der Videokonferenztechnik.

2.1 Netzwerk

Im Folgenden werden die technischen Grundlagen beschrieben, die zur Analyse des Netzwerkes benötigt werden.

Zunächst werden die Grundlagen zur Separierung des Netzwerkes und der Priorisierung von Paketen erörtert. Dann folgt mit SNMP ein Protokoll, welches eine Zugriffsmöglichkeit auf die vorhandenen Netzwerkgeräte bietet. RMON, sFlow und NetFlow sind Statistikprotokolle, welche den Datenverkehr ermitteln und weitergeben können.

2.1.1 **VLAN**

Ein VLAN (virtuelles Netzwerk) ermöglicht die Separierung von Endgeräten, ohne die physikalische Verkabelung eines Netzwerkes zu verändern. Der zu diesem Zweck verabschiedete Standard 802.1Q des *Institute of Electrical and Electronic Engineers (IEEE)* aus dem Jahr 1995 sieht vor, dass die Größe des Paketrahmens von 1518 Bytes auf 1522 Bytes erhöht wird, um Netzwerke virtuell zu trennen (vgl. Zisler 2012, S. 155).

Die folgende Abbildung zeigt die Unterschiede (hier grau dargestellt) beim Aufbau eines Paketes zwischen dem für nicht-virtuelle Netzwerke üblichen Standard IEEE802.3 und dem VLAN-Standard IEEE802.1Q auf Ebene der Sicherungsschicht (Layer-2).

6 Byte	6 Byte	2 Byte	3 Bit	1 Bit	12 Bit	2 Byte	Max. 1500 Byte	4 Byte
MAC-Zieladresse	MAC-Quelladresse	0x8100	Priorisierung	CFI	VID (VLAN-Kennung)	Länge der Daten	Daten	Prüfsumme

Tabelle 2-1: Rahmenunterschiede durch Einführung von IEEE802.1Q zu IEEE802.3

Durch IEEE802.1Q wurden vier neue Felder im Rahmen eingeführt.

- 1. Feld, enthält die statische Protokollkennung 0x8100 (2 Byte)
- 2. Feld, enthält die Priorität des VLANs (QoS, siehe Kapitel 2.1.2). So kann entschieden werden, ob die ankommenden Pakete bevorzugt behandelt werden sollen.
- 3. Feld (CFI), enthält eine Kennziffer, die anzeigt, ob die MAC-Adresse im Little- oder im Big-Endian Format vorliegt.
- 4. Feld, enthält die VLAN Kennung, dabei sind theoretisch 2^{12} VLANs möglich, allerdings sind die VLAN Kennungen 0 sowie 4095 nicht gestattet, so dass 4.094 verschiedene virtuelle Netzwerke aufgebaut werden können.

2.1.2 **QoS**

Die Dienstgüte *(Quality of Service)* beschreibt die Priorisierung von Daten in einem Netzwerk, hierfür wurde der Standard IEEE802.1P verabschiedet. Dieser sorgt dafür, dass Pakete bevorzugt behandelt werden, wenn die Priorisierung durch das VLAN-Feld nach IEEE802.1Q gesetzt wurde.

Gerade IP-Telefonie sowie Videokonferenzsysteme sind kritische Anwendungen, bei denen dem Benutzer eine ungleichmäßige Verzögerung (*Jitter*), ein Verlust oder eine lange Laufzeit von Paketen auffällt. Es ist daher wichtig, diese Systeme vom normalen Datennetzwerk zu trennen und den Datenverkehr zu bewerten (vgl. Beasley 2004, S. 495; vgl. Scherff 2010, S. 58).

Die Priorisierungslevel wurden wie folgt festgelegt:

Level	**Bezeichnung**
0	Hintergrundaufgaben
1	Gute Leistung
2	Exzellente Leistung
3	Kritische Anwendungen
4	Video
5	Sprache
6	Netzwerksteuerung (global)
7	Netzwerksteuerung (lokal)

Tabelle 2-2: Priorisierung nach IEEE802.1P

Eine interessante Technik macht sich ein spezifisches Verhalten von TCP-Verbindungen zunutze - treffen niedrig und hoch priorisierte Pakete beim Router ein, so werden die niedrig priorisierten Pakete verworfen und nur die hoch priorisierten Pakete verschickt. Dies hat zur Folge, dass der Datenstrom durch das Verkleinern des Sendefensters zum Router verlangsamt wird. Diese Technik nennt sich *Weighted Random Early Discard (WRED)* (vgl. Beasley, 2004, S. 496).

2.1.3 **SNMP**

Das *Simple Network Management Protocol* bietet die Möglichkeit, Netzwerkgeräte von einem zentralen Ort aus zu konfigurieren und Informationen des Gerätes auszulesen.

Das Protokoll liegt in verschiedenen Versionen vor, die Grundstruktur ist nach RFC 1157 beschrieben und wird auch in den Versionen 2 und der momentan aktuellen Version 3 verwendet. Es definiert dabei die Kommunikation zwischen dem Manager und dem Agenten, welcher auf dem zu überwachenden Netzwerkgerät eingerichtet ist.

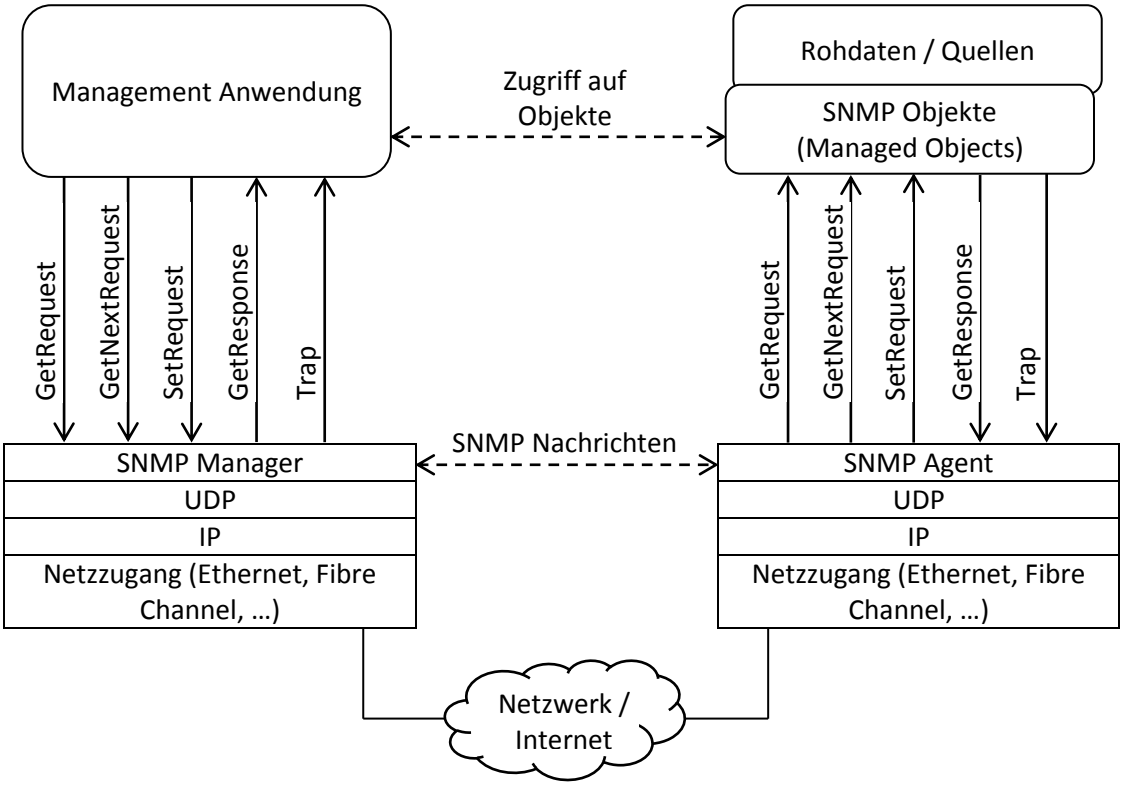

Abbildung 2-1: SNMP-Kommunikation

SNMP-Agenten sorgen dafür, dass Informationen des Gerätes ausgelesen und verändert werden können. Zudem besitzen sie eine Schnittstelle zum gekoppelten Netzwerk, zwecks Verwaltung durch entfernte SNMP-Manager. Daten werden dann zustandslos (unabhängige Transaktionen) über UDP versendet (vgl. Stallings 1999).

SNMP-Objekte oder auch *managed objects* enthalten sämtliche abrufbaren Informationen. Die Menge aller *managed objects* wird *management information base (MIB)* genannt. Sie ist als Inhaltsverzeichnis zu sehen, an welchen Positionen sich *managed objects* befinden, welche Daten sie beinhalten, wie sie abgerufen werden können und ob diese verändert werden dürfen. Die MIB dient daher als Schnittstelle zwischen Agent und den Rohdaten, die über die *managed objects* zu erreichen sind.

SNMP bietet mit der Standard-MIB selbst nur Zugriff auf einfachste Geräteinformationen (z.B. Name des Gerätes) (vgl. Rose 1993, S. 81-91). Um erweiterte Informationen abzurufen, ist es möglich die Schnittstelle zu erweitern. Im nächsten Kapitel wird daher mit RMON eine weitere MIB vorgestellt, welche Zugriffe auf beispielsweise Flussdaten ermöglicht.

Man unterscheidet zwischen zwei Arten von Informationsgewinnung über das *Simple Network Management Protocol*.

Die Management Anwendung kann sich die Informationen über sogenanntes *polling* aneignen. Dabei werden die Netzwerkgeräte in einem bestimmten Zeitintervall wieder und wieder nach einer Information gefragt. Aber gerade in großen Netzwerken verursacht dieses *polling* eine hohe Auslastung in der IT-Infrastruktur. Zudem können Fehlverhalten zwischen zwei Abfragen nicht immer erkannt werden.

Daher bietet die SNMP-Architektur sogenannte *traps*, dabei agieren die Agenten aktiv und der Manager passiv. Sollte ein vorkonfigurierter Schwellenwert, z.B. die Auslastung eines Ports, überschritten werden, so sendet der Agent selbstständig die nötigen Informationen zum Manager. Der Manager kann dann bei Erhalt weitere Daten anfordern (vgl. Rose 1993, S. 53).

Die Netzwerkgeräte des Unternehmens unterstützen die Versionen SNMPv2c und SNMPv3 des Protokolls. Die genauen Spezifikationen dieser Versionen sind in RFC 1901 sowie in RFC 3410 zu finden.

2.1.4 **RMON**

Die Abkürzung RMON steht für *Remote Network Monitoring* und erweitert damit die *management information base* der SNMP-Architektur. Durch die Implementierung von RMON ist es möglich, statistische Werte des Netzwerkverkehrs auf den entsprechenden Netzwerkgeräten zu protokollieren. Einen Überblick über die RMON Spezifikation bietet RFC 3577.

Man unterscheidet zwischen den Versionen 1 und 2 von RMON, diese werden im Folgenden vorgestellt.

RMON1 wurde nach RFC 2819 definiert und bietet Zugriff auf folgende Daten:

Gruppe	**Beschreibung**
ethernet statistics	Enthält gemessene Werte und stellt diese als Statistik zur Verfügung
history control	Bietet Einstellungen zum Erfassen von Netzwerkdaten
ethernet history	Erfasst über einen Zeitraum Werte und stellt diese gemittelt als Historie dar
alarm	Ermöglicht den Vergleich zwischen erfassten Werten und Grenzwerten. Sollte dabei ein gemessener Wert den Grenzwert überschreiten, so wird ein Ereignis generiert
host	Speichert die Datenmenge, die von einem angeschlossenen Gerät (Erkennung durch MAC-Adresse) verursacht wurde
hostTopN	Bietet die Sortierung und Ausgabe der gemessenen Daten aus der Gruppe „host“ an
matrix	Speichert die Datenmenge, die zwischen 2 Geräten anfällt, dabei werden die Geräte durch die MAC-Adresse erkannt
filter	Ermöglicht die Erkennung spezieller Pakete mit Hilfe eines Filters; sollte ein solches Paket erkannt werden, so wird ein Ereignis generiert
packet capture	Speichert Pakete, die durch einen Filter erkannt worden sind
event	Ermöglicht die Generierung und Bekanntgabe von Ereignissen

Tabelle 2-3: RMON1-Funktionsgruppen

Anders als Version 1 operiert RMON2 nicht auf den ersten beiden Schichten des Netzwerkreferenzmodells, sondern auf Schicht 3 und höher. Diese Erweiterung bietet 2 entscheidende Vorteile:

1. Durch die Sicht auf die Vermittlungsschicht ist es möglich, geroutete Pakete zu analysieren und so auch indirekte Netzwerke zu erfassen.
2. Die Anwendungsschicht bietet den Vorteil, dass die Analyse in Abhängigkeit genutzter Protokolle durchgeführt werden kann. So ist es z.B. möglich, nur den HTTP-Verkehr zu betrachten.

RMON2 wurde in RFC 2021 definiert und erweitert die in Tabelle 2-4 gezeigten Funktionen von RMON1 um weitere 9 Funktionsgruppen, die in der nachfolgenden Tabelle beschrieben sind.

Gruppe	**Beschreibung**
protocol directory	Enthält die Liste der Netzwerkprotokolle, die gemessen werden können
protocol distribution	Enthält Statistiken für jedes erkannte Netzwerkprotokoll
address mapping	Ermöglicht die Zuordnung einer MAC-Adresse zu einer IP-Adresse
Network layer host	Bietet Statistiken pro einzelnem Gerät auf Layer-3 Ebene
network layer matrix	Bietet Statistiken zwischen zwei Geräten auf Layer-3 Ebene
application layer host	Bietet Statistiken pro einzelnem Gerät auf der Anwendungsschicht
application layer matrix	Bietet Statistiken zwischen zwei Geräten auf der Anwendungsschicht
user history	Erstellt benutzerdefinierte Stichproben
probe configuration	Ermöglicht eine Konfiguration zur Aufnahme von Messwerten

Tabelle 2-4: RMON2-Funktionsgruppen

2.1.5 **NetFlow**

Netzwerkgeräte, die NetFlow unterstützen, können den anfallenden Datenverkehr zeitlich genau bestimmt analysieren und einem Host zuordnen. NetFlow arbeitet dabei durch das Erkennen von Anfangs- und Endpunkten des Netzwerkstroms sehr viel genauer als RMON2.

Anders als RMON ist NetFlow keine Ergänzung zur *management information base* in SNMP und unterliegt somit auch nicht den Beschränkungen oder Vorgaben. Allerdings kann das Protokoll über SNMP konfiguriert werden.

Die statistischen Daten werden nach Erkennung der Beendigung eines zusammenhängenden Datenstroms per UDP an einen Kollektor auf einem anderen System übertragen, der diese dann aufbereitet und zusammenfasst. Die Übertragung dieser Daten wird ausschließlich vom Netzwerkgerät initiiert.

Die Nachteile dieses Protokolls werden gerade bei hoher Verkehrslast sowie einem schnellen Interface ab 1 Gbit/s deutlich. So steigt der anfallende Statistik-Datenverkehr, welcher an den Kollektor gesendet wird, stark an. Zudem wird die CPU des Netzwerkgerätes bei dieser Zuordnung von Daten stark belastet.

NetFlow wurde ursprünglich von der Firma Cisco Systems entwickelt, das Protokoll liegt in der aktuellen Version 9 allerdings als offener Standard vor, den auch andere Hersteller einsetzen können, um statistische Daten zum Netzwerkverkehr zu versenden. Das Protokoll wurde in RFC 3954 definiert.

Über das NetFlow Protokoll können zum Beispiel folgende Daten übertragen werden:

- IP-Adressen von Quelle und Ziel
- Zeitstempel von Start und Anfang des Stroms
- Port von Quelle und Ziel
- Eingangs- und Ausgangsinterface vom Netzwerkgerät
- Protokollart
- Byte- und Paketzähler

2.1.6 **sFlow**

Die Arbeitsweise sowie die Funktionen von sFlow unterscheiden sich in den meisten Punkten nicht von denen in NetFlow, trotzdem sind diese beiden Protokolle nicht kompatibel.

sFlow bietet allerdings gerade bei schnellen Netzwerken einen entscheidenden Vorteil gegenüber NetFlow. Netzwerkströme werden dabei nicht im Gesamten betrachtet, sondern es werden in Intervallen Stichproben des anfallenden Netzwerkverkehrs entnommen.

Über die sogenannte *Sampling-Rate* wird festgelegt, wann, bzw. wie oft Pakete analysiert werden sollen. Ein Wert von 1.000 bedeutet, dass 1 Paket aus 1.000 analysiert wird. Dieses Intervall sollte nicht zu klein gewählt werden, um die Auslastung des Netzwerkgerätes nicht zu beeinträchtigen. Je höher die Geschwindigkeit des Interfaces, desto größer sollte auch die *Sampling-Rate* sein.

Ist die *Sampling-Rate* allerdings zu groß gewählt, kann es vorkommen, dass nicht jeder Paketstrom erkannt wird, da er zwischen zwei zu analysierenden Paketen liegt.

Für die *Sampling-Rate* gibt es keine Richtlinien, jedoch zeigt die folgende Tabelle realistische Werte für die verschiedenen Netzwerkgeschwindigkeiten.

Geschwindigkeit des Interfaces	**Sampling-Rate**
100 Mbit/s	1.000
1 Gbit/s	2.000
10 Gbit/s	20.000

Tabelle 2-5: Sampling-Rate bezogen auf Geschwindigkeit des Interfaces

Über das *Polling-Intervall* kann festgelegt werden, nach wie vielen Sekunden die statistischen Daten an einen Kollektor gesendet werden sollen. Auch hier sollte kein zu kleiner Wert festgelegt werden, um die Netzwerkgeschwindigkeit nicht zu beeinträchtigen. Ein Wert von 60 Sekunden wäre realistisch, um einen zeitnahen Überblick über das Netzwerk zu erhalten, ohne es dabei zu stark zu belasten.

Wie auch bei sFlow wird die Statistik per UDP versendet, das Netzwerkgerät initiiert dabei die Verbindung zum Kollektor.

2.2 Videokonferenztechnik

In diesem Kapitel werden die aktuell eingesetzten Technologien vorgestellt, auf die im Handel befindliche Videokonferenzsysteme bereits zugreifen.

Die Kapitel 2.2.1 und 2.2.2 informieren über den aktuellen Stand der Technik im Video- und Audiobereich. Die Informationen wurden in einem Treffen mit einem möglichen Vertriebspartner für ein Videokonferenzsystem, der DEKOM AG in Hamburg, ermittelt. Weitere Informationen sind in DEKOM 2012 zu finden.

In Kapitel 2.2.3 und Kapitel 2.2.4 werden die Hauptprotokolle H.323 und SIP beschrieben, die einen Verbindungsaufbau ermöglichen. Die eigentlichen Nutzdaten werden dann über RTP versendet, welches in Kapitel 2.2.5 beschrieben wird.

Die erforderlichen Hardware-Komponenten für ein Videokonferenzsystem sind zum einen der in Kapitel 2.2.6 beschriebene Codec, zum anderen die MCU, welche die Verbindungen zwischen mehreren Codecs verwalten kann (Kapitel 2.2.7).

Das Kapitel wird dann mit dem Abschnitt Sicherheit in 2.2.8 abgeschlossen.

2.2.1 **Video**

In einem Konferenzraum ist es wichtig, seinen Gesprächspartner naturgetreu in möglichst korrekter Größe sehen zu können. Daher sind auch Monitore bis hin zu 108“ Diagonale in Konferenzräumen nicht unüblich. Wichtig ist hier auch der Mindestsitzabstand zum Bildschirm, damit keine einzelnen Bildpunkte wahrgenommen werden können. Eine Grundformel besagt, dass die Diagonale des Bildschirmes multipliziert mit 3 den optimalen Sitzabstand kennzeichnet. Wichtig bei der Wahl des Monitors sind Kontrast und Helligkeit – je heller ein Raum, desto höher sollten Kontrast und Helligkeitswerte des Bildschirms sein, um Spiegelungen zu vermeiden und so den Gesprächsteilnehmer uneingeschränkt erkennen zu können. Für größere Bilddiagonalen können Projektoren eingesetzt werden, allerdings erreichen diese nicht die Brillanz eines Bildschirms.

Bedingt durch den Fortschritt der Multimediaindustrie und die Empfehlung nach ITU R.709 sind folgende Auflösungen entstanden, welche auch in der Videokonferenztechnik zum Standard geworden sind.

Kurzname	Auflösung horizontal	Auflösung vertikal	Bilder pro Sekunde
720p (progressive)	1280	720	30 Vollbilder
1080i (interlaced)	1920	1080	60 Halbbilder
1080p (progressive)	1920	1080	30 Vollbilder

Tabelle 2-6: gängige Videoauflösungen bei Videokonferenzsystemen

Höhere Auflösungen mit den Kurznamen 4k und 8k, welche die vier- bzw. achtfache 1080p-Auflösung bereitstellen, werden noch spezifiziert, so dass zu diesem Zeitpunkt keine standardisierten Geräte im Handel erhältlich sind.

Zusätzlich zu den unter dem Begriff HD genannten Auflösungen können auch niedrigere Auflösungen dargestellt werden. Dies ist gerade bei Soft-Clients bzw. für auf Reisen befindliche Mitarbeiter nützlich, falls keine ausreichende Datenübertragungsgeschwindigkeit zur Verfügung steht.

Auch die Kameratechnik setzt die in Tabelle 2-6 genannten Auflösungen ein. Es ist möglich, Kameras frei schwenk- und drehbar zu lagern. Der aktive Sprecher kann anhand der Akustik erkannt, verfolgt und fokussiert werden. Diese Verfolgung kann auch mit Drucksensoren im Boden erreicht werden.

Bei Live-Bildern erfolgt die Komprimierung der aufgezeichneten Daten nach ITU H.264. Sollen allerdings auch PC-Dokumente gezeigt werden, so muss der Codec einen Dual Stream Modus aktivieren. Nach ITU H.239 wird empfohlen die Auflösung auf XGA (1024 x 768 Bildpunkte) zu drosseln.

Wie bereits angedeutet können Dokumente von einem externen Rechner allen Präsentationsteilnehmern verfügbar gemacht werden. Der Rechner wird dazu einfach über den analogen oder digitalen Bildschirmausgang an das Videokonferenzsystem angeschlossen und die Schnittstelle aktiviert (Screen Sharing). Je nach Anzahl der verbauten Monitore im Konferenzraum kann zur Anzeige der Bildschirminhalte entweder ein gesonderter Monitor benutzt werden oder aber die Bild in Bild Funktion.

Abbildung 2-2 zeigt die aktivierte Screen Sharing Funktion, mit der es möglich ist, auf einem zusätzlichen Bildschirm eine Zeichnung zu präsentieren.

Abbildung 2-2: Screen Sharing (http://www.dekom.com/uploads/pics/Cisco-Profile65-Dual_05.gif)

2.2.2 **Audio**

Anders als das Wort „Videokonferenzsystem“ vermuten lässt, ist der Ton meist wichtiger als das Bild der Teilnehmer. So fallen Paketverluste bei einem Audiodatenstrom schnell auf und äußern sich durch nicht vollständige Worte, nicht beabsichtigte Sprachpausen oder Stimmverfälschungen der Teilnehmer.

Wichtig ist die Wahl des Mikrofons. Je nach Sitzabstand der Teilnehmer zu diesem muss die Lautstärke angepasst werden. Auch ist eine integrierte Echounterdrückung notwendig, um Rückkopplungen zu vermeiden. Über intelligente Erkennung von Störquellen, wie z.B. die Lüftergeräusche eines Projektors, können Hintergrundgeräusche gefiltert werden. Gerade bei der Telefontechnik kann sich diese Rauschunterdrückung aber auch störend auf die Gesprächsteilnehmer auswirken. So kann nicht mehr erkannt werden, ob eine Verbindung noch besteht oder nicht, falls der Gesprächspartner mal eine längere Sprachpause macht.

In aktuellen Videokonferenzsystemen werden Audiodaten verlustbehaftet nach AAC codiert und an die beteiligten Codecs versendet.

2.2.3 **H.323**

Packet-based multimedia communications systems wurde nach ITU H.323 spezifiziert und ermöglicht die Kommunikation zwischen Clients, den sogenannten Terminals. Es wurde für die Kommunikation zwischen nicht IP-fähigen Geräten über IP-Netzwerke entwickelt, kann allerdings auch IP-fähige Geräte adressieren. Damit bietet das H.323 Protokoll in den Grundzügen die gleichen Funktionen wie das in Kapitel 2.2.4 beschriebene und neuere SIP-Protokoll, welches allerdings nur für IP-fähige Geräte verfügbar ist.

Eine Interaktion der Clients setzt in der Regel die Benutzung eines sogenannten Gatekeepers voraus. Lediglich für direkte Point-to-Point Verbindungen ist dieser nicht notwendig. Endpunkte suchen für ihre Zone einen passenden Gatekeeper und registrieren sich bei diesem. Bei Anfrage eines anderen Endpunktes wird Auf- und Abbau der Verbindung vom Gatekeeper initiiert und geleitet.

Da das H.323 Protokoll und die Verbindung zwischen Clients sehr komplex ist, wird an dieser Stelle auf ein Schaubild verzichtet. Trick 2005 vermittelt auf Seite 107 einen guten Überblick über die Kommunikationswege des Protokolls.

Die anfallenden Nutzdaten werden bei H.323 analog zu SIP verbindungslos über RTP, wie in Kapitel 2.2.5 erläutert, transportiert.

2.2.4 **SIP**

Das Session Initiation Protocol ist für das ordnungsgemäße Herstellen und Abbauen von Verbindungen zwischen Teilnehmern verantwortlich und stellt eine Alternative zum Protokoll H.323 dar, kann allerdings nur in einer homogenen Umgebung von IP-fähigen Geräten eingesetzt werden. Ein Teilnehmer erhält eine SIP-Anschlusskennung, die sogenannte SIP URI (Unified Ressource Identifier), ähnlich einer E-Mail Adresse in Form von SIP:USER@HOST. Ein Beispiel wäre „sip:hh-1@leser.com“.

Eine Registrierung von mehreren Geräten auf einen einzigen URI ermöglicht ein verzweigtes Rufen, so dass alle Geräte zur selben Zeit klingeln (vgl. Kanbach 2005, S. 42).

Die Verbindung wird in den meisten Fällen verbindungslos über UDP aufgebaut, da SIP bereits integrierte Funktionen bietet, um möglichen Verbindungsabbrüchen entgegenzuwirken (vgl. Trick 2005, S. 124).

Die Verbindungsinitiierung und der Verbindungsabbau werden in Abbildung 2-3 aufgezeigt.

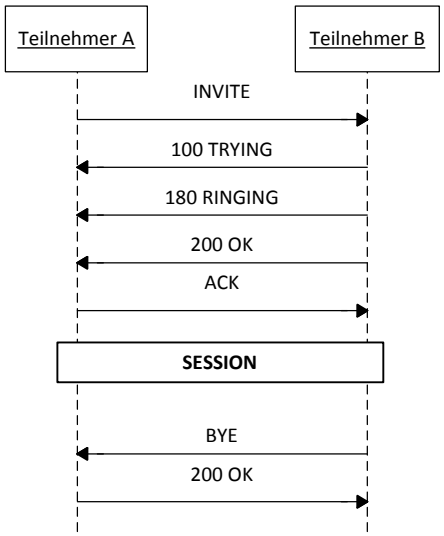

Abbildung 2-3: SIP-Verbindungsaufbau und Verbindungsabbau

Wie auch beim H.323-Protokoll werden Nutzdaten mit Hilfe von RTP übertragen (siehe Kapitel 2.2.5).

„Gegenüber der von der ITU-T spezifizierten H.323-Protokollsammlung bietet das SIP u.a. den Vorteil der verhältnismäßig einfachen, an typischen IP-Anwendungen orientierten Architektur. Standardabläufe wie z.B. der Verbindungsaufbau inkl. der Aushandlung von Medien sind in einer SIP-basierten Kommunikation deutlich einfacher realisiert und bedürfen bezüglich ihrer Analysierbarkeit keiner Decodierung bzw. Übersetzung.“ (Trick 2005, S. 123)

2.2.5 **RTP**

Das *Real-time Transport Protocol* erlaubt die Übertragung von Audio- und Videoechtzeitdaten über die Transportschicht mittels eines verbindungslosen, nicht gesicherten Ende-zu-Ende Transports.

RTP ist nach RFC 3550 spezifiziert. RTP-Datagramme werden per UDP so schnell wie möglich an den Empfänger versendet, ohne Pakete bei Verlust erneut zu senden. Durch eine zeitliche Synchronisation zwischen Sender und Empfänger wird das Echtzeitverhalten

gewährleistet (vgl. Trick 2005, S. 90). Pakete werden nummeriert und Zeitstempel eingefügt, um auf der Empfängerseite die Reihenfolge der Pakete wieder herstellen zu können, falls sich diese während des Transports geändert haben sollte. Des Weiteren ist eine qualitative Beurteilung über den Zeitstempel möglich. Durch die zeitliche Synchronisation kann die Verweildauer zwischen Sender und Empfänger ermittelt werden.

Pro sendendem Teilnehmer wird eine RTP-Sitzung initiiert und der zu nutzende Port (nur gerade Portnummern) festgelegt. Will ein Teilnehmer Audio- und Videoströme übertragen, wie es bei einer Videokonferenz der Fall ist, so müssen zwei RTP-Sitzungen initiiert werden.

Der Aufbau eines RTP-Paketes wird in Tabelle 2-7 veranschaulicht.

32 Bit								
2 Bit	1 Bit	1 Bit	4 Bit	1 Bit	7 Bit	16 Bit		
RTP Version	Padding Bytes folgen	Erweiterungs-header folgt	Anzahl der CSRC Bezeichner	Sprachpausen unterdrücken	Payload Daten zur Dekodierung	Sequenz Nummer	Header	erw. Header
Zeitstempel								
RTP –Nummer wird einmalig bei Initiierung der Sitzung generiert								
CSRC Bezeichner (nur bei Mischsignalen bei mehr als 2 Quellen) [optional]								
Nutzdaten								

Tabelle 2-7: Aufbau eines RTP-Paketes

Die Qualität der empfangenden Pakete kann periodisch an alle Teilnehmer gesendet werden. Für die Verteilung von Statistik- und Statusinformationen zur Beurteilung der Empfangsqualität kann das *RTP Control Protocol (RTCP)* verwendet werden. Genauere Informationen zum Protokoll sind in Kanbach 2005 sowie in RFC 3550 zu finden.

2.2.6 **Codec**

Ein Hardware Codec stellt die Schnittstelle zwischen Peripherie und Netzwerk dar. Ein- und Ausgabegeräte wie Bildschirm und Mikrofon werden an diesen angeschlossen, das System codiert deren Signale und sendet sie per SIP, H.323, bzw. RTP über den LAN-Anschluss an einen entfernten Teilnehmer, der diese Signale decodiert.

Abbildung 2-4 zeigt einen Codec mit den typischen Schnittstellen.

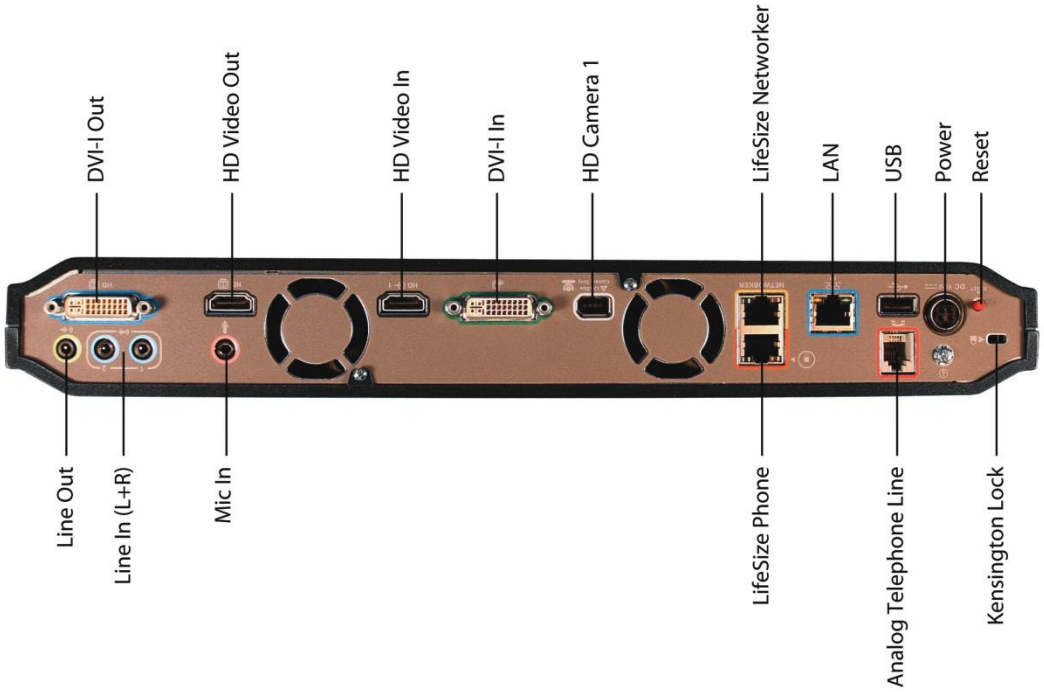

Abbildung 2-4: Codec (Lifesize Team 220)
http://www.lifesize.com/~/media/Media_Kit/Product_Images/LifeSize_Team/Team_220/Team220_back_panel.ashx

2.2.7 MCU und Verbindungsaufbau

Die *Multipoint Control Unit* bietet die Möglichkeit eine Konferenz mit mehr als zwei Teilnehmern aufzubauen. Sie dient als Knotenpunkt zwischen den einzelnen Konferenzpartnern und mischt die einzelnen Audiosignale zu einem Gesamtsignal, welches in Form von Nutzdaten wiederum an alle Teilnehmer gesendet wird.

Die MCU hat einen eigenständigen SIP URI, der an den Standorten bekannt sein muss. Konferenzpartner bauen die Verbindung zu diesem „Conference Server“ auf und senden die unterstützten Kompressionsverfahren und Codecs an diesen. Die Aushandlung findet dann auf der MCU statt (vgl. Rosenberg 2005).

Folgende Abbildung zeigt das Zusammenspiel zwischen den Teilnehmern sowie der MCU. Zu beachten ist, dass die MCU nicht zwangsläufig als dediziertes System gesehen werden muss, eine Verlagerung der MCU in einen der Clients ist ebenso möglich. Zur besseren Verständlichkeit ist sie hier allerdings als eigenständiges System abgebildet (vgl. Trick 2005, S. 209).

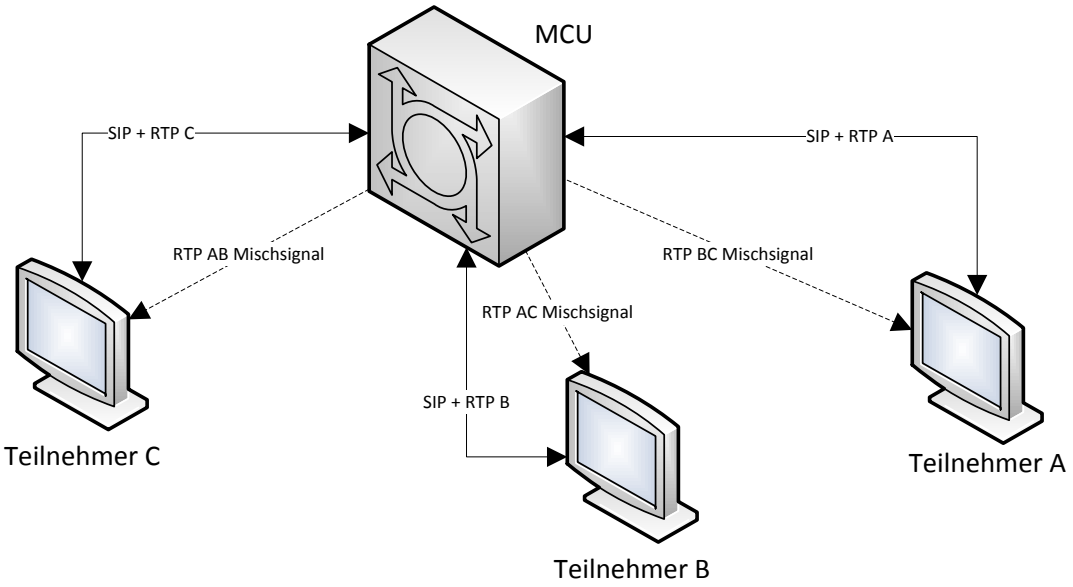

Abbildung 2-5: MCU-Verbindung

Der Verbindungsaufbau geschieht über das bereits in Kapitel 2.2.4 beschriebene SIP-Protokoll. Nutzdaten werden dann über das RTP-Protokoll übertragen. Alle Teilnehmer senden Audio- und Videodaten an die MCU, die dort vermischt und an den Endpunkt weitergeleitet werden. Beispielhaft werden die gemischten Audiosignale von Teilnehmer A und B als Strom AB zusammengefasst und an Teilnehmer C gesendet. Eine Mischung aller Audiosignale ist nicht gewünscht, da sich Teilnehmer zeitverzögert selbst hören könnten.

Es ist möglich Ports auf einer entfernten MCU bei einem Anbieter zu mieten. Dies bietet die Möglichkeit, bei einer Erweiterung des Systems die Anzahl der gemieteten Ports feingranular zu variieren. Service Level Agreements (SLA) definieren den Wartungszeitraum, die garantierte Datentransferleistung, sowie den Verfügbarkeitszeitraum eines solchen Systems.

Sollen weitere Unternehmen an einer eigenen Videokonferenz teilnehmen, so muss das Videokonferenzsystem auch außerhalb des Firmennetzwerkes erreichbar sein. Dies ist mit Traversal Servern möglich, die für eine Adressübersetzung und eine sichere Verbindung zwischen den Systemen sorgen.

2.2.8 **Sicherheit**

Die Videokonferenztechnik ermöglicht zwar den einfachen Austausch von Informationen, allerdings muss beachtet werden, dass auch unternehmensrelevante Daten über dieses Medium gesendet werden.

Eine Verschlüsselung der Datenströme kann auf zwei Wegen erreicht werden.

Interne Verschlüsselung

Auf dem Markt befindliche Codecs verschlüsseln nach Empfehlung der *International Telecommunication Union* die Daten mit dem *Advanced Encryption Standard (AES)* mit einer Schlüssellänge von 128 Bit. Eine detaillierte Beschreibung dieses Verfahrens sowie des Schlüsselaustauschs ist in ITU H.235 zu finden. Die mathematischen Aktionen zur Erzeugung von einer AES Blockchiffre sind Schmeh 2007 zu entnehmen.

Externe Verschlüsselung

Reicht die interne Verschlüsselung des eingesetzten Systems nicht aus oder sollen individuelle Schlüssel benutzt werden, so muss auf ein externes System zurückgegriffen werden. Dabei wird vor dem Codec ein weiteres System platziert, welches IP- und MAC-Adresse des Codecs übernimmt und so transparent wirkt. Die Schlüssellänge erhöht sich bei diesem Verfahren auf mindestens 256 Bit.

Der Vorteil eines solchen Systems liegt zum einen in der besseren Verschlüsselung der Daten und auch der Entlastung des Codecs. Zum anderen wird sichergestellt, dass auch Codecs verschiedener Hersteller sicher kommunizieren können, da Inkompatibilitäten ausgeschlossen werden.

3 Anforderungen und Szenarien

Dieses Kapitel beschreibt die Anforderungen des Unternehmens an ein Videokonferenzsystem, zudem werden in Kapitel 3.3 Anwendungsszenarien eines Beispielbetriebs aufgezeigt. Die Vorbedingungen müssen erfüllt sein, um die Einführung des Systems mit den direkten Anforderungen durchführen zu können.

3.1 Anforderungen

Das Unternehmen LESER GmbH & Co. KG hat folgende Anforderungen an ein Videokonferenzsystem. Sie wurden in Gesprächen mit den entsprechenden Stakeholdern ermittelt:

Allgemeine Anforderungen und Wirtschaftlichkeit

1. Es sollen zwei Konferenzräume an den Standorten Hamburg und Hohenwestedt eingerichtet werden. Das Konzept zur Einrichtung soll auf weitere Standorte übertragbar sein
2. Die maximale Teilnehmerzahl einer Konferenz sind:
    - 15 für Hamburg (General Management Meeting)
    - 8 für Hohenwestedt
3. Das Herstellen einer Verbindung zu anderen Standorten oder Mitarbeitern soll einfach und intuitiv möglich sein (der Schulungsaufwand der Anwender muss dazu so gering wie möglich sein)
4. Die Reisekosten sollen durch ein solches System um etwa 25 % vermindert werden (vgl. IMWF 2008)

Anforderungen an die Hardware

5. Die Hardware (Monitore, Mikrofon, Kamera) soll in den beiden Konferenzräumen fest montiert werden
6. Die Oberkörper aller Konferenzteilnehmer sollen sichtbar sein, um die Körpersprache deuten zu können

Anforderungen an die Software

7. Es soll möglich sein Mitarbeiter, welche auf Reisen sind, per VPN den Konferenzen zuzuschalten. Die Mitarbeiter benötigen zu diesem Zweck eine entsprechende Anwendung auf dem mobilen Gerät (Laptop Microsoft Windows 7, Apple iPad 2)
8. Es soll möglich sein, den Konferenzteilnehmern Bildschirminhalte zu präsentieren, um Schulungen in Anwendungen zu geben und Präsentationen zu halten (Screen-Sharing)

Durch die Einführung des Systems sollen durch Reisen verursachte Kosten und die Ausfallzeit von Mitarbeitern durch Reiseaktivitäten verringert werden. Zudem soll der Vorteil der „schnellen Kommunikation“ genutzt werden, um wichtige Entscheidungen zeitnah auch ohne die Buchung von Flügen und Hotels treffen zu können.

3.2 Vorbedingungen und indirekte Anforderungen

Da keine Dokumentation des aktuellen Netzwerkes sowie der Topologie zum Zeitpunkt der Erstellung dieser Arbeit vorlag, muss das Netzwerk hinsichtlich der Struktur, der Geschwindigkeit und der Ausfallsicherheit analysiert werden:

- Das Netzwerk und die entsprechenden Knotenpunkte müssen visualisiert werden, um die Struktur des Netzwerkes erkennen zu können
- Die Paketübertragungszeiten (Latenzen) zwischen Standorten müssen gemessen werden
- Die maximal verfügbare Datenübertragungsrate der Standorte muss ermittelt werden
- Die gemittelte, tatsächlich genutzte Datenübertragungsrate der Standorte muss über einen längeren Zeitraum erfasst werden

Zusätzlich zu den bereits gegebenen Anforderungen sind besonders folgende nichtfunktionalen Anforderungen wichtig. Diese sind allerdings nicht an das System selbst geknüpft, sondern an das Zusammenspiel zwischen Videokonferenzsystem und dem bestehenden Netzwerk.

Verfügbarkeit

Das Videokonferenzsystem sollte eine hohe Verfügbarkeit aufweisen. Dafür müssen zum einen die Hauptstandorte über eine stabile Internetverbindung verfügen, zum anderen muss das Videokonferenzsystem selbst zu jeder Zeit eine Verbindung aufbauen und aufrechterhalten können.

Sicherheit

Es darf nicht möglich sein, Videokonferenzen abzuhören oder gar zu verändern. Das Netzwerk muss also auf mögliche Schwachstellen untersucht werden. Ein weiterer Schutz besteht in einer Verschlüsselung des Datenstroms zwischen den Endgeräten der jeweiligen Konferenzteilnehmer.

Leistung und Effizienz

Das System sollte mit möglichst kleiner Transferrate möglichst viele Informationen übertragen können, um den Anschluss zum Internet bzw. die VPN Tunnel nicht unnötig zu belasten.

3.3 Anwendungsszenarien

Szenario 1 – Global Management Meeting:

Ein denkbarer Einsatzzweck des Videokonferenzsystems sind regelmäßige Treffen der Geschäftsführung sowie der Abteilungsleiter im Unternehmen. An diesem sind etwa 15 Personen in Deutschland (14 leitende Personen + 1 Referent), sowie 6 Personen in den Außenstandorten beteiligt. Die Außenstandorte sind dabei übergangsweise nicht mit einem Hardwarekonferenzsystem, sondern aufgrund der geringen Anzahl der Mitarbeiter mit einer softwareseitigen Lösung angebunden. In diesem Treffen müssen alle Personen erkennbar sein. Zusätzlich zu diesem General Management Meeting finden noch weitere Treffen statt, die Gesamtanzahl der Teilnehmer ist allerdings bei diesem Treffen am höchsten. Aufgrund der hohen Teilnehmeranzahl wird auch die zu benutzende Datenübertragungsrate zwischen Konferenzinitiator und Teilnehmern die höchste sein.

Szenario 2 – Produktschulungen:

Die Marketing Abteilung ist für die Schulung der LESER-eigenen Anwendung VALVESTAR® zuständig. Dabei wird ein Mitarbeiter in Hamburg die Software über das Konferenzsystem vorstellen und den Bildschirminhalt seines PCs (Laptops) für die Allgemeinheit zur Verfügung stellen, so dass die Teilnehmer der Präsentation der Anwendung folgen können. Eine weitere Rolle nimmt die LESER-ACADEMY ein, hier werden entfernte Mitarbeiter im Umgang mit den Produkten oder z.B. SAP geschult.

Szenario 3 – Optimierung der Fertigungsprozesse:

Es findet ein regelmäßiges Treffen zwischen der Produktion am Standort Hohenwestedt sowie der Entwicklung in Hamburg statt. An diesem Treffen sind etwa 8 Mitarbeiter beteiligt, die sich gleichmäßig auf die Standorte verteilen. Der Diskussionsgegenstand ist die Problembehebung und Optimierung der Fertigungs- und Entwicklungsprozesse. Die Grundlagen bieten hier technische Dokumente und Zeichnungen, die allen Konferenzteilnehmern angezeigt werden sollen.

Szenario 4 – Kurzfristige Kommunikation:

Die bereits genannten Szenarien beschreiben eine regelmäßige und planmäßige Kommunikation zwischen den Teilnehmern. Der Hauptanteil der Kommunikation kommt allerdings durch kurzfristige Gespräche zustande. So müssen z.B. Probleme bei der Fertigung, Abstimmungen in Projekten und Reklamationen geklärt werden.

4 Analyse des bestehenden Netzwerkes

Um das Netzwerk nun für die Einführung eines Videokonferenzsystems wie in Kapitel 3.2 beschrieben zu analysieren, sind mehrere Schritte nötig.

In Kapitel 4.1 wird der IST-Zustand des Netzwerkes aufgenommen und Standorte werden durch Netzwerkpläne visualisiert. Zudem werden Gerätetabellen erstellt, die einen Überblick über die verwendete Hardware geben.

In Kapitel 4.2 wird eine Erfassungs- und Überwachungssoftware (im folgenden Kollektor genannt) evaluiert und eingerichtet, um Netzwerkströme und Fehler erkennen zu können. Die eingesetzten Netzwerkgeräte werden so konfiguriert, dass sie den Netzwerkverkehr protokollieren und die Informationen dann an das Überwachungssystem senden.

In Kapitel 4.3 werden die empfangenen Daten ausgewertet, zudem werden Messungen durchgeführt, um das Netzwerk zu bewerten.

In Kapitel 4.4 wird dann eine Empfehlung zur Konfiguration des Netzwerkes erstellt, um mögliche Engpässe bei der Einführung eines Videokonferenzsystems zu erkennen und zu umgehen.

4.1 Bestandsaufnahme und Visualisierung

Als Basis zur Untersuchung des Netzwerkes auf Engpässe im Betrieb werden dessen Knotenpunkte inventarisiert und visualisiert. Als Knotenpunkte werden dabei Switches, Gateways, Router sowie Firewalls bezeichnet.

Die Visualisierung dient dazu, einen Überblick über die Gesamtstruktur des Netzwerkes zu erhalten und das Zusammenspiel der einzelnen Komponenten zu erfassen. Zusätzlich wird ermittelt, inwieweit die Netzwerkgeräte die bereits genannten Techniken zur Erhebung von statistischen Daten unterstützen.

Die LESER GmbH & Co. KG ist ein Unternehmen, welches historisch gewachsen ist und seine Ursprünge in den Standorten Hamburg und Hohenwestedt hat. In den letzten Jahren wurden mehrere Tochtergesellschaften gegründet, die nicht nur den Vertrieb von Sicherheitsventilen übernehmen, sondern auch die Produktion und Montage.

Das Unternehmen agiert dabei über folgende Standorte:

- Deutschland, Hamburg
- Deutschland, Hohenwestedt
- USA, Charlotte
- Indien, Mumbai
- Indien, Paithan
- Singapur
- Bahrain, Manama
- Brasilien, Rio de Janeiro

Abbildung 4-1: Standorte des Unternehmens

Alle Standorte sind dabei über ein IPSEC Sternnetzwerk (Site-to-Site VPN) mit dem Knotenpunkt Hamburg vernetzt. Der Schlüsselaustausch wird über IKEv1 realisiert, zur Verschlüsselung der Daten wird der AES Algorithmus mit 128 Bit verwendet.

Genaue Spezifikationen zur Verschlüsselung und zum Schlüsselaustausch sind in Eckert 2008 auf den Seiten 702-711 zu finden.

Zusätzlich zu den VPN-Verbindungen sind zwei Standleitungen vorhanden, zum einen in Deutschland zwischen Hamburg und Hohenwestedt, zum anderen in Indien zwischen Mumbai und Paithan.

Im Unternehmen werden hauptsächlich Layer-2 und Layer-3 Netzwerkgeräte der Marken Hewlett-Packard (HP) und Cisco Systems eingesetzt. Es handelt sich dabei um Geräte auf UNIX-Basis, welche einen SSH, Telnet oder Webzugang anbieten. Nähere Informationen zu den Netzwerkschichten liefert Tanenbaum 2003 auf Seite 67.

Eine Dokumentation des bestehenden Netzwerkes im Unternehmen war nicht gegeben, so dass die Erkennung der einzelnen Komponenten über verschiedene Strategien durchgeführt werden musste. Diese werden im Kapitel 4.1.1 beschrieben.

Im Rahmen dieser Arbeit werden alle Standorte visualisiert, jedoch werden nur die Hauptstandorte Hamburg und Hohenwestedt exemplarisch in Kapitel 4.1.2 und Kapitel 4.1.3 im Detail ausgeführt, um die Wirksamkeit dieser Strategie zu demonstrieren.

Der Standort Hamburg ist der Hauptstandort des Unternehmens. In diesem werden die Entwicklung, Konstruktion und der Verkauf von Sicherheitsventilen vorangetrieben. Zudem befinden sich hier der strategische Einkauf und die Finanzabteilung. In Hamburg werden momentan etwa 180 Mitarbeiter beschäftigt.

Der Standort Hohenwestedt ist mit einer Mitarbeiteranzahl von etwa 300 der größte Standort des Unternehmens. Hier werden die Sicherheitsventile produziert, montiert und versendet. Zudem finden hier die Qualitätskontrolle sowie die Produktions- und Fertigungsplanung statt.

4.1.1 Strategie zur Visualisierung eines unbekannten Netzwerkes

Dadurch, dass für die Namensdienste Windows-Systeme eingesetzt werden, kann eine bestimmte Eigenschaft der Namensauflösung ausgenutzt werden. In Verbindung mit einen IP-Adressbereich-Scanner und *nslookup* können Geräte identifiziert werden, die im firmeninternen DNS-Server keinen registrierten Hostnamen besitzen, allerdings auf *ICMP-Echo-Reply (Ping)* reagieren. Diese Geräte sind „nicht-Windows-Geräte“ - ein erstes Indiz dafür, dass es sich um Netzwerkkomponenten handeln könnte.

Ein anschließender Portscan auf diesen erkannten Geräten kann die Suche weiter eingrenzen. So sind folgende Ports für ein Netzwerkgerät der eingesetzten Marken typisch:

Port	Protokoll
22	SSH
23	TELNET
80	HTTP
443	HTTPS

Tabelle 4-1: Zuordnung Port/Protokoll

Durch diese Informationen entsteht nun eine Menge aus Geräten, die als Knotenpunkt in Frage kommen.

Über den Zugriff auf das entsprechende Webinterface oder den Shell Zugang können im nächsten Schritt die Netzwerkgeräte nun eindeutig identifiziert werden.

Um allerdings den Anschluss dieser Komponenten untereinander zu erfassen, ist ein Zugang zur Konsole erforderlich, die in diesem Fall per SSH oder Telnet erreicht werden kann.

Angeschlossene Geräte können über das *Cisco Discovery Protocol (CDP)* erkannt werden. Sowohl HP- als auch Cisco-Geräte unterstützen dieses Protokoll gleichermaßen, es ist nicht herstellergebunden.

Der Befehl dafür ist auf Geräten beider Hersteller identisch.

```
show cdp neighbors
```

Es erscheint eine Liste der direkt angeschlossenen Geräte und der zugehörigen physikalischen Portinformation.

Sollte CDP nicht unterstützt werden, so müssen die Anschlussinformationen über die MAC-Adress-Tabellen der einzelnen Netzwerkgeräte ausgelesen werden.

Die MAC-Adress-Tabellen können folgendermaßen angezeigt werden:

Hersteller	Befehl
Hewlett-Packard	`show mac-address [Port]`
Cisco Systems	`show mac-address-table [|include Port]`

Tabelle 4-2: Befehle zur Anzeige der MAC-Adressen

Beide Befehle zeigen alle bekannten Geräte im Netzwerk. Dabei kann eine Filterung nach physikalischen Ports angegeben werden. Mit Hilfe dieser Methoden kann nun eine Netzwerktopologie erstellt werden, allerdings ist die maximale Datenübertragungsrate zwischen diesen Geräten noch unbekannt.

Analog zur Ausgabe der angeschlossenen Geräte können die Informationen über die Verbindungsgeschwindigkeit zu diesen ausgegeben werden.

Hersteller	Befehl
Hewlett-Packard	`show interfaces brief`
Cisco Systems	`show interfaces status`

Tabelle 4-3: Befehle zur Anzeige der Übertragungsrate zwischen Geräten

4.1.2 **Netzwerktopologie – Deutschland – Hamburg**

Abbildung 4-2 zeigt die Netzwerktopologie des Standortes Hamburg, die mit der in Kapitel 4.1.1 beschriebenen Strategie erstellt wurde.

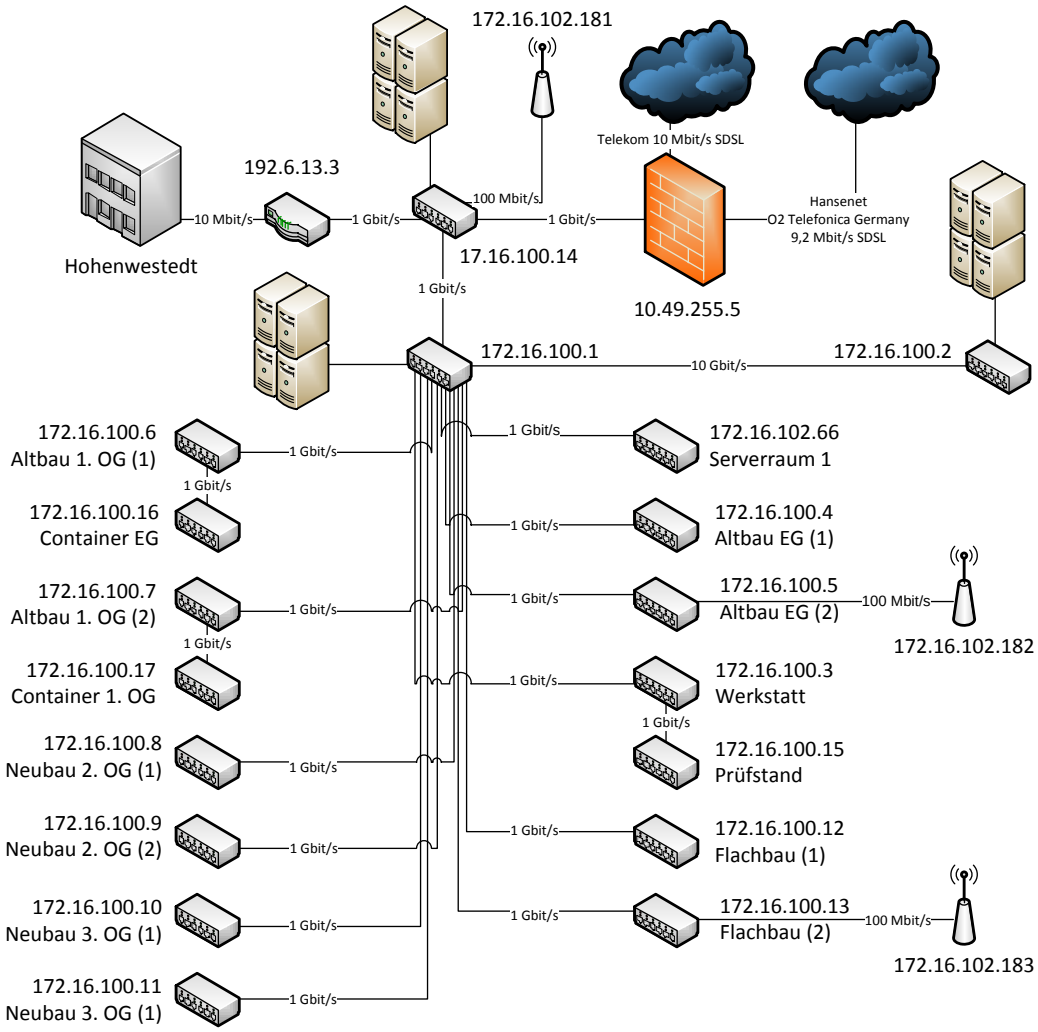

Abbildung 4-2: Netzwerkplan - Deutschland - Hamburg

Um einen Überblick der genutzten Netzwerkgeräte zu erhalten, wurde zusätzlich zur Visualisierung der Topologie eine tabellarische Ansicht erstellt, welche Auskunft über die

Typenbezeichnungen der Netzwerkgeräte, die Portauslastung und das unterstütze Statistikprotokoll gibt.

IP-Adresse	Typ	Typenbezeichnung	Portbelegung	Statistik
10.49.255.5	Firewall	Cisco ASA 5510 (2x)	-	NetFlow
192.6.13.3	Gateway	Cisco 2821	-	NetFlow
172.16.100.1	Backbone	HP ProCurve 5406zl-48G PoE	47/60	sFlow
172.16.100.2	Backbone	HP ProCurve 3500yl-48G-PWR	37/48	sFlow
172.16.100.3	Switch	HP ProCurve Switch 2610-24/12-PWR	3/24	sFlow
172.16.100.4	Switch	HP ProCurve Switch 2610-24-PWR	16/24	sFlow
172.16.100.5	Switch	HP ProCurve Switch 2610-24-PWR	12/24	sFlow
172.16.100.6	Switch	HP ProCurve Switch 2610-24-PWR	13/24	sFlow
172.16.100.7	Switch	HP ProCurve Switch 2610-24-PWR	11/24	sFlow
172.16.100.8	Switch	HP ProCurve Switch 2610-24-PWR	21/24	sFlow
172.16.100.9	Switch	HP ProCurve Switch 2610-24-PWR	11/24	sFlow
172.16.100.10	Switch	HP ProCurve Switch 2610-24-PWR	21/24	sFlow
172.16.100.11	Switch	HP ProCurve Switch 2610-24-PWR	16/24	sFlow
172.16.100.12	Switch	HP ProCurve Switch 2520-24-PoE	14/24	RMONv1
172.16.100.13	Switch	HP ProCurve Switch 2520-24-PoE	16/24	RMONv1
172.16.100.14	Switch	HP ProCurve Switch 2650-PWR	39/48	RMONv1
172.16.100.15	Switch	HP ProCurve Switch 2650	6/48	RMONv1
172.16.100.16	Switch	HP ProCurve Switch 2610-24/12-PWR	12/24	sFlow
172.16.100.17	Switch	HP ProCurve Switch 2610-24-PWR	12/24	sFlow
172.16.102.66	Switch	Dell Power Connect 5324	21/24	RMONv1
172.16.102.181	Access Point	Cisco RV110W	-	-
172.16.102.182	Access Point	Cisco RV110W	-	-
172.16.102.183	Access Point	Cisco RV110W	-	-

Tabelle 4-4: eingesetzte Netzwerkgeräte - Deutschland - Hamburg

4.1.3 **Netzwerktopologie – Deutschland – Hohenwestedt**

Analog zum Standort Hamburg wurde der größte Standort des Unternehmens in Hohenwestedt visualisiert. Abbildung 4-3 zeigt die Netzwerktopologie des Standortes.

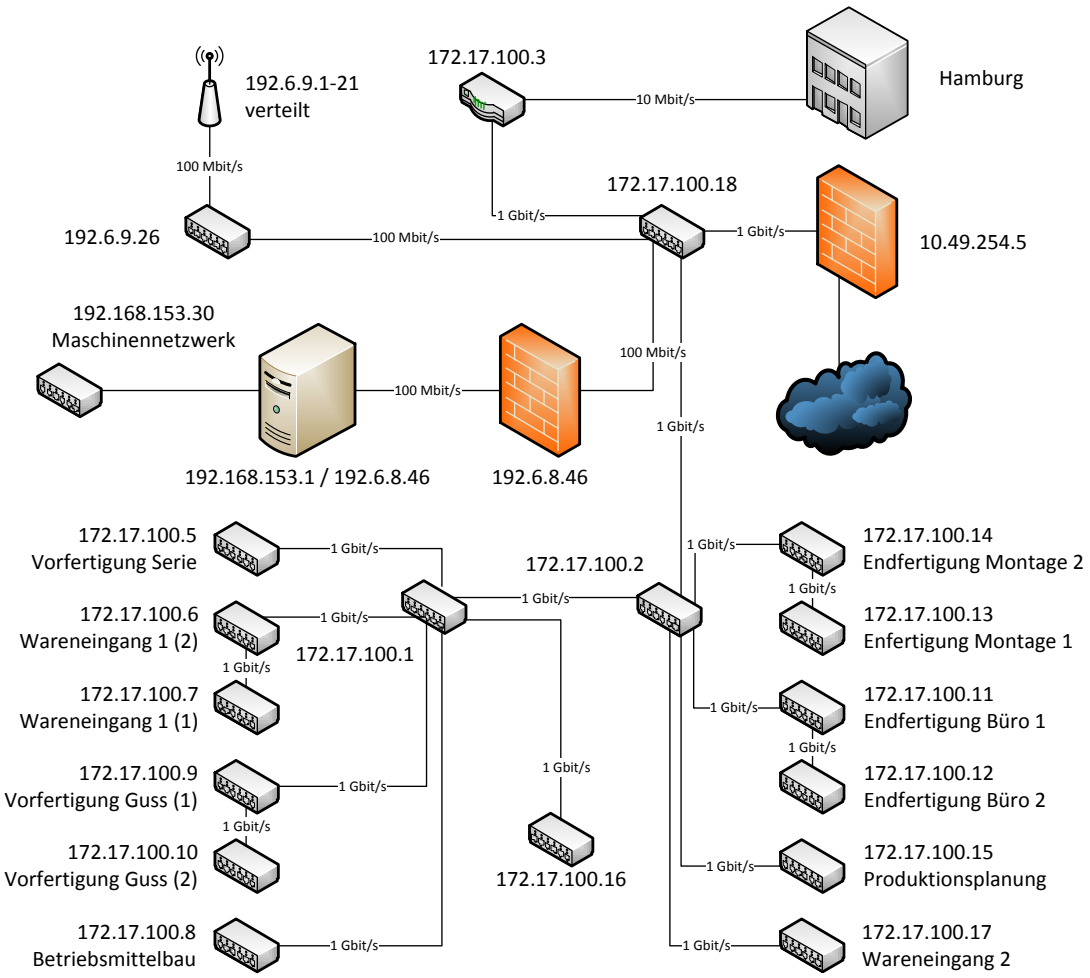

Abbildung 4-3: Netzwerkplan - Deutschland - Hohenwestedt

Tabelle 4-5 zeigt die eingesetzten Netzwerkgeräte, deren Portbelegung und das unterstützte Statistikprotokoll.

IP-Adresse	Typ	Typenbezeichnung	Portbelegung	Protokoll
10.49.254.5	Firewall	Cisco ASA 5510	-	NetFlow
172.17.100.1	Gateway	Cisco 2821	-	NetFlow
172.17.100.2	Switch	Cisco WS-C3750-12S	6/12	RMONv1
172.17.100.3	Switch	Cisco WS-C3750-12S	6/12	RMONv1
172.17.100.5	Switch	HP ProCurve Switch 2610-24-PWR	17/24	sFlow
172.17.100.6	Switch	HP ProCurve Switch 2650	18/48	RMONv1
172.17.100.7	Switch	HP ProCurve Switch 2610-24-PWR	19/24	sFlow
172.17.100.8	Switch	HP ProCurve Switch 2610-24/12-PWR	9/24	sFlow
172.17.100.9	Switch	HP ProCurve Switch 2626-PWR	14/24	RMONv1
172.17.100.10	Switch	HP ProCurve Switch 2650	15/48	RMONv1
172.17.100.11	Switch	HP ProCurve Switch 2626-PWR	15/24	RMONv1
172.17.100.12	Switch	HP ProCurve Switch 2650	32/48	RMONv1
172.17.100.13	Switch	HP ProCurve Switch 2610-24/12-PWR	17/24	sFlow
172.17.100.14	Switch	HP ProCurve Switch 2650	45/48	RMONv1
172.17.100.15	Switch	HP ProCurve Switch 2650-PWR	24/48	RMONv1
172.17.100.16	Switch	HP ProCurve Switch 2650-PWR	36/48	RMONv1
172.17.100.17	Switch	HP ProCurve Switch 2626-PWR	17/24	RMONv1
172.17.100.18	Switch	HP ProCurve Switch 2810-24G	21/24	sFlow
192.6.9.26	Access Point	Cisco AIR-WLC2125-K9	-	-
192.6.9.1-21	Access Point	Cisco AIR-AP1242AG-E-K9	-	-
192.6.8.46	Firewall	Systola SystoLAN Gateway	-	-
192.168.153.30	Switch	Nortel Networks BP2000	-	-

Tabelle 4-5: eingesetzte Netzwerkgeräte - Deutschland - Hohenwestedt

4.2 Vorbereitungen zur Messung

Um nun an zentraler Stelle einen Überblick über das Netzwerk zu erhalten, muss zum einen eine Kollektor Software ausgewählt und eingerichtet werden. Zum anderen müssen die zuvor erfassten Netzwerkgeräte so konfiguriert werden, dass diese mit dem Kollektor kommunizieren und statistische Daten senden, die der Kollektor zusammenfasst und grafisch präsentiert.

Auf Basis der Netzwerkpläne wurde eine Auswertung der eingesetzten Statistikprotokolle erstellt, um die Anforderungen an eine Analyseanwendung definieren zu können. Diese Anforderungen sind dem Kapitel 4.2.1 zu entnehmen.

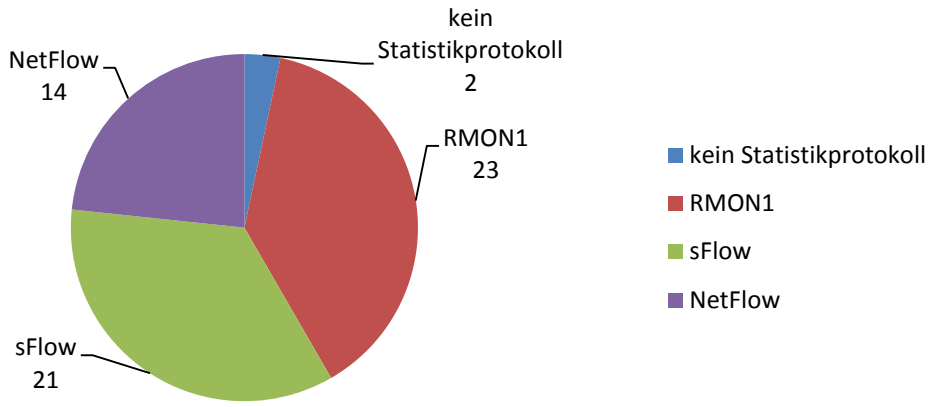

Abbildung 4-4: verwendete Statistikprotokolle

60 erkannte Netzwerkknotenpunkte wie Router, Firewalls, Switches und Gateways wurden zusammen in den 8 Standorten ermittelt, dabei wurden Accesspoints nicht betrachtet, da diese für die Anwendung eines Videokonferenzsystems eine untergeordnete Rolle spielen.

Deutlich zu erkennen ist die relativ gleichmäßige Verteilung der verfügbaren Protokolle. Hier wird deutlich, dass das Unternehmen noch keine einheitliche, für sich einsetzbare Hardware ermittelt hat. Erschwerend kommt hinzu, dass selbst bei Vereinheitlichung nicht jedes Netzwerkgerät auch im Ausland beschafft werden könnte.

4.2.1 **Softwareevaluierung und Installation**

Nach der statischen Aufnahme des Netzwerkes und unter Betrachtung der verwendeten Statistikprotokolle ergeben sich folgende Anforderungen an einen Kollektor.

- Aufnahme der Daten von SNMP mit RMON-, sFlow- und NetFlow-fähigen Geräten
- Automatische Erstellung eines Netzwerkplanes zur Überprüfung der statischen Aufnahme
- Speicherung von Daten über einen Zeitraum von 8 Stunden zwecks Erkennung von Netzwerkfehlern nachtsüber
- Erfassen von Geräteauslastungen
- Einfache und schnelle Einrichtung des Kollektors

Unter Berücksichtigung des Budgets ist für die Netzwerkanalyse eine kostenlose Version als freie Version oder eine kommerzielle Software als Testversion einer rein kostenpflichtigen Anwendung vorzuziehen. Die uneingeschränkte Laufzeit der Anwendung darf 30 Tage nicht unterschreiten.

Aufgrund von Beratergesprächen und Empfehlungen kommen mehrere Anwendungen in die nähere Auswahl.

Von der Firma Paessler wird ein Programm namens **PRTG Network Monitor** (http://www.de.paessler.com/prtg) beworben. Dieses wurde als 30 Tage Testversion in der Version 9 installiert. Es ermöglicht nicht nur die Überwachung von Netzwerkgeräten, sondern auch von Serversystemen. Dabei wird auf ein interessantes Lizenzmodell gesetzt – Es wird nicht nach Anzahl der Geräte lizensiert, sondern nach Anzahl der überwachenden Sensoren. Ein Sensor wird dabei als atomar gesehen. Soll nur ein Port eines Switches überwacht werden, so wird nur ein Sensor benötigt. Die Anzahl der benötigten Sensoren summiert sich allerdings schnell bei Netzwerkgeräten mit vielen Ports. Für das bestehende Netzwerk wäre eine Lizenz mit 2.500 Sensoren noch gerade ausreichend. Die Kosten betragen dabei 4.165,00 € brutto (Stand 05.06.2012). Die nächste größere Lizenz erlaubt eine Überwachung unbegrenzter Sensoren, die Kosten liegen dann bei 9.520,00 € brutto. Leider bietet PRTG keine Möglichkeit zum automatischen Erstellen einer Netzwerktopologie.

Die Firma Network Instruments liefert das Produkt **Observer Infrastructure** (http://www.networkinstruments.com/products/observer-infrastructure/). Auch dieses bietet eine übersichtliche Oberfläche. Die Anwendung wird konventionell nach der Anzahl von Geräten lizensiert. Da allerdings die Funktion zur Erstellung einer Netzwerktopologie des vorgestellten Netzwerkes fehlerbehaftet ist, wurde kein Angebot zur Lizensierung dieser Software eingeholt. Auch hier bietet der Hersteller eine 30 Tage Testversion an, welche wie auch PRTG Network Monitor unter Microsoft Windows 7 x86 funktioniert.

Eine freie Alternative ist das Programm **nTop** (http://www.ntop.org/), dessen Installation auf einem Linux Debian System sehr viel aufwändiger ist als bei den bereits genannten Programmen. Allerdings bietet es die Möglichkeit, über Plugins NetFlow und sFlow Datenströme aufzunehmen. Eine Kommunikation per SNMP ist nicht gegeben, daher können weder spezifische Geräteinformationen ausgelesen werden noch ist es möglich, die Statistikprotokolle der Netzwerkgeräte zentral zu konfigurieren. Verschiedene Standorte können mit einem Geo-IP Dienst auf einer Weltkarte lokalisiert werden.

Traffic Sentinel von der Firma InMon (http://www.inmon.com/products/trafficsentinel.php) bietet die Möglichkeit alle aktuellen auf dem Markt befindlichen Statistikprotokolle wie auch sFlow, NetFlow und RMON auszulesen. Die Anwendung kann zudem die sFlow- und NetFlow-Funktionen auf den entfernten Netzwerkgeräten aktivieren, so dass ein manuelles Konfigurieren dieser nicht notwendig ist. Traffic Sentinel ist daher nicht nur ein einfacher Kollektor, sondern dient gleichzeitig als SNMP-Manager. Die Netzwerktopologie kann mit Hilfe von CDP und MAC-Adressen automatisch aufgebaut werden, auch die Auslastung der einzelnen Ports ist ermittelbar. Allerdings ist der Preis dieser Anwendung mit etwa 16.000 € brutto einmalig und jährlichen Wartungskosten von etwa 3.000 € sehr hoch. Lizensiert wird über die Anzahl der Geräte, die Kosten wurden über einen Händler der Firma InMon per Angebot mitgeteilt.

sFlowTrend-Pro (http://www.inmon.com/products/sFlowTrend-Pro.php) ist die funktionsärmere Version von Traffic Sentinel. Sie bietet nur die Auswertung des sFlow Protokolls. Auch eine Erstellung des Netzwerkplanes ist nicht vorgesehen. Der Anwender kann allerdings entscheiden, wie er diese Software lizensiert. Es wird zwischen einer einmalig bezahlbaren Lizenz für 4.995 $ und einer jährlichen Lizenz für 995 $ unterschieden. Letztere muss dann vor Ablauf erneuert werden. Die unbegrenzte Anzahl von Endgeräten ist bei beiden Lizenzmodellen inbegriffen.

Tabelle 4-6 zeigt eine Übersicht aller evaluierten Produkte zur Erfassung von statistischen Daten.

Produkt	**Eigenschaften**
Paessler PRTG	+ komplexe Überwachungsmöglichkeiten + sehr übersichtlich + Unterstützung aller nötigen Statistikprotokolle - keine Erstellung der Netzwerktopologie - hoher Preis
Network Instruments Network Infrastructure	+ Überwachungsmöglichkeit für Server bzw. Dienste + Unterstützung von NetFlow - keine Unterstützung von sFlow - Fehlerhafte Erstellung der Netzwerktopologie
nTop	+ niedriger Preis - aufwändige Installation - keine SNMP-Unterstützung - sFlow und NetFlow-Unterstützung nur durch Plugins
InMon Traffic Sentinel	+ sehr übersichtlich + Unterstützung aller nötigen Statistikprotokolle + Topologie Erkennung - hoher Preis
InMon sFlowTrend-Pro	+ sehr übersichtlich + gute sFlow-Überwachung + niedriger Preis - keine Unterstützung weiterer Statistikprotokolle - keine Anzeige der Netzwerktopologie

Tabelle 4-6: Vergleich von Statistikanwendungen

Zwei weitere Softwarelösungen, welche nicht weiter betrachtet, aber erwähnt werden sollten, sind das frei verfügbare Nagios sowie das kommerzielle Splunk. Beide bieten eine Vielzahl von Überwachungsmöglichkeiten auf Server, Client und Netzwerkebene. Allerdings ist der Konfigurationsbedarf beider Lösungen über Addins und Skripte so groß, dass eine Evaluierung und Nutzung im Rahmen dieser Arbeit nicht möglich gewesen wäre.

Bedingt durch den großen Funktionsumfang von InMon Traffic Sentinel und der Möglichkeit, dieses uneingeschränkt 30 Tage lang zu testen, wurde eine Evaluierungslizenz auf einem dedizierten Cent-OS 6 Server eingerichtet. Dieser ist mit 2 CPUs und 4 GB RAM sowie 120 GB HDD ausreichend bemessen. Für größere Netzwerke empfiehlt InMon einen leistungsstärkeren Server.

4.2.2 Konfiguration der Netzwerkgeräte

Wie bereits beschrieben bietet InMon Traffic Sentinel die Möglichkeit, Netzwerkgeräte als SNMP-Manger so einzurichten, dass Daten gesammelt werden können. Allerdings muss der Zugriff auf SNMP freigegeben sein.

Hier unterscheidet man wieder zwischen den Befehlen für HP- und Cisco-Geräte.

Hersteller	**Befehl**
Hewlett-Packard	`snmp-server community [Passwort] unrestricted`
Cisco Systems	`snmp-server community [Passwort] rw`

Tabelle 4-7: Befehle zum Aktivieren des Zugriffs auf SNMP

Diese erlauben uneingeschränkten Zugriff auf das jeweilige Gerät. Das Passwort sollte in unsicheren Umgebungen überlegt gewählt werden. Die Standardeinstellungen sehen den Wert *public* vor.

Zusätzlich zum Aktivieren des SNMP-Servers sollten für einen fehlerfreien Betrieb die Kontaktdaten sowie der Standort des Gerätes angegeben werden. Die Befehle sind bei den aufgeführten Gerätearten identisch.

	Befehl
Kontakt	`snmp-server contact [Kontaktdaten]`
Standort	`snmp-server location [Standort]`

Tabelle 4-8: Zusätzliche Befehle zur Konfiguration von SNMP

Sollte eine Konfiguration von sFlow oder NetFlow vom Kollektor nicht unterstützt werden, so können diese Funktionen auch manuell aktiviert und eingerichtet werden. Erforderliche Informationen sind die Netzwerkadresse des Kollektors sowie der Port, auf welchem Daten zur Auswertung entgegengenommen werden können. Bei der Anwendung InMon Traffic Sentinel sind dies der Port 9985 für NetFlow- sowie Port 6343 für sFlow-Daten.

sFlow	**Befehl**
Aktivierung	`sflow 1 destination [IP] [Port]`
Sampling Intervall	`sflow 1 sampling ethernet [Interface] [Intervall]`
Polling Intervall	`sflow 1 polling ethernet [Interface] [Polling Rate in Sekunden]`

Tabelle 4-9: Befehle zum Aktivieren von sFlow

Falls diese Befehle nicht zur Verfügung stehen sollten, muss die Konfiguration über `setMIB` erfolgen. Nähere Informationen sind im Handbuch des jeweiligen Gerätes zu finden.

NetFlow	**Befehl**
Ziel	`ip flow-export destination [IP] [Port]`
Version	`ip flow-export version [1, 5, 7, 9]`
Interface	`interface [Interface Name]`
Aktivierung NetFlow	`ip route-cache flow`
Protokollierung ausgehend	`ip flow egress`
Protokollierung eingehend	`ip flow ingress`

Tabelle 4-10: Befehle zum Aktivieren von NetFlow

InMon Traffic Sentinel unterstützt die Versionen 1, 5, 7 und 9 des NetFlow-Protokolls. Version 9 ist der offene Standard wie in Kapitel 2.1.5 beschrieben.

4.3 Auswertung

In diesem Kapitel werden die Netzwerke der Standorte Hamburg und Hohenwestedt näher betrachtet. Wie bereits in Kapitel 4.1 beschrieben, kommt eine interne Analyse der weiteren Standorte nicht in Betracht, allerdings wird die Kommunikation zwischen den einzelnen Netzwerken ermittelt.

Ein Hinzufügen der Netzwerkgeräte des Standortes Hamburg in Traffic Sentinel liefert eine automatisch generierte Topologie des Netzwerkes, welche in Abbildung 4-5 gezeigt wird. Diese entspricht der Topologie, die in Kapitel 4.1.2 beschrieben wurde.

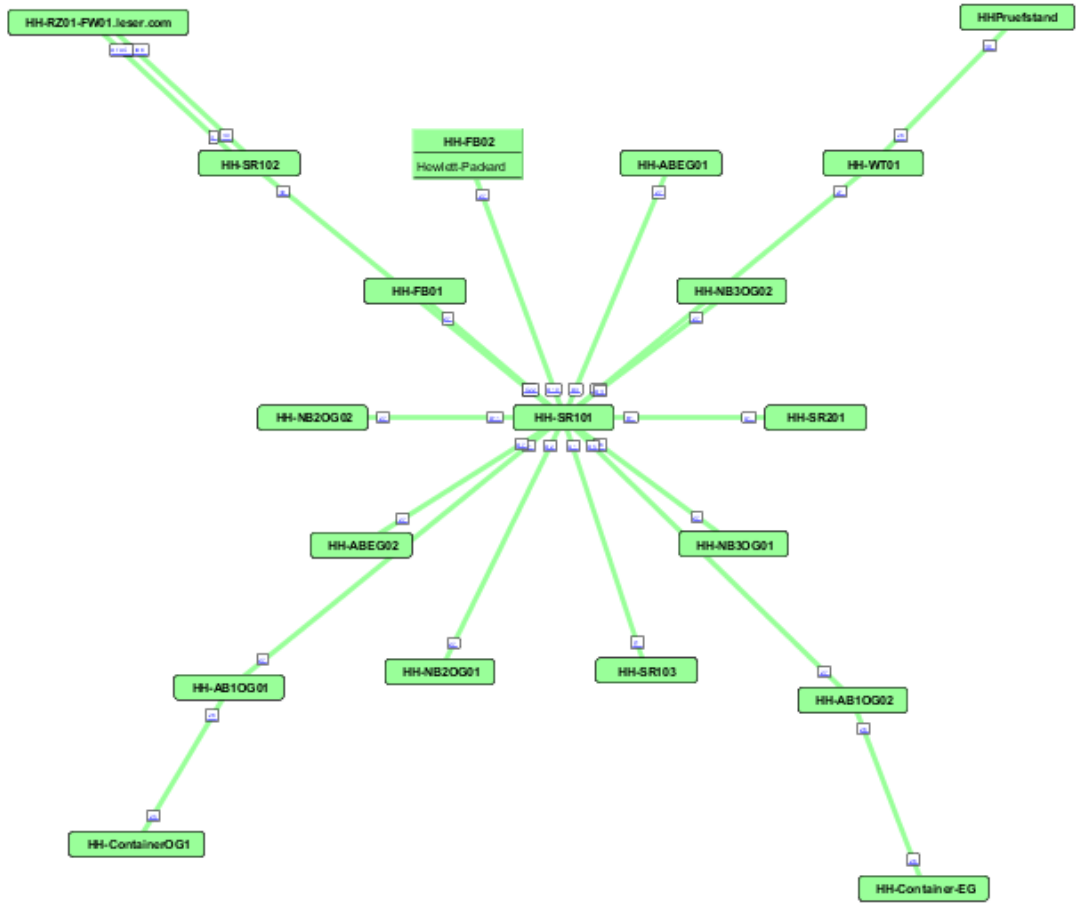

Abbildung 4-5: automatisch generierte Topologie des Standortes Hamburg

4.3.1 **Latenz zwischen Standorten**

Die Latenz gibt die Laufzeit eines Paketes zwischen dem Senden und dem Empfangen an. Bei Telefonie und Videotelefonie ist eine möglichst geringe Verzögerung für die Gesprächsteilnehmer angenehmer, damit die Gesprächspausen nicht zu lang erscheinen. Die *International Telecommunication Union* empfiehlt eine maximale Paketlaufzeit von 400 ms pro Strecke (ITU G.114), damit Gespräche nicht als störend empfunden werden. Das entspricht einer *Round Trip Time (RTT)* von 800 ms, sofern die gleiche Route für das Übertragen der jeweiligen Pakete benutzt wird.

Über 5 Tage hinweg wurden stündlich die Laufzeiten von Paketen gemessen. Hier wird zwischen der Laufzeit im IPSec-Tunnel und der Laufzeit ohne Tunnel über die externe IP-Adresse unterschieden. Stichproben haben gezeigt, dass sich die Laufzeiten der Pakete im Tunnel um maximal 3 ms erhöhen. Diese Differenz liegt im Rahmen von Messungenauigkeiten, eine Unterscheidung wird daher nicht in Betracht gezogen. Da die Standorte im Ausland nur über eine Verbindung zum Internet verfügen, über die dieser Tunnel aufgebaut wird, ist dieser Wert als „erwartet“ zu bezeichnen.

Betrachtet man das globale Unternehmensnetzwerk als vollständigen Graphen K_8, so ergibt sich eine Anzahl von $\frac{n*(n-1)}{2} = \frac{8*(8-1)}{2} = 28$ möglichen Verbindungen bei 8 Standorten (vgl. Diestel 2010). Die Paketumlaufzeiten (RTT) über das Internet sind gemittelt in Tabelle 4-11 dargestellt.

	Rio de Janeiro 200.201.148.146	Manama 217.17.237.42	Singapur 202.55.94.18	Paithan 110.234.248.49	Mumbai 110.234.102.218	Charlotte 74.223.225.226	Hohenwestedt 87.139.22.153
Hamburg 213.39.250.58	269	272	291	213	146	122	64 10[1)]
Hohenwestedt 87.139.22.153	315	360	332	301	223	167	
Charlotte 74.223.225.226	147	249	252	290	263		
Mumbai 110.234.102.218	402	421	70	12 13[1)]			
Paithan 110.234.248.49	463	418	97				
Singapur 202.55.94.18	392	212					
Manama 217.17.237.42	375						

Tabelle 4-11: gemessene Umlaufzeiten zwischen den Standorten über das Internet (in ms)

Die mit [1)] gekennzeichneten Werte repräsentieren die Laufzeit über die Standleitungen der betroffenen Standorte.

Hervorzuheben sind die Messungen am Standort Manama. Dort variieren die Verzögerungszeiten zu anderen Standorten stark. Abbildung 4-6 zeigt die Umlaufzeiten zwischen den Standorten Manama und Singapur zwischen dem 10.06.2012 und dem 11.06.2012. Messungen zwischen Manama und den weiteren Standorten auch an anderen Tagen zeigten das gleiche Verhalten. Ein stabiler Betrieb eines Videokonferenzsystems ist hier nicht gegeben.

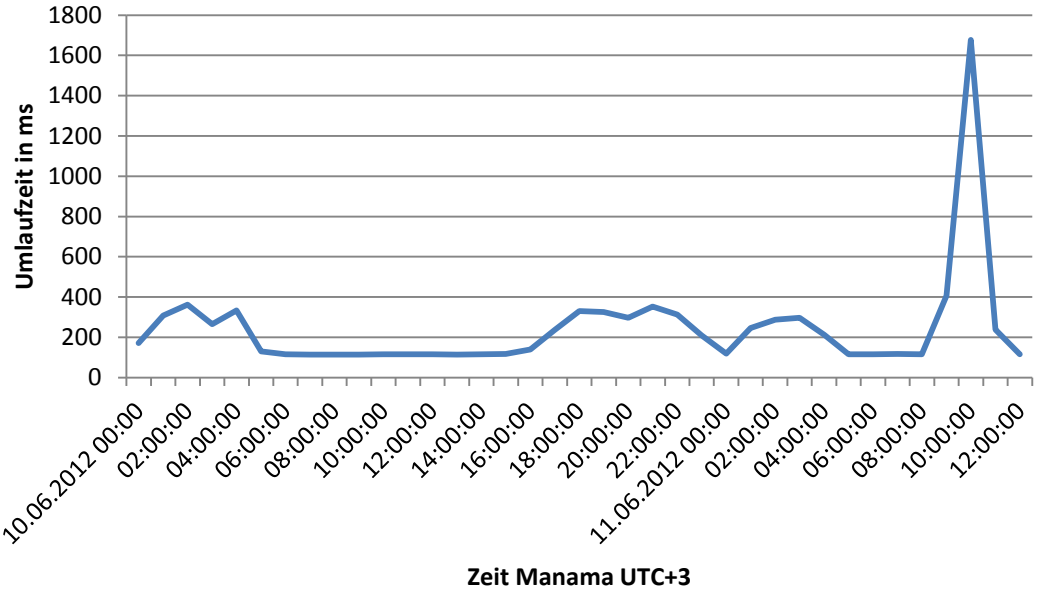

Abbildung 4-6: Umlaufzeiten Manama - Singapur

Alle Standorte, ausgenommen Manama, zeigen ein stabiles Verhalten der Paketverzögerung.

Die dargestellten Ergebnisse sind zufriedenstellend. Ob Messwerte größer als 800 ms tatsächlich für eine Verschlechterung der Kommunikationsqualität sorgen, muss sich durch Tests im Kapitel 5.3 zeigen.

4.3.2 Maximale Datenübertragungsrate der Standorte zum Internet

Um die verfügbare Übertragungsrate der einzelnen Standorte zum Internet zu ermitteln, wird eine knapp 20 MB große Datei per FTP übertragen. Das Protokoll zeichnet sich durch den sehr geringen Overhead aus, so dass die Transferrate für Nutzdaten nicht eingeschränkt wird.

Für den Test ist es wichtig, dass der FTP-Server keinesfalls die Ergebnisse durch zu geringe Transferraten verfälscht. Daher wurde ein dedizierter FTP-Server gewählt, welcher in einem Rechenzentrum im Raum Nürnberg untergebracht ist. Dieser ist direkt an das DE-CIX Backbone angeschlossen.

Des Weiteren sollten in einem internationalen Unternehmen die verschiedenen Zeitzonen der Standorte beachtet werden. Da die maximale Datenübertragungsrate ermittelt werden soll, werden die entsprechenden Tests zwischen 22.00 Uhr und 04.00 Uhr durchgeführt. Als Vergleich dient ein Test bei Tag, um realistische Werte während des Betriebs zu erhalten.

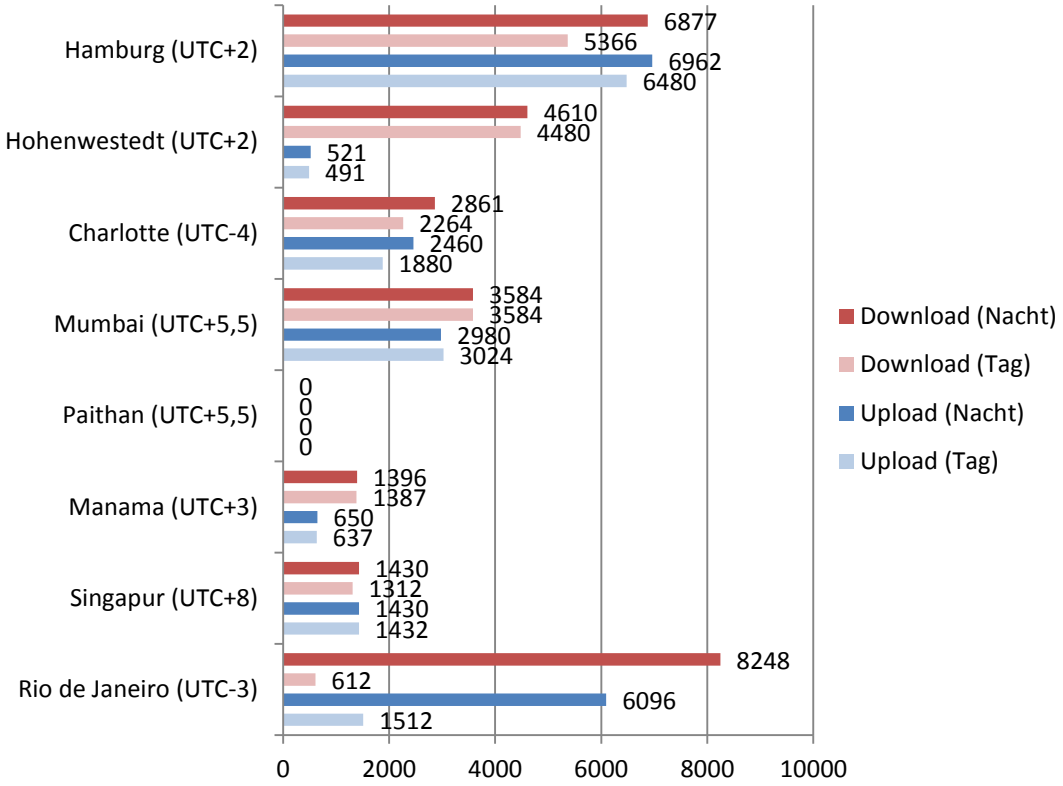

Abbildung 4-7: maximale benutzbare Transferrate der Standorte (in kbit/s)

Am Standort Paithan war zwar die Nutzung des FTP-Steuerkanals auf Port 21 möglich, allerdings wurde der Datenkanal auf Port 20 blockiert. Über das HTTP-Protokoll war es zudem nicht möglich, Dateien mit mehr als 1 MB Größe zu übertragen. Dieses Verhalten deutet auf eine restriktiv arbeitende Firewall oder auf einen fehlerhaft konfigurierten Gateway hin. Messungen zur Transferrate konnten daher an dieser Stelle nicht stattfinden und müssen nach Problembehebung durchgeführt werden.

In Zukunft werden die Transferraten weiter steigen, jedoch hat dies keinen Vorteil, solange diese nicht stabil bleiben. Gerade beim Standort in Brasilien sind extreme Schwankungen der nutzbaren Übertragungsrate zu erkennen. Auch nach weiteren Übertragungen änderte sich dieses Ergebnis nicht. Die Vermutung liegt hier nahe, dass sich mehrere Endbenutzer diese Transferleistung teilen.

Alle weiteren Messergebnisse sind zeigen keine Auffälligkeiten und können als realistisch angesehen werden.

Zwar wurden nun die maximal möglichen Datenübertragungsraten stichprobenartig ermittelt, allerdings ist die Auslastung über den Tag noch unbekannt. Mit Hilfe der evaluierten Statistiksoftware wird diese in Kapitel 4.3.3 ermittelt.

4.3.3 Durchschnittliche Datenübertragungsrate der Standorte

Traffic Sentinel protokolliert nach dem Konfigurieren der Netzwerkgeräte nun die Flussdaten zwischen den einzelnen Clients und die Auslastungen aller einzelnen Interfaces der letzten 6 Stunden.

Der folgende Befehl zeigt eine Übersicht aller Interfaces mit den zugeordneten IP-Adressen auf dem Router.

```
show ip interface brief
```

Im Anhang A dieser Arbeit befinden sich die Zuordnungen der genutzten Interfaces.

Exemplarisch wird nachfolgend die Auslastung des virtuellen Interfaces HANSENET, welches die Schnittstelle zum Internet darstellt, auf der Firewall am Standort Hamburg gezeigt. Gut zu erkennen ist der Anstieg des Datenverkehrs um etwa 12:00 Uhr, welcher dann bis 13:00 Uhr wieder stark abnimmt. In dieser Zeit ist den Mitarbeitern gestattet privat auf das Internet zuzugreifen.

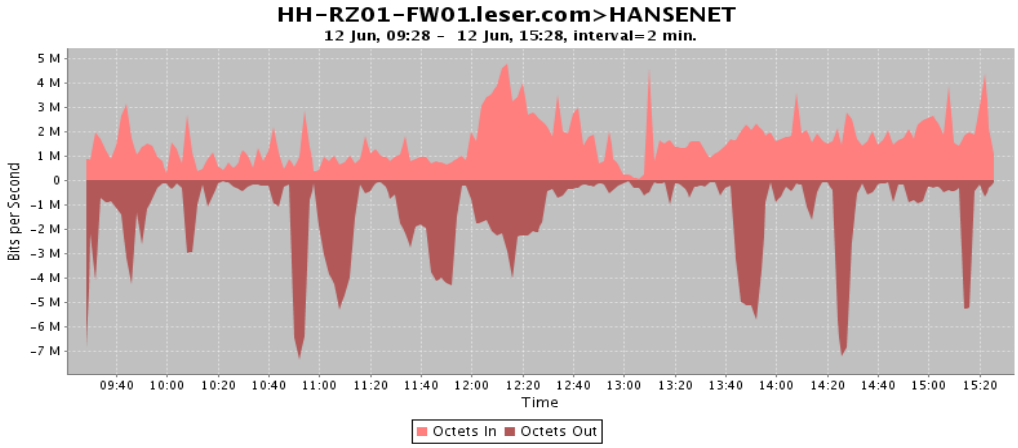

Abbildung 4-8: Beispielhafte Auslastung des Interfaces

Abbildung 4-8 zeigt die Auslastungen aller relevanten Interfaces der einzelnen Standorte. Die Auslastungen wurden über 5 Tage mit Hilfe von Traffic Sentinel beobachtet und ein Mittelwert gebildet. Abbildung 4-9 zeigt die während der täglichen Arbeitszeit genutzten Transferraten der Mitarbeiter bzw. Maschinen.

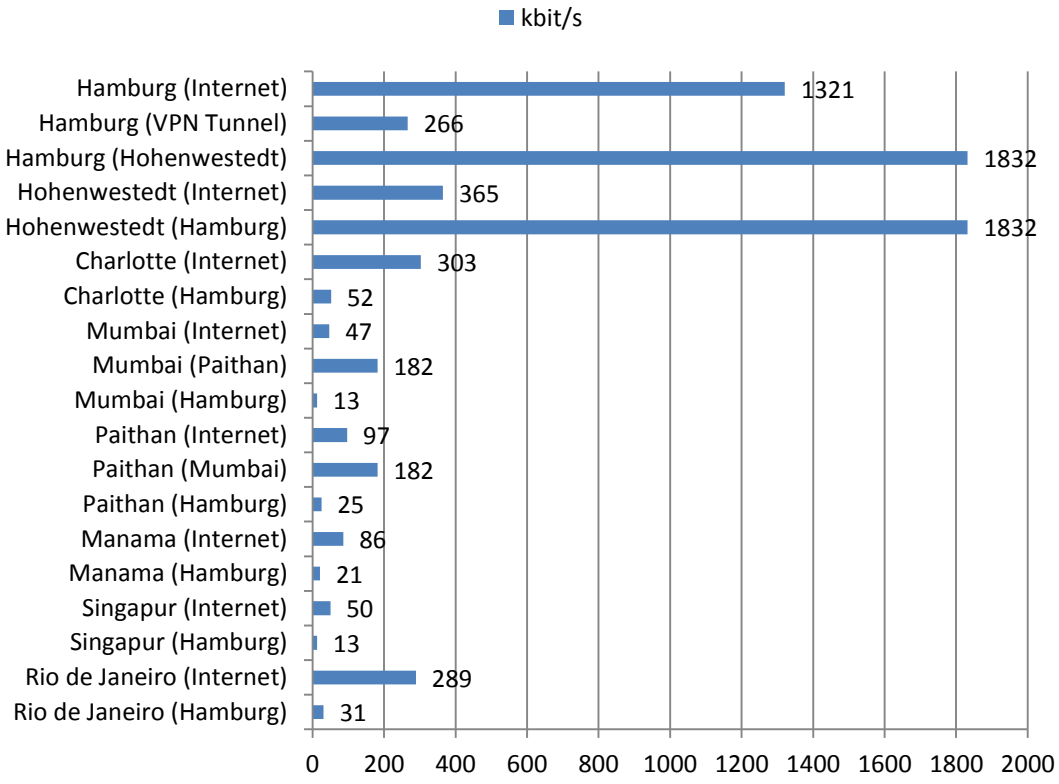

Abbildung 4-9: durchschnittliche synchrone Auslastung zwischen 8:00-18:00 Uhr lokaler Ortszeit

4.3.4 **Drop-/Error-Rates**

Durch die Statistiksoftware fiel ein nicht nachvollziehbares Verhalten auf. Während der Sicherung der SAP-Systeme wurden vermehrt Paketverwerfungen (Discards) und Paketfehler (Errors) an Traffic Sentinel gemeldet.

Es zeigte sich, dass die Pakete zwischen den Backbones 172.16.100.1 und 172.16.100.2 auch an alle anderen Switches am Standort Hamburg weitergeleitet wurden und Ausfälle der betroffenen Geräte verursachten. Lastspitzen von etwa 4,5 GBit/s waren zur gleichen Zeit auf allen Switches erkennbar.

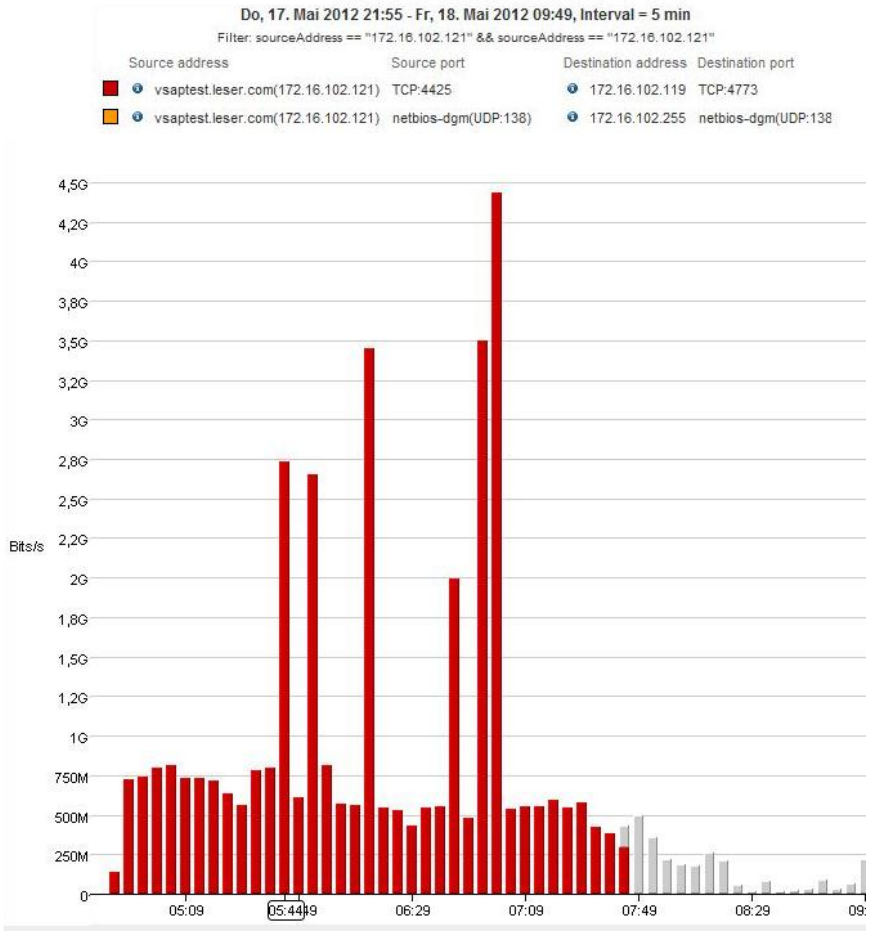

Abbildung 4-10: Lastspitzen

In weiteren Tests zeigte sich, dass die Funktion „Spanning-Tree“, welche für das Erkennen von Zyklen und mehreren Verbindungen zwischen Knotenpunkten zuständig ist, für dieses Verhalten verantwortlich war. Auf den entsprechenden Geräten wurde das RST-Protokoll erzwungen, obwohl es scheinbar nicht von allen Geräten im Netzwerk unterstützt wurde.

Nach dem Konfigurieren des Standard Spanning Tree Modus trat dieses Verhalten nicht mehr auf.

4.3.5 **VLAN und QoS**

Wie bereits beschrieben ist es wichtig, Pakete für echtzeitkritische Anwendungen wie IP-Telefonie und Videoübertragungen zu priorisieren.

Da das Unternehmen seit längerer Zeit die Vorteile der IP-Telefonie nutzt, wurden auch bereits entsprechende VLANs und Priorisierungen erstellt.

VLAN Kennung	Name	Bezeichnung
1	DEFAULT_VLAN	-
10	HANSENET	Internet
11	DTAG	Internet
100	Management	Management VLAN
104	VoIP	IP-Telefonie
108	Clients	Standard VLAN
112	Guests	Eingeschränktes Gäste VLAN
116	<reserviert>	<externes Systemhaus>
900	XFER	Tunnel für Standorte

Tabelle 4-12: VLAN-Kennungen

Tabelle 4-12 zeigt, dass firmenfremde PCs (VLAN 112 - Guests) bereits aus dem Hauptnetzwerk ausgeschlossen werden. Sie erhalten direkt beim Rechnerstart eine IP-Adresse aus einem separierten Bereich. Firmenfremde PCs werden über die nicht eingetragene MAC-Adresse auf einem RADIUS-Server erkannt. Zusätzlich dienen Zertifikate sowie die 802.1X Authentifizierung dazu, dass diese Clients keine Möglichkeit haben, dem Firmennetzwerk beizutreten. Den Gästen wird somit nur der Zugriff auf das Internet gewährt.

Ein weiteres Beispiel zeigt das VLAN mit der Kennung 104. Hier werden bereits vorhandene IP-Telefone in ein anderes virtuelles Netzwerk überführt, das eine höhere Datenpriorität erhält. So werden Telefongespräche bei einem hohen Datenverkehr nicht gestört.

Die Prioritätsstufe wurde nicht, wie nach IEEE empfohlen, auf 5 (Sprache) gesetzt, sondern auf 6 (Netzwerksteuerung) (vgl. IEEE802.1Q 2005, S. 279-280). Auch für das noch zu

wählende Videokonferenzsystem sollte, um den Jitter und die Übertragungsverzögerung so gering wie möglich zu halten, ein VLAN erstellt und QoS aktiviert und konfiguriert werden.

Die VLANs 10, 11 und 900 sind nur auf den Geräten in Hamburg zu finden. Die VLANs 10 und 11 sind den beiden Internetanschlüssen zugeordnet, um Routen trennen zu können. Dadurch, dass die Internetverbindungsgeräte der beiden Internet Service Provider (ISP) in Hamburg mangels ausreichender Interfaces nicht physikalisch an der Cisco ASA (10.49.225.5), sondern am HP-Switch 172.16.100.4 angeschlossen sind, wird das VLAN 900 benötigt, um den internen Datenverkehr vom externen Datenverkehr zu trennen. Das VLAN ist daher nur auf den beiden genannten Geräten zu finden.

4.3.6 **IP-Bereiche und VPN**

Das Unternehmensnetzwerk hat eine Vielzahl von genutzten IP-Adressbereichen, die im Folgenden übersichtshalber dargestellt werden.

Standort	**Bereich (intern)**	**Bereich (extern)**
Hamburg	172.16.100-112.0 / 255.255.255.0 192.6.12.0 / 255.255.252.0 10.49.255.0 / 255.255.255.0	213.39.250.58 (Internet) 212.184.86.235 (VPN)
Hohenwestedt	172.17.100-112.0 / 255.255.255.0 192.6.8.0 / 255.255.252.0 10.49.254.0 / 255.255.255.0	87.139.22.153
Charlotte	192.168.50.0 / 255.255.255.0	74.223.225.226 / 255.255.255.254
Mumbai	192.168.10.0 / 255.255.255.0	110.234.102.218 / 255.255.255.240
Paithan	192.168.20.0 / 255.255.255.0	110.234.248.49 / 255.255.255.240
Rio de Janeiro	192.168.64.0 / 255.255.255.0	200.201.148.146
Singapur	192.168.55.0 / 255.255.255.0	202.55.94.18
Manama	192.168.53.0 / 255.255.255.0	217.17.237.42

Tabelle 4-13: verwendete IP-Adressbereiche

Deutlich zu sehen ist die Benutzung eines nicht privaten Netzwerkbereiches in Hamburg und Hohenwestedt sowie die Menge der verwendeten Bereiche.

Das Netzwerkprotokoll IPv6 wird im Unternehmen nicht verwendet. Aufgrund der geringen Anzahl von IP-fähigen Geräten (max. 2000) ist dies intern aber auch nicht notwendig. Eine externe Verwendung wird wahrscheinlich in den nächsten Jahren stattfinden, wenn die IPv4-Adressräume erschöpft sind und weitere Standorte gegründet und angebunden werden sollen. Die Protokolle IPv4 und IPv6 können parallel betrieben werden, so dass kein abrupter Wechsel erfolgen muss. Sogenannte *IPv4-mapped IPv6* IP-Adressen ermöglichen die Zuordnung einer bisherigen v4 Adresse in das neue Format des IPv6 Protokolls, außerdem ist es möglich, IPv4 und IPv6 zu tunneln (vgl. Zisler 2012, S. 99-100).

Falls Mitarbeiter des Unternehmens auf Reisen sind, so verbinden sie sich mit Hilfe des PPTP-Protokolls zum jeweiligen Heimatstandort. Über dieses VPN erhalten sie Zugriff auf das Netzwerk der Firma.

Eine Alternative bzw. eine Erweiterung dazu, bietet *Mobile IP*. Es ermöglicht das Innehalten der IP-Adresse eines mobilen Gerätes, egal in welchem (Fremd-) Netzwerk es sich befindet (vgl. Schiller 2003, S. 307.ff). Es kann so jederzeit von externen Geräten adressiert werden. Eine Vereinfachung bietet *Mobile IPv6*, welches nach RFC 6275 spezifiziert ist - dort ist es möglich, auf einen *Foreign Agent* in einem Fremdnetzwerk zu verzichten (vgl. Solimann 2004). Die Funktionsweise von *Mobile IP* und IPv6 ist allerdings nicht Bestandteil dieser Arbeit, so dass nur Literaturhinweise gegeben werden.

4.4 Bewertung und Empfehlung zur Verbesserung

Wie gezeigt wurde ist für die Einführung eines neuen Systems die Aufnahme der bereits vorhandenen Struktur durchaus von Vorteil. Durch die Analyse des Netzwerkes wurden Schwachstellen offenbart, die nicht nur generell, sondern auch speziell bei der Integration des Videokonferenzsystems zu Problemen führen könnten.

Übertragungsraten und Latenzen

Die Messung der Übertragungsrate verdeutlicht insbesondere im Bereich Rio de Janeiro, dass die maximal erreichbaren Datenraten sehr gering sind. Auch am Standort Hohenwestedt zeigt die Messung die niedrige mögliche Uploadgeschwindigkeit von Dateien. Hier sollte darauf geachtet werden, dass der Datenverkehr bei einer Systemintegration zwingend über die Standleitung zum Standort Hamburg geleitet wird. Die Auslastung dieser Verbindung beträgt im Mittel etwa 18 % von möglichen 10 Mbit/s.

Wie beschrieben sollten die Paketlaufzeiten 400 ms nicht übersteigen, die Messungen über den angegebenen Zeitraum zeigen allerdings, dass diese Empfehlung nur teilweise eingehalten werden kann. Gerade die instabile Verbindung am Standort Manama scheint für einen reibungslosen Betrieb nicht geeignet zu sein.

Bei einem weiteren Wachstum des Unternehmens sollten MPLS-Verbindungen zwischen den Standorten in Betracht gezogen werden, da diese eine garantierte Datenübertragungsrate gewährleisten. Ein MPLS-Provider kann seine Routen bewerten und die besten für den vorgesehenen Betrieb auswählen, so dass sich kürzere Paketlaufzeiten ergeben. Gerade für den Einsatz von Sprach- und Videoübertragung ist dies ein wichtiger Faktor. Die Funktionsweise von MPLS wird in Balakrishnan 2008 und Borowka 2002 beschrieben.

Für einen Betrieb sollte ein global agierender MPLS-Anbieter gewählt werden, der alle Standorte des Unternehmens anbinden kann. Dies hat den Vorteil, dass der Ansprechpartner bei Verbindungsproblemen klar definiert ist.

IP-Adressen

Durch das stetige Wachstum der IT-Infrastruktur entstanden nicht nur sehr viele IP-Adressbereiche, sondern auch solche, die keinen privaten Adressbereich abdecken. An den Standorten Hamburg und Hohenwestedt, welche die IP-Adressbereiche 192.6.11.0/22 sowie 192.6.8.0/22 benutzen, sollte daher nicht nur für die Einführung eines Konferenzsystems, sondern auch grundsätzlich die Nutzung des IP-Adressbereichs überdacht werden. Neue Netzwerkgeräte wurden im Bereich 172.16.0.0/12 angelegt und das Routing für die IP-Adressbereiche aktiviert. Allerdings wird der Umzug aller Netzwerkgeräte auf einen gültigen Bereich noch mehrere Monate in Anspruch nehmen. Eine Vereinheitlichung würde gerade für das Erkennen der Netzwerktopologie zu Vereinfachungen führen, auch müssten keine Routingaufgaben geleistet werden, was zu Geschwindigkeitsvorteilen führen kann.

Eine Adressumstellung auf IPv6 wird wahrscheinlich in den nächsten Jahren erforderlich sein. Aufgrund des großen Themenbereichs von (M)IPv6 erscheint eine weitere Analyse in Hinblick auf die Sicherheit, die eingesetzte Hardware und die IPv6-Kompatibilität sinnvoll, damit dann eine Strategie zur Umstellung erarbeitet werden kann. Die Zuordnung zwischen IPv4 und IPv6, wie in Kapitel 4.3.6 beschrieben, erleichtert immerhin eine Migration.

Statistiksoftware

Während der Ermittlung der Daten über das SNMP- und das NetFlow-Protokoll kam es zu Verbindungsabbrüchen zu den Standorten Rio de Janeiro und Singapur. Wie in Kapitel 2.1.5 angedeutet kann gerade NetFlow erhöhte Datenmengen erzeugen und bei schwachen Verbindungen solche Trennungen verursachen. Die Tests zeigen, dass diese Protokolle, insbesondere das *Polling,* nur dann genutzt werden sollten, wenn es tatsächlich notwendig ist. Die Netzwerküberwachung in den Standorten Hamburg und Hohenwestedt bleibt über den Zeitraum dieser Arbeit aktiv. Die Überwachung der externen Knotenpunkte wurde direkt nach der Datenerfassung deaktiviert.

Mehr durch Zufall als durch konkretes Wissen über einen Fehler wurden Probleme von Netzwerkausfällen in der Nacht bei der Datensicherung bekannt. Diese konnten auf eine Inkompatibilität zwischen den Spanning Tree Versionen zurückgeführt werden. Der Einsatz einer solchen Überwachungssoftware, die nicht nur die Verfügbarkeit, sondern auch die Flussdaten ermittelt, macht sich gerade in größeren Unternehmen mit vielen Knotenpunkten bezahlt. Sie gibt einen Überblick über die Netzwerktopologie, die eingesetzte Hardware und zeigt mit kurzer Verzögerung die aktuellen Transferraten an.

5 Auswahl eines Videokonferenzsystems

In den vorangegangenen Kapiteln wurden die Anforderungen an ein Videokonferenzsystem definiert, die Grundlagen beschrieben und die Analyse des bisher eingesetzten Netzwerkes im Unternehmen durchgeführt. Dieses Kapitel beschreibt nun die Ermittlung eines geeigneten Videokonferenzsystems, welches den Anforderungen entspricht und sich in die Netzwerkinfrastruktur integrieren lässt.

In Kapitel 5.1 werden Anbieter bzw. deren Produkte aufgeführt und verglichen. Das darauf folgende Kapitel 5.2 gibt einen Überblick über die Kosten eines Systems und stellt die Reisekosten von Mitarbeitern als Kosten-Nutzen-Analyse in Abhängigkeit dar.

In Kapitel 5.3 und 5.4 werden die Systeme im Rahmen des Möglichen evaluiert. Kapitel 5.5 liefert Informationen zur Bedienung und Administration des Systems. Nach Abschluss der Tests werden in Kapitel 5.6 die vorgestellten Systeme bewertet und eine Empfehlung gegeben.

5.1 Marktanalyse

Aufgrund des hohen Umfangs werden im Rahmen dieser Arbeit nur drei Anbieter von Videokonferenzsystemen betrachtet. Ausschlaggebend für diese Auswahl war zum einen die Präsenz der Anbieter im Internet, zum anderen die Empfehlungen von Gartner 2011. Die Hersteller sind auf dem internationalen Markt schon seit mehreren Jahren etabliert und gefestigt – dies ist ein Indiz für eine gewisse Produktzuverlässigkeit und erleichtert auch eine mögliche Beschaffung der Produkte im Ausland.

Die Produkte der Unternehmen **Polycom** (http://www.polycom.de/), **Logitech LifeSize** (http://www.lifesize.com/), sowie **Cisco Systems / Tandberg** (http://www.cisco.com/) werden in den nachfolgenden Kapiteln beschrieben und in Kapitel 5.1.1 verglichen. Die vorgestellten Systeme beherrschen den Verbindungsaufbau über SIP bzw. H.323 und sind somit untereinander kompatibel.

Weitere Anbieter sind neben Radvision (http://www.radvision.com/), Emblaze-Vcon (http://www.vcon.com/) und CeeLab (http://ceelab.com/) auch Vidyo (http://www.vidyo.com/) und StarLeaf (http://www.starleaf.com/).

In Kapitel 5.1.2 wird ein Ausblick auf Schulungssysteme gegeben, die die gestellten Anforderungen in Kapitel 3.1 zwar nur zum Teil erfüllen, als Alternative für

Produktpräsentationen oder zum Schulen von Mitarbeitern aber dennoch in Frage kommen könnten.

Da das Unternehmen vermehrt die VoIP-Software Skype für den Austausch von Dokumenten sowie die videogestützte Kommunikation nutzt, wird diese Anwendung näher in Kapitel 5.1.3 erläutert.

5.1.1 **Vergleich der Systeme**

In den folgenden Tabellen werden die angebotenen Raumlösungen der Hersteller über Ihre Leistungsdaten verglichen. Die Daten wurden DEKOM 2012 und den Produktdatenblättern entnommen.

Tabelle 5-1 zeigt die Leistungswerte in Bezug auf die Videoqualität.

	LifeSize			**Polycom**			**Cisco Systems**		
Produkt	Express 220	Team 220	Room 220	HDX 7000-1080	HDX 7000-1080 MP	HDX 8000-1080 MP	C20	C40	C60
Max. Videoauflösung	1920 x 1080			1920 x 1080			1920 x 1080		
Max. mögliche Auflösungen	200+			9			13		
Max. Screen Sharing Auflösung	1920 X 1080			1280 X 720			1280 X 768		1600 x 1200
Dualsteam 720p30	Ja			Nein			Ja		
Minimaldatenrate 720p30	768 kbit/s			1728 kbit/s			1152 kbit/s		
Minimaldatenrate 720p60	1100 kbit/s			2048 kbit/s			2200 kbit/s		
Minimaldatenrate 1080p60	1700 kbit/s			2500 kbit/s			2500 kbit/s		
Kamerazoom (optisch)	10x			12x			4x	12x	12x
Packet Recovery	Ja			Ja			Ja		

Tabelle 5-1: Leistungsdatenvergleich der Videokonferenzlösungen (Video)

Gerade in Bereich der nötigen Datenrate setzt sich die Firma LifeSize mit Ihren Produkten klar von der Konkurrenz ab. Hier sollte man allerdings beachten, dass diese Werte Herstellerangaben sind. In Kapitel 5.4 werden die angegebenen Transferraten in einem gesonderten Testsystem auf Plausibilität überprüft.

Alle Raumsysteme beherrschen Screen-Sharing, mit dem es möglich ist Dokumente bzw. Bildschirminhalte von einem Endgerät wie Notebook oder PC seinen Gesprächsteilnehmern zu zeigen. Dazu wird ein zweiter Datenstream (Dualstream 720p30) erstellt, der für die Übertragung der externen Inhalte zuständig ist. Die Abbildung 2-2 zeigt einen typischen Dualstream-Betrieb.

Der Begriff „Packet Recovery“ bezeichnet die Erkennung von verlorenen Paketen, die aufgrund von zu hohen Auflösungen und zu geringer Transferleistung nicht beim Teilnehmer eintreffen können. Alle Systeme können die Auflösungen dynamisch anpassen, um bestmögliche Übertragungen auch bei geringen Übertragungsraten erreichen zu können. Je höher die maximal möglichen Auflösungsabstufungen, desto feingranularer kann das Bild der Datenrate angepasst werden.

Die nachfolgende Tabelle 5-2 präsentiert die Leistungswerte in Bezug auf die Audioqualität.

	LifeSize			**Polycom**			**Cisco Systems**		
Produkt	Expr. 220	Team 220	Room 220	HDX 7000-1080	HDX 7000-1080 MP	HDX 8000-1080 MP	C20	C40	C60
Frequenz	16 kHz			22 kHz (nur zwischen HDX Systemen)			20 kHz		
AAC Standardkonform	Ja			Nein			Ja		
Stereo	Nein			Ja			Ja		
Rauschunterdrückung	Ja			Ja			Ja		
Echocancelling	Ja			Ja			beschr.	Ja	
Störquellenunterdrückung	Ja			Nein			Nein		
Maximalabstand Mikrofon	450 cm			200 cm			250 cm		
Mikrofonlösung	16er Insel			Single			Single		
Stummstelltaste am Mikrofon	Ja			Ja			Ja	Nein	

Tabelle 5-2: Leistungsdatenvergleich der Videokonferenzlösungen (Audio)

Tabelle 5-3 stellt die Leistungsdaten im Betrieb mit mehreren Teilnehmern dar. Sie gibt Auskunft über die zu erreichenden Auflösungen sowie die Anzahl der maximal möglichen Teilnehmer über die integrierte MCU.

	LifeSize			**Polycom**			**Cisco Systems**		
Produkt	Express 220	Team 220	Room 220	HDX 7000-1080	HDX 7000-1080 MP	HDX 8000-1080 MP	C20	C40	C60
Maximal nutzbare Datenrate (in Mbit/s)	4	6	10	2	4	6	4	6	10
Integrierte MCU	Nein	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja
Auflösung bei Mehrpunktkonferenzen	-	1920 x 1080		-	702 x 576	1280 x 720	-	1024 x 576	1280 x 720
Maximale Teilnehmeranzahl	1	4	8	1	4	4	1	4	4
Speedmatching	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Ja	Ja

Tabelle 5-3: Multipointfähigkeit

Speedmatching ist eine Technologie zur Erkennung und Anpassung von verschiedenen Auflösungen der einzelnen Teilnehmer, um höchstmögliche Video- und Audioqualität zu erreichen.

Positiv hervorzuheben ist, dass die vorgestellten Systeme durch die Verwendung der in Kapitel 2.2.3 und Kapitel 2.2.4 beschriebene Protokolle untereinander kompatibel sind. Dies ermöglicht eine Erweiterbarkeit des Systems ohne an einen bestimmten Hersteller gebunden zu sein.

Die Produkte der Firma Polycom werden in den nächsten Kapiteln nicht weiter berücksichtigt, da die Leistungsdaten im Vergleich zu den beiden anderen Anbietern LifeSize und Cisco Systems nicht überzeugen. So sind die maximal verfügbaren Auflösungen gerade im Bereich der Mehrpunktkonferenzen gering, des Weiteren wird der Ton nicht per AAC codiert, sondern über ein proprietäres Protokoll. Ein Speedmatching ist nicht vorhanden.

5.1.2 **Schulungssysteme**

Die vorgestellten Anbieter erfüllen die in Kapitel 3.1 formulierten Anforderungen an eine Videokonferenzlösung, dennoch sollen an dieser Stelle auch Alternativen genannt werden, mit denen es möglich ist, direkt über den PC Konferenzen aufzubauen und Dokumente bzw. den Bildschirm für andere sichtbar zu machen.

Citrix GoToMeeting (http://www.gotomeeting.de/) und Cisco WebEx (http://www.webex.de/) sind kostenpflichtige Produkte, die monatlich nach Anzahl der Konferenzteilnehmer lizensiert werden. Hier ist es nötig, einen Software Client zu installieren und sich mit diesem bei dem Server des jeweiligen Anbieters anzumelden.

Eine freie Alternative bietet eine Software namens BigBlueButton (http://www.bigbluebutton.org/) - Der Server kann heruntergeladen und in die Netzwerkstruktur eingebunden werden. Konferenzteilnehmer verbinden sich per Webbrowser mit diesem Server und können virtuelle Räume betreten. Einzig eine aktuelle Version des Adobe Flash Players ist Voraussetzung.

5.1.3 **Skype**

Die Anwendung Skype des gleichnamigen Unternehmens, welches seit Mitte 2011 zu Microsoft gehört, hat im Firmenumfeld eine besondere Position. Skype ermöglicht die Konferenzschaltung im reinen Audio, im Audio und Videomischbetrieb sowie den Austausch von Dokumenten.

Allerdings setzt Skype ein proprietäres Protokoll ein, welches der Öffentlichkeit nicht zugänglich ist, dies macht die Interoperabilität zu anderen Produkten unmöglich. Da Skype ein ausländisches Unternehmen ist, ist die Verwendung oder Weitergabe von persönlichen Daten und/oder Gesprächen nicht zu 100 % ausgeschlossen.

Skype wird in den beiden Standorten Hamburg und Hohenwestedt auf 79 von 431 Rechnern eingesetzt. Dies entspricht einem Abdeckungsgrad von etwa 18 %. Der Anteil der genutzten Datenübertragungsrate kann allerdings nicht ermittelt werden, da die benutzten Ports und Verbindungsanfragen unbekannt sind. Cisco bietet mit nBAR ein Analysewerkzeug, welches auf entsprechenden Netzwerkgeräten eingerichtet werden muss. Darüber ist es möglich den Traffic-Anteil einzelner Applikationen zu ermitteln, dies ist jedoch nicht Teil dieser Arbeit.

5.2 Kostenaufstellung und Kosten-Nutzen-Analyse

In Kapitel 5.2.1 werden nur die Kosten aufgezeigt, die unmittelbar durch den Erwerb eines Systems entstehen würden.

Die Kapitel 5.2.2 und 5.2.3 zeigen die momentanen im Durchschnitt anfallenden Reisekosten von Mitarbeitern, die sich für Konferenzen und Meetings zu entfernten Standorten begeben müssen. Diese Kosten werden dann im Kapitel 5.2.4 in einer Kosten-Nutzen-Analyse in Relation zu den Investitionskosten für ein Videokonferenzsystem gestellt. Eine Betrachtung der Investitionssicherheit erfolgt dann In Kapitel 5.2.5.

5.2.1 Kostenaufstellung Videokonferenzsystem

Angebotsanfrage

Von der DEKOM AG in Hamburg wurde ein Angebot zur Inbetriebnahme eines Videokonferenzsystems für alle Unternehmensstandorte erstellt.

Nach der Marktanalyse in Kapitel 5.1.1 wurden die Anforderungen genauer auf die am Markt befindlichen Produkte spezifiziert. Die folgende Tabelle 5-4 gibt diese Anforderungen wieder.

Standort	Standort	Systemart	Personen	gleichzeitige Verbindungen zu anderen Standorten	Anzahl Bildschirme
Deutschland	Hamburg	Raum	15	7	2 (Aktiv + ScreenSharing)
Deutschland	Hamburg	Raum	6	2	2 (Aktiv + ScreenSharing)
Deutschland	Hohenwestedt	Raum	8	4	2 (Aktiv + ScreenSharing)
Indien	Mumbai	Einzelplatz (stationäres System)	2	1	1
Indien	Paithan	Raum	4	2	2 (Aktiv + ScreenSharing)
Brasilien	Rio de Janeiro	Raum	4	1	2 (Aktiv + ScreenSharing)
USA	Charlotte	Raum	4	1	2 (Aktiv + ScreenSharing)
Singapur	Singapur	Einzelplatz (stationäres System)	2	1	1
Bahrain	Manama	Einzelplatz (stationäres System)	2	1	1

Tabelle 5-4: Anforderungen für Angebotsanfrage

Zusätzlich zu den oben genannten Anforderungen werden 40 Lizenzen benötigt, die zur Installation des Desktop Clients auf einem Microsoft Windows 7 System und Apple iPad2 berechtigen. Mitarbeiter haben so die Möglichkeit, extern per VPN-Verbindung einer Konferenz beizutreten.

Betriebsszenarien

Es wird zwischen zwei möglichen Szenarien für die Realisierung von Mehrpunktkonferenzen unterschieden, die unterschiedliche Anforderungen an die Hardware stellen:

Szenario A – integrierte MCU:

> Mehrpunktkonferenzen werden über die Codecs aufgebaut, so dass diese eine integrierte MCU besitzen müssen. Dadurch erübrigt sich der Einsatz einer externen MCU weitestgehend.

Szenario B – externe MCU:

> Mehrpunktkonferenzen werden über eine externe MCU aufgebaut, die Codecs benötigen daher also keine integrierte MCU. Der Vorteil dieses Szenarios ist der geringere Bedarf der Datentransferleistung bzw. die Konzentration dieser auf einen Standort.

Angebote und Kostenaufstellungen

Aufgrund der Größe der Angebote und der Optionsvielfalt sei hier nur eine Zusammenfassung der einzelnen Positionen gegeben. Tabelle 5-5 zeigt die Kostenaufstellung für die Produkte von LifeSize. Die darauf folgende Tabelle 5-6 enthält die Aufstellung der Kosten für das äquivalente System von Cisco Systems.

Die Kosten der Cisco Systems Endpunkte beinhalten bereits die Optionen für eine hochauflösende Videoübertragung, die Freischaltung der Mehrpunkt-Option und eines zweiten Monitors sowie die Kosten für ein Bedienpult. LifeSize nutzt ein solches Lizenzmodell nicht, zusätzliche Optionen müssen nicht freigeschaltet werden. Auch ein Bedienpult ist dort bereits im Preis enthalten.

In dieser Kostenaufstellung sind die Ersteinrichtungs- und Wartungsgebühren für das erste Jahr noch nicht enthalten. Diese belaufen sich auf etwa 40.000 € - 50.000 €. Sie sind abhängig vom Standort des Systems, der anzuschaffenden Hardware und dem Vertriebspartner.

Zusätzlich sollten noch Kosten für die Gestaltung und Umänderung von Räumen sowie der Beschaffung von geeigneten Lautsprechern und Receivern eingeplant werden. Pro Raum würden dann zusätzliche Kosten von etwa 5.000 € - 10.000 € entstehen.

Kostenaufstellung LifeSize

		Szenario A		Szenario B	
Artikel	**Preis pro Stück**	**Stückzahl**	**Preis**	**Stückzahl**	**Preis**
Endpunkte					
Unity 50 mit 24“ Display	3.000 €	3	9.000 €	3	9.000 €
Express 220, 10x Zoom	6.750 €	2	13.500 €	6	40.500 €
Team 220, 10x Zoom	10.500 €	2	21.000 €	0	0 €
Room 220, 10x Zoom	13.500 €	2	27.000 €	0	0 €
Endpunkte Zubehör					
Sony 60“ Monitor FWD-60NX720P	1.750 €	12	21.000 €	12	21.000 €
Wandhalterung (für 2 Monitore)	500 €	3	1.500 €	3	1.500 €
Ständer (für 2 Monitore)	1.720 €	3	5.160 €	3	5.160 €
Zentrale Administration					
LifeSize Control	375 €	9	3.375 €	9	3.375 €
MCU					
MCU Bridge 2200 12 Ports	37.500 €	0	0 €	1	37.500 €
Firewall Traversal/Gatekeeper/SIP Registrar					
UVC Server 1100	3.750 €	1	3.750 €	1	3.750 €
UVC Server 3300	8.250 €	1	8.250 €	1	8.250 €
UVC Transit Client – 5T	4.500 €	1	4.500 €	1	4.500 €
UVC Transit Server – 5T	4.500 €	1	4.500 €	1	4.500 €
UVC Access – 25 Reg. (GK)	1.125 €	1	1.125 €	1	1.125 €
Recording und Streaming (optional)					
UVC Server 3300	8.250 €	1	8.250 €	1	8.250 €
UVC Video Center 1 HD	7.500 €	1	7.500 €	1	7.500 €
Microsoft Windows, Apple iOS Support (Desktop Clients)					
LifeSize ClearSea CS100 Server VM 6 Ports 100 Benutzerkonten	6.375 €	1	6.375 €	1	6.375 €
ClearSea iOS Client	2.625 €	1	2.625 €	1	2.625 €
Gesamt (ohne Service und Inbetriebnahme)					
			146.910 €		**163.410 €**

Tabelle 5-5: Kostenaufstellung LifeSize

Kostenaufstellung Cisco Systems

		Szenario A		Szenario B	
Artikel	**Preis pro Stück**	**Stückzahl**	**Preis**	**Stückzahl**	**Preis**
Endpunkte					
EX60 mit 21,5“ Display	6.443 €	3	19.329 €	3	19.329 €
SX20 12x Zoom	12.229 €	2	24.458 €	0	0 €
C40 Integrator 12x Zoom	19.460 €	2	38.920 €	0	0 €
C60 Integrator 12x Zoom	25.496 €	2	50.992 €	6	152.976 €
Endpunkte Zubehör					
Sony 60“ Monitor FWD-60NX720P	1.750 €	12	21.000 €	12	21.000 €
Wandhalterung (für 2 Monitore)	500 €	3	1.500 €	3	1.500 €
Ständer (für 2 Monitore)	1.720 €	3	5.160 €	3	5.160 €
Zentrale Administration					
TP Management Suite 10x Lizenzen	2.007 €	1	2.007 €	1	2.007 €
MCU					
5310 MCU (max. 5 Ports)	13.201 €	1	13.201 €	0	0 €
5320 MCU (max. 10 Ports)	24.201 €	0	0 €	1	24.201 €
MCU Port Lizenz	6.601 €	5	33.005 €	10	66.010 €
Firewall Traversal/Gatekeeper/SIP Registrar					
Basis System VCS	6.799 €	2	13.598 €	2	13.598 €
10x Lizenzen non-Traversal	4.357 €	1	4.357 €	1	4.357 €
5x Lizenzen Traversal	4.951 €	1	4.951 €	1	4.951 €
FindMe Option	5.875 €	0	0 €	1	5.875 €
Dual Network Option	5.215 €	0	0 €	1	5.215 €
Recording und Streaming (optional)					
TCS 5 RecPorts	27.770 €	1	27.770 €	1	27.770 €
Microsoft Windows, Apple iOS Support (Desktop Clients)					
Jabber 100x	5.941 €	1	5.941 €	1	5.941 €
Gesamt (ohne Service und Inbetriebnahme)					
			266.189 €		**359.980 €**

Tabelle 5-6: Kostenaufstellung Cisco Systems

Obwohl Szenario A besagt, dass keine externe MCU genutzt werden sollte, muss bei einem System von Cisco Systems dennoch eine MCU eingeplant werden, da die Hardware Codecs nur maximal 4 gleichzeitige Verbindungen zulassen. Die Endpunkte mit der Bezeichnung C40 und SX20 ermöglichen keine HD-Auflösung bei Mehrpunktkonferenzen, so dass in Szenario B Cisco Systems C60 Codecs gewählt wurden.

5.2.2 **Reisekosten Hamburg – Hohenwestedt**

Da keine Reisekostenabrechnungen zwischen den Standorten Hamburg und Hohenwestedt existieren, müssen die einzelnen Positionen abgeschätzt werden.

Ein Fuhrpark von 7 Fahrzeugen für den Transport zwischen oben genannten Standorten steht den Mitarbeitern zur freien Verfügung. Diese Fahrzeuge sind jeweils als Ressource in Microsoft Exchange angelegt und sind reservierbar. Auch die 2 in Hamburg und 4 in Hohenwestedt befindlichen, bereits vorhandenen Konferenzräume sind über Microsoft Outlook reservier- und einsehbar.

Über die letzten 6 Monate wurden pro Woche im Durchschnitt 4 Konferenzräume von Mitarbeitern des jeweiligen anderen Standortes reserviert. Um an einer Konferenz teilnehmen zu können, wurden im Schnitt pro Woche 3 PKW reserviert.

Über diese bekannten Grundgrößen können nun Reisekosten ermittelt werden. Geht man davon aus, das Konferenztreffen in Zukunft zu 100 % über das Videokonferenzsystem abgewickelt werden, könnte der Fuhrpark verkleinert und Zeit eingespart werden.

Grundgrößen

Anzahl der PKW	3
Fahrten zwischen den Standorten im Monat	40 (9 pro Woche, 4,5 Wochen im Monat)
Anzahl der Mitarbeiter pro Fahrt	1,5
Wegstrecke zwischen Standorten	170 km

Sachmittelaufwand pro Monat und PKW (Fixkosten)

Versicherung	45,00 €
KFZ-Steuer	35,00 €
Wartungskosten	40,00 €
Leasingrate/Finanzierungsgebühr	400,00 €
Gesamt	**605,00 €**

Sachmittelaufwand pro Monat und PKW (dynamische Kosten)

Preis pro l Diesel	1,40 €
Verbrauch pro 100 km	7 l
Gesamt Kraftstoffkosten	**666,40 €** **(Gesamtwegstrecke x Anzahl Fahrten x Verbrauch / 100 x Spritkosten)**

Personalkosten pro Monat und Mitarbeiter

Kosten pro Stunde	40,00 €
Ausfallzeit (Reise + Planung) pro Fahrt	3 Std.
Gesamtkosten Personal	**4.800,00 €** **(Anzahl der Fahrten x Kosten pro Stunde x Ausfallzeit)**

Gesamtaufstellung (Kosten pro Monat)

Kostenart	**Einzelkosten**	**Anzahl**	**Gesamt**
Sachmittelaufwand (Fix)	605,00 €	3	1.815,00 €
Sachmittelaufwand (dyn.)	666,40 €	3	1.999,20 €
Personalkosten	4.800,00 €	1,5	7.200,00 €
			11.014,20 €

Tabelle 5-7: Reisekostenaufstellung Hamburg - Hohenwestedt

Leider wurden in großer Anzahl die Konferenzräume so reserviert, dass keine Teilnehmer sichtbar waren. Es ist davon auszugehen, dass die bestehende Rechnung nur einen gewissen Teil der Kosten erfasst, die tatsächlich anfallen. Eine genauere Aufstellung ist allerdings nicht möglich.

5.2.3 **Reisekosten gesamt**

Die Reisetätigkeiten und die daraus resultierenden Reisekosten sind in den letzten Jahren stark gestiegen. Die nachfolgende Abbildung 5-1 zeigt die kumulierten Reisekosten der letzten Geschäftsjahre des Unternehmens.

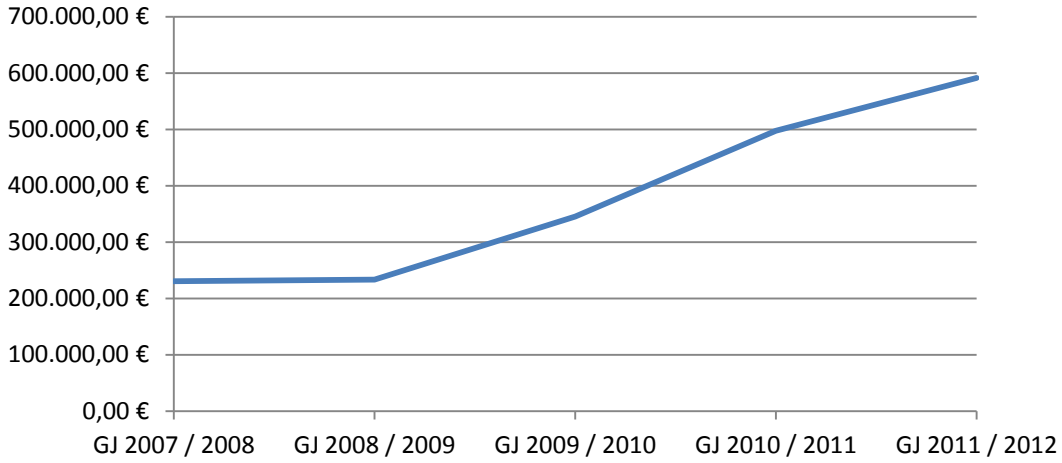

Abbildung 5-1: Reisekosten des Unternehmens der letzten Jahre

Wird die geplante Senkung der Reisekosten um 25 % tatsächlich erreicht oder gar überschritten, könnten etwa 150.000 € pro Jahr eingespart werden.

Ob durch Einführung eines Videokonferenzsystems die in den Anforderungen in Kapitel 3.1 definierte Minderung der Reisekosten um 25 % tatsächlich möglich ist, kann nicht überprüft werden. Laut einer Studie scheint diese Schätzung allerdings nicht unrealistisch zu sein (vgl. IMWF 2008, S. 9). Nach Inbetriebnahme eines Videokonferenzsystems sollte die Notwendigkeit einer Reisetätigkeit auf jeden Fall stärker in Frage gestellt werden, als es bisher der Fall war.

5.2.4 **Kosten-Nutzen-Analyse**

Zur besseren Beurteilung der Investition wurde eine Kosten-Nutzen-Analyse durchgeführt. Dabei wurde die Problematik des Messens und Bewertens in Pietsch 2003, S. 30 treffend formuliert:

„Zu den Problemen, die den Einsatz neuer Technologien in vielen Fällen erschweren, gehört der im Planungsstadium fehlende Nachweis über das Eintreten und die Höhe der Auswirkungen dieser neuen Arbeitsmittel. Konventionelle Investitionsrechenverfahren sind nur begrenzt in der Lage, neue Technologien zu bewerten, da erhebliche indirekte Wirkungen der Systeme, die auch in andere Unternehmensbereiche hineinreichen, und eine Vielzahl monetär nicht quantifizierbarer Faktoren zu berücksichtigen haben."

	Kosten	**Nutzen**
Direkt	Vorbereitung von Maßnahmen Anschaffung Wartung und Pflege	Durchlaufzeitverkürzung Qualitätsverbesserung Erhöhung der Kundenbindung
Indirekt	Umstellung Einarbeitung „Reibungsverluste"	Motivationssteigerung Know-how Aufbau Imageverbesserung

Tabelle 5-8: Kosten-Nutzen Faktoren (Pietsch 2003, S. 30)

Eine nicht messbare Größe in Projekten sind die Kosten, die durch einen Verzug entstehen. Ein Verzug entsteht immer dann, wenn Projektentscheidungen nicht direkt getroffen werden können, sondern aufgrund von personellen oder technischen Gegebenheiten verschoben werden müssen. Hier sei ein Beispiel gegeben: Die Produktion in Hohenwestedt muss sich mit einem Entwickler aus Hamburg treffen, um ein Bauteil zu überarbeiten. Da der entsprechende Mitarbeiter für den nächsten Monat bereits eine Fahrt nach Hohenwestedt plant, wird die Überarbeitung des Dokumentes auf diesen Termin gelegt. Das Bauteil wird bis zu diesem Treffen noch in alter Herstellung gefertigt, obwohl eine mögliche Designänderung des Bauteils Kosten in der Fertigung gesenkt hätten.

Da diese und andere Kosten nicht abgeschätzt werden können, werden an dieser Stelle nur die Kosten gegenübergestellt, deren Wert bekannt ist oder für die zumindest eine realistische Annahme getroffen werden kann. Wie bereits in Kapitel 5.2.1 beschrieben werden dabei nur die Systeme von LifeSize und Cisco Systems betrachtet und zwischen den Szenarien A (integrierte MCU) und B (externe MCU) unterschieden. Tabelle 5-9 zeigt exemplarisch eine vereinfachte dynamische Investitionsrechnung für das System von LifeSize (Szenario A). Die Kapitalwerte für alle vier Systeme sind der Tabelle 5-10 zu entnehmen.

		Periode (Werte in €)				
		1	2	3	4	5
Fixkosten						
Wartung		30.000	30.000	30.000	30.000	30.000
Ersteinrichtung		20.000	0	0	0	0
Raumgestaltung		67.500	0	0	0	0
Schulungskosten		10.000	0	0	0	0
Summe fixe Kosten		**127.500**	**30.000**	**30.000**	**30.000**	**30.000**
Variable Kosten (gesamt)						
Energie		800	800	800	800	800
Summe variable Kosten		**800**	**800**	**800**	**800**	**800**
Erlös/Einsparungen						
Reisekosten		150.000	160.000	170.000	180.000	190.000
Erlös gesamt		**150.000**	**160.000**	**170.000**	**180.000**	**190.000**
Cashflow	-146.910	21.700	129.200	139.200	149.200	159.200
Abzinsungsfaktor		0,87	0,76	0,66	0,57	0,50
Einzelbarwert	-146.910	18.870	97.694	91.526	85.306	79.151
Kapitalwert		**-128.040**	**-30.347**	**61.180**	**146.485**	**225.636**

Tabelle 5-9: dynamische Investitionsrechnung (LifeSize A)

Der Abzinsungsfaktor wurde mit einem kalkulatorischen Zinssatz von 15 % (gemäß Finanzvorgaben des Unternehmens) errechnet.

		Kapitalwert (Periode) in €				
Hersteller	**Szenario**	**1**	**2**	**3**	**4**	**5**
LifeSize	A	-128.040	-30.347	61.180	146.485	225.636
LifeSize	B	-144.540	-46.847	44.680	129.985	209.136
Cisco Systems	A	-247.319	-149.626	-58.099	27.206	106.357
Cisco Systems	B	-341.110	-243.417	-151.890	-66.585	12.566

Tabelle 5-10: Kapitalwerte nach 5 Jahren

Der Break-Even-Point ist bei den Systemen von LifeSize nach etwa 2,5 Jahren erreicht. Die Systemlandschaft von Cisco Systems rentiert sich erst nach etwa 4 bzw. 5 Jahren. Die Abbildung 5-2 verdeutlicht dies. Die geschätzten Einsparungen der nächsten Jahre durch entfallende Reisekosten zeigt die Tabelle 5-9.

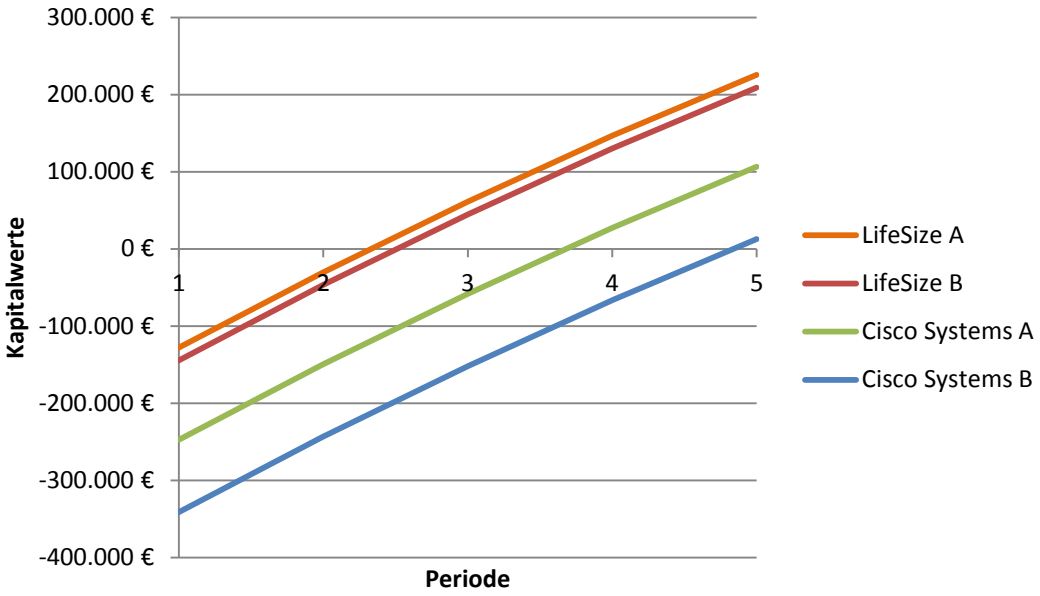

Abbildung 5-2: Gewinn- und Nutzenschwelle

5.2.5 Investitionssicherheit

Wie bereits erwähnt sind die in Kapitel 5.1.1 beschriebenen Systeme über die Protokolle H.323 sowie SIP kompatibel. Es gibt aktuell keine Hinweise, dass diese beiden Standards in den nächsten Jahren abgelöst werden könnten. Auch die Codecs zur Datenkomprimierung H.264 und AAC haben sich zu weit etabliert, als dass sie in absehbarer Zeit abgelöst werden würden. Selbst wenn ein neuer Standard verabschiedet wird, beherrschen die eingesetzten Geräte in der Regel auch die älteren Standards weiterhin.

Eine langjährige Nutzung und eine Erweiterbarkeit des Systems durch weitere Endpunkte oder MCUs sind durch diese Kompatibilität gegeben. Selbst wenn ein Hersteller die Insolvenz anmelden müsste, so könnte auf die Produkte der jeweiligen anderen Hersteller zurückgegriffen werden.

Sollte man den Kauf einer dedizierten MCU in Betracht ziehen, so ist es möglich, die Leistung durch Kopplung einer weiteren MCU oder durch Freischalten von Optionen zu

erhöhen. Aber auch ohne Kopplung ist ein Betrieb mehrerer MCUs im Netzwerk möglich, so dass die Videokonferenzinfrastruktur beliebig skalierbar und modifizierbar ist.

Nachfolgende Tabelle zeigt die Unternehmensdaten von Logitech und Cisco Systems. 2009 wurde die Firma LifeSize Communications von Logitech übernommen, die Firma Tandberg durch Cisco Systems im Jahr 2010. Umsätze und Gewinne wurden den jährlichen Geschäftsberichten 2011 entnommen.

Unternehmen:	**Gründungsjahr:**	**Umsatz:**	**Gewinn:**
Logitech (LifeSize)	1981 (2003)	2,3 Mrd. $	128,5 Mio. $
Cisco Systems (Tandberg)	1984 (1933)	43,2 Mrd. $	6,5 Mrd. $

Tabelle 5-11: Logitech / Cisco Systems Unternehmensdaten

5.3 Aufbau Testsystem

Ein Videokonferenzsystem kann in eigener Umgebung natürlich nicht in vollem Umfang getestet werden, daher werden in diesem Kapitel, soweit möglich, die von den Herstellern zur Verfügung gestellten Soft-Clients evaluiert und auf Performanz überprüft.

Für diese Umgebung sind 3 Systeme notwendig. Teilnehmer A und B sind einfache Endgeräte auf Microsoft Windows 7 Basis, auf denen die Soft-Clients installiert sind und die ein Mikrofon, Lautsprecher und eine Webcam bereitstellen.

Mit einem System zwischen diesen Teilnehmern ist es möglich, die verfügbare Transferrate einzuschränken, Paketlaufzeiten zu verändern und Pakete gezielt zu verwerfen. Diesen Funktionsumfang bietet die freie Software WANulator (http://wanulator.de/), welche zum Testzeitpunkt in der Version 2.01 vorlag. Die Anwendung muss nicht installiert werden, sondern lässt sich als Live System von CD starten.

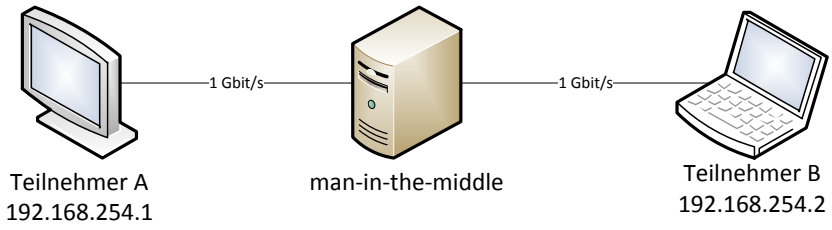

Abbildung 5-3: Aufbau Testsystem

Pakete, die zwischen den Teilnehmern A und B ausgetauscht werden, passieren das dritte System und werden dort manipuliert. Alle 3 Systeme sind von weiteren Netzwerken physikalisch getrennt, um Störfaktoren ausschließen zu können.

Die Testsysteme haben folgende Leistungsdaten:

	Teilnehmer A	**man-in-the-middle**	**Teilnehmer B**
CPU	Intel Core i3-2310M 2x 2,10 GHz	Intel Pentium Dual Core E5300 2x 2,60 GHz	Intel Core i3-2100 2x 3,10 GHz
RAM	8 GB	2 GB	4 GB
LAN	Intel 82579LM 1 Gbit/s	Intel 82567LM 1 Gbit/s Intel 82574L 1 Gbit/s	Intel 82579LM 1 Gbit/s
WEBCAM	Integriert HD 720p	-	Microsoft LifeCam Studio 1080p
Monitor Auflösung	1366 x 768	1680 x 1050	1920 x 1080
Mikrofon	X	-	X
Lautsprecher	X	-	X

Tabelle 5-12: Leistungsdaten der Testsysteme

Mit diesem Testaufbau werden in Kapitel 5.4 verschiedene Messungen durchgeführt, um die Performanz, Stabilität und Qualität der Übertragung zu bewerten. Zusätzlich wird geprüft, ob die empfohlene maximale Umlaufzeit von Paketen von 800 ms, wie in Kapitel 4.3.1 beschrieben, als realistisch betrachtet werden kann.

Für die *Software Cisco Jabber Video* und *LifeSize ClearSea* muss der Testaufbau abgeändert werden, da der Datenverkehr in der Testversion zwingend über einen externen Server geleitet wird. Der Testaufbau wird in Abbildung 5-4 gezeigt.

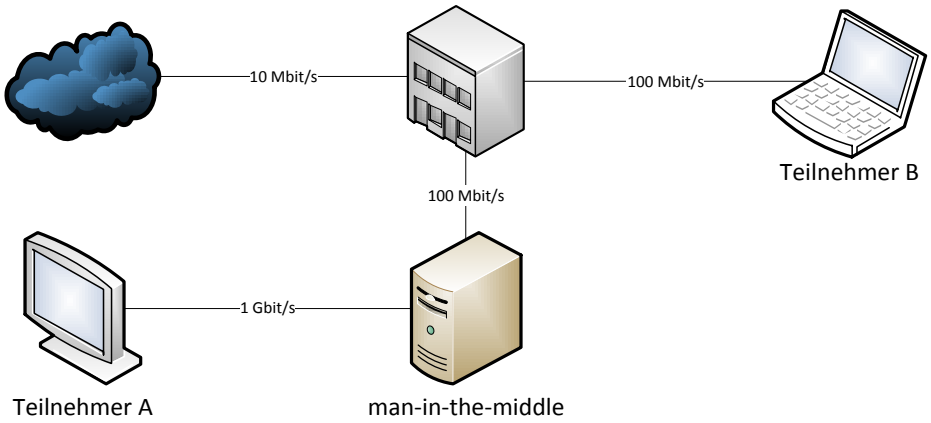

Abbildung 5-4: abgeänderter Testaufbau

Aufgrund des Anschlusses an das Firmennetzwerk können Störfaktoren beim Test auftreten, da der Datenverkehr nicht nur innerhalb des Netzwerkes gedrosselt werden kann, sondern auch dann, wenn er über das Internet geleitet wird.

5.4 Messungen

Mit dem in Kapitel 5.3 vorgestellten Messsystem werden nun die Leistungen der einzelnen Soft-Clients überprüft. Ziel ist es, die Grenzwerte für einen reibungslosen Betrieb zu ermitteln. Daher wird im ersten Schritt die Latenz soweit künstlich erhöht, dass eine Kommunikation über die Teilnehmer nicht mehr flüssig möglich ist. Dies ist natürlich ein subjektiver Eindruck und kein messbarer.

Im zweiten Schritt wird die verfügbare Übertragungsrate so lange gedrosselt, bis Bild oder Ton nicht mehr flüssig übertragen werden können. In diesem Test wird ermittelt, wie hoch die minimal verfügbare Transfergeschwindigkeit sein muss, um Videokonferenzen halten zu können.

Im dritten und letzten Schritt werden Pakete verworfen und Jitter erzeugt, auch hier können die Ergebnisse nur subjektiv bewertet werden. Dieser Test simuliert eine nicht stabile Internetverbindung wie sie z.B. am Standort Manama Kapitel 4.3.1 vorliegt.

Latenzmessung

Die Latenz wurde bei dieser Messung künstlich um jeweils 50 ms pro Route erhöht, um die Empfehlungen der ITU wie in Kapitel 4.3.1 beschrieben zu validieren. Die Anwendung LifeSize Desktop wurde als Testobjekt gewählt, da sie im Gegensatz zu LifeSize ClearSea und Cisco Jabber Video ohne einen Server betrieben werden kann und direkte Verbindungen zwischen Clients ermöglicht. Die Probanden sollten bei diesem Test eine Diskussion führen, um zu erkennen, ab welchem Zeitpunkt sich Gesprächspartner unbeabsichtigt, bedingt durch die Verzögerung, ins Wort fallen.

Dabei zeigte sich, dass eine RTT von etwa 300 ms noch als angenehm empfunden und der Gesprächsablauf nicht gestört wurde. Bei einer Paketumlaufzeit von etwa 500 ms kamen die ersten Missverständnisse auf, da unklar war, ob eine Sprachpause im Satz vorlag oder ob der Gesprächspartner seinen Dialog komplett beendet hatte.

Der empfohlene Grenzwert der ITU von 800 ms kann dann als realistisch betrachtet werden, wenn die Gesprächsteilnehmer darauf achten, laut und deutlich zu sprechen und Gesprächspausen möglichst kurz halten. Bei ungeübten Anwendern wird diese Umlaufzeit allerdings zu einem Unwohlsein und einer gestörten Konversation führen.

Die maximale Umlaufzeit von 463 ms wird im Unternehmen zwischen den Standorten Paithan und Rio de Janeiro erreicht und liegt damit deutlich unter dem Grenzwert der ITU und sogar etwas unter dem in Messungen ermittelten Wert.

Datenübertragungsgeschwindigkeit und Jitter

LifeSize ClearSea und auch *Cisco Jabber Video* reagierten auf eine künstliche Datentransferdrosselung gleich. Erwartungsgemäß zeigten sich Artefakte im Bild und auch die Tonübertragung war für kurze Zeit gestört. Nach etwa 5-10 Sekunden passten die Systeme die Auflösungen an die Übertragungsgeschwindigkeit an, so dass ein fehlerfreies Bild zu erkennen war.

Bei diesem Test kam erschwerend hinzu, dass die zur Kommunikation benötigen Server in den USA stehen und die beiden angebundenen Clients über die verfügbare Internetanbindung des Unternehmens kommunizieren mussten (vgl. Abbildung 5-4).

Da für die Codierung der Daten die gleichen Codecs verwendet wurden, lag auch das Datenvolumen gleich auf. Eine 720p Verbindung benötigt im Up- und Downstream jeweils etwa 1.200 kbit/s.

Ein Vergleich der Anwendungen bei Übertragung des Datenstromes mit einer Auflösung von 1080p war in dieser Testumgebung nicht möglich, da *Cisco Jabber Video* die Webcam nicht vollständig unterstützt. *LifeSize ClearSea* benötigte etwa 1.800 kbit/s, wobei es nach einer gewissen Zeit zu einem Verbindungsabbruch kam. Dieser wurde wahrscheinlich durch die Verbindung zu den Testservern verursacht. Beim Wiederherstellen der Konnektivität wurde die Übertragung automatisch wieder aufgenommen.

Die aus den Datenblättern entnommenen Herstellerangaben zu den Transferleistungen konnten somit durch die vorgenommenen Messungen, soweit möglich, validiert werden. Warum bei Cisco Systems allerdings etwa 2.500 kbit/s bei einer 1080p Übertragung nötig sein sollen und bei LifeSize nur etwa 1.800 kbit/s kann nicht verifiziert werden, da die genutzten Protokolle und Codecs bei beiden Produkten augenscheinlich gleich sind.

5.5 Bedienung und Administration

Bedienung der Endpunkte

Bei den Endpunkten ist eine Evaluierung natürlich nur teilweise möglich, so wird im Folgenden nur die Bedienung der Desktop Clients betrachtet.

Mögliche Teilnehmer können in beiden Anwendungen in Favoriten bzw. Kontaktlisten aufgenommen werden, so dass ein Gesprächspartner per Doppelklick direkt kontaktiert werden kann. Über einen Verlauf können zusätzlich die letzten Gesprächspartner angezeigt werden. Das Teilen des Bildschirminhaltes sowie das Aktivieren und Deaktivieren der Kamera und des Mikrofons ist in beiden Anwendungen möglich, ebenso die Installation auf Systemen mit Microsoft Windows und Apple iOS.

Abbildung 5-5: LifeSize ClearSea Desktop Client

Teilnehmer haben über die Benutzeroberfläche die Möglichkeit, die entfernte Kamera, sofern dies unterstützt wird, zu steuern bzw. auszurichten. Die *Far-End-Camera-Control (FECC)* Technologie wird in Anhang Q von ITU H.323 beschrieben.

Im Gegensatz zu *Cisco Jabber Video* bietet *LifeSize ClearSea* eine Option zum Aufnehmen von Gesprächen an, die dann als WMV-Datei exportiert werden können.

Administration

LifeSize und auch Cisco Systems bieten eine zentrale Administrations-Software an, welche optional zu erwerben ist. Diese Anwendung wird nach Anzahl der Geräte lizensiert, die eingebunden werden sollen. In der Kostenaufstellung in Tabelle 5-5 und in Tabelle 5-6 sind diese Positionen bereits aufgeführt.

Über die zentrale Administration können die Endpunkte überwacht und konfiguriert werden. Hier ist es zudem möglich, ein globales Adressbuch zu pflegen und Reservierungen durchzuführen. Beide Systeme bieten eine Integration mit Microsoft Exchange, das bereits im Unternehmen eingesetzt wird.

Keiner der beiden Hersteller bietet eine Live-Version dieser Anwendung an, so dass eine Evaluierung nicht stattfinden kann.

5.6 Bewertung

Die Marktanalyse hat gezeigt, dass die Anforderungen des Unternehmens von mehreren Produkten bzw. Herstellern abgedeckt werden können.

Die Hersteller LifeSize und Cisco Systems und deren Produkte wurden näher betrachtet, da diese schon lange am Markt etabliert sind. Die Differenz der Kosten beider Hersteller ist allerdings, wie in Kapitel 5.2.1 gezeigt wurde, ungeachtet des Szenarios beträchtlich.

In Sachen Leistung und Handhabung sind die Systeme ähnlich, wobei die Produkte von LifeSize stärker auf die Technologie FullHD, also das Senden und Empfangen von 1080p Streams, vorbereitet zu sein scheinen. Selbst die kleinsten Produkttypen ermöglichen den Einsatz dieser Technologie. Cisco Systems erlaubt dies erst durch separate Lizenzen und größere Produkttypen.

Nun stellt sich hier die Frage, ob eine Übertragung von 1080p tatsächlich notwendig ist oder ob eine geringere Auflösung von 720p ausreichen würde. Betrachtet man die ermittelten und empfohlenen symmetrischen Transferleistungen von etwa 1,4 Mbit/s bei einer Übertragung von 720p zu etwa 3 Mbit/s von 1080p im Dualstream-Betrieb (mit aktivierter Screensharing Funktion), so muss abgewogen werden, welche Übertragungsrate an den Standorten auch realistisch möglich und bezahlbar sind. Ohne Screensharing würden die Transferrate bei etwa 1,2 Mbit/s bei 720p und 2,5 Mbit/s bei 1080p liegen.

Die ermittelten Ergebnisse aus Kapitel 4 liefern hier ein entsprechendes Bild. Die meisten Standorte würden maximal mit einer Auflösung von 720p arbeiten können. Einzig die Standorte in Hamburg, Hohenwestedt und Mumbai könnten mit der momentanen Infrastruktur mit 1080p senden. Wobei hier nochmals erwähnt werden sollte, dass der Datenverkehr über die Standleitung von Hohenwestedt nach Hamburg genutzt werden sollte. Ein Senden von 1080p ist in Hohenwestedt über das Internet nicht möglich.

Durch die hohen Paketumlaufzeiten von bis zu 463 ms kann zudem keine nicht flüssige Konversation geführt werden, dies zeigt auch der Test in Kapitel 5.4.

Die beiden gezeigten Szenarien beschreiben den optionalen Einsatz einer MCU bei Einsparung der integrierten MCU der Endgeräte. Da dieses Szenario zwar in der Erstanschaffung teurer ist, sich aber durch die Skalier- und Erweiterbarkeit auszeichnet, sollten sich diese Ausgaben spätestens mit der Anbindung eines weiteren Standortes rentiert haben. Der weitere Vorteil liegt hier auch in der geringeren Datenübertragungsrate, welche an den Standorten vorliegen muss, da der Hauptverkehr an der MCU entsteht.

6 Konzeption zur Einführung des empfohlenen Systems

Die folgenden Kapitel geben Auskunft über die erforderlichen Maßnahmen, um das Videokonferenzsystem in die Unternehmensstruktur zu integrieren.

6.1 Systemauswahl

Die Systeme von LifeSize bieten bei gleicher oder höherer Leistung das klar bessere Preis-Leistungs-Verhältnis (siehe Kapitel 5.2.1). Daher werden die Produkte dieses Herstellers an dieser Stelle empfohlen.

MCU

Aus Gründen der Skalier-, und Erweiterbarkeit und der geringeren Datenübertragungsleistung an den Standorten sollte eine dedizierte MCU (MCU Bridge 2200 12 Ports) gekauft und im Unternehmensstandort Hamburg bereitgestellt werden. Dies hat den Vorteil der Kontrollierbarkeit des Gerätes sowie der niedrigeren Reaktionszeit bei Problemen. Die MCU lässt sich per Lizenz auf maximal 16 simultane Verbindungen erweitern. Sollte dann eine erneute Erweiterung von Nöten sein, so muss in eine zweite baugleiche MCU mit Clustering-Lizenz investiert werden.

Stationäre Endpunkte

Alle Konferenzräume können aufgrund der zentralen MCU mit dem kleinsten zu erwerbenden Raumsystem (Express 220, 10x Zoom mit jeweils 2 Bildschirmen) in Betrieb genommen werden. Die Standorte Manama, Singapur und Mumbai erhalten mit dem Einzelsystem Unity 50 mit 24“ Display ein System, welches flexibel einsetzbar ist.

Zusätzlich müssen Wandhalterungen oder Ständer und entsprechende Bildschirme (mindestens 60“ Diagonale) beschafft werden.

Mobile Endpunkte

Die Anwendung *LifeSize ClearSea* für mobile Endgeräte ist wie gefordert auf Microsoft Windows sowie Apple iOS Geräten lauffähig. Die Anwendung kann über den Appstore von Apple bezogen werden. Auf Microsoft Windows Endgeräten liegt die Anwendung als MSI-Datei vor, die dann verteilt werden kann. Die Anforderungen des Desktopclients an die Hardware sind moderat:

- 2 x 2GHz
- 1 GB RAM
- 60 MB Kapazität auf der Festplatte

Der entsprechende Server CS100 liegt virtuell als VMware Image vor und kann auf dem bereits existierenden VMware ESX Cluster des Unternehmens untergebracht werden. Folgende Anforderungen an die Hardware werden gestellt:

- Hostsystem XEON Nehalem 4x2GHz
- 2 GB RAM
- 10 GB HDD
- 2 Netzwerkkarten für optionales NAT Traversal

Die Lizenz zur Unterstützung von Apple iOS Geräten muss zusätzlich erworben werden. Auf dem Server können 100 Benutzerkonten erstellt werden, mit denen eine Authentifizierung möglich ist. 6 gleichzeitige Verbindungen sind in der kleinsten Ausstattung möglich.

Gatekeeper und Traversal Server

Um die Sicherheit der Endpunkte zu gewährleisten und auch externe Unternehmen bei Bedarf in einer Videokonferenz anbinden zu können, werden 2 Traversal Server benötigt. Die schwächer dimensionierte Appliance UVC1100 (Traversal Server) sollte außerhalb des internen Netzwerkes (DMZ) betrieben werden. Die stärker dimensionierte Appliance UVC3300 (Traversal Client) sollte im Unternehmensnetzwerk untergebracht werden. Die Kommunikation dieser beiden Appliances geschieht über einen gesicherten Tunnel durch die Firewall des internen Netzwerkes.

Der Vorteil dieser Server ist die integrierte Virtualisierung. So lässt sich per Lizenz der nötige UVC Access Dienst, der für die Registrierung der Endpunkte zuständig ist und somit als Gatekeeper dient, auf der UVC3300 zusammen mit dem Traversal Client aktivieren.

Des Weiteren müssen die entsprechenden Lizenzen erworben werden:

- UVC Access 25 Registrierungen
- UVC Transit Server 5 simultane Verbindungen
- UVC Transit Client 5 simultane Verbindungen

Streaming und Recording

Ein Recording Server ermöglicht die Aufnahme von Konferenzen. Folgende Vorteile bieten sich durch den Einsatz:

- Existenz potentieller Beweismittel bei Verhandlungen mit externen Firmen
- Verzicht auf einen Protokollanten während der Konferenz
- Verwendbarkeit aufgezeichneter Produktschulungen für ein anderes Publikum (Kapitel 3.3 – Szenario 2)

Ein Streaming- und Recording Server ist optional in der Kostenaufstellung vorhanden. Die Anschaffung beinhaltet eine UVC 3300 Appliance und eine entsprechende Lizenz, damit ein Strom aufgenommen werden kann.

Administration

LifeSize Control sollte im Unternehmen eingesetzt werden, um von zentraler Stelle die Endpunkte administrieren zu können. Dazu gehören das Einspielen von Aktualisierungen, das Erstellen eines zentralen Telefonbuches und das Aktualisieren der Systeme. Für *LifeSize Control* wird ein Server mit mindestens Microsoft Server 2003 benötigt. Es sind 9 *LifeSize Control* Lizenzen für die 9 Endpunkte nötig.

6.2 Netzwerkstrukturierung

Standortanbindung

Für die uneingeschränkte Benutzung eines Videokonferenzsystems an allen Standorten muss die Netzwerkinfrastruktur zwischen diesen neu strukturiert werden. Es wurde in Kapitel 4.3.3 und Kapitel 5.4 gezeigt, dass weder die Datenraten noch die Paketumlaufzeiten ausreichen, um einen störungsfreien Betrieb zu gewährleisten.

Ein internationaler MPLS-Anbieter wie die Telekom Deutschland GmbH oder die Nippon Telegraph and Telephone Corporation könnten alle Unternehmensstandorte verbinden, die Umlaufzeit der Pakete verringern und die Übertragungsgeschwindigkeiten garantieren.

Bei der Stationierung der MCU im Standort Hamburg müssen nur weitere 7 externe Räume angebunden werden. Folgende Tabelle zeigt die bisherigen durchschnittlichen

Auslastungen ohne Videokonferenzbetrieb sowie die zu erwartenden Auslastungen bei einer Konferenz mit allen vorhandenen Standorten im 720p und 1080p Betrieb.

Standort	Durchschnittliche Auslastung	Mindestdatenrate 720p	Mindestdatenrate 1080p
Hamburg	1.587	11.387	22.587
Hohenwestedt	2.197	3.597	5.197
Charlotte	355	1.755	3.355
Mumbai	242	1.642	3.242
Paithan	304	1.704	3.304
Manama	107	1.507	3.107
Singapur	63	1.463	3.063
Rio de Janeiro	320	1.720	3.320

Tabelle 6-1: synchrone Mindestdatenrate in kbit/s

Die Tabelle beschreibt die Mindestdatenrate, die anliegen muss, um die Datenmengen verarbeiten zu können. Peaks und auch Overhead können nicht erfasst werden, sollten aber bei der Auswahl des MPLS-Netzwerkes bedacht werden. Für jeden externen Mitarbeiter, der einer Konferenz beitreten möchte, erhöht sich am Standort Hamburg die nötige Transferleistung um 1,4 Mbit/s.

Sollte die Datenübertragungsrate nicht reichen, so sorgen die eingesetzten Systeme für eine Drosselung der Auflösung um eine optimale Qualität zu erreichen.

Die Kosten zur Strukturierung des Netzwerkes müssen über Angebote ermittelt werden. In der bisherigen Kostenrechnung wurden diese nicht berücksichtigt.

IP-Adressen und QoS

Bei Einführung des Systems müssen, wie in Kapitel 4.3.5 beschrieben, entsprechende VLANs mit der Datenpriorität 4 eingerichtet werden. Die IP-Adressen sollten aus dem bisherigen 172er IP-Adressbereich für die Standorte Hamburg und Hohenwestedt gewählt werden. Für alle weiteren Standorte sollten IP-Adressen aus dem 192er IP-Adressbereich genutzt werden (siehe Kapitel 4.3.6).

Wichtig bei der Umstellung auf ein MPLS-Netzwerk ist die Abstimmung der Datenprioritäten mit dem Netzwerkdienstleister, damit die Pakete auch beim Ein- und Austreten, sowie der Weiterleitung im Anbieternetzwerk korrekt behandelt werden.

6.3 Kosten und Beschaffung

Kosten/Kosten-Nutzen

Auch wenn die Kosten für ein Videokonferenzsystem hoch erscheinen, so können die Anschaffungskosten sich im besten Fall nach etwa 2,5 Jahren, im schlechtesten Fall nach 5 Jahren mit den Reisekosten angleichen.

Beschaffung im Ausland

Die Beschaffung der Hardware im Ausland sowie die Ersteinrichtung des Systems kann über das GDP (Global Deployment Program) von LifeSize erfolgen. Hier kann der beauftragte Dienstleister auf LifeSize Vertriebspartner im Ausland zurückgreifen. Der Ansprechpartner für das Unternehmen bleibt allerdings der Dienstleister, z.B. die DEKOM AG selbst.

Cisco Systems verfügt ebenfalls über Dienstleister, die selbstständig international tätig sind. Hier wäre Orange Business Services als Beispiel zu nennen (www.orange-business.com).

Dauer

Laut Dienstleister muss eine Zeitspanne von 3-5 Wochen von Auftragseingang bis zur Benutzbarkeit des Systems im Inland eingeplant werden. Die Gesamtdauer sollte im Ausland mit dem Faktor 2-3 berechnet werden. Hier liegen die Schwierigkeiten bei der Beschaffung der Hardware im Ausland sowie der Einrichtung dieser durch den Dienstleister bzw. dessen Partner.

6.4 Planung und Umsetzung

Einführungsstrategie

Es gibt zwei mögliche Strategien das Videokonferenzsystem in die Unternehmensstruktur zu integrieren. Zum einen wäre die *Big-Bang-Strategie* zu nennen, die das komplette Projekt in nur einer Phase umsetzt. Zwar wird so Zeit gespart, allerdings können Anfangsschwierigkeiten auf alle Standorte projiziert werden. Die Akzeptanz der Anwender gegenüber diesem System könnte leiden. Zudem könnten Fehlkalkulationen nicht rechtzeitig erkannt werden.

Auf der anderen Seite steht die *Proof of Concept-Strategie.* Diese ermöglicht es, die einzelnen Phasen im Projekt zu testen. Basierend auf den Ergebnissen kann das System dann weiter expandiert werden. Aufgrund der Anforderungen sollte diese Strategie bei der Projektumsetzung gewählt werden, um Komplikationen möglichst zu vermeiden.

Projektplan

Nach Rücksprache mit der Abteilungsleitung stellte sich heraus, dass die Hauptstandorte Hamburg und Hohenwestedt als Testobjekt für das System dienen sollen. Paithan und Rio de Janeiro sollen in zweiter Instanz am Test teilnehmen, da die dortigen Standorte erst wenige Monate alt sind. Das Projekt wird daher in 3 Phasen unterteilt. Nach jeder Phase können Erfahrungen gesammelt werden, die dann in die nächste Phase einfließen können.

Die angegebenen Kosten beinhalten nur die Hard- und Software. Wartungs- und Ersteinrichtungsgebühren werden nicht berücksichtigt – ebenso wenig wie Raumausstattungskosten.

1. Phase (Dauer: etwa 5 Wochen, Kosten: 32.845 €)

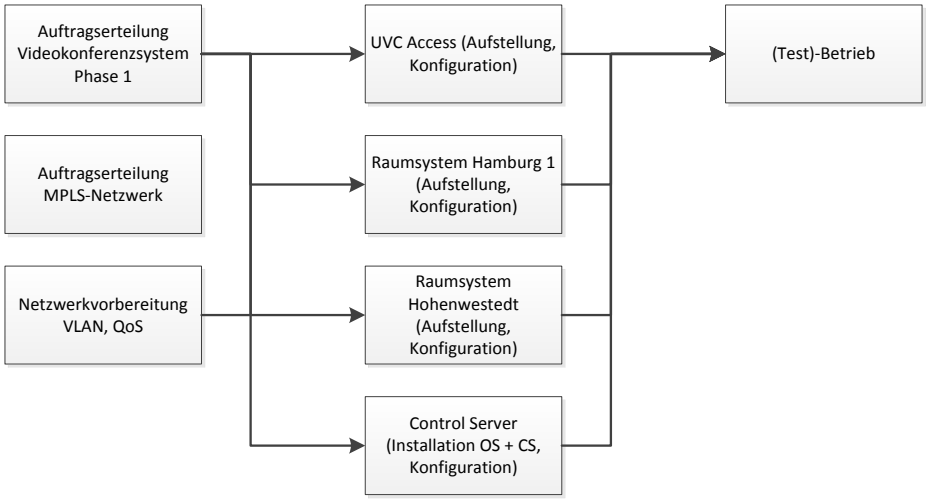

Abbildung 6-1: Projektplan – Phase 1

2. Phase (Dauer: etwa 12 Wochen, Kosten: 96.970 €)

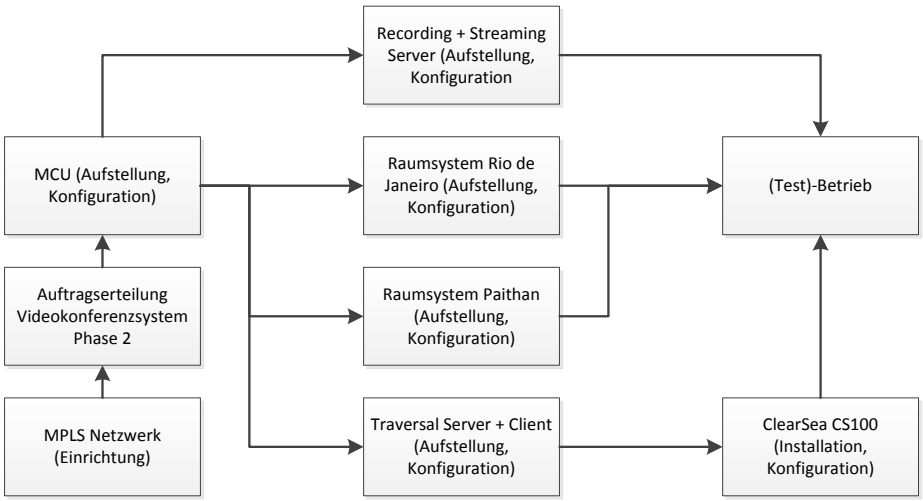

Abbildung 6-2: Projektplan – Phase 2

3. Phase (Dauer: etwa 10 Wochen, Kosten: 33.595 €)

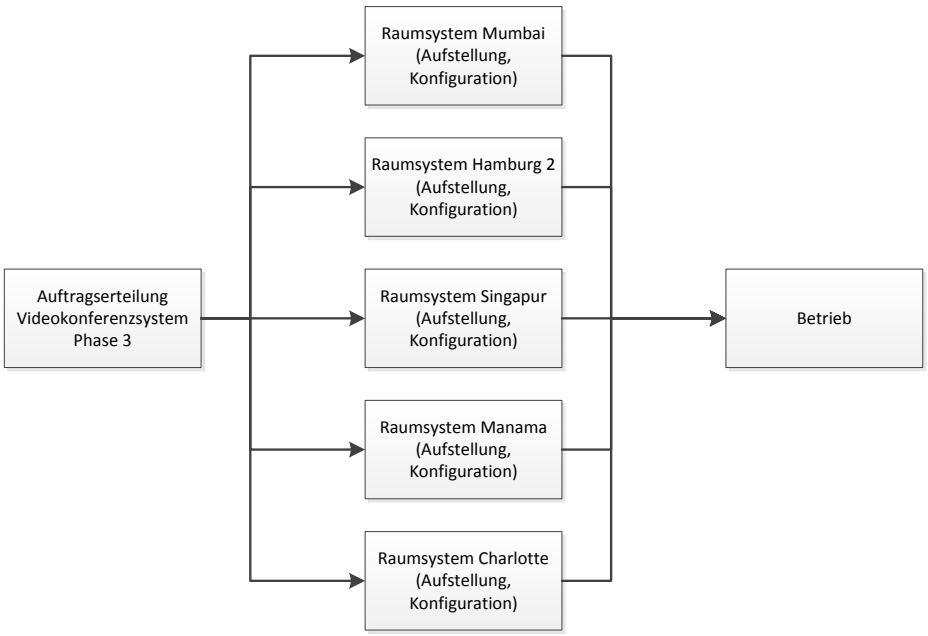

Abbildung 6-3: Projektplan – Phase 3

Ersteinrichtung und Konfiguration des Systems

Die Ersteinrichtung des Systems sollte und kann vom Dienstleister durchgeführt werden, um Fehler zu vermeiden. Die weitere Administration erfolgt dann zentral durch eine Administrationsanwendung, die eine Verbindung zu allen Endpunkten herstellen kann. Die entsprechenden Lizenzen für LifeSize oder der TP Management Suite müssen gesondert erworben werden. Diese Kosten sind in der Aufstellung in Tabelle 5-5 aufgeführt.

Schulungsaufwand

Aufgrund der einfachen Handhabung über die entsprechenden Kontaktlisten, welche zentral eingerichtet werden können, sollte der Schulungsaufwand nicht zu hoch ausfallen.

Der Schulungsaufwand fällt für die Mitarbeiter der IT-Abteilung, die das System administrieren sollen, höher aus als für die Mitarbeiter, die das Videokonferenzsystem lediglich bedienen sollen.

Positionierung und Raumausstattung

Das Videokonferenzsystem sollte so in einem Raum positioniert werden, dass sich keine Fenster im Rücken der Gesprächsteilnehmer befinden, um Reflexionen zu vermeiden. Eine indirekte Beleuchtung ist einer direkten Beleuchtung vorzuziehen.

Zusätzlich sollte darauf geachtet werden, dass sich keine Pflanzen oder Bilder im Sichtfeld der Kamera befinden. Diese verursachen ein schwaches Bildrauschen, das von den Teilnehmern als unangenehm empfunden werden kann. Die Hersteller der Systeme empfehlen eine gedeckte Wandfarbe im Hintergrund für bestmöglichen Kontrast.

Die Raumgröße muss vom entsprechenden Systemtyp abhängig gemacht werden. Für ein Raumsystem für 6 Personen im Zweischirmbetrieb sollte der Raum etwa 4 m breit und 5 m lang sein, um einen genügend großen Sitzabstand zu den Monitoren zu gewährleisten.

Ton

Wenn die Soundausgabe nicht über die integrierten Lautsprecher der Monitore erfolgen soll, so müssen pro Raum ein HDMI-Receiver und passende Stand- oder Hängelautsprecher ausgewählt werden. Je nach Raumbeschaffenheit sollte dann auf die Empfehlung des Dienstleisters gewartet werden, sobald die passenden Räume ausgesucht worden sind.

Das gleiche gilt für zusätzliche Mikrofone, die bei großen Räumen notwendig sind, damit alle Teilnehmer gleichmäßig gut zu verstehen sind. In der Tabelle 5-9 werden die Kosten für Raumgestaltung und Ton unter der Position „Raumgestaltung“ geführt.

7 Zusammenfassung und Ausblick

7.1 Zusammenfassung

Um die gestellten Anforderungen an ein Videokonferenzsystem in Kapitel 3.1 zu realisieren, musste im ersten Schritt das bisherige Unternehmensnetzwerk erkannt und hinsichtlich Übertragungsrate und Laufzeit analysiert werden.

Da das Netzwerk unbekannt war, musste eine einfache Strategie entwickelt werden, um Knotenpunkte zu erkennen. Nach Konfigurierung dieser ermittelten Knotenpunkte mit Hilfe von SNMP konnten anfallende Datenströme durch einen Kollektor ausgewertet und die mittleren Auslastungen der Interfaces ermittelt werden, um dann später eine Empfehlung zur möglichen Neustrukturierung des Netzwerkes geben zu können.

Im zweiten Schritt wurde in Kapitel 5.1 eine Marktanalyse vorhandener Systeme durchgeführt. Ein Vergleich der Systeme hat ergeben, dass die Produkte der Hersteller LifeSize sowie Cisco Systems die gestellten Anforderungen erfüllen. Durch den Einsatz offener Protokolle steigert sich die Investitionssicherheit, da die Produkte des jeweiligen anderen Herstellers kompatibel sind.

In Kapitel 5.2 wurden die Kosten für die jeweiligen Systeme und mögliche Optionen aufgezeigt und eine Kosten-Nutzen-Analyse erstellt. Hier zeigte sich, dass sich die Kosten bereits nach wenigen Jahren amortisiert haben, sofern die Vorgabe zur Verringerung der Reiseaktivitäten um 25 % eingehalten wird.

Durch Messungen der nötigen Datentransferrate stellte sich heraus, dass das bestehende Netzwerk zwischen den Standorten nicht ausreichend dimensioniert ist. Daher wurde eine Empfehlung zum Umstieg auf ein MPLS-Netzwerk gegeben. Durch die im Laufe der Arbeit ermittelten Informationen wurde dann im letzten Schritt in Kapitel 6 ein zusammenfassendes Konzept erstellt, welches zur Einführung des Systems genutzt werden kann.

7.2 Ausblick

Es wird erwartet, dass die Verbreitung von Videokonferenzsystemen in den nächsten Jahren stark zunimmt (vgl. Gartner 2011). Zwei Technologien werden sich wahrscheinlich in absehbarer Zukunft auch in der Technik der Videokonferenzsysteme durchgesetzt haben.

H.265 wurde von der ITU im Juli 2012 als Nachfolger des Standards H.264 offiziell vorgestellt. Der Standard sieht vor, höhere Auflösungen bis zu 7680 x 4320 Bildpunkte zu unterstützen. Zudem liegt die Kompressionsrate mit dem Faktor 2 deutlich über der des Vorgängers, ohne Einbußen in der Qualität zu verzeichnen (vgl. Corner 2012).

Wie bereits in Kapitel 2.2.1 angedeutet werden in Zukunft zertifizierte Bildschirme auf den Markt gebracht werden, die 4k und 8k Auflösungen unterstützen werden. Sollte dann auch noch die Bildschirmgröße signifikant steigen, so könnten auch Videokonferenzen mit mehreren Teilnehmern eine neue Dimension erlangen.

Unter dem Begriff *Telepresence 3D* sind bereits Videokonferenztechnologien zu finden, die ein Gespräch zwischen Teilnehmern noch realer aussehen lassen als es bisher schon der Fall ist. Der Antrieb der 3D-Technologie liegt ganz klar bei der Multimediaindustrie. Wenn der Markt nach 3D-Produkten verlangt, so werden sicherlich auch Videokonferenzsysteme von diesem Verlangen profitieren. Momentan hat sich 3D in der Konferenzwelt noch nicht durchgesetzt.

A – Zuordnungen der Interfaces

Standort	**Internet**	**Tunnel nach**
Hamburg	10.49.255.5>DTAG 10.49.255.5>HANSENET	192.6.13.3>Gi0/1 (Hohenwestedt)
Hohenwestedt	10.49.254.5>DTAG	192.6.11.2>Tu0 (Hamburg) 192.6.11.2>Gi0/1 (Hamburg)
Charlotte	192.168.50.254>Gi0/2	192.168.50.254>Tu0 (Hamburg)
Manama	192.168.53.1>Gi0/1	192.168.53.1>Tu0 (Hamburg)
Singapur	192.168.55.1>Gi0/1	192.168.55.1>Tu0 (Hamburg)
Rio de Janeiro	192.168.64.1>Gi0/1	192.168.64.1>Tu0 (Hamburg)
Mumbai	192.168.10.1>Gi0/1	192.168.10.1>Tu0 (Paithan) 192.168.10.1>Tu1 (Hamburg)
Paithan	192.168.20.1>Gi0/0	192.168.20.1>Tu0 (Mumbai) 192.168.20.1>Tu1 (Hamburg)

Literaturverzeichnis

Balakrishnan 2008

BALAKRISHNAN, Ram: *Advanced QoS for multi-service IP/MPLS networks.* Indianapolis, IN : Wiley, 2008. – ISBN 978-0-470-29369-0

Beasley 2004

BEASLEY, Jeffrey S.: *Networking.* Upper Saddle River, NJ : Pearson Prentice Hall, 2004. – ISBN 0130986593

Borowka 2002

BOROWKA, Petra: *Netzwerk-Technologien : [Gerätetechnik und Protokolltechnik ; alles über Bridges, Switches and Router ; SAN, VoIP, MPLS, Rapid STP, 802.1x Security, VPN].* 1. Aufl., (4. Aufl. des Titels InterNetworking). Bonn : mitp, 2002. – ISBN 3-8266-4093-4

Corner 2012

CORNER, Stuart: New MPEG standard halves video bandwidth with no quality loss. Juli 2012. – URL http://www.itwire.com/business-it-news/technology/56199-new-mpeg-standard-halves-video-bandwidth-with-no-quality-loss. Zugriffsdatum 20.08.2012

DEKOM 2012

DEKOM AG (Hrsg.): Visual Solutions. Hamburg, 2012

Diestel 2010

DIESTEL, Reinhard: *Graphentheorie.* 4. Aufl. Heidelberg [u.a.] : Springer, 2010. – ISBN 978-3-642-14911-5

Eckert 2008

ECKERT, Claudia: *IT-Sicherheit : Konzepte, Verfahren, Protokolle.* 5. Aufl. München [u.a.] : Oldenbourg, 2008. – ISBN 9783486582703

Gartner 2011

MASON, Robert F. ; MORRISON, Scott: MarketScope for Telepresence and Group Video Systems. Research Note G00215756. August 2011. – URL http://www.gartner.com/technology/reprints.do?id=1-174ZY5B&ct=110831&st=sb. Zugriffsdatum 06.08.2012

IEEE802.1Q 2005

IEEE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard for Local and metropolitan area networks : Virtual Bridged Local Area Networks. IEEE 802.1Q. Mai 2006. – URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1637340. Zugriffsdatum: 18.06.2012

IMWF 2008

IMWF INSTITUT FÜR MANAGEMENT-UND WIRTSCHAFTSFORSCHUNG GMBH: Face to Phase: Die Konvergenz von Geschäftsreisen und Virtual Meetings. Dezember 2008. – URL http://www.vdr-service.de/fileadmin/fachthemen/studien/easynet_konvergenz-v-geschaeftsreisen-u-virtualmeetings_20080113.pdf. Zugriffsdatum 22.08.2012

ITU G.114

INTERNATIONAL TELECOMMUNICATION UNION: One-way Transmission Time. ITU-T G.114. Februar 2003. – URL http://www.itu.int/itudoc/itu-t/aap/sg12aap/history/g.114/g114s.html. Zugriffsdatum: 23.06.2012

ITU H.235

INTERNATIONAL TELECOMMUNICATION UNION: H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems. ITU-T H.235. September 2005. – URL http://www.itu.int/rec/T-REC-H.235.0-200509-I/en. Zugriffsdatum: 24.07.2012

ITU H.323

INTERNATIONAL TELECOMMUNICATION UNION: Packet-based multimedia communications systems. ITU-T H.323. Dezember 2009. – URL http://www.itu.int/rec/T-REC-H.323-200912-I/en. Zugriffsdatum: 10.07.2012

ITU R.709

INTERNATIONAL TELECOMMUNICATION UNION: Parameter values for the HDTV standards for production and international programme exchange. ITU-T R.709. April 2002. – URL http://www.itu.int/rec/R-REC-BT.709-5-200204-I/en. Zugriffsdatum: 12.07.2012

Kanbach 2005

KANBACH, Andreas: *SIP - die Technik : Grundlagen und Realisierung der Internet-Technik ; für VoIP, Videotelefonie, Instant-Messaging und Presence-Service ; [mit Online-Service zum Buch].* 1. Aufl. Wiesbaden : Vieweg, 2005. – ISBN 383480052X

Pietsch 2003

PIETSCH, Thomas: *Bewertung von Informations- und Kommunikationssystemen : Ein Vergleich betriebswirtschaftlicher Verfahren.* 2. Aufl. Berlin : Erich Schmidt, 2003. – ISBN 3-503-07088-5

RFC 1157

CASE, J. ; FEDOR, M. ; SCHOFFSTALL, M. ; DAVIN, J.: Simple Network Management Protocol (SNMP). Request For Comments (RFC) 1157. Mai 1990. – URL http://tools.ietf.org/html/rfc1157. - Zugriffsdatum: 14.06.2012

RFC 3550

Schulzrinne, H. ; Casner, S. ; Frederick, R.: RTP: A Transport Protocol for Real-Time Applications. Request For Comments (RFC) 3550. Juli 2003. – URL http://tools.ietf.org/html/rfc3550. Zugriffsdatum: 04.07.2012

RFC 6275

PERKINS, C. E. ; JOHNSON, D. B. ; ARKKO, J.: Mobility Support in IPv6. Request For Comments (RFC) 6275. Juli 2011. – URL http://tools.ietf.org/html/rfc6275. – Zugriffsdatum: 27.06.2012

Rose 1993

ROSE, Marshall T.: *Einführung in die Verwaltung von TCP-IP-Netzen : Netzwerkverwaltung und das Simple Network Management Protocol (SNMP).* München ; Wien, London : Hanser; Prentice Hall Internat., 1993. – ISBN 3-446-16444-8

Rosenberg 2005

ROSENBERG, J.: A Framework for Conferencing with the Session Initiation Protocol draft-ietf-sipping-conferencing-framework-05. Mai 2005. – URL http://tools.ietf.org/html/draft-ietf-sipping-conferencing-framework-05. – Zugriffsdatum 04.07.2012

Scherff 2010

SCHERFF, Jürgen: *Grundkurs Computernetzwerke : Eine kompakte Einführung in Netzwerk- und Internet-Technologien ; [mit Online-Service].* 2. Aufl. Wiesbaden : Vieweg + Teubner, 2010. – ISBN 9783834803665

Schiller 2003

SCHILLER, Jochen H.: *Mobile communications.* 2. Aufl. London ;, Boston : Addison-Wesley, 2003. – ISBN 0321123816

Schmeh 2007

SCHMEH, Klaus: *Kryptografie : Verfahren, Protokolle, Infrastrukturen.* 3. Aufl. Heidelberg : Dpunkt-Verl., 2007. – ISBN 3898644359

Soliman 2004

SOLIMAN, Hesham: *Mobile IPv6 : Mobility in a wireless Internet.* Boston : Addison-Wesley, op. 2004. – ISBN 0201788977

Stallings 1999

STALLINGS, William: *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.* 3. Aufl. Reading, Mass : Addison-Wesley, 1999. – ISBN 0-201-48534-6

Tanenbaum 2003

TANENBAUM, Andrew S.: *Computernetzwerke.* 4. Aufl. München [u.a.] : Pearson Studium, 2003. – ISBN 3827370469

Trick 2005

TRICK, Ulrich ; WEBER, Frank: *SIP, TCP-IP und Telekommunikationsnetze : Next generation networks und VoIP - konkret.* 2. Aufl. München, Wien : Oldenbourg, 2005. – ISBN 3486577964

Zisler 2012

ZISLER, Harald: *Computer-Netzwerke : Grundlagen, Funktionsweise, Anwendung.* Bonn : Galileo Press, 2012. – ISBN 3836216981

Tabellenverzeichnis

Abbildungsverzeichnis

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _____

Jan Nissen