INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Virtuelle Lokale Netze
Analyse, Realisierung, Einsatzkonzept am Beispiel des Gebäudekomplexes Oettingenstraße

Bearbeiter:	Ute Schartner
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Norbert Wienold
	Ulrich Katzenschwanz
Abgabetermin:	15. August 1998

Hiermit versichere ich, daß ich die vorliegende Diplomarbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. August 1998

....
(Unterschrift des Kandidaten)

Zusammenfassung

Virtuelle LANs (VLANs) erlauben die logische Segmentierung von Netzen unabhängig von der physischen Netzstruktur. Diese Flexibilität beim Design und bei der Änderung der aktuellen Netzstruktur soll den Netzadministrator beim Netzbetrieb entlasten und Komponenten einsparen helfen.

In dieser Diplomarbeit wird der Einsatz von VLANs an einem speziellen Beispiel des Gebäudekomplexes Oettingenstraße untersucht.
Die Implementierung von VLANs hängt von zahlreichen Parametern ab. Analysiert werden hierzu die möglichen VLAN-Technologien, die vorhandene Organisationsstruktur, die Anforderungen der Anwender und des Betreibers und die Möglichkeiten der vorhandenen Komponenten.
Die Analyse der technischen Grundlagen ergab vier verschiedene VLAN-Konzepte und diverse, z.T. nicht-standardisierte, Lösungen für die Backbone-Anbindung der VLANs.
Das Ergebnis der Analyse der Aufbauorganisation ergab eine flache, hierarchische Organisationsstruktur, bestehend aus autonomen, eigenständigen Instituten (OE). Zwischen diesen OE findet keine Ablauforganisation und keine Beziehungsstruktur statt. Die Infrastruktur am Einsatzort ist relativ neu. Das Gebäude ist mit einer "modernen" strukturierten Verkabelung erschlossen. Die Kommunikation erfolgt mittels Datenswitches der Firma 3Com.
In der Planungs-Phase wurden verschiedene Szenarien, aufgrund der logischen Gruppierung der Endgeräte und der eingesetzten VLAN-Technik, durchgespielt und voneinander abgegrenzt, um eine optimale Lösung am Einsatzort zu erreichen. Aufgrund der Besonderheiten am Einsatzort (Ergebnisparameter aus Analyse-Phase) ist das Ergebnis dieser Untersuchung eine mögliche VLAN-Definition, die nicht notwendigerweise genau einer Klasse von VLANs zugeordnet werden kann, sondern aus einer Kombination von "infrastructural"- und "service-based"-VLANs besteht. Bei der Abbildung der VLAN-Szenarien auf die Voraussetzungen der Oettingenstraße wurde gezeigt, daß die Umsetzung sehr stark von den eingesetzten Komponenten und ihrer Funktionalität abhängt. Mit den vorhandenen Komponenten sind nur die einfachsten VLANs (portbasierende VLANs) realisierbar.
In der Realisierungs-Phase wurden die Aktivitäten beschrieben, die notwendig sind, um die Migration vom derzeitigen LAN zum Layer-1-VLAN durchzuführen. Dabei wurde auf die Vorbereitungen bei der Installation, der Konfiguration und der Netzadministration näher eingegangen.
Die Einsparungen der Komponenten und die Vereinfachung der Netzadministration durch den Einsatz von Layer-1-VLANs sind nur minimal und rechtfertigen den Umbau nicht. Der Einsatz neuer Komponenten und von Layer-3-VLANs könnten aber erhebliche Vorteile bieten.

Inhaltsverzeichnis

1 Einleitung **8**
1.1 Wettbewerbsbedingungen und U-Strukturen 8
1.2 Potentiale der IuK-Technik für die U im Markt 11

2 Aufgabenstellung und Vorgehensweise **12**
2.1 Motivation 12
2.2 Aufgabenstellung 13
2.3 Aktivitäten 14

I Eine Einführung in VLANs **18**

3 Technische Grundlagen **20**
3.1 VLANs und deren Voraussetzungen 20
3.2 Normgerechte Verkabelung 21
3.2.1 Strukturierte Verkabelung 22
3.2.2 Kabeltypen 24
3.3 Switches 27
3.4 Unterschiedliche VLAN-Konzepte 30
3.4.1 Layer-1-VLANs 32
3.4.2 Layer-2-VLANs 34
3.4.3 Layer-3-VLANs 37
3.4.4 Policy-basierende VLANs 40
3.5 VLANs im Backbone 41
3.5.1 Austausch von Adreßtabellen 42
3.5.2 Frame Tagging 43
3.5.3 Time Division Multiplexing 44
3.5.4 VLANs über ATM 44

II Analyse-Phase **46**

4 Ermittlung der Organisationsstruktur **48**
4.1 Begriffserklärung Organisation 48
4.2 Aufbauorganisation 48
4.3 Ablauforganisation 52
4.4 Koordination zwischen den OE 53

4.5 Eingliederung des Personalbedarfs in den OE 54
4.6 Ergebnis der Aufbauorganisation 55

5 Ermittlung der Anforderungen der Benutzer aus den OE 57
5.1 Fragebogen und Ergebnisse 57
5.2 Fazit 59

6 Ermittlung der vorhandenen Topologie 60
6.1 Infrastruktur 60
6.2 Komponenten 65
6.3 Netzplan 66

7 Ermittlung der Anforderungen des Betreibers 68
7.1 Überblick über das LRZ 68
7.2 Aufgaben des LRZ 70
7.3 Anforderungen des LRZ 71
7.4 Motivation für diese Diplomarbeit 72

III Planungs-Phase 74

8 VLAN Szenarien 76
8.1 Infrastructural VLANs 76
8.2 Service-Based VLANs 77
8.3 VLAN-Bildung im Gebäudekomplex Oettingenstraße 79

9 Umsetzung VLAN-Szenarien am Einsatzort 83
9.1 Layer-1-VLAN am Einsatzort 85
9.2 Layer-2-VLAN am Einsatzort 89
9.3 Layer-3-VLAN am Einsatzort 93
9.4 Abgrenzung der VLAN-Szenarien 96
9.4.1 Aufwand, um Endgeräte bei einer Erstinstallation einem VLAN zuzuordnen 96
9.4.2 Administrationsaufwand bei Änderungen jeder Art 97
9.4.3 Mehrere VLANs pro Port 98
9.4.4 Sicherheit 99
9.5 Bewertung 100

IV Realisierungs-Phase 102

10 VLANs in der Oettingenstraße 104
10.1 Planung der Installation 104
10.2 VLAN-Management-Aktivitäten 106
10.2.1 Konfigurations-Management 106
10.2.2 Fehler-Management 107
10.3 Schnittstellenbeschreibung LRZ-LMU 108

V Zusammenfassung **110**

11 Fazit **112**

Abkürzungsverzeichnis **118**

Literaturverzeichnis **118**

A Fragebogen **120**

B Diagramme **122**

Abbildungsverzeichnis

1.1 Hierarchische Organisation und Matrix-Organisation 9
1.2 Wandel der Marktsituation und Reorganisationsbedarf (Pribilla/Reichwald/Goecke 1996) 10

2.1 Flexible-Organisation / Dynamische-Teams 13
2.2 Teilausschnitt des MHN 14
2.3 Entscheidungsmatrix für VLAN-Implementierung am Einsatzort 15
2.4 Analyse- und Planungs-Phase 16

3.1 Strukturierte Verkabelung 23
3.2 Die "Normpyramide" 27
3.3 Cut Through-Switching 28
3.4 Store and Forward-Switching 29
3.5 VLAN-Kriterien für den Aufbau 31
3.6 Beispiel mit Layer-1-VLANs 33
3.7 Beispiel mit Layer-2-VLANs 36
3.8 Beispiel mit Layer-3-VLANs (IP) 39
3.9 Beispiel mit Policy-basierten VLANs 40
3.10 VLAN-Tag innerhalb eines Ethernet-Frames 44
3.11 Datenstrom zwischen zwei Switches 45
3.12 VLAN über ATM-Backbone 45

4.1 Beispiel einer top-down Zerlegung 50
4.2 Aufgabenanalyse im Gebäudekomplex Oettingenstraße 50
4.3 Organisationsstruktur des Gebäudekomplexes Oettingenstraße . . 56

6.1 Physische Sternstruktur mit Uplink 61
6.2 Strukturierte Verkabelung am Einsatzort 62
6.3 Logische Netztopologie Oettingenstraße 63
6.4 Verbindung über Router zw. Oettingenstr.- LRZ 65
6.5 Infrastruktur im Gebäudekomplex Oettingenstraße 67

8.1 Infrastructural VLAN 77
8.2 Entscheidungsmatrix für Service-Based VLAN 78
8.3 Service-Based VLAN 79
8.4 Entscheidungsmatrix: Institute - Server 80
8.5 VLAN-Bildung am Einsatzort 82

9.1 Layer-1-VLANs am Einsatzort: physischer Stand heute 85
9.2 Layer-1-VLANs am Einsatzort: nach Umkonfiguration 87
9.3 Layer-1-VLANs am Einsatzort: Lösung mit zusätzl. Switch . . . 88
9.4 Layer-1-VLANs am Einsatzort: Lösung mit Verb. zw. Switches . 89
9.5 Layer-2-VLANs am Einsatzort: physischer Stand heute 90
9.6 Layer-2-VLANs am Einsatzort: nach Umkonfiguration 91
9.7 Layer-2-VLANs am Einsatzort: Lösung 92
9.8 Layer-3-VLANs am Einsatzort: physischer Stand heute 93
9.9 Layer-3-VLANs am Einsatzort: nach Umkonfiguration 94
9.10 Layer-3-VLANs am Einsatzort: Lösung 95
9.11 VLAN-Struktur bei Umzügen 98

10.1 Planung der Installation 105
10.2 Beispiel einer gemeinsamen Komponente für zwei OE 105
10.3 Beispiel einer VLAN-Konfiguration 106

Tabellenverzeichnis

3.1 Aufbau einer erweiterten Adreßtabelle 42

9.1 Abgrenzung VLAN-Szenarien am Einsatzort 100

Kapitel 1

Einleitung

Die heutige Wirtschaft unterliegt einem ständigen Wandel, es gibt viele Trends und Modeströmungen. Hiervon ist auch die IT-Branche betroffen. Die Netztechnik hat sich inzwischen zu einer eigenständigen Industrie entwickelt und ist einer der Motoren des Wirtschaftswachstums.

1.1 Wettbewerbsbedingungen und U-Strukturen

Die klassische Beschreibung eines Unternehmens als abgeschlossenes, integriertes Gebilde entspricht nicht mehr dem heutigen Stand. "Die klassischen Grenzen der Unternehmung beginnen zu verschwimmen, sich nach innen wie nach außen zu verändern, teilweise auch aufzulösen." (zitiert aus [1]). Um heute wettbewerbsfähig und erfolgreich zu sein, müssen die Unternehmen und Märkte sich ständig weiterentwickeln und neue Strategien einführen wie:

- Auflösung von Hierarchien,
- Symbiosen und Kooperationen,
- Elektronische Märkte,
- virtuelle Unternehmen, etc.

Diese Herausforderung kann nur im Zusammenhang mit der Entwicklung und Veränderungen in Wettbewerb, Technologie und Gesellschaft erfolgen. (Quelle [1] Innovationspotentiale, Wettbewerbssituation und Innovationsstrategien)

Viele Unternehmen müssen ihre Wettbewerbsbedingungen verändern, um flexibel und schnell auf individuelle Kundenanforderungen zu reagieren und rasch und kostengünstig auf die sich ändernde Nachfrage einzugehen.

Auch die Informations- und Kommunikations-Technik (IuK) unterliegt einem permanenten Wandel. Die dramatische Leistungssteigerung, Miniaturisierung und Integration dieser Technologie hat zur Folge, daß neue Anwendungspotentiale geschaffen werden. Neue Formen der Arbeitsorganisation und Arbeitsteilung (Globalisierung der Märkte), neue Kooperationsformen in und zwischen

Unternehmen wie Teamkonzepte, Gruppenarbeit, modulare Organisation, Arbeit in mobilen Büros oder dezentralen Arbeitsstätten, Telekooperation und virtuelle Unternehmen stehen für diese Entwicklung.

Die oben dargestellte Entwicklung kann nur durch einen tiefgreifenden Wandel in der Gesellschaft und in der Arbeitswelt erfolgen. Ein wesentlicher Faktor für diesen Wandel ist eine Abflachung oder sogar Auflösung der hierarchischen Strukturen. Die klassischen Abteilungen und Hierarchieebenen verlieren an Bedeutung. Streng festgelegte Kommunikationsstrukturen werden ersetzt durch direkte Gruppenkommunikation. Dazu gewinnen Werte wie Eigenverantwortung, Selbstentscheidung und Selbstverwirklichung in der Arbeitswelt immer mehr Bedeutung.

Die permanenten Veränderungen der Wettbewerbsbedingungen sind Auslöser für den Reorganisationsbedarf in einer Unternehmung. Als Triebkräfte werden dabei die Globalisierung und Intensivierung des Wettbewerbs, die steigende Innovationsdynamik, die Potentiale der IuK-Techniken sowie der gesellschaftliche Wandel genannt. Die Effizienz einer Organisation ist im wesentlichen abhängig von der gewählten Unternehmensorganisation, die an die relevanten Umfeldbedingungen angepaßt wird.

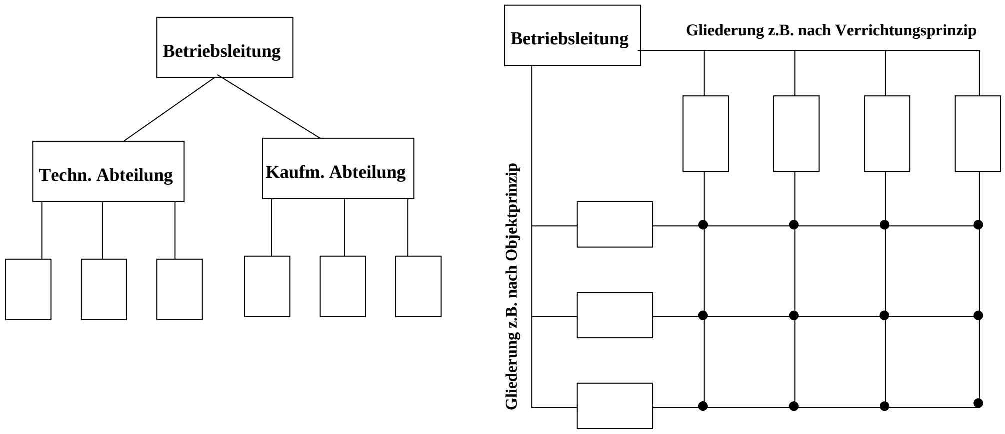


Abbildung 1.1: Hierarchische Organisation und Matrix-Organisation

Die veränderten Rahmenbedingungen des Wettbewerbs stellen neue Anforderungen an die Unternehmensorganisation. Die Reorganisation soll das Unternehmen dazu befähigen:

- schnell auf Änderungen des Marktes zu reagieren,
- global aufzutreten und dennoch lokal angepaßt zu handeln,
- kurze Durchlaufzeiten (Produktionsentwicklung, Auftragsabwicklung),
- durchgängige Ausrichtung auf den Kunden,

- die Kreativität der Mitarbeiter anzuspornen, etc.

Vor dem Hintergrund dieser Anforderungen sollen die beobachteten Defizite der klassischen Organisationsprinzipien: Hierarchie, Bürokratie, Taylorismus (Abb. 1.1) reduziert werden, indem neue organisatorische Unternehmensformen eingesetzt werden. Diese Unternehmensformen stellen flexible Strukturen dar und bilden so die Anforderungen des Marktes ab (vgl. Abb. 1.2).

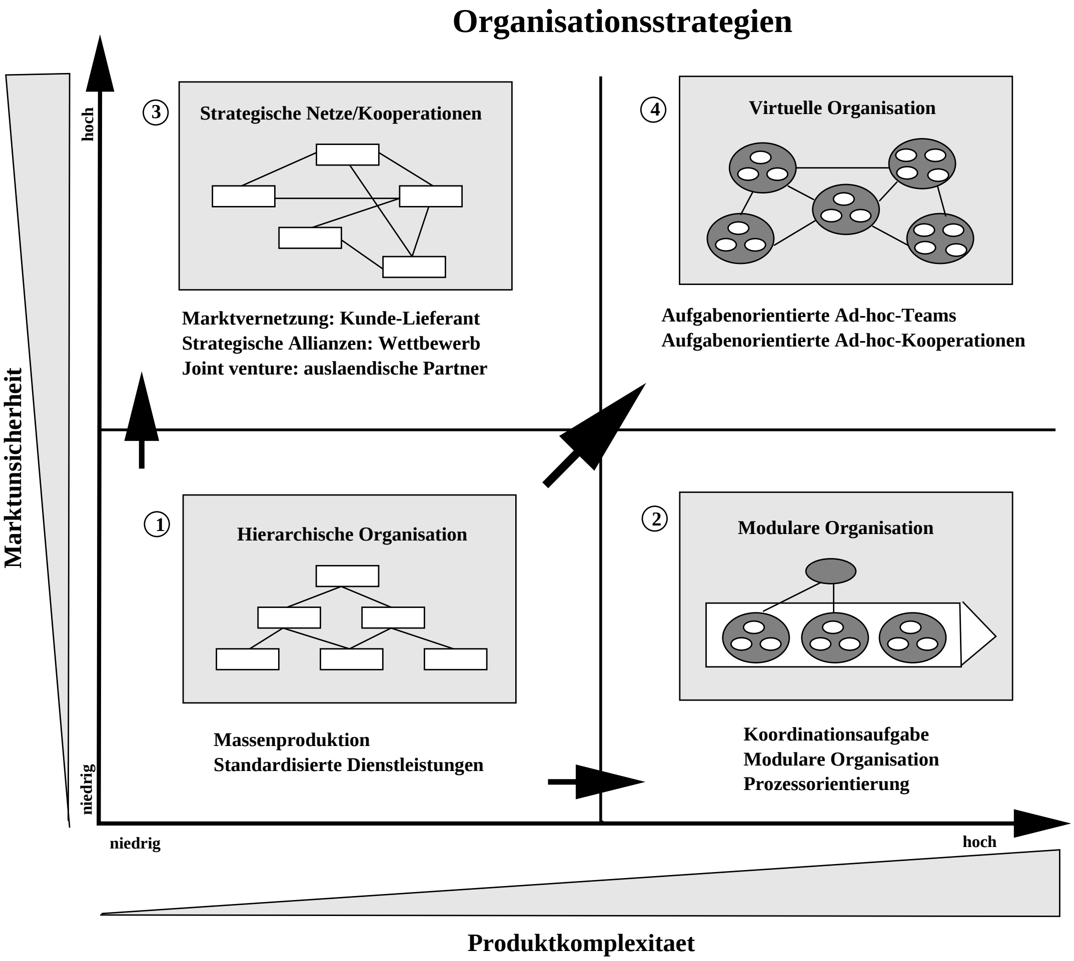


Abbildung 1.2: Wandel der Marktsituation und Reorganisationsbedarf (Pribilla/Reichwald/Goecke 1996)

Die veränderten Wettbewerbsbedingungen verlangen von den Unternehmen Flexibilität und Innovationsfähigkeit. Um diese Eigenschaften zu verwirklichen sind unternehmensweit koordinierte IuK-Systeme erforderlich.

1.2 Potentiale der IuK-Technik für die U im Markt

Die Entwicklung neuer Technik führt zu neuartigen Potentialen für das Leben jedes Einzelnen, für die Gesellschaft, aber nicht zuletzt für die Zukunft der Arbeitswelt, in denen arbeitsteilige Aufgabenprozesse abgewickelt werden.

Neue IuK-Techniken sind die Instrumente, mit deren Hilfe der notwendige Wandel vollzogen wird. Sie ermöglichen durch schnellere, kostengünstigere, raum- und zeitüberbrückende Nachrichtenübertragung und Informationsverarbeitung flexible Organisationsformen.

Neue IuK-Möglichkeiten ergeben sich im wesentlichen aus verschiedenen technologischen Weiterentwicklungen. Die enorme Steigerung der Leistungsfähigkeit von passiven und aktiven Komponenten ermöglicht die Übertragung und Verarbeitung immer größerer Datenmengen. Dies hat zur Folge, daß bestehende Engpässe bei unternehmensinternen und unternehmensübergreifenden Kommunikationsbeziehungen beseitigt werden. Auch die Integration von verschiedenen Informationsarten wie: Daten, Bild, Ton, Video, über eine gemeinsame Darstellungs- und Verarbeitungsweise ist möglich. Insgesamt kann festgehalten werden, daß neue IuK-Möglichkeiten sich in qualitativ verbesserten, schnelleren und billigeren Übertragungs- und Verarbeitungsformen zeigen. Daraus ergibt sich eine Vielzahl von individuellen Wettbewerbsvorteilen.

Neue Formen der Arbeitsorganisationen, der innerbetrieblichen Strukturen und nicht zuletzt des IuK-Flusses erfordern immer mehr Flexibilität, mehr Bandbreite in Netzen und eine Reduzierung des administrativen Aufwands. Schlagworte wie Internet, Extranet und Intranet gehören inzwischen zum allgemeinen Sprachgebrauch. Sie kennzeichnen oberflächlich die Veränderungsprozesse der IuK-Technologien.

Kapitel 2

Aufgabenstellung und Vorgehensweise

2.1 Motivation

Die Netz- und Rechnerkonzepte haben sich in den letzten Jahren erheblich verändert. In den achtziger Jahren setzten Unternehmen überwiegend hierarchische und zentralisierte Systemlösungen ein. Diese Architekturen wurden nach und nach durch viele voneinander unabhängige Geräte ersetzt, die über lokale Netze (LANs) oder auch Weitverkehrsnetze (WANs) miteinander verbunden wurden. Dieser Entwicklung ging ein quantitativer und qualitativer Leistungszuwachs der passiven und aktiven Komponenten voran:

- steigende Performance am Arbeitsplatz: Prozessoren (8088, 8086, ... , Pentium), Speicher-Ausruestung der PCs (256kB, 1MB, 8MB, 32MB...)
- Entwicklung der Netztechnologien: Ethernet (10, 100, 1000 Mbit), Token Ring (4, 16, 100(?)Mbit), ATM (2, 34, 45, 155, 622 Mbit, 2,4 bis 10 GBit)
- Kabel der Kategorie 1,2,3 (Datenübertragung), 4,5,6/7 (High-speed-Übertragung)

Es ist also ein ungebrochener Trend zu immer mehr Leistung erkennbar.

Neue HW-Technologien und die unterschiedlichen Strömungen im Netzdesign führen zu ständigen Neuentwicklungen in diesem Bereich. Dabei ist der Trend zu immer kürzeren Innovationszyklen zu erkennen. Angesichts der Dynamik der Märkte und der Kurzlebigkeit vieler Innovationen und Produkte bleibt den Unternehmen nicht viel Zeit, um sich auf neue Anforderungen und Rahmenbedingungen einzustellen.

Die Diplomarbeit muß nun diesem Trend bzw. dieser permanenten Weiterentwicklung Rechnung tragen. Aber neben reiner Performance und Geschwindigkeit ist die Flexibilität in einer Unternehmung wichtig. Wie in Kap. 1 schon erwähnt, ist die Schaffung von flexiblen Organisationsstrukturen (dynamischen Teams) (vgl. Abb. 2.1) notwendig.

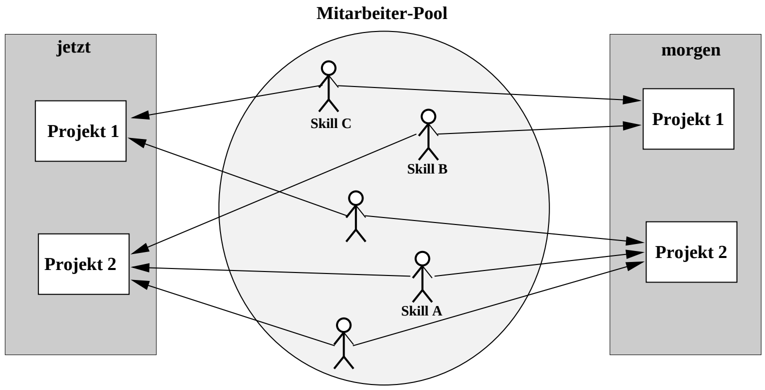


Abbildung 2.1: Flexible-Organisation / Dynamische-Teams

Untersuchungen zeigen, daß in deutschen Unternehmen durchschnittlich 30% aller Stationen im Jahr verlegt werden. Der Grund liegt in der ständigen Veränderung (Expansion, neue Aufgaben/Projekte) innerhalb einer Organisation. Z.B. eine Abteilung soll neue Aufgaben übernehmen, die aber mit vorhandener Manpower nicht zufriedenstellend gelöst werden kann, d.h. die Abteilung muß sich erweitern. Bei staendigem Wachstum reicht irgendwann der Platz nicht mehr aus und die Abteilung muß umziehen. Solche Umzüge können innerhalb eines Gebäudes, auf einem Campus, oder sogar in ein neues Gebiet erfolgen. Diese häufigen Umzüge haben zur Folge, daß Teilnehmer eines dynamischen Teams in sehr kurzer Zeit über das gesamte Netz verteilt sind, d.h. über alle Switchsysteme hinweg. In der Praxis bedeutet dies, daß alle Broadcasts an alle Systeme verteilt sind und das Netz unübersichtlich wird. Bei einem solchen Netzkonstrukt müssen also wesentlich höhere Anforderungen an das Netz gestellt werden.
In Abb. 2.1 ist exemplarisch eine flexible Organisation dargestellt. Hier wird auftragsbezogen gearbeitet, d.h. für jedes neue Projekt wird ein kompetentes Team zusammengestellt, das nach abgeschlossener Aufgabe wieder aufgelöst wird.

In jeder Organisation finden also Umzüge statt. Diese Umzüge haben zur Folge, daß eine Infrastruktur zur Verfügung stehen muß, so daß ohne große Kosten, Aufwand und Wartezeiten, praktisch per Mausklick, ein Umzug realisiert werden soll. Solch eine Infrastruktur setzt eine strukturierte Verkabelung (Kap. 3.2.1) und ein entsprechendes Netzdesign (z.B. VLANs) voraus.

2.2 Aufgabenstellung

In dieser Diplomarbeit soll nun der Einsatz von virtuellen LANs an einem speziellen Beispiel und zwar am Gebäudekomplex Oettingenstraße analysiert werden. Der Gebäudekomplex Oettingenstraße gehört zur Ludwig-Maximilians-Universität.

Der Standort Oettingenstraße ist über das Leibnitz-Rechnerzentrum (LRZ) an das Münchner Hochschulnetz (MHN) angeschlossen (vgl. Abb. 2.2 und Kap. 7.1). Die Verbindung zwischen dem Gebäudekomplex Oettingenstraße und LRZ besteht aus einer 3 km langen 100 MBit Glasfaser. Dieses Gebäude besteht

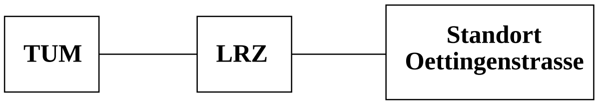


Abbildung 2.2: Teilausschnitt des MHN

aus 3 Stockwerken: Keller, Erdgeschoß und Obergeschoß und wird in mehrere Flügel eingeteilt. In diesem Gebäudekomplex sind mehrere Institute und die Bibliothek untergebracht, die alle mit eigenen EDV-Geräten (PC, Workstation, Drucker, Server) versorgt sind, aber über ein gemeinsames Backbone an des LRZ angekoppelt sind. Die Infrastruktur innerhalb des Gebäudekomplexes ist gemäß den Normen der strukturierten Verkabelung (siehe Kap. 6.1) aufgebaut. Die Verbindung zwischen den Etagen übernimmt ein Switch auf Ebene-2. Jedes Institut betreut sein eigenes Netz mit dediziert für sie zugewiesenen Komponenten. Diese Komponenten sind Eigentum vom LRZ und werden auch von diesem administriert.

Ziel dieser Diplomarbeit ist ein Design für die Strukturierung von intelligenten VLANs zu entwickeln, mit dem Ziel, den Einsatz der Komponenten zu minimieren und die Administration des Netzes zu optimieren. Aufgrund der VLAN-Szenarien (siehe Kap. 9) soll untersucht werden, ob durch gemeinsame Nutzung von Komponenten (Switches) und durch intelligenten Einsatz von VLANs, Komponenten eingespart werden können.

2.3 Aktivitäten

Die Diplomarbeit umfaßt fünf wichtige Stationen.

I. Eine Einführung in VLANs
   Zuerst werden die für die Diplomarbeit notwendigen technischen Grundlagen dargelegt. Insbesondere die technischen Voraussetzungen für den Einsatz von VLANs, wie strukturierte Verkabelung und geswitchtes Netz, werden genauer beschrieben. Anschließend werden die VLANs technisch untersucht, bzw. die verschiedenen VLAN-Techniken (Layer-1-VLAN, Layer-2-VLAN, Layer-3-VLAN und Policy-based-VLAN) definiert.

   Nachdem die grundlegenden technischen Voraussetzung betrachtet wurden, stellt sich die Frage nach der Vorgehensweise bei der VLAN-Implementierung. Bereits aus der allgemeinen VLAN-Beschreibung wird deutlich, daß es sich hier um ein sehr komplexes Gebilde handelt.

Eine mögliche Vorgehensweise bei der VLAN-Implementierung ist im folgenden Stufenplan dargestellt:

- Ist- und Anforderungs-Analyse ermitteln,
- VLANs am Einsatzort planen (aus organisatorischer und technischer Sicht) und
- Realisierung von VLANs (implementieren und betreiben).

II. Analyse-Phase
In der Analyse-Phase wird die Ist-Analyse bzgl. vorhandener Organisationsstruktur und Topologie und die Anforderungs-Analyse der Benutzer und Betreiber ermittelt.

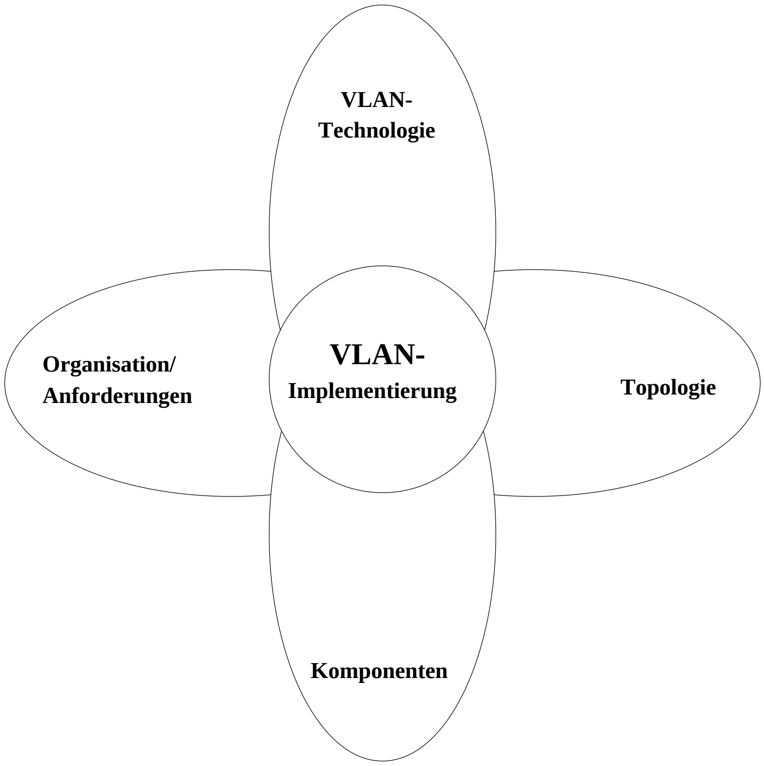


Abbildung 2.3: Entscheidungsmatrix für VLAN-Implementierung am Einsatzort

Der Aufbau eines virtuellen Netzes am Standort Oettingenstraße bedarf im Vorfeld einer genauen Vorbereitung. Mit einer VLAN-Implementierung zu beginnen, ohne eine intensive Vorbereitung voranzustellen, die auch alle Bereiche für diesen Einsatzort berücksichtigt, kann zu einer Verschlechterung im Netz und damit zu einer Unzufriedenheit der Benutzer und Betreiber führen. Folgende Bereiche (Abb. 2.3) müssen im Vorfeld untersucht und ermittelt werden: die bestehende Organisation, die Anforderungen der Benutzer, die Anforderungen der Betreiber, die vorhandene

Topologie und die verfügbaren VLAN-Technologien.
Um die Komplexität (Abb. 2.3) der Analyse-Phase am Einsatzort zu reduzieren, werden in den nachfolgenden Kapiteln alle notwendigen Bereiche genauer untersucht. Die Vorgehensschritte sind in Abb. 2.4 dargestellt.

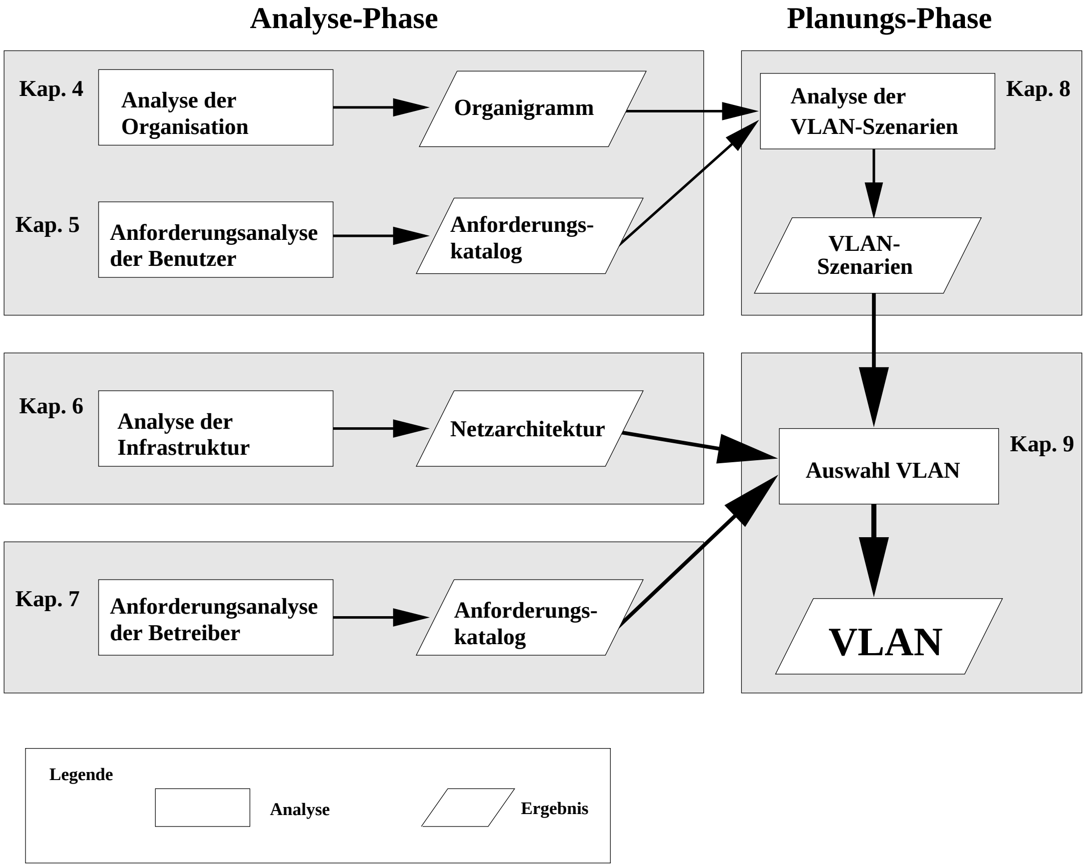


Abbildung 2.4: Analyse- und Planungs-Phase

III. Planungs-Phase
In der Planungs-Phase werden die verschiedenen VLAN-Szenarien (aus organisatorischer und technischer Sicht) aufgrund der Informationen aus der Analyse-Phase am Einsatzort ermittelt.

IV. Realisierungs-Phase
In der Realisierungs-Phase wird die VLAN-Technologie, die für diesen Einsatzort die meisten Vorteile bietet, genauer beschrieben. Hier wird konkret auf die Planung der Installation, Management-Aktivitäten und Schnittstellenbeschreibung zwischen LRZ und Einsatzort Oettingenstraße eingegangen.

V. Zusammenfassung
Die DA endet mit einer ausführlichen Bewertung, ob die VLAN-Technik

am Einsatzort auch sinnvoll ist.

Teil I

Eine Einführung in VLANs

Kapitel 3

Technische Grundlagen

3.1 VLANs und deren Voraussetzungen

Der Begriff des VLANs ist schon seit einigen Jahren bekannt. Es wird viel über dieses Thema gesprochen und geschrieben und VLANs fehlen auch in keiner Produktbeschreibung der großen Komponentenhersteller. Aber was ist nun ein VLAN wirklich?

Der Begriff VLAN (virtuelles lokales Netz) steht für die Trennung von physischer und logischer Netzstruktur. D.h. die virtuellen Netze erlauben es, die physische Struktur des Netzes und seine Systeme von der organisatorischen Zugehörigkeit der Mitarbeiter (und damit von der "logischen" Netzstruktur) zu trennen. Die Netzbenutzer bilden nicht mehr aufgrund ihres gemeinsamen Standortes eine Netzgruppe, sondern sie können mit den Kollegen zu einer Gruppe zusammengefaßt werden, mit denen sie tatsächlich zusammenarbeiten. Die Endgeräte der Benutzer werden zu logischen Gruppen zusammengefaßt, unabhängig von ihrem physischen Standort, und können miteinander kommunizieren als ob sie zum selben LAN gehören. Damit kann die Orts-Beziehung zwischen aktiven (Kap. 3.3) und passiven (Kap. 3.2.2) Komponenten aufgelöst oder - von höherer Ebene aus betrachtet - eine freiere Zuordnung von Benutzern zu Netzressourcen vorgenommen werden.

Die Gründe für den Zusammenschluß zu einer Interessensgruppe können organisatorischer oder technischer Art sein. Unter dem Aspekt der Unternehmensorganisation ist es z.B. möglich, alle Mitarbeiter einer Abteilung in eine Netzgruppe zusammenzufassen, auch wenn sie auf verschiedenen Etagen verteilt sind. Unter dem Aspekt der Arbeitsorganisation können Mitarbeiter, die gemeinsam an einem Projekt arbeiten, zu einer Netzgruppe zusammengefaßt werden, auch wenn sie zu verschiedenen Abteilungen gehören. Unter Performance-Aspekten können Mitarbeiter, die besondere Anforderungen an die Bandbreite oder Quality-of-Service (QoS) stellen, zu einer Netzgruppe zusammenfassen. Diese Anforderungen können mit Hilfe von virtuellen Netzen realisiert werden.

Durch die Zuordnung der Endgeräte zu logischen Gruppen (VLANs) beschränkt sich der Datenverkehr eines logischen Netzes auf eine Broadcastdomain. Jedes VLAN bildet also eine eigene, unabhängige Broadcastdomain, in der die Teilnehmer über geswitchte Strukturen auf Ebene 2 gekoppelt werden. Der Anwender hat u.U. die Möglichkeit, sein Endgerät an jedem beliebigen Ort innerhalb des Netzes anzuschließen, ohne daß er die Zugehörigkeit zu seinem VLAN verliert. Werden die Mitglieder eines VLANs über mehrere Switches verteilt, so steigt in der Praxis der Datenverkehr zwischen diesen Komponenten erheblich. Aus diesem Grund muß in dem Konzept der Switches die Möglichkeit einer adäquaten Backbone-Skalierbarkeit und der Broadcast-Reduzierung integriert sein. Die Kommunikation zwischen Teilnehmer unterschiedlicher VLANs erfolgt über Router auf Ebene 3.

Was verbirgt sich nun hinter den VLANs technisch und welche Voraussetzungen müssen erfüllt sein? Diese Frage wird in den nachfolgenden Kapiteln genauer untersucht. In Kap. 3.2 und 3.3 werden die Anforderungen der passiven und aktiven Netzkomponenten für den Einsatz von VLANs beschrieben und in Kap. 3.4 werden die unterschiedlichen VLANs definiert. Im Kapitel 3.5 werden die einzelnen Verfahrenstechniken, die zur Übertragung der VLAN-Informationen zwischen den Transitsystemen zur Auswahl stehen, beschrieben.

3.2 Normgerechte Verkabelung

Die heutigen Anforderungen an ein modernes Kabelsystem beinhalten die Übertragung von Sprach-, Daten-, Ton-, und Bildinformation durch ein einheitliches System an allen Arbeitsplätzen. Dieses Verkabelungssystem hat in der Regel eine Nutzungsdauer von 10 bis 15 Jahren. Das heißt, in diesen Jahren soll das Kabelsystem mit dem technischen Fortschritt Schritt halten. Mit Blick auf die Vergangenheit wird deutlich, daß so etwas nicht beeinflußbar ist, auch wenn hohe Kosten in die Investitionen von z.T. normgerechten Kabelsystemen in Kauf genommen werden. Als klassische Beispiele sind hier die sternförmige Koaxverkabelung, sternförmige ISDN-Verkabelung (für DV-Bildschirme), Yellow-Cable und Cheapernet sowie das IBM-Verkabelungssystem zu nennen. Keines dieser Verkabelungssysteme hat mehr als 10 Jahre die Anforderungen der Nutzer erfüllt. Die Begründung für die Ablösung sind im wesentlichen:

- herstellerspezifisch (IBM Koax),
- spezifisch für ein Übertragungsverfahren (Cheapernet, Yellow-Cable),
- zu geringe Datenrate je Benutzer (Cheapernet , ISDN-Verkabelung)
- zu geringe Datenrate als Backbone-Systeme (Yellow-Cable).

Im allgemeinen gilt, daß der Planungshorizont von passiven Netzen sich von dem für die aktiven Netzkomponenten unterscheidet. Für den Einsatz von aktiven Netzkomponenten plant man in der Regel 3 bis 5 Jahre. Das passive Netz muß somit zwei bis drei Komponentengenerationen überleben. Diese Sicherheit erhält der Anwender nur durch den Einsatz von genormten Verkabelungssystemen und standardisierten Übertragungs-Protokollen.

Dazu kommt noch, daß die lokalen Netze einem ständigen Wandel unterliegen. Dieser Wandel wird bedingt durch:

- die ständige Anpassung an neue Technologien (ATM[1], Fast Ethernet, Gigabit Ethernet),
- die unterschiedlichen Strömungen im Netzdesign,
- die wechselnden Anforderungen der Benutzer,
- die Expansion des Netzes,
- die Migration zu modernen Netzen, etc.

Die Basis für einen ständigen Wandel ist ein maßgeschneidertes Kommunikationsnetz, das genügend Flexibilität und Bandbreite zur Verfügung stellt. In vielen Fällen wird der Einsatz von einer strukturierten Verkabelung (Kap. 3.2.1) als ausreichend angesehen, wichtig sind aber auch die Eigenschaften der aktiven Komponenten. Die optimalen Ergebnisse werden nur dann erzielt, wenn sowohl die passiven als auch die aktiven Netzkomponenten aufeinander abgestimmt sind.

Um moderne Netzarchitekturen aufzubauen und zu betreiben, muß ein grundlegendes Wissen über die normgerechte Verkabelung vorliegen. Die normgerechte Verkabelung beinhaltet im wesentlichen

- die strukturierte Verkabelung und
- die Kabeltypen.

Deshalb soll in diesem Kapitel auf diese Bereiche besonders eingegangen werden.

3.2.1 Strukturierte Verkabelung

Die strukturierte Verkabelung wurde von ISO definiert und in der "ISO/IEC DIS 11801 Universelle Verkabelung für den Gebäudekomplex" dargelegt. Diese Norm schreibt vor, daß eine moderne Verkabelung stets nach einem festgelegten Muster erfolgt und so die notwendige Flexibilität für die Netzbetreiber garantiert. Das wesentliche Merkmal einer strukturierten Verkabelung ist die Schaffung einer dienstneutralen Infrastruktur. Das heißt, die Art des Kabels und die verwendete Struktur garantieren:

- die Nutzung aller bekannten Protokolle,
- den Einsatz von allen Technologien (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM),
- den Einsatz von verschiedenen Diensten (ISDN, SNA).

Die gesamte Kommunikations-Infrastruktur der Verkabelung (Abb. 3.1) wird daher von der Normung unterteilt in die Bereiche:

[1] Asynchronous Transfer Mode

- Primärbereich
- Sekundärbereich
- Tertiärbereich

Schon heute ist abzusehen, daß auch in den nächsten Jahren diese strukturierte Verkabelung Gültigkeit haben wird. Sie bietet die nötige Flexibilität und Neutralität für die unterschiedlichen Dienste, ist also dienstneutral. Dienstneutral bedeutet, daß über eine einzige Infrastruktur, bestehend z.B. aus LWL im Sekundärbereich und Kupferkabel im Tertiärbereich alle Dienste zum Teilnehmer übertragen werden können.

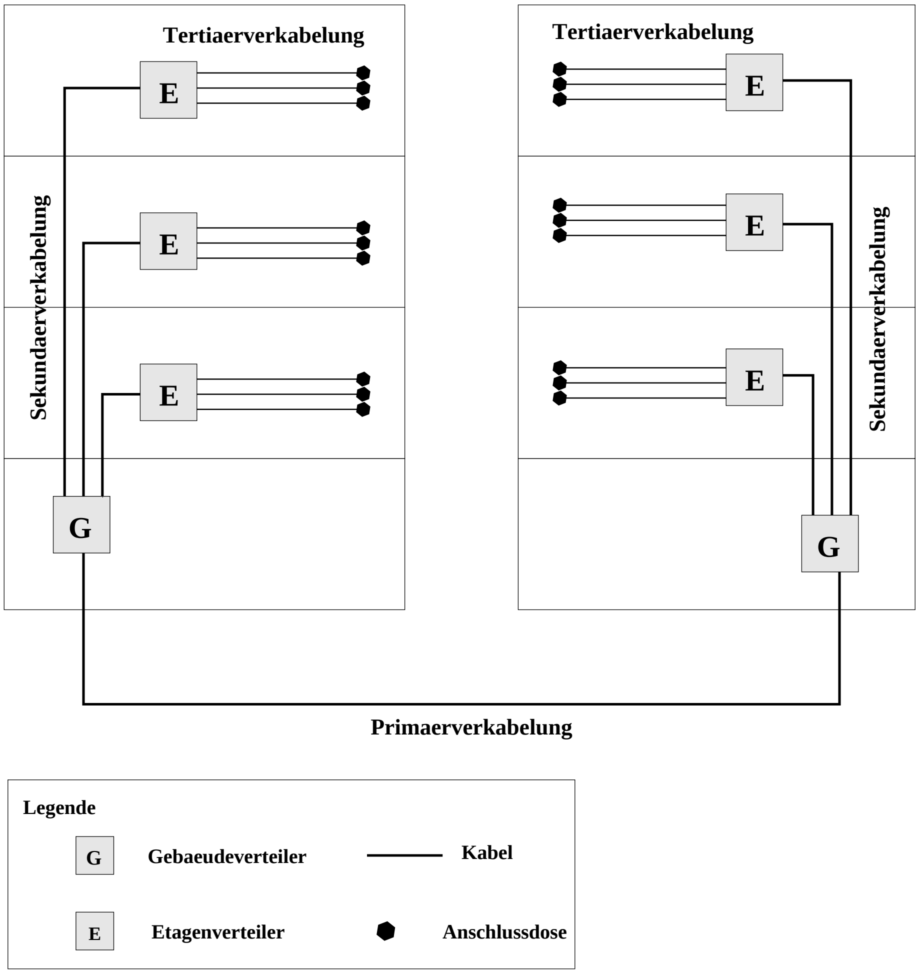


Abbildung 3.1: Strukturierte Verkabelung

Primärverkabelung

Als Primärverkabelung versteht man eine gebäudeübergreifende, firmenweite

Standortverkabelung zur Verbindung der Standort- bzw. Gebäudeverteiler. Dabei wird meistens im Rechenzentrum der Standortverteiler untergebracht und von da aus führen ein oder mehrere Kabel zu den entsprechenden Gebäudeverteilern. Das heißt, an einem Knoten können viele Verbindungen angeschlossen werden (die Etagenverteiler, die Gebäudeverteiler). Hierbei muß darauf geachtet werden, daß diese Struktur keinen "Single Point of Failure" besitzt. Um eine permanente Verfügbarkeit zu garantieren, sollte der Primärbereich redundant ausgelegt sein.
Für den Primärbereich verwendet man die Topologie Stern oder Ring und im allgemeinen LWL-Kabel. Der Grund warum LWL-Kabel vorteilhafter sind als Kupferkabel, wird in Abschnitt 3.2.2 erklärt.

Sekundärverkabelung
Unter Sekundärverkabelung versteht man die Verbindung zwischen den Gebäude- und Etagenverteilern. Dieser Bereich wird häufig auch Steigbereich genannt. Im Sekundärbereich können die Kabel entweder ringförmig oder sternförmig als Punkt-zu-Punkt-Verbindung gelegt werden. Auch hier empfiehlt sich der Einsatz von LWL-Kabeln, wie in 3.2.2 erläutert. Bei der Planung des Sekundärbereichs ist zu berücksichtigen, daß die Verkabelung ausreichend groß dimensioniert ist, da eine spätere Erweiterung mit großem Aufwand und mit hohen Kosten verbunden ist.

Tertiärverkabelung
Unter Tertiärverkabelung versteht man die Verbindung von den Etagenverteilern zu den Anschlußdosen. Im Tertiärbereich wird hauptsächlich symmetrisches Kupferkabel eingesetzt. Aber auch eine reine LWL-Verkabelung bis zur Anschlußdose ist möglich. Unabhängig vom Kabeltyp wird immer eine sternförmige Verkabelung realisiert.

Arbeitsplatzverkabelung
Unter Arbeitsplatzverkabelung versteht man die Verbindung von den Anschlußdosen zu den Endgeräten. Die Arbeitsplatzverkabelung wird nicht bei der Netzinstallation fest eingerichtet, sondern wird in der Regel erst bei einem notwendigen Netzanschluß von den betroffenen Netzadministratoren angeschlossen. Für diese Verbindung verwendet man hauptsächlich Patchkabel.

3.2.2 Kabeltypen

Mit wachsenden Aufgaben des Netzes ändern sich auch die Anforderungen an die Verkabelungssysteme. Die neuen Einsatzgebiete stellen immer höhere Anforderungen und der Bandbreitenbedarf steigt ständig. Für jeden Einsatzbereich sollte daher die Auswahl des Kabeltypes sehr sorgfältig überprüft werden. Wie in der strukturierten Verkabelung schon erwähnt wurde, beschränkt sich ein modernes Netz auf zwei Kabeltypen: LWL-Kabel und Kupferkabel. Während im Primärbereich und Sekundärbereich vorwiegend Glasfaser zum Einsatz kommt, wird im Tertiärbereich derzeit noch das Kupferkabel favorisiert.

Kupferkabel

Bei einer Tertiärverkabelung werden ausschließlich Kabel mit mehrfach verdrillten Leiterpaaren, sogenannten Twisted-Pair-Kabel, installiert. Diese Kabel werden schon seit einigen Jahren als Übertragungsmedium eingesetzt. Ursprünglich wurde das Twisted-Pair-Kabel im Fernmeldebereich eingesetzt. Der Durchbruch in der Computerwelt kam erst zu Beginn der 80er Jahre mit der steigenden Zahl vernetzter PCs und den steigenden Anforderungen an die Flexibilität der Verkabelung. Die wachsende Leistungsfähigkeit der Twisted-Pair-Kabel hat dazu geführt, daß sie die übliche Koax-Verkabelung ablöste. Twisted-Pair-Kabel weisen aufgrund ihrer Verdrillung eine hohe Störunterdrückung auf, die auf der Umkehrung der magnetischen Felder beruht. Die Kabel werden entsprechend ihrer Leistungsfähigkeit in "Kategorien" unterteilt. Dabei werden an jede Kategorie aufsteigend immer höhere Anforderungen bzgl. der Performance bei bestimmten Frequenzen gestellt. Folgende Industriestandards wurden entwickelt:

- Kat 3 : Bandbreite bis 16 MHz
- Kat 4 : Bandbreite bis 20 MHz
- Kat 5 : Bandbreite bis 100 MHz
- heute kurz vor Verabschiedung Kat 6 : Bandbreite bis 200 MHz
- heute kurz vor Verabschiedung Kat 7 : Bandbreite bis 600 MHz

Lichtwellenleiter (LWL)

Glasfaserverkabelung wird hauptsächlich im Primärbereich, also über größere Entfernungen, und im Steigbereich zu den Etagenverteilern (Inhouse-Verkabelung) eingesetzt. In manchen Fällen wird Glasfaser bis hin zum Arbeitsplatz (FTTD Fibre To The Desk) verlegt.

Der LWL besteht aus zwei Grundelementen: dem Kern und dem Mantel, jeweils aus optisch transparentem Material (z.B. Quarzglas), und der Beschichtung. Der Kern ist der zentrale Bereich des LWL, der zur Lichtwellenführung dient. Man unterscheidet zwei Fasertypen: Multimode mit Stufenprofil und Gradientenprofil ($50\mu, 62,5\mu$), und Monomode ($9\mu, 10\mu$). Der Unterschied liegt in der Anzahl der zu übertragenden Moden und demzufolge in der Übertragungsrate (Bit pro Sekunde). Mit einer 62,5-Multimodefaser lassen sich im Falle von ATM bis OC-12 (622 MBit pro Sekunde) sowie Gigabit Ethernet gemäß dem 1000Base-LX-Standard bis zu einer Distanz von 500m nutzen. Bei diesen Entfernungen sind allerdings die Kapazitäten von Multimodefasern ausgeschöpft. Der begrenzte Faktor ist hier das Bandbreitenprodukt, eine Maßzahl für das Verhältnis zwischen Entfernung und zu übertragender Frequenz auf dem LWL-Kabel. Ein wesentlich höheres Bandbreitenprodukt bieten Monomodefasern, über die sich im Gigabit Ethernet entsprechend dem 1000Base-LX-Standard über einen Link von 2000m übertragen läßt. Deswegen wird Multimode-LWL hauptsächlich für Inhouse-Verkabelungen und kurze Campus-Strecken und Monomode-LWL bei großen Entfernungen (Primärbereich) eingesetzt. Grundsätzlich sollte unabhängig von der gewählten Faser genügend Reservefaser berücksichtigt werden

und redundante Kabelwege eingeplant werden.
Die Vorteile von LWL:

- Die Photonen in einer Glasfaser beeinflussen sich nicht gegenseitig und werden auch nicht von externen Photonen beeinflußt (kein Nebensprechen).
- Die Glasfaser kann hohe Bandbreiten unterstützen.
- Bei Stromausfällen, elektromagnetischen Störungen oder Stromstößen wird die Glasfaser nicht beeinflußt.

Die Nachteile von LWL:

- LWL ist sehr aufwendig zu verlegen.
- Die Kabelpreise sind marginal teurer, aber die Verlegung erheblich teurer als beim Kupferkabel.
- Die Komponenten, die an ein LWL angeschlossen werden, sind teuer.

Mit beiden Kabeltypen können Hochleistungsverkabelungssysteme aufgebaut werden. Zum Beispiel: bei einem Bandbreitenlängenprodukt von 600 bis 800 MHz*km in den optischen Fenstern 850nm und 1300nm liefert Glasfasertechnik mit 1,2 bis 1,6 GBit pro Sekunde über 500m etwa die gleiche Übertragungsrate wie die Kupfertechnik bei 100m. Dabei wird deutlich, daß Kupfertechnik und Glasfasertechnik hinsichtlich der möglichen Datenübertragungsrate gleichwertig sind. Der nutzbare Vorteil von Glasfaser liegt in der größeren zu überbrückenden Entfernung.

Norm
Ziel einer Normierung ist, einer breiten Gruppe von Anwendern durch Bezug auf die Norm die Sicherheit zu geben, daß die neuen Technologien auf diese Normen aufbauen. Reichen dann die Anforderungen nicht aus, wie z.B. bei Gigabit Ethernet über Kat.5, werden neue Normen wie Kat.6 und Kat.7 entwickelt.
Der Einsatz von normgerechten passiven und aktiven Komponenten minimiert weiterhin die Fehlerhäufigkeit bei Störungen aller Art (Schnittstellenproblematik, Kompatibilität, Einhaltung der Längenrestriktion, etc.).

Die "Normpyramide" in Abb. 3.2 zeigt: je internationaler eine Norm plaziert wird, desto weitreichender waren die Kompromisse, die zu ihrer Verabschiedung eingegangen sind.
Die Europäische Norm EN 50173 ist besonders wichtig. Sie beinhaltet:

- die Anforderungen für die Realisierung (Errichtungsanforderungen)
- die Leistungsanforderungen an die Verkabelungsstrecken sowie an die Komponenten
- die Konformitätsanforderungen sowie die Meßverfahren zur Überprüfung

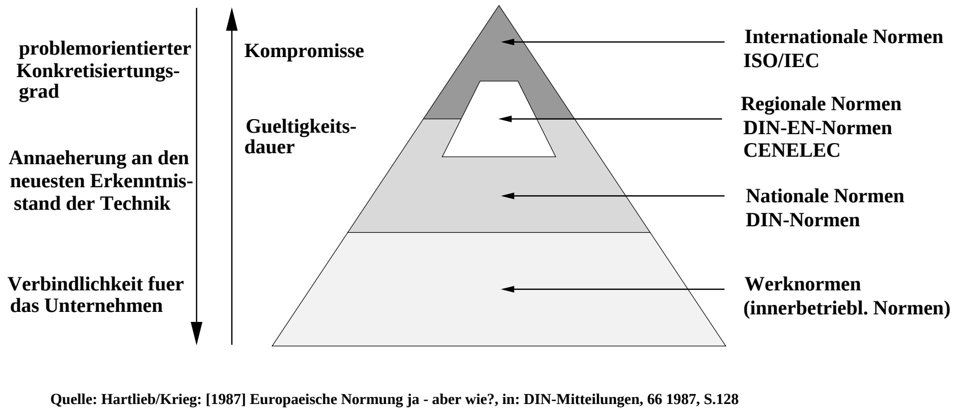


Abbildung 3.2: Die “Normpyramide”

- die Anforderungen an die Sicherheit (elektrisch, Brandschutz) und an die elektromagnetische Verträglichkeit
- die Struktur eines universellen Verkabelungssystems sowie die Auswahl der zugehörigen Kabel

Neben einer flexiblen, normgerechten Verkabelung ist auch eine leistungsfähige Übertragungstechnologie notwendig, um VLANs optimal einsetzen zu können. Im anschließenden Kapitel wird die Frage beantwortet: “Was bedeutet Switching für Netze?”, darüberhinaus wird die Arbeitsweise und Fähigkeiten der Switches beschrieben.

3.3 Switches

Switches sind Netzkomponenten die auf der Schicht 2 des ISO/OSI-Referenzmodells arbeiten. Sie werden eingesetzt für eine schnelle und effiziente Koppelung zwischen mehreren LAN-Teilnetzen. Auf der Schicht 2 wird mit MAC-Adressen gearbeitet. Grundsätzlich kann die Arbeitsweise von einem Switch mit der einer Transparent Bridge incl. Spanning Tree (im Ethernetbereich) oder Source Route Bridge (für Token Ring Netze) verglichen werden.
Im Gebäudekomplex Oettingenstraße wird nur Ethernet als Technologie eingesetzt, deswegen beschränken wir uns in dieser Diplomarbeit auf die Ethernet-Switches.

Switches bieten den Vorteil den Verkehr zu separieren. Sie erkennen, ob es sich bei einem Datenpaket um teilnetzübergreifenden oder teilnetzlokalen Verkehr handelt. Dementsprechend wird das Paket weitergeleitet oder nicht. Um diese Entscheidung treffen zu können muß ein Switch “lernen”, welche MAC-Adresse zu welchem Teilnetz gehört. Jeder Switch führt eine Adreßtabelle, in der jede MAC-Adresse und der dazugehörige Ausgangsport gespeichert ist. Hierzu liest der Switch zu jedem an einem Port eingegangenen Frame die Source-Adresse ein und überprüft, ob diese in der Adreßtabelle schon gespeichert ist. Wenn nein, merkt sich der Switch an welchem Port der Frame eingegangen ist und speichert die Information: MAC-Adresse - Port. Somit kann zu einem späteren Zeitpunkt die Zuordnung Destination-Adresse und Ausgangsport jederzeit abgefragt und zur Entscheidung der Weiterleitung herangezogen werden.

Innerhalb eines Switches gibt es verschiedene Verarbeitungsmechanismen: "Cut Through"- und "Store and Forward"-Switching.

- Cut Through-Switching :
  Beim Cut Through-Switching (siehe Abb. 3.3) wird die Zieladresse DA (ersten 6 Bytes) des MAC-Frames ausgelesen und in der gespeicherten Adreßtabelle die Zuordnung dieser Zieladresse zu dem entsprechenden Ausgangsport bestimmt. Danach werden die Datenpakete, ohne weitere Überprüfung und z.T. noch bevor das letzte Bit des Frames eingegangen ist, an den Ausgangsport weitergeleitet. Eine Überprüfung des CRC[2]-Feldes kann erst nach Ausgabe der ersten Bytes (DA, SA, ..) stattfinden. Dadurch erhält man zwar kurze Verzögerungszeiten, aber fehlerhafte Frames werden ebenso weitergeleitet.

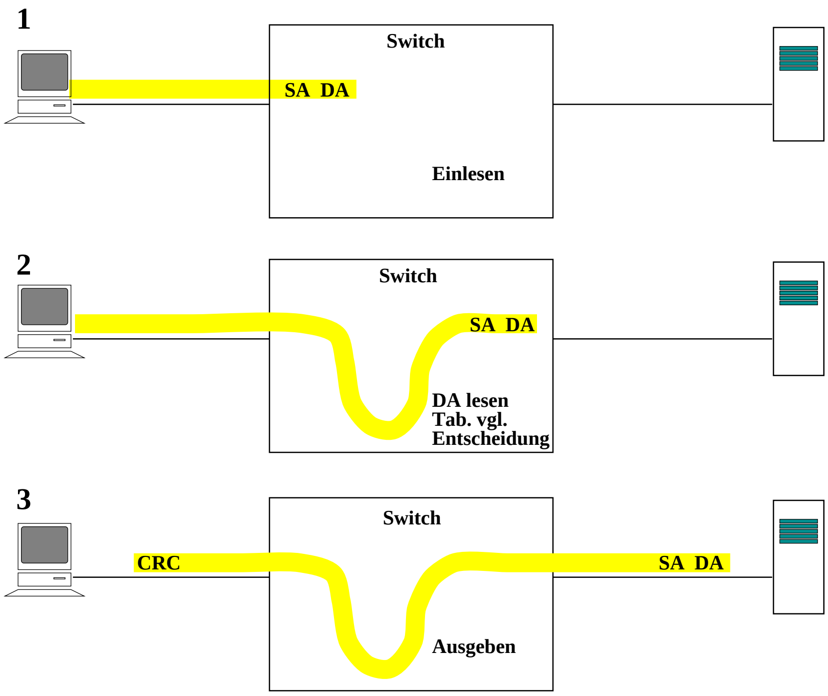


Abbildung 3.3: Cut Through-Switching

- Store and Forward-Switching
  Beim Store and Forward-Switching (siehe Abb. 3.4) wird dagegen der

[2]Cyclic Redundancy Checksum, zyklische Blockprüfung bei bitorientierten Prozeduren (Ethernet, HDLC, X.25, etc.)

gesamte MAC-Frame eingelesen und zwischengespeichert, um zunächst alle Steuerinformationen interpretieren zu können. Durch das Einlesen des kompletten Frames können Bitfehler identifiziert und damit fehlerhafte Frames verworfen werden. Dieser Mechanismus hat in der Regel eine längere Verzögerungszeit zur Folge. Store and Forward-Switching ist immer dann notwendig, wenn ein Sicherheitscheck durchgeführt werden soll, oder unterschiedliche Geschwindigkeiten (z.B. 10 Mbit/s zu 100 Mbit/s) angeglichen werden müssen.

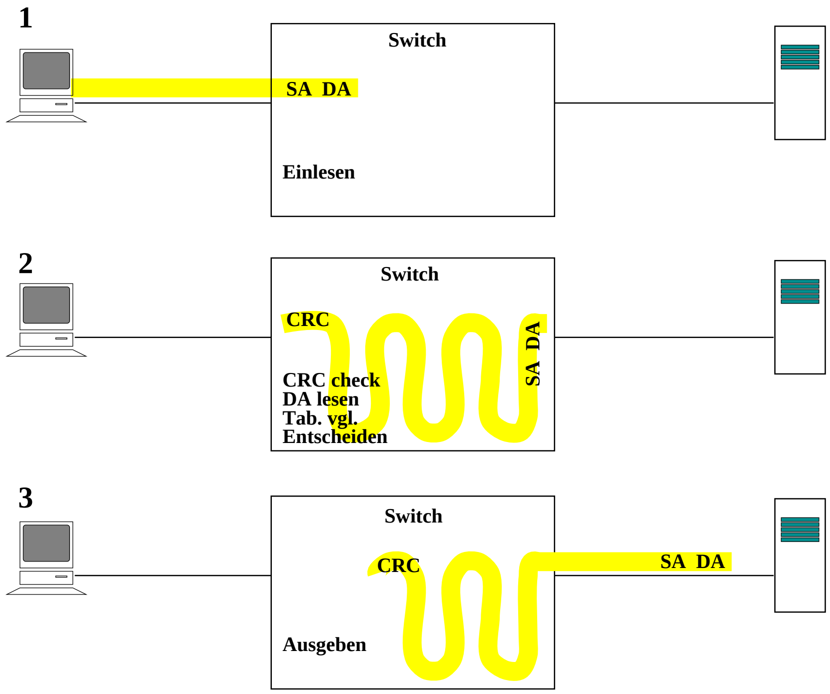


Abbildung 3.4: Store and Forward-Switching

Ein Switch wird bestimmt durch:

1. die Art des Gerätes (modular, stackable, stand alone)
2. die Art der Verarbeitungsmechanismen (Cut-Through, Store and Forward)
3. die Art der internen Übertragung (blocking, non blocking)
4. die Anzahl der zu verwaltenden MAC-Adressen pro Gerät/Port
5. die Art der unterstützenden Technologie (Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, Token Ring)
6. Anzahl der Ports (von einem Workgroup-Switch mit 8 Ports bis zu einem Enterprise-Switch mit über 100 Ports)

7. die unterstützte Geschwindigkeit pro Port
8. die Uplink-Ports (Anbindung an den Backbone)
9. die unterstützten VLAN-Typen
10. die Art des unterstützten Managements (Protokolle, MIBs)
11. die Kompatibilität mit Switches anderer Hersteller (Standards)

Um virtuelle Strukturen in einem unternehmensweiten LAN einzuführen, müssen weitere Bedingungen erfüllt sein, um einen reibungslosen, schnellen und erfolgreichen Datenverkehr zu ermöglichen. Dabei ist zu beachten, daß sich die Anforderungen nicht mehr nur auf Einzelsysteme beziehen, sondern auf das Zusammenspiel mit anderen Geräten im Netz. Die Switches müssen miteinander kommunizieren und Informationen austauschen, um einen korrekten Datenverkehr in einem VLAN zu gewährleisten. Für die Übertragung von VLAN-Informationen zwischen den Switches werden folgende Lösungen angeboten:

- Austausch von Adreßtabellen
- Tagging auf MAC-Ebene
- Time Division Multiplexing
- ATM

In Kap. 3.5 werden diese Techniken ausführlich beschrieben. Switches erlauben verschiedene Zuordnungen von Endgeräten zu einem VLAN. Diese Möglichkeiten werden in den nachfolgenden Kapiteln beschrieben.

3.4 Unterschiedliche VLAN-Konzepte

Der allgemeine Begriff von VLANs, die Trennung von physischer und logischer Netzstruktur, wurde im obigen Kapitel beschrieben. Die VLAN-Definition muß aber noch konkretisiert werden, um eine genaue Vorstellung über die Leistungsmerkmale zu erhalten.
Zunächst besteht die Notwendigkeit, die Menge der Nutzer eines LANs in VLAN-Gruppen aufzuteilen. Dazu müssen Regeln geschaffen werden, mit deren Hilfe die Nutzer in die jeweiligen VLANs zugewiesen werden. Hierbei sind verschiedene Ansätze realisiert.
Die Zuordnung der Endgeräte zu VLANs kann auf unterschiedliche Art und Weise erfolgen. Jede Variante hat hierbei andere Auswirkungen auf das Netzdesign.
Folgende Zuordnungsvarianten können gewählt werden:

- der Switch Port,
- die MAC-Adresse des angeschlossenen Endgerätes,

- das benutzte Network-Layer Protokoll (IP, IPX, Appletalk, NetBIOS, DECnet, Banyan Vines, etc.),
- die verwendeten Anwendungen (Services),
- die verschiedenen Kombinationen.

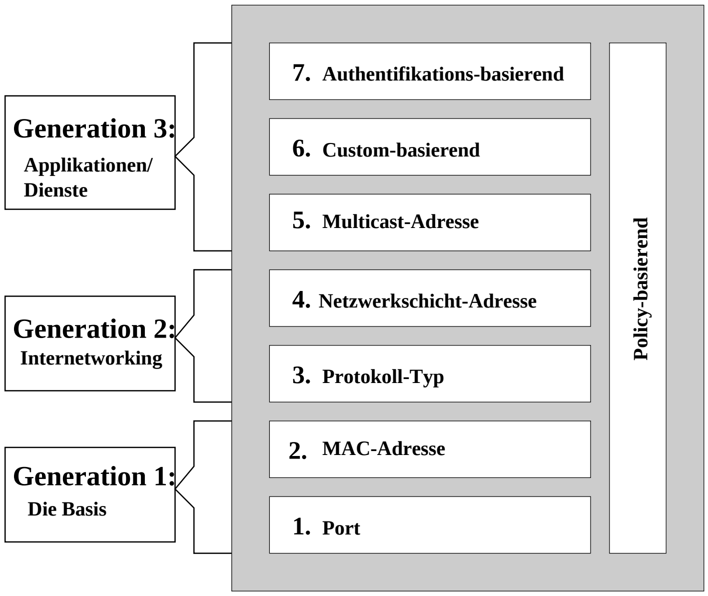


Abbildung 3.5: VLAN-Kriterien für den Aufbau

Der Aufbau eines VLANs (Abb. 3.5 aus [11]) erfolgt also nach unterschiedlichen Kriterien, die sich vom ISO-OSI-Referenzmodell, Schichten 1 bis 7 erstrecken. In der Regel unterscheidet man drei verschiedene Gruppen von VLANs.
Zu der ersten Gruppe zählen VLANs, bei denen die Zuordnung der Teilnehmer auf Basis von Ports oder von MAC-Adressen erfolgt. Diese VLANs werden von den meisten Herstellern unterstützt.
Die zweite Gruppe, die auch als "Internetworking-VLANs" bekannt sind, werden auf Basis der übergeordneten Protokolle (Network Protocol) oder logischen Netzadresse (Network Layer Adress) gebildet. Diese VLANs bieten mehr Funktionalität als die Gruppe 1, werden aber nur von wenigen Herstellern unterstützt.
Die VLANs der Gruppe drei verfügen z.Zt. über die umfassendsten und leistungsfähigsten Eigenschaften. Üblicherweise werden diese VLANs auf Multicast-Adressen, kundenspezifisch festgelegten Definitionen oder der Anwender-Authentifikation, festgelegt.
Die Kombination aus diesen drei Gruppen bildet die Policy-basierenden VLANs.

Diese VLAN-Typen können teilweise innerhalb der Gruppen noch weiter untergliedert werden und bieten verschiedene Leistungsmerkmale. Bei einer Netzplanung erfordern diese VLAN-Typen unterschiedlich großen Aufwand (siehe

Kap.9). Welche der möglichen Varianten die geeigneteste ist, hängt neben den konkreten Anforderungen auch von der ausgewählten Technik ab.
In den nachfolgenden Abschnitten werden die am meist verbreiteten VLAN-Typen auf ihre Merkmale untersucht.

3.4.1 Layer-1-VLANs

Die Layer-1-VLANs oder portbasierte-VLANs werden von einer Reihe von Herstellern unterstützt und werden auch im zukünftigen VLAN-Standard (IEEE 802.1Q) vorgesehen. Die Layer-1-VLANs bilden die einfachste Form von virtuellen LANs und sind bekannt seit dem Aufkommen von sogenannten Portswitching- Hubs.

Zuordnung der Endgeräte
Die Layer-1-VLANs oder portbasierten VLANs gehen im Prinzip von einer starren Anweisung aus. Es ist ein geradliniges Modell, das die physischen LANs virtualisiert.
Bei den portbasierten VLANs werden, wie die Bezeichnung schon andeutet, die Switch-Ports einzelnen VLANs zugewiesen. Jeder Port ist Teilnehmer von einem (oder mehreren) VLANs, so daß alle Stationen, die an diesem Port angeschlossen sind, automatisch diesem VLAN zugeordnet werden.
Zur anschaulichen Darstellung wird jedem VLAN eine eindeutige Farbe zugewiesen. Alle Endgeräte, die an diesem Port angeschlossen werden, gehören zum selben VLAN, besitzen also dieselbe Farbe. Wird ein Hub an einen Port angeschlossen, so bekommen alle am Hub hängenden Endgeräte die Farbe vom entsprechenden Port, bzw. gehören zum selben VLAN. Die Anbindung von Shared-Media-Hubs mit nur einem Segment hat zur Folge, daß alle daran angeschlossenen Endgeräte sich im selben VLAN befinden.
Diese Beschreibung ist zum besseren Verständnis in Abb. 3.6 grafisch dargestellt.

Hardware-Voraussetzung
Mit Hilfe von Layer-2 Switches werden die portbasierten VLANs aufgebaut. Dabei lernt der Switch selbständig, welche MAC-Adresse an welchem Port angeschlossen ist und damit, zu welchem VLAN sie gehört. Diese Informationen werden in einer zentralen Adreßtabelle gespeichert. Switches bieten den Vorteil, daß der Datenverkehr auf seine VLAN-Zugehörigkeit analysiert werden kann. Durchläuft ein MAC-Frame den Switch, wird neben der Destination-Adresse auch die Source-Adresse gelesen. Nun überprüft der Switch in seiner Adreßtabelle, ob die Destination-Adresse im gleichen VLAN liegt wie die Source-Adresse. Ist dies der Fall, so wird der Frame an einem entsprechenden Ausgangsport ausgegeben. Andernfalls findet der Switch entweder die Destination-Adresse nicht oder der Empfänger ist Mitglied eines anderen VLANs. Dann wird der Frame verworfen, da nur lokaler VLAN-Verkehr zugelassen wird.

VLAN-1-Management
Die Layer-1-VLANs lassen sich in der Regel sehr leicht in bestehende Netze

implementieren. Weitere Vorteile liegen auf der Hand. Die Fehlersuche wird vereinfacht, da eine direkte Zuordnung der VLANs zu den physischen Ports bekannt ist.
Der Umzug einer Station an einen anderen Switchport macht unter Umständen die Umkonfiguration dieses Ports zum gewünschten VLAN erforderlich. Ein automatisierter Umzug ist daher nur eingeschränkt möglich. Die portbasierten VLANs bieten wenig Flexibilität in der Wahl des Standortes. Wenn die Mitglieder eines VLANs über mehrere Standorte verteilt sind, ist ein VLAN mit Portzuweisung wenig effektiv.

Beispiel
Das Beispiel in Abb.3.6 veranschaulicht nochmal die oben genannten Punkte. In Abb.3.6 ist ein geswitchtes Teilnetz dargestellt. Der Switch Nr.1 dient als

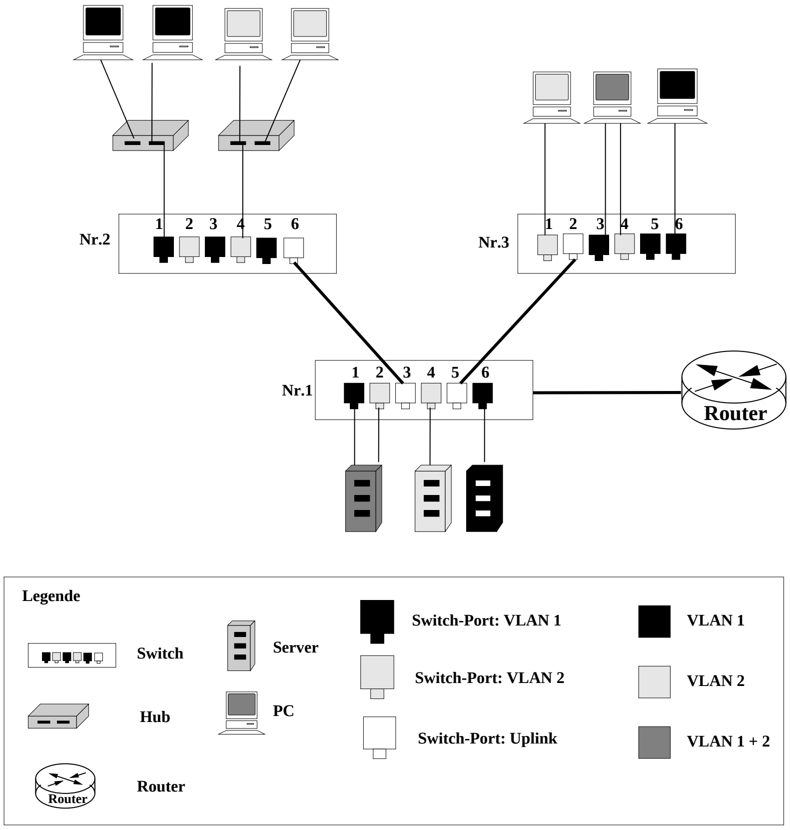


Abbildung 3.6: Beispiel mit Layer-1-VLANs

Gebäudeverteiler und Switch Nr.2/Nr.3 dienen als Etagenverteiler. Alle Server befinden sich an einer zentralen Stelle, sie bilden einen sogenannten Server-Pool und werden direkt an den Gebäudeverteiler angeschlossen. Für dieses Teilnetz existieren drei logische VLAN-Gruppen: VLAN 1 (Farbe: schwarz), VLAN 2 (Farbe: hellgrau) und VLAN 1+2 (Farbe: dunkelgrau). Die Endgeräte (PCs und Server) werden diesen drei VLAN-Gruppen zugeteilt. Endgeräte die Mit-

glied von VLAN 1 und von VLAN 2 sind, gehören zum VLAN 1+2. Nach der Zuordnung der Endgeräte zu ihren VLANs (Endgeräte werden mit entsprechender Farbe markiert), müssen sie an die Switches angeschlossen werden. Jeder Teilnehmer bekommt die gleiche Farbe wie sein Switch-Port, er wird also explizit für ein VLAN zur Verfügung gestellt.
Am Switch Nr.2 hängt am 1-ten Port (Farbe: schwarz) ein Hub. Alle Endgeräte die nun an diesen Hub angeschlossen werden, sind nun automatisch im selben VLAN (hier VLAN 1). Soll ein Teilnehmer mehreren VLANs zugeordnet werden, muß der Switch eine Mehrfach-VLAN-Zuordnung pro Port unterstützen. Die in der Oettingenstraße eingesetzten Komponenten unterstützen dieses Feature nicht. Hier stellt die Zuweisung mehrerer VLANs zu einem Endgerät bei den portbasierten VLANs eine besondere Herausforderung dar. Die einfachste Form ein Endgerät verschiedenen portbasierten VLANs (VLAN 1 und VLAN 2) zuzuweisen, kann durch den Einsatz von mehreren Netzkarten realisiert werden. Diese Netzkarten werden in das entsprechende Endgerät (z.B. linker Server) eingebaut und dann auf die verschiedenen VLAN-Ports geschaltet. Somit ist der Server Mitglied von VLAN 1 und VLAN 2. Die Verbindung zwischen den Switches wird mit Hilfe eines Uplink-Ports (Farbe: weiß) realisiert. Durch dieses Feature ist es möglich, Daten von verschiedenen VLANs (VLAN 1 und VLAN 2) über eine gemeinsame Leitung zu übertragen.
Die portbasierten VLANs werden im Kap.9.1 am konkreten Beispiel des Gebäudekomplexes Oettingenstraße nochmals erläutert.

3.4.2 Layer-2-VLANs

Zuordnung der Endgeräte
Layer-2-VLANs werden auf Basis von MAC-Adressen gebildet. Jede Station (Netzkomponente, Endgerät, etc.) hat eine MAC-Adresse. Die MAC-Adresse ist eine, auf der Adapterkarte eingestellte, nicht veränderbare, eindeutige, festverdrahtete Adresse. Ein Layer-2-VLAN besteht nun aus einer Gruppe von MAC-Adressen, die jeweils eine Broadcast Domain bilden (= VLAN). Die Zuordnung der Stationen zu einem VLAN erfolgt durch Eintragung der jeweiligen Station-MAC-Adresse in die VLAN-Tabelle. In Abb. 3.7 ist ein Layer-2-VLAN dargestellt.

Hardware-Voraussetzung
Wie die portbasierten VLANs werden auch die MAC-adreßbasierten VLANs in der Regel mit Hilfe von Layer-2-Switches realisiert. Verwendet werden hierfür ausschließlich Switches, welche nach Art einer Multiportbridge funktionieren. Hier gibt es zwei Möglichkeiten, Adressen zu erlernen, positiv oder negativ. "Positiv learning" bedeutet, daß der Switch zuerst die Adresse kennen muß, bevor der Frame weitergeleitet wird. "Negativ learning" bedeutet, daß der Switch im Zweifelsfall unknown Unicasts an alle Ports verschickt.

VLAN-2-Management
Die MAC-adreßbasierten VLANs sind etwas aufwendiger und schwieriger zu implementieren als die portbasierten VLANs. Ein Nachteil ist, daß in den Swit-

ches bei der Erstkonfiguration eine zusätzliche Funktion benötigt wird, damit nicht alle MAC-Adressen manuell eingetragen werden müssen. Das Problem dabei ist, daß die MAC-Adressen aus Zahlen- und Buchstabenkombinationen bestehen, die schwer zu lesen und identifizieren sind und deswegen die Gefahr besteht, daß bei der Eingabe dieser Adressen viele Fehler entstehen. Damit eine Zuordnung unternehmensweit erfolgen kann, müssen diese Informationen entweder zwischen den Switchsystemen ausgetauscht werden, oder es müssen alle Switchsysteme einzeln konfiguriert werden.
Die MAC-adreßbasierten VLANs bieten den Vorteil bei Umzügen von Endgeräten. Dabei werden die Netz-Administratoren von Routinearbeiten entlastet, da die Endgeräte nach einer Umstrukturierung automatisch dem richtigen VLAN zugeordnet werden. Wird also ein Endgerät bzw. eine MAC-Adresse einmal einem VLAN zugeteilt, so ist dieses Endgerät unabhängig von ihrem physischen Standort immer Mitglied dieses VLANs. Diese Art von VLAN ist aber nur dann sinnvoll, wenn die Endgeräte bei einem Umzug, innerhalb eines Netzes, immer zum selben VLAN gehören.
Untersuchungen haben ergeben, daß in deutschen Unternehmen durchschnittlich dreißig Prozent aller Stationen im Jahr verlegt werden. Dies hat zur Folge, daß die Teilnehmer aller VLANs in kurzer Zeit über alle Switchsysteme verteilt sind. In der Praxis bedeutet dies, daß alle Broadcasts an alle Systeme zu verteilen sind und das Netz unübersichtlich wird. Bei einem solchen Netzkonstrukt müssen also wesentlich höhere Anforderungen an das Netzmanagementsystem gestellt werden.

Mobile Systeme
Auch der Einsatz von mobilen Komponenten wie Laptops in Netzen muß bei der VLAN-Planung und VLAN-Betrieb berücksichtigt werden. Es gibt zwei Möglichkeiten, einen Laptop in ein MAC-basiertes VLAN zu integrieren. Erstens: die Laptops besitzen eine PCIMCA-Schnittstelle. An diese Schnittstelle kann eine Einschubkarte mit einer entsprechenden MAC-Adresse angeschlossen werden. Dies ist zwar eine etwas teure Anschaffung, bietet aber den Vorteil, daß der Laptop flexibel im ganzen Netz angeschlossen werden kann. Die zweite Alternative einen Laptop in ein VLAN einzubinden, ist der Einsatz von einigen Docking Stations. Das Problem dabei ist, daß die Docking Station mit dem integrierten Netzadapter (inklusive der festverdrahteten MAC-Adresse) fest an dem Desktop angeschlossen ist, während der Laptop ständig den Standort innerhalb des Netzes ändert. Wenn ein Benutzer umzieht oder einfach in einem anderen Raum den Laptop ans Netz, bzw. an ein Desktop mit einer Docking Station, anschließen möchte, so kann sich seine VLAN-Mitgliedschaft ständig verändern. Dieser Effekt ist aus Sicherheitsgründen oft nicht vertretbar. In einer derartigen Umgebung muß auch die VLAN-Zugehörigkeit des Laptops ständig an die Docking Station angepaßt werden. Dies erfordert einen zusätzlichen administrativen Aufwand.

Beispiel
Am Beispiel in Abb. 3.7 werden die Layer-2-VLANs nochmals beschrieben.

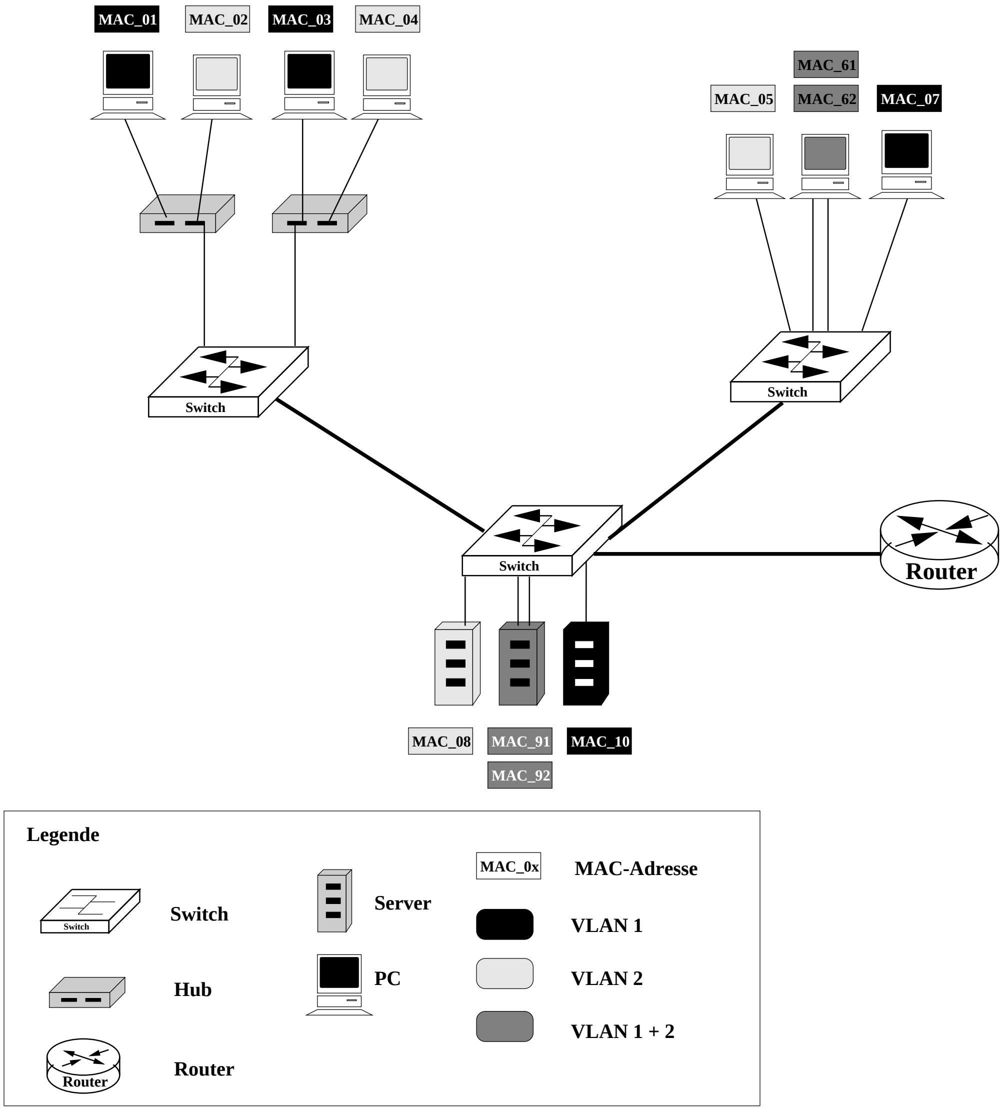


Abbildung 3.7: Beispiel mit Layer-2-VLANs

Es liegt die gleiche Ausgangssituation wie in Abb. 3.6 vor:

- strukturierte Verkabelung und geswitchtes Netz (Gebäudeverteiler, Etagenverteiler, Server-Pool)

- 3 VLAN-Gruppen: VLAN 1 (Farbe: schwarz), VLAN 2 (Farbe: hellgrau) und VLAN 1+2 (Farbe: dunkelgrau)

Die Zuordnung der Endgeräte zu den einzelnen VLANs basiert bei den Layer-2-VLANs auf den MAC-Adressen.

- VLAN 1: MAC_01, MAC_03, MAC_07 und MAC_10

- VLAN 2: MAC_02, MAC_04, MAC_05 und MAC_08
- VLAN 1+2: MAC_61, MAC_62 und MAC_91, MAC_92

Die Endgeräte "grau" sind Mitglied von VLAN 1 und VLAN 2. Die Mitgliedschaft mehrerer VLANs zu einem Endgerät wird ebenfalls durch den Einsatz mehrerer Netzkarten realisiert.
Da die Zuordnung der Endgeräte zu einem VLAN bei den MAC-adreßbasierten VLANs völlig unabhängig von dem angeschlossenen Switchport ist, können die Endgeräte MAC_01 und MAC_02 zu verschiedenen VLANs gehören, obwohl sie an einem gemeinsamen Hub hängen.
In Kap. 9.2 wird am spezielle Beispiel Oettingenstraße die Layer-2-VLANs untersucht.

3.4.3 Layer-3-VLANs

Ein interessanter Ansatz ist die VLAN-Konfiguration auf Basis der Ebene 3 Adressen. Diese Strukturen werden auch als Layer-3-VLANs bezeichnet. Hier besteht die Möglichkeit, Subnetzstrukturen (z.B. IP-, IPX-Subnetze) zu virtualisieren.

Zuordnung der Endgeräte
Durch die Zuordnung der Netzadresse eines Endgerätes zu einer Gruppe entsteht die Bildung der Layer-3-VLANs. Es gibt mehrere Kriterien nach denen man VLANs bilden kann:

- nach Art der Layer-3-Protokolle: IP-, IPX-VLAN, etc. Dabei befinden sich nur Anwender, die das gleiche Protokoll (z.B. IP, IPX) benutzen, in einem gemeinsamen VLAN.
- nach der Subnetzbildung: z.B. IP-Subnetze. Alle Benutzer die im gleichen Subnetz angeschlossen sind, gehören auch zum selben VLAN.

Durch die Bildung von Subnetzstrukturen kann eine Trennung von logischer Struktur (Subnetz) und topographischer Lokalität (Routerport) erreicht werden.

Hardware-Voraussetzung
Voraussetzung für den Einsatz von Layer-3-VLANs ist die entsprechende HW. Der Begriff des Layer-3-VLANs ist eng mit den sogenannten Layer-3-Switches[3] verbunden. Diese sollen auf Kosten der Komplexität schneller sein als herkömmliche Backbone-Router. Ein wesentlicher Schritt, dieses zu ermöglichen ist das Abspecken der Protokollvielfalt. Traditionelle (Backbone)-Router unterstützen sehr viele unterschiedliche Protokolle. Neben den meistverbreiteten (LAN)-Protokollen IP und IPX werden auch Protokolle wie DecNet, AppleTalk, OSI, XNS und Banyan Vines unterstützt. Hinzu kommen bei herkömmlichen Routern WAN-Protokolle bzw. -Schnittstellen. Layer-3 Switches beschränken sich

[3] schnelle Router

häufig auf IP und IPX. Auch bei den möglichen Routingprotokollen wird gespart. So fallen z.B. bei IP neben BGP auch häufig OSPF und RIP-II weg. Layer-3 Switches müssen genauso wie herkömmliche Router in der Lage sein, die Protokollinformationen der Frames auszuwerten und die Frames an den entsprechenden Ports auszugeben. Dazu mušen sie die Netzadresse erkennen und mit einem bestimmten VLAN verbinden. Sie benötigen eine erweiterte Adreßtabelle, in der die Zuordnungen von $Netzadresse \rightarrow Port \rightarrow MAC-Adresse$ vorhanden sind. Der Inter-VLAN-Verkehr wird weiterhin über den Router transportiert. Einige Hersteller bieten Layer-3-Switches an, die die Protokollinformationen auswerten können und selbst routen. Aus Sicherheitsgründen sollte ein Layer-3-VLAN, der über mehrere Standorte gebildet wurde, immer über einen Router gekoppelt sein.
Layer-3 VLANs bzw. Layer-3 Switches erlauben allerdings auch Ergänzungen zu den gängigen Konfigurationsmöglichkeiten von Routern. So ist neben dem bekannten Multinetting auch die Verteilung eines Subnetzes auf mehrere Ports möglich. Damit ist eine größere Freiheit bei der Konfiguration möglich und es können Subnetz-Adressen weit besser ausgenutzt werden.

VLAN-3-Management
Die protokollbasierenden VLANs ermöglichen eine optimale Verkehrsüberwachung. Alle Broadcasts können entsprechend der Protokolle segmentiert werden. Auch Stationen mit Multiprotokoll-Stacks bzw. Shared-Media-Segmente mit Stationen unterschiedlicher Protokolle werden bei diesem Verfahren unterstützt.
Ein IP-VLAN ist in diesem Sinne ein Subnetz und steht für viele Benutzer zur Verfügung. Soll ein neuer Benutzer eingerichtet werden, so ist durch seine Subnetzzugehörigkeit auch automatisch die VLAN-Zugehörigkeit gegeben. Bei Umzügen wird der Netzadministrator wesentlich entlastet, da die Endgeräte automatisch wieder dem gleichen VLAN angehören. Layer-3-VLANs sind dann sinnvoll einzusetzen, wenn die Endgeräte eines Netzes an wechselnden Standorten betrieben werden und die Zugehörigkeit zum VLAN nicht abhängig von der eingesetzten HW (Netzkarten) und dem Standort ist.
Bevor Layer-3-VLANs implementiert werden, ist eine gründliche Planung wichtig. Man benötigt Informationen über:

- das derzeitige Netz,
- Verkehrsbeziehungen im Netz,
- eingesetzte Protokolle,
- mögliche Reduzierung der Protokollvielfalt, etc.

Nachteilig ist die größere Komplexität des Modells, die einen höheren Administrationsaufwand erfordert. Vom Administrator werden detaillierte Kenntnisse über die eingesetzten Protokolle verlangt.
Die Layer-3-VLANs bieten in der Regel sehr sichere Strukturen. Das einzige Problem liegt in der Handhabung von Layer-3-Adressen. So lassen sich z.B. die IP-Adressen sehr leicht mit einer entsprechenden SW (z.B. Windows)

verändern. Damit können die Anwender ihre Netz-Adresse in eine andere umwandeln und dadurch ihre VLAN-Zugehörigkeit verändern. Um einen solchen Mißbrauch zu verhindern, müssen die Netzadministratoren entsprechende Vorkehrungen treffen. Die Konfiguration der Endgeräte sollte auf jeden Fall nur von den Netzverantwortlichen gemacht werden. Die Gruppierung der Endgeräte nach ihren Subnetzen sollte nicht veröffentlicht werden, da u.U. ein Angriff (Veränderung der eigenen Netz-Adressen) nicht auszuschließen ist.

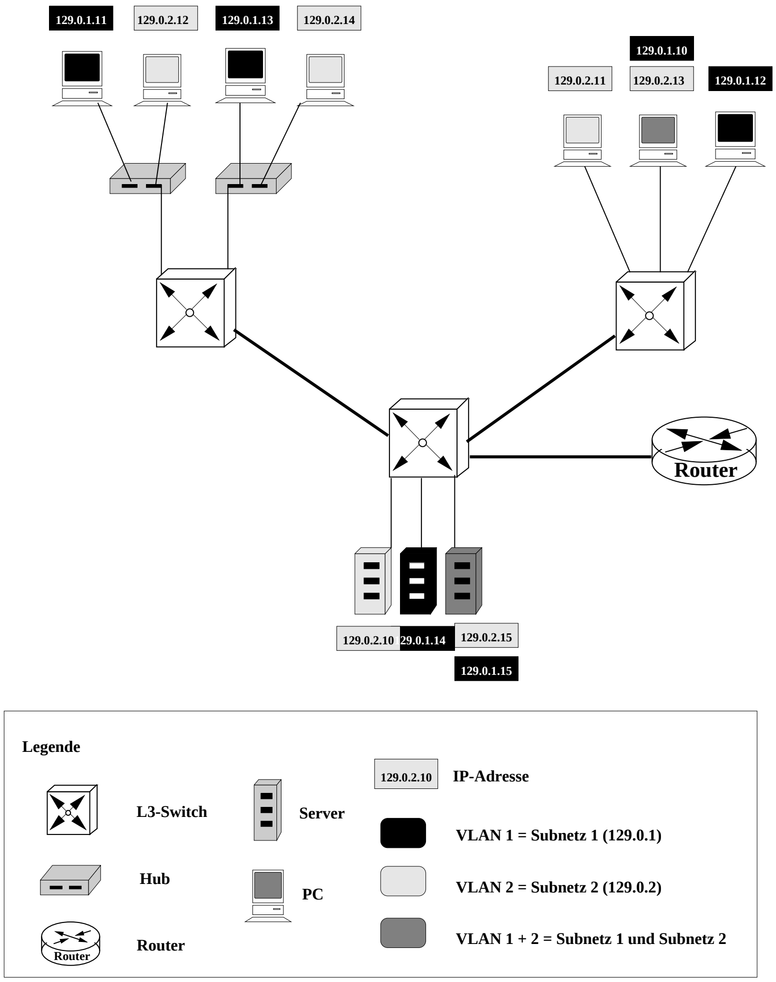


Abbildung 3.8: Beispiel mit Layer-3-VLANs (IP)

Beispiel

Abb. 3.8 zeigt ein kleines geswitchtes IP-Netz, das logisch aus zwei Subnetzen besteht:

- Subnetz 1 (129.0.1) entspricht VLAN 1 (Farbe: schwarz)

- Subnetz 2 (129.0.2) entspricht VLAN 2 (Farbe: hellgrau)

Alle Endgeräte bzw. Benutzer mit der gleichen Subnetz-Adresse gehören automatisch zu einem VLAN.

3.4.4 Policy-basierende VLANs

Policy-basierende VLANs verwenden logische Zuordnungen (Port, MAC, Protokoll, Netzadresse). Sie sind die flexibelste Form, Endgeräte zu einer Gruppe zusammenzufassen.

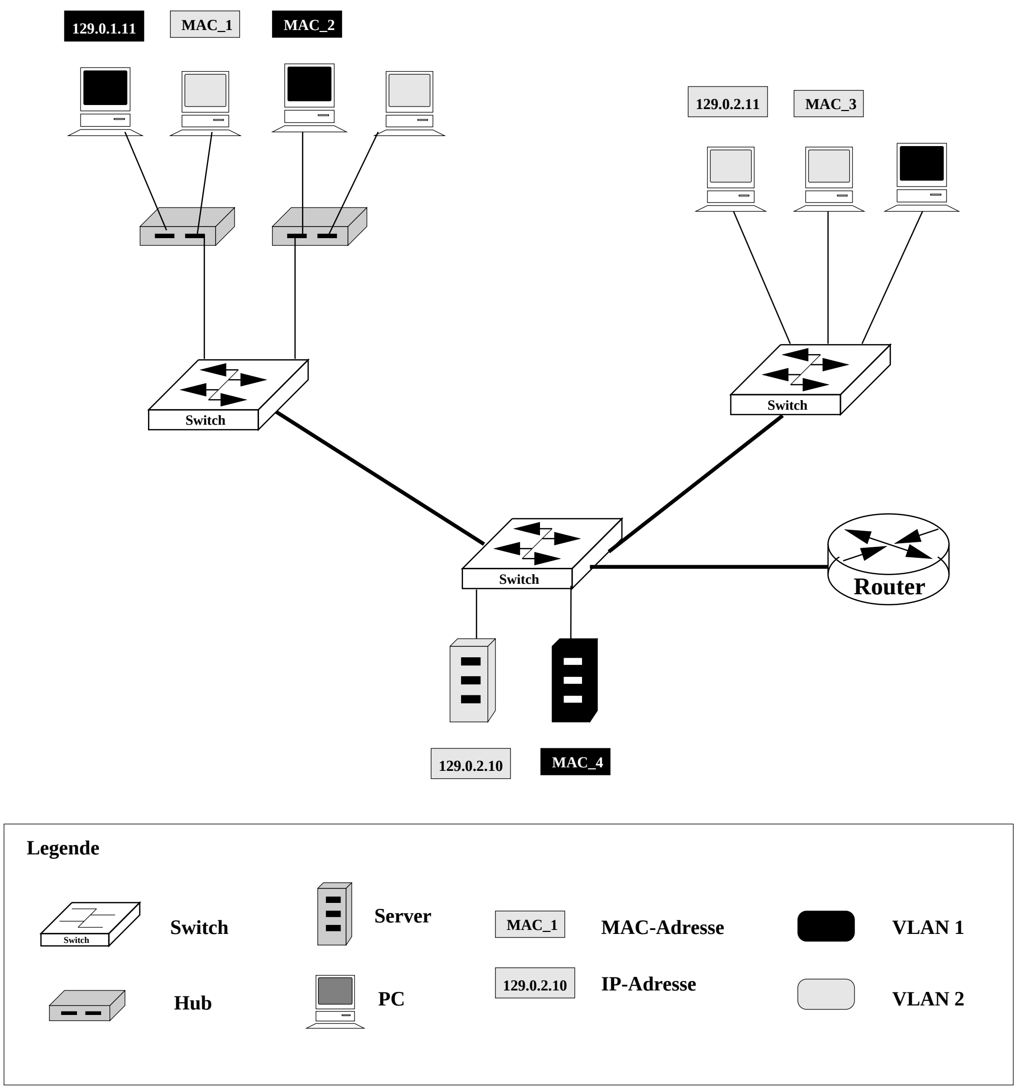


Abbildung 3.9: Beispiel mit Policy-basierten VLANs

Zuordnung der Endgeräte
Die Endgeräte können aufgrund ihrer Portzugehörigkeit, ihrer MAC-Adresse oder der IP-Adresse einem VLAN zugeordnet werden. Auch eine Kombination dieser Möglichkeiten können ein VLAN definieren (siehe Abb. 3.9).

Protocol Policy VLAN
Eine Art, VLANs zu definieren, ist das Zusammenfassen von bestimmten Protokollen. In einem heterogenen Netz, bestehend aus UNIX, DEC, SNA, Novell, NT, etc. gibt es die Möglichkeit, diese jeweils zu einem VLAN zu konfigurieren und somit die Protokolle strikt voneinander zu trennen.

VLAN-Management
Ein Vorteil dieses Verfahrens ist, daß dieses VLAN-Modell alle vorherigen Modelle nachbilden und kombinieren kann. Der Administrator kann das Verhältnis zwischen Sicherheit, Verkehrsoptimierung und Kontrolle selbst bestimmen.
Ein Nachteil ist, daß die Administration sehr komplex wird und nur von erfahrenen Administratoren geleistet werden kann. Die eingeschränkte Verfügbarkeit stellt weitere Nachteile dar.

Beispiel
Das Netz aus Abb. 3.9 ist in drei VLANs aufgeteilt. Die Endgeräte aus diesen drei OE werden durch Kombination aus Layer-1,-2,-3-VLANs gebildet:

- VLAN 1: IP-Adresse 129.0.1.11, MAC-Adressen MAC_2, MAC_4 und die Zuordnung zu einem Port
- VLAN 2: MAC-Adresse MAC_1, MAC_3, IP-Adressen 129.0.2.11, 129.0.2.10 uns die Zuordnung zu einem Port

3.5 VLANs im Backbone

Um nun die oben definierten VLAN-Techniken in ein unternehmensweites LAN einzuführen, müssen noch einige Bedingungen erfüllt sein, um eine schnelle und erfolgreiche Umsetzung dieser virtuellen Strukturen zu gewährleisten. In einem unternehmensweiten LAN müssen alle Einzelsysteme in das Gesamtsystem integriert und aufeinander abgestimmt werden. Neben der Anpassung der Einzelsysteme in das Gesamtsystem gehören auch die möglichen Verfahren, die zur Übertragung der VLAN-Informationen zwischen den Koppelungselementen notwendig sind.

Bei der Untersuchung der Koppelverbindung zwischen den Switchsystemen wird zwischen paketbasierenden Protokollen (z.B. Ethernet) oder zellbasierenden Protokollen (z.B. ATM) unterschieden. Bei beiden Verfahren kann jeder Hersteller selbstverständlich ein proprietäres Verfahren implementieren, das den Informationsaustausch innerhalb der VLANs konkret beschreibt. Aber eine proprietäre Implementierung geht natürlich auf Kosten der Interoperabilität, die in der Zeit der heterogenen Netze immer wichtiger wird. Deswegen sind in diesem

Zusammenhang standardisierte Verfahren notwendig.

In diesem Kapitel werden die einzelnen Verfahrenstechniken, die zur Übertragung der VLAN-Informationen zwischen den Transitsystemen zur Auswahl stehen, erläutert. Diese Verfahrenstechniken sind notwendig, damit erstens jedes VLAN in das Gesamtsystem integriert werden kann und zweitens jedes Einzelgerät zu einem VLAN zugeordnet werden kann. Genau diese Informationen müssen über das gesamte Netz, über alle Transitsysteme, bekannt sein.

3.5.1 Austausch von Adreßtabellen

Der Austausch von Adreßtabellen über die Transitsysteme hinweg, ist eine mögliche Verfahrenstechnik bei der Übertragung von VLAN-Informationen. Abhängig von der eingesetzten VLAN-Technik (Layer-1-VLANs oder Layer-2-VLANs) gibt es Unterschiede in der Informationsverteilung. Der Informationsaustausch findet jeweils zwischen den Switches statt. Dazu ist es notwendig, daß die Adreßtabellen (MAC-Adresse $\rightarrow$ Port) im Switch um entsprechende VLAN-Informationen (VLAN-ID) erweitert werden. Diese erweiterte Adreßtabelle (Beispiel siehe Tabelle 3.1) gibt Auskunft über eine genaue Zuordnung der MAC-Adresse bzw. des Switch-Ports zu ihrem VLAN.

Port	MAC-Adresse	VLAN
1	400000000010	1
2	400000000011	1
3	400000000012	1
4	400000000013	2
5	400000000014	2
6	400000000015	2
7	400000000016	3
8	400000000017	3

Tabelle 3.1: Aufbau einer erweiterten Adreßtabelle

Bei den portbasierten VLANs bestimmt der Switch-Port, zu welchem VLAN das angeschlossene Endgerät (MAC-Adresse) zugeteilt wird. Aufgrund der ständigen Veränderung (Umkonfiguration und Neukonfiguration der Ports) der Adreßtabelle eines Switches, müssen dann auch die anderen Switches informiert werden, damit jeder Frame auch weiterhin einem VLAN eindeutig zugeteilt werden kann. Für die permanente Aktualisierung der Adreßtabelle gibt es mehrere Lösungen: die gesamte Adreßtabelle wird in bestimmten Intervallen an die anderen Switches im Netz gesendet oder nur Teile (Änderungen) der Adreßtabelle werden in kurzen Abschnitten an die anderen Switches weitergegeben.

Bei den MAC-basierten VLANs bestimmt die MAC-Adresse die Zugehörigkeit zu einem VLAN. D.h. alle MAC-Adressen müssen erfaßt und in die Adreßtabelle eingetragen werden. Die Adreßtabelle wird dann manuell um die VLAN-ID

erweitert. Die vollständige Konfigurationstabelle wird an alle Switches im Netz gesendet.
Bei der Auswertung eines Datenframes (Zugehörigkeit MAC-Adresse → VLAN → Ausgangsport) benötigt man einen effizienten Suchalgorithmus, um die Verzögerungszeiten möglichst klein zu halten. Eine optimale Lösung bietet so eine erweiterte Adreßtabelle, die die Konfigurationstabelle als Referenz nutzt ([4]). Bei dieser Methode wird nach dem Erkennen einer neuen Source-Adresse die entsprechende VLAN-Zugehörigkeit in der zentralen Konfigurationstabelle abgefragt und in die dynamische Tabelle (Aging) des Switches eingetragen. So können die Frames mit Hilfe einer zentralen Tabelle (Konfigurationstabelle) im Switch abgearbeitet werden. Wird nun diese Tabelle verändert, wird die VLAN-Zugehörigkeit in den Switch-Tabellen automatisch angepaßt.

Zu beachten ist weiterhin, daß der Austausch der Tabellen zwischen den Switches synchronisiert werden muß, damit die Empfänger auch wissen, wann neue Informationen bereitstehen.
Der Adreßaustausch findet nur zwischen Switches statt. Existiert nun ein Router im bestehenden Netz, so dient er nur zum Datentransport zwischen den Segmenten auf Ebene 3. D.h. Router können keine VLAN-Zugehörigkeit überprüfen.

3.5.2 Frame Tagging

Eine zweite Verfahrenstechnik ist das Tagging, welches es ermöglicht, VLAN-Informationen innerhalb der Datenframes auf Layer-2 (MAC-Ebene) zu übertragen. Die Arbeitsgruppe IEEE 802.1Q beschäftigt sich mit dem Thema Frame-Tagging. Es ist ihnen gelungen einige wichtige Punkte zusammenzufassen, um in der heutigen heterogenen LAN-Welt eine kompatible und interoperable Lösung zu ermöglichen. Diese lauten: (aus [4])

- Unterstützung der bestehenden IEEE 802.X MAC-Services
- eine Erweiterung des Quality of Service (IEEE 802.1P)
- Beschränkung in der ersten Form auf portbasierte VLANs
- ein Spanning Tree pro VLAN
- Unterstützung von Token Ring-basierten Strukturen

Bei diesem Verfahren werden die MAC-Frames nach IEEE 802.1Q "Tagging Verfahren" mit einem zusätzlichen *Tag*[4] erweitert. Die Plazierung dieses Tags innerhalb des Headers muß an einer bestimmten Stelle (Bit) stehen, damit die Systeme diese VLAN-Informationen auch finden und auswerten können. Abhängig von den eingesetzten Protokollen (Ethernet, Token Ring, FDDI) wird das Tag an unterschiedlicher Stelle plaziert. In Abbildung 3.10 ist ein Ethernet-Frame mit dem VLAN-Tag dargestellt. Die Tag-Informationen werden in zwei Teilbereiche gegliedert:

[4]eindeutige Kennzeichnung im Header eines MAC-Frames, für die VLAN-Zugehörigkeit

Praeambel	FD	Destination-Adresse	Source-Adresse	Laengen-Feld	DSAP	SSAP	CF	Protokoll-ID	SVPID	VID	Information	FCS

Abbildung 3.10: VLAN-Tag innerhalb eines Ethernet-Frames

- SVPID (8 Bytes) bedeutet SNAP[5] encoded VLAN Protocol Identifier
- VID (2 Bytes) bedeutet VLAN-Identifier

Die VLAN-Tag-Information eines Frames wird in den Switches erzeugt bzw. entfernt. Dies wird folgendermaßen ablaufen: wird ein Datenframe an einem Switch-Port eingelesen, so kann der Switch anhand des Ports oder MAC-Adresse, oder Layer-3-Adresse des Senders erkennen, zu welchem VLAN der Frame gehört. Der Ethernet-Frame wird um die ermittelte VLAN-Information (VLAN-Tag) ergänzt und anschließend am Backboneport ausgegeben. Dieser erweiterte Frame wird so von Switch zu Switch gesendet bis er am Zielswitch angekommen ist. Da findet eine Überprüfung statt, ob die MAC-Adresse des Empfängers sich im selben VLAN befindet, wie die im Tag-Feld gespeicherte Information. Stimmt diese überein, so wird das Tag-Feld entfernt und der Frame am Ausgangsport an den Empfänger gesendet. Sind Sender um Empfänger aber nicht im selben VLAN, kann der Frame nicht weitergeleitet werden.
Durch die eindeutige Kennzeichnung der zu sendenden Frames gelangen die VLAN-Informationen schnell und ohne großen Overhead an die betreffenden Systeme. Bei diesem Verfahren benötigt man auch keine zusätzliche Synchronisierungsmechanismen.

3.5.3 Time Division Multiplexing

Beim Time Division Multiplexing (TDM) wird die VLAN-Zugehörigkeit durch die Plazierung des Paketes im Datenstrom ermöglicht. Auf der sendenden Switch-Seite werden die verschiedenen VLAN-Pakete gemultiplext und über eine gemeinsame Leitung transportiert (siehe Abb. 3.11). Da die Reihenfolge der VLAN-Pakete fest ist, kann auf der Empfängerseite der Datenstrom wieder korrekt demultiplext und die Pakete dem richtigen VLAN zugeordnet werden.

3.5.4 VLANs über ATM

ATM ist ein idealer Partner von VLAN, da bereits vorhandene Standards existieren:

- Multiprotocol Encapsulation over AAL 5 (IETF RFC 1483)
- Classical IP and ARP over ATM (IETF 1577)
- LAN-Emulation (ATM-Forum).

[5] SubNetwork Access Protocol

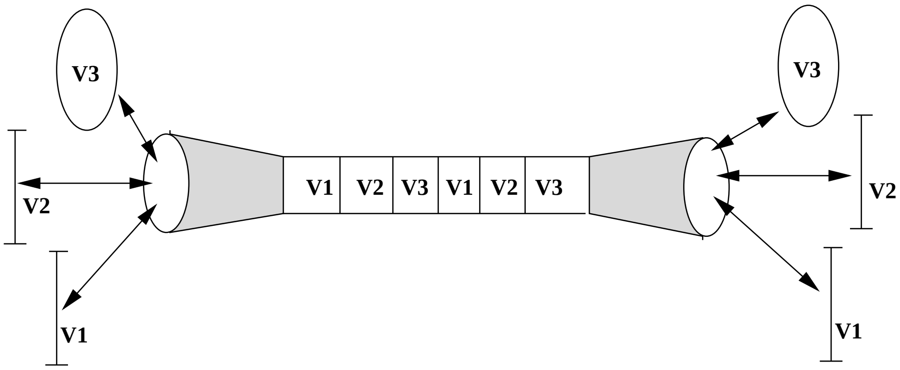


Abbildung 3.11: Datenstrom zwischen zwei Switches

ATM ist also ein weiteres Verfahren um VLANs über ein unternehmensweites Netz zu realisieren.
ELAN[6] wurde spezifiziert, um die Verbindung von LANs über einen ATM-Backbone zu ermöglichen. Ein emuliertes LAN wird als Gruppe von Geräten definiert, die an das ATM-Netz angekoppelt werden. Jedes emulierte LAN ist völlig unabhängig von den anderen emulierten LANs, es stellt eine eigene Broadcast Domain dar. Für jedes VLAN im Netz, das Daten über einen ATM-Backbone transportieren möchte, muß ein separates ELAN definiert werden (Abb. 3.12). Eine Kommunikation zwischen zwei emulierten LANs muß über einen Router geführt werden. Mit einem ATM-Backbone ist es bei der

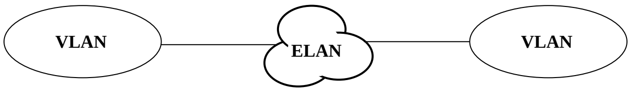


Abbildung 3.12: VLAN über ATM-Backbone

Nutzung der LAN-Emulation möglich, in einer standardisierten Art und Weise virtuelle Netze ohne Einschränkung aufzubauen.

[6]Emulated LAN

Teil II

Analyse-Phase

Kapitel 4

Ermittlung der Organisationsstruktur

In diesem Kapitel wird die Organisationsstruktur des Gebäudekomplexes Oettingenstraße untersucht. Hierbei werden die vorhandenen Strukturen nach der Aufbauorganisation und Ablauforganisation analysiert.

4.1 Begriffserklärung Organisation

Die Aufgaben eines Betriebes bzw. einer Unternehmung sind in der Regel sehr komplex. Will man nun diese Aufgaben "auf einen Schlag" lösen, stößt man sehr schnell an Kapazitätsgrenzen. Um diese Komplexität zu reduzieren, entsteht die Notwendigkeit, die Aufgaben zu zerlegen und zu verteilen, um sie trotz der erwähnten Kapazitätsgrenzen zielgerecht zu erfüllen.
Auch der Ablauf innerhalb eines Betriebes muß berücksichtigt werden, da sich das gesamte betriebliche Geschehen in einer bestimmten Ordnung und nach bestimmten Regeln vollzieht. Diese Ordnung und die Aufgabenteilung muß geplant werden.

Unter Organisation versteht man nun einerseits den Prozeß der Entwicklung der Ordnung aller betrieblichen Tätigkeiten (Strukturierung der Tätigkeiten) und die Gesamtheit der Regeln, die notwendig sind, diese Prozesse zu realisieren.
Der wichtigste Punkt der Organisation ist also die Zerlegung der Gesamtaufgabe in Teilaufgaben und deren zielorientierte Abstimmung.

Jede Unternehmung hat eine Organisation. Diese Organisation wird beschrieben in der Aufbauorganisation und Ablauforganisation.

4.2 Aufbauorganisation

Unter Aufbauorganisation versteht man die Zergliederung der Unternehmung in aufgabenteilige Subeinheiten (Stellen, Instanzen, Abteilungen, Projekte). D.h.

ausgehend von der gegebenen Gesamtaufgabe des Betriebes erfolgt eine Aufspaltung in so viele Teilaufgaben (oder Einzelaufgaben), so daß durch die anschließende Kombination dieser Teilaufgaben "eine sinnvolle arbeitsteilige Gliederung und Ordnung der betrieblichen Handlungsprozesse"[1] entsteht.

Bei der Analyse der Aufbauorganisation ermittelt man im wesentlichen die Aufgabenanalyse und die Aufgabensynthese.

Die erste Aufgabe der Aufbauorganisation (Aufgabenanalyse) beinhaltet die Analyse und Zerlegung der Gesamtaufgabe des Betriebes. Die Zerlegung der Gesamtaufgabe in Teilaufgaben läßt sich als mehrstufiger Vorgang darstellen. Auf der ersten Stufe erfolgt eine erste Teilung der Gesamtaufgabe in die entsprechenden Bereiche (= Teilaufgaben). Jeder auf der ersten Stufe entstandene Bereich wird, sofern dafür Bedarf besteht, auf der zweiten Stufe nochmals zerlegt. Dieser Teilungsvorgang kann solange fortgesetzt werden, bis ein für den organisatorischen Gestaltungszweck befriedigendes Detaillierungsniveau der Teilaufgaben gefunden ist.
Die Gliederung der Aufgaben auf einer Stufe bezeichnet man als horizontale Aufgabenteilung. Die Gliederung der Aufgaben von Stufe zu Stufe als vertikale Aufgabenteilung. Das Ergebnis der Aufgabenanalyse sind Aufgabengliederungspläne, die nach verschiedenen Merkmalen entstehen können.

Die zweite Aufgabe der Aufbauorganisation (Aufgabensynthese) besteht dann darin, die Einzelaufgaben zusammenzufassen, indem z.B. "Stellen" gebildet werden, wobei sich aus der Aufgabenstellung Beziehungszusammenhänge zwischen diesen Stellen ergeben. Jede Stelle bildet eine sogenannte Organisationseinheit (OE).

Unter einer Organisationseinheit (OE) eines Unternehmens verstehen wir eine Anzahl von Mitarbeitern, die für ein fest definiertes Aufgabengebiet verantwortlich sind. Einer der Mitarbeiter innerhalb einer OE ist Leiter dieser OE. An ihn berichten die Mitarbeiter der OE. Er ist für die Ergebnisse der OE verantwortlich und berichtet darüber seinen Vorgesetzten. Die OE ist damit das Grundelement der Aufbauorganisation.

Zusätzliche Bemerkungen zu den OE:

1. Grafische Darstellung einer OE: $\boxed{\text{Name}}$

2. Die Aufgaben einer OE sollten sachlich zusammenhängend und in sich abgeschlossen sein.

3. OE können beliebig groß und beliebig klein sein. Im allgemeinen haben sie eine Unterstruktur, das heißt sie sind in kleinere OE zerlegt (Zerlegung auf Stufe 2, 3, usw.).

[1] Kosiol, E., Aufbauorganisation, HdO, 1. Aufl., Stuttgart 1969, Sp. 172

4. Findet eine Zerlegung in OE statt, so muß die Aufbauorganisation (Aufgaben- und Verantwortungsverteilung, Weisungs- und Berichtswege) und die Ablauforganisation definiert werden.

5. Zur grafischen Darstellung der Aufbauorganisation benutzt man häufig sogenannte Organisationsdiagramme (Organigramme) wie in Abb. 4.1 grafisch dargestellt.

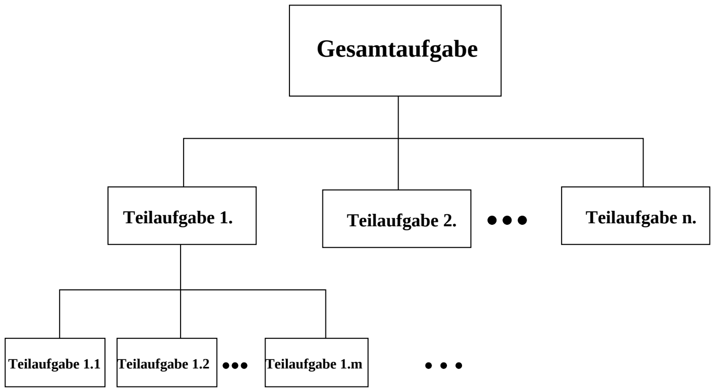


Abbildung 4.1: Beispiel einer top-down Zerlegung

Die oben beschriebene theoretische Struktur eines Unternehmens soll nun auf dem Gebäudekomplex Oettingenstraße angewendet werden. Der Gebäudekomplex Oettingenstraße, in dem verschiedene Institute der Ludwig-Maximilians-Universität untergebracht sind, ist nun keine typische Unternehmung. Dieses Gebäude wird ausschließlich der Bildung & Forschung zur Verfügung gestellt. Es finden keine betrieblichen Tätigkeiten, im Sinne von Gewinnerbringung, statt. Die Gesamtaufgabe (vgl. Abb. 4.2) ist in diesem Fall der Gebäudekomplex Oettingenstraße, ein Standort der Ludwig-Maximilians-Universität. Innerhalb die-

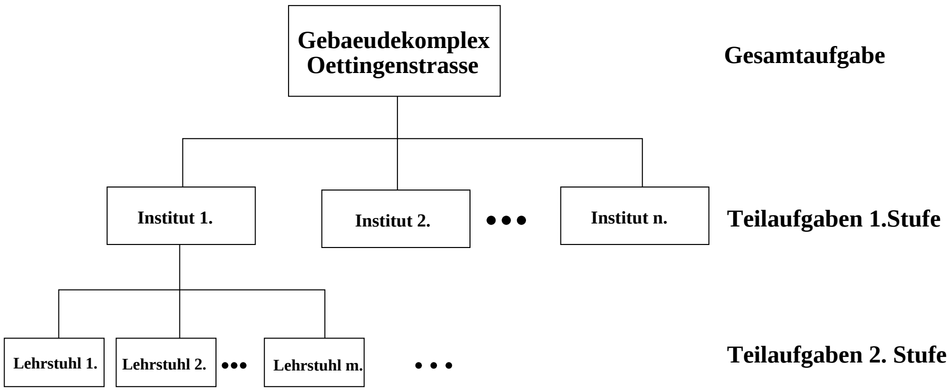


Abbildung 4.2: Aufgabenanalyse im Gebäudekomplex Oettingenstraße

ses Gebäudekomplexes kann man in einer ersten Ausbaustufe die Gesamtaufgabe in die verschiedenen Bereiche zerlegen:

- zeitlich unbefristete Institute
- zeitlich befristetes Institut
- CIS (Centrum für Informations- und Sprachverarbeitung)
- Japan Zentrum
- Bibliothek

In einer weiteren Stufe wird der Bereich "zeitlich unbefristete Institute" in sieben Institute aufgeteilt:

- Institut für Phonetik und Sprachliche Kommunikation
  Sprechwissenschaften und Psycholinguistik
- Geschwister-Scholl-Institut für Politische Wissenschaft
- Institut für Informatik
- Institut für Medizinische Optik
- Institut für Japanologie
- Institut für Völkerkunde und Afrikanistik
- Institut für Kommunikationswissenschaften
  (Zeitungswissenschaften)

Eine Zerlegung auf der dritten Stufe wird nur für das Institut für Informatik vorgenommen. Innerhalb dieses Institutes gibt es fünf Lehr- und Forschungseinheiten:

- Kommunikationssysteme und Systemprogrammierung
  Prof. Hegering, Prof. Ludwig, Prof. Seegmüller (emer.)
- Datenbanksysteme
  Prof. Kriegel
- Programmierung und Softwaretechnik
  Prof. Wirsing, Prof. Kröger, Prof. Haggenmüller (apl.)
- Progammier- und Modellierungssprachen
  Prof. Bry
- Theoretische Informatik
  Prof. Clote
- CIP-Pool

Die Ergebnisse dieser Zergliederung bilden nun jeweils eine bestimmte Organisationseinheit:

- IfP&SK
  Institut für Phonetik und Sprachliche Kommunikation
  Sprechwissenschaften und Psycholinguistik
- GSI
  Geschwister-Scholl-Institut für Politische Wissenschaft
- Bib
  Bibliothek
- IfInfo
  Institut für Informatik
  - LFE NM (Kommunikationssysteme und Systemprogrammierung)
  - LFE DBS (Datenbanksysteme)
  - LFE PST (Programmierung und Softwaretechnik)
  - LFE PMS (Progammier- und Modellierungssprachen)
  - LFE TCS (Theoretische Informatik)
  - CIP (CIP-Pool)
- IfMO
  Institut für Medizinische Optik
- IfJap
  Institut für Japanologie
- JapZ
  Japan Zentrum
- CIS
  Centrum für Informations- und Sprachverarbeitung
- IfV&A
  Institut für Völkerkunde und Afrikanistik
- IfKW
  Institut für Kommunikationswissenschaften
- IfPäd (If?)
  Institut für Pädagogik (zeitl. befristet)

4.3 Ablauforganisation

Die bisherigen Untersuchungen haben sich auf die Ermittlung der Aufbauorganisation beschränkt. Nun soll auch die Ablauforganisation im Gebäudekomplex Oettingenstraße untersucht werden.

Unter Ablauforganisation versteht man die Gestaltung von Arbeitsprozessen. Bei dieser Untersuchung werden die sachlichen, in Raum und Zeit ablaufenden Prozesse im Vordergrund stehen, die sich bei und zwischen den Aufgabenträgern vollziehen. Dabei muß der Arbeitsablauf in verschiedener Hinsicht gegliedert werden. Man unterscheidet:

1. die Ordnung des Arbeitsinhalts,
2. die Ordnung der Arbeitszeit,
3. die Ordnung des Arbeitsraums,
4. die Arbeitszuordnung.

Da die Universität bzw. die Institute der LMU des Gebäudekomplexes Oettingenstraße nun keine typische Unternehmung ist, und keine betrieblichen Arbeitsprozesse ablaufen, kann auch keine Zuordnung zu den oben genannten Punkten erfolgen. Zu dem Punkt (1) Ordnung des Arbeitsinhalts ist es möglich, eine Zuordnung zu machen. Im Rahmen der Aufgabenanalyse (Kap. 4.2) wurde, wie wir gesehen haben, die Gesamtaufgabe in Teilaufgaben zerlegt. Insofern baut also die Ablauforganisation auf einem Ergebnis der Aufgabenanalyse auf. Da aber die Verkettung der einzelnen Teilaufgaben (OE), bzw. die Arbeitsabläufe zwischen den Teilaufgaben (OE) hier nicht von Bedeutung ist, werden keine weiteren organisatorischen Aufgaben untersucht.

Innerhalb dieses Gebäudekomplexes sind z.Zt. keine übergreifenden Abläufe zwischen den Instituten abgesprochen. Dies soll aber nicht heißen, daß keine Abläufe in diesem Gebäudekomplex existieren. Dieser Standort gehört zu der Ludwig-Maximilians-Universität und wird über das LRZ[2] ans Münchner Hochschulnetz angeschlossen. Auch dieser Standort wird in alle Prozesse der LMU und MHN mit eingebunden. In dieser Diplomarbeit konzentrieren wir uns auf den Standort Oettingenstraße, so daß alle gebäudeübergreifenden Abläufe hier nicht relevant sind.

4.4 Koordination zwischen den OE

In diesem Abschnitt wird die Beziehung zwischen den oben definierten Organisationseinheiten (OE) untersucht. Die Aufbauorganisation erstreckt sich auf die Verknüpfung der organisatorischen Grundelemente (Institute, Lehrstühle, etc.), die als OE definiert wurden. In einer zweiten Phase werden die Beziehungen zwischen diesen OE definiert.
Die Untersuchung der “Unternehmung” Oettingenstraße hat ergeben, daß die OE in keiner Beziehung[3] zueinander stehen. Eine Ausnahme macht die OE “Bibliothek”, da sie für alle Institute zur Verfügung steht.

[2]Leibniz-Rechenzentrum, Betreiber des Münchner Hochschulnetzes (MHN)
[3]organisatorisch, inhaltlich

4.5 Eingliederung des Personalbedarfs in den OE

Wie in Kap. 4.2 schon erwähnt, ist die Organisationseinheit (OE) das Grundelement der Aufbauorganisation. Sie stellt die Zusammenfassung von Teilaufgaben zum Arbeitsbereich einer Person dar. Da sich der zweite Teil der DA mit technischen Themen befaßt, ist es sinnvoll schon an dieser Stelle jeder OE auch einen Netzverantwortlichen zuzuordnen. Die Zuordnung dieser Personen, soweit bekannt, zu den OE stellt sich wie folgt dar:

- IfP&SK

  Netzverantwortlicher: Dr. Draxler
  Institutsleiter: Prof. Tillman

- GSI

  Netzverantwortlicher: N.N
  Institutsleiter: k.A.

- Bib

  Netzverantwortlicher: Dr. Degenhardt
  Bibliotheksleiterin Fr. McKenzy

- IfInfo

  Netzverantwortliche: Fr. Kostelezky
  Institutsleiter: Prof. Hegering

- LFE NM

  Netzverantwortliche: Fr. Kostelezky
  Lehrstuhlinhaber: Prof. Hegering

- LFE DBS

  Netzverantwortlicher: Hr. Krojer
  Lehrstuhlinhaber: Prof. Kriegel

- LFE PST

  Netzverantwortlicher: Hr. Fasching
  Lehrstuhlinhaber: Prof. Wirsing

- LFE TCS

  Netzverantwortlicher: Hr. Fremann
  Lehrstuhlinhaber: Prof. Clote

- CIP

  Netzverantwortlicher: Fr. Kostelezky
  Lehrstuhlinhaber: Prof. Hegering

- IfMO

  Netzverantwortlicher: Hr. Hartl
  Institutsleiter: Prof. Zinth

- IfJap

  Netzverantwortliche: Fr. Haußer
  Institutsleiter: Prof. Laube

- JapZ

  Netzverantwortliche: Hr. Törkel
  Institutsleiter: k.A.

- CIS

  Netzverantwortlicher: Hr. Hadersbeck
  Institutsleiter: k.A.

- IfV&A

  Netzverantwortlicher: Dr. Schubert
  Institutsleiter: Prof. Laubscher

- IfKW

  Netzverantwortlicher: Dr. Degenhardt
  Institutsleiter: k.A.

- IfPäd (If?)

  Netzverantwortliche: N.N
  Institutsleiter: N.N

4.6 Ergebnis der Aufbauorganisation

Als Ergebnis der aufbauorganisatorischen Tätigkeit, d.h. von der Aufgabenanalyse (Zergliederung der Gesamtaufgabe), ergibt sich eine Gliederung, aus der hervorgeht, welche OE überhaupt geschaffen werden und ob Beziehungen zwischen diesen OE bestehen. Dieses Ergebnis kann man zusammenfassen und grafisch in einem Organigramm darstellen. Das Organigramm aus Abb. 4.3 stellt eine sehr flache, hierarchische Organisation dar.

.

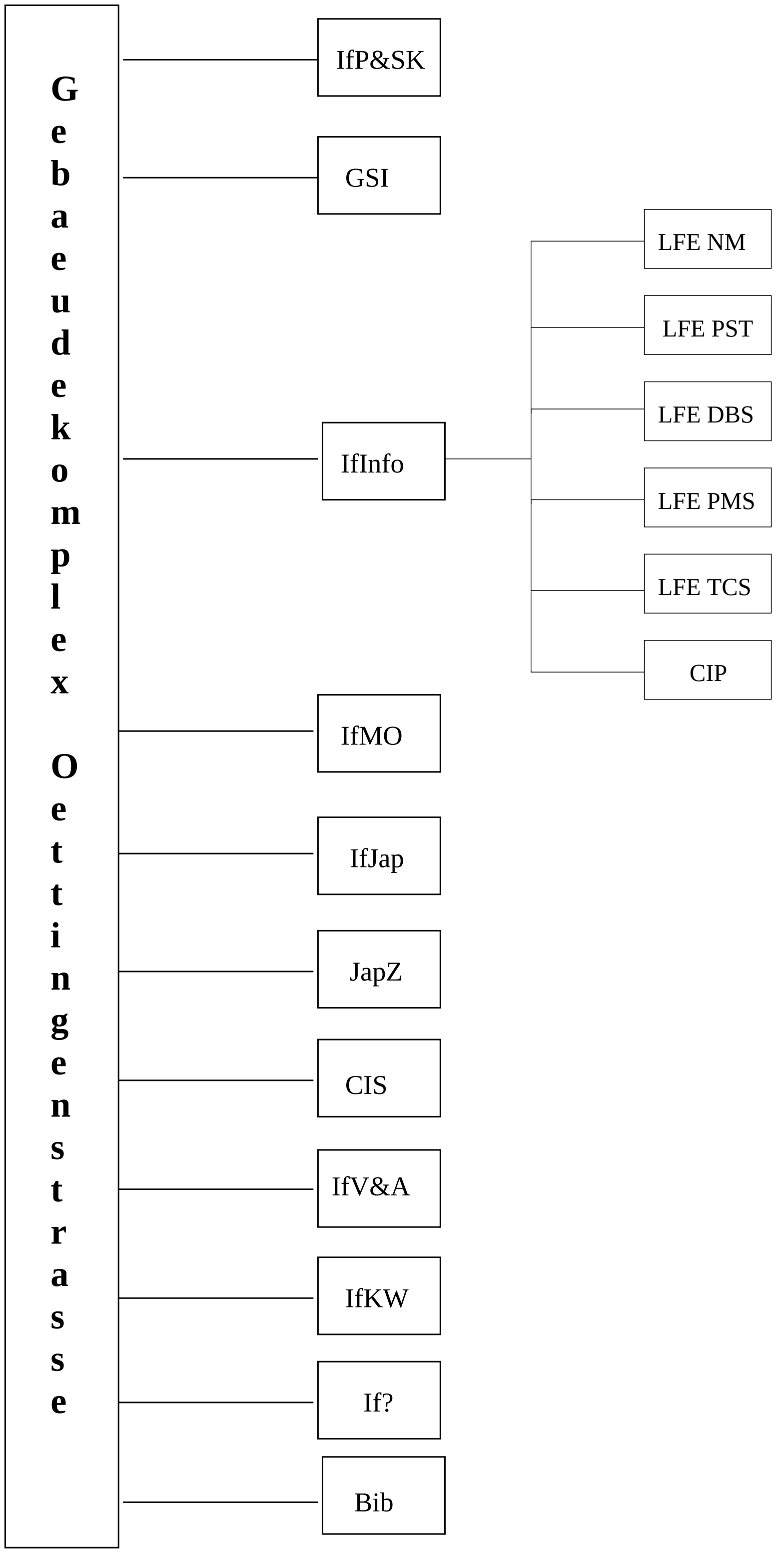


Abbildung 4.3: Organisationsstruktur des Gebäudekomplexes Oettingenstraße

Kapitel 5

Ermittlung der Anforderungen der Benutzer aus den OE

In Kapitel 3.1 Technische Grundlagen wurde u.a. der VLAN-Begriff definiert und die VLAN-Arten beschrieben. Aus dieser technischen Beschreibung der VLANs ergeben sich weitere Fragen, deren Antworten wichtig für die optimale Planung von VLANs sind. Konkret muß nun die vorhandene Situation in den ermittelten OE und die Anforderungen der Benutzer erfaßt werden.
Mit Hilfe eines Fragenkataloges, der an alle Netzverantwortlichen der Institute adressiert war, konnten alle wichtigen Fragen, die für eine VLAN-Implementierung notwendig sind, gestellt und anschließend ausgewertet werden. Weiterhin sind die Anforderungen der Benutzer an das derzeitige und zukünftige Netz von großer Bedeutung.

5.1 Fragebogen und Ergebnisse

Die individuellen Benutzer-Anforderungen und weitere besondere Gegebenheiten am Standort Oettingenstraße sind zwingend notwendig, um ein den Erfordernissen angepaßtes Netz zu realisieren. Als Hilfestellung zur Aufnahme dieser Informationen eignet sich ein Fragenkatalog. Der von mir erstellte Fragenkatalog ist vollständig im Anhang A zu finden und enthält eine Reihe von Fragen, deren Antworten bei der Planung vor der Definition der VLANs vorliegen sollten.

Die Struktur des Fragebogens und eine Zusammenfassung der Antworten sieht wie folgt aus:

1. Allgemeine Angaben
   Hier werden Informationen abgefragt über die Anzahl der Netzbenutzer und über die vorhandene Infrastruktur des Institutes bzw. Lehrstuhls. Diese Informationen sollen einen Überblick über das Institut geben und Besonderheiten, wie verfügbare Betriebssysteme, häufig verwendete Applikationen, Basisdienste, etc. festhalten und bei der Planung des Netzes berücksichtigen.

2. Kommunikationsbeziehungen im Netz
Eine wichtige Voraussetzung bei der Bildung von VLANs ist die Kenntnis über die Kommunikationsstrukturen im Netz. Hier sind die Client-Server-Beziehungen und der Zugriff auf Client-Ressourcen (Drucker, Plotter, Scanner, etc.) zu erfassen.
Die verwendeten Server werden unterschieden nach:

   - lokale (institutseigene/lehrstuhleigene) Server,
   - zentrale Server (innerhalb dieses Gebäudekomplexes, aber außerhalb des Institutes/Lehrstuhls) und
   - externe Server (außerhalb des Gebäudekomplexes z.B. am LRZ oder in der Schellingstraße).

   Die Ergebnisse bieten Einblicke in die Struktur der Institute (OE) und in die Kommunikationsbeziehungen zwischen den Instituten, die z.T. auch schon im Bereich Organisationsstruktur, Kapitel 4 ermittelt wurden. Die OE sind eigenständige Bereiche, die hauptsächlich mit lokalen Servern (falls vorhanden) arbeiten und zur Anbindung an das WWW auf externe Server (LRZ) zugreifen. Zwischen den OE finden kaum Kommunikationsbeziehungen statt. Die 80/20-Regel wird eingehalten, so daß 80% des lokalen Verkehrs im Institut verbleibt und nur 20% geroutet werden muß. Das Institut für Informatik wurde in einer zweiten Ausbaustufe Kap. 4 in die einzelnen Lehrstühle und CIP-Pool unterteilt. Innerhalb dieser OE findet ein Datenaustausch statt. Es werden lokale Server (NFS, News, email, etc.) auch zentral für die anderen OE zur Verfügung gestellt.

   Es gibt aufgrund der Auswertung der Daten keine Gruppenbildung unter den OE, weil jedes Institut/Lehrstuhl unabhängig ist. D.h. eine interdisziplinäre VLAN-Bildung, die dynamisch nach Projekten/Aufgaben/Teams gebildet werden muß, kommt selten bis gar nicht vor. Die einzigen interdisziplinäre Dienste sind die zentral genutzten Server, die aber unabhängig von den Teams betrieben werden.
   Ein einziges Institut am Standort Oettingenstraße arbeitet mit zeitlich befristeten Teams, die projektabhängig gebildet und aufgelöst werden.

3. Zukünftige Anforderungen an das Netz
Der letzte Teil des Fragebogens beinhaltet Fragen bzgl. der zukünftigen Anforderungen für die nächsten drei Jahre an das Netz: Expansion innerhalb des lokalen Netzes, geplante Applikationen, Verbesserung der Dienstgüte und Organisation des Netz-Managements. Die Auswertung der Daten hat ergeben, daß in den nächsten Jahren mit einem Zuwachs (Anzahl Netzanschlüsse) von 10% zu rechnen ist. Die meisten Institute erhoffen sich eine ständige Anpassung an die neuesten Trends (Betriebssysteme, Applikationen, Übertragungsgeschwindigkeit, etc.). Zum Thema Netz-Administration gibt es unterschiedliche Meinungen. Die Institute mit dem entsprechenden Know-How möchten ihr eigenes lokales Netz verwalten, Institute ohne einen ausgebildeten Administrator bevorzugen

eine Administration von externer Seite.
Viele Benutzer sehen die vorhandene Struktur als sinnvoll und richtig und möchten keine Veränderungen vornehmen, wenn ihre Eigenständigkeit dadurch nicht beibehalten wird. Es macht auch keinen Sinn, die Struktur innerhalb einer OE weiter zu analysieren, da jede OE selbständig ist und auch keine gebäudeglobale Struktur erwünscht ist.

Die allgemeinen Anforderungen, wie Expansionsmöglichkeiten, Migrationsmöglichkeiten zu neuen Technologien, Sicherheitskonzepte, sollen weiterhin unterstützt werden, aber ohne sonstige Einschränkungen in Kauf zu nehmen.

In der heutigen Netzstruktur werden alle Zugriffe auf einen zentralen Server innerhalb des Gebäudekomplexes Oettingenstraße über einen Router geleitet. Die Performance und Geschwindigkeit dieses Routers wird als nicht ausreichend bewertet und bildet einen Flaschenhals bei der Kommunikation auf zentrale Dienste. Gewünscht wird ein Zugriff auf die zentralen Server über ein geswitchtes Netz und nicht mehr über den Router.

Diese Informationen benötigt man, um den Einsatz der VLANs sinnvoll zu begründen.

5.2 Fazit

Die Auswertung des Fragebogens hat ergeben, daß die Angaben zum Teil unvollständig waren. Speziell die Angabe über zentral genutzte Server (Art, Anzahl, Lokalität) wurde oft nicht ausreichend beantwortet, so daß in Kapitel 8.3 auch nur ein Teil der zentralen Server aufgelistet bzw. zugeordnet werden konnte. Dies ergibt zwar eine gewisse Unschärfe in der Gesamtstruktur, die aber aufgrund der vorwiegenden Lokalität des Datenverkehrs keine große Auswirkung auf die weiteren Untersuchungen hat.

Kapitel 6

Ermittlung der vorhandenen Topologie

Dieses Kapitel beinhaltet die derzeitige Infrastruktur und die eingesetzten Komponenten am Standort Oettingenstraße. Unter Infrastruktur versteht man hier die Verkabelung im Gebäudekomplex, die Segmentierung des Netzes und die eingesetzte Übertragungstechnik. Das Ergebnis dieser Untersuchung ist ein Netzplan, der die geografische und physische Netztopologie am Einsatzort darstellt.

6.1 Infrastruktur

Der Gebäudekomplex Oettingenstraße wurde vor zwei Jahren der LMU zur Verfügung gestellt. Im Auftrag vom Netzbetreiber (LRZ) wurde die entsprechende Infrastruktur in diesem Gebäude errichtet.
Die Grundlage dieses Gebäudes bildet eine relativ neue Infrastruktur, die nach den damals neuesten Standards errichtet wurde. Hier findet man ein geswitchtes, PC- und Workstation-basierendes Netz.

Verkabelung
Da es sich hier um eine relativ neue Infrastruktur handelt, ist das Gebäude mit einer "modernen" strukturierten Verkabelung (Grundlagen siehe Kap. 3.2.1) erschlossen. Im Gebäudekomplex Oettingenstraße wurde eine sternförmige Verkabelung realisiert.
Bei der Sternstruktur ist jede Station mit einer zentralen Vermittlungsstation verbunden, die die Nachrichten gemäß ihrer Zieladresse an den Empfänger weiterleitet. Bei jedem Übertragungsvorgang ist also die zentrale Vermittlungsstation einzuschalten (Bild 6.1).
Die Vorteile der Sternstruktur sind: die relativ einfache und kostengünstige zentrale Netzsteuerung, -kontrolle und -wartung, und die leicht erweiterbare Struktur. Beim Ausfall einer Leitung oder einer Station wird das Gesamtsystem nicht beeinträchtigt. Die Abhängigkeit aller Endgeräte von der zentralen Vermittlungsstelle ist allerdings ein gravierender Nachteil der Sternstruktur. Fällt diese Vermittlungsstelle aus, ist keine Datenübertragung mehr möglich und das Gesamtsystem bricht zusammen.

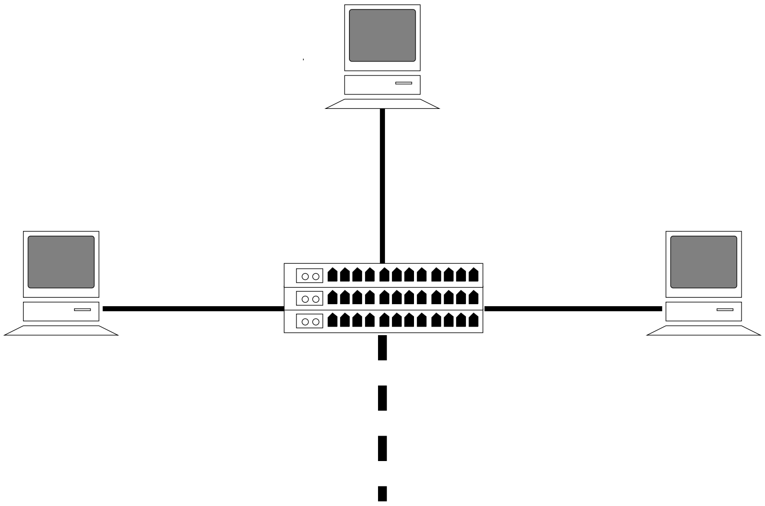


Abbildung 6.1: Physische Sternstruktur mit Uplink

In Bild 6.2 ist exemplarisch die strukturierte Verkabelung mit den Vermittlungsstationen dargestellt. Die Endgeräteanschlüsse werden sternförmig mit einem Verteiler in der Etage verbunden. Diese Etagenverteiler werden an einen zentralen Gebäudeverteiler angeschlossen. An diesem Gebäudeverteiler wird die Anbindung an das MHN über eine 100 Mbit-Leitung zum LRZ realisiert.
Wie in der strukturierten Verkabelung (Kap. 3.2.1) schon erwähnt wurde, beschränkt sich ein modernes Netz auf zwei Kabeltypen: LWL-Kabel und symmetrische Kupferkabel (Kap. 3.2.2). Auch im Gebäudekomplex Oettingenstraße sind diese zwei Kabeltypen im Einsatz, und zwar:

- im Primärbereich (zwischen LRZ und Standort Oettingenstraße)
  → Singlmode LWL (9/125 μm)
- im Sekundärbereich (zwischen den Etagen)
  → Multimode LWL (50/125 μm)
- im Tertiärbereich (auf den Etagen)
  → Twisted Pair (Kat. 5, 100 Ω)
- als Arbeitsplatzverkabelung (zwischen Dosen und Endgeräten)
  → Patchkabel

Segmentierung
Das derzeitige Netz wird durch Switches und Router in Subnetze unterteilt. Der Router segmentiert dieses Netz in acht Subnetze, wobei jede OE einem (oder mehreren) Subnetz(en) zugeteilt wird. Die logische Netzstruktur des Gebäudekomplexes Oettingenstraße ist in Abb. 6.3 dargestellt.

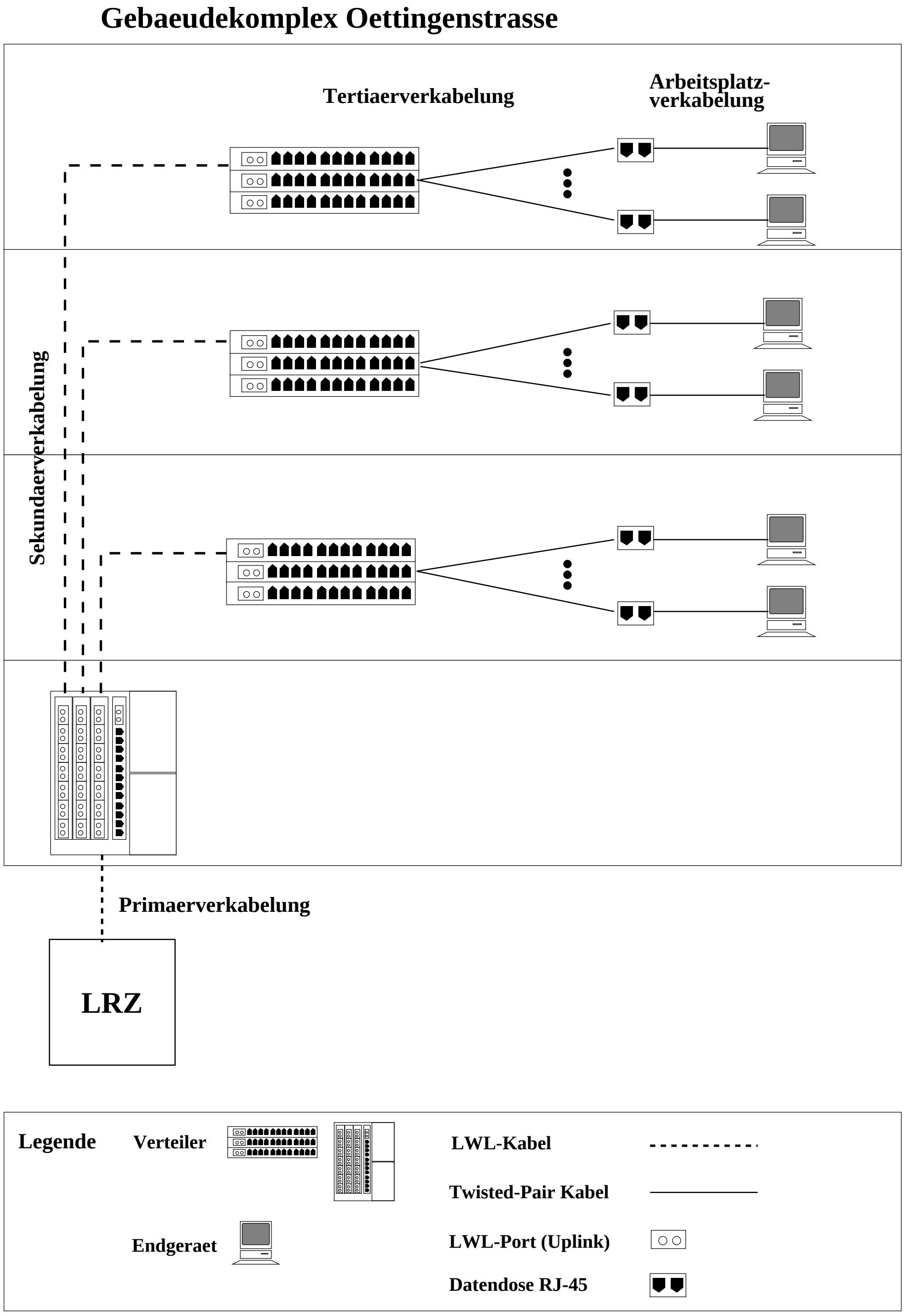


Abbildung 6.2: Strukturierte Verkabelung am Einsatzort

Der Router begrenzt den Broadcast-Verkehr auf ein Subnetz und damit auf eine OE. Innerhalb eines Subnetzes werden, abhängig von der Anzahl der Benutzer einer OE, Switches eingesetzt. Diese teilen die Subnetze in mehrere unabhängige Collision-Domains. Da die Anzahl der Benutzer pro Collision-Domain drastisch reduziert wird, kann der Datendurchsatz innerhalb eines Subnetzes deutlich

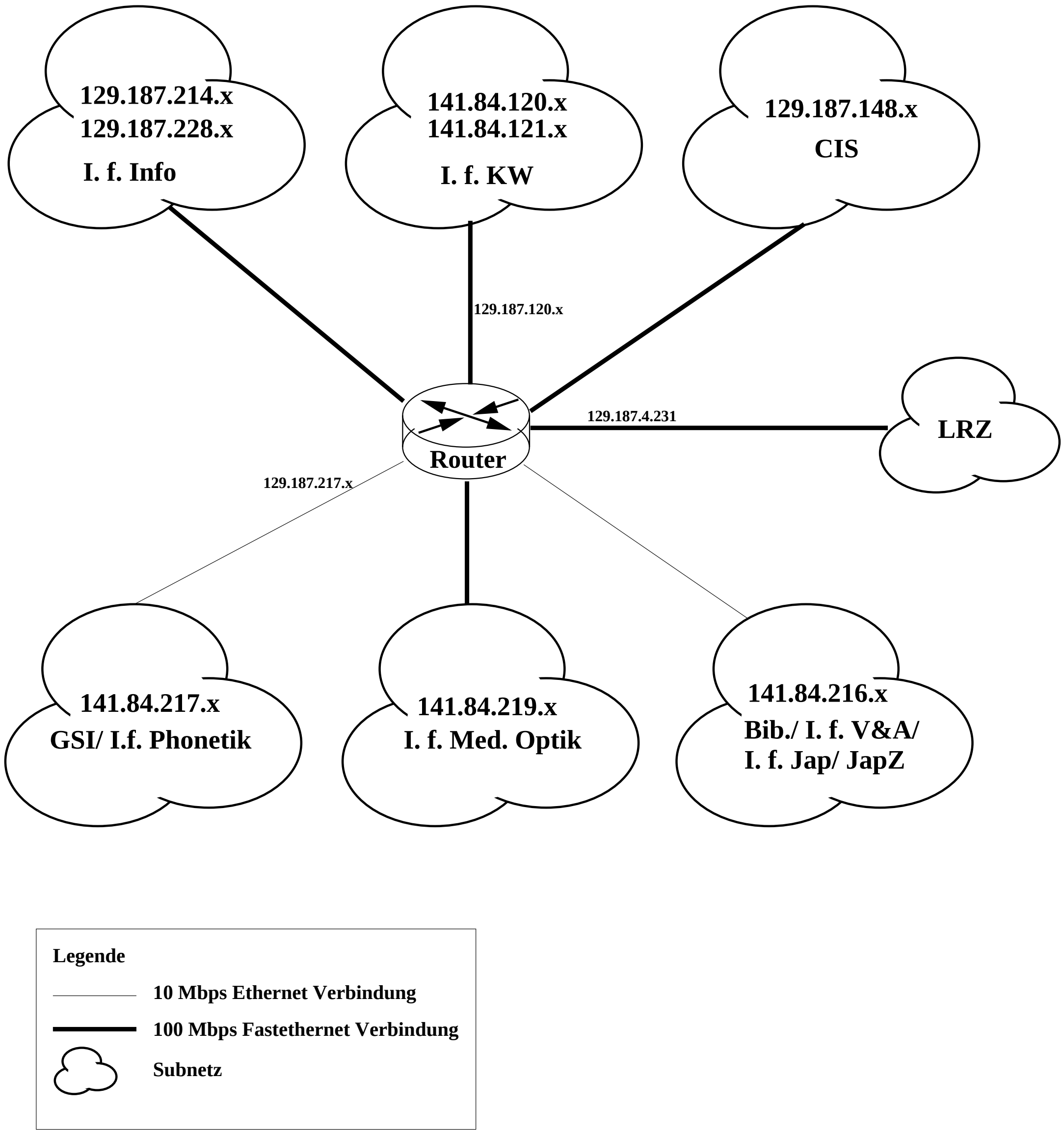


Abbildung 6.3: Logische Netztopologie Oettingenstraße

gesteigert werden.

Technologie

Im Gebäudekomplex Oettingenstraße wird Ethernet und Fast-Ethernet als Übertragungstechnik eingesetzt. Ethernet wurde in den 80er Jahren zum IEEE-Standard 802.3 erklärt und zählt zu den traditionellen Netzen. Aufgrund der großen Verbreitung (70 %) und der ständigen Weiterentwicklung kann davon ausgegangen werden, daß diese Technologie noch sehr lange in den Netzen zu

finden sein wird.
Im ursprünglichen Standard wurde das Ethernet als Busstruktur, basierend auf einem Koaxkabel als gemeinsamem Übertragungsmedium, konzipiert. Durch den häufigen Einsatz in verschiedenen Umgebungen waren im Laufe der Zeit Adaptionen auf andere Übertragungsmedien nötig, die dann als Erweiterung des Standards veröffentlicht wurden. Der IEEE 802.3 Standard umfaßt folgende Untergruppen:

- 10Base5 Standard-Ethernet (Yellow Cable)
- 10Base2 Thin-Ethernet (Cheapernet)
- 1Base5 StarLAN
- 10BaseT Ethernet auf Twisted-Pair
- 10Broad36 Ethernet auf Breitband
- 10BaseF Ethernet auf Lichtwellenleiter
- 100BaseX Fast-Ethernet (X = T oder F)
- 1000BaseX Gigabit-Ethernet

Im Gebäudekomplex Oettingenstraße sind heute die 10BaseT, 100BaseT und 100BaseF Standards eingesetzt.

- 10BaseT
  Mit diesem Standard können Ethernet-Daten auf Vierdraht-Twisted-Pair (symmetrisches Kupferkabel) mit einer Impedanz von 100 Ω übertragen werden. Die maximale Daten-Geschwindigkeit beträgt bei dem 10BaseT-Standard 10 MBit/s. Die Länge eines Twisted-Pair-Segments beträgt aufgrund der maximal zulässigen Dämpfung von 11,5 dB bei 10 MHz nur 100 Meter.
  Mit dem 10BaseT-Standard werden heute sternförmige Technologien aufgebaut, die aber logisch wie ein Bus arbeiten.

- 100BaseX
  Auf der physikalischen Ebene unterstützt Fast-Ethernet sowohl Twisted-Pair (100BaseTx und 100BaseT4) als auch Glasfaser-Kabel (100Base-Fx). Auf der logischen Ebene ändert sich beim 100BaseX-Standard nichts gegenüber dem alten 10 MBit/s-Standard, so daß die bisher eingesetzten SW-Produkte weiterverwendet werden können. Die maximale Daten-Geschwindigkeit beträgt 100 MBit/s. Der Fast-Ethernet-Standard unterstützt den Full-Duplex-Übertragungsmodus, sodaß eine Gesamt-Übertragungsrate von 200 MBit/s erreicht werden kann.

6.2 Komponenten

Rechnernetze können auf verschiedenen Schichten miteinander verbunden werden. Die Schicht auf der die Koppelung stattfindet, bestimmt welche Hardware eingesetzt wird. Bei einer Koppelung auf der physikalischen Schicht (Physical Layer) sind Komponenten notwendig, die einzelne Bits auf den Leitungen zwischen zwei (oder mehreren) Kabelsträngen kopieren. Diese Geräte werden als Repeater bezeichnet. Der Koppelung auf der Sicherungsschicht (Data Link Layer) dienen Bridges und Switches. Diese Komponenten kopieren die Frames eines Teilnetzes in ein anderes Teilnetz. Router verbinden unabhängige Netze auf der Vermittlungsschicht (Network Layer) und haben daher eine Gateway-Funktion. Findet die Koppelung auf einer höheren Schicht statt, werden Protokollkonverter benötigt.
Im Gebäudekomplex Oettingenstraße werden folgende Komponenten eingesetzt: ein Router, Switches und Hubs.

- Router
  - Hersteller: Bay Networks
  - Bezeichnung: Typ Backbone Concentrator Node (BCN)
  - Der Router verbindet die 8 Netzsegmente (Subnetze) in diesem Gebäude.
  - Über eine festgeschaltete Verbindung wird zwischen dem Gebäudekomplex Oettingenstraße und dem LRZ - und damit für alle Endgeräte - ein transparenter Datenfluß auf der Schicht-3 über den Router möglich (Bild 6.4).

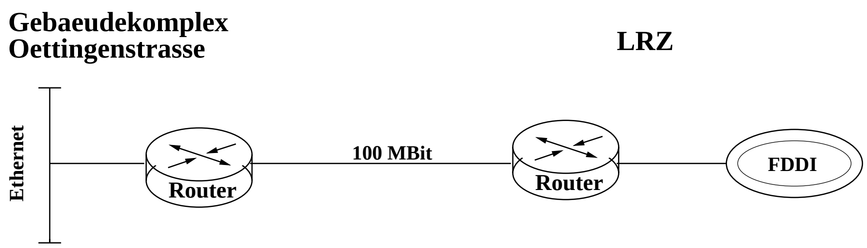


Abbildung 6.4: Verbindung über Router zw. Oettingenstr.- LRZ

- Switch
  - Hersteller: 3Com
  - Bezeichnung: SuperStack II Switch 1000 (LS1000) und SuperStack II Switch 3000 (LS3000)
  - Funktionen: allg. siehe Kap. 3.3. Diese Switches unterstützen Ethernet- und Fast-Ethernet (100BaseX) Infrastrukturen.
- Hubs

  - Hersteller: 3Com
  - Bezeichnung: SuperStack II Hub 10 und SuperStack II Hub 100
  - Funktionen: Diese Hubs unterstützen Ethernet- und Fast-Ethernet (100BaseX) Infrastrukturen.

6.3 Netzplan

Das Ergebnis der Ist-Analyse der Topologie am Einsatzort ist ein Netzplan. Die grafische Darstellung in Abb. 6.5 beinhaltet die geografische Netztopologie (Verkabelung, Komponenten, etc.) im Gebäudekomplex Oettingenstraße.
Im gesamten Gebäudekomplex liegt eine strukturierte Verkabelung vor. Die besteht aus einem zentralen Gebäudeverteiler und 10 weiteren Verteilerräumen (Etagenverteiler), die jeweils einen speziellen Versorgungsbereich abdecken. Um die räumlichen Gegebenheiten (Entfernung der Endgeräte innerhalb einer OE) und die Exklusivität der Komponenten (für jede OE eigene Komponenten/Switches) zu unterstützen, gibt es mehrere Versorgungsbereiche. Unter einem Versorgungsbereich (VB) versteht man ein oder mehrere Switches und ihre Verbindungen zu den Anschlußdosen, an die man die Endgeräte anschließen kann. Manche Versorgungsbereiche bedienen ausschließlich Endgeräte einer einzigen OE, andere Versorgungsbereiche bedienen Endgeräte aus mehreren OE.
Der "zentrale Gebäudeverteiler" (Keller, Z) besteht aus mehreren Komponenten. Fast jeder OE wird ein Switch als Koppelelement zwischen dem Router und den OE-eigenen[1] Etagenverteilern zur Verfügung gestellt.

- I.f.Info → 2 Switches
- I.f.Komm.Wiss. → 1 Switch
- CIS → 1 Switch
- GSI/Phonetik → 1 Switch
- Bib/V&A/Jap/JapZ → 1 Hub
- I.f.Med.Optik → 1 Switch

In diesem Verteilerraum befinden sich aber auch Etagenverteiler (1 Switch für GSI/Phonetik, 2 Switches für I.f.Med.Optik). In Abb. 6.5 definiert ein Rechteck die Gesamtanzahl der Komponenten einer OE in einem Verteilerraum. Zur grafischen Vereinfachung führt jeweils nur eine Verbindung vom OE-eigenen Gebäudeverteiler zu den einzelnen Etagenverteiler. In der Praxis existiert zu jedem Etagenverteiler einer OE eine explizite Verbindung zum OE-eigenen Gebäudeverteiler.
Im Anhang B findet man eine ähnliche Darstellung des Netzplanes.

[1] Switches, die fast ausschließliche einer OE zur Verfügung gestellt werden

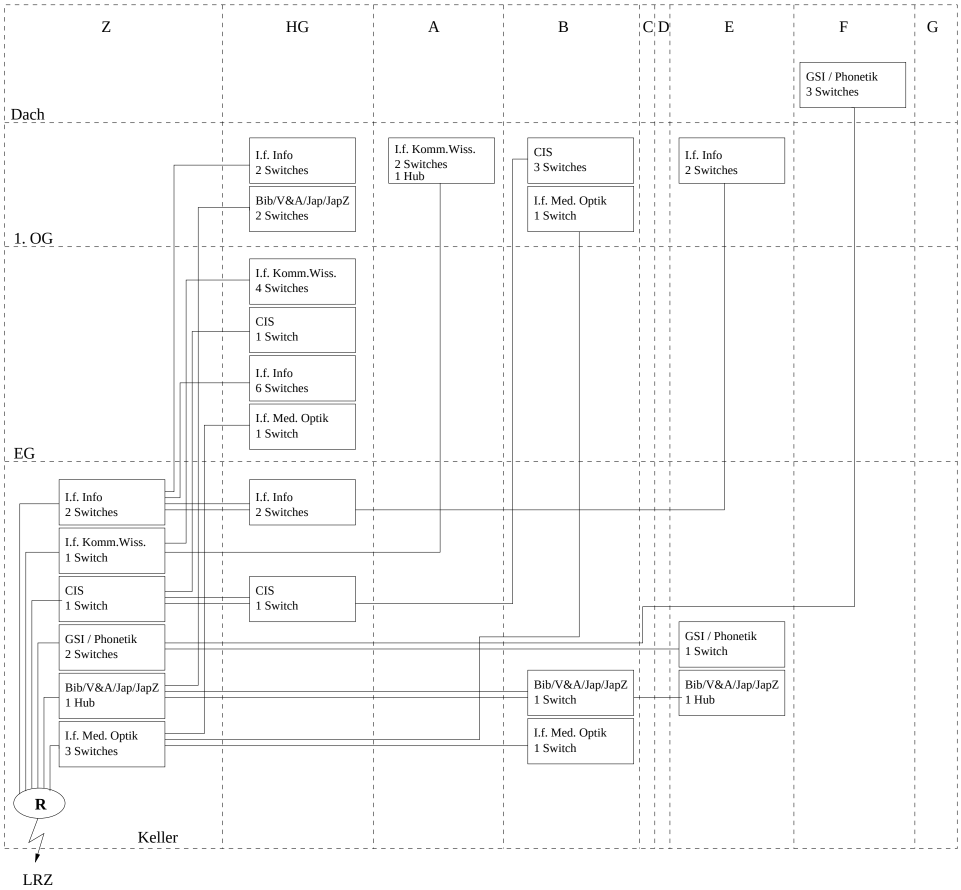


Abbildung 6.5: Infrastruktur im Gebäudekomplex Oettingenstraße

Kapitel 7

Ermittlung der Anforderungen des Betreibers

7.1 Überblick über das LRZ

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften betreibt das Münchner Hochschulnetz (MHN). Das MHN ist eine nachrichtentechnische Infrastruktureinrichtung zum Zweck der Datenkommunikation. Das MHN besteht aus:

- den Gebäudenetzen,
- den Campusnetzen, die die Gebäudenetze miteinander verbinden, und
- dem Backbonenetz, das die Campusnetze miteinander verbindet.

An dieses Netz sind derzeit der größte Teil der Münchner Hochschulen und Fachhochschulen im Münchner Raum angeschlossen.
Zu dem MHN gehören die Standorte:

- Ludwig-Maximilians-Universität (LMU)
- Technische Universität München (TUM)
- Bayerische Akademie der Wissenschaft (BAdW)
- Fachhochschule München (FHM)
- Fachhochschule Weihenstephan

Zum MHN gehören alle Übertragungseinrichtungen (aktive und passive Komponenten) einschließlich der Anschlußpunkte der Endgeräte.

Allgemeines zum MHN

- **Struktur**
  Das MHN besteht aus einem FDDI-Backbonenetz, an dem z.Zt. über Router und Switches die einzelnen Netze der Hochschuleinrichtungen an den

verschiedenen Standorten angeschlossen sind. Der Router trennt die verschiedenen Instituts- und Gebäude-LANs. Abhängig von der Größe und dem Verkehrsaufkommen des einzelnen Standortes erfolgt die Anbindung mit unterschiedlichen Technologien (sternförmig, ringförmig) an das LRZ. Die Router und Switches sind untereinander z.Zt. je nach Bandbreitenbedarf des einzelnen Standortes mittels FDDI (100 Mbit/s) oder (Fast)-Ethernet (10 Mbit/s oder 100Mbit/s) verbunden. Das physische Medium besteht in der Regel aus Glasfaserstrecken, die von der Deutschen Telekom AG bzw. von den Münchner Stadtwerken langfristig angemietet worden sind.

- **transportierte Protokolle**
  Standardmäßig wird IP und IPX als Transportprotokoll eingesetzt. Aber auch andere Protokolle können nach Rücksprache mit dem LRZ verwendet werden.

- **eingesetzte Netzkomponenten**
  Aus Support-Gründen (Management, Konfiguration, Logistik) werden im MHN für gewisse Aufgaben nur eine Klasse bzw. ein Typ von Geräten eingesetzt.

  - FDDI-Switch: Hersteller XYLAN
  - Router: Hersteller Bay Networks
  - Switches und Hubs: Hersteller 3Com
  - FDDI-Konzentratoren: Hersteller Interphase

- **Management-Systeme**
  Die eingesetzten Management-Anwendungen werden alle auf die Netzmanagementplattform HP-OpenView aufgesetzt. Für das Management der 3Com-Switches wird das Produkt Transcend 4.2 verwendet.

- **Backbone**
  Die Art des Anschlusses der einzelnen Standorte (FDDI, Ethernet) an das Backbonenetz des MHN ist abhängig vom transferierten Datenvolumen und der Größe des jeweiligen Standortes.

- **Administration**
  Das LRZ ist für das gesamte Backbonenetz, für die Anbindung der oben aufgezählten Netze an das MHN und z.T. für die angeschlossenen Institute zuständig. Die meisten Gebäude-LANs werden zentral vom LRZ betreut. Als Übergabeschnittstelle wird in der Regel die Endgeräteschnittstelle angesehen. Das Management der einzelnen LANs erfolgt dann in Absprache mit den Institutsverantwortlichen. In definierten Fällen, wenn Know-how im Institut vorhanden ist (Institut für Informatik der TUM, Medizinische Fakultäten Rechts der Isar, Großhadern und der Innenstadt-Kliniken haben eigene Rechenzentren), kann als Übergabeschnittstelle auch die Schnittstelle zum Router festgelegt werden.

Die Standorte, die an das MHN angeschlossen werden, sind über die gesamte Münchner Region verteilt (i.w. Münchner Stadtgebiet, Garching, Fürstenfeldbruck und Weihenstephan). Insgesamt gehören 36 Standorte zu dem MHN.
Diese Standorte werden weiter in Gebäude- und/oder Instituts-LANs segmentiert.

LANs zentral vom LRZ betreut	ca. 200+
LANs vom Institut selbst betreut	ca. 10+

Das LRZ betreut insgesamt weit über 20.000 Hosts, davon:

- IP-Objekte: ca. 20.000+,
- Novell-Server: ca. 130+,
- Novell-Clients: Anzahl unbekannt.

- **Außenanbindung**
  Das MHN ist über einen 155 Mbit/s-Anschluß an das deutsche Breitband-Wissenschaftsnetz (B-WiN) angeschlossen. Über diesen Anschluß wird der gesamte Datenverkehr des MHN von und nach außen, d.h. national über das deutsche Wissenschaftsnetz (WiN und B-WiN) und international über das weltweite Internet, abgewickelt.

7.2 Aufgaben des LRZ

Das LRZ als Betreiber des MHN, u.a. auch des Standortes Oettingenstraße (LMU), ist verantwortlich für einen sicheren und möglichst störungs- und unterbrechungsfreien Betrieb, und die Bereitstellung diverser Dienste. Zu seinen Aufgaben gehören ([10]):

1. der Betrieb und die Weiterentwicklung des MHN.
   Das LRZ verwaltet nicht nur den laufenden Betrieb, sondern plant auch für die Zukunft. Im Rahmen des Netzwerk-Investitions-Programm (NIP) wird eine flächendeckende Verkabelung der Hochschulgebäude vorgesehen, so daß alle Institute an das MHN angeschlossen werden können. Weiterhin bemüht sich das LRZ um die ständige Anpassung des Netzes an die technische Entwicklung und den vorhandenen Betrieb.

2. das Netzmanagement.
   Das LRZ ist für das Netzmanagement (z.B. Betrieb, Fehlerbehebung, Konfiguration von Netzkomponenten) zuständig. Das Netzmanagement ist aber nur für die Teile und Komponenten des Netzes möglich, die vom LRZ beschafft, bzw. die auf Empfehlung und mit Zustimmung des LRZ beschafft wurden. Das Netzmanagement ist dem LRZ zudem nur unter aktiver Mitarbeit von Netzverantwortlichen möglich. Diese werden durch den Einsatz geeigneter HW/SW-Werkzeuge vom LRZ unterstützt. Weiterhin teilt das LRZ den einzelnen Bereichen Namens- und Adreßräume zu, deren Eindeutigkeit sowohl bei Adressen als auch bei Namen eindeutig ist, um einen reibungslosen Betrieb zu garantieren.

3. die Bereitstellung diverser Dienste.
   Das LRZ stellt den Benutzern eine Reihe von Diensten zur Verfügung, wie WWW, Email, News, FTP, DNS, Backup, Modem-/ISDN-Zugang, etc.

4. die Unterstützung der Benutzer bei der Durchführung ihrer DV-Aufgaben (Beratung, Ausbildung, Bereitstellung von Dokumentationen und Anwendersoftware).

Es ist zu erkennen, daß die Aufgaben des LRZ weit gefächert und sehr umfangreich sind, so daß in den einzelnen Punkten Bedarf nach Optimierung und Minimierung des Aufwands besteht.

7.3 Anforderungen des LRZ

Das LRZ als Netzbetreiber verwaltet viele LANs, viele Endgeräte und damit die gesamte Infrastruktur des MHN. Aufgrund dieser Größe (in Kap. 7.1 beschrieben) besteht natürlich Bedarf, den administrativen Aufwand zu minimieren. Dazu soll sowohl Manpower, Ressourcen als auch Kosten reduziert werden.

Der Einsatz von virtuellen LANs wird in dieser DA am Beispiel des Gebäudekomplexes Oettingenstraße untersucht. Es soll geklärt werden, ob mit Hilfe dieser modernen Netze eine Optimierung in Manpower, Ressourcen und Kosten zu erreichen ist. Es gibt natürlich noch andere Gründe, warum VLANs in ein Netz eingeführt werden sollen, die aber für diese Arbeit nicht weiter untersucht werden:

- Einschränkung des Broadcast-Verkehrs,
- Sicherheit innerhalb des Netzes zu verbessern etc.

Am Standort Oettingenstraße, der zur LMU gehört, sind 9-10 Institute und die Bibliothek über einen Router ans MHN angeschlossen. Der Router segmentiert das Netz in weitere Instituts-LANs, an die über mehrere Switches die Endgeräte angeschlossen werden. Die heutige Netzstruktur sieht eine exklusive Zuordnung der Switches zu den einzelnen Instituten (OE) vor. Eine OE kann sich räumlich über mehrere Flügel und Etagen im Gebäude erstrecken. Wegen der strukturierten Verkabelung und den räumlichen Gegebenheiten gibt es mehrere Verteilerräume, an die die Endgeräte der OE angeschlossen werden. Ein Verteilerraum beinhaltet z.B. einen Versorgungsbereich von 20 Endgeräten aus einem Flügel. Diese Endgeräte gehören aber zu verschiedenen OE, und sind dementsprechend an die "institutseigenen"-Switches gekoppelt. Daraus resultiert, daß in vielen Verteilerräumen mehrere identische Komponenten eingesetzt werden müssen, obwohl die Teilnehmer-Anschlüsse auf weniger Komponenten aufgeteilt werden könnten. Eine solche Aufteilung soll mit Hilfe der VLANs durchgeführt werden.

Mit dem Einsatz von virtuellen Netzen und mit der Tatsache, daß ein Versorgungsbereich Endgeräte aus verschiedenen Gruppen abdeckt, ist es möglich, an eine gemeinsame Komponente verschiedene Endgeräte eines Versorgungsbereiches anzuschließen. Dadurch werden die Switch-Ports besser ausgelastet und es können einige Switches eingespart und folglich Kosten reduziert werden.

Das LRZ erhofft sich durch den Einsatz von virtuellen LANs im Gebäudekomplex Oettingenstraße eine Ressourcenoptimierung und u.U. eine Dezentralisierung der Netzadministration in den einzelnen Instituten.

7.4 Motivation für diese Diplomarbeit

Die Anforderungen des Betreibers (LRZ) an das MHN, bzw. für den Spezialfall des Standortes Oettingenstraße, stellen gleichzeitig die Motivationsgründe für diese Diplomarbeit dar.
Zusammenfassend kann festgehalten werden, was man sich konkret durch den Einsatz von VLANs am Standort Oettingenstraße erhofft:

- Ressourcenoptimierung → Kosten reduzieren
- Administration vereinfachen

Teil III

Planungs-Phase

Kapitel 8

VLAN Szenarien

Dieses Kapitel beschreibt die Analyse verschiedener VLAN-Szenarien, in denen die Endgeräte bzw. die Teilnehmer in logische Gruppen zusammengefaßt werden. Alle Teilnehmer, die einer Interessensgruppe angehören, können unabhängig von ihrem Standort eine Netzgruppe (VLAN) bilden.

VLANs können nun nach verschiedenen Kriterien konzipiert werden. Deshalb ist es notwendig, eine Vorstellung zu entwickeln, welche Kriterien beim Design und bei der Realisierung von VLANs ausschlaggebend sein sollen. Von diesem strategischen Standpunkt aus betrachtet, können VLANs auf zwei Arten gebildet werden. Das sind:

- Infrastructural VLANs
- Service-Based VLANs

Zunächst werden die zwei VLAN-Bildungskriterien allgemein definiert und anschließend an den Gegebenheiten im Gebäudekomplex Oettingenstraße gespiegelt. Dies geschieht zunächst unabhängig von den technischen Implementierungsdetails.

8.1 Infrastructural VLANs

Die Bildung von "infrastructural" VLANs beruht auf der direkten Abbildung der Organisationsstruktur. Wie in Kapitel 4 bereits erwähnt, kann die Organisationsstruktur grafisch in einem Organisationsdiagramm dargestellt werden. Die einzelnen Organisationseinheiten (wie z.B. Funktionsbereiche, Abteilungen, Arbeitsgruppen, etc.) bilden ihr eigenes VLAN.
Das Infrastruktur-Modell ist exemplarisch in Abb. 8.1 dargestellt. Alle Teilnehmer sollen auf einen zentralen email-Server zugreifen können. Hierzu ist notwendig, daß dieser Server Teilnehmer in allen VLANs (OE: Entwicklung, Finanzen, Vertrieb) ist. Der Abrechnungs-Datenbank-Server soll nur für die Finanzabteilung zugänglich sein. Somit ist dieser Server auch nur Teilnehmer in dem VLAN 2.
Dieses Modell sieht eine VLAN-Strukturierung anhand der organisatorischen

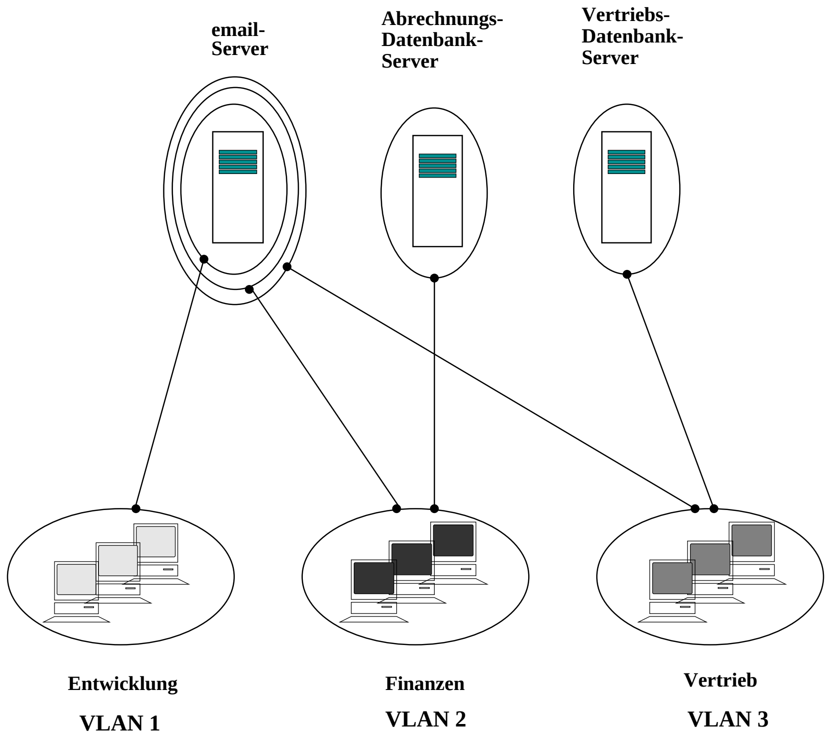


Abbildung 8.1: Infrastructural VLAN

Einheiten im Unternehmen vor. Server und darauf implementierte Dienste werden gezielt einzelnen Abteilungen, und damit einzelnen VLANs, zugeordnet. Dies hat zur Folge, daß zentral genutzte Server Teilnehmer in mehreren VLANs sind.
Das Infrastruktur-Modell orientiert sich strikt an den vorhandenen Organisationsstrukturen im Unternehmen und ist deshalb oft der erste und einfachste Versuch, VLANs zu bilden.

8.2 Service-Based VLANs

Die Bildung von "service-based" VLANs beruht nicht auf der Abbildung der Organisationsstruktur, sondern auf den individuellen in Anspruch genommenen Diensten. Die Definition der einzelnen VLANs richtet sich in diesem Fall nach den angebotenen Diensten. Jeder Server wird als eigenständiges VLAN betrachtet. Deshalb ist es notwendig, alle zentral zur Verfügung stehenden Dienste zu erfassen und jedem Dienst/Server ein eigenes VLAN zuzuordnen. In Beispiel 8.3 existieren folgende Dienste:

- email-Server → VLAN 1
- Abrechnungs-Datenbank-Server → VLAN 2
- Vertriebs-Datenbank-Server → VLAN 3

Alle Endgeräte, die den Dienst auf einem Server nutzen wollen, müssen auch Teilnehmer dieses VLANs sein. Endgeräte, die verschiedene Dienste beanspruchen, sind immer auch gleichzeitig Teilnehmer in verschiedenen VLANs. Um die Endgeräte den entsprechenden VLANs zuweisen zu können, ist zunächst eine Erfassung der jeweils benötigten Dienste notwendig (siehe oben). Danach erfolgt die Zuweisung der Endgeräte zu den VLANs. Dies kann anhand einer Ent-

Dienst / Teilnehmer	email-Server VLAN 1	Abrechnungs-Datenbank-Server VLAN 2	Vertriebs-Datenbank-Server VLAN 3
A	x		
B	x	x	
C	x		x
D	x		
E	x		x
F	x		
G	x		x
H	x	x	

Abbildung 8.2: Entscheidungsmatrix für Service-Based VLAN

scheidungsmatrix, wie in Abb 8.2 dargestellt, ermittelt werden. Hierbei können Teilnehmer, unabhängig von ihrer Organisations-Zugehörigkeit, Mitglied von verschiedenen VLANs werden (vgl. Abb. 8.3). Es können unterschiedliche Benutzerprofile gebildet werden:

- Teilnehmer A, D, F
- Teilnehmer B, H
- Teilnehmer C, E, G

In Abb. 8.3 ist exemplarisch ein "service-based"-VLAN dargestellt. Die Teilnehmer der Organisationseinheit Marketing werden, abhängig von ihrem Aufgabenschwerpunkt, verschiedenen VLANs zugeteilt. Alle Teilnehmer bekommen Zugriff auf den email-Server. Aber Teilnehmer H darf zusätzlich auf den Abrechnungsdatenbank-Server und Teilnehmer C auf den Vertriebs-Datenbank-Server zugreifen, obwohl ihre Organisations-Zugehörigkeit nur Marketing ist.

Dieses kleine Beispiel zeigt schon, wie komplex ein "service-based"-VLAN zu entwickeln ist. Es muß eine genaue Kenntnis über die Benutzung (Art, Zugangsberechtigung, etc.) der verschiedenen Servern von den einzelnen Teilnehmern vorliegen. Daraus ergibt sich, daß viele Teilnehmer Mitglied einer Menge von VLANs werden. Die Komplexität dieses Modells ist also abhängig von der Anzahl der zu managenden VLAN-Mitgliedschaften innerhalb einer Gruppe. Diese Komplexität kann nur mit Hilfe von Automatismen beim VLAN-Management

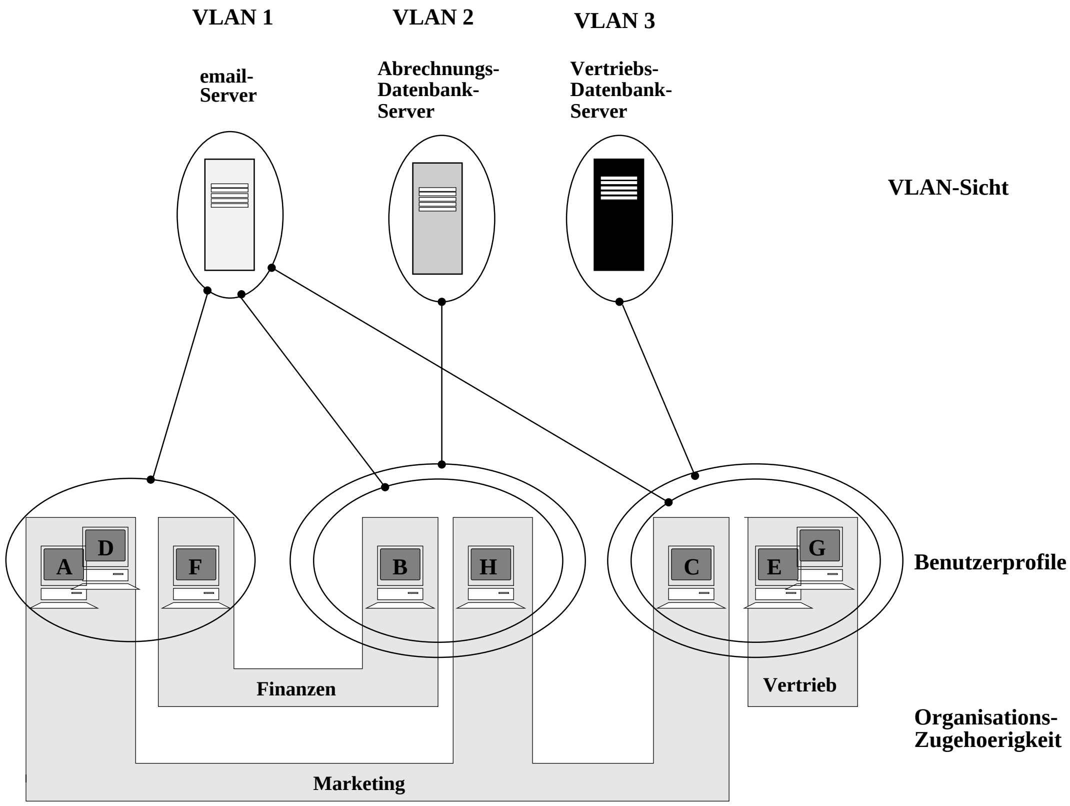


Abbildung 8.3: Service-Based VLAN

(Konfiguration) reduziert werden.
Das “service-based”-Modell ist wesentlich komplexer aufgebaut und erfordert erheblich mehr Aufwand bei der Definition der Strukturen als das “infrastructural”-Modell. Es bietet aber größere Flexibilität bei der Zuweisung der individuellen Anforderungen der Teilnehmer zu verschiedenen VLANs. Speziell im Zuge der Zentralisierung von Diensten in einem Server-Pool bietet dieses Modell eine bessere Lösung im Vergleich zum “infrastructural”-Modell.

8.3 VLAN-Bildung im Gebäudekomplex Oettingenstraße

Die logische Gruppierung der Endgeräte soll nun am Einsatzort, anhand der soeben definierten VLAN-Architekturen und den ermittelten Informationen aus den vorigen Kapiteln, vorgenommen werden:

- Infrastructural VLANs
  Design aufgrund der Informationen aus Kap. 4
- Service-Based VLANs
  Design aufgrund der Informationen aus Kap.5

Im Gebäudekomplex Oettingenstraße befinden sich 10 Institute und die Bibliothek, die im wesentlichen eigenständig ihre lokalen Server betreuen, die angeschlossenen Teilnehmer administrieren und ihre Ressourcen verwalten. Diese Struktur eignet sich ideal für ein Infrastruktur-Modell, bei dem die OE eigenständige VLANs bilden. Jedes Institut bzw. jeder Lehrstuhl bildet ein VLAN, d.h. alle Teilnehmer eines Institutes/Lehrstuhls gehören zu einer logischen Gruppe. Mit diesen Voraussetzungen ist ein reines Infrastruktur-Modell sehr leicht zu implementieren.
In dieser Organisation finden wir aber auch einen Sonderfall vor. Es existieren zentral genutzte Server, auf die mehrere OE zugreifen können. Diese Server sind in der Regel lokale, instituts- oder LRZ-eigene Server, die für mehrere OE zur Verfügung gestellt werden. Somit kann man zu dem "Infrastruktur"-Modell parallel auch eine "service-based"-Struktur aufbauen, die jedem Institut Zugang zu den zentralen Servern ermöglicht. Die Netzverantwortlichen der Institute bestimmen, wer auf die "lokalen" Server zusätzlich zugreifen dürfen.

Inst. / Appl. Dienste	IfP&SK	GSI	LFE NM	LFE PST	LFE DBS	LFE PMS	LFE TCS	CIP	JfMO	IfJap	JapZ	CIS	IfV&A	IfKW	If?	Bib
LRZ WWW	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
LRZ email		ja								ja	ja		ja		ja	ja
IfP&SK email, ... (Schellingstr.)	ja															
IfInfo email,news, DNS, NFS 1,2			ja	ja	ja	ja + NFS_2	ja	ja + NFS_2				NFS_1				
LFE NM NFS1,email NFS2,DNS,...			ja	NFS_2												

Abbildung 8.4: Entscheidungsmatrix: Institute - Server

Die in Tabelle 8.4 dargestellte Entscheidungsmatrix beschreibt, welche Institute/Lehrstühle Zugriff auf die zentralen Server haben. Diese Tabelle ist nicht vollständig in Bezug auf die Anzahl, Art und Benutzung der zentralen Server, aber für die weitere Untersuchung völlig ausreichend.
Abbildung 8.5 stellt nun gezielt die Zuordnung der einzelnen zentralen Server zu den VLANs (OE) dar. In diesem Bild erkennt man, daß keine vollständige Umsetzung des "service-based"-Modells vorgenommen wird. Es werden nicht einzelne Teilnehmer aus dem gesamten Gebäudekomplex nach ihren Anforderungen gruppiert, sondern die einzelnen OE (Institut/Lehrstuhl) bilden jeweils eine logische Gruppe. Jedem Institut/Lehrstuhl, das/der schon ein eigenes VLAN ist, werden zusätzlich ein oder mehrere zentrale Server zugewiesen, d.h. sie werden Mitglied in den VLANs der Services.

Das Ergebnis dieser Untersuchung ist eine mögliche VLAN-Definition, die nicht notwendigerweise genau einer Klasse von VLANs zugeordnet werden kann, sondern aus einer Kombination von “infrastructural”- und “service-based”-VLANs besteht. Diese Mischkonfiguration besteht aus dem “infrastructural”-Modell und dem “service-based”-Modell. Jede OE stellt ein eigenes VLAN dar. Zusätzlich kann jede OE Teilnehmer in weiteren VLANs sein, um auf zentrale Dienste zuzugreifen.

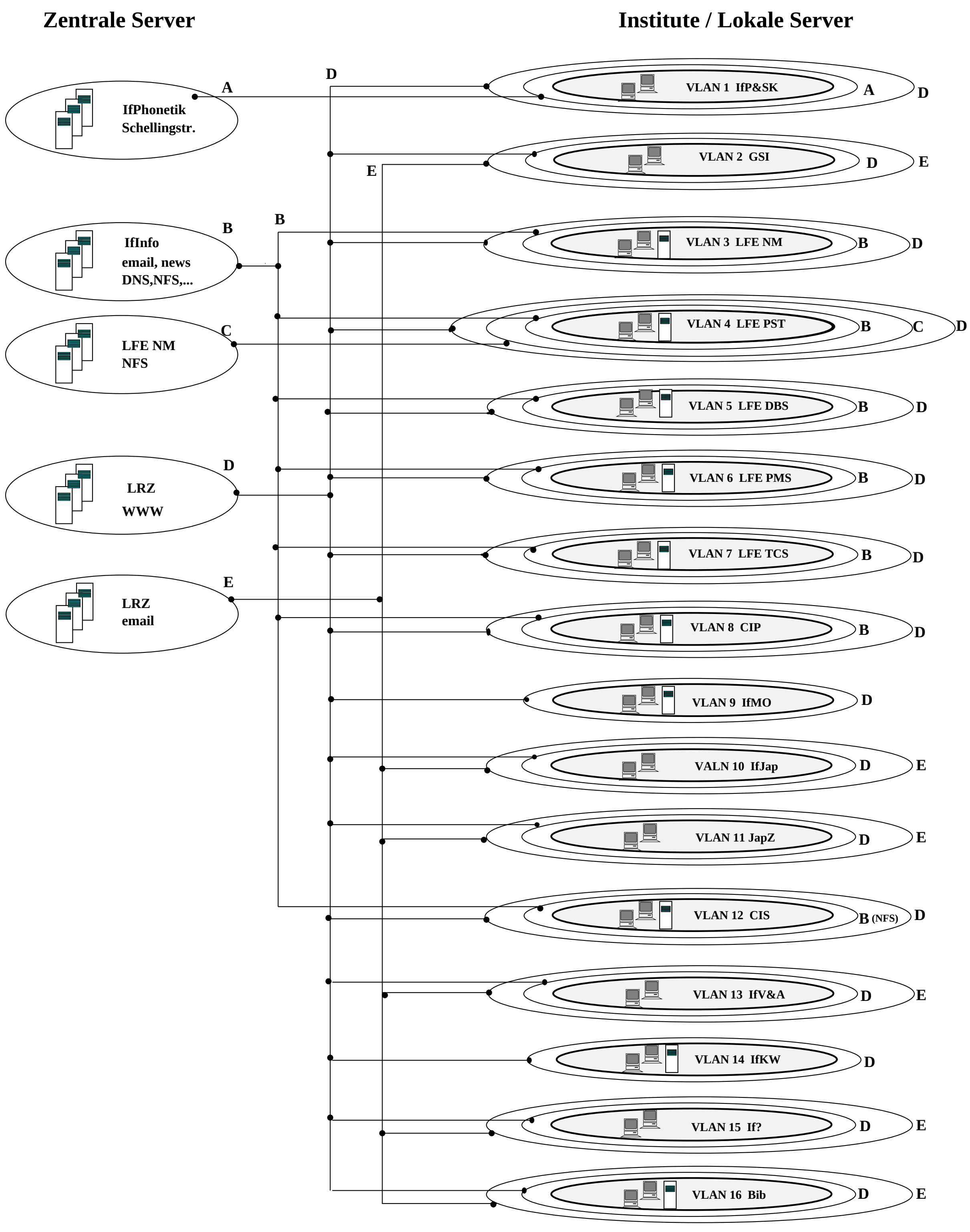


Abbildung 8.5: VLAN-Bildung am Einsatzort

Kapitel 9

Umsetzung VLAN-Szenarien am Einsatzort

Dieses Kapitel umfaßt die Untersuchung der verschiedenen VLAN-Techniken, die in Kap. 3.4.1, 3.4.2, 3.4.3 definiert wurden, am speziellen Beispiel Oettingenstraße. Dabei wird für jede Variante:

- Ausgangssituation,
- Umsetzung,
- Probleme und Lösungen,
- Vor- und Nachteile erläutert.

Ausgangssituation

Die Ausgangssituation, die für alle VLAN-Untersuchungen identisch ist, wird einmal am Anfang dieses Kapitels definiert. Die Ist-Voraussetzung (Ergebnis aus der Analysephase) des Gebäudekomplexes Oettingenstraße wird folgendermaßen charakterisiert:

- VLAN-Bildung
  Die VLAN-Bildung beruht auf dem Infrastruktur-Modell (Kap.8.1), d.h. eine direkte Abbildung der Organisationsstruktur. Das Netzwerk ist in 16 VLANs aufgeteilt:
  - VLAN 1 : IfP&SK
  - VLAN 2 : GSI
  - VLAN 3 : LFE NM
  - VLAN 4 : LFE PST
  - VLAN 5 : LFE DBS
  - VLAN 6 : LFE PMS
  - VLAN 7 : LFE TCS
  - VLAN 8 : CIP

  - VLAN 9 : IfMO
  - VLAN 10 : IfJap
  - VLAN 11 : JapZ
  - VLAN 12 : CIS
  - VLAN 13 : IfV&A
  - VLAN 14 : IfKW
  - VLAN 15 : If?
  - VLAN 16 : Bib

- OE/Benutzer
  Die OE sind statisch, abgeschlossen und eigenständig. Es finden weder Kommunikationsbeziehungen noch Mitarbeiter-Austausch zwischen den Instituten statt.
  Die Zuordnung der Endgeräte zu den OE ist vordefiniert.

- Anzahl der Endgeräte
  Im Gebäudekomplex Oettingenstraße existieren zur Zeit mehr als 400 Endgeräte. Es ist mit einem Wachstum, für die nächsten 5 Jahre, von ca. 10% zu rechnen (vgl. Kap. 5). Die Anschaffung von neuen Endgeräten ist z.T. abhängig von den dazukommenden Teilnehmern und dem verfügbaren Budget.

- vorhandenes Netz
  - geswitchtes Netz
  - Topologie: Ethernet und Fast Ethernet
  - Protokoll: überwiegend IP
  - Router als Koppelelement zwischen den OE
  - zentrale und externe Server (z.B. am LRZ)
  - Kommunikationsbeziehungen zwischen den VLANs: 80/20-Regel wird eingehalten (vgl. Kap. 5)

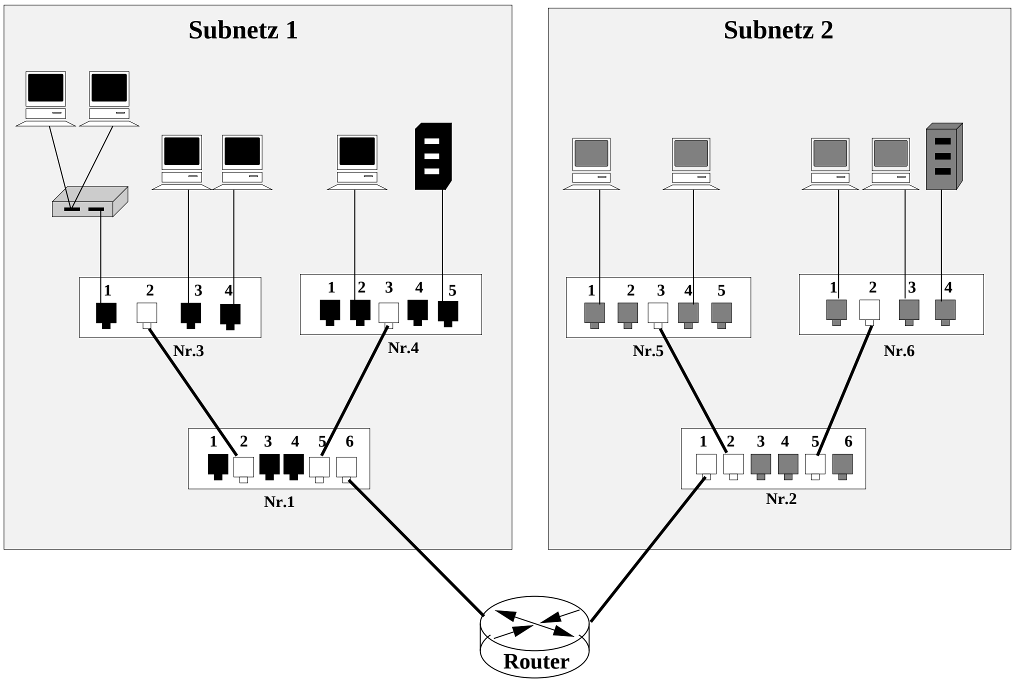
- Strukturierte Verkabelung
  Im gesamten Gebäudekomplex liegt eine strukturierte Verkabelung vor. An einer zentralen Stelle (Raum) findet die Anbindung an die Primär- und die Sekundärverkabelung statt. Als Gebäudeverteiler stehen z. Zt. sechs Switches für die jeweiligen OE zur Verfügung. Um die räumlichen Gegebenheiten (Entfernung der Endgeräte innerhalb einer OE) und die Exklusivität der Komponenten (für jede OE eigene Komponenten/Switches) zu unterstützen, gibt es mehrere Versorgungsbereiche. Unter einem Versorgungsbereich (VB) versteht man ein oder mehrere Switches und ihre Verbindungen zu den Anschlußdosen, an die man die Endgeräte anschließen kann. Ein Versorgungsbereich kann für mehrere OE bereitgestellt werden.

- Pläne für die nächsten Jahre
  - LRZ: ständige Anpassung an technologische Entwicklung
  - OE : kostenabhängig und teilnehmerabhängig

9.1 Layer-1-VLAN am Einsatzort

Die Layer-1- oder portbasierten-VLANs sind die einfachste Form VLANs zu implementieren. Deswegen werden in der Regel bei dem ersten VLAN-Einsatz portbasierte VLANs implementiert.

Ausgangssituation
Das derzeitige Netz ist logisch nach IP-Adressen segmentiert. Jede OE besitzt ihr eigenes Subnetz siehe Abb. 6.3. An einem Beispiel (Abb. 9.1) soll die vorhandene Situation dargestellt werden. Die Organisationsstruktur dieses Teilnetzes



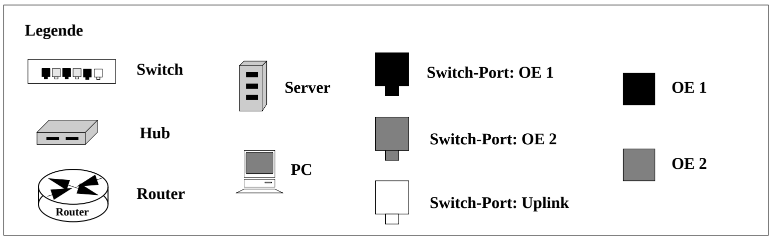


Abbildung 9.1: Layer-1-VLANs am Einsatzort: physischer Stand heute

besteht aus zwei OE. Die Endgeräte werden den entsprechenden OE zugeordnet, OE 1 (Farbe: schwarz) und OE 2 (Farbe: dunkelgrau). Die Subnetze werden analog zu den OE gebildet. Der Router dient als Koppelelement zwischen den Subnetzen. Die Kommunikationsbeziehungen beruhen auf der 80/20 Regel, also 80 % des lokalen Verkehrs verbleibt im eigenen Subnetz und nur 20 % des

Verkehrs werden geroutet.
Jedes Subnetz (OE) besteht aus einer Menge von Switches. Die Anzahl der Switches hängt von der Anzahl der Endgeräten in den OE ab. Die exklusive Zuordnung der Switches zu den OE kann eine unbestimmte Anzahl von nichtgenutzten Anschlüssen bei diesen Switches zur Folge haben. Allgemein gilt, daß die Anzahl der Teilnehmer einer OE nicht mit der Anzahl der ihnen zur Verfügung gestellten Switch-Ports entspricht.
Obwohl das derzeitige LAN-Netz alle wesentlichen Anforderungen erfüllt, stellt der Netzbetreiber (LRZ) noch die Anforderung, die Ressourcen zu optimieren.

Umsetzung
In Kap. 3.4.1 wurden die Grundlagen von portbasierten VLANs beschrieben. Die portbasierten VLANs sollen nun auf die Gegebenheiten des Gebäudekomplexes Oettingenstraße abgebildet werden. Diese Gegebenheiten wurden in der Ausgangssituation dargestellt.
Um die angesprochenen Probleme (Anforderungen) zu lösen, wird das LAN zu einem Layer-1-VLAN ausgebaut. Jedes Endgerät ist an einen Switch-Port angeschlossen. Die Zuordnung jedes Switch-Ports zu seinem VLAN muß konfiguriert werden. Wenn nun innerhalb eines Versorgungsbereiches die Komponenten nicht vollständig ausgelastet sind, können u.U. einige Switches eingespart werden, indem die freien Ports eines Switches mit den Endgeräten eines anderen Switches verbunden werden. Im Beispiel 9.1 stehen Switch Nr.4 und Switch Nr.5 in einem Raum und sind beide bis zu 50% belegt. Die Endgeräte, die an diesen Switches hängen, werden durch einfache Umkonfiguration alle an Switch Nr.5 aus Subnetz 2 angeschlossen. In diesem Fall kann Switch Nr.4 eingespart, oder für andere OE des Gebäudekomplexes zur Verfügung gestellt werden. Die portbasierte VLAN-Bildung, Abb. 9.2, sieht nun folgendermaßen aus:

- VLAN 1: Switch Nr.3 (Port 1,3,4) und Switch Nr.5 (Port 2,5)
- VLAN 2: Switch Nr.5 (Port 1,4) und Switch Nr.6 (Port 1,3,4)

Probleme
In dieser ersten Ausbaustufe, siehe auch Abb. 9.2, entstehen einige Probleme. Will ein Endgerät (Switch Nr. 3, Port 3) eine Verbindung zu einem Server (Switch Nr.5, Port 5) im eigenen VLAN (VLAN 1: schwarz) und Subnetz (Subnetz 1) aufbauen, so entstehen Kommunikationsprobleme. Die Kommunikation im eigenen VLAN (VLAN 1) kann nur über den Router stattfinden. Da aber der Router zum Flaschenhals wird, sollten die Broadcaststürme auf Subnetze beschränkt werden (Broadcastverkehr soll lokal, innerhalb eines Subnetzes, begrenzt werden). Dadurch soll die Auslastung des gesamten Netzes reduziert werden.

Lösung
Die Voraussetzungen für einen sinnvollen Einsatz von portbasierten VLAN müssen erfüllt werden.

- Die Switches müssen die portbasierten VLANs unterstützen.

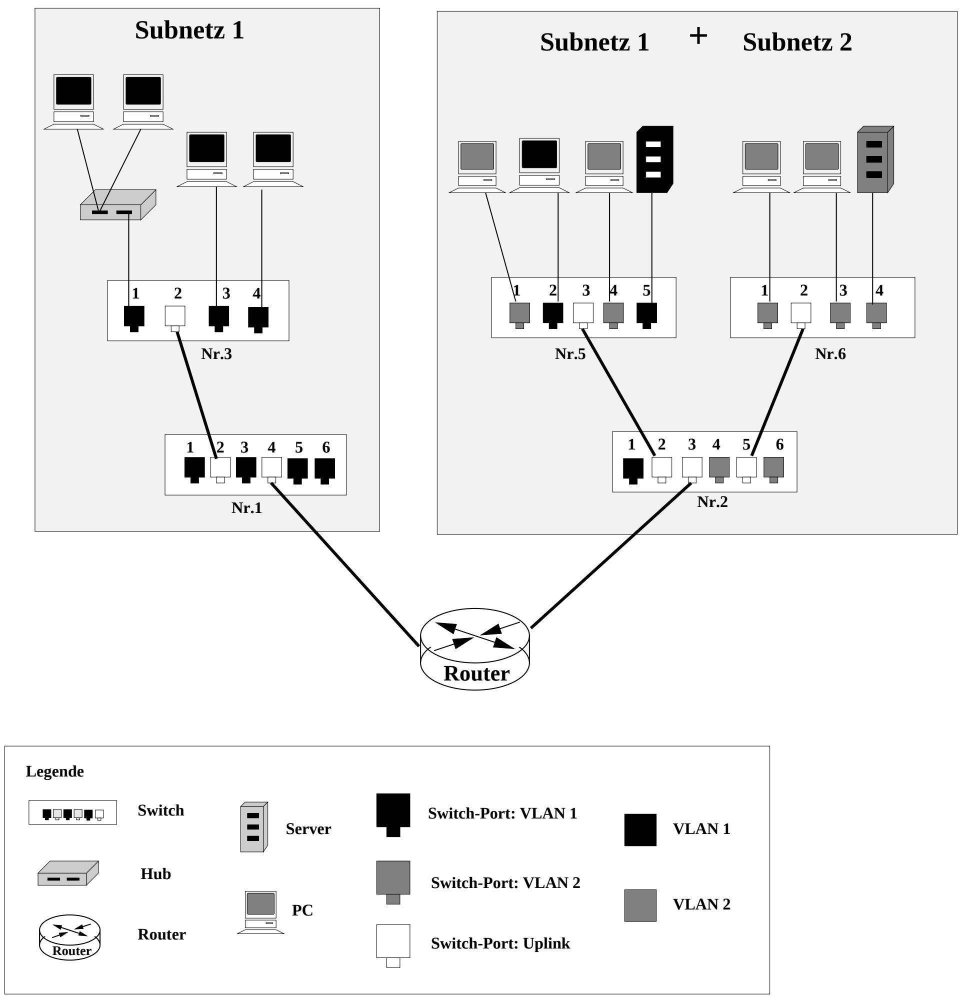


Abbildung 9.2: Layer-1-VLANs am Einsatzort: nach Umkonfiguration

- Die freien und belegten Ports der Switches müssen bekannt sein.
- Die Unterstützung mehrerer VLANs pro Switch-Port.
- VLANs über mehrere Subnetze sind nicht sinnvoll, da sonst die Kommunikation über Router geleitet wird. Bei routbaren Protokollen ist ein Datenaustausch nur möglich, wenn der Netzanteil beider Layer-3-Adressen identisch ist. Bei einem IP-Netzwerk sollten Server und Clients (allgemein die Endgeräte) zum gleichen IP-Subnetz gehören.
- Die Notwendigkeit eines zusätzlichen Switches, der am zentralen Router und an den Gebäudeverteilern angeschlossen ist (siehe Abb. 9.3), oder einer direkten Verbindung zwischen den Gebäudeverteilern (siehe Abb. 9.4) um den Intra-VLAN-Verkehr optimal zu ermöglichen.
- Der Router hat die Aufgabe den Inter-VLAN-Verkehr zu transportieren

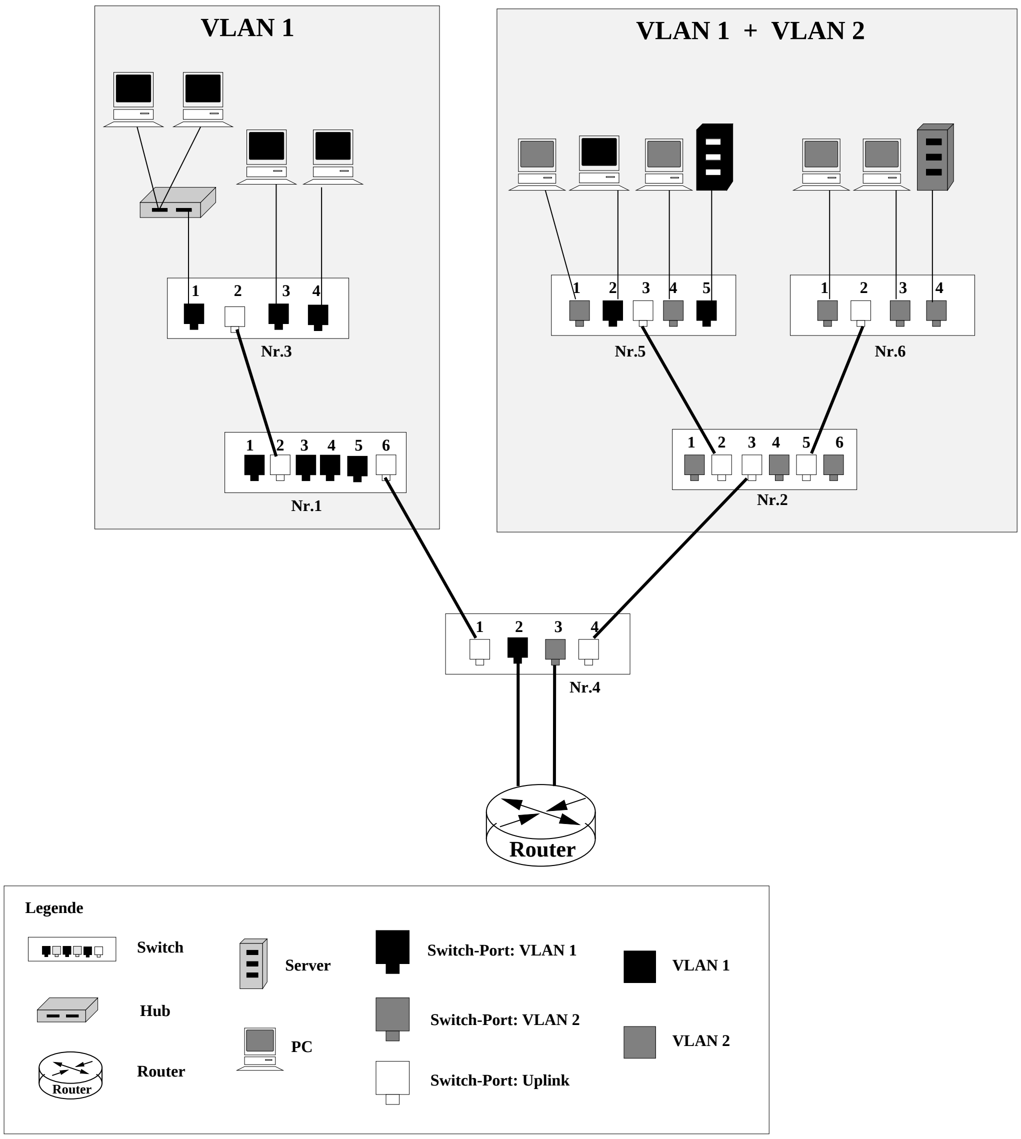


Abbildung 9.3: Layer-1-VLANs am Einsatzort: Lösung mit zusätzl. Switch

auf Basis der Layer-3-Adressen (IP). Dazu benötigt er zu jedem VLAN eine explizite Verbindung (Trunk-Leitung), über die die Pakete in die entsprechenden Broadcastdomains geleitet werden.

Vorteile

- schnelle, einfache Konfiguration
- ideale, einfache Lösung Ressourcen zu sparen, bzw. zu optimieren
- z.T. optimale Umsetzung von OE auf physische Struktur (OE festen

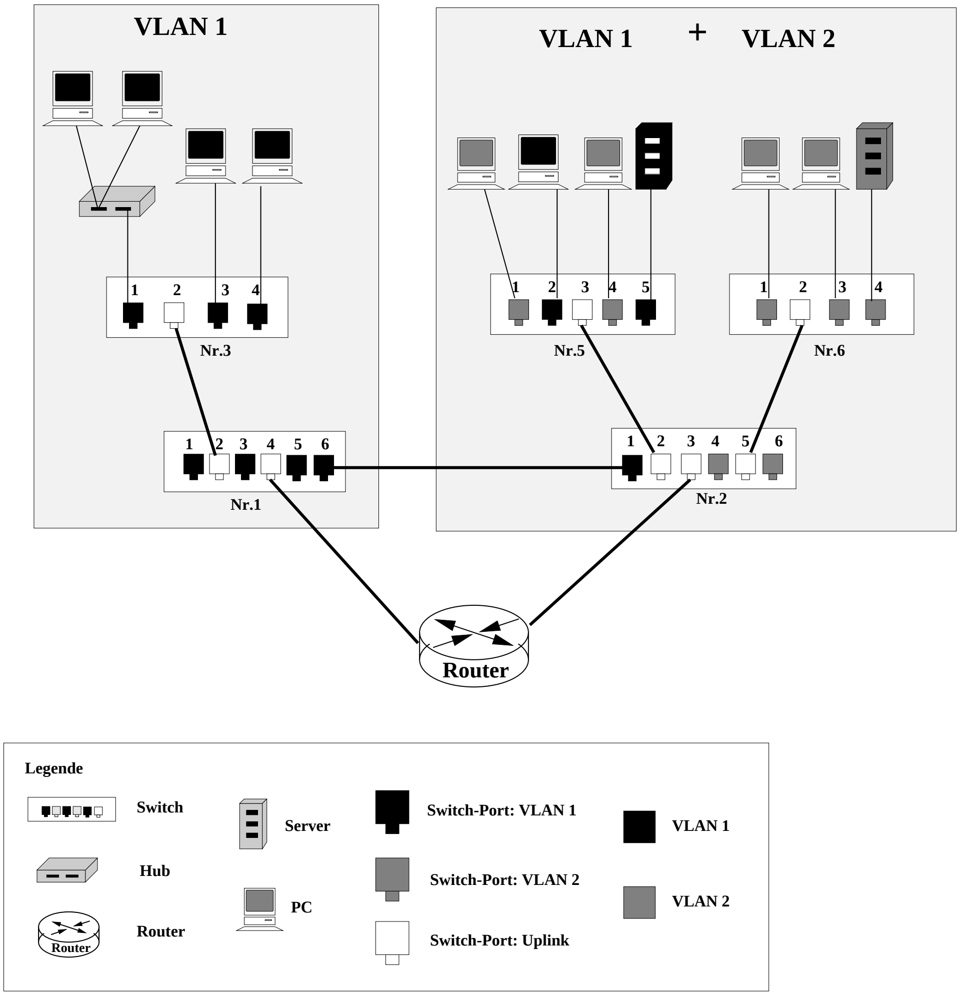


Abbildung 9.4: Layer-1-VLANs am Einsatzort: Lösung mit Verb. zw. Switches

Standort, kaum Umzüge)

Nachteile

- genaue Kenntnis über freie und belegte Ports von verschiedenen OE
- exakte Dokumentation über die Zuordnung der Endgeräte zu Switch-Port
- Ein Endgerät in mehreren VLANs → mehrere Netzkarten und je eine eigene Zugangsschnittstelle zu den verschiedenen VLAN-Ports

9.2 Layer-2-VLAN am Einsatzort

Bei der Planung von Layer-2-VLANs in diesem Gebäudekomplex gehen wir von der gleichen Ausgangssituation wie in Kap. 9.1 aus. Jede OE ist einem festen

IP-Subnetz zugeordnet und bildet ein VLAN. In diesem Fall bestimmen nicht

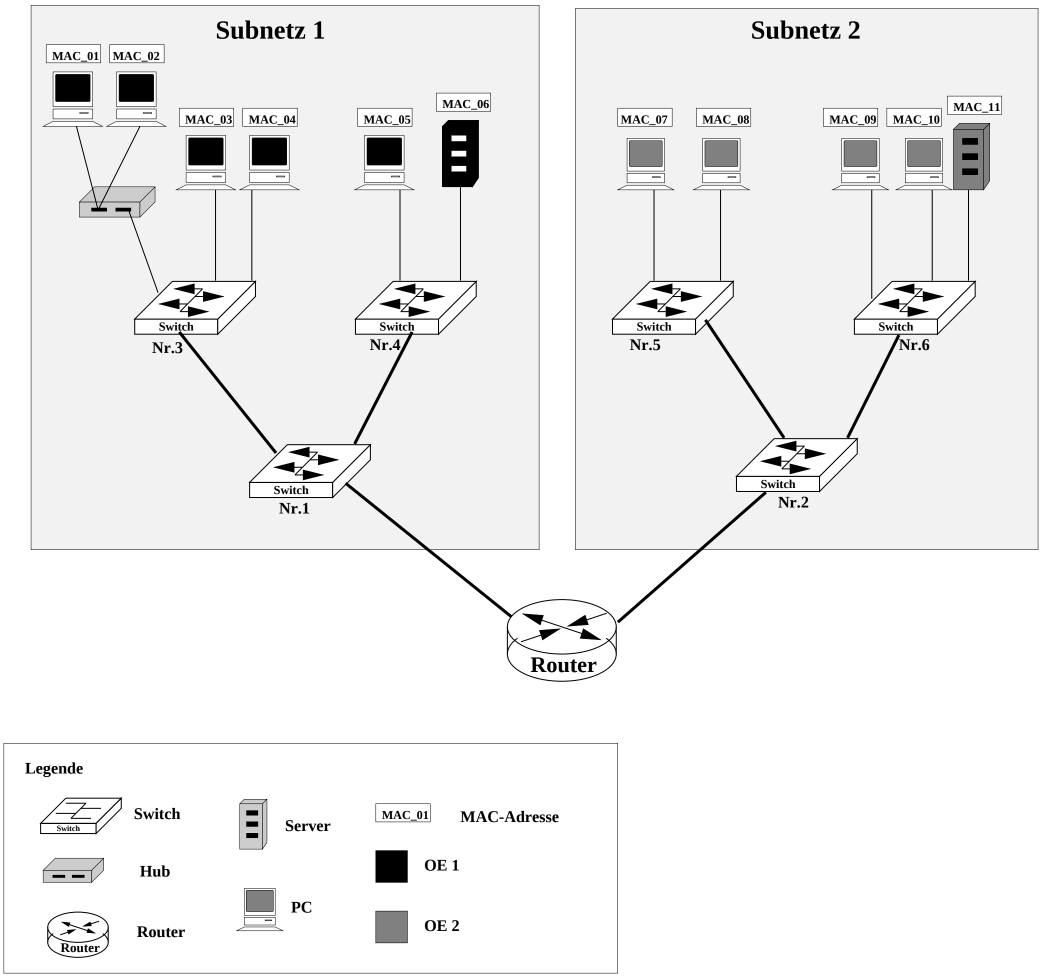


Abbildung 9.5: Layer-2-VLANs am Einsatzort: physischer Stand heute

die Ports die Zugehörigkeit zu einem VLAN, sondern die Endgeräte (speziell die MAC-Adressen) einer OE.

Umsetzung

An einem kleinen Netzausschnitt in der Oettingenstraße mit nur 2 Subnetzen (OE) wird die Gruppierung der Endgeräte innerhalb einer OE nach ihrer MAC-Adresse vorgenommen. Diese Situation ist in Abb. 9.5 dargestellt. Die OE 1 (=Subnetz 1) bildet VLAN 1 (Farbe: schwarz) und wird durch folgende Endgeräte bestimmt: MAC_01, MAC_02, MAC_03, MAC_04, MAC_05 und MAC_06. Zur OE 2 (Subnetz 2), also zum VLAN 2, gehören die Endgeräte MAC_7, MAC_08, MAC_09, MAC_10 und MAC_11. Zur Ressourcenoptimierung können die Endgeräte MAC_05, MAC_06, MAC_07 und MAC_08 an eine gemeinsame Komponente, Switch Nr.5, angeschlossen werden, da sie zu einem

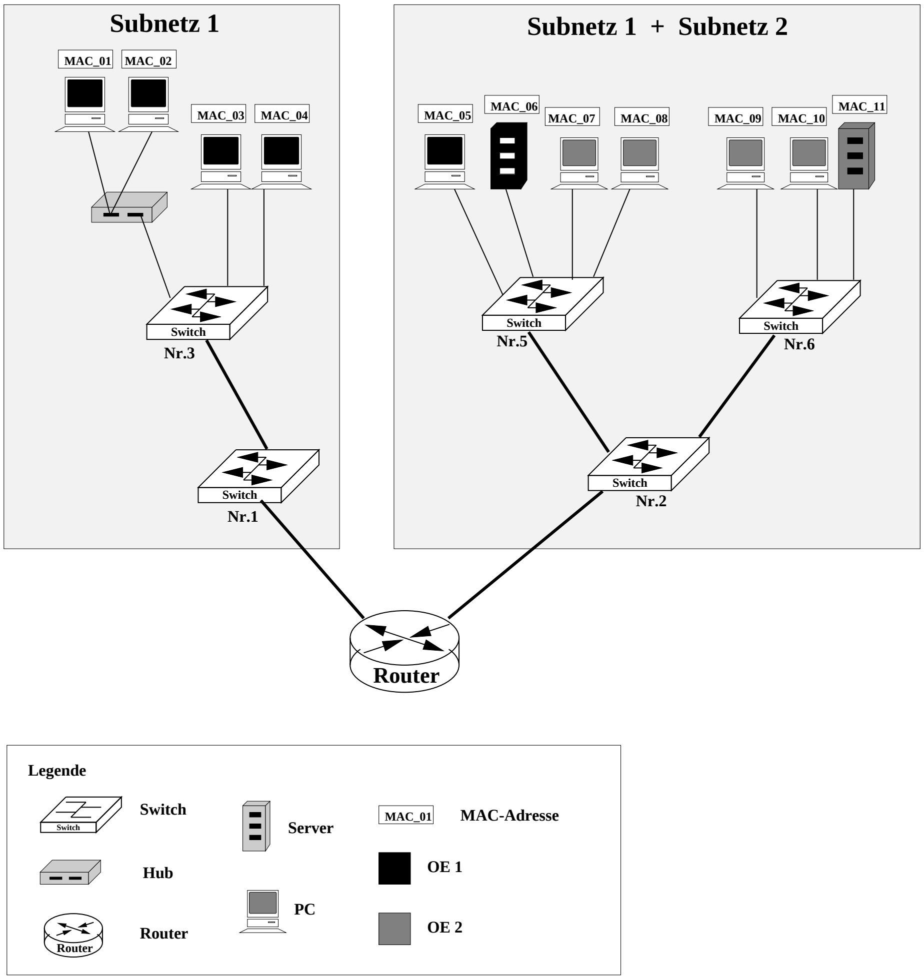


Abbildung 9.6: Layer-2-VLANs am Einsatzort: nach Umkonfiguration

Versorgungsbereich gehören (Abb. 9.6). Voraussetzung für eine Inter-Switch-Kommunikation ist, daß jeder Switch die Datenpakete bezüglich ihrer VLAN-Zugehörigkeit richtig interpretiert. Diese Informationen können durch Tagging oder Austausch von Adreßtabellen zur Verfügung gestellt werden.

Problem und Lösung

Es treten die gleichen Probleme auf wie bei den portbasierten VLANs. Der Intra-VLAN-Verkehr z.B. zwischen MAC_01 und MAC_6 wird über den Router geleitet. Deshalb ist auch hier eine direkte Verbindung zwischen den Gebäudeverteilern notwendig. Danach wird der Inter-VLAN-Verkehr weiterhin über den Router laufen aber der Intra-VLAN-Verkehr wird geswitcht. Die Funktionsweise kann aus Abb. 9.7 abgeleitet werden.

Vorteile

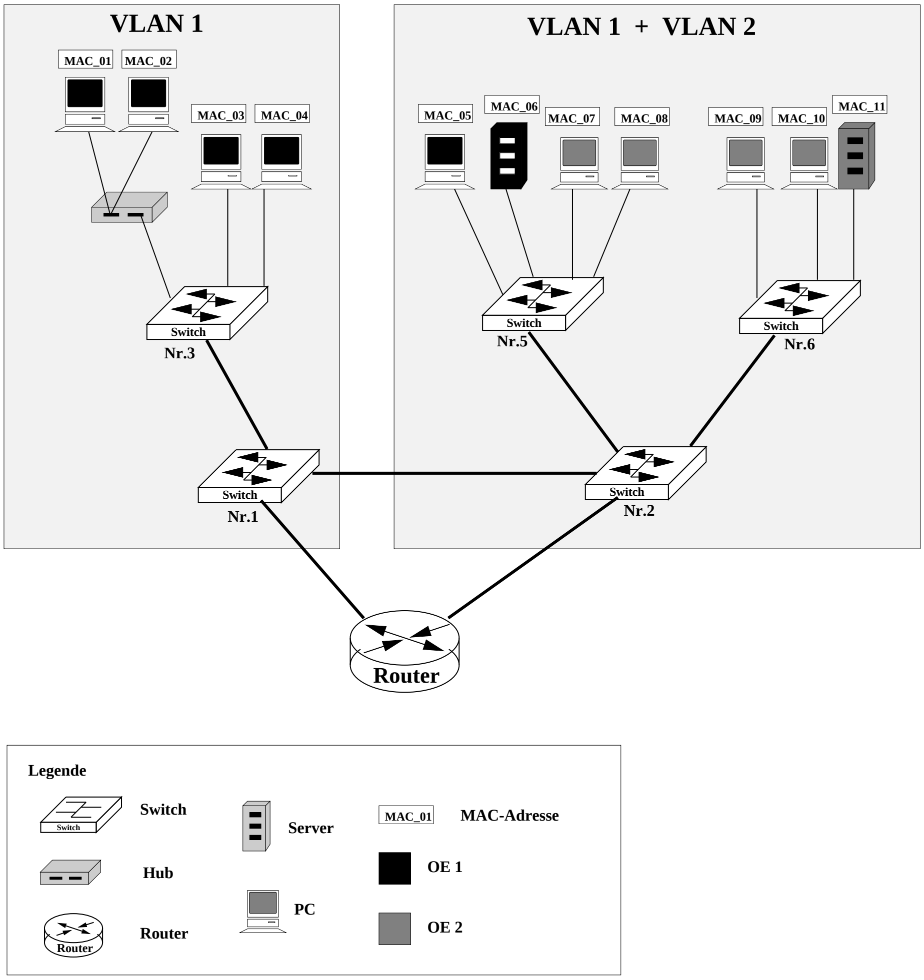


Abbildung 9.7: Layer-2-VLANs am Einsatzort: Lösung

- Ein möglicher Trend in Richtung mobile Systeme (Laptop mit integrierter Netzkarte) ist mit Hilfe von Layer-2-VLANs zu erreichen. Die Mitarbeiter einer OE oder die Studenten können sich dann innerhalb dieses Gebäudekomplexes, unabhängig vom Raum oder Institut (Bibliothek, CIP-Raum oder Büro) jeweils ins "richtige" Netz (VLAN) einloggen.
- An einen Hub können unterschiedliche VLANs/Teilnehmer angeschlossen werden (MAC_12, MAC_01, MAC_02).
- Die Netzadministration wird erheblich vereinfacht. Der Umzug innerhalb eines IP-Netzes/VLANs benötigt keinen administrativen Eingriff.

Nachteil

- hoher Konfigurationsaufwand, da jede MAC-Adresse explizit durch den Administrator einem VLAN zugeordnet werden muß

9.3 Layer-3-VLAN am Einsatzort

Im Gebäudekomplex Oettingenstraße existiert bereits ein IP-Netz, das nach Subnetzen (Layer-3-Adressen) logisch gebildet ist. Alle Endgeräte einer OE gehören zum selben Subnetz. In Abb. 9.8 ist auch erkennbar, daß alle Endgeräte einer OE nicht nur logisch zusammengefaßt werden, sondern auch physisch. Für jede OE werden eigene Netzkomponenten (Switches) zur Verfügung gestellt, als Gebäudeverteiler und Etagenverteiler.

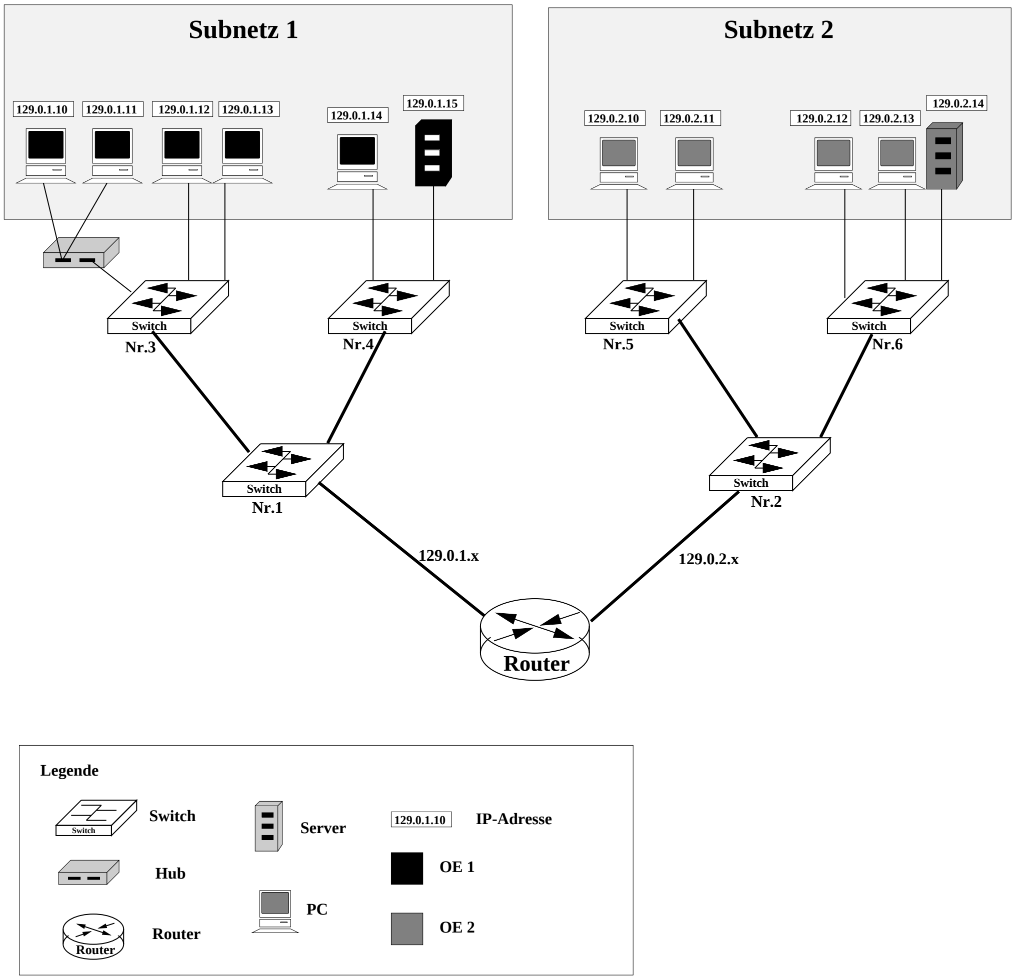


Abbildung 9.8: Layer-3-VLANs am Einsatzort: physischer Stand heute

Umsetzung

Die Zuordnung der Endgeräte einer OE zu ihrem VLAN ist hier automatisch durch die Subnetzbildung gegeben, siehe Abb. 9.8. Mit Hilfe von vorhandenen Operationen ist auch die Zugehörigkeit der Subnetze zu ihren entsprechenden VLANs einfach zu konfigurieren.

Um nun die Netzressourcen wie Switch Nr.4 und Switch Nr.5, die im selben Raum (gleichen Versorgungsbereich) stehen, aber unterschiedlichen OE gehören, optimal auszunutzen, werden alle Endgeräte von Switch Nr.4 an Switch Nr.5 angeschlossen. Nach dieser Umkonfiguration, Abb.9.9, wird der Intra-VLAN-Verkehr nicht mehr geswitcht, da nur eine Verbindung über den Router existiert.

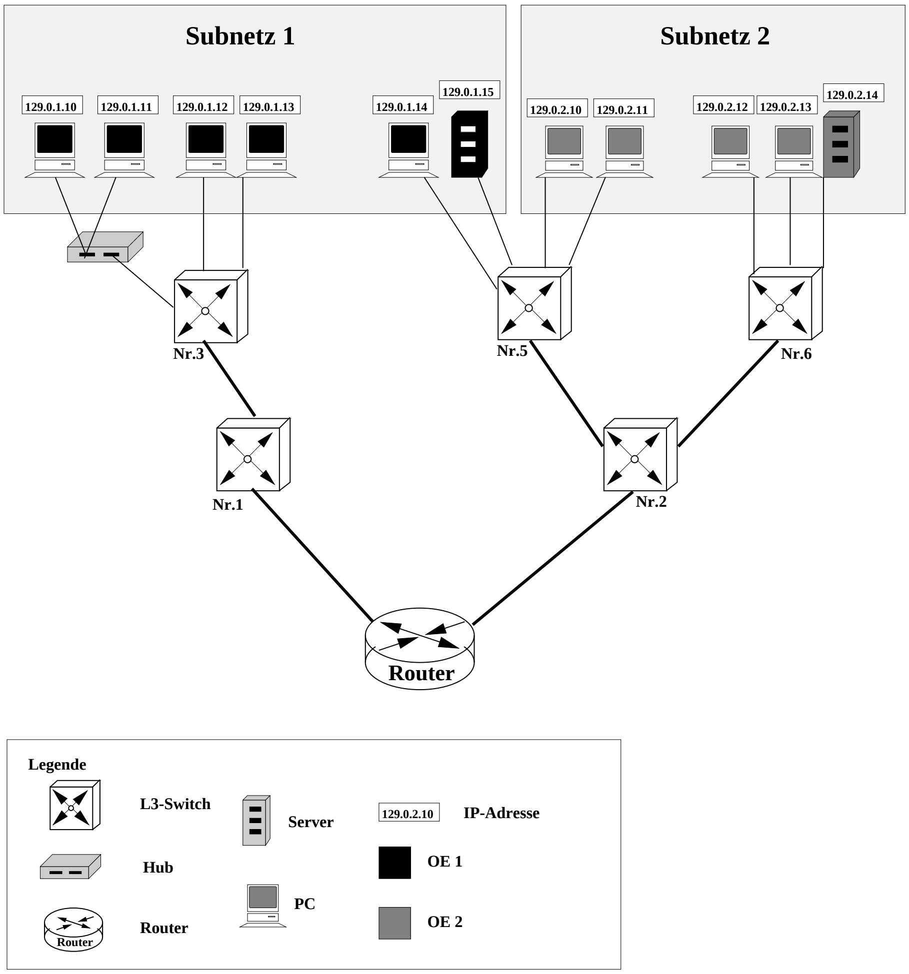


Abbildung 9.9: Layer-3-VLANs am Einsatzort: nach Umkonfiguration

Problem und Lösung

Bei dem Einsatz von Layer-3-VLANs (basierend auf IP-Subnetze) kann eine Trennung zwischen physischer und logischer Struktur erst dann erreicht werden, wenn der Intra-VLAN-Verkehr geswitcht wird. Dazu benötigt man Layer-3-Switches und eine direkte Verbindung zwischen den Gebäudeverteilern, die den Intra-VLAN-Verkehr ermöglichen. Somit kann jedes Endgerät eines Subnetzes (OE) unabhängig von seinem physischen Ort auf Schicht 2 erreicht werden. Diese Lösung ist in Abb. 9.10 dargestellt.

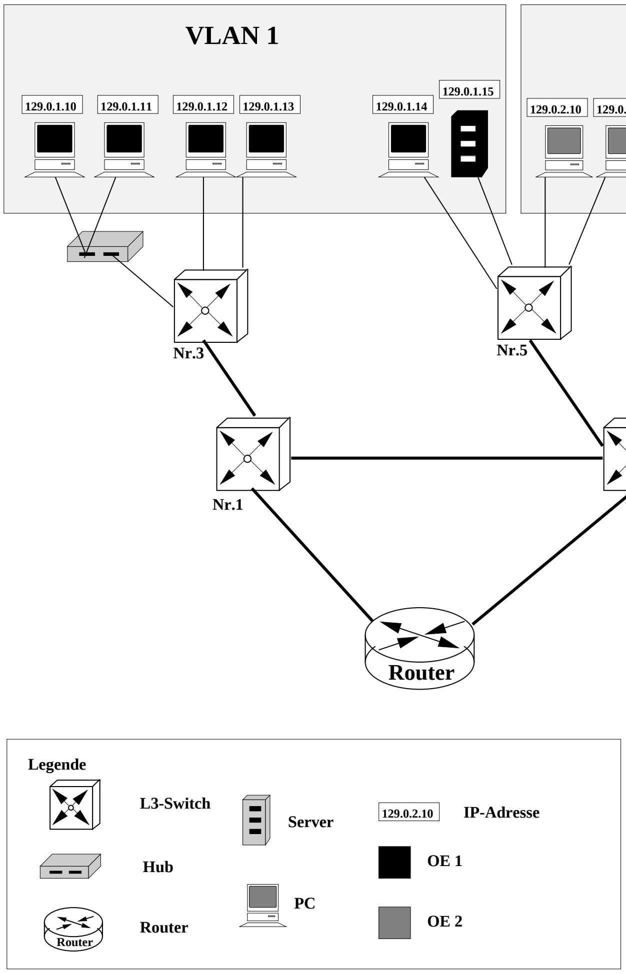


Abbildung 9.10: Layer-3-VLANs am Einsatzort: Lösung

Vorteile

- leichte Konfiguration und Administration bei moves, adds and changes (Umgang mit IP-Adreßstruktur bekannt, Einsatz von DHCP)
- wenn der Adreßraum (Subnetze) ausreichend groß gewählt wird, so ist eine Skalierung innerhalb eines VLANs jederzeit möglich.

Nachteil

- minimale Sicherheit. Die IP-Adressen lassen sich leicht mit entsprechender SW manipulieren. (Abhilfe mittels DHCP, bzw. einer zentralen IP-Vergabestelle).

9.4 Abgrenzung der VLAN-Szenarien

In diesem Kapitel werden die verschiedenen VLAN-Szenarien (portbasierte, MAC-basierte, IP-basierte VLANs), aufgrund einiger Kriterien, gegenübergestellt. Die Tabelle 9.1 soll einen kleinen Überblick geben, welche VLAN-Formen am Einsatzort unter bestimmten Anforderungsprofilen vorteilhaft sind.

9.4.1 Aufwand, um Endgeräte bei einer Erstinstallation einem VLAN zuzuordnen

Bei der Planung von VLANs stellt sich jeder Netzadministrator die Frage, welcher Aufwand (Zeit bei Netzkonfiguration) bei der Erstimplementierung anfällt. Da die meisten VLANs nicht bei einer Netzeinführung eingesetzt werden, sondern bei einer Weiterentwicklung eines bestehenden LANs, sollte der zeitliche Aufwand bei der Migration zum VLAN im Vorfeld berechnet und eingeplant werden. Dieser Zeitfaktor ist abhängig von verschiedenen Parametern:

- der Anzahl der Endgeräte
- der Anzahl der Netzkomponenten (Switches)
- der Art der VLAN-Technik (Port, MAC, IP)
- dem unterstützenden Netzmanagementsystem
- dem Know-How des Administrators
- der Implementierung der VLANs, etc.

Eine allgemeine Aussage, über die zu investierende Zeit bei einer Erstimplementierung, ist deshalb nicht möglich. Trotzdem kann individuell der Zeitaufwand geschätzt werden, wenn die zu realisierenden Managementaktivitäten bekannt sind.

Die portbasierten VLANs sind die einfachste Form, VLANs zu implementieren. Diese Netztechnologie kann sehr schnell in die bestehende Netzumgebung integriert werden. Die Ports der Switches werden dabei durch Konfigurationsschritte den entsprechenden VLANs zugeordnet. Z.Zt. existieren am Standort Oettingenstraße ca. 40 Switches á 24 Ports, d.h. im "worst case" Fall müßten ca. 1000 Ports konfiguriert werden. Da aber die meisten Switches genau einem Institut zugeteilt werden, oder maximal zwei Institute sich einen Switch teilen, beschränkt sich der zusätzliche Konfigruationsaufwand auf wenige Switches. Im "best case" Fall würde jedem Switch genau ein VLAN zugeordnet.

Die MAC-basierten VLANs können u.U. bei der Erstkonfiguration sehr zeitaufwendig sein. Jede MAC-Adresse muß quasi manuell einem VLAN zugeordnet werden. D.h. je größer die Anzahl der Endgeräte ist, um so mehr MAC-Adressen müssen einem VLAN zugeordnet und anschließend verwaltet werden. Deswegen sollten Systeme, die Layer-2-VLANs unterstützen, ein leistungsfähiges Netzmanagementsystem bieten, das in der Lage ist alle MAC-Adressen dem Administrator grafisch aufzubereiten. Dann kann man sehr leicht per "Drag and Drop" jede MAC-Adresse dem entsprechenden VLAN zuweisen. Am Standort Oettingenstraße müßten ca. 400 MAC-Adressen ihren VLANs zugeordnet werden.

Die Konfiguration von Layer-3-VLANs kann weitestgehend automatisiert werden. Die über einen DHCP-Server zugewiesenen IP-Adressen werden dann den entsprechenden VLANs zugeordnet. Abhängig von der Art der Gruppenbildung, muß nicht jede IP-Adresse einzeln einem VLAN zugewiesen werden, sondern ganze IP-Subnetze erhalten eine VLAN-Zugehörigkeit. Wie in Kap. 6.1, Abb. 6.3 schon ermittelt, besteht das derzeitige IP-Netz aus 8 Subnetzen, die jeweils fast ausschließlich einem Institut zur Verfügung gestellt werden. D.h. die Erstkonfiguration kann auch mit einem minimalen Aufwand durchgeführt werden.

9.4.2 Administrationsaufwand bei Änderungen jeder Art

Hier wird untersucht, welcher Aufwand entsteht, wenn Änderungen im Netz auftreten und welche Management-Aktivitäten der Administrator für die Änderungen vornehmen muß. Änderungen im Netz können unterschiedlicher Natur sein:

- Umzüge innerhalb des Netzes (Beispiele siehe Abb. 9.11)
  Bei den portbasierten VLANs aus Abb. 9.11 wird davon ausgegangen, daß alle Ports an den Switches bereits für VLAN 1 bzw. VLAN 2 vorkonfiguriert sind. Dies hat zur Folge, daß keine Management-Aktivitäten bei Umzügen durchgefürt werden müssen. Aus Sicherheitsgründen sollten freie Ports auf ein "Default VLAN" gesetzt werden. Bei Belegung der Ports, muß dann die VLAN-Zugehörigkeit konfiguriert werden.

- Neueinträge bzw. Löschungen von Netzteilnehmern

- Migration zu einem VLAN auf einer höheren ISO-OSI-Schicht

- Wechsel der VLAN-Zugehörigkeit, ohne den Arbeitsplatz zu verlassen (Bildung von virtuellen, projektbezogenen Teams)

Die portbasierten VLANs bieten nur eine eingeschränkte Flexibilität. Bei häufigen Umzügen innerhalb des Netzes oder bei VLAN-Wechsel ist eine Portzuweisung wenig effektiv, da jede Änderung auch zu einer Aktualisierung der VLAN-Tabelle führt. Die statische Zuordnung der Ports ist nur dann vorteilhaft, wenn die Netzteilnehmer ihren Standort nicht oder nur selten verlassen, was genau auf den Standort Oettingenstraße zutrifft.

Bei MAC-basierten und IP-basierten VLANs entsteht kein zusätzlicher administrativer Aufwand, wenn die Endgeräte in einen Umzug einbezogen werden und sich deren VLAN-Zugehörigkeit nicht ändert. Konfigurationsaufwand entsteht erst dann, wenn Endgeräte einem anderen VLAN zugewiesen werden. Aufgrund

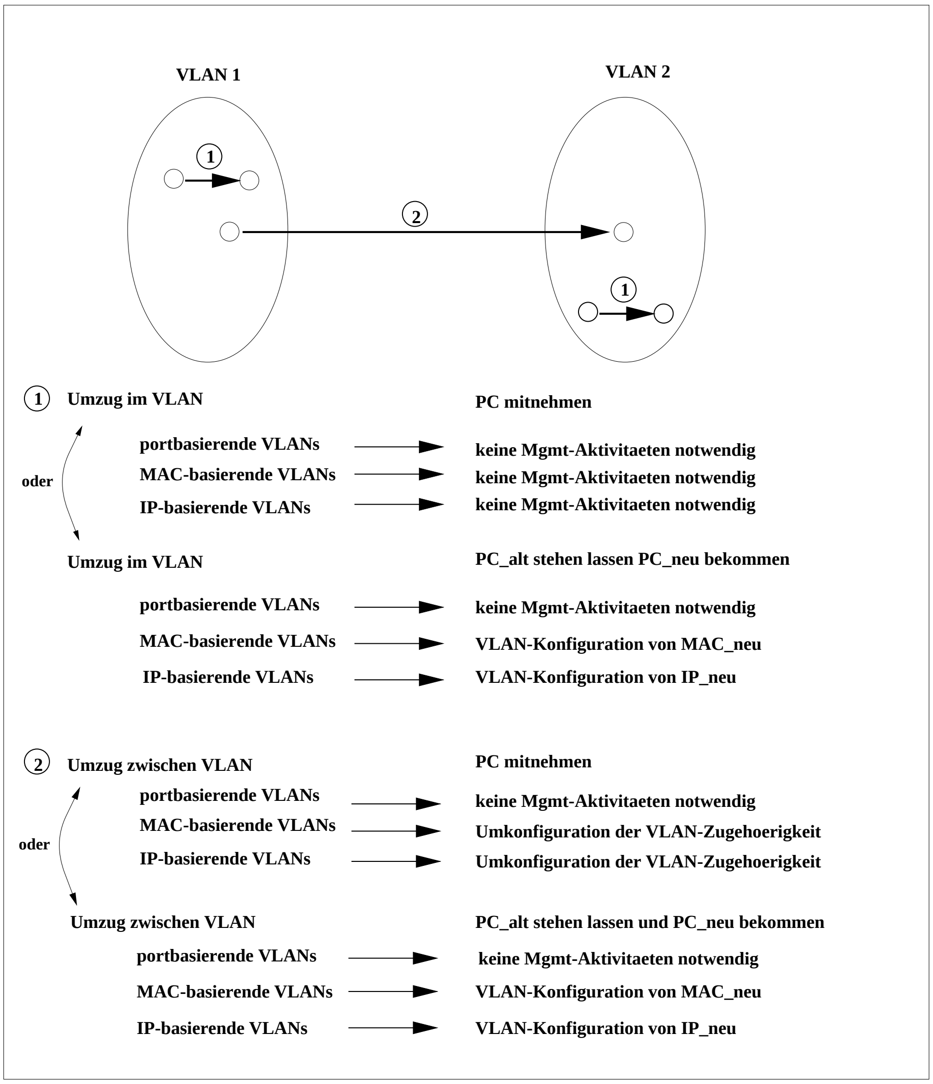


Abbildung 9.11: VLAN-Struktur bei Umzügen

der relativ autonomen, in sich abgeschlossenen Organisationseinheiten am Einsatzort bieten auch die MAC- und IP-basierten VLANs einen minimalen Administrationsaufwand bei Änderungen.

9.4.3 Mehrere VLANs pro Port

Viele Hersteller bieten bei den Port-, MAC- und IP-basierten VLANs die Möglichkeit mehrere VLANs an einen Switch-Port zu konfigurieren. Wird diese Funktionalität bei den eingesetzten Switches erfüllt, könnten u.U. weitere Komponenten eingespart werden.

9.4.4 Sicherheit

Neben dem administrativen Aufwand beim Einsatz von VLANs ist die Sicherheit, die durch die eingesetzte Technik gegeben ist, auch eine wichtige Anforderung, die erfüllt sein muß. Unter Sicherheit versteht man hier die Zugangssicherheit zu fremden Netzen/VLANs und Abhörsicherheit von fremden Daten.

Bei den portbasierten VLANs ist zu bedenken, daß jede Station, die an einem Port angeschlossen ist, immer automatisch dem entsprechenden VLAN angehört. Beim Einsatz von mobilen Systemen (Laptops) kann diese Technik eine gewisse Sicherheitslücke aufweisen, da nicht berechtige VLAN-Teilnehmer durch einfaches anschließen des Laptops an eine Dose automatisch in dem virtuellen Netz sind, die durch den Port des Switches definiert ist. Aber wenn bestimmte Randbedingungen erfüllt sind, können auch die niedrigen Sicherheitsmechanismen überwunden werden.
Folgende Randbedingungen müssen erfüllt sein:

- Zutritt zu den Räumen mit VLAN-Anschlußdosen darf nur berechtigten Personen gegeben sein.
- Zusätzliche Authentifikation des VLAN-Benutzers (Passwort) ist sinnvoll.
- Jedes VLAN hat einen Netzverantwortlichen, der als einziger berechtigt ist, Änderungen vorzunehmen.
- Der Netzverantwortliche muß eine genaue Liste führen, welche Teilnehmer Zugang zu den aktiven Ports haben und diese Berechtigung auch regelmäßig überprüfen. Dies kann eventuell mit Hilfe geeigneter Netzmanagement-Tools automatisiert werden.

Durch Einhaltung dieser Randbedingungen können am Standort Oettingenstraße, durch der Einsatz von portbasierten VLANs, sichere Strukturen aufgebaut werden.

Bei den MAC-basierten VLANs entscheidet der Switch und nicht die Anschlußdose, zu welchem VLAN jeder empfangene Frame gehört. Anhand der MAC-Adresse wird entschieden, ob der Frame weitergeleitet wird oder nicht. Ein geübter Anwender kann sein Endgerät durch Umkonfiguration mit einer anderen MAC-Adresse ausrüsten und damit unmittelbar mit einem anderen VLAN kommunizieren. Auch hier müssen weitere Sicherheitsmechanismen eingeführt werden. Z.B. Änderungen werden sofort beim Netzverantwortlichen gemeldet. Neue, noch nicht konfigurierte MAC-Adressen werden automatisch einem "Default VLAN"[1] zugeordnet, oder sie werden abgewiesen. In beiden Fällen bekommt der Netzadministrator sofort eine Meldung. Die MAC-Adressen können nur durch den Austausch oder mit Hilfe einer zusätzlichen Adapterkarte verändert werden, die aber in der Regel von den Netzverantwortlichen ausgetauscht werden.

[1] VLAN mit minimalen Rechten

Ähnlich wie bei den MAC-basierten VLANs entscheidet bei den IP-basierten VLANs der Switch, zu welchem VLAN das IP-Paket gehört. DHCP als dynamisches Verfahren ermöglicht eine dynamische Adreßzuordnung. Somit kann zu jedem Zeitpunkt die aktuelle IP-Adreß-Tabelle ermittelt werden. Da die IP-Adressen sehr leicht verändert werden können, müssen hier besondere Vorsichtsmaßnahmen getroffen werden. Erstens darf ein Neueintrag nur vom Netzverantwortlichen selbst vorgenommen werden und zweitens sollte jede nicht genehmigte IP-Adresse, die über DHCP erfaßt wird, sofort vom System gemeldet und einem "Default VLAN" zugewiesen werden.

9.5 Bewertung

In Tabelle 9.1 werden die Ergebnisse von Kap. 9.4 kurz zusammengefaßt.

Charakteristika	Layer-1-VLAN	Layer-2-VLAN	Layer-3-VLAN
Aufwand, um Endgeräte einem VLAN zuzuordnen	gering	hoch	mittel
Administrationsaufwand bei Änderungen	gering	mittel	mittel bis gering
Mehrere VLANs pro Port	möglich	möglich	möglich
Sicherheit, Def. 9.4.4	ja	ja	minimal

Tabelle 9.1: Abgrenzung VLAN-Szenarien am Einsatzort

Aus der Tabelle kann man entnehmen, daß die Vorteile der Layer-1- und Layer-2-VLANs aufgrund ihrer Sicherheit überwiegen.
Jetzt müssen zusätzlich weitere Randbedingungen berücksichtigt werden. Die heute eingesetzten Switches der Firma 3Com SuperStack II 1000 unterstützen nur die portbasierten VLANs. Sie werden in der nächsten Zukunft nicht ausgetauscht. Aufgrund dieser Voraussetzungen können wir heute nur die portbasierten VLANs planen. Eine Migration auf höhere VLAN-Philosophien setzt den Einsatz von moderneren Komponenten voraus.
Zusätzlich bin ich der Meinung, daß man bei einer Erstinstallation schrittweise vorgehen soll. Man muß dabei beachten, daß es sich hier um ein Produktionsnetz handelt. Es ist also keine Planung auf der "grünen Wiese" möglich. Der Aufwand und das Risiko bei einer Erstinstallation von VLANs muß auf ein Minimum reduziert werden, um den laufenden Betrieb nicht zu stören. Deswegen sollen in einer ersten Ausbaustufe die Migration vom LAN zum Layer-1-VLAN vorgenommen werden.
Abhängig von den Ergebnissen dieses virtuellen Netzes, soll dann in einer zweiten oder sogar dritten Ausbaustufe alle bis dahin vorhandenen Anforderungen unterstützt werden. Dies kann durch Migration zu Layer-2 oder Layer-3-VLANs erreicht werden. Eventuell ist auch eine Kombination dieser VLAN-Typen notwendig.

Diese weiteren Entwicklungsschritte werden aber erst dann sinnvoll, wenn das bestehende VLAN die aktuellen Anforderungen nicht mehr erfüllen kann.

Es gibt bei Netzen keine Standardlösung, deshalb sollte auch am Beispiel des Gebäudekomplexes Oettingenstraße bei einer Neukonfiguration noch keine endgültige Lösung verabschiedet werden.

Wir haben gesehen, daß aufgrund der vorgefundenen Situation und der ermittelten Randbedingungen in der ersten Implementierungsphase nur der Einsatz von Layer-1-VLANs in Frage kommt. Hier werden also die Endgeräte anhand ihrer Zugehörigkeit zu einzelnen OE entsprechenden VLANs zugewiesen. Diese portbasierte Zuordnung erlaubt die Trennung der jeweiligen Collision Domains bei gleichzeitigem Zugang zu zentralen Diensten.
Die nachfolgende Realisierungs-Phase kann dann beginnen.

Teil IV

Realisierungs-Phase

Kapitel 10

VLANs in der Oettingenstraße

Dieses Kapitel beschreibt die wichtigsten Aktivitäten die notwendig sind, um die Migration vom derzeitigen LAN zum Layer-1-VLAN durchzuführen.

10.1 Planung der Installation

Bevor die angesprochenen Layer-1-VLANs am Einsatzort implementiert werden, müssen im Vorfeld noch einige Aktivitäten durchgeführt werden. Primäres Ziel bei dieser Installation ist eine Ressourcenoptimierung zu erreichen. Die vorhandene Netzstruktur soll aber beibehalten werden. Die strukturierte Verkabelung in der Oettingenstraße besteht aus einem zentralen Gebäudeverteiler und 10 weiteren Verteilerräumen (Etagenverteiler), die jeweils einen speziellen Versorgungsbereich abdecken. Manche Versorgungsbereiche bedienen ausschließlich Endgeräte einer einzigen Organisationseinheit (OE), andere Versorgungsbereiche bedienen Endgeräte aus mehreren OE. Unter Beibehaltung der vorhandenen Struktur können nur in solchen Versorgungsbereichen Komponenten eingespart werden, die mehrere OE bedienen. Ob tatsächlich Komponenten eingespart werden können, muß die genaue Analyse der OE und der Versorgungsbereiche ergeben.

Eine Aufgabe der Netzplaner ist also die genaue Untersuchung aller Verteilerräume. Es muß untersucht werden, wie jeder Switch innerhalb eines Versorgungsbereiches ausgelastet ist. Sind noch freie Ports vorhanden, können Endgeräte von anderen Switches - eventuell von einer anderen OE - angeschlossen werden. Der Einsatz von virtuellen LANs macht eine solche Gemeinsamnutzung erst möglich. Auf diese Weise können Komponenten besser ausgelastet und im besten Fall sogar eingespart werden.

Der "zentrale Gebäudeverteiler" besteht aus mehreren Komponenten. Fast jeder OE wird ein Switch als Koppelelement zwischen dem Router und den OE-eigenen[1] Etagenverteilern zur Verfügung gestellt. Wird nun auf einer höheren Ebene (Etagenverteiler) eine Umkonfiguration der Endgeräte auf eine gemeinsame Komponente vorgenommen, muß u.U. auch auf der Ebene des Gebäude-

[1]Switches, die nur einer OE zur Verfügung gestellt werden

verteilers eine zusätzliche Verbindung zwischen den OE-eigenen Switches vorgenommen werden (vgl. Abb.10.1), um eine geswitchte Verbindung zwischen Endgeräten einer OE zu realisieren.

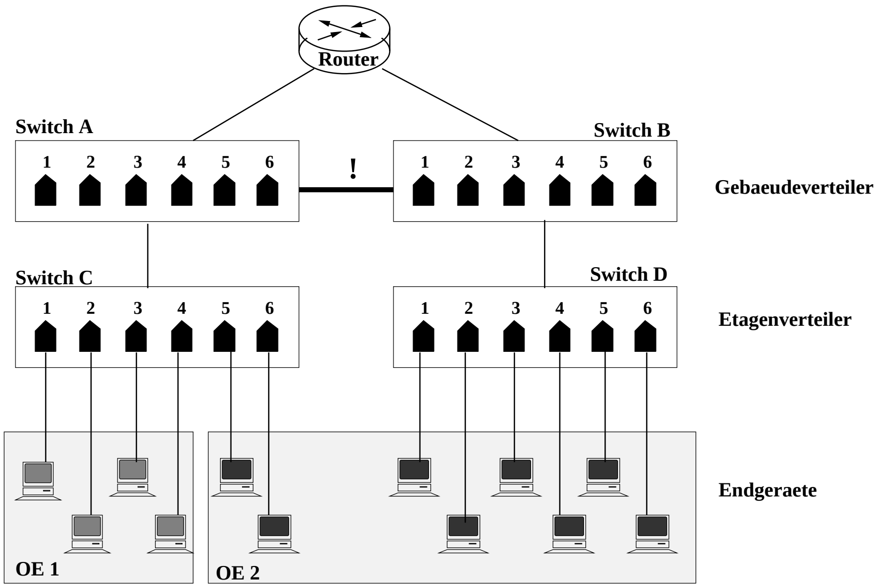


Abbildung 10.1: Planung der Installation

Die Planung und Realisierung der Installation bedarf einer exakten Protokollierung. Für jeden Switch muß eine Bestandsaufnahme nach der Umkonfiguration erfolgen (vg. Abb. 10.2):

- Switch A
  - Port 1-6 und 13-18 für OE_1 oder VLAN I
  - Port 7-12 und 19-24 für OE_2 oder VLAN II

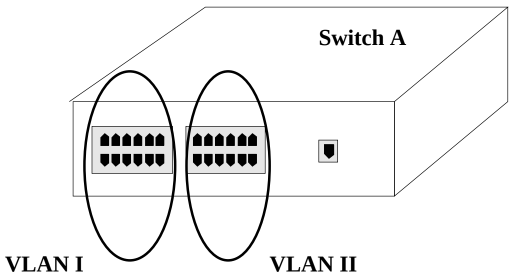


Abbildung 10.2: Beispiel einer gemeinsamen Komponente für zwei OE

10.2 VLAN-Management-Aktivitäten

Nachdem die Installation (Belegung der Ports) abgeschlossen ist, beginnen die eigentlichen Management-Aktivitäten. Die VLANs müssen nun in den einzelnen SuperStack II-Switches konfiguriert und anschließend überwacht werden.

10.2.1 Konfigurations-Management

In den nächsten Abschnitten wird die VLAN-Implementierung für den "Switch 1000" beschrieben.
Der "Switch 1000" unterstützt bis zu 16 VLANs, die jeweils mehrere Ports belegen können. Aber jeder Switch-Port unterstützt nur ein VLAN. Wird an einen solchen Port ein Hub mit mehreren Teilnehmern angeschlossen, so werden alle diese Teilnehmer implizit dem VLAN dieses Ports zugewiesen.
Bei jedem Switch ist VLAN 1 als "Default VLAN" vom Switch vorgesehen. Dieses "Default VLAN" besitzt folgende Eigenschaften:

- Es beinhaltet alle Ports eines neuen oder initialisierten Switch.
- Es ist das einzige VLAN, das den Zugriff einer Netzmanagementstation auf den SNMP-Agenten des Switches erlaubt.

An einem Beispiel (siehe Abb. 10.3) werden die notwendigen Schritte bei einer VLAN-Konfiguration beschrieben.

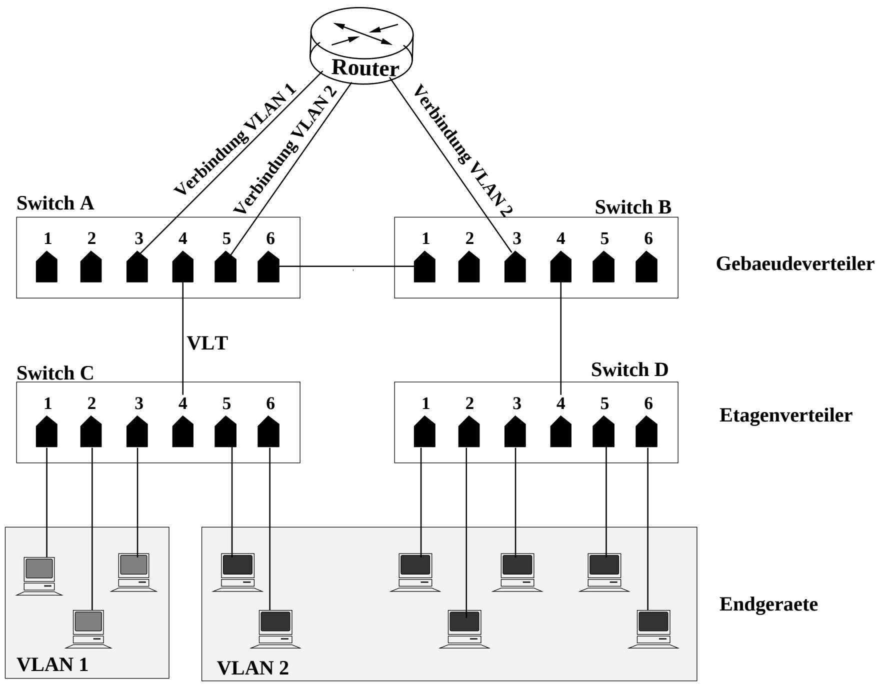


Abbildung 10.3: Beispiel einer VLAN-Konfiguration

1. Zuordnung : Ports → VLAN

   - Switch C: Zuordnung von Port 1-3 zu VLAN 1
     Zuordnung von Port 5-6 zu VLAN 2
   - Switch D: Zuordnung von Port 1-3 und 5-6 zu VLAN 2

2. Definiere für jeden Switch einen Backboneport. Über einen Backboneport kann eine Switch-to-Switch-Verbindung erstellt werden. Dieser Port kann eine spezielle Eigenschaft besitzen: Virtual LAN Trunk (VLT). Ein VLT ermöglicht die Übertragung verschiedener VLAN-Frames zwischen den Switches. Werden nun an beiden Enden einer Switch-to-Switch-Verbindung jeweils ein VLT konfiguriert, so benötigt man nur eine Verbindung für die Übertragung aller VLANs.

   - Switch A: Backboneport/VLT 4 (VLAN 1/VLAN 2) und Backboneport 6 (VLAN 2)
     Port 4 besitzt VLT, da sowohl Frames von VLAN 1 als auch von VLAN 2 übertragen werden.
     Port 6 von Switch A und Port 1 von Switch B sind einfache Backboneports, da nur Frames von VLAN 2 übertragen werden.
   - Switch B: Backboneport 1 und 4 (VLAN 2)
   - Switch C: Backboneport/VLT 4 (VLAN 1/VLAN 2)
   - Switch D: Backboneport 4 (VLAN 2)

3. Stelle Verbindung zwischen Switch A/Switch B und Router her. Für jedes VLAN muß eine eigene Verbindung zum Router hergestellt werden. Bei "one-armed Router" braucht man nur eine Verbindung (vgl. VLT) für die Übertragung von VLAN-1 und VLAN-2-Frames. Aber die Switches müssen diese Funktionalität auch unterstützen. Der "Switch 1000" unterstützt dieses Feature nicht.

   - Switch A: Port 3 → VLAN 1
     Port 5 → VLAN 2
   - Switch B: Port 3 → VLAN 2

10.2.2 Fehler-Management

Sind die VLANs eingerichtet, müssen sie im laufenden Betrieb gepflegt werden. Im täglichen Betrieb des Managementsystems zeigt sich erst, ob mit dem gewählten Ansatz die in der Anforderungs-Phase und Planungs-Phase aufgestellten Anforderungen auch tatsächlich bewältigt werden. Treten Fehler jeglicher Art auf, müssen sie erkannt, erfaßt und behoben werden. Im Bereich der Fehlersuche liegt das wesentliche Problem. Es gibt keine Ethernet-Segmente im eigentlichen Sinne mehr, sondern jedes Endgerät hat sein eigenes Segment. Dies erhöht die Komplexität bei der Fehlersuche. Hilfreich bei der Fehlersuche können Hilfsmittel sein wie Meßgeräte, Protokollanalysatoren, Einsatz von

RMON[2] Probs, etc.

10.3 Schnittstellenbeschreibung LRZ-LMU

Es ist noch zu klären, wer diese Management-Aktivitäten durchführen soll. Das LRZ als Netz-Betreiber oder die OE als Netz-Benutzer? Vielleicht ist sogar eine Rollenaufteilung zwischen diesen Institutionen möglich?
In den folgenden Abschnitten werden zwei Szenarien durchgespielt, in denen die Management-Aufgaben von jeweils einer Institution durchgeführt werden.

1. Szenario
Alle OE haben Schreib- und Leserechte (R/W) auf dem virtuellen Netz.
Jedes VLAN (OE) wird lokal von einem Netzverantwortlichen betreut. Nicht für alle OE rechnet sich ein festangestellter Netzadministrator. OE, die über keinen eigenen Netzadministrator verfügen, werden von Administratoren anderer OE oder sogar vom LRZ unterstützt. Diese Netzverantwortlichen bekommen nun alle Rechte, um das virtuelle Netz in der Oettingenstraße zu konfigurieren und den laufenden Betrieb zu überwachen. Um einen reibungslosen Betrieb zu gewährleisten, müssen einige Aspekte geklärt werden.

- Ausbildung der Netzverantwortlichen
  Ein modernes Netz sollte nur von einem hochqualifizierten Netzadministrator gewartet und gepflegt werden. Die Netzspezialisten müssen über ein tiefes Know How (Betriebssysteme, Management-Systeme, Netztechniken, VLANs, etc.) verfügen. Sie sollten sehr zuverlässig und beständig sein, und in der Regel festangestellt.

- Auswirkung im Fehlerfall
  Jeder Netzadministrator muß sich einen Überblick über das gesamte virtuelle Netz verschaffen. Tritt ein Netzproblem auf, stellt sich die Frage, wer diesen Fehler beheben soll. Die vorhandene Netzstruktur und die installierten Komponenten erlauben es, über ein Monitoring- und Netzmanagementsystem die Fehler zu erkennen und beheben. Ist die Ursache des Problems erfaßt und lokalisiert (VLAN lokal oder VLAN übergreifend), muß geklärt werden, wer die Fehlerbehandlung durchführen darf.

- Aufwand für die Rechtevergabe
  Nun stellt sich die Frage, wer die Rechtevergabe definieren soll und speziell welche Rechte jeder Netzverantwortliche erhalten darf. Genau diese Problematik bringt nicht nur einen Mehraufwand beim LRZ, sondern auch eine gewisse Unsicherheit im Netz: "Viele Administratoren machen ein Netz kaputt".

2. Szenario
Das virtuelle Netz in der Oettingenstraße wird vom LRZ gewartet, betreut und

[2] Remote Monitoring MIB (Management Information Base), System zur Überwachung von (entfernten) LANs

gepflegt. Die gesamte Administration wird vom Standort ausgelagert und vom LRZ als kompetenter, zuverlässiger Profi übernommen. Das LRZ als erfahrener Betreiber des MHN, übernimmt die Installation der Planung, Konfiguration der Ports und den Betrieb des laufenden Netzes.

Ich bin der Meinung, daß Variante 2 für den Einsatzort die bessere Alternative ist. Gerade für ein Netz, bestehend aus mehreren autonomen OE (VLANs), die zum Teil keine ausreichend ausgebildeten Netzadministratoren besitzen, ist eine zentrale Administration mit erfahrenem Personal eine gute Lösung. Die OE können weiterhin mit Einschränkung ihr lokales Netz betreuen.

Teil V

Zusammenfassung

Kapitel 11

Fazit

Obwohl VLAN-Beschreibungen kaum in einem Herstellerprospekt fehlen und viel über dieses Thema geschrieben wird, lassen praktische Implementierungen bisher im großen Umfang auf sich warten. (Auch die Marketingaktivitäten der Systemhersteller werden in Bezug auf virtuelle Netze geringer.) Sind nun fehlende Produkte die Ursache der mangelnden Akzeptanz? Oder wurde die Technik am Markt vorbei entwickelt? Sind VLANs bereits Vergangenheit?

Ich bin der Meinung, daß der einzige Grund, warum sich VLANs nur langsam durchsetzen, in der präzisen und aufwendigen Planung liegt. Die Implementierung der virtuellen Netze bedarf einer exakten Vorbetrachtung und Planung, wenn sie erfolgreich und nutzenbringend verlaufen soll.

Die VLAN-Technik bietet bei einer Reihe von Netzkonstellationen sehr gute Möglichkeiten, um die Flexibilität zu erhöhen und die Kosten für den Netzbetrieb zu senken. Die meisten namenhaften Komponentenhersteller integrieren die VLAN-Funktionalität in ihre Komponenten. Einige Hersteller bieten sogar komplette, individuelle VLAN-Lösungen an: von der Analyse am Einsatzort, Bereitstellung der Komponenten, Konfiguration und Betrieb des Netzes sowie eine integrierte System- und Management-Plattform (Bsp. CABLETRON SYSTEMS, The Complete Networking Solution).

Das Themengebiet der virtuellen Netze wurde in dieser Diplomarbeit, an einem konkreten Beispiel des Gebäudekomplexes Oettingenstraße, ausführlich beschrieben. Dabei wurde untersucht, unter welchen Voraussetzungen diese neue Technologie in die vorhandene Netzstruktur integriert werden kann.
In den nachfolgenden Abschnitten werden die Ergebnisse der jeweiligen DA-Phasen kurz zusammengefaßt.

Virtuelle Netze dienen dazu, Netze unter logischen Gesichtspunkten, d.h. losgelöst von der physischen Topologie, die durch das Kabelnetz vorgegeben ist, zu strukturieren. In den traditionellen Shared-Media-LANs bilden die Endgeräte eines physischen Verkabelungsbereiches, z.B. einer Etage oder eines Gebäudes, eine Netzgruppe. Damit ist die Netzstrukturierung vom Standort der Teilneh-

mer bzw. der Endgeräte abhängig. In Netzen auf Basis von Switchingtechnologien kann über die physische Netzstruktur eine zweite, logische Netzstruktur gelegt werden. Alle Teilnehmer, die einer Interessensgruppe angehören, können unabhängig von ihrem Standort zu einer Netzgruppe (virtuelles Netz/VLAN) zusammengefaßt werden. Das Ergebnis dieser neuen Struktur ist ein flexibles LAN, das u.U. Änderungen jeder Art ohne großen Administrationsaufwand unterstützt.
Es gibt unterschiedliche VLAN-Konzepte, abhängig von der Art und Weise der Zuordnung der Endgeräte zu den VLANs. Folgende Zuordnungsvarianten wurden in Kapitel 3.4 beschrieben:

- Layer-1-VLANs (portbasierende VLANs)
- Layer-2-VLANs (MAC-basierende VLANs)
- Layer-3-VLANs (Spezialfall IP-basierende VLANs)
- Policy-basierende VLANs

Zur Übertragung der VLAN-Information im Backbonenetz können folgende Verfahren genutzt werden (siehe Kapitel 3.5):

- Austausch von Adreßtabellen
- Frame Tagging
- Time Division Multiplexing
- ATM

Die VLAN-Technologie ist bzgl. der Standardisierung noch relativ neu. Die oben aufgelisteten Verfahren (Austausch von Adreßtabellen, Frame Tagging und TDM) sind größtenteils proprietär implementiert. Die Interoperabilität zwischen den Hersteller ist nicht gewährleistet. Ein Draft-Standard (IEEE 802.1Q) spezifiziert Tagging für den Austausch der VLAN-Information. Im ATM-Umfeld hat die Standardisierung bereits nach der Verabschiedung der ELAN (Version 1.x) stattgefunden.

Mit dem Einsatz von VLANs können flexible und sichere Strukturen aufgebaut werden, wenn im Vorfeld alle dazu benötigten Parameter ermittelt werden. In der Analyse-Phase wurde die Ist-Analyse, der vorhandenen Organisationsstruktur und Topologie, und die Anforderungs-Analyse, der Netzbenutzer und des Netzbetreibers, ermittelt.
Die am Einsatzort vorhandene Organisationsstruktur entspricht nicht üblichen Unternehmens-Strukturen, da die Universität keine typische Unternehmung ist, in dem betriebliche Tätigkeiten, im Sinne von Gewinnerbringung, stattfinden. Das Ergebnis der Analyse der Aufbauorganisation ergab eine flache, hierarchische Organisationsstruktur, bestehend aus autonomen, eigenständigen Instituten (OE). Zwischen diesen OE findet keine Ablauforganisation und keine Beziehungsstruktur statt.

Da es sich am Einsatzort um eine relativ neue Infrastruktur handelt, ist das Gebäude mit einer "modernen" strukturierten Verkabelung erschlossen. Das derzeitige Netz wird durch Switches und Router in Subnetze unterteilt. Der Router segmentiert dieses Netz in acht Subnetze, wobei jede OE einem (oder mehreren) Subnetz(en) zugeteilt wird.
Das LRZ als Netzbetreiber erhofft sich durch den Einsatz von virtuellen LANs im Gebäudekomplex Oettingenstraße eine Ressourcenoptimierung und u.U. eine Vereinfachung der Netzadministration.
Die allgemeinen Anforderungen der Netzbenutzer, wie Expansionsmöglichkeiten, Migrationsmöglichkeiten zu neuen Technologien, Sicherheitskonzepte, sollen weiterhin unterstützt werden, aber ohne sonstige Einschränkungen in Kauf zu nehmen.
Diese Aspekte müssen alle bei der Planungs-Phase berücksichtigt werden.

In der Planungs-Phase wurden verschiedene Szenarien, aufgrund der logischen Gruppierung der Endgeräte und der eingesetzten VLAN-Technik, durchgespielt und voneinander abgegrenzt, um eine optimale Lösung am Einsatzort zu erreichen. Aufgrund der Besonderheiten (Ergebnisparameter aus Analyse-Phase) am Einsatzort ist das Ergebnis dieser Untersuchung eine mögliche VLAN-Definition, die nicht notwendigerweise genau einer Klasse von VLANs zugeordnet werden kann, sondern aus einer Kombination von "infrastructural"- und "service-based"-VLANs besteht. Diese Mischkonfiguration besteht aus dem "infrastructural"-Modell und dem "service-based"-Modell. Jede OE stellt ein eigenes VLAN dar. Zusätzlich kann jede OE Teilnehmer in weiteren VLANs sein, um auf zentrale Dienste zuzugreifen.
Aufgrund von weiteren technischen Voraussetzungen wie, die heute eingesetzten Switches der Firma 3Com SuperStack II 1000 unterstützen nur die portbasierten VLANs und aufgrund der Sicherheit die sie bieten, können heute nur die portbasierten VLANs implementiert werden.
Diese Layer-1-VLANs werden in einer weiteren Phase bzgl. ihrer Implementierung genauer beschrieben.

In der Realisierungs-Phase wurden die Aktivitäten beschrieben, die notwendig sind, um die Migration vom derzeitigen LAN zum Layer-1-VLAN durchzuführen. Dabei wurde auf die Vorbereitungen bei der Installation, der Konfiguration und der Netzadministration näher eingegangen.

Diese Diplomarbeit enthält einen möglichen Stufenplan, der bei der Planung von virtuellen Netzen mindestens eingehalten werden muß, um einen sinnvollen Einsatz von virtuellen Netzen zu garantieren.
Diese Diplomarbeit umfaßt nur eine theoretische Untersuchung, ob VLANs am Einsatzort auch sinnvoll wären. Ich bin der Meinung, daß der Einsatz von VLANs im Gebäudekomplex Oettingenstraße zwar einige Vorteile (vgl. Kap. 9.4) bietet, aber die erhofften Einsparungen der Netzressourcen und die erhoffte Vereinfachung der Netzadministration zu minimal sind und eine Migration vom derzeitigen LAN zu Layer-1-VLAN nicht rechtfertigen.

Aufgrund der benötigten technischen Informationen bei der Diplomarbeit, habe ich tiefergehende Einblicke in die neuesten LAN-Technologien bekommen, die für mehr Flexibilität und besseren Einsatz der Ressourcen dienen könnten. Ich bin der Meinung, daß der Einsatz von neuen Komponenten und von Layer-3-VLANs am Einsatzort mehr Vorteile bieten könnte, als der hier erarbeitete Lösungsvorschlag.

Abkürzungsverzeichnis

AAL	ATM Adaption Layer
ATM	Asynchronous Tranfer Mode
B-WiN	Breitband-Wissenschaftsnetz
DA	Diplomarbeit
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsche Industrienorm
DNS	Domain-Name-Server
FDDI	Fiber Distributed Data Interface
FE	Fast Ethernet
FTTD	Fiber To The Desk
GE	Gigabit Ethernet
IEEE	Institute of Electrical and Electronical Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetworking Packet Exchange Protocol
ISO	International Standardization Organization
IT	Informations-Technologie
LAN	Local Area Network
LANE	LAN-Emulation
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LRZ	Leibniz-Rechnerzentrum
MA	Mitarbeiter
MAC	Medium Access Control
MHN	Münchner Hochschulnetz
MIB	Management Information Base
MPOA	Multiprotocol over ATM
NIP	Netzwerk-Investitions-Programm
OE	Organisationseinheit
OS	Organisationsstruktur
OSI	Open System Interconnection
RFC	Request for Comment
RMON	Remote Monitoring
SNA	System Network Architecture
TP	Twisted Pair
TCP	Transmission Control Protocol
VB	Versorgungsbereich
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WWW	World Wide Web

Literaturverzeichnis

[1] Arnold Picot/Ralf Reichwald/Rolf T. Wigand, *Die grenzenlose Unternehmung – Information, Organisation und Management*, Betriebswirtschafltlicher Verlag Dr. Th. Gabler GmbH, Wiesbaden 1996

[2] Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften, Wöhe, *Einführung in die Allgemeine Betriebswirtschaftslehre*, Verlag Vahlen, 15. Auflage, München 1984

[3] *Vahlens Kompendium der Betriebswirtschaftslehre*, Verlag Vahlen, Band 1 und Band 2, München 1984

[4] Jens Dittrich/Uwe von Thienen, *VLANs Migration zu modernen Netzwerken*, THOMSON PUBLISHING – DATACOM, Bonn 1997

[5] Gilbert Held *Virtual LANs – Construction, Implementation, and Management*, Verlag Wiley, 1997

[6] Heinz-Gerd Hegering/Sebastian Abeck *Integriertes Netz- und Systemmanagement*, Verlag ADDISON-WESLEY, 1. Auflage, 1993

[7] Franz-Joachim Kauffels *Lokale Netze*, Verlag Thomson Publishing, 9. Auflage, Bonn 1997

[8] Andrew S. Tanenbaum *Computernetzwerke*, Verlag Prentice Hall, 3. Auflage, München 1997

[9] Wolfgang Kemmler/Mathias Hein *Gigabit-Ethernet – Der Standard – Die Praxis*, FOSSIL-Verlag, Köln 1998

[10] LRZ, *Überblick über das MHN, Richtlinien zum Betrieb des MHN*, März 1998, http://www.lrz.de

[11] LANLine – *Das Magazin für Netze, Daten- und Telekommunikation*, Dezember 1997

[12] LANLine – *Das Magazin für Netze, Daten- und Telekommunikation*, 1997

[13] LANLine – *Das Magazin für Netze, Daten- und Telekommunikation*, Mai 1998

[14] DATACOM, Zeitschriften-Verlag GmbH, Bergheim, Januar 1998

[15] DATACOM, Zeitschriften-Verlag GmbH, Bergheim, November 1997

[16] 3Com, *SuperStack II Switch 1000, User Guide*, September 1996

[17] 3Com, *3Com Transcend VLANs – Leveraging Virtual LANs Technology to Make Networking Esier*, Februar 1998, http://www.3com.com/0files/strategy/537VLAN.html

[18] XYLAN, *Auto Tracker: Virtual LAN – Architecture*, Dezember 1997, http://www.xylan.com/whitepaper/AUTOTRAC

[19] XYLAN, *Network Layer Switching*, Dezember 1997, http://www.xylan.com/whitepaper/NETLAYER

[20] decisys, *The Virtual LAN – Technology Report*, 1996, http://www.decisys.com

[21] Cisco, *Extending Virtual LANs to the Server, VLANs and Routers, Cisco-Fusion VLAN RoadMap for Scalable..., LAN Emulation*, Dezember 1997, http://www.cisco.com/warp/public

Anhang A

Fragebogen

Anhang B

Diagramme