CSN
Chemnitzer StudentenNetz

Netzentwicklung im CSN

Bestands- und Strategiepapier

Autor:

Markus Schade (csn@markusschade.com)

Inhaltsverzeichnis

1 Bestandsaufnahme **2**
- 1.1 Einführung . . . 2
- 1.2 Übersicht Netztopologie . . . 2
- 1.3 Backbone . . . 3
  - 1.3.1 Zentraler Router . . . 3
  - 1.3.2 Glasfaserleitungen . . . 3
  - 1.3.3 Technologie und Geschwindigkeiten . . . 3
- 1.4 Vetterstraße 52 . . . 4
- 1.5 Vetterstraße 54 . . . 4
- 1.6 Vetterstraße 64/66 . . . 5
- 1.7 Vetterstraße 70/72 . . . 5
- 1.8 Reichenhainer Straße 35/37 . . . 6
- 1.9 Reichenhainer Straße 51 . . . 6
- 1.10 Thüringer Weg 3 . . . 6

2 Konfiguration **7**
- 2.1 Zentraler Router . . . 7
- 2.2 Vettersstraße 52 . . . 8
- 2.3 Vettersstraße 54 . . . 8
- 2.4 Vettersstraße 64/66 . . . 8
- 2.5 Vettersstraße V70/72, Reichenhainer Straße 35/37, Thüringer Weg 3 . . . 9

3 Planung **10**
- 3.1 Backbone . . . 10
- 3.2 Vettersstraße 52 . . . 10
- 3.3 Vettersstraße 54 . . . 10
- 3.4 Vettersstraße 64/66 . . . 11
- 3.5 Vettersstraße 70/72 . . . 11
- 3.6 Reichenhainer Straße 35/37 . . . 11
- 3.7 Reichenhainer Straße 51 . . . 11
- 3.8 Thüringer Weg 3 . . . 11
- 3.9 Neue Technologien . . . 12
  - 3.9.1 Voice over IP . . . 12
  - 3.9.2 Netzzugang nach IEEE 802.1X . . . 12
  - 3.9.3 WLAN Zugang . . . 13

4 Anhang **14**
- 4.1 Router-Konfiguration . . . 14
  - 4.1.1 Generische Einstellungen . . . 14
  - 4.1.2 NetFlow . . . 14
  - 4.1.3 VLAN . . . 15
    - 4.1.3.1 Beschreibung . . . 15
    - 4.1.3.2 Interfaces . . . 16
  - 4.1.4 Uplink und Multicast-Tunnel . . . 18
  - 4.1.5 Hausuplinks . . . 19
  - 4.1.6 direkt angeschlossene Ports V54 . . . 20
    - 4.1.6.1 Etagenuplink . . . 20

4.1.6.2 Zwischenbau 20
4.1.7 Ports für CSN-eigene Rechner 20
4.1.8 IP Routing 21
4.1.9 Logging und ACLs 21
4.1.10 NTP 22
4.1.11 Intrusion Detection 22

1 Bestandsaufnahme

1.1 Einführung

2004 - Seit zehn Jahren haben Studenten die Möglichkeit auch im Wohnheim sich an das Campusnetz der TU-Chemnitz anzuschließen. Die Netzwerkinfrastruktur hat sich bis dato von einem frei verkabelten BNC-Netz mit Leihgeräten durch das Universitätsrechenzentrum (URZ) zu einem heterogenen Twisted-Pair/BNC-Netz mit fast professionellen und nahezu vollautomatisierten Netzmanagement entwickelt. Das Chemnitzer Studenten-Netz (CSN) kümmert sich um die Verwaltung der Technik und unterstützt die Studenten beim Anschluß. Die Technik wurde zum Großteil vom Studentenwerk Chemnitz-Zwickau finanziert.
Das vorliegende Papier dokumentiert die technische Infrastruktur in den Wohnheimen, welche durch das CSN verwaltet werden. In den darauf folgenden Abschnitten werden mögliche Entwicklungen und entsprechende Bewertungen angeführt.

1.2 Übersicht Netztopologie

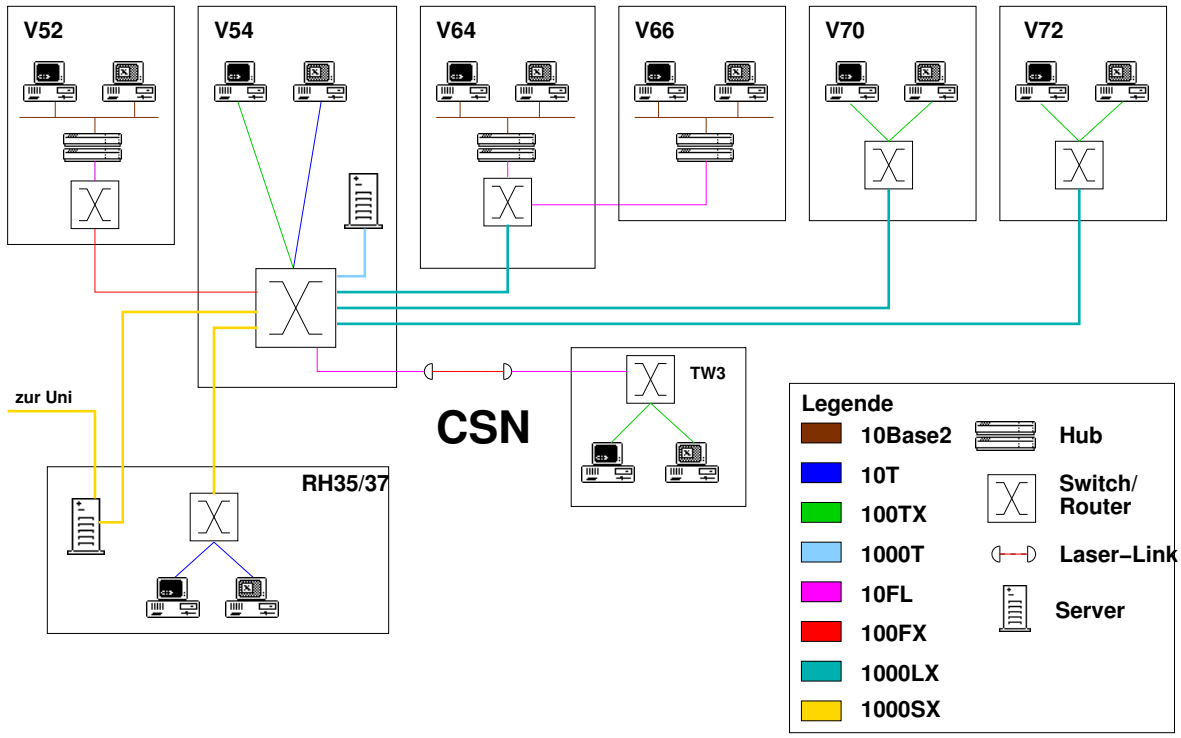


Abbildung 1: Netztopologie des CSN im Sommer 2004

Aktuell bindet das CSN 9 Wohnheime an des Campusnetz der TU Chemnitz an. Davon sind 3 Wohnheime mit BNC verkabelt und 6 mit Twisted-Pair (TP). Alle Wohnheime sind mit MMF[1] untereinander verbunden, mit Ausnahme des Thüringer Weg 3 (TW3), welcher über einen Laserlink über das Dach der Vettersstraße 54 (V54) angebunden ist.

[1] Multi Mode Fiber - Multi-Mode-Glasfaser

1.3 Backbone

1.3.1 Zentraler Router

Seit Februar 2004 wird das zentrale Routing durch einen Hardwarerouter der 6500er Serie von Cisco Systems realisiert. Zuvor war ein **Cisco 3550** mit 10 1000BASE-T Ports und 2 GBIC[2] Einschüben zum Einsatz gekommen. Der Einsatz dieser Geräte war notwendig geworden, da die zuvor eingesetzte Technik nicht in der Lage war statische ARP-Einträge in der gewünschten Größenordnung (1500+ Hosts) zu verwalten. Zusätzlich bestand und besteht die Notwendigkeit, den CSN-internen Netzverkehr zu zählen. Auch hier waren die ursprünglichen Geräte überfordert. Die internen 32-Bit-Zähler könneninnerhalb von etwas mehr als 5 Minuten durch die 100 MBit-Nutzeranschlüsse zum Überlauf gebracht werden. Bei einem Aktualisierungzyklus von teilweise mehreren Minuten führte dies zum Verlust jeglicher nutzbarer Meßwerte.
Die neue Lösung nutzt die auch vom URZ eingesetzte NetFlow-Technologie des Cisco-Routers. Hier wird der Netzverkehr in sogenannte Flows eingeteilt und zu einem dedizierten Host (*wins.csn*) exportiert. Dieser wertet die empfangenen Daten aus und erstellt eine Abrechnung. Über eine verschlüsselte Verbindung wird diese an den Datenbankserver übertragen und eingepflegt. Über eine Web-Schnittstelle kann jeder Nutzer seine persönlichen Daten einsehen.

1.3.2 Glasfaserleitungen

Verbindung	Fasern	Typ	Geschwindigkeit	Länge	Bemerkung
Rh35 - Rh39	8	50 μm MMF	1000BASE-SX	n/a	Uplink(2), UniCC(2),URZ(2)
Rh35/37 - V54	8	50 μm MMF	1000BASE-SX	366 m	Uplink(2), Rh35/37(2)
V52 - V54	4	62.5 μm MMF	100BASE-FX	n/a	
V64 - V54	4	62.5 μm MMF	1000BASE-LX	387 m	V64/66 (2)
V70 - V54	4	62.5 μm MMF	1000BASE-LX	351 m	V72 (2), V70(2)

Über eins der 2 ungenutzen Adernpaare zwischen Rh35 und Rh39 wurde bis Ende 2003 die Rh51 angebunden. (Das Adernpaar führte zu einem LED-Link auf dem Dach der Rh37/39)

1.3.3 Technologie und Geschwindigkeiten

Die Mehrheit der Wohnheime ist über Gigabit am zentralen Router angeschlossen. Dabei werden aufgrund des Kabeltyps die V64/V66 mit einem Adernpaar, V70 und V72 mit je einem Adernpaar über 1000BASE-LX GBICs angebunden. Für die Rh35/37 genügte 1000BASE-SX. Die V52 liegt mit 100BASE-FX über einen Medienkonverterblock im Keller der V54 (SC/TP) von Allied-Telesyn am Kupfermodul des Routers an. Aus finanzielle Gründen wurde die Lösung über Medienkonverter gewählt, da die Switches mit 100BASE-FX Ports zu diesem Zeitpunkt nicht erschwinglich waren.

[2] **G**iga**B**it **I**nterface **C**onverter

1.4 Vetterstraße 52

Die Etagenverkabelung (Eigenverkabelung) besteht aus 3 BNC-Segmenten in jeder Etage. Durch die Unzulänglichkeiten der BNC-Technik ändert sich die Verkabelung häufiger als in den TP-Wohnheimen.
In einigen Fällen sind die BNC-Kabel von 2 Etagen in einem E-Raum an einen Repeater angeschlossen.
In anderen Fällen sind die Segmente über Medienkonverter an SOHO-Switches angeschlossen, welche die Segmente untereinander switchen. Von den E-Räumen liegen in der Regel 2 Adern 62,5μm MMF bis in den E-Raum der ersten Etage. Dort werden an einem **Allied-Telesyn AT-3714FXL/SC** Glasswitch die Etagen zusammengefasst. Von diesem wird der Uplink der V52 über ein Adernpaar in den Keller der V54 realisiert.

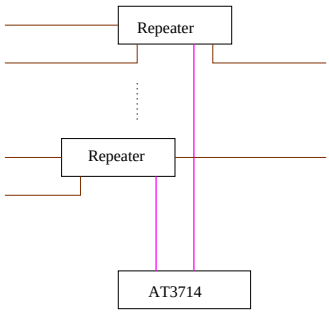


Abbildung 2: Aufbau V52

Das Wohnheim wird zur Zeit saniert und mit neuer Verkabelung und Technik ausgestattet. Die geplante Ausstattung ist auf Seite 10 näher beschrieben.

1.5 Vetterstraße 54

Mit dem Einsatz des Cisco 6500 ist die klassische Anbindung eines Wohnheims über einen Hausswitch abgelöst worden. Die einzelnen Etagen der V54 sind über je ein 100FX 50μm MMF an einem Medienkonverterblock angeschlossen. Die resultierenden Kupferanschlüsse liegen an einem 48-Port 10/100/1000 TP-Modul im 6500er an. Die jeweiligen Etagen sind mit verschiedenen 3com Geräten ausgestattet. In den Etage 0, 1, 3, 5 und 7 sind jeweils 2 **3com 1100** (10BASE-TX, 1x 24 Ports, 1x 12 Ports) mittels Matrix-Kabel gestackt. In den übrigen Etagen wurden je ein **3com 3300** (10/100 TX, 24 Ports) und ein **3com 1100** (10BASE-TX, 12 Ports) verbaut und über ein normales TP-Patchkabel verbunden. Als Reserve liegt ein weiteres Adernpaar in jeder Etage, welches aber ohne Anschlüsse ist. In der Anfangsphase mußten mehrere Geräte ausgetauscht werden. Aktuelle Ausfälle betreffen die Glas-Module in den Geräten.
Im Rahmen einer Teststellung konnten wir Geräte von HP testen. Dabei wurde auch der Uplink der Etage erfolgreich über 1000BASE-SX getestet.

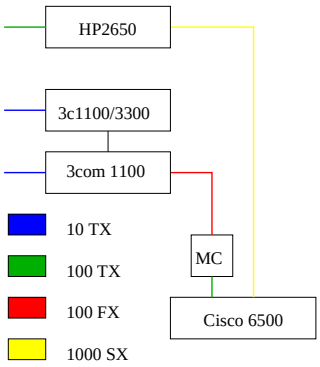


Abbildung 3: Aufbau V54

1.6 Vetterstraße 64/66

Analog zur V52 existiern 3 BNC-Segmente pro Etage (Abb. 2 Seite 4). Um die Ausfälle der Repeater zu kompensieren und die Qualität zu verbessern, kommen auch hier BNC/TP-Medienkonverter in mehreren Etagen zum Einsatz. Änderungen im Etagenbereich sind häufig und nicht dokumentierbar. Die Etagenuplinks beider Häuser führen über 62,5μm MMF und einen weiteren Medienkonverter zum gemeinsamen Hausswitch. Hier kommt ein **Cisco 3550** mit 24 10/100 TX Anschlüssen zum Einsatz. Der Uplink der beiden Wohnheime wird über ein LX GBIC in Richtung V54 realisiert.

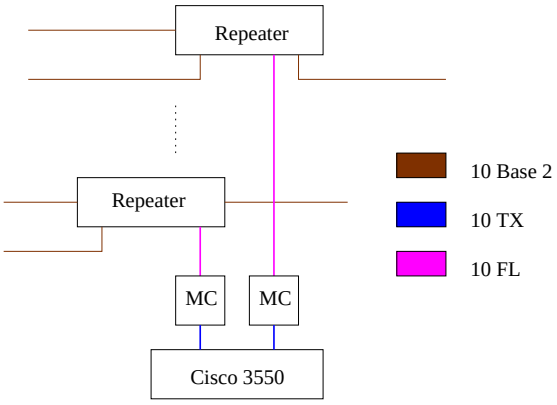


Abbildung 4: Aufbau V64/66

1.7 Vetterstraße 70/72

Die Vettersstraße 70 (V70) wurde 1996/1997, die Vettersstraße 72 (V72) 1998 ans Campusnetz angebunden. Im Mai 2002 wurde die Erstausstattung beider Wohnheime, bestehend aus 10 Mbit TP-Hubs der Firma 3com ersetzt. Auf jeder Etage wurden ein **3com 3300 Classic** und ein **3com 3300 XM** (durch Matrix-Kabel gestackt) verbaut. Damit hat die V70/72 als erstes Wohnheim 100Mbit-Nutzeranschlüsse. Aus Kostengründen konnten die Etagen-Uplinks nicht auf Gigabit-Technik aufgerüstet werden. Der prinzipielle Aufbau der Hausverkabelung entspricht im wesentlichen dem der V54.

Leider mußten allein im ersten Jahr nach dem Einbau mehr als die Hälfte der Technik wegen Defekten ausgetauscht werden. Betroffen waren fast ausschließlich die Switches der XM-Serie, die scheinbar billigere EEPROMs[3] bzw. Flash-Bausteine besitzen, welche die nächtlichen Schreibzyklen des Konfigurationsskripts nicht lange verkrafteten. Symptomatisch für einen Defekt war der komplette Ausfall des Managements. Neuere Erkenntnisse legen auch Anfälligkeit gegenüber bestimmten Netzwerkkarten nahe, welche fast unmöglich zu finden sind.

1.8 Reichenhainer Straße 35/37

Die Rh35/37 ist das erste Wohnheim, welches im Zuge einer Sanierung durch das Studentenwerk mit Switch-Technik statt Hubs ausgestattet wurde. In jeder zweiten Etage ist ein E-Raum mit 3 **3com 1100** (10BASE-TX) Durch eine ungenaue Spezifikation der Anforderungen sind statt „echten“ Stacking über Matrix-Kabel nur einfache Patchkabel zum Verbinden der einzelnen Geräte zum Einsatz gekommen. Der Nachkauf von Stacking-Modulen und entsprechenden Kabeln wurde aus Kostengründen nicht realisiert. Die Etagenuplinks bilden jeweils ein Glasfasermodul mit 100BASE-FX und führen über 50μm MMF bis in den Keller der Rh35.

1.9 Reichenhainer Straße 51

Nach Rückbau der BNC-Technik im Januar 2004 stand das Wohnheim mehrere Monate leer. Im Rahmen der Wiederinbetriebnahme wurden in Eigenregie die Zimmer mit Twisted-Pair (Cat.7) und einer Doppeldose pro Zimmer verkabelt. Aufgrund der geringen Gebäudehöhe wurden alle Anschlüsse in einen zentralen E-Raum geführt. Nach Beschaffung der Technik sollen die Nutzer mit 100MBit zunächst einen Port pro Dose nutzen können. Für die Anbindung des Wohnheimes muß auf einen LED-Link mit 10MBit zurückgegriffen werden, da noch keine Glasfaserkabel existieren.

1.10 Thüringer Weg 3

Die obersten 2 Etagen des TW3 sind im Zuge einer Sanierung mit Twisted-Pair verkabelt worden. 3 über Matrix-Kabel gestackte **3com 3300** (10/100BASE-TX) stellen die komplette Technik für die Nutzer. Ein Laserlink auf Dach versorgt das Gebäude wetterabhängig mit Netz. Das Campusradio UniCC sendet ebenfalls über diese Strecke.

[3] Electrically Erasable and Programmable Read Only Memory

2 Konfiguration

Vor dem Einbau wurden alle Geräte mit einer Grundkonfiguration versehen, welche unter anderem aus IP-Adresse, SNMP-Communities und VLAN[4]-Konfiguration. Remotezugänge zu den Geräten werden durch ein Passwortschema abgesichert.

2.1 Zentraler Router

Im CSN verwendete VLANs:

VLAN-ID	Subnetz	Wohnheim	Bemerkung
1	134.109.101/24		Default-VLAN und Management
2	134.109.84.0/22	Rh37	
3	134.109.80.0/22	Rh35	
4	134.109.112.0/22	TW3	
5	134.109.108.0/22	V72	
6	134.109.88.0/22	V70	
7	134.109.116.0/22	V64	
8	134.109.104.0/22	V66	
9	134.109.96.0/22	V54	
10	134.109.92.0/22	V52	
12	ohne IP		Ersatz-VLAN
144	134.109.144.0/24		URZ-VLAN 144

Das Ersatz-VLAN 12 ist für die Interoperabilität zwischen Geräten verschiedener Hersteller nötig. Ursprünglich waren nur 3com Geräte im Einsatz, so daß keine Probleme auftraten. Hintergrund ist, daß 3com erlaubt, daß alle VLANs einer Verbindung *tagged*[5] sein können. Bei Cisco-Geräten ist dagegen immer ein *untagged* VLAN notwendig. Um nicht über 60 Geräte umkonfigurieren zu müssen, wurde im Router dieses VLAN *untagged* zusätzlich über die Strecken geschickt, wo die Gegenseite die genutzten VLANs *tagged* erwartet. Da über dieses VLAN kein Netzverkehr läuft, kann es problemlos von der Gegenseite verworfen werden.
Hierbei offenbaren sich weitere Designschwächen und Probleme mit den Geräten von 3com. Per Definition wird bei Fehlern im VLAN-Tagging der Traffic in das Default-VLAN geleitet. Dieses VLAN 1 ist im CSN das Management-VLAN in dem das Transfernetz (134.109.100.0/24) liegt. Daher wird von empfohlen, daß VLAN 1 mit möglichst wenig Rechten auszustatten. Es ist bei keinem 3com-Gerät jedoch möglich festzulegen, in welchem VLAN die IP des Gerätes liegt. Desweiteren ist jeglicher Zugriff auf Managementfunktionen (Telnet, SNMP, WWW) auf das VLAN 1 beschränkt. Das bedeutet, daß die IP des Gerätes automatisch im VLAN 1 liegt. In der Vergangenheit konnte bereits beobachtet werden, daß es zu VLAN-Fehlern kommen kann, so daß man dies Einschränkung durchaus als ein Sicherheitsproblem klassifizieren kann. Eine Änderung dieses Zustandes sollte bei Neubeschaffung und Ersatz berücksichtigt werden. Andere Möglichkeiten zur Lösung des Problems sollten ebenfalls überdacht werden.

[4] Virtual Local Area Network
[5] siehe IEEE 802.1q

2.2 Vettersstraße 52

Der Hausswitch `mpr-52-at` besitzt keine VLAN Konfiguration. Das Default-VLAN liegt an allen Ports an. Dies ist auch der einzige Switch mit einer IP, die im IP-Bereich des Hauses liegt. Das statische Eintragen aller freigeschalteten MAC-Adressen jeder Etage an dem entsprechenden Port des `mpr-52-at` wird nicht realisiert. Grund hierfür ist die sich häufig ändernde, nicht in der Datenbank abgebildete BNC-Netzstruktur im Etagenbereich.
Im Rahmen der Sanierung des Gebäudes wird die vorhandene Technik abgelöst.

2.3 Vettersstraße 54

In der Grundkonfiguration ist jeder Port außer dem Uplink abgeschaltet und auf das VLAN des Hauses (`VLAN ID 9 "v54/96"`) konfiguriert. Auf dem Uplink-Port liegt zusätzlich das globale Management-VLAN (`VLAN ID 1`) an. Dazu ist das standardisierte VLAN-Tagging nach IEEE 802.1q für beide VLANs aktiviert. Auf den übrigen Ports (Nutzeranschlüsse) ist das Tagging abgeschaltet (`native`). Auf Routerseite ist zusätzlich das VLAN 12 als „Native-Ersatz“ angelegt.

VLAN	802.1q	Port
1	ja	Uplink
9	ja	Uplink
9	nein	Nutzerports

2.4 Vettersstraße 64/66

Der Hausswitch `mpr-64-k` (**Cisco 3550-24**) ist die einzige „moderne“ Komponente des Doppelwohnheims. Der Uplink beider Wohnheime erfolgt über eine gemeinsame 1000BASE-SX MMF Leitung zur V54. Über diese liegen die VLANs 1,7 und 8 (tagged) und 12 (untagged) an.

2.5 Vettersstraße V70/72, Reichenhainer Straße 35/37, Thüringer Weg 3

In den übrigen Wohnheimen entspricht die Konfiguration dem Modell der V54. Die Geräte sind mit dem untagged Haus-VLAN (V70: `VLAN ID 6 "v70/88"`, V72: `VLAN ID 5 "v72/108"`, Rh35: `VLAN ID 3 rh35/80"`, Rh37: `VLAN ID 2 rh37/84"`) auf den Nutzer-Ports konfiguriert. Das Management-VLAN (`VLAN ID 1`) und Haus-VLAN liegen über IEEE 802.1q am Uplink-Port jeder Etage an.

3 Planung

Grundsätzlich sollte sich die Planung von neuen Technologien an offenen und verbreiteten Standards orientieren. Proprietäre Lösungen sind möglichst zu vermeiden.

3.1 Backbone

Schon jetzt ist die Mehrzahl der Häuser mit Gigabit-Technik angebunden. Mittelfristig bietet diese Strecken genügend Kapazitäten. Langfristig ist die Möglichkeit der Aufrüstung auf 10 Gigabit denkbar. Dazu ist es notwendig neue Glasfaser zu verlegen, da Technik für 62,5 μm Kabel (1000BASE-LX) schwer bis nicht mehr beschaffbar ist. Konkret sind je 12 neue Fasern mit 50 μm der Klasse OM3 für die Verbindungen V54-V70, V54-72 und V54-64 angedacht. Desweiteren ist es notwendig die Haupstrecke V54-Rh35 mit zusätzlichen Fasern zu versorgen. Auch hier sind 12 Fasern angedacht.

3.2 Vettersstraße 52

Im Rahmen der Sanierung dieses Wohnheims wird die bestehende BNC-Technik abgelöst und durch Twisted-Pair ersetzt. Hinsichtlich der Mehrfachnutzung von IP-Technologie für Telefon oder auch Video wird jedes Zimmer mit eine Doppeldose ausgestattet.

- 8 Etagen mit je 31 Zimmer
- 2 Klubräume mit je 2 Doppeldosen
- insgesamt 504 10/100Base-TX Ports

Hierbei wird bei der technischen Ausstattung die Verfügbarkeit von zukunfsweisenden Technologien berücksichtigt. So sind die Hälfte aller Anschlüsse fähig Strom für IP-Telefone und andere Geräte nach dem IEEE Standard 802.3af (Power over Ethernet) zu liefern.
Durch den Vollanschluß aller 8 Adern ist es möglich in Zukunft durch andere Technik Gigabit an jedem Port anzubieten.
Ein Novum innerhalb des CSN soll das redundante Netzwerkdesign werden. Durch Zusatzverkabelung wird erstmals eine Sicherheit gegen Hardware- und Netzdefekte erprobt. Ebenfalls richtungsweisend ist die Vorbereitung von drahtlosem Netzzugang in den Clubs und auf den Wiesen vor dem Wohnheim. Zur Absicherung soll ein VPN[6] zum Einsatz kommen.

3.3 Vettersstraße 54

Im Etagenbereich sind bereits einige Geräte mit 100Base-TX Ports ausgestattet. Diese Entwicklung soll konsequent fortgesetzt und alle Etagen über jeweils 1000BASE-SX am Router angebunden werden.
Das nicht angeschlossene 2. Aderpaar in jeder Etage bietet zusätzlich die Möglichkeit einer redundanten Anbindung.

[6] Virtual Private Network

3.4 Vettersstraße 64/66

Die bisher ungewisse Situation in diesen beiden Wohnheimen erlaubt noch keine Planung für einen zukünftigen Netzausbau. Tendenziell ist jedoch klar, daß auch hier das Ziel 100Base-TX am Nutzerport und 1000BASE-SX pro Etage heißen muß.

3.5 Vettersstraße 70/72

Nachdem sich die Investition in 3com Technik leider nicht bezahlt gemacht hat, ist die Zukunft des weiteren Ausbaus dieses Wohnheims mehr als ungewiss. Theoretisch fehlen lediglich 1000Base-SX Module auf jeder Etage um die beiden Häuser auf den aktuellen Stand der Technik zu bringen.

3.6 Reichenhainer Straße 35/37

Als zuletzt saniertes Wohnheim ist die verbaute Technik schon relativ alt. Nach der V54 ist dies das nächste Objekt.

3.7 Reichenhainer Straße 51

Die Anbindung von 125 Nutzern über einen 10MBit LED-Link kann keine Lösung auf Dauer sein. Hier ist es Ziel eine Glasfaserleitung zu verlegen, die das Wohnheim mit dem restlichen CSN-Backbone verbindet.

3.8 Thüringer Weg 3

Die wetterabhängige Anbindung stellt das größte Problem in diesem Wohnheim dar. Alternativen wären der Einsatz von Richtfunk-Technik oder eine Anbindung über Glasfaser. Richtfunk-Technik ist entwicklungstechnisch eine Einbahnstraße und sollte nur als Notbehelf in Erwägung gezogen werden.
Bei einer zuverlässigen Anbindung der Rh51 über Glasfaser besteht die Möglichkeit über eine neue Glasfaser-Strecke auch dieses Wohnheim mit dem CSN-Backbone zu verbinden. Diese würde dann vom Thüringer Weg 3 über Mensa zur Rh51 führen.
Als weitere Alternative bieten sich die bestehenden Glasfaser-Kabel des URZ durch den TW3 in Richtung TW11 an.

3.9 Neue Technologien

3.9.1 Voice over IP

Warum?

- innerhalb der Wohnheime kostenfrei telefonieren
- Rollout von VoIP Technik im Campus
- Kommunikation mit Professoren, Prüfungsamt, StudSek, etc.

Wie?

- zusätzliche Dosen im Zimmer (separater Telefonanschluß)
- QoS-fähige Technik bis in die Etagen
- Power over Ethernet nach IEEE 802.3af
- Voice VLANs

Wann?

- bei Sanierungen werden Doppeldosen verlegt (V52,RH51 - 2004)
- QoS, 802.3af - bei Beschaffung berücksichtigt (z.B.: Cisco 3750-48PS)
- erste Tests 2004/2005
- CSN-interne Telefonate 2005/06

3.9.2 Netzzugang nach IEEE 802.1X

Warum?

- Zusätzliche Absicherung
- Instant-Access für Neuanschlüsse
- Absicherung für drahtlose Zugänge
- Roaming innerhalb des Campus

Wie?

- Netzkomponenten im Etagenbereich mit 802.1X
- RADIUS Server mit Authentifizierung über Zertifikate od. URZ Login

Wann?

- neue Geräte 802.1X fähig (2004-)
- zentraler RADIUS Server (2006)

3.9.3 WLAN Zugang

Warum?

- Versorgung der Studentenclubs
- Versorgung der Wiesen vor den Wohnheimen
- In den Vorlesungssäalen und der Mensa sehr erfolgreich

Wie?

- Access Points an Gebäude und in Clubräumen
- VPN Gateway (kein ungesicherter Zugang)
- Authentifizierung über URZ Login / Zertifikate (802.1X) an RADIUS

Wann?

- eventuell nach Sanierung V52 - 2005

4 Anhang

4.1 Router-Konfiguration

4.1.1 Generische Einstellungen

```
service timestamps debug datetime
service timestamps log datetime
service password-encryption
service sequence-numbers
!
hostname mpr-54-r
!
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
vtp mode transparent
ip subnet-zero
!
ip domain-list csn.tu-chemnitz.de
ip domain-list tu-chemnitz.de
ip domain-name csn.tu-chemnitz.de
ip name-server 134.109.102.249
!
ip multicast-routing
ip sap cache-timeout 30
```

4.1.2 NetFlow

```
! Netflow Konfiguration - kurze Alterungszeiten fuer die Flows
! um eine hoehere Zeitaufloesung zu erhalten
! Nachteil: hoehere Anzahl an Flows werden exportiert
! Flows mit weniger als 64 Paketen werden innerhalb von 8 Sekunden
! verschickt
mls aging fast time 8 threshold 64
!
! Ein Flow wird nach spaetestens 64 Sekunden abgesetzt
! und exportiert
mls aging long 64
!
! Normale Alterungszeit 32 Sekunden
mls aging normal 32
!
! Export der vollstaendigen IP Information
! (Absende-IP, Ziel-IP, Sendeport, Zielport, Protokoll
! Oktets und Packete)
mls flow ip full
!
! Netflow Version 5 (enthaelt o.g. Informationen)
mls nde sender version 5
```

4.1.3 VLAN

4.1.3.1 Beschreibung

```
vlan 2
 name rh37/84
!
vlan 3
 name rh35/80
!
vlan 4
 name tw3/112
!
vlan 5
 name v72/108
!
vlan 6
 name v70/88
!
vlan 7
 name v64/116
!
vlan 8
 name v66/104
!
vlan 9
 name v54/96
!
vlan 10
 name v52/92
!
vlan 12
 name NativeErsatz
!
vlan 144
 name Vlan144/hrz
```

4.1.3.2 Interfaces

```
! da keine redundanten Strecken existieren
! ist Spanning-Tree auf allen VLANs abgeschaltet
no spanning-tree vlan 1-10,12
!
!
interface Vlan1
 ip address 134.109.102.3 255.255.254.0
 ip access-group 105 out
 ip route-cache flow
 mls netflow sampling
!
interface Vlan2
 ip address 134.109.87.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan3
 ip address 134.109.83.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan4
 ip address 134.109.115.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan5
 ip address 134.109.111.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
```

```
interface Vlan6
 ip address 134.109.91.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan7
 ip address 134.109.119.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan8
 ip address 134.109.107.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan9
 ip address 134.109.99.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan10
 ip address 134.109.95.254 255.255.252.0
 ip helper-address 134.109.102.249
 ip helper-address 134.109.102.1
 ip pim sparse-dense-mode
 ip route-cache flow
 mls netflow sampling
!
interface Vlan12
 no ip address
!
interface Vlan144
 no ip address
```

4.1.4 Uplink und Multicast-Tunnel

```
interface Tunnel0
 description UniCC MultiCast Tunnel
 ip unnumbered Vlan1
 ip pim sparse-dense-mode
 ip multicast boundary 12
 tunnel source Vlan1
 tunnel destination 134.109.100.248
!
!
interface GigabitEthernet1/1
 description Uplink URZ
 speed nonegotiate
 switchport
 switchport mode access
 rmon collection stats 1 owner monitor
 no cdp enable
```

4.1.5 Hausuplinks

```
interface GigabitEthernet3/5
 description Uplink RH35/37
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1-3
 switchport mode trunk
!
interface GigabitEthernet3/6
 description Uplink V64/66
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1,7,8
 switchport mode trunk
!
interface GigabitEthernet3/7
 description Uplink V70
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1,6
 switchport mode trunk
 no cdp enable
!
interface GigabitEthernet3/8
 description Uplink V72
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1,5,144
 switchport mode trunk
 no cdp enable
!
interface GigabitEthernet5/42
 description Uplink TW3
 switchport
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1,4
 switchport mode trunk
 power inline never
 no cdp enable
```

```
interface GigabitEthernet5/43
 description Uplink V52 Link 1
 switchport
 switchport access vlan 10
 switchport mode access
 power inline never
 no cdp enable
```

4.1.6 direkt angeschlossene Ports V54

4.1.6.1 Etagenuplink

```
interface GigabitEthernet3/1
 description V54 7. Etage
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport trunk allowed vlan 1,9
 switchport mode trunk
```

4.1.6.2 Zwischenbau

```
interface GigabitEthernet5/13
 description V52/54 Zwischenbau
 switchport
 switchport access vlan 9
 switchport mode access
 power inline never
 no cdp enable
```

4.1.7 Ports für CSN-eigene Rechner

```
interface GigabitEthernet5/45
 description Asgard Interface 1
 switchport
 switchport mode access
 power inline never
 no cdp enable
```

4.1.8 IP Routing

```
ip default-gateway 134.109.102.249
ip classless
ip route 0.0.0.0 0.0.0.0 134.109.102.249
ip route 10.0.0.0 255.0.0.0 Null0
ip route 169.254.0.0 255.255.0.0 Null0
ip route 172.16.0.0 255.240.0.0 Null0
ip route 192.168.0.0 255.255.0.0 Null0
ip flow-export source GigabitEthernet5/47
ip flow-export version 5
ip flow-export destination 134.109.102.1 12000
no ip http server
ip mroute 0.0.0.0 0.0.0.0 Tunnel0
```

4.1.9 Logging und ACLs

Export aller Systemnachrichten auf den zentralen CSN-Server

```
logging trap debugging
logging facility local6
logging 134.109.102.249
```

Zugriffkontrolle auf verschiedene Dienste

```
! Zugang zum NTP Server des Router verboten
access-list 1 deny   any
!
! NTP Aktualisierung nur von URZ NTP Rechnern
access-list 2 permit 134.109.200.7
access-list 2 permit 134.109.102.1
access-list 2 permit 134.109.2.15
!
! Zugang zum Management des Routers nur von bestimten IPs (gekuerzt)
access-list 5 permit 134.109.102.249
access-list 5 permit 134.109.102.1
access-list 5 permit 134.109.102.63
access-list 5 deny   any
```

```
! Zugang zum kompletten Management VLAN nur fuer Admin-IPs
! Zugang fuer alle zu CSN-Rechnern mit Diensten
! ICMP erlaubt zur Netzwerkdiagnose
access-list 105 permit ip host 134.109.108.1 134.109.102.0 0.0.1.255
access-list 105 permit ip host 134.109.96.70 134.109.102.0 0.0.1.255
access-list 105 permit ip host 134.109.96.136 134.109.102.0 0.0.1.255
access-list 105 permit ip host 134.109.88.29 134.109.102.0 0.0.1.255
access-list 105 permit ip host 134.109.88.3 134.109.102.0 0.0.1.255
access-list 105 permit ip any host 134.109.102.1
access-list 105 permit ip any host 134.109.102.63
access-list 105 permit ip any host 134.109.102.249
access-list 105 permit icmp any 134.109.102.0 0.0.1.255
access-list 105 deny   tcp any 134.109.102.0 0.0.1.255 range 0 65535 log
access-list 105 deny   udp any 134.109.102.0 0.0.1.255 range 0 65535 log
access-list 105 deny   ip any 134.109.102.0 0.0.1.255
access-list 105 permit ip any any
!
! Dummy-MAC wird nicht geroutet (VLAN 2-10)
mac-address-table static dead.beef.dead vlan 9 drop
```

4.1.10 NTP

```
ntp access-group peer 2
ntp access-group serve-only 1
ntp server 134.109.102.1
ntp server 134.109.2.15
ntp server 134.109.200.7
```

4.1.11 Intrusion Detection

```
monitor session 1 source vlan 2 - 10 rx
monitor session 1 destination interface Gi5/48
```