Design und Umsetzung einer verlässlichen Internet-Infrastruktur auf Basis von lizenzfreiem Richtfunk

Bachelorarbeit

zur Erlangung des Grades „Bachelor of Science“

an der
Hochschule Niederrhein
Fachbereich Elektrotechnik und Informatik
Studiengang Informatik

vorgelegt von: **Gunnar Graßhoff**
Matr.-Nr.: 783359

Prüfer: Prof. Dr. Steffen Goebbels
Zweitprüfer: Dipl.-Ing. Immo Wehrenberg

Krefeld, den 01.03.2013

Ich versichere durch meine Unterschrift, dass die vorliegende Abschlussarbeit ausschließlich von mir verfasst wurde. Es wurden keine anderen als die angegebenen Quellen und Hilfsmittel benutzt.

Krefeld, den

Unterschrift:

Aus Gründen der Lesbarkeit wird in dieser Arbeit nur die männliche Personenform verwendet.

Inhaltsverzeichnis

1 Einleitung

Menschen haben seit jeher den Bedarf, Informationen auszutauschen. Computer-Netzwerke und insbesondere das Internet, haben sich als wesentliche Kommunikationsmedien etabliert. Einhergehend mit seiner Verbreitung hat sich das Internet gleichermaßen als ein essenzieller Teil von Organisation entwickelt. In urbanen Regionen ist die Verwendung des Internets für die Mehrheit der Bewohner ohne Komplikationen möglich geworden.

In strukturschwachen Regionen, in denen keine, wenige oder nur schlechte Verbindungen in das Internet bestehen, sind selbstorganisierte Infrastrukturen eine Alternative, um individuelle, kostengünstigere oder generell Anschlüsse und höhere Bandbreiten zu ermöglichen (vgl. [Kap09]).

In Katastrophenfällen kann das Internet als schnelles Verbreitungsmedium von Not- und Sicherheitsmeldungen und darüber hinaus zur Unterstützung bei der Suche nach Vermissten dienen. Wenn bestehende Strukturen durch Katastrophen zerstört werden, sind möglichst schnell und trivial zu errichtende, neue Strukturen notwendig (vgl. [Saf11]).

In Gebieten, in denen politische Spannungen herrschen, waren und sind Menschen mit Hilfe der sogenannten sozialen Medien dazu fähig, sich zu organisieren. Regimes, die die Infrastrukturen vor Ort kontrollieren, können diese Organisationsform unterbinden und einschränken, indem sie die Zugänge zensieren, sperren oder vollständig abschalten. Mit Hilfe von selbst verwalteten Strukturen, die schnell und einfach, parallel zu den staatlichen Strukturen aufgebaut werden können, sind Menschen in der Lage solche Kontrollen zu umgehen.

Die „Nutzung neuer Formen elektronischer Kommunikation zur Förderung eines freien und unzensierten Informationsaustauschs für interessierte Individuen und Gruppen“ ([Lie09]) sind erklärte Ziele des Vernetzungsprojektes „FREE!“. FREE! hat bereits mehrere Projekte durchgeführt, um Menschen unzensierte Informationen bereitzustellen und einen Zugang in das Internet anzubieten, der frei von staatlicher Kontrolle ist. So hat FREE!, als im Frühjahr 2011 in Ägypten das Internet buchstäblich abgeschaltet wurde, es den Ägyptern ermöglicht, sich über das Telefonnetz in das Internet einzuwählen und damit die Zensur zu umgehen (vgl. [Lie11]).

FREE! ist Bestandteil des gemeinnützigen Vereins Wissenschaftsladen Dortmund (WilaDo).

> „Wissenschaftsläden (WiLas) sind zuerst entstanden in den 70er Jahren in den Niederlanden – “wetenschapswinkel” – und stehen im Zeichen der gesellschaftlichen Verantwortung der Wissenschaft. Sie sehen sich als Bindeglied zwischen Wissenschaft und Gesellschaft. Das bedeutet zum einen wissenschaftliches Potential für gesellschaftliche Gruppen

verfügbar zu machen [...] und umgekehrt die Einbringung gesellschaftlich relevanter Fragestellungen in Forschung und Lehre.“ ([Wil96])

Problemstellung

Ziel dieser Arbeit ist das Design und die Umsetzung einer flexiblen Infrastruktur auf Basis von lizenzfreiem Richtfunk. Der Wissenschaftsladen Dortmund soll aus diesem Netzwerk einen konkreten Nutzen ziehen können, etwa indem Benutzer mit dem Wissenschaftsladen direkt oder untereinander verbunden werden und indem der Wissenschaftsladen Zugang zu anderen Netzwerken sowie Netzwerken des Internets erhält. Die wissenschaftlichen Ergebnisse dieser Arbeit sollen auch anderen gesellschaftlichen Gruppen, als Prototyp und Grundlage für eigene Netzwerke, die in den oben angedeuteten Szenarien eingesetzt werden können, zur Verfügung gestellt werden. Für solche Einsatzgebiete haben Richtfunkverbindungen gegenüber kabelgebundenen Netzwerken den Vorteil, erheblich schneller und einfacher aufgebaut werden zu können.

Als Voraussetzungen für die Realisierung dieser Ziele ist es wichtig, dass die Hardware nach ökonomischen und ökologischen Gesichtspunkten sinnvoll, d.h. energieeffizient und preiswert, ausgewählt wird. Die zu realisierenden Verbindungen sollen stabil, fehler- und ausfalltolerant sowie lizenzfrei sein und eine möglichst hohe Bandbreite gewährleisten.

Aufbau der Arbeit

In Kapitel 2 werden die technischen Grundlagen von Computernetzwerken, anhand des OSI-Modells veranschaulicht. Insbesondere wird auf notwendige Protokolle eingegangen, die für das Verständnis dieser Arbeit erforderlich sind.

Im Anschluss daran werden die Grundlagen von WLAN und der Richtfunktechnik in Kapitel 3 behandelt. Dieses Kapitel bildet die Grundlage für die Planung und den Aufbau der Funkstrecken.

Das Szenario, in dem die Bachelorarbeit entstanden ist und aus dem sich die Voraussetzungen für das Netzwerk ableiten, wird in Kapitel 4 behandelt. Dort werden die geplanten Verbindungen vorgestellt und anhand dessen werden die einzelnen Nutzungsarten genauer untersucht.

Der Entwicklungsprozess des Netzwerkdesigns wird in Kapitel 5 dargestellt. In diesem Kapitel wird geeignete Hardware vorgestellt. Des Weiteren werden dort verschiedene Lösungsansätze gegenübergestellt und anhand von Versuchen erläutert.

In Kapitel 6 wird nochmals knapp die eingesetzte Lösung vorgestellt, sowie die umgesetzten Richtfunkstrecken und deren Aufbau dargestellt.

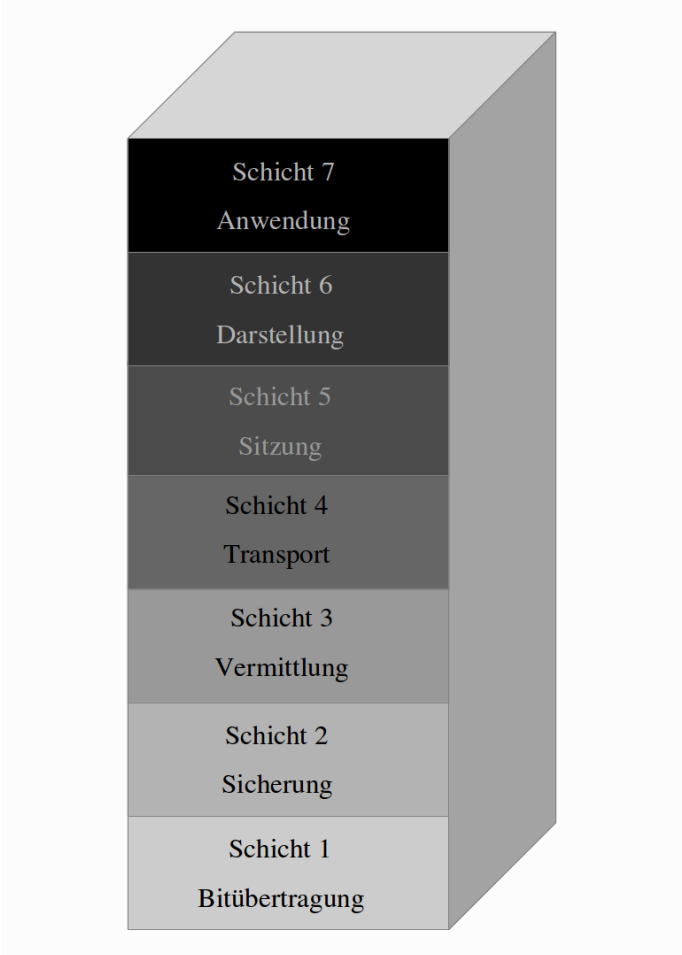
Abschließend wird in Kapitel 7 ein Fazit gezogen. Am Ende dieses Kapitels wird außerdem noch auf zukünftige Entwicklungen verwiesen.

2 Grundlagen von Computer-Netzwerken

> „Dienste und Funktionen von Kommunikationssystemen lassen sich in einer mehrschichtigen Struktur anordnen, wodurch die Einordnung von Protokollmechanismen und -funktionen erleichtert wird.“ ([Be05], S. 21)

Um die Netzwerkgrundlagen für diese Arbeit zu erläutern, werden die Datensicherungsschicht und die Vermittlungsschicht des “Open System Interconnection” OSI-Referenzmodells als Vergleichsbasis verwendet. Das OSI-Referenzmodell ist ein herstellerunabhängiges Gliederungsschema. Das Modell ist in sieben Schichten eingeteilt, auf den jeweiligen Schichten sind unterschiedliche Protokolle angesiedelt. Die einzelnen Schichten sind durch definierte Schnittstellen voneinander getrennt. Das heißt auch, dass jede Ebene Mechanismen besitzt, um die Daten der über ihr liegenden Schicht einzupacken und diese Daten durch eigene, schichtbezogene Daten zu erweitern. Diese Daten werden auch an die nächsttiefere Schicht weitergegeben und umgekehrt von tieferen zu höheren Schichten (Abs. vgl. [HPR+06], S. 258 und [Be05], S. 21f).

Abbildung 2.1: Das OSI-7-Schichtenmodell



Die Abbildung 2.1 zeigt das OSI-Modell (vgl. [HPR+06], S. 258). Die Datensicherungs- und die Vermittlungsschicht sind dabei an dem Datentransport orientiert und nicht wie die darüber liegenden Schichten - ab Schicht 5 - an den Anwendungen (vgl. [HPR+06], S. 258). Die Beschreibung der Übertragung, beispielsweise über Kabel oder über Richtfunkstrecken, ist auf Schicht 1 angesiedelt (vgl. Abschnitt 3.2.1).

2.1 Redundanz

Mit Redundanz ist allgemein das mehrfache Vorhandensein von Ressourcen gemeint. Mit redundanten Strukturen soll die Zuverlässigkeit und Verfügbarkeit eines Netzwerks oder von Teilnetzwerken verbessert werden. Für Redundanz gibt es folgende, unterschiedliche Entsprechungen auf den Ebenen des OSI-Modells:

- eine Anwendung kann mehrfach oder parallel ausgeführt werden
- Daten können wiederholt gesendet werden
- ein Gerät kann mehrere Wege zu einem Ziel kennen
- auf physikalischer Ebene kann die gleiche Hardware mehrfach vorhanden sein

Durch Redundanz entsteht eine höhere Komplexität. So müssen redundant angelegte Strukturen synchronisiert werden.

2.2 Vermittlungsschicht (Schicht 3)

Die dritte Ebene des OSI-Referenzmodells wird auch Netzwerkschicht genannt.

> „Die Netzwerkschicht stellt die Klasse der Netzwerkdienste bereit, deren wesentliche Aufgabe es ist, Kommunikation zwischen Endsystemen in einem nicht vollvermaschten Netz zu realisieren, d.h. in einem Netz, in dem nicht alle Endsysteme direkt miteinander kommunizieren können. Dies impliziert die Existenz von Zwischensystemen, sogenannten Routern, die an mehrere Teilnetze angebunden sind und Pakete zwischen diesen vermitteln. Für diese Vermittlungsfunktion ist eine Wegewahl notwendig, d.h., das Zwischensystem muss für jedes zu vermittelnde Paket feststellen, in welches der angeschlossenen Teilnetze und evtl. zu welchen weiteren Zwischensystemen es weitergesendet werden muss." ([Be05], S. 193)

2.2.1 Internet und das Internet Protocol (IP)

Damit Netzwerkgeräte gezielt miteinander kommunizieren können, wurden verschiedene Protokolle etabliert.

> „Das heute verbreitetste Schicht-3-Protokoll ist das Internet Protocol auch kurz IP genannt, bzw. IPv4 für Version 4 und IPv6 für Version 6 des Protokolls." ([Be05], S. 193)

Zum Internet Protocol gehören die IP-Adressen, die es erlauben, in Netzwerken eindeutige Nummern zu vergeben. Hierdurch lassen sich Daten direkt an die jeweilige IP-Adresse und damit an den zugehörigen Rechner versenden. Diese übermittelten Daten werden IP-Pakete genannt, wenn sie den IP-Spezifikationen entsprechen.

> „Die meisten IP-Pakete sind sogenannte Unicasts, sie werden an einen einzigen Zielrechner geschickt. IP-Pakete können auch Multicast (werden an eine Gruppe von Rechnern geschickt) oder Broadcast (sind für alle Rechner gedacht, die sie empfangen können) sein." ([DZCC02], S. 85)

Die Terminologie von Broadcasts und Unicasts wird auch auf anderen Schichten verwendet. Der Bereich, in dem ein Broadcast Paket oder Frame gesehen wird, heißt Broadcast Domäne (vgl. [Huc10], S. 432).

Der IP-Adressraum kann in Teilnetze (Subnetze) unterteilt werden. Endgeräte, die sich in einem Subnetz befinden, müssen dabei auf der Datensicherungsschicht direkt miteinander kommunizieren können. Um die einzelnen IP-Pakete zwischen Teilnetzen zu vermitteln, werden wie oben angedeutet (vgl. Abschnitt 2.2) Router eingesetzt. Die Router bekommen Routen, die dann den Pfad durch das Netzwerk festlegen. Dieser Vorgang heißt Routing. Diese Routen können statisch von einem Administrator eingetragen werden oder dynamisch gelernt werden. Auf der Vermittlungsschicht gibt es eine Vielzahl von Protokollen mit denen die Router untereinander die für das Routing relevanten Informationen austauschen können. Diese Protokolle werden Routing-Protokolle genannt.

Wenn ein Netzwerk gemeint ist, das nach außen hin eine einheitliche Routingstrategie hat, wird von einem Autonomen System gesprochen.

> „Das Internet ist logisch in so genannte Autonome Systeme (AS) untergliedert. Diese sind Teilnetze unter derselben Verwaltung mit einer klar definierten Routing-Policy, die beschreibt, welche Routen mit welchen anderen AS ausgetauscht werden." ([Be05], S. 323)

> „Routing-Protokolle werden entsprechend ihrem Einsatzgebiet in zwei große Klassen abhängig von ihrem Einsatzgebiet untergliedert." ([Be05], S. 323)

Innerhalb eines Autonomen Systems wird ein Interior Gateway Protocol (IGP) eingesetzt. Zwischen Autonomen Systemen wird ein Exterior Gateway Protocol (EGP) verwendet.

> „Protokolle, die nur innerhalb eines AS verwendet werden, werden Interior Gateway Protocol (IGP) genannt. Sie zeichnen sich dadurch aus, dass sie auf eine schnelle Konvergenz Wert legen, jedoch nicht mit großen Mengen von Routen ($<$ 20.000) umgehen können. RIP, OSPF und ISIS sind Beispiele für IGPS.“ ([Be05], S. 323)

Schnelle Konvergenz bedeutet in diesem Zusammenhang, dass die beteiligten Router sich in möglichst kurzer Zeit synchronisieren.

> „Protokolle, die auch für den Austausch von Routen zwischen Organisationen verwendet werden, werden Exterior Gateway Protocol (EGP) genannt. Sie können mit sehr vielen Routen ($>$ 1.000.000) umgehen, legen jedoch weniger Wert auf eine schnelle Konvergenz, sondern eher auf Stabilität.” ([Be05], S. 323)

Das Internet ist der größte und bedeutendste Zusammenschluss aus Autonomen Systemen, die IP verwenden.

2.2.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) ist auf vielen Routern und Unix ähnlichen Betriebssystemen wie OpenBSD oder Linux implementiert. Daher wird hier näher auf dieses Protokoll eingegangen.

> „[...] die Protokolle Open Shortest Path First (OSPF) und Intermediate System-Intermediate System (IS-IS oder ISIS) [gehören] zur Familie der Link-State-Protokolle. Diese zeichnen sich dadurch aus, dass ein Router seine Routing-Entscheidung nicht basierend auf der Sicht seiner Nachbarn trifft, sondern eine globale Sicht auf das Netz und seine Topologie hat und die Routing-Entscheidung selbst trifft. OSPF und ISIS basieren hierbei auf dem Graphenalgorithmus Shortest Path First von Dijkstra und unterscheiden sich nur in wenigen Aspekten.” ([Be05], S. 325)

Als Analogie für diese beiden Protokolle lässt sich eine Landkarte benutzen. Link-State-Protokolle tauschen zunächst Informationen aus, die es jedem Router erlauben, sich eine vollständige Übersicht über das Netzwerk zu bilden. Die Routen werden dann anhand des kürzesten Pfades, auf dieser „Landkarte“ bestimmt.

Mit Hilfe von Hello-Paketen wird die Betriebsbereitschaft von anderen OSPF -sprechenden Netzwerkteilnehmern geprüft (vgl.[Hun03], S. 202f).

> „Das Hello-Paket identifiziert den lokalen Router und führt die benachbarten Router auf, von denen Pakete empfangen wurden.” ([Hun03], S. 202)

> „Hello-Pakete werden von allen Routern in regelmäßigen Zeitabständen ausgesandt. Hört ein Router auf, diese Pakete zu senden, wird davon ausgegangen, daß der Router oder der Link, an dem er hängt, nicht betriebsbereit ist." ([Hun03], S. 203)

Nachdem alle Nachbarn erkannt wurden, führt ein Router ein sogenanntes Link State Advertisement (LSA) aus (vgl. ebd.).

> „Das LSA enthält die Adresse jedes Nachbarn und den Preis zum Erreichen jedes Nachbarn vom lokalem System aus." (ebd.)

Der Preis wird über eine Metrik berechnet, die die Kosten eines Pfades beschreibt. Diese Informationen werden von dem System, welches das LSA ausführt, über alle seine Netzwerkschnittstellen versendet. Die restlichen Netzwerkteilnehmer verfahren mit dem LSA gleichermaßen, allerdings wird die Netzwerkschnittstelle ausgelassen, über die die Informationen eingegangen sind (vgl. ebd.).

> „Um eine Überflutung mit doppelten LSAs zu vermeiden, speichern die Router eine Kopie der LSAs, die sie empfangen, und sortieren Duplikate aus." (ebd.)

LSAs verbreiten sich so im gesamten Netz (Flooding), wodurch jeder Router die gesamte Topologie des Netzes und die jeweiligen Verbindungskosten kennt. Aufgrund dieser Link State Database (LSD) kann ein Router seine Routingtabelle mit dem Shortest Path First Verfahren (Dijkstra-Algorithmus) berechnen.

2.2.3 Border Gateway Protocol (BGP)

Im Gegensatz zu den IGPs wie OSPF oder den hier nicht näher erläuterten IS-IS und OLSR ist das EGP Border Gateway Protocol (BGP) kein Link-State-Protokoll, sondern ein Path-Vector-Protokoll. Benachbarte BGP Router tauschen nicht nur die Information aus, welche Netzwerke sie jeweils erreichen können, sondern auch, welche Autonomen Systeme auf dem Weg zu diesem Netzwerk durchquert werden. Hierbei wird die Komplexität dadurch gesenkt, dass nicht jedes AS seine komplette Topologie weitergibt. Ein AS gibt nur die jeweiligen besten Pfade zum Ziel weiter, die es kennt.

> „In BGP wird ein autonomes System durch seine weltweit eindeutige AS Nummer (ASN, autonomous system number) identifiziert." ([KR08], S. 435)

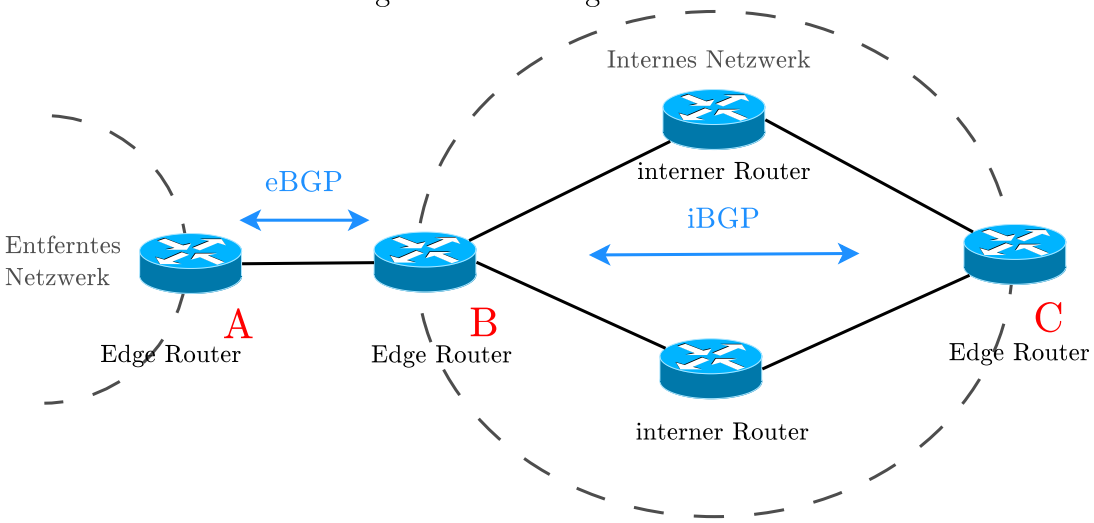
Findet ein BGP Router in der Pfadinformation einer ihm übermittelten Route die ASN desjenigen Autonomen Systems, zu dem er selbst gehört, so verwirft er diese

Route. Dadurch werden Routing-Schleifen verhindert. Im Gegensatz zu Link-State-Protokollen benötigt BGP keine globale Sicht auf das gesamte Netzwerk, also dem Internet.

Zur Auswahl der besten Route aus der Routingtabelle verwendet BGP die Anzahl der durchquerten Autonomen Systeme aus dem Pfad als wichtigen Teil seiner Metrik (vgl. [Be05], S. 326).

BGP-Verbindungen zwischen zwei Autonomen Systemen werden eBGP (external BGP) genannt. Verbindungen innerhalb eines AS werden als iBGP (internal BGP) bezeichnet.

Abbildung 2.2: Verteilung von BGP Routen



In Abbildung 2.2 stellt der als A dargestellte BGP-Edge-Router den Router eines benachbarten AS dar. B verteilt dessen Routen mittels iBGP über die Router im eigenen Autonomen System. So lernt der zweite Edge-Router (C) im eigenen System die Routen. Zusammengefasst bedeutet dies, dass iBGP eingesetzt wird, um die über eBGP gelernten Routen zu den anderen AS, in das eigene AS an andere BGP-Router zu verteilen (vgl. ebd., S. 433f).

Derzeit gibt es mehr als 40.900 vergebene AS-Nummern (vgl. [BSH13]). Jeder eBGP-Router kennt mindestens einen Weg zu jedem anderen erreichbaren AS.

> „Der Einsatz von BGP erfordert eine Vollvermaschung aller Router auf Protokollebene, d.h. alle BGP-sprechenden Router müssen mit allen anderen BGP-sprechenden Routern eine BGP-Verbindung aufbauen und halten. Somit steigt die Anzahl der Verbindungen quadratisch mit der Anzahl der BGP-Router“ ([Be05], S. 327)

Dies führt dazu, dass ein BGP Router eine sehr große Routing-Tabelle verwalten muss. Günstige Router, wie sie zum Beispiel in Komplettsystemen mit Richtfunkantennen ausgeliefert werden, sind i.d.R. zu leistungsschwach dafür.

2.2.4 Multiprotocol Label Switching (MPLS)

> „Multiprotocol Label Switching ist ein Verfahren zur Kennzeichnung (Labeling) von Datenpaketen bei der Datenübertragung. Anhand des Labels wird der direkte Weg des Pakets zum Ziel nur einmal am Netzeingang bestimmt und nicht mehr an jedem Router auf dem Weg zum Adressaten. Somit wird jedes Paket ohne Umwege durchs Netz transportiert. Die Konsequenz: Daten kommen ohne Verzögerung in der richtigen Reihenfolge am Ziel an." ([Köh04], S. 84f)

Die folgenden Informationen für diesen Abschnitt stammen aus dem RFC 3031 (vgl. [RVC01]). Alle MPLS nutzenden Router eines Netzwerks heißen Label Switching Router (LSR). Die Router, die an den Grenzen zu benachbarten Netzwerken stehen, werden MPLS Edge Node oder auch Label Edge Router (LER) genannt. Ein Weg durch das MPLS-Netzwerk wird Label Switch Path (LSP) genannt. IP-Pakete, die über den gleichen LSP gesendet werden, werden gemeinsam klassifiziert in einer Forwarding Equivalence Class (FEC). Ein Label ist ein kurzer Bezeichner mit fester Länge, der verwendet wird, um eine FEC zu identifizieren. Ein Label, das einem Paket vorangestellt ist, repräsentiert die FEC der das Paket zugeordnet ist.

Label Distribution Protocol (LDP)

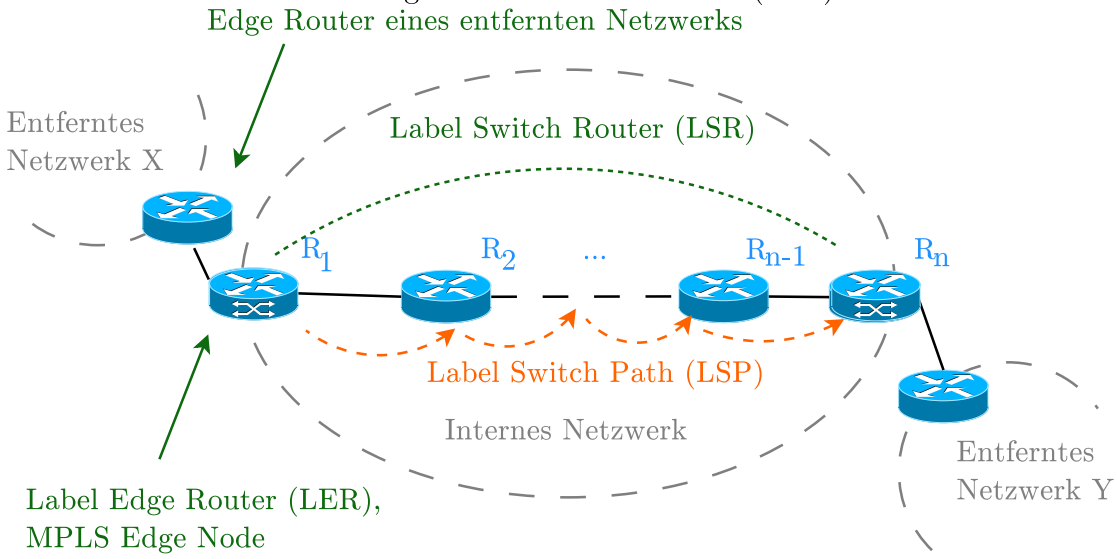
Um Label zu verteilen, wird das Label Distribution Protocol (LDP) verwendet. LDP ist eine Ansammlung von Prozessen und Nachrichten, verwendet von den LSR, die dazu dienen, die LSP durch ein Netzwerk zu errichten. Das LDP bildet dabei die Netzwerkschicht-Routing-Informationen direkt auf die Vermittlungspfade (Switch Paths) der Datenverbindungsschicht ab. In einer Tabelle, der Label Information Base (LIB), wird durch das LDP den Adressen ein Label und ein LDP Kennzeichner zugeordnet. Die Kennzeichner werden benutzt, damit ein LSR seine Nachbarn erkennt. Die LSR verteilen daher über das LDP ihre Zuordnungen von Adressen und Kennzeichnern an ihre Nachbarn. Aus diesen in der LIB gespeicherten Informationen, wird eine Forwarding Information Base (FIB), auch als Forwarding Table bezeichnet, erstellt. In dieser Tabelle ist eine Zuordnung zu finden, wohin Pakete weitergeleitet werden sollen.

Weiterhin wird das LDP von den LSR verwendet um mittels Hello-Paketen, ähnlich wie bei OSPF, Nachbarn zu finden und die eigene Bereitschaft zu signalisieren. Es gibt verschiedene Implementierungen von dem LDP. Die Informationen dieses Abschnittes können auch im RFC 5036 nachgelesen werden (vgl. [AMT07]).

Label Switch Path (LSP)

Ein Label Switch Path (LSP) für ein bestimmtes Paket ist der Weg dieses Paketes über eine Folge von Routern $R_1 \ldots R_n$. Der LSP beginnt bei einem LER, in seiner Rolle auch als LSP Ingress (R_1) bezeichnet. Er endet entweder, wenn das Ziel innerhalb des MPLS-Netzwerk erreicht ist oder bei einem LER (R_n), wenn die Paketweiterleitung nicht mehr auf Grund von MPLS getroffen wird (Abs. vgl. [RVC01]). In Abbildung 2.3) ist ein LSP dargestellt.

Abbildung 2.3: Label Switch Path (LSP)



> „Jedem IP-Paket, das über einen solchen LSP transportiert wird, werden ein oder mehrere MPLS-Protokollköpfe vorangestellt, die die Labels enthalten, die dann als Kennung für einen LSP für gewisse Zeit in Bezug auf die Wegewahl ausschlaggebend sind.“ ([Be05], S.327)

Die Wegewahl kann auf unterschiedliche Weise erfolgen, mit:

- „Hop By Hop”, dabei entscheidet jeder LSR selbst über die Wahl des nächsten Routers für die FEC
- „Explicitly Routed LSP”, hierbei entscheidet ein Router, meistens ein LER, der am Anfang oder am Ende des LSP platziert ist, über mehrere oder alle Router, über die der LSP läuft. Wenn ein einzelner Router den ganzen LSP bestimmt, wird die Bestimmung als „strictly“ explicitly routed bezeichnet, ansonsten als „loosely“ explicitly routed.

Die Router, über die der Explicitly Routed LSP verläuft kann dabei (statisch) konfiguriert werden oder aufgrund der Tabelle des oder der Router, die den LSP bestimmen. Beim Eintreffen eines Datenpaketes bei einem LSR kann dieser einen einfachen Vergleich des Label mit seiner FIB durchführen. Anschließend schickt der Router das Paket ausschließlich anhand der Informationen in der FIB weiter (Abs. vgl. [RVC01] und [AMT07]). Dieses Verfahren ist effizienter, anstatt dass ein Router selbst wieder den Weg durch das Netzwerk „Hop By Hop" bestimmen würde, wie es auch bei OSPF, dort jedoch mit Hilfe eines IP Route Lookups (longest prefix match), passiert. LSR, die nicht an dem Pfadbestimmungsprozess beteiligt sind, werden somit entlastet.

Ein Vorteil von MPLS ist die Protokollunabhängigkeit (daher auch „Multiprotocol" im Namen). MPLS kann auch auf anderen Protokollen als dem Internet Protocol aufbauen (vgl. [Köh04], S. 85).

Ein wichtiger Nachteil von MPLS ist, dass es auf freien und quelloffenen Systemen nicht weit verbreitet ist. Bei den UNIX-basierten Betriebssystemen gibt es zur Zeit nur bei OpenBSD eine mit proprietären Systemen kompatible Implementierung. Zwar sind Implementierungen auf Linux und anderen freien Betriebssystemen derzeit in Entwicklung, zur Zeit allerdings noch nicht ausgereift bzw. einsatzbereit (vgl.[Fre11, LIN11] und [Jek11]).

2.2.5 MPLS Layer 3 VPN

Ein weiterer Vorteil von MPLS ist die Möglichkeit, Schicht 3 VPNs zu erstellen.

Ein Virtuelles Privates Netzwerk (VPN)

> „ist ein geschlossenes logisches Netzwerk zur sicheren Datenübertragung über öffentlich zugängliche Übertragungsnetzwerke" ([HPR+06], S. 269).
>
> „Ein wesentliches Ziel von virtuellen Netzen ist es, firmeninterne private und somit nicht global bekannte Adressen erreichen zu können." ([Be05], S. 126)

Eine Abgrenzung von MPLS-VPNs zu VPNs, bei denen Sicherheit und Verschlüsselung eine zentrale Rolle spielen, kann wie folgt beschrieben werden:

> "Hierbei hat der Begriff VPN jedoch nicht den Charakter eines durch Kryptographie geschützten VPNs, sondern bezieht sich darauf, dass mit MPLS Netzteile transparent verbunden werden können. So entsteht ein virtuelles Netz, das letztendlich aber auf Basis des Netzes von einem oder mehreren MPLS-Netzbetreibern basiert." ([Be05], S. 329)

Weiterhin werden i.d.R. MPLS Layer 3 VPNs eingesetzt, um den Nutzern ein eigenes IP-Netzwerk bereit zu stellen, auf das Dritte keinen Zugriff haben (vgl. [Be05], S. 127f).

> „Bei einem MPLS-VPN werden die durch den Netzbetreiber bereitgestellten Verbindungen abgegrenzt, so dass kein Kunde Zugriff auf Adressen oder Verbindungen anderer Kunden hat. Somit ist das 'privat' von VPN hier nicht auf den Schutz von Vertraulichkeit gerichtet, sondern auf die Abgrenzung der Netzwerkteilnehmer. “ ([Be05], S. 127)

Um zu gewährleisten, dass die Daten der Endnutzer voneinander getrennt sind, werden verschiedene „forwarding“ Tabellen verwendet, in denen die Weiterleitung der Pakete der Endnutzer verwaltet werden. Somit können mehrere Routingtabellen unabhängig voneinander operieren. Diese Methode wird auch Virtual bzw. VPN Routing & Forwarding (VRF) genannt (vgl. [RR06], [Jek11], S. 3).

Um die Label von verschiedenen MPLS-Tabellen zu verbreiten kann das LDP oder BGP eingesetzt werden. (vgl. [Jek11], S. 3)

2.3 Datensicherungsschicht (Schicht 2)

Der Transport auf Schicht 3 über das Internet Protokoll setzt voraus, dass Netzwerkgeräte innerhalb von Netzwerksegmenten logisch miteinander kommunizieren können. So ein Netzwerksegment entspricht auf Schicht 3 i.d.R einem Teilnetzwerk.

Die Datensicherungsschicht (engl. Link Layer oder Layer 2) ist „zuständig für den unverfälschten Datentransport über einen einzelnen Übermittlungsabschnitt“ ([HPR+06], S. 258). Sie leistet damit diese logische Verbindung. Auf Schicht 2 gibt es wiederum verschiedene standardisierte Protokolle. Hierzu zählen Token Ring, Fiber Distributed Data Interface (FDDI) und Ethernet. Das heutzutage mit Abstand wichtigste Protokoll auf Schicht 2 ist Ethernet. In dieser Arbeit wird nur Ethernet basierte Technologie genutzt. Die anderen Protokolle werden aus diesem Grund nicht behandelt.

2.3.1 Ethernet

> „Ist die Bezeichnung für eine serielle Datenübertragung zwischen mehreren Teilnehmern, die an einem gemeinsam genutzten Medium über Netzwerkkarten angeschlossen sind.” ([HPR+06], S. 261)
>
> „Die Datenübertragung erfolgt dabei im Rahmenformat (Frames).” (ebd.)

Zur Identifikation wird auf der Datensicherungsschicht die Media Access Control (MAC)-Adresse verwendet (vgl. [HPR+06], S. 251).

„Diese Adresse wird der Netzwerkkarte des Rechners in Form einer 48 Bit großen Zahl zugeordnet." (ebd.)

Zur Verbindung von mehreren Netzwerkteilnehmern kommen Switches oder auch Multiport Bridges zum Einsatz. Ein Schicht 2 Switch ist im Grunde eine „Multiport Transparent Bridge", wobei jede Netzwerkschnittstelle des Switches ein eigenes, von den anderen isoliertes LAN-Segment darstellt. Dabei schaltet der Switch die Datenverbindung zwischen den Netzwerkschnittstellen durch. Die Frame Weiterleitung basiert ausschließlich auf den MAC-Adressen, die in jedem Frame enthalten sind (Abs. vgl. [Huc10], S. 20 und [HPR+06], S. 268).

Diese Geräte führen Forwarding-Adresstabellen. In diesen Tabellen werden die MAC-Adressen und die Port-Nummern von den Netzwerkteilnehmern, die den entsprechenden Frame gesendet haben, gespeichert. Somit ist eine Zuordnung und Identifikation zwischen den Ports des Switches und den Endgeräten möglich (Abs. vgl. [Be05], S.142 und [Sch06], S. 267ff sowie [HPR+06], S. 268).

Auf Schicht 2 des OSI-Modells können durch redundante Wege Schleifen entstehen. Durch diese Schleifen tritt ein kontinuierliches Zirkulieren der gesendeten Daten auf, die wiederum die Konnektivität negativ beeinflussen können (vgl. [Har12], S. 57).

2.3.2 Virtuelle LANs (VLANs)

„Switches sind oft in der Lage, ihre LAN-Ports zu verschiedenen Gruppen zusammenzufassen. Damit lassen sich die dort angeschlossenen Geräte in sogenannte Virtuelle LANs (VLANs) gruppieren". ([Be05], S. 144)

Ein VLAN stellt dabei ein eigenes Schicht 2 Segment dar.

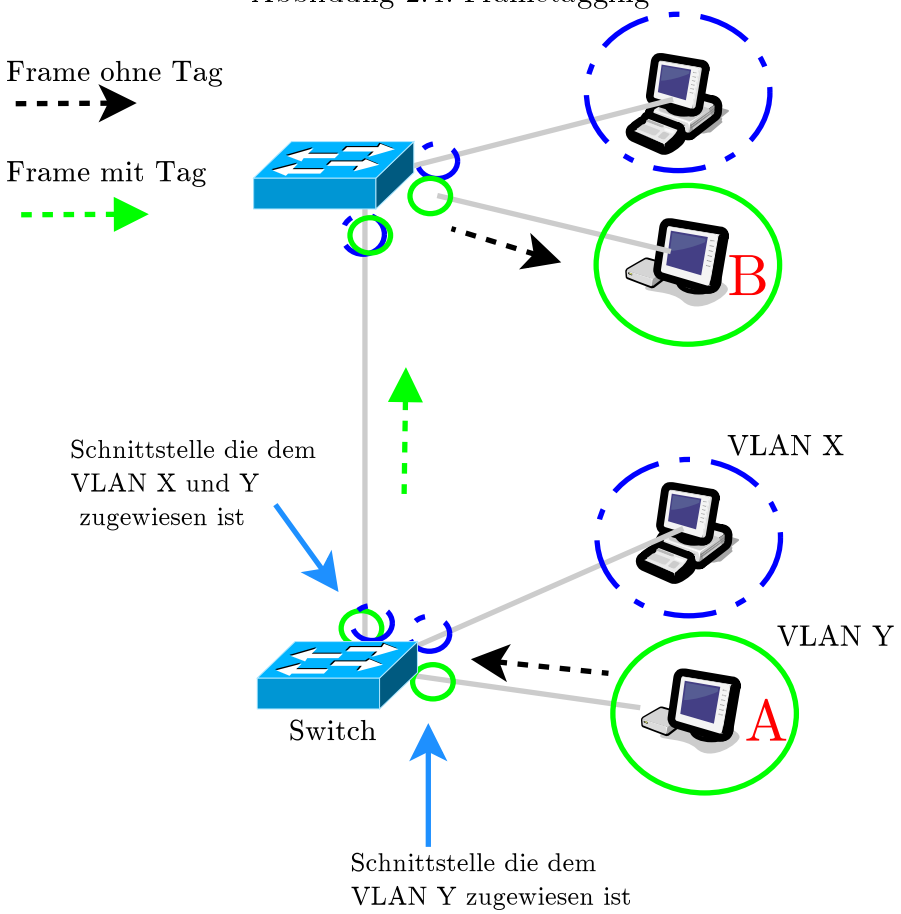
Abbildung 2.4 veranschaulicht die Funktionsweise von VLANs.

Hierbei stellt der mit A gekennzeichnete Computer den Sender eines Frames dar und der mit B markierte Computer entspricht dem Empfänger. Beide befinden sich für die Switches im gleichem VLAN.

Die kleinen Kreise stellen die Ports des Switches dar, welche einer oder mehreren VLAN-Gruppen zugeordnet sind. Die großen Kreise stellen die VLAN-Gruppen dar. Die verschiedenen Farben und Stricharten symbolisieren verschiedene VLANs. Es wird deutlich, dass nur Frames ohne Tag bei dem Endgerät ankommen.

Die Ports der Switches sind also verschiedenen VLAN-Gruppen zugeordnet. Die Frames zwischen VLAN-Switches bekommen hierfür eine eigene Markierung, genannt VLAN-Tag (abk. Tag). Bei Ankunft eines neuen Frames überprüft der Switch, ob ein Tag zu einer VLAN-Gruppe passt. Bei einer Übermittlung an mehrere Netzwerkteilnehmer leitet der Switch den Frame entsprechend seiner Gruppe an den oder die zur VLAN-Gruppe zugehörigen Ports weiter. Befindet sich hinter einem

Abbildung 2.4: Frametagging



Port ein Netzwerkteilnehmer bzw. eine „Endstelle", für den das Paket bestimmt ist, so wird der VLAN-Tag wieder entfernt, bevor der Frame weitergeleitet wird (Abs. vgl. [Sch07], S. 131ff).

Mitglieder verschiedener VLAN-Gruppen sind also auf Layer 2 getrennt, dass bedeutet, sie können insbesondere nicht ohne Weiteres miteinander kommunizieren. So werden auch Broadcast Frames nur innerhalb eines VLANs verbreitet, d.h. jedes VLAN bildet eine separate Broadcast Domäne.

2.3.3 Spanning Tree Protocol (STP)

Das Spanning Tree Protococol (STP) basiert auf dem Spanning Tree Algorithmus (vgl. [Com07], S. 375).

Es wurde entwickelt, um die in Abschnitt 2.3.1 angesprochenen Probleme (Schleifen) von redundanten Strukturen auf Schicht 2 des OSI-Modells zu vermeiden.

> „Es soll vermeiden, dass Datenpakete in einem geswitchten LAN auf redundante Wege oder in Loops geschickt werden. Basis einer Spanning-Tree-Topologie ist die sogenannte Root Bridge, von der aus die Pfade definiert werden, über die die weiteren Bridges im Netzwerk erreichbar

> sind. Jede Bridge soll nur über einen einzigen Pfad anzusprechen sein, eventuell vorhandene zusätzliche Ports werden daher deaktiviert. Gewählt wird der jeweils kostengünstigste Pfad. Die Root Bridge und die ihr hierarchisch unterstellten Designated Bridges signalisieren einander permanent ihre Verfügbarkeit. Entfällt das Signal, hat sich die Topologie geändert und der Spanning Tree muss sich neu organisieren“ ([Com07], S. 375)

Diese Vermeidung von Schleifen ist in einem Netzwerk mit redundanten Verbindungen essenziell, da ein ständiges Zirkulieren der Frames zum Einbruch der Verbindungen führen kann.

Zu erwähnen ist noch, dass es inzwischen verbesserte Verfahren als das ursprüngliche STP gibt. Diese sind Rapid Spanning Tree Protocol (RSTP), Per-VLAN Spanning Tree (PVST) und Multiple Spanning Tree Protocol (MSTP).

Einer der Hauptkritikpunkte an STP ist, dass es bei dem Ausfall einer Verbindung vergleichsweise sehr lange braucht, bis sich der Spannbaum neu berechnet hat. Dies kann bis zu 30 Sekunden dauern. Um diese Problematik zu beheben, wurde RSTP entwickelt (vgl. [Huc10], S. 143).

Um RSTP zusammen mit VLANs einzusetzen, wurden MSTP und PVST bzw. PVST+ entwickelt.

> „Das Multiple Spanning Tree Protocol (MSTP) ist eine Erweiterung des RSTPs. Es ermöglicht im Zusammenhang mit Virtual Local Area Network (VLAN)s verschiedene Instanzen des Spannbaums. Für ein VLAN oder eine Gruppe von VLANs können also voneinander unabhängige STP-Instanzen gebildet werden, die innerhalb eines LANs jeweils eigene unterschiedliche Spannbäume nutzen.“ (ebd.)

PVST arbeitet mit separaten Instanzen von STP auf den verschiedenen VLANs. Dies erlaubt es STP auf jedem VLAN unabhängig zu konfigurieren. Wenn einzelne redundante Verbindungen verschiedenen VLANs zugeordnet sind, ist es mit PVST möglich, diese gleichsam zu benutzen und eine Lastbalancierung zu erreichen (vgl. [Huc10], S. 147). PVST+ basiert auf RSTP anstelle von STP.

Zur Verteilung von Konfigurationen versendet STP sogenannte Bridge Protocol Data Unit (BPDU). Bei PVST werden pro VLAN BPDU's versendet, bei MSTP nur insgesamt eine BPDU.

RSTP, MSTP und insbesondere PVST/PVST+, da es proprietär von Cisco ist, werden allerdings nicht von jeder Hardware und jedem Betriebssystemen unterstützt.

2.4 Bitübertragungsschicht (Schicht 1)

Auf der Bitübertragungsschicht werden die physikalischen Eigenschaften der Übertragungsstrecke spezifiziert.

Als Übertragungsmedium kommt Licht, Strom, elektrische Felder (Funk) oder akustische Übertragung (vgl. Modems) in Frage.

Die Übertragung mittels Funkwellen ist die einzige in dieser Arbeit behandelte Schicht 1 Technologie. Sie wird im nächsten Kapitel behandelt. Daher wird hier nicht näher auf die Bitübertragungsschicht eingegangen.

3 Grundlagen der Richtfunktechnik

Die bisherigen Grundlagen handelten von der Vermittlung von Daten in Computer-Netzwerken. Wie und womit die Daten physikalisch in der Luft bzw. im Freiraum mit der WLAN-Technologie übertragen werden, wird im Folgenden erläutert. Dargestellt ist dies auf OSI-Layer 1 der Bitübertragungsschicht.

Wireless Local Area Network (WLAN) ist eine Technologie, die dafür gedacht ist, Geräten in einem kleinen Umfeld (typischerweise <100m entfernt von dem Accesspoint, welcher das Funknetzwerk zur Verfügung stellt) per Funk Netzwerkkonnektivität zur Verfügung zu stellen. Um mit WLAN große Distanzen zu überbrücken, kann auf Richtfunk zurückgegriffen werden.

Richtfunk (Microwave radio systems) bezeichnet eine Funkstrecke zwischen zwei festen Punkten, deren elektromagnetische Energie gebündelt im Freiraum übertragen wird (vgl. [HPR+06], S. 312 und [DKe81], Band 18, S. 250).

> „Unter Richtfunkverbindungen versteht man Systeme zur drahtlosen Nachrichtenübertragung, bei denen Frequenzen von mehr als dreißig Megahertz als Nachrichtenträger benutzt werden. Die verfügbare Sendeleistung wird durch Richtantennen für Senden und Empfang in einer Vorzugsrichtung stark gebündelt.
>
> Zum Überbrücken großer Entfernungen werden Zwischenstellen als Verstärker eingesetzt.“ ([Car72], S. 9)

In diesem Kapitel wird zunächst auf die Wellenausbreitung (Unterabschnitt 3.1), insbesondere Funkfelddämpfung, die Bedeutung von freier beziehungsweise behinderter Sicht und danach auf Auswirkungen der Umgebung eingegangen. Abschließend für dieses Kapitel werden aktuelle Standards bei der Richtfunktechnik behandelt (Unterabschnitt 3.2).

3.1 Wellenausbreitung

> „Die Ausbreitung einer elektromagnetischen Raumwelle im erdnahen Raum hängt einerseits von der verwendeten Frequenz bzw. Wellenlänge und andererseits von der Leitfähigkeit der Erdoberfläche sowie verschiedenen physikalischen Erscheinungen in der Atmosphäre ab.” ([Wei02], S. 391)

Die Ausbreitung der elektromagnetischen Wellen wird durch mehrere Faktoren beeinflusst. Freie Sicht- und Ausbreitungsverhältnisse sind für die Richtfunkübertragung wichtig. Auf langen Strecken muss zudem die Krümmung der Erdoberfläche berücksichtigt werden.

> „Die Annahme einer ebenen, ungekrümmten Erde entspricht nur in Ausnahmefällen den tatsächlichen Verhältnissen, im allgemeinen müssen bei jeder Streckenuntersuchung die Erdkrümmung und die Hindernisse der Ausbreitungsrichtung berücksichtigt werden.“ ([Car72], S. 45)

Eine Dämpfung „Verringerung der Amplitude” (nach [DB86], S. 84) kann durch eine behinderte (also nicht freie) Funkstrecke zustande kommen. Aus diesem Grund sollte der Bereich zwischen Sender und Empfänger, insbesondere in der sogenannten 1. Fresnelzone (siehe Abschnitt 3.1.2), frei sein.

Weiterhin gibt es auch nicht offensichtliche Faktoren, wie beispielsweise Wettereinwirkungen (Niederschlag, Luftdichte, siehe Unterabschnitt 3.1.3), welche eine Dämpfung oder andere „Schwunderscheinungen”, d.h. Schwankungen der Empfangsfeldstärke, zur Folge haben können (vgl. [Don74], S. 42). Reflexionen an einem Medium, wie der Erdoberfläche oder dem Wasser, können ebenfalls solche Effekte, aber auch „Überreichweiten” (vgl ebd.) zur Folge haben.

3.1.1 Dämpfung

> „Bei geringer Dämpfung lassen sich längere Distanzen überbrücken. Die Dämpfung ist sehr stark von der übertragenen Frequenz abhängig. Geringere Dämpfung ergibt auch ein höheres Signal-Rausch-Verhältnis, das zu einer niedrigeren Bitfehlerrate führt und/oder den Einsatz einfacherer Empfänger ermöglicht.“ ([Ste04], S. 53)

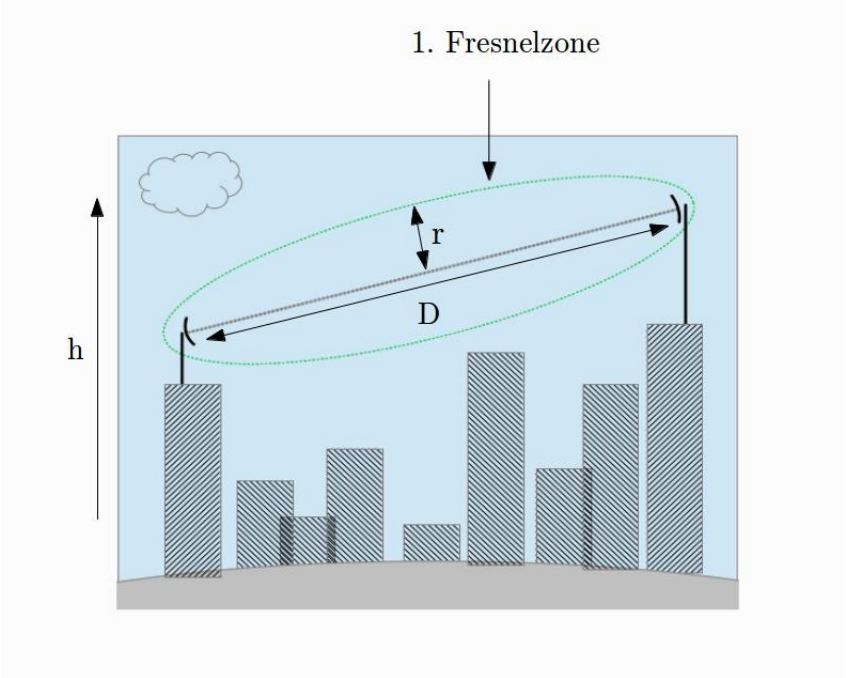
Als praktische Näherungsformel für den Paket- bzw. Pfadverlust kann folgende Formel nach [Güt13], S. 18 benutzt werden.

> „$L \,/\, \mathrm{dB} = 32,44[/\,\mathrm{dB}] + 20\lg(f \,/\, \mathrm{MHz}) + 20\lg(R \,/\, \mathrm{km})$“
>
> f: Frequenz [MHz]
>
> R: Distanz zwischen Sende- und Empfangsantenne [km]
>
> L: Pfadverlust [dB]
>
> 32,44: Konstante für die Ausbreitung im erdnahen, freien Raum [dB]

3.1.2 Bedeutung der 1. Fresnelzone

Für eine reflexionsfreie Übertragung ist eine freie Sicht zwischen den Antennen wichtig. Der Bereich, in dem sich der Hauptteil der Energie überträgt, wird 1. Fresnelzone genannt. Sie bildet dabei eine „Ellipse günstiger Reflexionen“ ([Car72], S. 42) zwischen zwei Richtfunkantennen ab (vgl. [Don74], S. 32). Abbildung 3.1 veranschaulicht die 1. Fresnelzone.

Abbildung 3.1: 1. Fresnelzone



Der Buchstabe D steht für die Distanz und der Buchstabe h für die Höhe und r steht für den Radius.

> „Ist die Sichtlinie ungestört oder sogar die erste Fresnelzone hindernisfrei, so ist von der Geländebeschaffenheit keine zusätzliche Dämpfung zu erwarten.“ ([Car72], S. 45)

Da die 1. Fresnelzone „ein Ellipsoid mit den Antennen als Brennpunkte” ([HPR+06], S. 312) skizziert, lässt sich der maximale Radius eines Querschnittes in der Mitte zwischen Sende- und Empfangsantenne mit folgender Formel bestimmen:

$$r = 0,5 \cdot \sqrt{\lambda \cdot \mathrm{D}}$$

λ: Wellenlänge

D: Distanz zwischen Sende- und Empfangsantenne

r: Radius (nach [HPR+06] auch mit B bezeichnet)

3.1.3 Störungsquellen

An der Empfangsantenne kann die Empfangsfeldstärke stark variieren (Schwund). Solche Schwunderscheinungen können durch Brechung des Strahls an Oberflächen, Höhendifferenzen, in denen der Strahl durch verschiedene Luftschichten muss, die verschiedene Reflexionseigenschaften besitzen, und Wettereinwirkungen, wie starkem Regen oder Schneefall, erzeugt werden.

„Bei Mehrwegausbreitung durch Reflexion am Boden oder an Luftschichten verschiedener Dichte oder durch Beugung des Strahls an Wasser oder Staubwolken entstehen Interferenzen zwischen den verschiedenen Wellen, die den Empfänger mit Zeit- oder Wegdifferenzen, auf jeden Fall mit Phasenverschiebungen erreichen.“ ([Car72], S. 50)

3.2 Standards

Bis zum Jahr 1998 war das Bundesministerium für Post und Telekommunikation (BMPT) in Deutschland für die Festlegung der Standards von lizenzfreien Richtfunksystemen zuständig. Das BMPT legte fest, dass bestimmte Funktechniken und Frequenzen frei, d.h. ohne Genehmigungen nutzbar sind (vgl. [Mül13] Unterabschnitt „Gesetzliche Bestimmungen für FunkLAN“ und [Wik13] Abschnitt „Bundesministerium für Post und Telekommunikation“ (abgerufen am 27.02.2013)).

„Das Betreiben von Datenfunksystemen ist durch das Amtsblatt 14/1997 des BMPT ohne jede Einschränkung durch Grenzen eines Grundstücks erlaubt. Somit ist die grundstücksübergreifende Datenübertragung genehmigt.“ ([Mül13], Unterabschnitt „Gültigkeitsbereich für WLAN nach IEEE 802.11ac/a/b/g/n“)

Die Aufgaben in Bezug auf Richtfunksysteme, Standards und nutzbare Frequenzbereiche sind von dem BMPT auf die Bundesnetzagentur übergegangen (Abs. vgl. [Wik13] Abschnitt „Bundesnetzagentur“ und [Wik13] Abschnitt „Bundesministerium für Post und Telekommunikation“ (beide abgerufen am 27.02.2013)).

Nachfolgend werden die Standards im Funkbetrieb und im kabellosen, lokalen Netzwerk erläutert.

3.2.1 IEEE 802.11n

Das Institute of Electrical and Electronics Engineers (IEEE) verabschiedet mit einer Arbeitsgruppe Standards zur Verwendung von drahtlosen Netzwerken. 802.11 beschreibt den „physikalischen Transport der digitalen Informationen“ (vgl. [HPR+06], S. 258), der auf der Bitübertragungsschicht angesiedelt ist.

Funksysteme nach 802.11 können ohne Nutzungsgebühr und lizenzfrei betrieben werden.

„WLAN Systeme nach IEEE 802.11 sind anmelde- und gebührenfrei.“
([Mül13], Unterabschnitt „Gültigkeitsbereich für WLAN nach IEEE 802.11ac/a/b/g/n“)

IEEE 802.11n beschreibt einen Standard für WLAN.

„IEEE 802.11n ist die Spezifikation für ein WLAN mit Übertragungsraten von 150, 300, 450 und 600 MBit/s.“ ([Kom13] Unterabschnitt „IEEE 802.11n / WLAN mit 100 MBit/s“(abgerufen am 27.02.2013))

„Erreicht werden diese Geschwindigkeiten mit mehreren Antennen und Signalverarbeitungseinheiten (MIMO), die Verdopplung der Funkkanal-Bandbreite auf 40 MHz, sowie die parallele Nutzung des 2,4- und 5-GHz-Frequenzbandes.“ (ebd.)

3.2.2 Frequenzen

„Richtfunksysteme arbeiten bei Frequenzen oberhalb 300 MHz, vorzugsweise oberhalb 1 GHz.“ ([Don74], S. 11)

Für den lizenzfreien Richtfunk mit dem Standard IEEE 802.11n, kommen in Deutschland Frequenzen im Bereich 2,4 bis 2,4835, im Bereich 5,15 bis 5,35 und 5,47 bis 5,725 in Frage. (vgl. [Kom13] Unterabschnitt „IEEE 802.11n / WLAN mit 100 MBit/s“ (abgerufen am 27.02.2013))

„IEEE 802.11n beherrscht sowohl das 2,4-GHz- wie auch das 5-GHz-Band. Das bedeutet, es stehen zwei Frequenzbänder zur Verfügung“ ([Kom13] Unterabschnitt „IEEE 802.11n / WLAN mit 100 MBit/s“ (abgerufen am 27.02.2013))

Die Nutzung der 5 GHz-Frequenz hat den Vorteil, dass Störungen durch andere Funknetze und Hindernisse verringert werden. Außerdem sind kleinere Antennen nutzbar, als es bei Frequenzen mit 2,4 GHz möglich wäre (vgl. ebd. und vgl. [Kap09]).

„Im 5-GHz-Band sind 19 verschiedene nicht überlappende Kanäle mit jeweils 20 MHz Kanalbreite nutzbar.“ ([Kom13] Unterabschnitt „IEEE 802.11n / WLAN mit 100 MBit/s“ (abgerufen am 27.02.2013))

3.2.3 Multiple Input Multiple Output (MIMO)

„MIMO sieht vor, mehrere Sende- und Empfangsantennen zu verwenden. [...] Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was zur Steigerung der Übertragungsrate durch Spatial Multiplexing genutzt werden kann. Dabei werden mehrere Datenströme parallel in einem Funkkanal übertragen. Die parallele Signalverarbeitung bringt verbesserten Signalempfang und vermindert die Nachteile durch Mehrwegeempfang, der durch reflektierte Signale entsteht. Insgesamt verbessert sich die Leistung des ganzen Funksystems durch MIMO erheblich.“ (ebd.)

Mit dieser Technik ist es möglich, Bruttodatenraten bis zu 600 Mbit/s zu erreichen (vgl. [Tre10], S. 95). Die Funktionsweise lässt sich folgendermaßen beschreiben:

> „Die signalverarbeitende Empfangseinheit bekommt durch mehrere Funksignale eine räumliche Information. Denn bei zwei Antennen trifft das selbe Funksignal aus zwei verschiedenen Richtungen beim Empfänger ein. Jedes eingehende Funksignal weist in der Regel einen eigenen 'räumlichen Fingerabdruck' auf, der auch 'Spatial Signature' genannt wird. Der Empfänger setzt die Signale wieder passend zusammen. Dadurch verbessert sich die Leistung des ganzen Funksystems erheblich." ([Kom13] Unterabschnitt „MIMO - Multiple Input Multiple Output" (abgerufen am 27.02.2013))

Diese Technik ist mit Richtfunkantennen so nicht möglich, da die Signale immer aus einer Richtung kommen. Indem eine zweifache Polarisation (Dual Polarity) verwendet wird, kann aber das gleiche Ergebnis erzielt werden. Dabei werden die Signale in horizontaler und vertikaler Polarisation versendet.

3.2.4 Antennen

Allgemein ist für eine Richtfunkantenne bezeichnend, dass sie die meiste Energie in eine Richtung sendet. Als Vergleichswert wird hierzu ein isotroper Strahler verwendet. Diese isotropen Strahler lassen sich allerdings nicht herstellen (Abs. vgl. [Don74], S. 28).

> „Im Idealfall strahlt ein isotroper Strahler mit gleicher Intensität in alle Richtungen. Wenn durch irgendwelche Maßnahmen die Intensität in einer Vorzugsrichtung höher ist als in den übrigen Richtungen, sprechen wir von Richtantennen oder Antennen mit Richtwirkung." ([DB86], S 126)

Für den Richtfunk kommen verschiedene Antennen in Frage.

> „Für Richtfunksysteme haben sich zwei Antennenarten durchgesetzt: Dipolgruppenantennen für den Bereich unterhalb 1 GHz und Parabolantennen für Frequenzen oberhalb 1 GHz." ([Don74], S. 101)

Die auch für den 5 GHz-Bereich nutzbaren Parabolantennen werden umgangssprachlich auch Antennenschüssel oder Satellitenschüssel genannt (vgl. [Wik13] Abschnitt „Parabolantenne" (abgerufen am 27.02.2013)). Im Anhang (vgl. Abbildung 8.1) sind solche Antennen abgebildet. Nach Empfang der Funkwellen müssen diese Daten noch in das Computernetzwerk gelangen. Für diesen Zweck gibt es Komplettsysteme, bestehend aus Antenne und Router.

Außerdem gibt es die Möglichkeit, Antennen einzeln zu beziehen. So ist es denkbar, eigene oder andere Router und bei Bedarf Power over Ethernet (PoE) Adapter zu verwenden.

Für den lizenzfreien Richtfunk gelten die behandelten Frequenzen (vgl. Unterabschnitt 3.2.2). Zusätzlich ist eine Unterstützung des „802.11n" Standards angestrebt. Dieser ermöglicht, wie angesprochen, die Technik MIMO (vgl. Unterabschnitt 3.2.3) und damit schnelle Datenraten.

4 Szenario Wissenschaftsladen Dortmund

Teile der nachfolgenden Informationen wurden durch mündlichen und schriftlichen Austausch mit Aktiven des Wissenschaftsladen Dortmund sowie durch Recherche zusammengetragen.

Wie bereits in der Einleitung erwähnt bemüht sich der Wissenschaftsladen Dortmund insb. mit seinem Vernetzungsprojekt FREE! um die Förderung des „freien und unzensierten Informationsaustauschs für interessierte Individuen und Gruppen" ([Lie09]). Um diese Ziele zu erreichen wurden im WiLaDo seit 1991 mit Computern und Vernetzungstechnik Versuche angestellt und Infrastruktur zur Teilnahme an Computer-Netzwerken und der Verbreitung von Informationen selbstorganisiert aufgebaut und betrieben, sowie auch anderen Interessierten zur Verfügung gestellt (vgl. [Nor12]). Die dabei gemachten Erfahrungen werden entsprechend einem Grundprinzip von Wissenschaftsläden - nämlich der „Hilfe zur Selbsthilfe" - weitergegeben. So soll das im Folgenden vorgestellte Szenario auch als Prototyp für weitere Einsatzgebiete dienen. Die unterschiedlichen Einsatzgebiete, in denen solche selbstverwalteten Netzwerke zum Einsatz kommen können, haben verschiedene Anforderungen. Um die unterschiedlichen Anforderungen der Einsatzgebiete nicht im Vorfeld zu stark einzuschränken, ist das Hauptziel der angestrebten Lösung ein flexibel einsetzbares Netzwerk. Neue Anforderungen sollen zudem in das vorliegende Szenario, auch zu einem späteren Zeitpunk, noch einfließen können.

Die für den Wissenschaftsladen bisher identifizierten Ziele werden anhand der Richtfunkverbindungen, wie sie in Abbildung 4.1 dargestellt sind, erläutert. Hierbei ist es von essenzieller Bedeutung, dass es ein Konzept gibt, nach dem aus den einzelnen Richtfunkverbindungen ein zusammenhängendes Netzwerk gebildet wird.

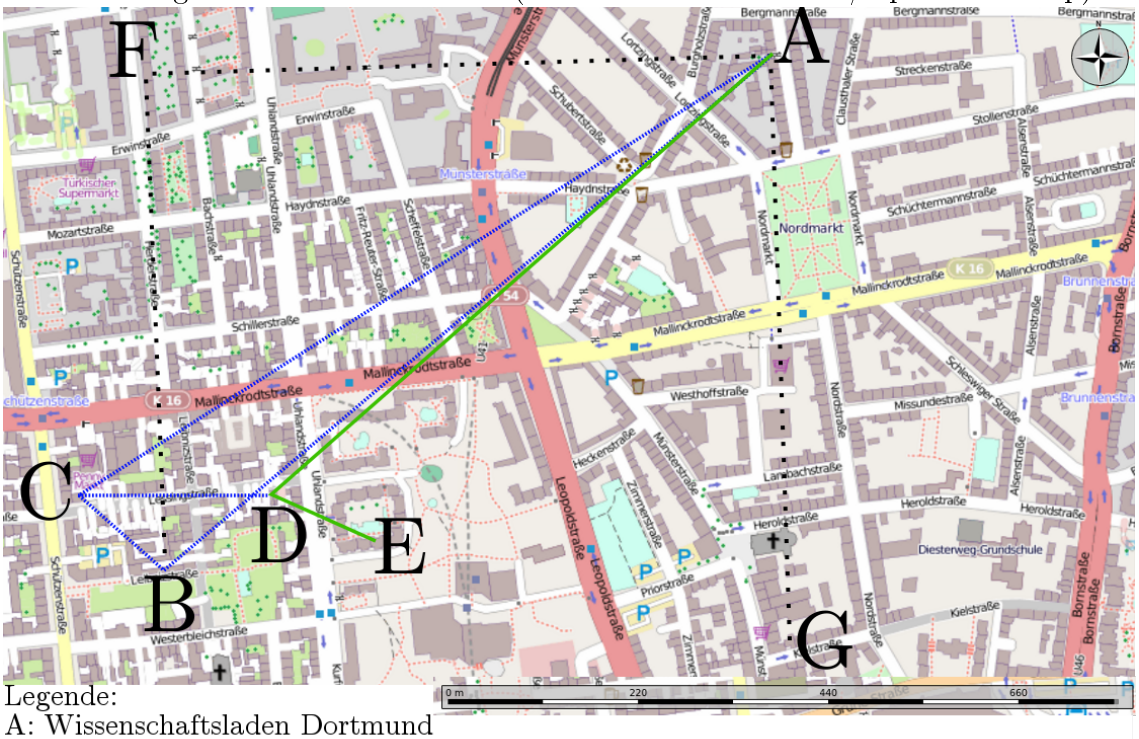
Eine geplante Art der Nutzung des Netzwerks ist die direkte Anbindung von Individuen oder Gruppen an das Netzwerk des Wissenschaftsladens und damit auch an das Internet. Diese Art der Nutzung wird in der Abbildung 4.1 durch die Zwischen- oder Endstellen C, D, E, F und G dargestellt.

Der andere identifizierte Verwendungszweck des Netzwerks besteht darin, über Punkt B einen weiteren Zugang zum Internet für den Wissenschaftsladen zu erhalten. Die Zwischenstellen C und F bekommen hier zusätzliche Bedeutung, da durch diese Punkte auch Redundanz und damit Ausfallsicherheit erzeugt wird.

Diese beiden Arten der Nutzung des Netzwerks unterscheiden sich stark in den Anforderungen, die an das Netzwerk gestellt werden. Diese Anforderungen werden in den nachfolgenden Unterabschnitten behandelt.

Eine dritte Nutzungsart des Netzwerks ist eine Anbindung von WLAN Ad-hoc Netzwerken an das Richtfunknetzwerk. WLAN Ad-hoc Netzwerke ermöglichen es, weiteren Menschen an dem Netzwerk des Wissenschaftsladen sowie dem Internet

Abbildung 4.1: Richtfunkstrecken (Kartenmaterial: Marble/OpenStreetMap)



teilzuhaben, vor allem solchen Menschen, die nicht die Möglichkeit haben, sich über Dachantennen und Hausverkabelung direkt an das Richtfunknetz anzuschließen. Zu diesem Zweck kann an einem Richtfunkstandort zusätzlich zu der bzw. den Richtfunkantennen auch ein Rundstrahler oder ggf. Sektorantennen aufgebaut und an einen speziellen Router angeschlossen werden. Auf den genauen Aufbau dieser Netze einzugehen, würde den Rahmen dieser Arbeit sprengen. Für die Planung des Netzwerks muss dennoch folgendes berücksichtigt werden: Ein relevantes Auswahlkriterium von geeigneten Netzwerktechnologien ist ihre Fähigkeit zu skalieren. Wenn in einem Netzwerk auch Ad-Hoc Netzwerke betrieben werden, kann diese Skalierungsgrenze schnell erreicht werden.

Um sämtliche Anforderungen zu gewährleisten, müssen zunächst die physikalischen und personellen Gegebenheiten berücksichtigt werden: Damit die Antennen auf den Dächern platziert werden können, müssen die Hausbesitzer der Montage zustimmen. Zusätzlich müssen Termine gefunden werden, an denen die Wetterlage ausreichend günstig ist und eine eventuelle Beaufsichtigung der Anbringung der Antennen, durch die Hausbesitzer, gewährleistet werden kann.

In der Dortmunder Nordstadt stellen Hindernisse eine Herausforderung für die reflexionsfreie Richtfunkverbindung dar. Zwischen den Punkten A (Wissenschaftsladen) zu den Punkten B, C und D ragen Gebäude oder Bäume in die erste Fresnelzone oder in die direkte Sichtlinie der Verbindungen. Da sich in diesem Bereich der Hauptteil der Energie überträgt, kann es wegen solcher Hindernisse zu Datenverlusten oder Ausfall der Verbindungen kommen (vgl. Abschnitt 3.1.2). In dem Fall von Punkt A nach E ist die Beeinträchtigung dermaßen groß, dass auf eine direkte Verbindung verzichtet wird und stattdessen D als Relaistation verwendet wird.

Eine weitere Problematik ist die Wetterlage. Bei Regen oder Schneefall können die gleichen Effekte auftreten, diese sind aber schwer vorhersehbar (vgl. Abschnitt 3.1.3).

4.1 Aspekt: Zusätzliche Anbindung an das Internet

In diesem Abschnitt geht es um die Nutzungsart des Funknetzwerks als Verbindung zwischen verschiedenen Teilnetzwerken des Internets. Dies bedingt auf den Vermittlungseinrichtungen eine große Anzahl von Pfadeinträgen zu Zielen im Internet und das Border Gateway Protocol. Außerdem muss aufgrund des Serverbetriebs seitens des Wissenschaftsladen Dortmund eine hohe Verfügbarkeit gewährleistet sein.

Für die zusätzliche Anbindung an das Internet sind folgende Anforderungen zu erfüllen: Damit die Dienste, die vom WiLaDo zur Verfügung gestellt werden und die sich im Internet befindenden entfernten Netzwerke dauerhaft erreichbar sind, muss das Netzwerk eine hohe Verfügbarkeit der Verbindungen gewährleisten. Eine mögliche Struktur kann mit redundanten Pfaden arbeiten.

Die Netzwerke oder Teilnetzwerke, die als Zusammenschluss das Internet ergeben, werden als Autonome Systeme (AS) bezeichnet. Um zu diesen Autonomen Systemen Verbindungen aufzubauen und Routen auszutauschen, werden an den Knotenpunkten sogenannte Edge-Router eingesetzt. Damit die Edge-Router untereinander kommunizieren können, bedarf es eines gemeinsam genutzten Protokolls, einem Exterior Gateway Protocol (EGP). Im Internet hat sich das Border Gateway Protocol (BGP) etabliert (vgl. Abschnitt 2.2.3).

Für die eigene Anbindung an andere Autonome Systeme sind also Router, auf denen BGP implementiert und konfiguriert ist, Voraussetzung.

Die Edge-Router benutzen untereinander external BGP (eBGP). Die Router, die keine direkte Verbindung zu einem anderen Autonomen System haben, aber auf dem Weg innerhalb eines AS liegen, werden mit (internal BGP) iBGP betrieben und verteilen die Routen, die über eBGP gelernt wurden, innerhalb des AS (vgl. Abschnitt 2.2.3).

Wie auch in Abschnitt 2.2.3 beschrieben, beinhalten die Internetroutingtabellen derzeit eine große Anzahl an Pfaden (vgl. [BSH13]). Längst nicht alle Router eignen sich, um diese großen Tabellen verwalten zu können.

Grundsätzlich können Routen statisch vom Administrator eingetragen werden. Der administrative Aufwand steigt allerdings mit der Größe des Netzwerks. Bei Verbindungen im Internet sind statische Routen auch deshalb keine Möglichkeit, da sich die Pfade häufig ändern. Bei der sehr großen Anzahl der Routen in das Internet sind diese Änderungen mit statischen Routen nicht zu handhaben. Diese Änderungen betreffen zudem entfernte Netzwerke und liegen daher nicht in dem Verantwortungsbereich von lokalen Administratoren. Schlussendlich müssen die BGP-Routen intern auch weiter verbreitet werden, aus den ausgeführten Gründen ist dies jedoch ebenso nicht möglich.

Es kann also festgehalten werden, dass ein auf Schicht 3 mit dynamischen Routen gewählter Lösungsansatz auch BGP voraussetzt.

4.2 Aspekt: Anbindung von Nutzern

Dieser Abschnitt stellt die Anforderungen an das Netzwerk heraus, die durch die Anbindung von Nutzern bedingt werden.

Eines der Ziele von FREE! ist es, „Vernetzungshilfe für Gruppen und Individuen [zu sein], um das Entstehen neuer sozialer Netze zu fördern" (vgl. [Nor08]). Soweit solche Individuen und Gruppen mit den Zielen von FREE! übereinstimmen und den Verein unterstützen wollen, können sie im Rahmen der Möglichkeiten mit dem Netzwerk des Wissenschaftsladen verbunden werden. Beispielsweise gibt es Glasfaserstrecken zu Benutzern im gleichen Gebäude. Mit dem geplanten Netzwerk soll der Teilnehmerkreis erweitert werden.

Konkret ist hier zu gewährleisten, dass die Anzahl der Benutzer und angeschlossenen Geräte, sowie die geographische Größe des Netzwerks im Laufe seines Bestehens zunehmen kann. Um diese Ziele zu erreichen, muss es auch möglich sein, an das Netzwerk angeschlossen zu werden, wenn vergleichsweise wenig finanzielle Mittel für die Nutzer oder den Verein zur Verfügung stehen. Diese Forderung lässt sich auch auf andere Szenarien, wie beispielsweise über Spenden finanzierte Hilfe für Rettungsmissionen oder von Aktivisten aufgebaute Netzwerke übertragen. Daher muss die Netzwerkstruktur mit preiswerter Hardware geplant werden.

Daraus lässt sich zudem ableiten, dass neue Benutzer an den für sie günstigst zu erreichenden Punkten des Netzwerks integriert werden sollten. Außerdem ist angestrebt, dass die einzelnen Knotenpunkte des Netzwerks über mehrere, also redundante Verbindungen erreichbar sind. Die sich daraus ergebende Topologie (Struktur des Netzwerks) ist also nicht sternförmig, sondern nimmt vermaschte Strukturen an.

Die Benutzer sollen außerdem die Möglichkeit haben, verschiedene Dienste, d.h. Anwendungen, Betriebssysteme und Protokolle in diesem Netzwerk verwenden zu können. Das Netzwerk wird daher als heterogen betrachtet und das Design muss auf Grund dessen neutral zu den laufenden Diensten sein.

Schlussendlich müssen das Netzwerk und die zugehörigen Geräte möglichst einfach zu administrieren sein. Auch diese Anforderung ist auf andere Szenarien übertragbar, da nicht davon ausgegangen werden kann, dass dort alle Administratoren eine entsprechende Ausbildung besitzen.

5 Netzwerkdesign

Ein wesentlicher Teil dieser Arbeit besteht darin, ein Netzwerkdesign für das geplante Funknetzwerk zu erarbeiten, das den in Kapitel 1 und 4 beschriebenen Anforderungen möglichst gut gerecht wird. Die in den Grundlagen angesprochenen Konzepte müssen dafür aufgegriffen, gegenüberstellt und mit Erfahrungen, die in der Praxis gemacht wurden, abgeglichen werden.

5.1 Auswahl geeigneter Hardware

Die Auswahl der Hardware und die Auswahl der Protokolle, die für die Richtfunkstrecke und das zugrunde liegende Netzwerk in Frage kommen, beeinflussen sich gegenseitig.

Um in Erfahrung zu bringen, ob sich bestimmte Antennen und Komplettsysteme für die geplante Richtfunkstrecke eignen, wurde verschiedene Hardware gesichtet und einiges davon getestet. Es wurde nach zahlreichen Einzelantennen und einigen Komplettsystemen, bestehend aus jeweils einer Antenne und integriertem Router, recherchiert. Im Folgenden sind einige Komplettsysteme aufgelistet, deren Preis, Verfügbarkeit und die Erfahrung, die mit gleichen oder ähnlichen Geräten gemacht wurden, den Anforderungen zu entsprechen schienen. Wichtige Kriterien für die Auswahl wurden auch aus den Richtfunkgrundlagen entnommen. Ein weiteres Kriterium war die Verfügbarkeit von Multiple Input Multiple Output (MIMO), was die Leistung der Antennen verbessert (vgl. Abschnitt 3.2.3).

Die Geräte, die in der Zeile „Quelle“, mit einem * gekennzeichnet sind, wurden selbst getestet.

Tabelle 5.1: 5 GHz Richtfunkkomplettsysteme

Bezeichnung	ATLAS CPE 411-5	Nano Bridge M5	SEXTANT	SXT-5HPnD	Tera CPE 5D
MIMO	k.A.	Ja	Ja	Ja	k.A.
(R/M)STP	k.A.	STP	RSTP	RSTP	RSTP
VLANs	Ja	Ja	Ja	Ja	Ja
MPLS	k.A.	Nein	Ja	Ja	Ja
BGP	k.A.	Nein	Ja	Ja	Ja
ISIS	k.A.	Nein	Nein	Nein	Nein
OSPF	Ja	Nein	Ja	Ja	Ja
Preis in Euro	~ 200	~ 75	~ 100	~78	~ 177
Hersteller	MikroTik	Ubiquiti	MikroTik	MikroTik	MikroTik
Quelle	[ATL13]	[Nan13],[Air13],*	[SEX13],*	[SXT13],*	[Ter13]

5.2 Ansatz: Schicht 3 mit dynamischem Routing

In diesem Unterabschnitt wird ein Lösungsansatz vorgestellt, der der Schicht 3 des OSI-Modells zugeordnet werden kann. Hierbei wird erläutert, wie eine mögliche Lösung aussehen müsste und warum diese letztendlich nicht allen Anforderungen gerecht werden kann.

Wie in Kapitel 4 bereits angesprochen, wird eine neutrale Infrastruktur gesucht. Eine Möglichkeit dies zu gewährleisten, ist ein auf Schicht 3 des OSI-Modells basierendes Netzwerk. Bei einem solchem Netzwerk werden Router als Vermittlungsstellen zwischen den Teilnetzen eingesetzt.

Innerhalb von Autonomen Systemen kommt ein Interior Gateway Protocol (IGP) zum Einsatz (vgl. Abschnitt 2.2.2).

In Abschnitt 2.2.2 wurden bereits Open Shortest Path First (OSPF) beschrieben und Intermediate System - Intermediate System (ISIS) als weiteres link state basiertes IGP erwähnt. Weil keines der ausgesuchten Geräte in der Lage ist, mit ISIS umzugehen, fällt es aus der weiteren Betrachtung heraus (vgl. Tabelle 5.1).

Ein Netzwerk auf der Basis von OSPF, ohne BGP, ist nicht in der Lage mit anderen Autonomen Systemen vollständige Internet-Routingtabellen auszutauschen. Daher kann es alleinstehend nicht für das Szenario eingesetzt werden.

Eine Kombination aus BGP und OSPF, oder einem anderen IGP, ist also die naheliegende Lösung.

Bei der vorliegenden Hardware war unmittelbar ersichtlich, dass BGP zwar aktiviert werden kann, die Geräte jedoch zu wenig Leistung haben, um große BGP-Tabellen zu verwalten.

Durch diese Erkenntnisse hat sich ergeben, dass OSPF sowie andere IGPs alleinstehend nicht für die Nutzung des geplanten Netzwerks ausreichend sind. Auch eine Kombination aus OSPF und BGP ist auf Grund der begrenzten Ressourcen der verwendeten Hardware nicht möglich.

5.3 Ansatz: Umsetzung als Schicht 2 Netzwerk

In diesem Teil geht es um die Bewertung von Netzwerkarchitekturen, die ausschließlich der Schicht 2 des OSI-Modells zugeordnet werden können. Bei der folgenden Betrachtung werden die Stärken und Schwächen einer Lösungsarchitektur auf der Datensicherungsschicht vorgestellt und in einem Unterabschnitt ein Ansatz, der in Kombination mit dem ersten Ansatz dessen Schwächen ausgleichen kann. Letzterer hat jedoch gewisse Skalierungsgrenzen. Für Szenarien, in dem die Anzahl der Verbindungen nicht darauf ausgelegt ist immer mehr zu expandieren, hat dieser Lösungsansatz besondere Relevanz.

Grundsätzlich besteht die Möglichkeit, ein Netzwerk auf Basis von Ethernet auf Schicht 2 des OSI-Modells zu entwerfen. Bei einer solchen Lösung werden die Komponenten wie ein Switch als Vermittlungseinrichtung eingesetzt. In der einfachsten Form sieht eine Realisierung so aus, dass alle aktiven Komponenten als transparente Bridge auf Schicht 2 betrieben werden, wobei die Topologie baumförmig angeordnet sein muss, um schleifenfrei zu sein. Anschließend können sich alle mit diesem Netzwerk verbundenen Geräte gegenseitig auf Schicht 2 erreichen.

Eine solch einfache Architektur ist aber für die in Kapitel 4 ermittelten Anforderungen unzureichend. In dieser einfachen Architektur gibt es keine Schutzmechanismen vor Fehlkonfigurationen oder Angriffen. Dies kann mit Hilfe einer logischen Aufteilung erreicht werden. Der Ansatz gewährleistet zudem nicht die angestrebte Redundanz ohne dabei ein Ständiges zirkulieren der Frames verhindern zu können (vgl. Abschnitt 4.1). Die Lösungsmöglichkeiten zu diesen Problematiken wird in den beiden folgenden Unterabschnitten behandelt.

5.3.1 Logische Segmentierung - Virtuelle LANs (VLANs)

Bei einem Netzwerk, das eine einfache Form hat, befinden sich alle Netzwerkgeräte in der gleichen Broadcast Domäne. Dies hat den Nachteil, dass alle Broadcast Frames an all diese Geräte, und damit auch über alle aktiven Funkstrecken, übertragen werden. Bei zunehmender Größe des Netzwerkes würde so immer mehr Bandbreite verbraucht. Gleichzeitig sind auch alle Geräte im Netzwerk von Fehlkonfigurationen oder Angriffen auf das Netzwerk betroffen.

Um ein Netzwerk logisch zu unterteilen, ohne dabei die physikalische Anordnung zu verändern, werden Virtuelle LANs (VLANs) eingesetzt. Eine weitere Möglichkeit, die mit VLANs besteht, ist auseinander liegende Netzwerke logisch so einzuteilen, dass sie sich wiederum in einem gemeinsamen virtuellem Netzwerk befinden. VLANs bringen somit auch noch den Vorteil mit sich, vergleichsweise flexibel zur physikalischen Unterteilung oder Zusammenführung der Netzwerke zu sein.

Von der in Betracht gezogenen Richtfunkhardware (vgl. Tabelle 5.1) sind alle Geräte in der Lage, mit VLANs umzugehen.

Ein wichtiger Nachteil für das geplante Netzwerk besteht darin, dass nicht ohne weiteres Schleifen innerhalb der virtuellen Teilnetze vermieden werden (vgl. Abschnitt 2.1). Um Schleifen zu vermeiden, muss eine zusätzliche Technik eingesetzt werden.

VLANs können also einen Teil der Voraussetzung erfüllen, die sich aus den Anforderungen ergeben haben, allerdings ist es nicht sinnvoll sie in diesem Kontext alleine einzusetzen.

5.3.2 Schleifenvermeidung - Spanning Tree Protocol (STP)

Das Spanning Tree Prototcol (STP) stellt eine Möglichkeit dar, auf Schicht 2 basierende, schleifenlose Netzwerkstrukturen aufzubauen. Hierzu werden bestimmte Netzwerkschnittstellen abgeschaltet.

> „Um eine fiktive schleifenlose Topologie aufzubauen, werden einige potentielle Verbindungen zwischen den LANs ignoriert." ([Tan03], S. 361)

Um STP mit VLANs einsetzen zu können und so die potentiellen Schleifen in den Netzwerksegmenten zu vermeiden, gibt es zwei Varianten von STP, die mit VLANs umgehen können. Die eine Möglichkeit ist eine von Cisco entwickelte Variante, Per-VLAN Spanning Tree (PVST), bei der pro VLAN STP individuell konfiguriert wird. Für jeden dieser Spannbäume werden dann eigene BPDU's durch das Netzwerk gesendet. Die andere Möglichkeit ist das Multiple Spanning Tree Protocol (MSTP), welches in einem Netzwerk mehrere Spannbäume, anstelle von nur einem, wie es bei STP der Fall ist, aufbauen kann. Hierbei werden für jede VLAN-Gruppe eigene Root-Bridges und aktive bzw. deaktivierte Netzwerkschnittstellen bestimmt. Hier wird insgesamt nur eine BPDU durch das Netzwerk geschickt. Mit beiden Varianten ist es möglich, für verschiedene VLANs verschiedene Pfade zu verwenden und so redundante Wege durch ein Netzwerk ohne Schleifen zu benutzen. Dies bringt einerseits eine größere Flexibilität als reines STP mit sich, bedeutet allerdings auch erhöhte Komplexität (vgl. Abschnitt 2.3.3).

Die in Tabelle 5.1 dargestellten Systeme sind jedoch nicht in der Lage, MSTP oder PVST anzuwenden. Diese Geräte in einer vermaschten Schicht 2 Lösung ohne VLANs und STP einzusetzen bedeutet einerseits, dass sich alle diese Geräte in einer Broadcast-Domäne befinden und gleichzeitig, dass entweder die Geräte in einer baumartigen Struktur aufgebaut werden oder Schleifen in Kauf genommen werden müssen.

Trotz dieser Erkenntnis ist es vorstellbar, ein Netzwerk auf Basis von Schicht 2 aufzubauen (vgl. Unterabschnitt 5.3) und die Schleifen, die in so einem Netzwerk entstehen können, mit Hilfe von STP zu vermeiden. Das Funknetzwerk soll jedoch wie bereits angesprochen auch skalierbar und anpassungsfähig sein (vgl. Abschnitt 4.2). Mit STP kann es jedoch mehr als 30 Sekunden dauern, bis nach einer Änderung der Topologie ein neuer Spannbaum bestimmt wurde und die dementsprechend zu aktivierenden Netzwerkschnittstellen wieder Frames weiterleiten. Änderungen in der Topologie können bei einer Richtfunkverbindung häufiger auftreten als in kabelgebundenen Netzwerken, etwa durch zeitweiligen Verbindungsabbruch bei Niederschlag oder Veränderung der Luftdichte (vgl. Abschnitt 3.1.3). Das ursprüngliche STP ist daher hinderlich.

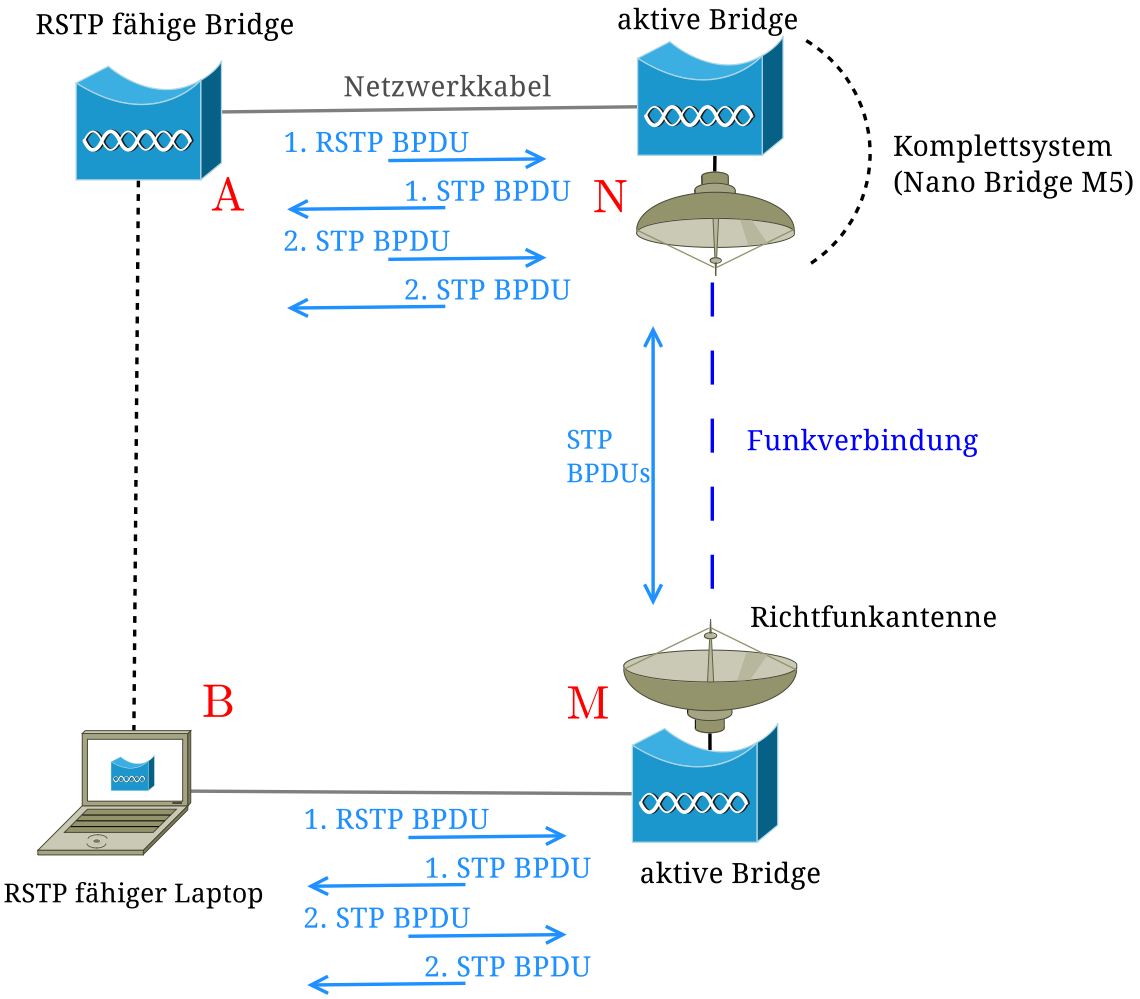
Von dem ursprünglichen STP gibt es jedoch inzwischen das Nachfolgeprotokoll RSTP, welches bei Änderungen, wie dem Ausfall von Pfaden im Netzwerk schneller reagiert als STP. Ein Versuch mit RSTP ist daher unternommen worden und im nachfolgenden Unterabschnitt dargestellt.

Versuch RSTP mit Nano Bridge M5

In diesem Versuch sollte die Nano Bridge M5, ein Richtfunkkomplettsystem von der Firma Ubiquiti, darauf hin überprüft werden, ob es in der Lage ist, RSTP einzusetzen, da dies aus ihrer Dokumentation nicht hervorgeht. RSTP ist derzeit aber Standard, daher war eine Überprüfung notwendig. MSTP und PVST wurden in diesem Versuch nicht getestet, da die Nano Bridge M5 diese Mechanismen nicht verwenden kann.

Der Testaufbau ist in der Abbildung 5.1 dargestellt.

Abbildung 5.1: Testaufbau STP



Eingesetzt wurden zwei baugleiche Komplettsysteme Nano Bridge M5 (N, M), ein RSTP fähiger Switch (A) sowie ein RSTP fähiger Laptop (B), auf dem ein Programm installiert war, um den Netzwerkverkehr mitzuschneiden.

Die beiden Nano Bridge M5 (N, M) wurden über ihre Antennen miteinander per WLAN verbunden. Die Netzwerkschnittstellen der Nano Bridges wurden jeweils mit RSTP-fähigen Bridges, davon eine am Laptop (B), verbunden. Auf diesem wiederum wurde der Datenverkehr von und zu den Nano Bridges beobachtet. Die installierte Software überwachte dabei die Netzwerkschnittstellen von B und über eine unabhängige Remote-Verbindung auf Bridge A, deren Schnittstelle in Richtung M.

Bei der Durchführung des Versuchs wurde auf beiden Nano Bridges STP aktiviert. Nachdem die RSTP-fähigen Bridges (A, B) zunächst RSTP Bridge Protocol Data Units (BPDUs) über ihren jeweiligen Port in Richtung NanoBridge ausgesandt hatten, schalteten sie nach Empfang der ersten STP BPDU von der NanoBridge, auf diesem Port von RSTP auf STP um. Nachdem STP konvergierte, was ca. 30 Sekunden dauerte, waren alle beteiligten Ports in den Zustand „Forwarding“ gesetzt, sodass Datenframes zwischen A und B über die Funkverbindung zwischen N und M gesendet und empfangen wurden, d.h. A und B auf Schicht 2 Daten austauschen konnten.

Als Ergebnis für diesen Versuch wurde festgehalten, dass die Nano Bridge M5 lediglich in der Lage ist, STP und nicht RSTP einzusetzen.

Versuch transparente Nano Bridge M5

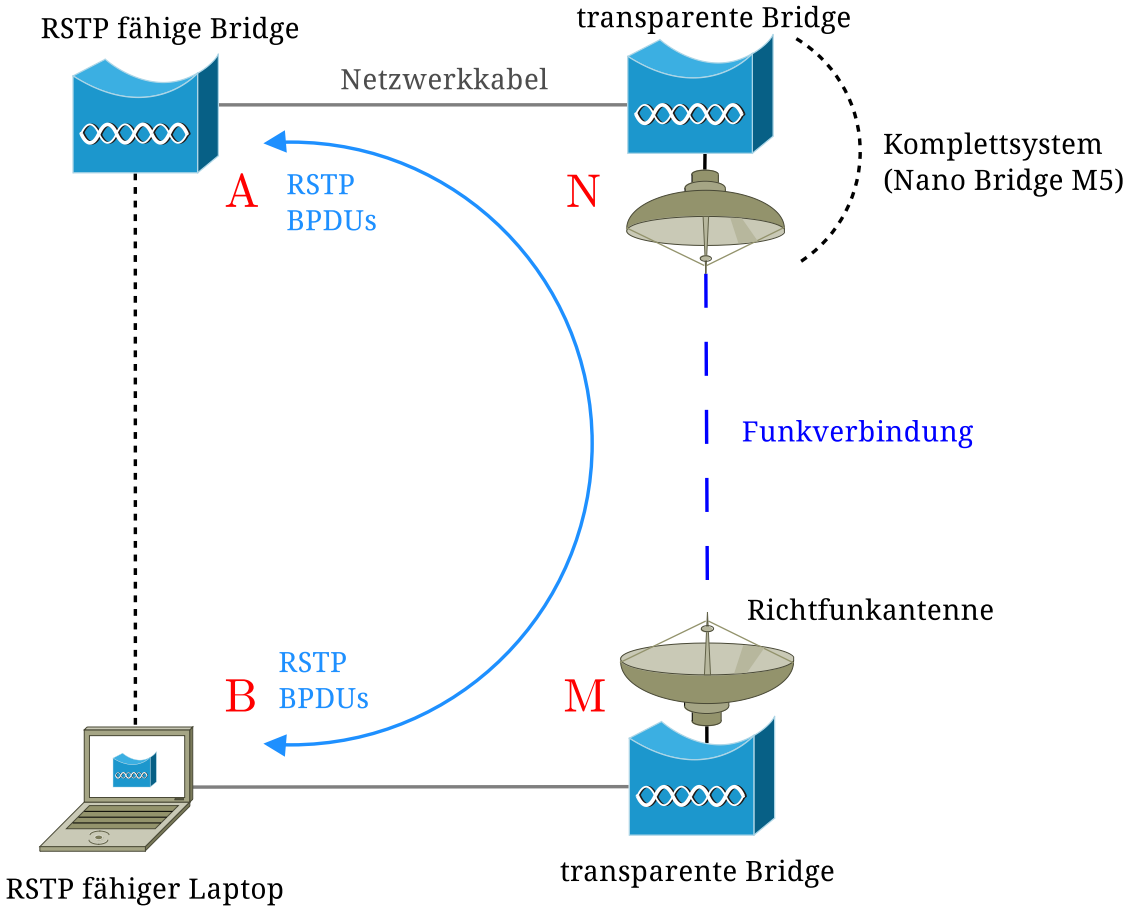
Da der erste Versuch ergab, dass die Nano Bridge M5 selbst nicht in der Lage ist, aktiv RSTP zu verwenden, wurde ein weiterer Versuch mit identischem Aufbau vorgenommen, bei dem die Nano Bridges transparent betrieben werden. Dieser Testaufbau ist in Abbildung 5.2 dargestellt.

In diesem Versuch wurde STP auf den Nano Bridges (M, N) abgeschaltet, RSTP war auf der verkabelten Bridge (A), sowie dem Laptop (B) weiterhin aktiviert.

Hierbei ließ sich beobachten, dass die RSTP BPDUs von A über N und M zu B gelangten und umgekehrt, woraufhin RSTP diese Verbindung zwischen A und B für Datenframes freigab, d.h. die Kabelports auf A nach N und von B nach M in den Zustand „Forwarding“ setzte.

Fazit des zweiten Versuchs: Nano Bridges können als transparente Bridges eingesetzt werden, sodass eine Richtfunkverbindung wie eine direkte Kabelverbindung zwischen den an sie angeschlossenen Bridges wirkt.

Abbildung 5.2: Testaufbau Transparenz



Konsequenzen des Versuchsaufbaus

Wie bereits in den Abschnitten 2.3.3 und 5.3.2 angesprochen, konvergiert ein Netzwerk mit STP sehr langsam. RSTP hat diesen Nachteil nicht. Wegen dieser langsamen Konvergenz von STP ist es nicht sinnvoll, STP auf den Nano Bridges zu aktivieren, sondern diese sollten besser als transparente Bridges genutzt werden. Dadurch wird es möglich, ein Richtfunknetzwerk mit redundanten Verbindungen auf Schicht 2 zu realisieren, indem das schneller konvergierende RSTP über die Funkverbindungen genutzt wird. Durch die transparente Verwendung der Nano Bridges ist es auch möglich andere MSTP/PVST-Kompatible Hardware, und damit die Nutzung dieser Methoden zu verwenden.

Dieser Lösungsansatz lässt sich gut auf Szenarien anwenden, die wie beim Wissenschaftsladen BGP verwenden. Da die leistungsschwachen Geräte transparent betrieben werden können, werden sie nicht mit den großen Internet-Routing-Tabellen belastet.

5.3.3 Schlussfolgerung für eine Schicht 2 Architektur

Bei der Verwendung von (R)STP werden nur die zum Spannbaum gehörigen Verbindungen zwischen Bridges bzw. Switches aktiviert. Alle anderen Verbindungen werden so lange deaktiviert, bis sie den Ausfall eines bisher aktiven links im Rahmen eines neuen Spannbaums ausgleichen müssen. Durch diese Funktionsweise von (R)STP wird zu jedem Zeitpunkt die Last auf die wenigen aktiven Pfade des aktuellen Spannbaums konzentriert.

Weiterhin gibt es in dem Funknetzwerk keinen zentralen bzw. geeigneten Punkt für eine Root Bridge, der für alle Netzwerkteilnehmer ideal ist. Insbesondere für Anwender, deren Zugang physikalisch in der Nähe eines Internet-Providers liegt, ist es am sinnvollsten, wenn die Root Bridge ebenfalls dort in der Nähe platziert ist. Bei zwei Internet-Providern (hier: AS), wie es in dem „Szenario Wissenschaftsladen“ der Fall ist, gibt es keine geeignete Root-Bridge für alle Anwender, die sich in der Nähe dieser AS bzw. Provider befinden. Dies bedeutet, dass selbst wenn statt RSTP MSTP oder PVST auf anderen Geräten und über die transparent eingestellten Richtfunksysteme betrieben wird, es für einzelne mögliche VLAN-Gruppen eine günstige Root-Bridge position geben kann, für die Gruppe aller Anwender aber z.B. nicht. Je größer das Netzwerk wird und die Anzahl der Nutzungsarten steigen, desto komplexer wird die Planung zur Bestimmung der Root Bridge für eine neue VLAN Gruppe. Damit nimmt auch die Anzahl konfigurationsbedingter Fehler mit hoher Wahrscheinlichkeit zu.

Für die geplanten Richtfunkverbindungen ist diese Skalierungsgrenze noch nicht erreicht. Falls aber, wie angedacht, an einzelnen Netzwerkknoten noch Ad-Hoc Netzwerke oder viele Richtfunkstrecken hinzukommen, ist diese Grenze, durch die Anzahl der Verbindungen, sehr bald erreicht.

Zusammenfassend kann festgestellt werden, dass die transparente Verwendung der Nano Bridges insbesondere für andere Szenarien von Wert ist. Für das Szenario Wissenschaftsladen wäre die Verwendung eines Protokolls aus der STP-Familie eine Möglichkeit um das derzeit geplante Netzwerk zu realisieren. Für die zukünftige Entwicklung, besonders bezogen auf die Skalierbarkeit des Netzwerks, reicht dies jedoch nicht mehr aus. Hierfür müssen andere Technologien oder teure Geräte, die den preislichen Rahmen übersteigen, benutzt werden.

5.4 Ansatz: Multiprotocol Label Switching (MPLS)

In diesem Unterkapitel wird eine Lösungsarchitektur vorgestellt und mit Hilfe von zwei Versuchen bewertet, die in der Lage ist den Prozess des Routings auf ausgewählte Router zu verlagern. Dabei wird herausgestellt, in welchem Rahmen sie sich für das Szenario eignet und warum ihre alleinige Anwendung nicht ausreichend ist.

Multiprotocol Label Switching (MPLS) ist ein protokollunabhängiges Verfahren zum Kennzeichnen von Paketen und Pfaden in einem Netzwerk.

Dabei ist es prinzipiell eher der Schicht 3 des OSI-Modells zuzuordnen, verhält sich allerdings teilweise wie ein Schicht 2 Protokoll. Es kann daher als Hybrid-Protokoll oder als sogenanntes Schicht 2,5 Protokoll bezeichnet werden.

Mit Hilfe von MPLS können IP-Pakete unabhängig von ihrer IP-Adresse weitergeleitet werden. Dafür bekommen diese IP-Pakete eine Marke (Label) zugewiesen. Dieses Verfahren führt dazu, dass IP-Pakete in kürzerer Zeit weitergeleitet werden können (vgl. [Ste04], S. 370f und Abschnitt 2.2.4).

Der Weg, den ein Paket vom Adressaten zum Ziel nimmt, wird dabei Label Switch Path (LSP) genannt. Dieser Weg kann von ausgewählten Routern mit Hilfe des Label Distribution Protocol (LDP) bestimmt werden. Ist dies der Fall, so wird von „Explicitly Routed LSP“ gesprochen. Diese Aufgabe übernehmen meist Router, die am Anfang oder Ende des Pfades stehen. Diese Router werden als Label Edge Router (LER) oder MPLS Edge Node bezeichnet. Alle Router, auf denen auch MPLS läuft, heißen Label Switch Router (LSR). Ein LSR, der nicht am Routingprozess beteiligt ist, leitet die ankommenden Pakete weiter, daher das „Switch“ in LSR (Abs. vgl. Abschnitt2.2.4).

Dieses Verfahren kann also eingesetzt werden, um die Komplexität des Routings auf einzelne Router auszulagern. Die eigene Schlussfolgerung war nun, MPLS einzusetzen, um leistungsschwache Richtfunkkomplettsysteme vom Routing zu befreien und dies auf andere Router auszulagern.

MPLS wird nicht von allen Geräten und nicht von jedem Betriebssystem unterstützt. Daher war eine Sichtung der zur Verfügung stehenden Implementierungen notwendig. Diese ergab, dass unter den unixartigen Betriebssystemen nur die Implementierung von OpenBSD als produktionsreif angesehen wird (vgl. [Jek11], S. 1,[Fre11, LIN11]).

Da nicht sicher war, ob die Implementierung von OpenBSD weit verbreitet ist, war zweifelhaft, ob sie tatsächlich entsprechend ausgereift genug ist, um für die gedachten Zwecke geeignet zu sein. Um dies nachzuprüfen, wurden komplexere Versuche mit einem gemischten Testaufbau durchgeführt. Im Testaufbau wurden verschiedene Router verwendet. Genauere Erläuterungen dazu befinden sich im nachfolgenden Unterabschnitt.

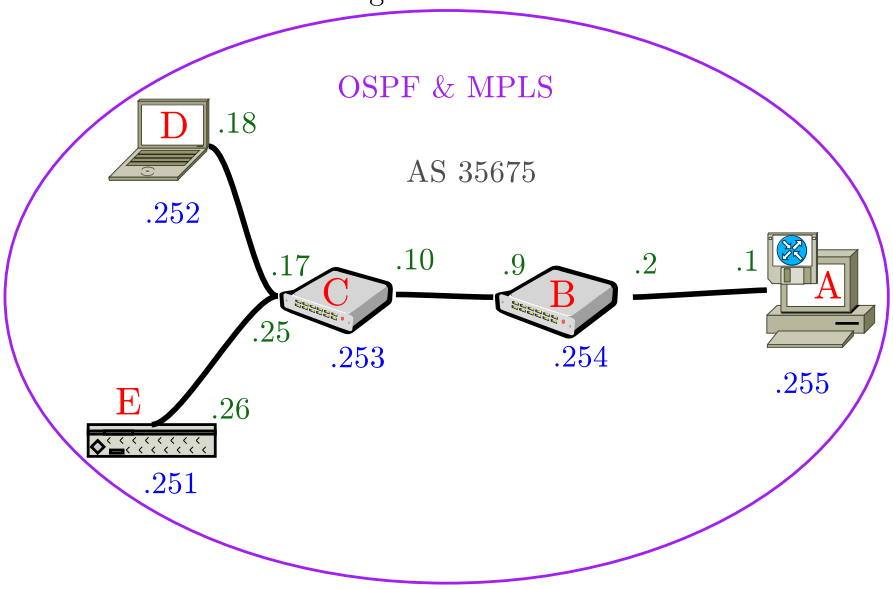
Um MPLS nutzen zu können, sollte zusätzlich ein Interior Gateway Protocol zum Einsatz kommen. Andernfalls bliebe nur eine Lösung, bei der iBGP und statische Routen als Alternative Verwendung finden. Dies würde allerdings hohen Wartungsaufwand mit sich bringen, wie schon im Unterabschnitt 4.1 beschrieben. Da LDP die LSP durch das Netzwerk anhand der Routingtabelle entwickelt, schränken statische Routen eine dynamische Wegewahl mittels MPLS sehr ein.

Als IGP wurde deswegen und aufgrund seiner Vorteile gegenüber anderen IGP, OSPF im nachfolgendem Versuch eingesetzt (vgl. Abschnitt 5.2, Abschnitt 2.2.2 und Tabelle 5.1)

Testaufbau MPLS

In Abbildung 5.3 ist die Struktur des Testaufbaus zu sehen.

Abbildung 5.3: MPLS-Testaufbau



AS - Autonomes System
MPLS - Multiprotocol Label Switching
OSPF - Open Shortest Path First

Legende
Loopback + ID's: 193.43.221.X /32
Adressen: 193.43.220.Y /29
Physikalische Verkabelung

Als Geräte wurden ein Desktop-PC (mit A bezeichnet), ein Embedded-PC-System „ALIX“ (mit E bezeichnet), ein Laptop (D) und zwei Router von MikroTik (B, C) eingesetzt.

Auf den beiden Routern von MikroTik lief die bis dato aktuelle Version (5.21) von „RouterOS“, dem Betriebssystem von MikroTik-Routern. Die Geräte A, D und E bekamen die derzeitige Version von OpenBSD (5.2) installiert.

Die Router (B, C) sollen die Richtfunksysteme simulieren, da auf den MikroTik Richtfunksytemen, wie sie in Tabelle 5.1 aufgelistet sind, auch RouterOS mit gleichem Softwarestand installiert ist. Hierbei war lediglich das Übertragungsmedium bei dem Testaufbau mit einem Kabel realisiert, während es bei dem Richtfunksystem als Wireless-Lan Verbindung besteht.

Um MPLS auf den Geräten in Betrieb nehmen zu können, wurde zunächst OSPF eingerichtet. Das Label Distribution Protocol (LDP) baut seine interne Labeltabelle auf der Routingtabelle von (in diesem Fall) OSPF auf (vgl. Abschnitt 2.2.4).

OSPF bindet die direkt angeschlossenen Netzwerke in seine Routingtabellen ein und verbreitet anschließend seine „Sicht“, d.h. seine Nachbarn und den Preis diese zu erreichen, an seine Nachbarrouter.

Um später die Router in den Routingtabellen wiederzuerkennen, wurden RouterIDs in Form von „Loopbackadressen“ angelegt und in den Routingprozess mit einbezogen. Die Loopbackadressen sind in der Grafik unterhalb der Geräte dargestellt.

MPLS wurde wie folgt umgesetzt: Um die vergleichsweise leistungsschwachen MikroTik Router zu entlasten, wurden sie so eingerichtet, dass sie nicht am Routing beteiligt waren. Von diesen Routern wurde LDP nur verwendet, um eine Tabelle aufzubauen, in der diese Router nachsehen konnten, wohin Pakete geschickt werden sollten (vgl. Abschnitt 2.2.4).

Die anderen Router (A, D und E) wurden als LER eingesetzt. Sie waren dafür an den Endstellen des Netzwerks platziert worden und bestimmten mit Hilfe von LDP den Label Switch Path. LDP benutzte dabei die Routingtabelle von OSPF und versah die einzelnen Routen mit einem Label. Diese Label wurden wiederum mit LDP an die andern Router propagiert.

Nachdem die passende Konfiguration auf allen Geräten gefunden war, funktionierte der Testaufbau wie erwartet.

Aus den Labeltabellen konnte entnommen werden, dass die Geräte MPLS verwenden um Label auszutauschen und somit ein dynamischer Label Switch Path durch das Netzwerk entsteht. Abbildung 5.4 zeigt beispielhaft einen LSP von PC A zu Laptop D.

Die vollständigen Tabellen der drei Router (A, B, C), die sich auf dem Label Switch Path befanden, können im Anhang eingesehen werden (siehe Tabelle 8.1 , Tabelle 8.2 und Tabelle 8.3).

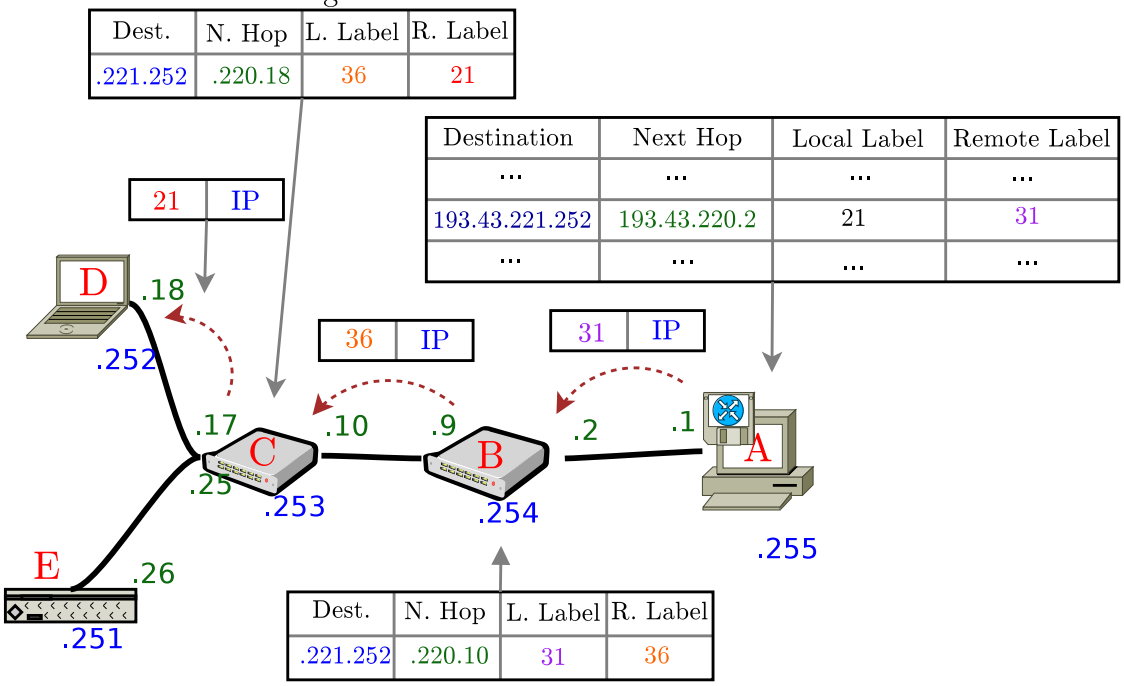
Das Ergebnis dieses Versuchs ist, dass sich MPLS eignet, einzelnen Routern die Bestimmung der Pfade durch das Netzwerk zu überlassen und andere Router von diesem Prozess zu befreien. Hiermit können Ressourcen dementsprechend gut ausgelastet und die Paketweiterleitung beschleunigt werden.

Testaufbau MPLS und BGP

Um herauszufinden, ob sich die Standardkonfiguration von MPLS eignet, um über dieses auch die BGP-Routen zu verteilen, wurden die Edge-Router von FREE! an den Testaufbau angeschlossen.

Abbildung 5.5 zeigt den Aufbau, bei dem zu dem MPLS noch das Border Gateway Protocol hinzugekommen ist.

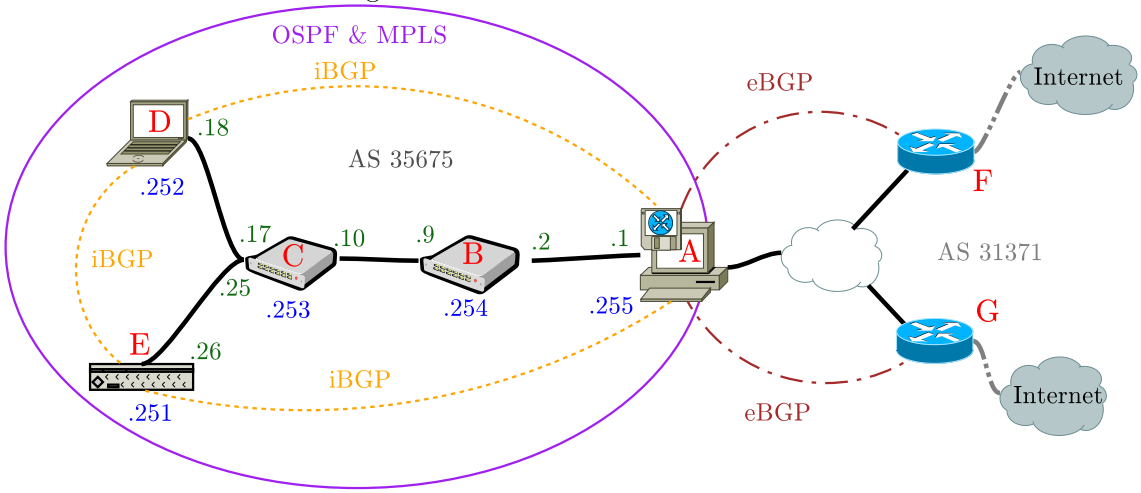
Abbildung 5.4: Ein Label Switch Path im Testaufbau



AS - Autonomes System
MPLS - Multiprotocol Label Switching
OSPF - Open Shortest Path First

Legende
Loopback + ID's: 193.43.221.X /32
Adressen: 193.43.220.Y /29
Physikalische Verkabelung
Label Switch Path

Abbildung 5.5: Testaufbau mit MPLS und BGP



AS - Autonomes System
eBGP - external Border Gateway Protocol
iBGP - internal Border Gateway Protocol
MPLS - Multiprotocol Label Switching
OSPF - Open Shortest Path First

Legende
Loopback + ID's: 193.43.221.X /32
Adressen: 193.43.220.Y /29
Physikalische Verkabelung
Verbindung in das Internet

Neu in der Abbildung sind die beiden Edge-Router von FREE! (F, G). Zwischen diesen beiden und dem Desktop-PC (A) wurde eBGP eingerichtet. Die beiden Edge-Router hatten außerdem eine Verbindung zu anderen Autonomen Systemen, also in das Internet. Zwischen A, E und D wurde iBGP konfiguriert. Die Konfiguration der MikroTik-Router wurde beibehalten.

Der Desktop-PC (A) sollte in diesem Szenario die BGP-Routen von den Edge-Routern (F, G) erhalten und diese anschließend an die Geräte E und D weitergeben. Auf diesen sollten sich dann anschließend die gleichen Routen befinden wie auf A.

Die beiden LSR (B, C) sollten mit der Größe dieser Routing-Tabellen nicht belastet werden. Auf diesen wurde daher auch kein iBGP konfiguriert.

In diesem Aufbau legte MPLS auf A für jede eBGP-Route ein eigenes Label an und verteilte diese an seine Nachbarn. LDP auf A synchronisierte also auch hier die Labeltabelle mit den Routingtabellen, aber nicht ausschließlich mit OSPF, sondern auch mit BGP. Die von A propagierten Label sollten auch an B und C weitergeleitet werden. Dies führte dazu, dass B, sobald er von dieser Vielzahl an Labeln erfuhr, stark überlastet war. Nach sehr kurzer Zeit stürzte B dann ab. So war es nicht möglich, die Routen an D und E weiter zu leiten.

Als Ergebnis für den zweiten Testaufbau mit MPLS kann festgehalten werden, dass sich die Standardkonfiguration von MPLS nicht eignet, um BGP-Tabellen über leistungsschwache Label Switch Router hinweg zu verteilen. Die Komplexität der großen BGP-Tabellen wurde damit nicht von den leistungsschwachen Routern genommen, sondern nur in Label umgewandelt.

5.5 Ansatz: MPLS Layer 3 VPN

Der folgende Lösungsansatz beschreibt ein auf Schicht 3 angesiedeltes, modifiziertes Verfahren. Seine Tauglichkeit für das Szenario wird mit Hilfe eines durchgeführten Versuchs dargelegt.

Der Versuch mit MPLS, der im vorigen Unterkapitel beschrieben ist, zeigte, dass die Standardkonfiguration von MPLS mit den eingesetzten Geräten funktioniert. Die Koppelung von MPLS und BGP war allerdings so nicht möglich. Aus diesen Gründen wurde nach einer Lösung mit MPLS gesucht, die dafür sorgt, dass die leistungsschwachen Router entlastet werden.

Das MPLS Layer 3 VPN ist eine Methode, mit der ein Dienstanbieter oder Netzwerkbetreiber ein IP Backbone, i.d.R für verschiedene Kunden betreibt. Es wird dazu verwendet, mit einem VPN verschiedene Netzwerke eines Kunden zu verbinden oder über dieses Netzwerk verschiedene Dienste anzubieten. Dazu senden die Router der Kunden ihre Routen an die Router des Anbieters. Die Router des Anbieters ver-

walten die verschiedenen Kundenrouten separat, so dass diese „virtuellen Instanzen“ dann voneinander getrennt sind (vgl. Abschnitt 2.2.5).

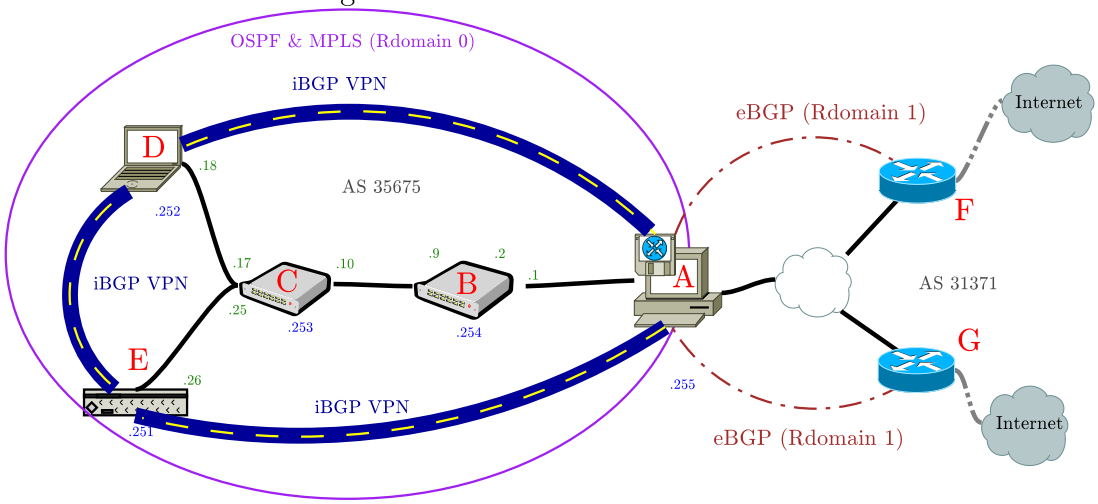
Die Implementierung auf OpenBSD verwendet zum Trennen von Routingtabellen und Netzwerkschnittstellen sogenannte Rdomains. Eine oder mehrere Routingtabellen und Schnittstellen können dabei einer Rdomain zugewiesen werden. Die Netzwerkschnittstellen operieren dann nach den Routen, die sich auf den Tabellen befinden, die der gleichen Rdomain zugewiesen sind (vgl. [Jek11], S. 3). Standardmäßig sind alle Prozesse und Schnittstellen der Rdomain 0 zugewiesen.

Um ein MPLS-Netzwerk mit einer anderen Rdomain zu verbinden, wird eine spezielle, virtuelle Netzwerkschnittstelle verwendet. Diese Schnittstelle heißt MPLS Provider Edge (MPE) (vgl. [Jek11], S. 5). Diese Eigenschaften lassen sich für das vorliegende Szenario wie folgt ausnutzen.

Testaufbau MPLS Layer 3 VPN

Abbildung 5.6 veranschaulicht die Umsetzung eines Versuchs mit MPLS Layer 3 VPN mittels Rdomains.

Abbildung 5.6: MPLS Testaufbau mit Rdomains



AS - Autonomes System
eBGP - external Border Gateway Protocol
iBGP - internal Border Gateway Protocol
MPLS - Multiprotocol Label Switching
OSPF - Open Shortest Path First
VPN - Virtual Private Network

Legende
Loopback + ID’s: 193.43.221.X /32
Adressen: 193.43.220.Y /29
Physikalische Verkabelung
Verbindung in das Internet

Auf den LSR wurde die MPLS-Standardkonfiguration verwendet, wie sie im Abschnitt 5.4 vorgestellt wurde. Diese Konfiguration war der Rdomain 0 zugewiesen. Dieser Teil war für die Wegewahl innerhalb des Netzwerks zuständig.

Einer weiteren Rdomain (Rdomain 1) wurde ein mit BGP eingerichtetes VPN zugeteilt. Dem VPN wurden Router, die BGP-Routen miteinander teilen sollten, zugeteilt (A, D, E). Die Konfiguration von eBGP zwischen Computer A und den Edge-Routern F und G wurde der Rdomain 1 zugeteilt.

Schlussendlich wurde der Rdomain 1 eine MPE-Schnittstelle zugewiesen. Auf der Rdomain 0 wurde eine statische Route eingerichtet, die auf die IP-Adresse des MPE verweist. A hat am Ende also einen iBGP Prozess, zu D und E auf Rdomain 0, sowie einen eBGP Prozess zu F und G auf Rdomain 1 konfiguriert.

Damit war es möglich Pakete, die an die IP-Adresse der MPE Schnittstelle gesendet wurden, von Rdomain 0 nach 1 zu transferieren. Durch diese Konfiguration konnte realisiert werden, dass die Routen, die Computer A von den externen Edge-Routern gelernt hat, an die Geräte D und E verteilt wurden. Die Label Switch Router (C, B) wurden mit diesen Routen nicht belastet. Auch die eBGP und LDP Tabellen konnten auf den Routern voneinander getrennt werden.

Dieser Testaufbau hat verdeutlicht, dass ein abgewandeltes MPLS Layer 3 VPN für das vorliegende Szenario einen geeigneten Lösungsansatz darstellt.

6 Ergebnisse

In diesem Kapitel wird das gewählte Design mit seinen verschiedenen Ebenen erläutert. Daran anschließend wird der abschließende Aufbau der Richtfunksysteme vorgestellt.

6.1 MPLS Layer 3 VPN

Das entwickelte Design hat verschiedene Ebenen der Implementierung. Im Folgenden sollen diese Ebenen von oben nach unten erläutert werden.

Auf der obersten Ebene ist das MPLS Layer 3 VPN angesiedelt. Dies wird einerseits durch ein virtuelles Netzwerk zwischen den an der Pfadbestimmung beteiligten Routern realisiert. Die BGP-Internetrouten werden nur über dieses VPN verteilt. Andererseits ermöglicht diese Aufteilung der Routing-Tabellen auf verschiedene Rdomains, dass die Tabellen für die Internet-Routen und die Tabellen für die Routen innerhalb des Netzwerks getrennt sind.

Für die Pfadbestimmung ist eine Ebene darunter MPLS auf allen an diesem Prozess beteiligten Routern konfiguriert. Die restlichen Geräte werden transparent betrieben. Für die Synchronisation der Label und um herauszufinden ob andere Router betriebsbereit sind, wird das LDP verwendet. Dabei verwendet das LDP, durch die Trennung auf verschiedene Rdomains, nur die Routen des lokalen Netzwerks für die LIB und die FIB.

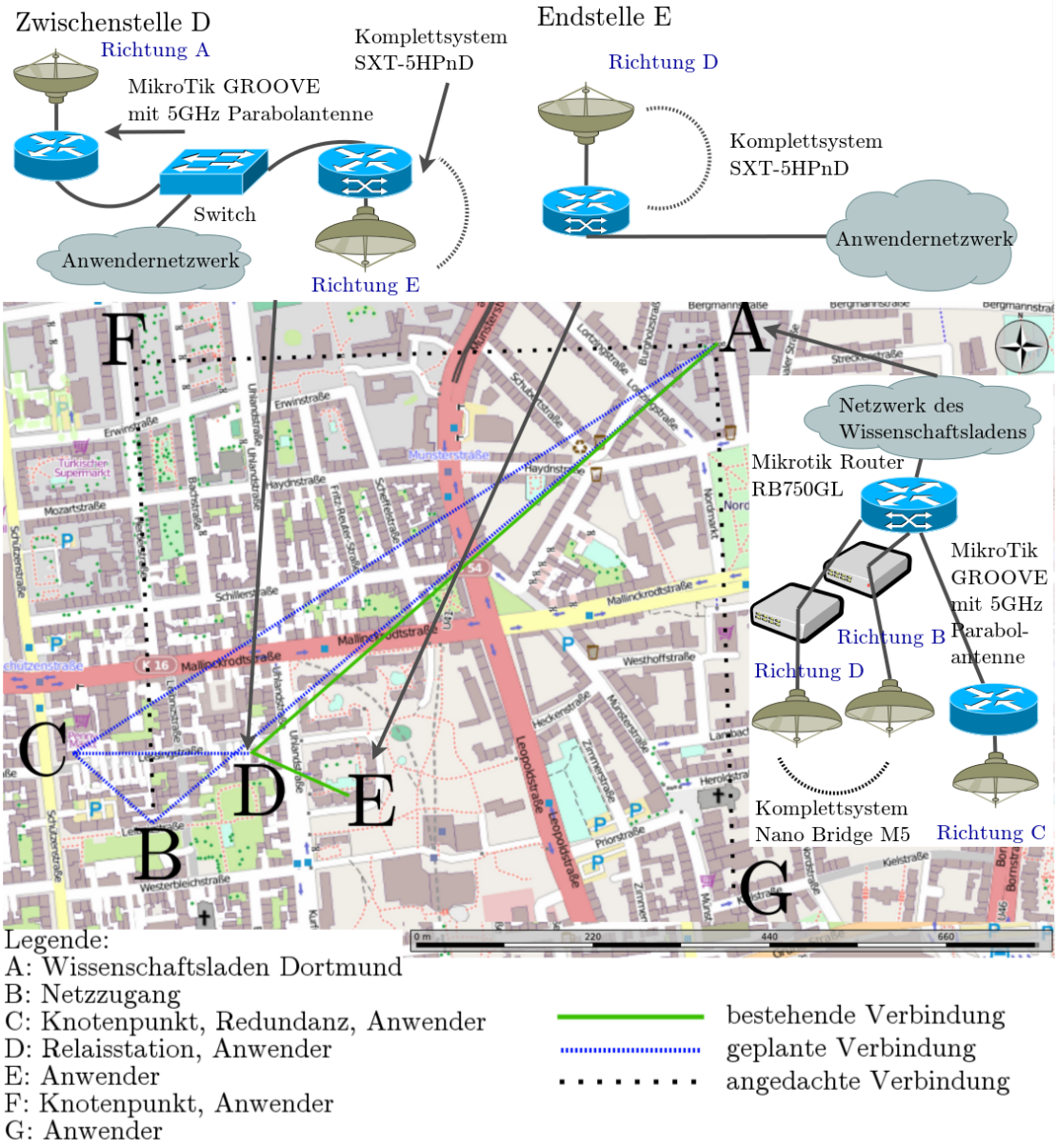
Das LDP wiederum basiert auf OSPF, da die Label in den Labeltabellen (LIB und FIB) den von OSPF aufgebauten Pfaden zugewiesen werden. Damit die Pakete auf den von OSPF bestimmten Pfaden zu ihrem Ziel gelangen können, sind den Routern und Endgeräten IP-Adressen, die auf dem IP-Protokoll basieren, zugewiesen. IP wiederum setzt voraus, dass Endgeräte, die in einem Teilnetzwerk sind, direkt miteinander kommunizieren können. In dem vorliegendem Design wird diese Kommunikation über die Richtfunkverbindungen und damit über WLAN realisiert. Die physikalische Übertragung wird durch Funkwellen im 5 GHz Frequenzbereich gewährleistet.

6.2 Abschließender Aufbau

In Abbildung 6.1 ist die zum Einsatz gekommene Hardware an den entsprechenden Stellen eingezeichnet.

Realisiert sind die Verbindungen zwischen A über D nach E. Zum Einsatz kommt dabei an Endstelle E das Komplettsystem SXT-5HPnD. Der integrierte Router übernimmt hier die Routingfunktion und die Verbindung zum Anwendernetzwerk.

Abbildung 6.1: Eingesetzte Hardware (Kartenmaterial: Marble/OpenStreetMap)



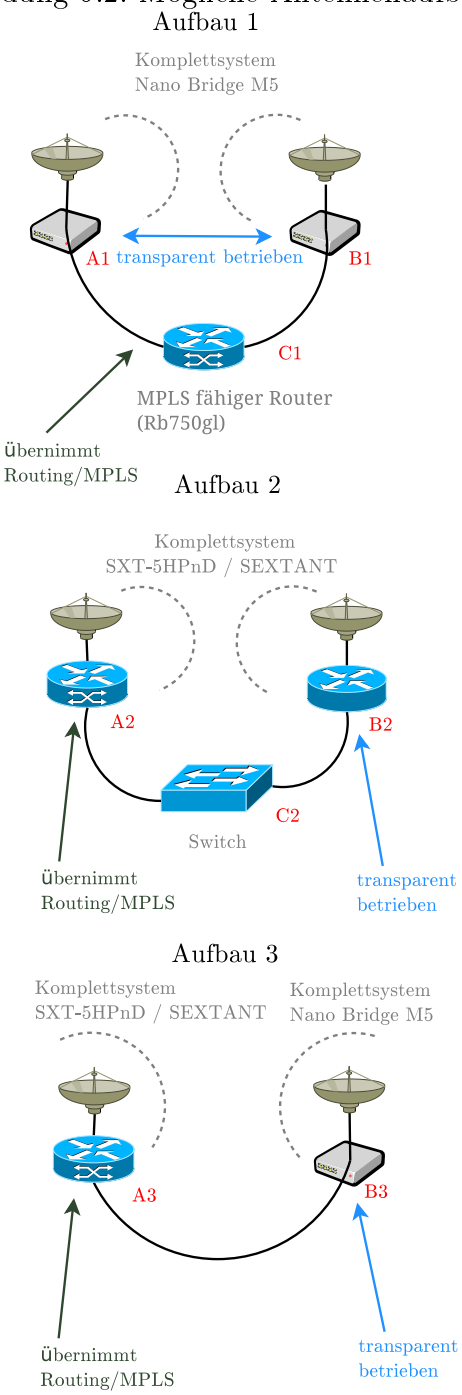
An der Zwischenstelle D übernimmt diese Funktion der gleiche Router, der ebenso in das Komplettsystem SXT-5HPnD integriert ist, das in Richtung E ausgerichtet ist. Über einen Switch ist das Anwendernetzwerk und ein MikroTik Router (GROOVE) verbunden. An dem MikroTik GROOVE ist eine in Richtung Wissenschaftsladen (A) ausgerichtete Parabolantenne angeschlossen. Im Anhang (Abbildung 8.1, 8.2) kann der Aufbau an der Zwischenstelle A und D eingesehen werden.

Am Wissenschaftsladen sind in Richtung D eine Parabolantenne und ein baugleicher MikroTik GROOVE Router angeschlossen. Dieser ist wiederum mit einem MikroTik Router (RB750GL), wie er auch im MPLS Testaufbau (vgl. Abschnitt 5.4) verwendet wurde, verbunden. Dieser Router ist an dieser Stelle für das Routing zuständig. Gleichsam sind an dem RB750GL zwei Komplettsysteme Ubiquity

Nano Bridge M5 angeschlossen, die in Richtung B und C ausgerichtet sind. Auf der gegenüberliegenden Seite sind derzeit noch keine Antennen vorhanden, daher sind beide Systeme noch nicht in Betrieb.

Jedoch wurden mit den vorhandenen und getesteten Systemen verschiedene Konzepte für die übriggebliebenen Zwischenstellen entwickelt. Zu sehen sind diese in Abbildung 6.2.

Abbildung 6.2: Mögliche Antennenaufbauten



7 Fazit

Ziel dieser Arbeit war es, ein wiederverwendbares Design für ein flexibel nutzbares Richtfunk-Netzwerk zu entwickeln und umzusetzen. Die erarbeiteten Ergebnisse sollten auch auf andere Einsatzgebiete übertragbar sein. Für das Szenario „Wissenschaftsladen Dortmund" wurden als spezielle Ziele die Nutzung des Netzwerks als eine Verbindung in das Internet für den Wissenschaftsladen und die Anbindung von Anwendern an den Wissenschaftsladen identifiziert. Wesentlich war, dass die Möglichkeit bestehen blieb, nachträglich weitere Nutzungsmöglichkeiten - etwa Ad-Hoc Netzwerke - zu realisieren. Als besonders herausfordernd erwies sich die Anforderung, Internet Routing mit kompletten Internet Routing Tabellen zu gewährleisten. Hierfür musste das Border Gateway Protocol, da es das etablierte Protokoll ist um die Routen zu allen erreichbaren Autonomen Systemen im Internet zu verwalten, eingesetzt werden. Weil die Erreichbarkeit der Dienste, die auf den Servern des Wissenschaftsladens betrieben werden, gewährleistet sein soll, war eine weitere Anforderung, dass die Verbindungen eine hohe Verfügbarkeit gewährleisten. Einerseits kann dieses Ziel durch vermaschte Strukturen erreicht werden, anderseits sind mehrfache Verbindungen von einzelnen Knotenpunkten auch für die angebundenen Nutzer angestrebt, da bei dem Wegfall einer Verbindung die Erreichbarkeit über andere Punkte gewährleistet ist und die Verbindung nicht über einen zentralen Punkt laufen soll, da auch zwischen den Anwendern Datenverkehr denkbar ist.

Die zu verwendenden Systeme sollten einfach zu administrieren sein, weil damit mit möglichst wenig Aufwand das Netzwerk verwaltet werden kann. Langfristig sollte es neuen Anwendern, die auch wenig finanzielle Mittel zur Verfügung haben, möglich sein mit dem Wissenschaftsladen mit Hilfe von Richtfunksystemen verbunden zu werden. Daher musste die ausgewählte Hardware vorzugsweise günstig sein. Ein Design, das den Einsatz von unterschiedlichen Diensten ermöglicht, war notwendig, da die Anwender in der Auswahl ihrer Dienste nicht eingeschränkt werden sollten.

Was die Verwendung von BGP als Protokoll in dem Netzwerk angeht, so konnten mit Hilfe von mehreren Versuchen zwei verschiedene Lösungsansätze erarbeitet werden. Die Problematik bestand darin, dass die ausgewählten Geräte zu leistungsschwach waren, um die Tabellen mit den vielen Routen zu den anderen Autonomen Systemen zu verwalten.

Der erste Lösungsansatz basiert auf Schicht 2 des OSI-Modells mit dem Rapid Spanning Tree Protocol (RSTP). Hierbei werden die Richtfunksysteme transparent betrieben. Sie sind damit in der Lage, Pakete ausschließlich weiter zu leiten, ohne selbst in den Prozess der Pfadwahl auf Schicht 2 einzugreifen. Andere Geräte übernehmen in diesem Fall den Prozess des Switching. Dieser Lösungsansatz hat den klaren Vorteil, dass er mit wenig Aufwand und daher schnell umzusetzen ist. Er

eignet sich insofern besonders für Szenarien, bei denen es in kurzer Zeit möglich sein soll, ein Richtfunknetzwerk aufzubauen.

Andererseits musste festgestellt werden, dass sich dieser Lösungsansatz für das vorliegende Szenario nur bedingt eignet, weil zu den einzelnen Anwendern mehrere Richtfunkstrecken führen sollen und das Netzwerk vermaschte und nicht sternförmige Strukturen annehmen soll. Die vermaschten Strukturen werden bei der Verwendung von RSTP jedoch nicht genutzt. Der eigentliche Vorteil, der also durch diese mehrfachen Verbindungen entsteht, kann damit nicht realisiert werden.

Zu diesem Zweck wurde ein weiterer, aber auch komplexerer Lösungsansatz entworfen. Dieser Ansatz wurde mit einem Virtuellen Privaten Netzwerk (VPN) auf Basis von Schicht 3 Multiprotocol Label Switching (MPLS) umgesetzt. Mit diesem Entwurf war es möglich, die verschiedenen Pfade gleichzeitig zu nutzen und die Verwaltung von BGP, sowie den Routingprozess einzelnen, ausgewählten Routern zu überlassen. Gewährleistet wird dies, da Rdomains die Routingtabellen auf den Internetroutern trennen und indem das eingerichtete VPN die BGP-Tabellen, die sich auf den Internetroutern befinden, kapselt und über das Netzwerk als IP-Pakete verteilt. Die Internet-Routen sind daher für die leistungsswachen Richtfunksysteme transparent. Diese Lösung eignet sich besonders, wenn die Anzahl der Netzwerkteilnehmer stark zunehmen soll.

Zwei unterschiedliche Lösungsansätze haben den Vorteil, dass für ein spezielles Szenario der passende Lösungsansatz ausgewählt werden kann.

7.1 Ausblick

Da es fristgerecht aufgrund der vielen geplanten Verbindungen und der Wettereinwirkungen nicht möglich war, alle Verbindungen zu verwirklichen, sind die verbleibenden Verbindungen, sowie hinzukommende noch zu realisieren. Weil der Wissenschaftsladen Interessierten die Möglichkeit bieten möchte, sich direkt mit dem Wissenschaftsladen zu verbinden, wird das Netzwerk in Zukunft höchstwahrscheinlich noch erweitert.

Eine Erweiterung ist bereits angedacht. Die Standorte der Richtfunkverbindungen sollen genutzt werden um dort Ad-Hoc Netzwerke zu errichten. Gerade für Interessierte, die nicht direkt an die Richtfunkverbindungen angeschlossen werden können, sind Ad-Hoc Netzwerke eine Option, sich trotzdem mit dem WilaDo zu verbinden.

Falls preiswerte Geräte, wie die Nano Bridge M5 zukünftig in der Lage sind die vielen Internet-Routen zu verwalten oder MSTP einzusetzen, ist es denkbar mit solchen Geräten ein ähnliches Richtfunk-Netzwerk, möglicherweise mit noch weniger Konfigurationsaufwand, zu betreiben. Auch andere Protokolle, die anstel-

le eines Spannbaums Link-State-Verfahren auf Datensicherungsschicht verwenden, wären eine attraktive Alternative. Derzeit sind solche Entwicklungen jedoch noch nicht ausgereift oder sprengen den preislichen Rahmen.

Für die Entwicklung von MPLS bleibt zu hoffen, dass in Zukunft weitere freie Implementierungen unter Linux, FreeBSD oder anderen Betriebssystemen zur Verfügung stehen werden.

Danksagung

Ich möchte hiermit allen danken, die mich bei der Fertigstellung meiner Bachelorarbeit unterstützt haben. Danke für die Motivationen und das Korrekturlesen!

Insbesondere einen großen Dank an meinen Betreuer seitens des Wissenschaftsladen Dortmund Immo Wehrenberg, vor allem dafür, dass er soviel Zeit für mich erübrigt hat. Außerdem vielen Dank an Frank Nord für anregende Kommentare.

8 Anhang

8.1 Tabellen

Tabelle 8.1: Labeltabelle von Rechner A

Destination	Nexthop	Local Label	Remote Label
0.0.0.0/0	193.43.221.254	25	-
91.204.5.192/26	193.43.220.2	16	Pop tag
193.43.220.0/29	0.0.0.0	3	Untagged
193.43.220.0/29	193.43.220.1	3	Untagged
193.43.220.8/29	193.43.220.2	17	Pop tag
193.43.220.16/29	193.43.220.2	18	24
193.43.220.24/29	193.43.220.2	19	26
193.43.221.252/32	193.43.220.2	21	31
193.43.221.253/32	193.43.220.2	22	27
193.43.221.254/32	193.43.220.2	23	Pop tag
193.43.221.255/32	193.43.221.255	24	Untagged

Tabelle 8.2: Labeltabelle von Router B

Destination	Nexthop	Local Label	Remote Label
193.43.220.16/29	193.43.220.10	24	-
193.43.220.24/29	193.43.220.10	26	-
193.43.221.253/32	193.43.220.10	27	-
193.43.221.255/32	193.43.220.1	29	24
193.43.221.252/32	193.43.220.10	31	36
193.43.221.251/32	193.43.220.10	32	37

Tabelle 8.3: Labeltabelle von Router C

Destination	Nexthop	Local Label	Remote Label
0.0.0.0/0	91.204.5.193	17	-
193.43.220.0/29	193.43.220.9	29	-
193.43.221.254/32	193.43.220.9	32	-
193.43.221.255/32	193.43.220.9	34	29
193.43.221.252/32	193.43.220.18	36	21
193.43.221.251/32	193.43.220.26	37	19

8.2 Abbildungen

Abbildung 8.1: Parabolantennen auf dem Dach des WilaDo

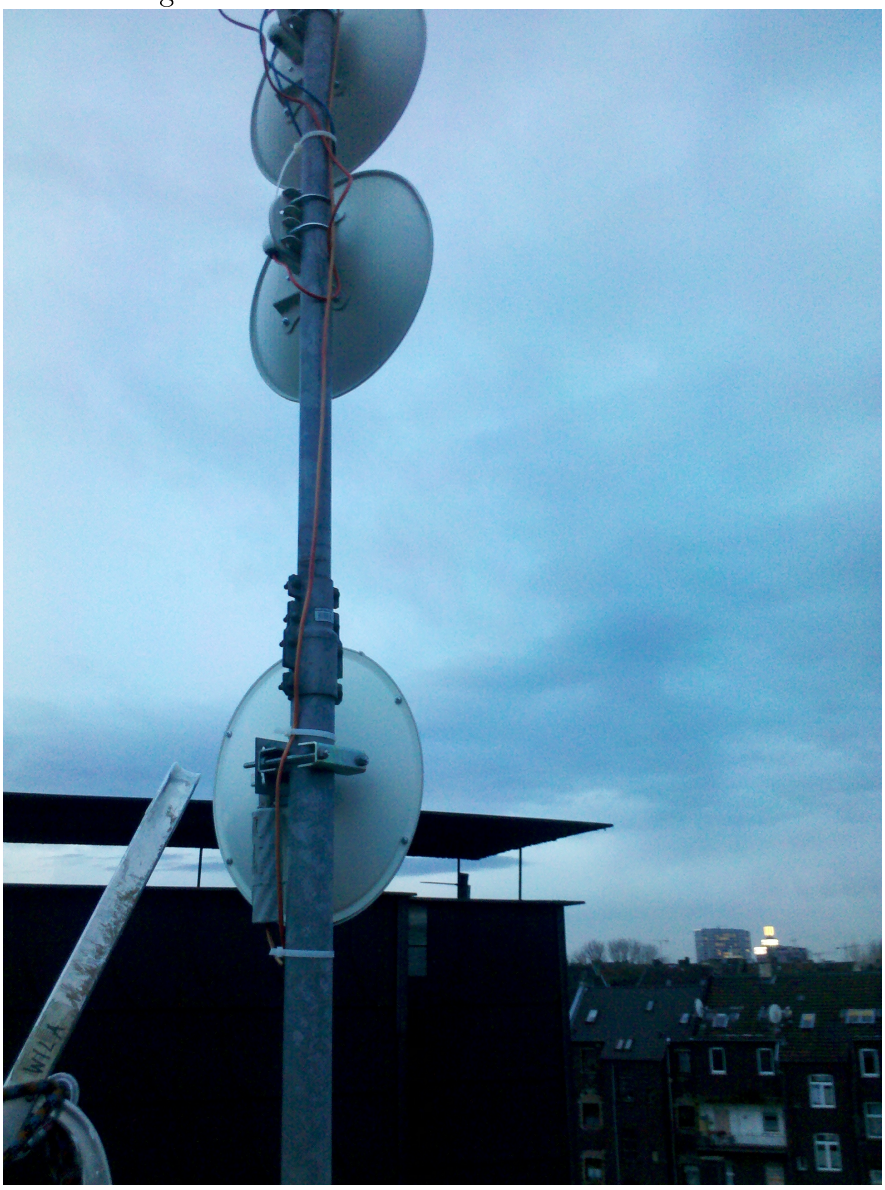


Abbildung 8.2: Aufbau an der Zwischenstelle D

8.3 Verzeichnisse

Literatur

[Air13] *airOS v5.5.2 User Guide.* 2013 `http://dl.ubnt.com/guides/airOS/airOS_UG.pdf`. – Abgerufen am 27.02.2013 (PDF)

[AMT07] Andersson, L. ; Minei, I. ; Thomas, B.: *RFC 5036 - LDP Specification.* 2007 `https://tools.ietf.org/html/rfc3031`. – Abgerufen am 16.02.2013

[ATL13] *mikrotik-shop.de: ATLAS CPE 411-5.* 2013 `http://www.mikrotik-shop.de/Komplettsysteme/ATLAS-CPE-411-5::183.html`. – Abgerufen am 15.01.2013

[Be05] Bless, R. ; et al: *Sichere Netzwerkkommunikation.* Berlin/Heidelberg/Wiesbaden : Springer Verlag, 2005. – ISBN 9783540218456

[BSH13] Bates, T. ; Smith, P. ; Huston, G.: *www.cidr-report.org*. 2013 http://www.cidr-report.org/as2.0/. – Abgerufen am 23.01.2013

[Car72] Carl, H.: *Richtfunkverbindungen*. Stuttgart/Berlin/Köln/Mainz : Berliner Union, 1972. – ISBN 9783408530362

[Com07] Computerworld: *Lexikon: aktuelle Fachbegriffe aus Informatik und Telekommunikation*. Vdf Hochschulverlag, 2007 (Computerworld-Lexikon). – ISBN 9783728131089

[DB86] Dodel, H. ; Baumgart, M.: *Satellitensysteme fuer Kommunikation, Fernsehen und Rundfunk - Theorie und Technologie*. Heidelberg : Huethig, 1986. – ISBN 9783778511633

[DKe81] Digel, W. ; Kwiatkowski, G. ; et al: *Meyers grosses Taschenlexikon in 24 Baenden*. Mannheim/Wien/Zuerich : Bibliographisches Institut, 1981. – ISBN 9783411019205

[Don74] Donnevert, J.: *Richtfunkuebertragungstechnik*. München/Wien : R. Oldenbourg, 1974. – ISBN 9783486346016

[DZCC02] D. Zwicky, E. ; Cooper, S. ; Chapman, C. B.: *Einrichten von Internet Firewalls*. Köln : O'Reilly, 2002. – ISBN 9783897213463

[Fre11] *MPLS implementation on FreeBSD*. 2011 http://freebsd.mpls.in/. – Abgerufen am 17.02.2013

[Güt13] Gütter, D.: *Rechnernetzpraxis - Ausbreitung elektromagnetischer Wellen*. 2013 http://www.guetter-web.de/education/rnp/rnp_4.pdf. – Abgerufen am 18.02.2013 (PDF)

[Har12] Hartpence, B.: *Praxiskurs Routing und Switching*. Köln : O'Reilly, 2012 (OReillys basics). – ISBN 9783868991857

[HPR+06] Huebscher, H. ; Petersen, H.-J. ; Rathgeber, C. ; Richter, K. ; Scharf, D.: *IT-Handbuch - IT-Sytemelektroniker/-in, Fachinformatiker/-in*. Braunschweig : Westermann, 2006. – ISBN 9783142250427

[Huc10] Hucaby, D.: *CCNP SWITCH 642-813 Official Certification Guide*. Indianapolis : Cisco Press, 2010. – ISBN 9781587202438

[Hun03] Hunt, C.: *TCP/IP Netzwerk-Administration*. Köln : O'Reilly, 2003. – ISBN 9783897211797

[Jek11] Jeker, C.: *Demystifying MPLS, The MPLS framework in OpenBSD.* 2011 http://2011.eurobsdcon.org/papers/jeker/MPLS.pdf. – Abgerufen am 16.01.2013 (PDF)

[Kap09] Kaps, R.: *Breitband-Pioniere - WLAN-Richtfunk bringt schnelles Internet aufs Land.* 2009 http://www.heise.de/ct/artikel/Breitband-Pioniere-888283.html. – Abgerufen am 03.01.2013

[Köh04] Köhler, T.: *Netzwerk-Konsolidierung: Unternehmensnetze mit Communications Resourcing.* München : Addison Wesley Verlag, 2004. – ISBN 9783827321879

[Kom13] *Elektronik Kompendium, Abschnitt Netzwerktechnik.* www.elektronik-kompendium.de, 2013 www.elektronik-kompendium.de/sites/net/index.htm. – Abrufdatum jeweils angegeben

[KR08] Kurose, J.F. ; Ross, K.W.: *Computernetzwerke.* München : Addison Wesley Verlag, 2008 (IT - Informatik). – ISBN 9783827373304

[Lie09] Liebherr, P.: *Der WiLaDo.* 2009 http://www.wissenschaftsladen-dortmund.de/der-wissenschaftsladen-dortmund/. – Abgerufen am 18.02.2013

[Lie11] Liebherr, P.: *2. Feb '11: Solidarität mit den Ägypterinnen und Ägyptern.* 2011 http://www.free.de/archives/21-Solidaritaet-mit-den-AEgypterinnen-und-AEgyptern.html. – Abgerufen am 26.02.2013

[LIN11] *MPLS for Linux - BETA.* 2011 http://sourceforge.net/projects/mpls-linux/. – Abgerufen am 17.02.2013

[Mül13] Müller, M.: *Wireless LAN, WLAN nach 802.11a 802.11b, 802.11g, 802.11n, 802.11ac. 802.11ad.* 2013 http://www.gepanet.com/wlan.htm. – Abgerufen am 03.01.2013

[Nan13] *shop.omg.de: Ubiquiti NanoBridge M5.* 2013 http://shop.omg.de/ubiquiti-networks/5-ghz/ubiquiti-nanobridge-m5-5ghz-22dbi-mimo-nbm5-22/a-83/. – Abgerufen am 15.01.2013

[Nor08] Nord, F.: *FREE!: Ziele.* 2008 https://www.free.de/pages/ziele.html. – Abgerufen am 18.02.2013

[Nor12] Nord, F.: *FREE!: Historie.* 2012 http://www.free.de/pages/historie.html. – Abgerufen am 27.02.2013

[RR06] Rosen, E. ; Rekhter, Y.: *RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs)*. 2006 https://tools.ietf.org/html/rfc4364. – Abgerufen am 18.02.2013

[RVC01] Rosen, E. ; Viswanathan, A. ; Callon, R.: *RFC 3031 - Multiprotocol Label Switching Architecture*. 2001 https://tools.ietf.org/html/rfc3031. – Abgerufen am 16.02.2013

[Saf11] *Workshop on Public Safety Networks, Techniques and Challenges*. 2011 http://www.hnps.eu/mass2011.html. – Abgerufen am 26.02.2013

[Sch06] Scherff, J.: *Grundkurs Computernetze*. Berlin/Heidelberg/Wiesbaden : Springer, 2006. – ISBN 9783528059026

[Sch07] Schreiner, R.: *Computernetzwerke*. München : Hanser, 2007. – ISBN 9783446410305

[SEX13] *mikrotik-shop.de: MikroTik SEXTANT*. 2013 http://www.mikrotik-shop.de/Komplettsysteme/MikroTik-SEXTANT::640.html. – Abgerufen am 15.01.2013

[Ste04] Stein, E.: *Taschenbuch Rechnernetze und Internet*. München/Wien : Carl Hanser Verlag, 2004. – ISBN 9783446225732

[SXT13] *mikrotik-shop.de: MikroTik SXT 5HPND*. 2013 http://www.mikrotik-shop.de/::702.html. – Abgerufen am 15.01.2013

[Tan03] Tanenbaum, A. S.: *Computernetzwerke*. München : Addison-Wesley Verlag, 2003. – ISBN 9783827370464

[Ter13] *mikrotik-shop.de: Tera CPE 5D*. 2013 http://www.mikrotik-shop.de/Komplettsysteme/Tera-CPE-5D::630.html. – Abgerufen am 15.01.2013

[Tre10] Treiber, J.: *Praxishandbuch Netzwerktechnik*. Willburgstetten : J. Schlembach Fachverlag, 2010. – ISBN 9873935340670

[Wei02] Weidenfeller, H.: *Grundlagen der Kommunikationstechnik*. Stuttgart/Leipzig/Wiesbaden : Teubner, 2002. – ISBN 9783519062653

[Wik13] *Wikipedia*. 2013 https://de.wikipedia.org. – Abrufdatum jeweils angegeben

[Wil96] *Mehr über Wissenschaftsläden - Was sind Wissenschaftsläden?* 1996 http://www.wissenschaftsladen-dortmund.de/

der-wissenschaftsladen-dortmund/about/. – Abgerufen am 18.02.2013

Abbildungsverzeichnis

Tabellenverzeichnis

Index