Humboldt University Berlin
Computer Science Department
Systems Architecture Group

Rudower Chaussee 25
D-12489 Berlin-Adlershof
Germany

Phone: +49 30 2093-3400
Fax: +40 30 2093-3112
http://sar.informatik.hu-berlin.de


# Auswahl von Internet-Gateways und VLANs im Berlin RoofNet

**HU Berlin Public Report**
**SAR-PR-2007-05**

**July 2007**

Author(s):
Jens Müller

Humboldt-Universität zu Berlin
Fakultät für Informatik
Lehrstuhl für Systemarchitektur

Betreuer: Mathias Kurth
Gutachter: Prof. Dr. Jens-Peter Redlich
Abgabedatum: 26. Juli 2007

# Auswahl von Internet-Gateways und VLANs im Berlin RoofNet

Studienarbeit vorgelegt von

Name: Jens Müller
E-Mail: jmueller@informatik.hu-berlin.de

## Zusammenfassung

Diese Arbeit stellt im ersten Teil die Mechanismen vor, die im Berlin RoofNet (BRN) verwendet werden um Nutzer mit dem Internet zu verbinden. Dabei wird insbesondere eine Abwägung zwischen einer verbindungs- und einer paketorientierten Auswahl von Internet-Gateways besprochen.

Im zweiten Teil wird die Implementierung von VLANs für das BRN vorgestellt. Die Implementierung beider Projekte erfolgte in Click.

# Inhaltsverzeichnis

# 1 Auswahl von Internet-Gateways

## 1.1 Einleitung

Die Vernetzung von Communities durch selbstorganisierte dezentrale Netze wird größtenteils von Enthusiasten betrieben. Die Ziele sind derzeit stark von Faktoren, wie Experimentierfreude und Forscherdrang bestimmt. Hauptaugenmerk ist die Entwicklung eines funktionierenden Netzwerks, das für seine Benutzer einen Nutzen mit sich bringt, aber dabei frei ist.

Für die Benutzer solcher Netzwerke besteht der größte Wert in dem alternativen Zugang zum Internet. Dies ist derzeit der Hauptzweck der alternativen Community-Netzwerke. Teilweise sind sie sogar aus diesem Grund erst entstanden.

In ersten Teil dieser Arbeit wird der Mechanismus beschrieben, der die Nutzer des Berlin RoofNet (BRN) mit dem Internet verbindet. Das BRN [BRN] wird in Anlehnung an das MIT Roofnet [MIT] am Lehrstuhl für Systemarchitektur der Humboldt Universität zu Berlin entwickelt. Kurz zusammengefasst handelt es sich um ein drahtloses selbstorganisiertes multi-hop Netzwerk.

Auf die, für die Implementierung des „Internet Service“ relevanten, Eigenschaften des BRN wird an den entsprechenden Stellen eingegangen.

## 1.2 Analyse

Internet-Gateways im BRN zu finden, ist eine Aufgabe, die in Unteraufgaben zerlegt werden kann. Es wurden folgende Teilprobleme ermittelt:

- Erkennen eines lokalen Gateways

  Bei dieser lokal ausführbaren Aufgabe entscheidet ein Knoten eigenständig, ob er ein Internet-Gateway ist, d.h. eine Verbindung ins Internet hat. Dabei ist zu beachten, dass die Verbindung ins Internet durch andere Gateways im drahtlosen Netzwerk nicht als „lokale“ Internetverbindung betrachtet wird. Denn dies hätte den Effekt, dass sich jeder Knoten als Gateway begreifen würde, sobald auch nur ein Gateway aus dem drahtlosen Netzwerk bekannt ist. Die Abbildung 1 verdeutlicht den Zusammenhang. In der Abbildung ist ein Knoten mit einer Verbindung ins Internet per DSL und ein anderer Knoten mit einer Verbindung über einen Router, der per DSL ans Internet angebunden ist, zu sehen. Die anderen Knoten sind keine Gateways, auch wenn sie Gateways aufgrund der Vermaschung des Netzwerks erreichen können.

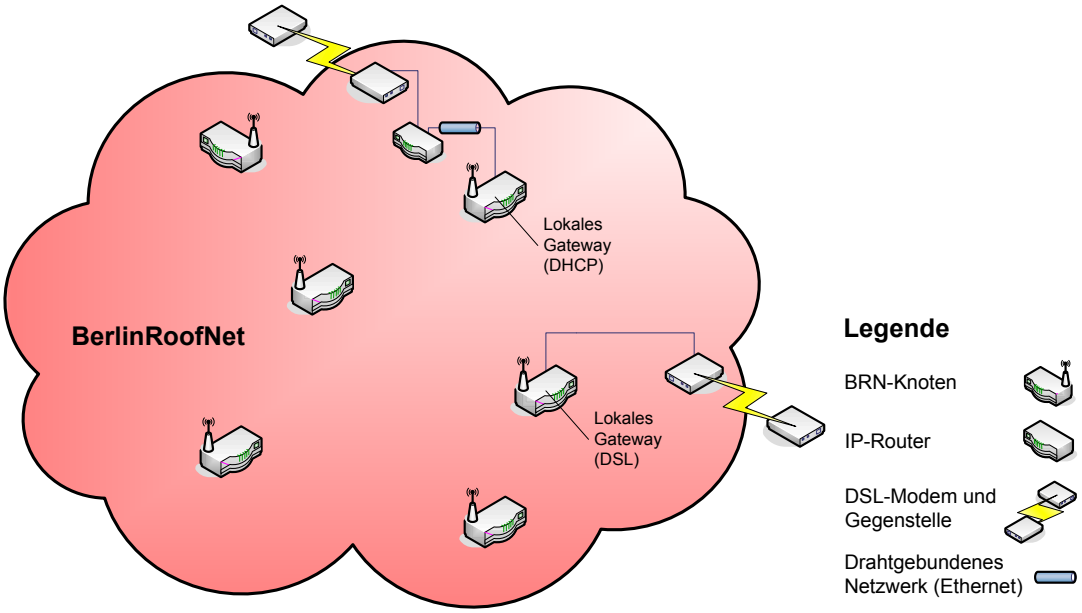



Abbildung 1: Lokale Gateways

- Verbreitung der Informationen über verfügbare Gateways

  Die Informationen über bekannte Gateways werden in einer Distributed hash table (DHT) gespeichert. Ein Knoten, der festgestellt hat, dass er ein Gateway ist, trägt sich in die DHT ein. Andere Knoten können alle Gateways unter einem zuvor vereinbartem Schlüssel in der DHT nachschlagen.

- Auswahl eines Gateways

  Liegen einem Knoten die Informationen zu den vorhandenen Gateways vor, so ist es seine Aufgabe Pakete, die ins Internet geroutet werden müssen, optimal unter den Gateways zu verteilen. Dabei müssen zwei Faktoren abgewägt werden. Auf der einen Seite sollte ein Paket durch das drahtlose Netzwerk auf bestem Wege transportiert werden. Das ist die Aufgabe des Routingprotokolls. Aus diesem Grund wird bei der Auswahl eines Gateway unter Zuhilfenahme des Routing das aussichtsreichste Gateway gewählt. Es werden die vom Routingprotokoll ermittelten Werte der Routen zu den Gateways verwendet. Auf der anderen Seite sollte die Auswahl eines Gateway nicht zu seiner Überlastung führen. Ein Gateway, das aus Sicht des Routingprotokolls besonders gut erreichbar ist, muss dennoch nicht alle Pakete weiterleiten können. Grund dafür ist meist die eingeschränkte Bandbreite eines DSL-Anschlusses. Eine Gateway-Metrik beschreibt die Auslastung des Gate-

way. Bekommt ein Gateway zu viele Pakete, so könnte es den Wert dieser Metrik verringern. Die Metrik könnte entsprechend der Auslastung der Internetverbindung, z.B. durch den Füllstand einer Paket-Queue, modelliert werden. Für diese Arbeit spielt diese Metrik aber eine untergeordnete Rolle.

Im Folgenden betrachten wir diese Teilaufgaben getrennt voneinander. Dabei ist unter einem Knoten eine Einheit zu verstehen, auf der die BRN-Software ausgeführt wird und Netzwerkgeräte wie Ethernet und WLAN integriert hat. Ein Knoten verfügt über mehrere Ethernet-Ports.

### 1.2.1 Erkennen von Gateways

Lokal festzustellen, ob ein Knoten Pakete ins Internet zu stellen und Pakete aus dem Internet empfangen kann, ist ein schwieriges Unterfangen.

Eine Möglichkeit ist es, einen Mechanismus anzustoßen, sobald ein bestimmtes Gerät per Dynamic Host Configuration Protocol (DHCP) konfiguriert wurde. Wird bei dieser Konfiguration eine default-Route gesetzt, so ist in der Regel davon auszugehen, dass der Knoten Verbindung ins Internet hat. Zusätzlich sollte überprüft werden, ob der Knoten tatsächlich Zugang zum Internet hat. Ob ein Knoten Pakete der BRN-Nutzer korrekt ins Internet weiterleiten kann oder die Pakete an einem späteren Zeitpunkt verworfen werden, ist schwer zu entscheiden. Denn nachdem das Paket das BRN verlassen hat, gibt es nur sehr eingeschränkte Kontrollmöglichkeiten.

Es sind lediglich Heuristiken denkbar. Diese verhindern, dass ein Knoten sich als Gateway aufgefasst wird, obwohl er eine dazu notwendige Eigenschaft nicht erfüllen kann. Eine simple Heuristik würde überprüfen, ob der Knoten einen allgemein bekannten Internetdienst erreichen kann.

Um auch Knoten direkt mit dem DSL-Modem zu verbinden, ist eine Möglichkeit ein Shell-Skript auszuführen, sobald ein Kabel in den entsprechenden Ethernet-Port des Knotens gesteckt wird. Das Skript hat dann die Aufgabe den DSL-Anschluss zu konfigurieren. Bei DSL-Anbietern muss Benutzername und Passwort des DSL-Zugangs für die Konfiguration bekannt sein. Eine Nutzerinteraktion wird notwendig.

Die Kombination beider Ansätze existiert bereits. So konfiguriert FON [FON] ihren Router „La Fonera“ für DHCP oder DSL und weitere Zugänge, je nach Auswahl des Benutzers. Insgesamt ergibt sich der Ablauf:

1. (Auto-)Konfiguration des Zugangs (u.U. mit Abfrage von Zugangsdaten)
2. Überprüfen, ob eine default-Route gesetzt ist.

3. Mögliche weitere Heuristiken überprüfen (z.B. Erreichen eines allgemein bekannten Internetdienstes).

4. Eintragen des Knotens als Gateway

### 1.2.2 Verbreitung der Informationen über Gateways

In den bisherigen Ansätzen zur Verteilung lokaler Internetverbindung wurde die Verfügbarkeit von Gateways in das Netz geflutet. Beim MIT Roofnet wird die Existenz eines Internet-Gateway an alle anderen Knoten des Netzes per Flooding verteilt [BABM05].

Im Falle des Routingprotokolls Optimized Link State Routing (OLSR) wird die Information über Internet-Gateways durch Nachrichten in das Netz geflutet. Dazu wurde das „Dynamic Internet gateway plugin“ entwickelt, das dem olsrd beiliegt [OLS].

Im BRN wird zur Verbreitung der Informationen über bekannte Gateways die bereits vorhandene Distributed hash table (DHT) verwendet. Vorteil dieses Ansatzes ist die Möglichkeit Probleme wie Knotenausfall und Netzwerkpartition durch die DHT an einer Stelle zu lösen und für ihre Dienste zu abstrahieren. Alternativ ist eine proaktive bzw. reaktive Verteilung der Gateway-Informationen möglich. Proaktiv meint dabei, dass jedem Knoten stets die Gateways bekannt sind. Im Unterschied zu reaktiv, wo die Gateways erst ermittelt werden, wenn ein Paket ins Internet zugestellt werden muss. Diese beiden Ansätzen wurden bereits in [GHP+04] miteinander verglichen.

Ein Problem, das bei der Nutzung einer DHT entsteht, ist die Semantik einer Hashtabelle mit der Zuordnung von Schlüssel zu Wert. Unter einem global bekannten Schlüssel werden alle Gateway-Informationen abgelegt. Dieser Wert ist eine Liste von Gateway-Einträgen. Der Schlüssel muss global eindeutig sein, damit die Knoten ihn nachschlagen können. Desweiteren muss jeder Knoten in der Lage sein seinen eigenen Eintrag zu aktualisieren, d.h. hinzufügen, anzupassen und zu löschen. Ein Knoten, der nun einen Wert verändern will, lädt den Wert des gesamten Schlüssels, passt seinen entsprechenden Eintrag an und speichert den gesamten Wert wieder unter dem Schlüssel. Bei diesem Vorgehen kann es zum sogenannten *Problem des verlorenen Updates* kommen, da zwei Knoten ihre Werte zur gleichen Zeit ändern könnten. Ihre Operationen auf der DHT können sich beliebig überschneiden. In Betriebssystemen wird diesem Problem mit Semaphoren begegnet, um Kombinationen zu unterbinden, die zu falschen Ergebnissen führen. Dabei wird der Zugriff auf die Ressource synchronisiert, so dass falsche Ergebnisse vermieden werden.

Die Ursache dieses Problems liegt auch in der Tatsache, dass mehrere Knoten gleich-

zeitig den Wert desselben Schlüssels schreiben. Um das Problem zu vermeiden, wird für jeden Knoten ein eigener Wert eingeführt. Jeder Knoten trägt unter dem Oberschlüssel für Gateways unter *seinem* eigenen Unterschlüssel seine Werte ein. Der Unterschlüssel muss eindeutig genau einem Knoten zugeordnet werden. Kein anderer Knoten darf die Werte eines Anderen schreiben. Will ein Knoten nun alle Gateway-Einträge lesen, so liest er den Wert zum Oberschlüssel und erhält eine Liste aller Gateway-Einträge. Da sich alle Informationen unter dem Oberschlüssel befinden, werden alle Informationen durch die DHT auf einem Knoten gespeichert.

Für das Nachschlagen aller bekannten Gateways ist eine DHT-Anfrage mit dem Oberschlüssel notwendig. Weiterhin wird eine Anfrage für das Verändern eines Eintrags benötigt. Dabei sollte beachtet werden, dass in den Anfragen die Kosten für die DHT selbst noch nicht enthalten sind.

### 1.2.3 Auswahl eines Gateway

Aus dem Wissen über alle existenten Gateways entscheidet ein Knoten lokal, welches Gateway aus seiner Sicht die beste Wahl ist. Wie bereits erwähnt, ist dabei einerseits die Qualität der Routen zu den Gateways im drahtlosen Netzwerk wichtig, andererseits darf es aber nicht zur Überlastung von Gateways kommen.

Aus diesem Grund verwendet der Auswahlmechanismus die Metrik des zu Grunde liegenden Routingprotokolls. Im BRN wird Dynamic Source Routing (DSR) [JMB01] in Kombination mit der Expected Transmission Count (ETX)-Routingmetrik [CABM03] verwendet. Ist für ein Gateway die Metrik unbekannt, so werden „leere“ Pakete geschickt um die Metrik ermitteln zu lassen. Beim DSR werden nicht zu jedem Ziel Routen und ihre Metriken vorgehalten.

Zu jedem Paket, das über ein Gateway verschickt wird, wird in das Antwortpaket die Auslastung des Gateway mit übertragen. Für bidirektionale Verbindungen besteht so für die Auswahlinstanz die Möglichkeit festzustellen, ob das Gateway eventuell überlastet ist. Die Metrik zur Auslastung eines Gateway wird nur verwendet um festzustellen, ob der Knoten ein Gateway ist. Für diese Arbeit soll die Gateway-Metrik nachrangig sein.

### 1.2.4 Kosten des Mechanismus

Wir betrachten den gesamten Mechanismus bis zur Zustellung der Pakete an ein Gateway um eine Übersicht über den Aufwand zu geben. Jeder Knoten fragt in einem konfigurierbaren Intervall alle bekannten Gateways in der DHT unter dem Oberschlüssel ab. Man kann also davon sprechen, dass das Nachschlagen der Gateways proaktiv über eine

DHT erfolgt. Im BRN wird eine auf Chord [SMLN+03] basierende DHT verwendet. Eine Anfrage bei dieser DHT verursacht bis zu $\log n$ Unicasts im Maschennetzwerk. Dabei wird noch nicht betrachtet, dass das DSR das Netz fluten muss, falls es ein Paket an einen bis dato unbekannten Knoten versenden soll. Eine Anfrage an die DHT verursacht also netzweite Broadcasts, falls keine Routen zu den Zielen bekannt sind.

Mit einem weiteren konfigurierbaren Intervall wird entschieden, in welchen zeitlichen Abständen ein Gateway seinen Wert unter seinem Unterschlüssel aktualisiert. Das ist notwendig, da aus Sicht der DHT sonst nicht klar ist, ob ein Wert noch gültig ist. So könnte es passieren, dass ein Gateway ausfällt und die Information in der DHT aber erhalten bleibt. Alle Gateways pflegen ihre Einträge in der DHT kontinuierlich. Die bisher behandelten Kosten des Mechanismus finden fortlaufend statt. Die Ermittlung „brauchbarer“ Werte für die besprochen Intervalle ist für diese Arbeit nicht von Interesse.

Erhält ein Knoten ein Paket zur Zustellung in das Internet, so bestimmt der Auswahl-Mechanismus das aussichtsreichste Gateway. Dabei kann die Routingmetrik zu einem Gateway noch unbekannt sein. In diesem Fall verursacht der Mechanismus ein Paket, dass an dieses Gateway geschickt wird.

Insgesamt werden die Kosten des Mechanismus durch die kontinuierlichen Anfragen an die DHT bestimmt. Dabei kann es zu netzweiten Broadcasts kommen, sofern keine Route bekannt ist. Zudem werden die Daten unter *einem* Oberschlüssel und folglich auf *einem* Knoten gespeichert. Langfristig kann sich dies als Flaschenhals erweisen.

### 1.2.5 Verbindungs- und paketorientierte Ansätze

In der Praxis stellt sich bei OLSR das Problem, dass Verbindungen zusammenbrechen. In [FC] beschreiben die Entwickler des Freifunk-Netzes in Berlin, dass die Verbindungen sehr unzuverlässig sind. Die Ursache ist in zwei Punkten zu sehen. Zunächst entscheidet beim OLSR-Protokoll jeder Knoten den nächsten Hop anhand seiner lokalen Informationen. Der Absender schreibt den Weg durch das Netz nicht vor. Weiterhin routet OLSR auf IP-Ebene. Im Falle von Paketen, die für Internet-Gateways bestimmt, entscheidet die default-Route über den nächsten Hop. Die Knoten entlang des Wegs, den das Paket nimmt, bestimmen den Weg. Ändert sich bei einem Knoten die default-Route, so ist es möglich, dass das Paket einem anderen Gateway zugestellt wird. In [Tø] wird vorgeschlagen IP-in-IP-Tunnel zum Gateway aufzubauen. So wird jedem Knoten genau ein Gateway zugeordnet und folglich die Pakete immer zum selben Gateway geschickt.

Beim MIT Roofnet wird für jede Verbindung anfangs ein Gateway gewählt und dann alle Pakete, die zu einer Verbindung gehören an dasselbe Gateway geschickt. So wird ver-

hindert, dass Verbindungen zusammenbrechen, auch wenn ein anderes Gateway besser erreichbar ist.

Diese Ansätze sind für mobile Clients unzureichend, da die Pakete im drahtlosen Netzwerk nicht den besten Internet-Uplink aus Sicht des Routing wählen. Zudem brechen Verbindungen zusammen, wenn das Gateway, über das die Verbindung läuft, ausfällt.

Man kann vier verschiedene Möglichkeiten unterscheiden Gateways zu zuordnen:

- Pro Client (auf der OSI-Schicht 2)

  Jedem Client wird ein Gateway zugeordnet. Genauer wird sich zu jeder Client-MAC-Adresse genau ein Gateway gespeichert.

- Pro Client-Sitzung (z.B. DHCP)

  Jeder Sitzung eines Clients, die mit Ablauf der Gültigkeit der per DHCP verteilten IP-Adresse endet, wird genau ein Gateway zugeordnet.

- Pro Verbindung

  Jeder Verbindung wird genau ein Gateway zugeordnet.

- Pro Paket

  Jedem Paket wird genau ein Gateway zugeordnet.

Die verschiedenen Ansätze sind hinsichtlich der Auswahl eines Gateway unterschiedlich restriktiv. Bestimmt man das Gateway pro Client, so hat man nur für das erste Paket vom Client Entscheidungsfreiheit. In Folge fließen alle Pakete eines Clients über das einmal gewählte Gateway. Am flexibelsten in der Auswahl ist eine Entscheidung pro Paket. In der Praxis erfolgt die Entscheidung aber meist anhand von Verbindungen, da die Verbindungen zusammenbrechen, wenn ein anderes Gateway für Pakete einer Verbindung gewählt wird. Die Ursache ist in der Verwendung von Network Address Translation (NAT) zu suchen. Da auf den Gateways NAT durchgeführt werden muss, wenn Pakete aus dem privaten IP-Adressraum (10.9.0.0/16) des BRN in das Internet weitergeleitet werden sollen. Jedes Gateway hat eine unterschiedliche öffentliche IP-Adresse. Zur Identifizierung von Verbindungen wird unter anderem diese IP-Adresse verwendet. Ändert sie sich durch die Auswahl eines anderen Gateway, so ist die Verbindung nicht mehr identifizierbar und der Empfänger verwirft das Paket.

Andererseits ist eine flexible Auswahl aus Sicht des Routing in drahtlosen Netzwerken wünschenswert, da sich die Bedingungen für den Transport von Paketen häufig ändern. Für verbindungsorientierte Protokolle wie Transmission Control (TCP) kann

| **Verbindungsortientiert** | **Paketorientiert** |
|---|---|
| (-) Erkennung von Verbindungen | (+) Keine Erkennung notwendig |
| (-) Probleme beim Ausfall eines Gateway in Kombination mit NAT | (+) Keine Probleme beim Ausfall |
| | (-) Verwendung verbindungs-orientierter Protokolle |
| | (-) Kryptographische Protokolle, die die Absender-IP-Adresse verwenden |
| (-) Unflexibler in der Auswahl | (+) Flexibler |
| (-) Lastverteilung auf Verbindungsebene | (+) auf Paketebene |

Tabelle 1: Vor- und Nachteile von verbindungs- und paketorientierter Auswahl

keine Auswahl auf Paketebene aus den geschilderten Gründen erfolgen. Selbst für das User Datagram Protocol (UDP) kann das Problem entstehen, wenn es im Verbindungsmodus betrieben wird. Bei diesem Modus kann der Socket angewiesen werden nur Pakete von einer bestimmten IP-Adresse und Port zu akzeptieren. Aufgrund der verbreiteten Anwendung verbindungsorientierter Protokolle, wird meist eine Auswahl auf Verbindungsebene durchgeführt. Community-Netzwerke wie das Freifunk-Netz erzielen damit eine gute Nutzerakzeptanz.

Im verbindungsorientierten Fall wählt ein Knoten lediglich einmal ein Gateway pro Verbindung aus. Danach ordnet er eintreffende Pakete einer Verbindung zu und sendet sie an das gespeicherte Gateway. Für dieses Vorgehen müssen Verbindungen erkannt werden. Dennoch ist zu beachten, dass eine Abschätzung des zu erwartenden Verkehrs unzureichend sein kann. Es ist schwer abzuschätzen, wie viel Verkehr und damit Ressourcen eine Verbindung belegen wird. Die Vor- und Nachteile von verbindungs- und paketorientierter Auswahl von Gateways sind in der Tabelle 1 zusammengefasst.

Als Alternative zu dem bisherigen Weg schlägt diese Arbeit einen anderen Ansatz vor. Anstatt mit verbindungsorientierten Protokollen zu arbeiten, werden die Nutzer über ein UDP-basiertes Virtual Private Network (VPN) mit dem Internet verbunden. Dieser Ansatz tunnelt jeglichen Verkehr (inklusive verbindungsorientiertem) aus dem drahtlosen Netzwerk. Ein besonderer Vorteil ist, dass selbst bei Ausfall eines Gateway über das Pakete liefen, daraus keine Folgen für bestehende Verbindungen entstehen. Insgesamt werden die Pakete zu einem zentralen Ort hinter dem drahtlosen Netzwerk getunnelt und von dort weitergeleitet.

Für das BRN entsteht dadurch eine zentrale Komponente und zusätzlicher Administrationsaufwand. Der Betrieb der VPN-Server kann auf Provider ausgelagert und als

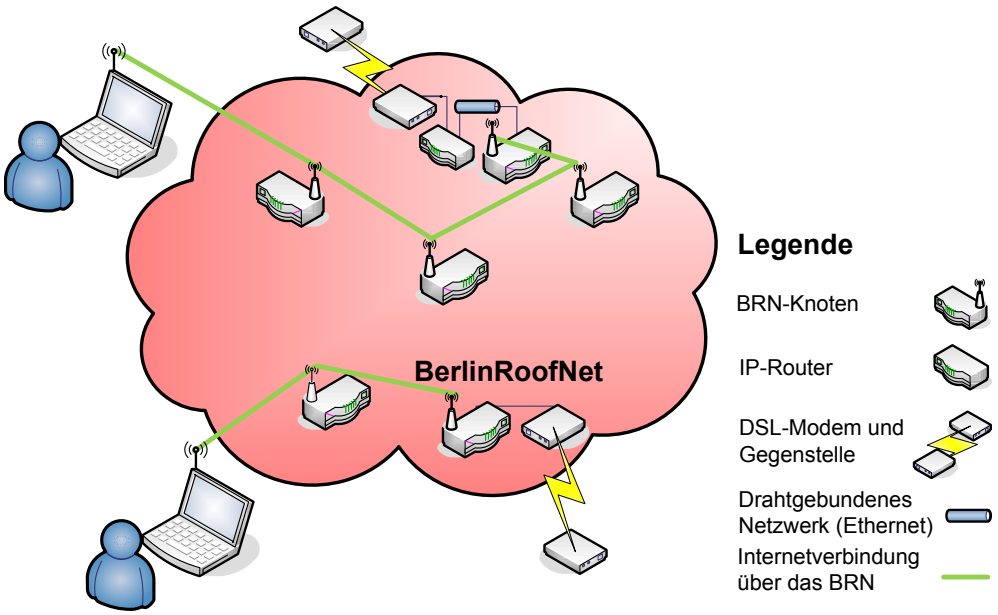



Abbildung 2: BRN aus Client-Sicht

eine Art Dienstleistung aufgefasst werden. Aktuell bieten bereits Anbieter, wie Hotsplots (http://www.hotsplots.de) und sofanet (http://www.sofanet.de) VPN-Zugänge an. Derzeit ist der Fokus dieser Dienste aber die Absicherung des unverschlüsselten Netzwerkverkehrs, wie er häufig bei öffentlichen Internetzugängen insbesondere über WLAN, anzutreffen ist. Zusammengefasst wird durch den Einsatz eines Tunnels das Problem der Verbindungen in einem drahtlosen Netzwerk auf eine Stelle hinter dem Netzwerk verlagert und so im drahtlosen Netzwerk selbst vermieden.

## 1.3 Design und Implementierung

Für das BRN wird die Software vorwiegend mit Click [KMC+00] entwickelt. Click ist eine API zum Entwickeln von Routersoftware. Zu diesem Zweck entwickelt man Elemente in C++, die in einer Click-spezifischen Beschreibungssprache verbunden werden und den Paketfluss als Graph abbilden.

Clienten im BRN können bereits per DHCP konfiguriert werden. Über diesen Weg wird mitgeteilt, wohin Pakete geschickt werden sollen, für die der Client keine Route hat. Zu diesem Zweck gibt es eine spezielle IP-Adresse aus dem Adressraum des BRN. Der IP-Adresse 10.9.0.1 ist die private MAC-Adresse 10:00:00:AA:AA:AA zugeordnet und wird an die Clienten als Gateway verteilt. Diese Adresse steht stellvertretend für den BRN-Knoten mit dem der Client gerade assoziiert ist. Selbst bei einem Weiterreichen

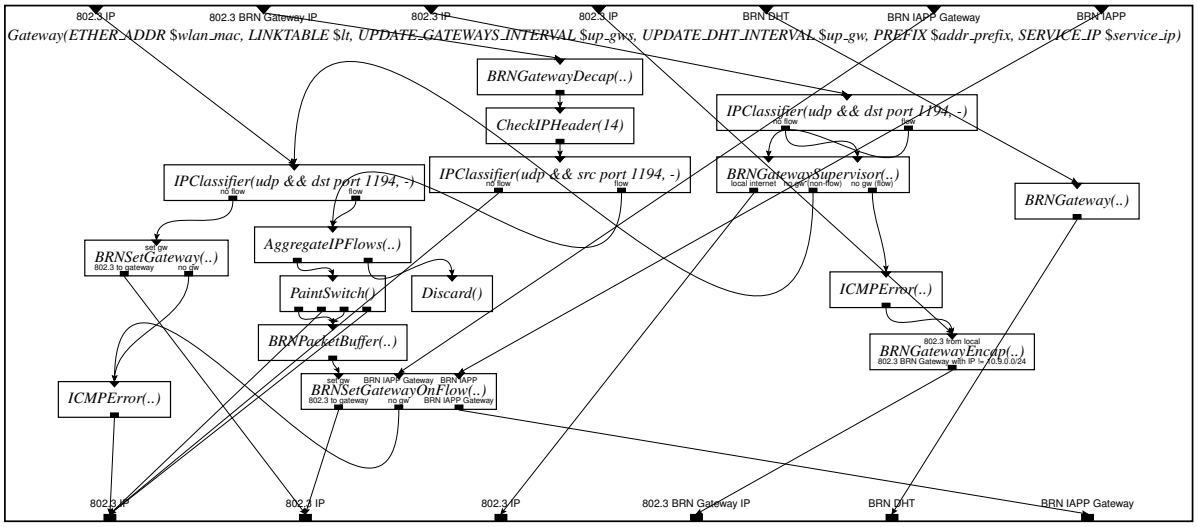



Abbildung 3: Paketfluss zwischen den BRN-Gateway-Elementen

(Handover) eines Clients (auf Schicht 2 bei IEEE 802.11) werden die Pakete immer an den assoziierten BRN-Knoten gesendet. So ist es möglich für jedes Paket beim Eintritt in das BRN ein Gateway zu bestimmen.

Das Element *BRNGateway*, das die Liste aller Gateways vorhält, kümmert sich um die Verbreitung der Informationen mit Hilfe der DHT. Dieses Element implementiert Handler zum Lesen aller bekannten Gateways und zum Setzen des lokalen Gateway. Es wird zur Verbreitung der Informationen und als Speicher verwendet.

Das Element *BRNSetGateway* setzt für einkommende Pakete die Ziel-MAC-Adresse um. Bisher steht die Adresse auf 10:00:00:AA:AA:AA für unser „virtuelles“ Gateway. Das Element bestimmt nun unter Verwendung aller bekannten Gateways (es verwendet dazu das Element *BRNGateway*) ein Gateway und setzt die MAC-Adresse entsprechend.

Ähnlich dazu arbeitet das Element *BRNSetGatewayOnFlow* mit der Besonderheit, dass es zu Paketen die passende Verbindung bestimmt und das Paket an das Gateway schickt, das für diese Verbindung bereits ausgewählt worden war. Um Verbindungen zu erkennen, wird das Element *AggregateIPFlows* verwendet, das in [Koh06] vorgestellt wurde. Zusätzlich überträgt es die bekannten Verbindungen eines Clients beim Weiterreichen zu einem neuen Access Point (AP). So bleiben die Verbindungen selbst bei einem Handover bestehen. Dies ist insbesondere für mobile Clients wichtig.

Das Element *BRNGatewaySupervisor* verhindert das Zustellen von Paketen in Richtung Linux-Kernel, wenn der Knoten kein Gateway ist. Wird also ein Knoten als Gateway bestimmt, der zur Zeit der Ankunft des Pakets kein Gateway ist, filtert dieses Element

die Pakete aus. Handelt sich dabei um Pakete, die nicht verbindungsorientiert sind, so werden sie nicht verworfen, sondern für sie lokal ein neues Gateway ermittelt.

Die Elemente *BRNGatewayEncap* und *BRNGatewayDecap* haben die Aufgabe Antwortpakete in ein zusätzliches Protokoll zu verpacken und auf der Gegenseite wieder auszupacken. So erhält ein Knoten kontinuierlich Informationen über das genutzte Gateway bei bidirektionalen Verbindungen.

Da man einem UDP-Paket nicht ansehen kann, ob der Ziel-Socket im Verbindungsmodus arbeitet, ist es nicht möglich für solche Pakete zu entscheiden, ob sie zu einer Verbindung gehören. Aus diesem Grund werden alle UDP-Pakete, die über den OpenVPN Port 1194 laufen, nicht als Verbindungspakete behandelt.

Ein OpenVPN-Server muss dazu mit der Option „float“ konfiguriert werden, damit er die Absender-IP-Adresse sowie den Absender-Port ignoriert, wenn er die Pakete einer VPN-Sitzung zuordnet. Standardmäßig wird erwartet, dass das Paket einer Sitzung von derselben IP-Adresse sowie Port abgesendet wurde. Leider wird die Option „float“ nicht für Transport Layer Security (TLS) unterstützt und kann nur bei Verwendung statischer Schlüssel genutzt werden. Für die Praxis ist der Einsatz damit sehr eingeschränkt, soll aber als eine mögliche Grundlage für weitere Überlegungen nicht unerwähnt bleiben. Langfristig könnte eine auf Mobile IP basierende Lösung in Betracht gezogen werden und hinsichtlich der Vor- und Nachteile abgewogen werden.

In Abbildung 3 ist die Verschaltung der besprochenen Elemente zu sehen. Es wird anhand des Protokolls UDP und des Ports 1194 (OpenVPN) festgelegt, ob es sich um Pakete einer Verbindung handelt oder nicht. Für Pakete, die nicht verbindungsorientiert sind, wird dann der flexiblere Ansatz verwendet. Es werden also beide Ansätze paketorientiert und verbindungsorientiert kombiniert. So kann ein Nutzer durch Verwendung von OpenVPN verhindern, dass Verbindungen zusammenbrechen, wenn nur ein Gateway von mehreren ausfällt.

## 1.4 Vergleich mit 802.11s

Derzeit befindet sich 802.11s, der Standard zur Erweiterung von 802.11 für Maschennetzwerke, im Standardisierungprozess bei der IEEE. Bisher gab es keinen Standard des IEEE für das drahtlose Verbinden der APs. Übertragungen zwischen den APs erfolgten drahtgebunden über ein Local Area Network (LAN). Das drahtlose Medium wurde lediglich für den Zugang verwendet. Ein AP nimmt die Frames drahtlos entgegen und leitet sie in ein drahtgebundenes Netzwerk weiter. Mit 802.11s können kleine bis mittlere (ca. 32 Knoten) Maschennetzwerke aufgebaut werden. Die Notwendigkeit eines draht-

gebundnenen Netzwerks entfällt damit. Für Protokolle höherer Schichten soll sich ein Maschennetzwerk wie ein LAN verhalten. Maschennetzwerke in 802.11s arbeiten dabei ausschließlich auf der Schicht 2. In 802.11s werden sie als *WLAN Mesh* bezeichnet. Für den Vergleich wurde der Entwurf [80206] von 802.11s verwendet.

Wir wollen das BRN mit der Auswahl für Gateways mit einem WLAN Mesh vergleichen, das seinen Clienten einen Internetzugang bereitstellt. Da die Funktionsweise für das BRN bereits beschrieben wurde, wird besonders auf die Unterschiede zu einem WLAN Mesh eingegangen. In 802.11s-Netzwerken können die Knoten in folgenden Ausprägungen auftreten:

**Mesh Point (MP)** Ein Mesh Point (MP) ist für die Bildung des Maschennetzwerks zuständig. Er baut Links zu benachbarten MPs auf. Gemeinsam führen die MPs das Routing im Maschennetzwerk durch.

**Mesh AP (MAP)** Ein Mesh AP (MAP) umfasst einerseits die Funktionalität eines MPs um am Maschennetzwerk teilzunehmen, andererseits aber auch die Funktion eines APs zur Kommunikation mit 802.11-Stationen.

**Mesh Portal (MPP)** Ein Mesh Portal (MPP) umfasst weitergehende Funktionen. Zusätzlich zur Funktion eines MPs verbindet das MPP das Maschennetzwerk mit einem auf 802.3-basierten Netzwerk (Ethernet).

Aus diesen Bestandteilen wird ein WLAN Mesh gebildet. Als Routingprotokolle werden Hybrid Wireless Mesh Protocol (HWMP) und Radio Aware (RA)-OLSR vorgeschlagen. Die genaue Funktionsweise dieser Routingprotokolle ist für unsere Betrachtung nicht von Interesse. Entscheidend ist, dass sie Pakete durch das Maschennetzwerk transportieren können und an das entsprechende Ziel zustellen. Das Routing stellt optional Unterstützung für netzweite Broadcasts, wie sie aus einem LAN bekannt sind, sowie für Multicasts bereit. Unterstützt das Routing keine Broadcasts bzw. Multicasts, so wird ein einfacher Mechanismus verwendet. Dabei leitet jeder Mesh Point (MP) den Frame weiter, sofern er ihn noch nicht weitergeleitet hatte.

Aus Sicht der Auswahl von Internet-Gateways ist interessant, wie in 802.11s ein MP einen Frame an eine drahtgebundene Station weiterleitet. Er wird dazu über ein Mesh Portal (MPP) verschickt. 802.11s arbeitet bei der Auswahl des MPP ausschließlich auf Schicht 2. Im Gegensatz dazu wird im BRN ein IP-Gateway ausgewählt. Dieser Mechanismus ist nicht mehr auf die Schicht 2 beschränkt. Es gibt noch einen weiteren konzeptionellen Unterschied: Die IP-Gateways sind untereinander gleichwertig, da sie

als Internetzugang verwendet werden und NAT durchführen. Für die Auswahl eines MPP ist jedoch entscheidend, ob die entsprechende Station an den MPP angeschlossen ist. Im Folgenden wird der Auswahlmechanismus von 802.11s erläutert und hinsichtlich der Einsetzbarkeit in Community-Netzwerken im Vergleich zur Lösung für das BRN vorgestellt.

Mit dem *MPP Announcement Protocol* werden den MPs die MPPs bekanntgeben. Die MPPs senden dazu periodisch *Portal Announcement*-Nachrichten aus. Empfängt ein MP so eine Nachricht, so vermerkt er sich den entsprechenden MPP und leitet die Nachricht weiter. In diesen Nachrichten wird jeweils ein Wert für *Metric*, *Hop Count* und *Time to Live* beim Weiterleiten aktualisiert. Über den *Time to Live*-Wert kann die Verbreitung der Nachricht beschränkt werden. Über das Feld *Metric* können die Kosten für den Pfad vom MPP zu den MPs kumulativ übertragen werden. Ähnlich dem *Hop Count* aber für eine eigene Metrik. Erhält nun ein MP ein Frame an eine externe Station, so führt er zuerst eine Suche nach dieser Station im WLAN Mesh durch. Findet er sie nicht (trifft im Falle einer drahtgebundenen/externen Station zu), so überträgt er den Frame an alle ihm bekannten MPPs. Damit erhält auch der zuständige MPP den Frame und stellt ihn der externen Station zu. Im Entwurf des 802.11s-Standards finden sich keine weiteren Verbesserungen für diesen Mechanismus. Die Verwendung des *Metric*-Feldes und die Übertragung an *einen* anstatt aller MPPs sind aber zur Aufwertung des Mechanismus gedacht.

Wir wollen nun betrachten, wie der Zugang zum Internet in einem WLAN Mesh aussieht. Wir gehen davon aus, dass ein DHCP-Server teil des WLAN Mesh ist. Zu Beginn konfiguriert eine Station den Zugang zum Netzwerk via DHCP. Sie bekommt dazu die IP-Adresse des Gateway mitgeteilt. Das Gateway ist mit einem MPP verbunden. Im BRN teilt der DHCP-Dienst die Adresse des „virtuellen“ Gateway aus. Möchte der Client nun ein Paket absenden, für das keine IP-Route bekannt ist, so ermittelt er zu der IP-Adresse des Gateway mit Hilfe von Address Resolution Protocol (ARP) die korrespondierende MAC-Adresse. Es ist zu beachten, dass sowohl ARP als auch DHCP Broadcasts verwenden, was sich in einem Maschennetzwerk als problematisch erweist. Werden keine besonderen Vorkehrungen getroffen, so kommt es zum *Broadcast-Strom-Problem* [NTCS99]. In 802.11s wird der ARP-Request vom MPP weitergeleitet und vom Gateway beantwortet. Der Client schickt nun sein Paket an die ermittelte MAC-Adresse. Das Routing stellt fest, ob sich das Ziel im WLAN Mesh befindet. Da sich das Gateway außerhalb des WLAN Mesh befindet, wird das Paket an alle MPPs gesendet. Im Unterschied dazu wird im BRN ein solches Paket immer vom AP der Station verarbeitet.

Dieser bestimmt ein Gateway und sendet das Paket weiter.

Für die Verwendung von 802.11s in einem Community-Netzwerk wie dem Freifunk-Netz ergeben sich daraus folgende Probleme. Zunächst ist der Mechanismus zum Finden der MPPs noch nicht sehr ausgereift. Gibt es desweiteren mehrere IP-Gateways (jeweils hinter einem MPP), so muss ein Dienst auf höherer Schicht diese IP-Gateways geschickt unter den Stationen verteilen. Ein DHCP-Server könnte je nach Station ein anderes IP-Gateway zurückliefern. Dem DHCP-Server muss dann der Ausfall sowie das Hinzukommen von Gateways mitgeteilt werden. Insgesamt erhöht sich die Komplexität eines DHCP-Dienstes. Die Verwendung eines „virtuellen“ Gateway über eine private MAC-Adresse ist möglich. Dann könnte auf einem MAP das „virtuelle“ Gateway durch ein bekanntes ersetzt werden. Dies ist sinnvoll, um Verbindungen oder gar einzelnen Paketen unterschiedliche Gateways zu zuordnen. Aber keine dieser Funktionen ist Bestandteil von 802.11s.

Im BRN wurden Mechanismen entwickelt, die die oben genannten Probleme lösen. So werden mehrere Gateways unterstützt und in die Auswahl miteinbezogen. Die Gateways können dabei im laufenden Betrieb hinzugefügt und entfernt werden. Für ein Community-Netzwerk sind diese Funktionen sehr wichtig. Interessant ist eine Kombination des Routing mit den Informationen über Gateways. 802.11s bietet bei HWMP in der proaktiven Variante sogenannte *root MPs* an. So könnte der *root MP* ein MPP sein, der das Gateway erreichen kann. Da Benutzer des Netzes vorwiegend das Internet nutzen, ist es sinnvoll über diese Kopplung das Routingprotokoll für diesen Anwendungsfall zu optimieren. HWMP erlaubt aber nur einen *root MP*, was für ein Community-Netzwerk nicht ausreichend sein wird.

## 1.5 Zusammenfassung

Die Arbeit stellt die Grundlagen für die Anbindung von Clients des BRN an das Internet dar. Insbesondere wurde dabei eine Abwägung zwischen der Auswahl von Gateways auf Paketebene im Vergleich zur Auswahl auf Verbindungsebene betrachtet. Dabei wurde festgestellt, dass für die Auswahl auf Paketebene ein zustandsloses Tunnelprotokoll notwendig ist. Als Bestätigung, dass eine Auswahl auf Paketebene möglich ist, wurde OpenVPN mit statischen Schlüsseln verwendet. Neben der Auswahl auf Paketebene wurde auch eine Auswahl auf Verbindungsebene realisiert.

## 1.6 Mögliche zukünftige Entwicklungen

In Zukunft könnten Messungen interessant sein, die das Verhältnis der Last auf das Netzwerk von paketorientierter im Vergleich zu verbindungsorientierter Auswahl von Internet-Gateways untersucht. In diesem Zusammenhang ist auch die vorbereitete Implementierung zur Lastverteilung zu nennen. Ein Ausbau und weitergehende Untersuchung einer Lastverteilung für Internet-Verkehr in drahtlosen Netzwerken könnte zu einer besseren Verteilung der Pakete führen.

Ein geeigneteres Tunnelprotokoll zur Gateway-Auswahl auf Paketebene bringt Vorteile, wenn bspw. ein Gateway ausfällt. Hierbei ist insbesondere von Interesse, dass das eingesetzte Protokoll von vielen Benutzern unterstützt wird. Mobile IP im BRN könnte eine Lösung versprechen. Allerdings ist Mobile IP noch nicht sehr verbreitet.

Eine Verbesserung und Erweiterung des Erkennens von Internet-Gateways ist erstrebenswert. So sollten Internet-Gateways, die durch ein anderes BRN-fremdes drahtloses Netzwerk Internetzugang haben, unterstützt werden. Insgesamt ist ein Ausbau der Auto-Konfiguration eines BRN-Knoten ein weiteres mögliches Ziel, da sich diese Arbeit vorwiegend mit der Auswahl von Gateways beschäftigte.

Um den Verbreitungsmechanismus, der derzeit DHT-basiert ist, hinsichtlich Effizienz zu vergleichen, ist es denkbar eine broadcast-basierte Verteilung zum Zweck des Vergleichs zu implementieren.

Etwas weiter in die Zukunft geschaut, ist es dann vorstellbar, ein neuartiges Routingprotokoll zu entwickeln, das die bekannten Internet-Gateways verwendet. Das Protokoll benutzt diese zusätzliche Infrastruktur zur Verbesserung des Routing. Ebenso könnte das Routing zu Gateways optimiert werden, wie es HWMP in Ansätzen bereits umsetzt.

# 2 Drahtlose VLANs

## 2.1 Einleitung und Motivation

Mit der Einführung von „Virtual APs“ des MadWifi-Treibers [Mad] für Atheros-Chipsätze, ist es möglich auf einer Atheros-Netzwerkkarte mehrere virtuelle APs zu betreiben. Man spricht von „virtuellen APs“, da gleichzeitig mehrere APs mit nur einer Netzwerkkarte betrieben werden können. Es ist möglich für jeden „virtuellen“ AP einen anderen Basic Service Set Identifier (BSSID) zu verwenden. Der Zweck des BSSID wird später von Interesse sein.

Möchte man den Netzwerkverkehr trennen, so konfiguriert man sich virtuelle APs. Dies ist eine einfache Möglichkeit den Netzwerkverkehr bereits auf OSI-Schicht 2 zu trennen. [FON] verwendet diese Funktionalität um zwischen einem öffentlichen und privaten Zugang zu ihrem Router zu unterscheiden. Für ein drahtloses multi-hop Netzwerk ist dies allerdings nicht ausreichend, da die Trennung lediglich auf einem Gerät erfolgt. Wird ein Paket von einem Gerät zum nächsten übertragen, so ist zunächst nicht klar, wie die Trennung gewährleistet wird. Die Unterstützung von virtuellen APs ist im Falle des MadWifi-Treibers lediglich für den Zugang zu einem Knoten ausgelegt.

Im Folgenden wird beschrieben, wie eine netzwerkweite Trennung des Netzwerkverkehrs, die für das BRN implementiert wurde, aussehen kann. Doch zunächst soll das Konzept Virtual Local Area Network (VLAN) näher betrachtet werden. Die Idee von VLANs findet in drahtgebundenen Netzwerken bereits große Anwendung.

Mit VLANs kann ein physikalisches Netzwerk in mehrere logische Netzwerke zergliedert werden. Damit ist es nicht mehr notwendig mehrere physikalische unabhängige Infrastrukturen aufzubauen, was entsprechend kostspielig sein kann. Anstatt also mehrere Kabel verlegen zu müssen, wird ein vorhandenes Kabel logisch geteilt unter Erhaltung der Trennung des Netzwerkverkehrs. Für drahtlose Netzwerke könnte die Vision darin bestehen langfristig eine physikalische Infrastruktur zu betreiben, die entsprechend weitreichend ist, aber dennoch verschiedene Netze logisch bereit stellt. So würden bei einem Stadt weitem drahtlosen Community-Netzwerk einmal die Knoten aufgestellt und es könnten verschiedene logische Netze über das eine physikalische Netze betrieben werden. Verschiedene Communities könnten sich die Hardware teilen. Das ist effizienter als mehrere eigenständige Infrastrukturen aufzubauen. Zudem stören sich mehrere eigenständige Infrastrukturen gegenseitig beim Zugriff auf das gemeinsam genutzte Medium.

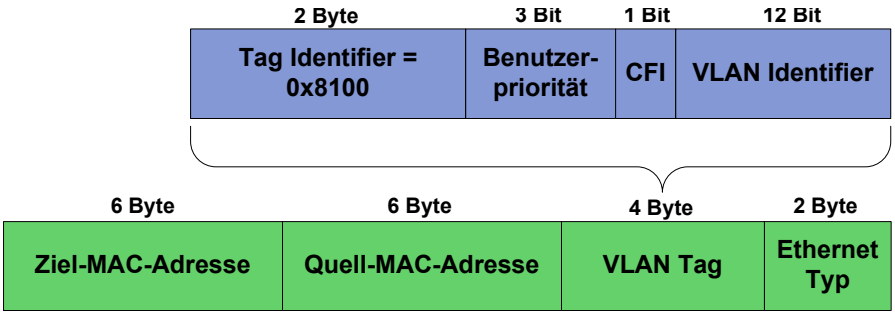



Abbildung 4: 802.1Q-Frame-Format (Ethernet-kodiert)

## 2.2 VLANs im Ethernet

Derzeit sind VLANs besonders stark in Ethernet-basierten Netzwerken verbreitet. Die bekannteste Umsetzung wird im Standard IEEE 802.1Q beschrieben. Der Standard beschreibt die Anpassung des Ethernet-Datenframes zur Unterstützung von VLANs. Ein Ethernet-Header (mit *Ethernet II framing*) besteht aus 14 Bytes. Die ersten 6 Bytes beschreiben die Ziel-MAC-Adresse. Die folgenden 6 Bytes beschreiben die Quell-MAC-Adresse. Die verbleibenden 2 Bytes beschreiben das Protokoll im Datenbereich. Für IPv4 wird der Wert 0x0800 verwendet.

802.1Q erweitert den Ethernet-Header um 4 Bytes. Dabei werden nach der Quell-MAC-Adresse 4 Bytes eingefügt, der sogenannte *VLAN-Tag*. Die ersten 2 Bytes des Tags legen fest, dass es sich um einen VLAN-Frame handelt. Sie sind festgelegt auf 0x8100. Man spricht vom sogenannten *Tag Protocol Identifier*. Die nächsten 3 Bit werden zum Setzen der Benutzerpriorität verwendet (siehe dazu IEEE 802.1p). Das nächste Bit beschreibt die Kodierung von MAC-Adressen im Datenteil des MAC-Frame. Es wird *Canonical Format Indicator (CFI)* genannt. Für Ethernet hat es den Wert 0. Interessant ist das letzte Feld des Tags. Der VLAN Identifier (VID) ordnet dem Frame ein VLAN zu. Das Feld umfasst 12 Bit. Es sind also 4096 verschiedene Werte möglich. Der Wert 0x000 bedeutet, dabei dass der Frame keinem VLAN zugeordnet ist und lediglich die Benutzerpriorität ausgewertet werden soll. Der größte Wert 0xFFF ist reserviert. Zudem gibt es noch den Wert 0x001, der eine herausgehobene Bedeutung hat. Diesen Wert bekommen die Frames, wenn ihnen kein VLAN-Tag explizit zugewiesen wurde (siehe 802.1Q S. 86). In der Abbildung 4 wird die Erweiterung des Ethernet-Header durch 802.1Q veranschaulicht.

Über den VID werden die Frames unterschieden. So kann man einen Switch konfigurieren allen Frames, die über einen bestimmten Port in den Switch geschickt werden,

ein bestimmtes VLAN zu zuordnen. Werden Frames auf Ports hinausgegeben, so wird überprüft, ob der Frame den passenden VID hat.

VLANs haben die folgenden Vorteile:

- Einmalige Verkabelung mit anschließender flexibler Konfiguration

  Durch die logische Trennung der Netze kann dieselbe Verkabelung genutzt werden. Anstatt für jedes Netz eigene Kabel zu verlegen, benutzen alle Netze dieselben Kabel und die Trennung erfolgt logisch. Dies erfordert eine Konfiguration der VLANs durch den Netzwerkadministrator. Das flexible Anlegen und Verwalten von Netzwerken ist der Hauptvorteil von VLANs.

- Beschränkung der Broadcast-Domaine

  Mittlerweile können Netze auf der Schicht 2 sehr groß werden. Sind viele Ethernet-Geräte in dem selben Netz, so verursachen Broadcasts eine sehr hohe Netzlast. Durch VLANs können größere Netze ohne signifikante Performance-Einbußen in kleinere zerlegt werden.

- Prioritäten auf Ebene von Ethernet

  Durch den VLAN-Tag von 802.1Q ist es möglich Prioritäten bereits auf der Schicht 2 zu verwenden. Dadurch kann in Firmennetzwerken, die ihr Netz für Voice over IP (VoIP) verwenden wollen, bereits unterhalb der IP-Schicht Netzwerkverkehr prioritisiert werden.

Da sich diese Arbeit mit VLANs in drahtlosen Netzwerken beschäftigt, wollen wir nun den möglichen Einfluss von VLANs für drahtlose Netzwerke genauer untersuchen.

## 2.3 VLANs in drahtlosen Netzwerken

Die bisher am weitesten verbreitete Technologie, die in drahtlosen Netzwerken für Communities eingesetzt wird, basiert auf IEEE 802.11. Im Vergleich zum drahtgebundenen Ethernet, wo man sich mit dem Netz durch das Einstecken eines Ethernet-Kabels in einen Ethernet-Port verbindet, weicht das Verbinden mit einem 802.11-Netzwerk stark ab. Zunächst sucht eine 802.11-Station nach drahtlosen Netzwerken. Im Infrastruktur-Modus folgt danach eine Authentifikation gegenüber dem AP und im Anschluss die Assoziierung mit dem AP. Durch die Assoziierung wird die Station logisch mit dem AP verbunden. Der Moment der erfolgreichen Assoziierung ist mit dem Einstecken des Kabels in einen Port bei Ethernet vergleichbar [Gas05].

Durch die Einführung von VLANs in drahtlosen Netzwerken ist es möglich verschiedene virtuelle Netzwerke in einem physikalischen Netzwerk zu betreiben. Zudem können den verschiedenen VLANs unterschiedliche Prioritäten zugeordnet werden, so dass ein Notfall-Netz höchste Priorität bekommt. Im Unterschied zum Feld für Prioritäten im IP-Header, das durch eine Applikation gesetzt wird, kann dieses Feld im Netzwerk selbst gesetzt werden. So ist es vorstellbar, dass ein Betreiber für ein bestimmtes Netz die Latenz von Paketen minimiert. Insbesondere erfolgt das Setzen der Priorität erst beim Eintritt des Pakets in das Netzwerk. So muss nicht zur Entwicklungszeit einer Applikation entschieden werden, welche Priorität verwendet werden soll. Für Endgeräte ist ein Setzen der Prioritäten meist gar nicht möglich. Zusammengefasst bestimmt der Netzwerkbetreiber, welche Prioritäten er unterstützt und setzt diese zur Laufzeit um.

Die Beschränkung von Broadcasts kann ein erstrebenswertes Ziel sein. Allerdings ist dabei auf die Umsetzung von Broadcasts in drahtlosen Netzwerken acht zu geben. Denn im Unterschied zu Ethernet teilen sich alle VLANs dasselbe Medium.

Der Hauptvorteil besteht jedoch in der Trennung des Netzwerksverkehrs. Der Netzwerkverkehr eines VLAN bleibt in diesem VLAN. In drahtgebundenen Netzwerken wird der Schutz eines Netzwerks durch physikalischen Schutz erreicht. Gelingt es einem Angreifer nicht an die Ports eines VLAN zu gelangen, so hat er keine Möglichkeit den Netzwerkverkehr zu belauschen. So wird Vertraulichkeit und Integrität sichergestellt, in der Annahme, dass kein Angreifer Zugriff auf das Netzwerk erlangt.

In drahtlosen Netzwerken stellt sich diese Situation schwieriger dar. Es gibt keinen physikalischen Zugriffsschutz auf ein gemeinsam genutztes Medium, wie es bei 802.11 verwendet wird. Zur Sicherstellung von Vertraulichkeit und Integrität ist die Verwendung von kryptographischen Protokollen notwendig. Für 802.11-basierte Netzwerke sollte dies durch Wired Equivalent Privacy (WEP) erreicht werden. Wie der Name bereits nahe legt, sollte die Sicherheit dabei vergleichbar zu der in kabelgebundenen Netzen sein. WEP konnte diese Ziele allerdings nicht verwirklichen, da früh Angriffe bekannt und schrittweise ausgebaut wurden. So kann mittlerweile ein durch WEP geschütztes Netz mit großer Wahrscheinlichkeit in weniger als einer Minute gebrochen werden [TWP07].

## 2.4 VLANs im BRN

Im Folgenden soll die Implementierung von VLANs für das BRN erläutert werden. Zunächst werden dazu die Anforderungen beschrieben.

### 2.4.1 Anforderungen

Das BRN arbeitet aus Sicht der Stationen im Infrastruktur-Modus. Es werden Beacons ausgesendet und die Stationen durchlaufen eine Authentifikation und eine Assoziation um sich mit dem BRN zu verbinden. In einem Beacon sind dabei die Netzwerk-relevanten Informationen enthalten.

Besonders wichtig ist in diesem Zusammenhang der Service Set Identifier (SSID). Analog zum Ethernet muss unterschieden werden mit welchem „Port“ eine Station verbunden ist. Der SSID dient als Kennung für ein drahtloses Netzwerk. Wir führen weitere solche Kennungen ein, um einer Station „quasi“ mehrere Ports anzubieten zu können. Die Netzwerkkennung wird periodisch über Beacons verteilt. Das Versenden von Beacons ermöglicht einer Station passiv drahtlose Netzwerke zu entdecken. Für die Unterscheidung von VLANs über den SSID ist es denkbar für die „virtuellen“ SSIDs ebenfalls Beacons zu versenden. In der Implementierung für das BRN wurde diese Entscheidung aber nicht getroffen, da dies pro VLAN zusätzliche Bandbreite verbraucht. Die Anzahl der Beacons, die ein AP aussendet, wäre linear abhängig von der Anzahl der VLANs. Bei einer großen Anzahl von VLANs würde dementsprechend Bandbreite an jedem Knoten verbraucht werden. Deshalb muss eine Station einen aktiven Scan durchzuführen, sofern sie sich mit einem drahtlosen VLAN verbinden will. Für das Verständnis von aktiven und passiven Scans in 802.11 sei auf [Gas05] oder den Standard selbst verwiesen. Zusammengefasst wird also der „normale“ SSID des BRN über Beacons bekannt gegeben, hingegen werden „virtuelle“ SSIDs, d.h. SSIDs von drahtlosen VLANs, nur über einen aktiven Scan auffindbar.

Weiterhin gibt es einen Mechanismus um VLANs anzulegen. Ist ein VLAN angelegt, so können sich drahtlose Stationen im gesamten BRN über den „virtuellen“ SSID mit dem Netz verbinden. Lediglich Stationen in dem selben VLAN können sich per Unicast erreichen. VLANs können über einen ähnlichen Mechanismus gelöscht werden.

Zudem soll es ein spezielles VLAN geben, das ausschließlich lokal ist, d.h. Frames dieses VLAN werden nicht geroutet. Es dient dazu sich sicher mit einem Knoten zu verbinden und Geräte wie Drucker auf dem Ethernet erreichen zu können. Im Grunde handelt es sich um eine Wireless-Ethernet-Bridge zwischen dem lokalen VLAN und dem drahtgebundenen Netzwerk eines Knotens. Das lokale VLAN soll lediglich mit WEP verschlüsselt werden. Eine notwendige sichere Verschlüsselung ist nicht Fokus der Arbeit.

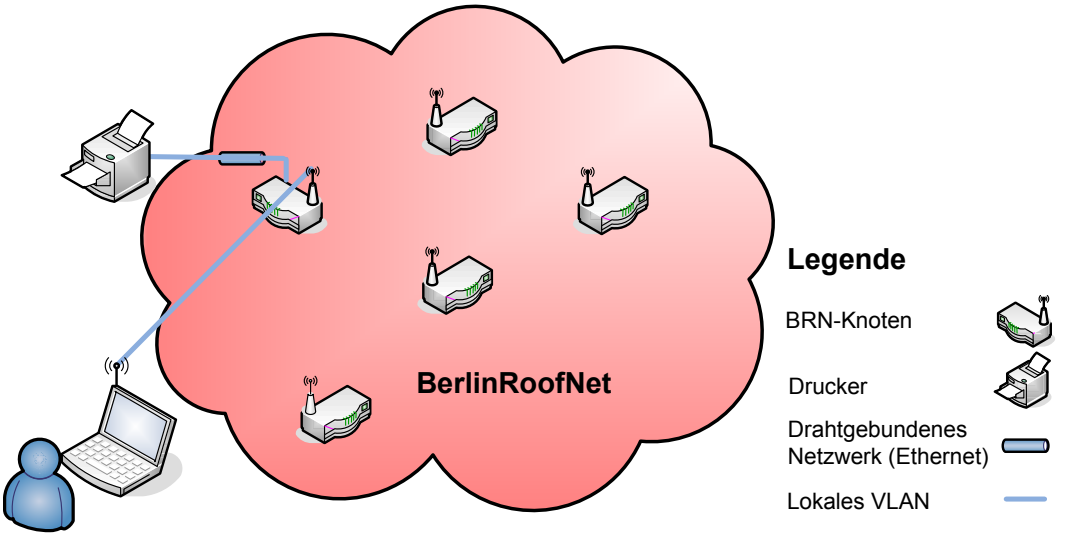



Abbildung 5: Lokales VLAN

### 2.4.2 Implementierung

**SSID eines VLANs** Ein VLAN im BRN wird durch einen besonderen SSID benannt. Es soll nicht möglich sein VLANs mit beliebigen SSIDs anzulegen, da dies zu Verwirrung mit anderen drahtlosen Netzwerken führen kann. Ein VLAN im BRN hat immer einen Namen nach folgender Konvention 'String@SSID', wobei 'String' eine Zeichenkette bezeichnet, die nur Zeichen enthalten darf, die ein SSID nach 802.11 enthalten darf. '@' stellt ein Trennzeichen dar und 'SSID' steht für den SSID des BRN. Verwendet das BRN beispielsweise den SSID 'MyBRN', dann ist 'MyVLAN@MyBRN' ein erlaubte Kennung für ein VLAN im BRN.

Jedem VLAN ist damit ein Name zugeordnet und über den Namen kann sich eine Station mit einem VLAN verbinden. Im Folgenden soll der SSID des BRN 'BRN' sein.

**Anlegen und Löschen eines VLANs** Das Anlegen eines VLAN geschieht über den Aufruf eines Click-Handlers. Zur Vereinfachung wurde ein rudimentäres Web-Interface entwickelt. Als Eingabe wird eine Zeichenkette erwartet und per Formular an den Click-Handler weitergereicht. Wird z.B. 'MyVLAN' eingetragen so wird das VLAN 'MyVLAN@BRN' angelegt.

Wenn ein VLAN angelegt wird, so wird der Name des VLAN, sowie der VID in der DHT des BRN gespeichert. Zunächst wird dazu zufällig ein VID ermittelt. Es wird probiert diesen VID in der DHT des BRN einzutragen. Schlägt dies fehl, weil der VID schon

Benutzung ist, so wird ein neuer VID zufällig ermittelt und der Vorgang wiederholt. Unter der VID wird dann der Name des VLAN hinterlegt. Jetzt haben wir einen Eintrag in der DHT, der einer VID ein VLAN zuordnet. Nun wird umgekehrt zu dem Namen der VID eingetragen. Schlägt dies fehl, weil das VLAN schon in Benutzung ist, so wird der bereits angelegte Eintrag für den VID gelöscht. Das VLAN konnte in diesem Fall nicht erfolgreich angelegt werden.

Zum Löschen eines VLAN wird zuerst der Eintrag mit dem Namen als Schlüssel gelöscht. Er liefert den VID des VLAN zurück. Anschließend wird zu dem VID der Name gelöscht.

**Verbinden mit einem VLAN** Für die VLANs werden keine Beacons versendet. Folglich muss die Station aktiv nach dem VLAN suchen. Sie sendet dazu *Probe Requests* aus, die als SSID z.B. 'MyVLAN@BRN' enthalten. Normalerweise würde das Click-Element *BeaconSource* nicht mit einem *Probe Response* für diese Kennung antworten, da es sich lediglich für den SSID 'BRN' zuständig fühlt. Die *BeaconSource* wurde dahingehend erweitert das Element *BRNVLAN* über bekannte VLANs abzufragen und entsprechende Anfragen zu beantworten. Dazu erfolgt im Hintergrund eine DHT-Abfrage für das entsprechende VLAN. Die BeaconSource beantwortet den *Probe Request* der Station für das Netz 'MyVLAN@BRN' mit einem *Probe Response*. Die Station weiß nun, dass das gesuchte VLAN existiert. Beim Durchlaufen der Kanäle und Testen auf die SSID verbringt eine Station eine bestimmte Zeit pro Kanal. Im Standard wird diese Zeit durch die Werte *MinChannelTime* und *MaxChannelTime* bestimmt. Die Werte sind im Standard nicht festgelegt. Durch die Anfrage an die DHT, ist es möglich, dass die Station bereits zum nächsten Kanal gewechselt ist, wenn die Antwort der DHT eintrifft. In diesem Fall würde die Station das VLAN nicht finden. Ein erneutes Scannen kann durch den Benutzer ausgelöst werden. Im Falle des MadWifi-Treibers wird solange gesucht bis das Netzwerk gefunden wurde oder die Suche abgebrochen wird.

Da im BRN eine offene Authentifizierung verwendet wird, d.h. jede Station wird erfolgreich authentifiziert, muss für die Authentifikation keine Anpassung vorgenommen werden.

Anschließend führt die Station mit dem VLAN 'MyVLAN@BRN' eine Assoziierung durch. Diese würde fehlschlagen, da das Click-Element *BRNAssocResponder* das Netz mit dem SSID 'MyVLAN@BRN' nicht kennt und folglich die Assoziierung zurückweist. Daher wurden hier Anpassungen vorgenommen, so dass der *BRNAssocResponder* das Element *BRNVLAN* konsultiert um festzustellen, ob eine Assoziierung möglich ist. Nach

erfolgreicher Assoziierung wird eine Station in dem Element *AssocList* gespeichert. Es werden so alle Stationen und ihr VLAN erfasst.

**Kommunikation in einem VLAN** Eine Station konfiguriert sich meist per DHCP. Da das BRN einen verteilten DHCP-Dienst zur Verfügung stellt, sollte dieser für jede Station unabhängig vom ihrem VLAN nutzbar sein. Es wäre es möglich, für jedes VLAN einen (virtuellen) DHCP-Dienst bereit zu stellen. Anstatt den DHCP-Dienst dahingehend anzupassen, wird der DHCP-Dienst weiterhin als *ein* Dienst betrachtet und Dienste sind für alle Stationen nutzbar. Ein weiterer wichtiger Dienst im BRN ist ARP. Grundlegende Dienste sind also unabhängig vom VLAN und können von jeder Station in Anspruch genommen werden. Sobald die „normale“ Kommunikation in einem VLAN erklärt ist, wenden wir uns der Einbindung der Dienste zu.

Im Nachfolgenden wird häufig der Weg eines Frame durch die Click-Konfiguration beschrieben. Dabei werden nicht alle Elemente erwähnt, die von dem Frame durchlaufen werden, sondern lediglich die, die für die Funktionsweise der VLANs von Interesse sind.

Sendet eine Station ein *802.11-Data-Frame* zum AP, so wird dieser vom Click-Element *WifiDecap* in einen Ethernet-Frame umgewandelt. Dieser Ethernet-Frame wird durch das Element *VLANEncap* in einen 802.1Q-Frame konvertiert, d.h. einen Ethernet-Frame mit VLAN-Tag. Zunächst hat der VID den Wert 0. Anschließend setzt das Element *BRNVLANTag* den richtigen VID. Zunächst schlägt es dazu in der *AssocList* nach mit welchem SSID die Station verbunden ist, anschließend schlägt es in dem Element *BRNVLAN* den passenden VID nach und setzt ihn entsprechend als Wert in dem Frame. Der Frame wird nun vom Routing des BRN zu dem Knoten übertragen, an dem die Ziel-Station assoziiert ist. Auf diesem Knoten passiert der VLAN-getaggte Frame das Element *BRNCheckVLAN*. Dieses Element ermittelt ausgehend von der MAC-Adresse der Ziel-Station das entsprechende VLAN. Zu dem VLAN bestimmt es nun den VID und vergleicht diesen mit der VID im Frame. Stimmen sie überein, so passiert der Frame das Element. Andernfalls wird er verworfen. Hat der Frame das Element erfolgreich passiert, so entfernt das Element *VLANDecap* den VLAN-Tag und der Frame durchläuft schließlich das Element *WifiEncap*, dass den Frame in einen 802.11-konformen Frame konvertiert.

Um die Unterstützung der Dienste zu erklären, ist nun die Grundlage gelegt. Kommt also im Besonderen ein DHCP-Paket von einer Station an, so sind die Schritte analog bis zum Zustellen des Frame zum DSR. Anstatt den Frame dem DSR zu übergeben, wird er an den DHCP-Server gereicht. Da der DHCP-Server aber keine VLAN-getaggten Frames kennt, speichern wir uns mit dem Element *StoreVLAN* den VID zu der Quell-

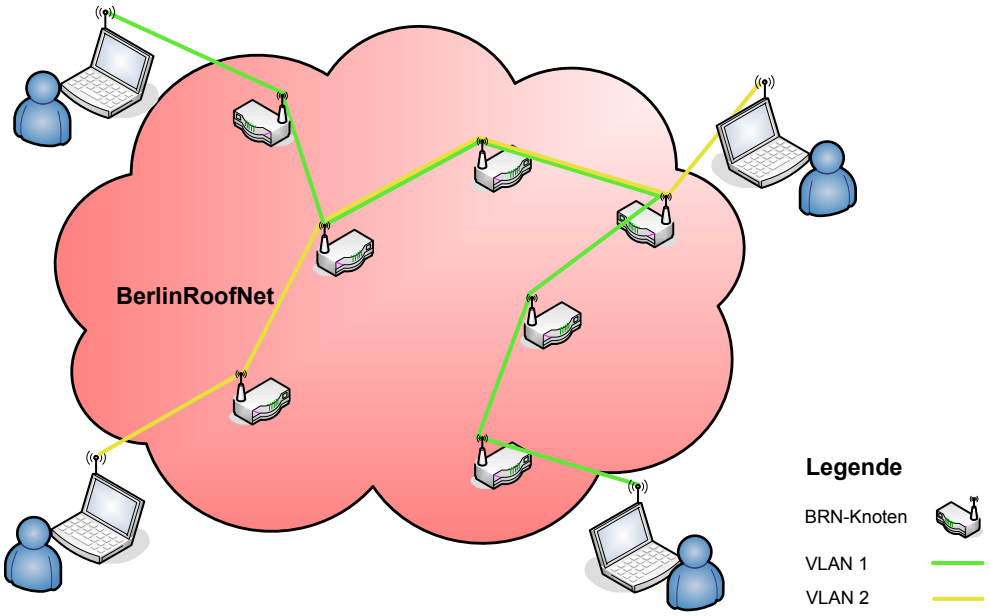



Abbildung 6: Zwei VLANs im BRN

MAC-Adresse des Frame. Danach entfernt das Element *VLANDecap* den Tag und der Frame wird an den DHCP-Server gereicht. Die Antworten von Diensten, also auch die des DHCP-Server, durchlaufen das Element *VLANEncap* und anschließend *RestoreVLAN*. *RestoreVLAN* ermittelt anhand der Ziel-MAC-Adresse den VID und schreibt ihn in den VLAN-Frame. So wird der ursprüngliche VID in den Frame geschrieben.

**Lokales VLAN** Zusätzlich wurde ein herausgestelltes VLAN implementiert. Das lokale VLAN hat einen Namen nach der bereits eingeführten Konvention, also z.B. 'local@BRN'. Das lokale VLAN wird durch WEP geschützt, was aus Sicherheitsaspekten nicht als ausreichender Schutz gewertet werden kann. Es soll lediglich die prinzipielle Möglichkeit eines solchen Schutzes verdeutlichen.

Dem lokalen VLAN ist statisch der VID 2 zugeordnet. Verschlüsselte 802.11-Frames passieren zunächst das Element *WepDecap*, welches den Frame entschlüsselt. Dann durchläuft er die Elemente *WifiDecap*, *VLANEncap* und *BRNTagVLAN*. Wird ein mit der VID 2 getaggter VLAN Frame dem DSR zugestellt, so wird dieser durch das Element *CheckVLAN* verworfen. Genauer gesagt, ist das Element *CheckVLAN* vor dem DSR so konfiguriert, dass ein Frame mit der VID 2 verworfen wird. Weiterhin befindet sich ein solcher Test vor dem Ausgang zu den Ethernet-Ports eines Knotens. Damit wird verhindert, dass Frames die nicht zum lokalen VLAN gehören, auf das Ethernet geben

werden. Umgekehrt werden Frames von Ethernet-Ports mit der VID 2 getaggt. Wird ein Frame an eine drahtlose Station zugestellt, so wird er zuvor verschlüsselt, falls er den VID 2 hat. Er wird dann durch das Element *WepEncap* geleitet.

Bisher wurde die Ethernet-Netzwerkkarte der BRN-Knoten noch nicht für Ethernet-Stationen benutzt. Um dies zu ermöglichen wurde das *EtherSwitch*-Element verwendet, welches sich die angeschlossenen Ethernet-Stationen merkt. Es ist in diesem Sinne analog zu der *AssocList*, die die drahtlosen Stationen speichert. So ist es möglich festzustellen, ob eine Station per Ethernet mit einem Knoten verbunden ist.

**Verteilung der Informationen** In diesem Abschnitt soll die Art der Verteilung der Informationen, die für die VLAN-Funktionalität verwendet wird, besprochen werden.

Für die Kommunikation in VLANs im BRN liegen die Informationen an unterschiedlichen Orten vor. Prinzipiell lassen sich drei Arten unterscheiden:

- Lokal

  Lokale Informationen umfassen all das, was ausschließlich lokal vorliegt und nicht verteilt gespeichert wird. Lediglich der Knoten selbst hat Zugriff auf diese Informationen.

- Direkt im Frame

  Informationen, die direkt in den Frame eingefügt werden, fallen in diese Kategorie.

- Verteilt

  Als verteilt sollen die Informationen angesehen werden, die in der DHT gespeichert werden.

Die Zuordnung einer Station zu einem VLAN wird ausschließlich lokal gespeichert. Der Name eines VLAN und seine VID hingegen werden verteilt in der DHT gespeichert. Die Information, zu welchem VLAN ein Frame gehört, d.h. seine VID, steht in dem Frame selbst, wie es in 802.1Q vorgeschlagen wurde.

Würde man die derzeit lokal gehaltene Information zu dem VLAN einer Station verteilen, so wäre es auch nicht notwendig, die Information an ein Frame zu binden. Dies soll hier lediglich eine andere mögliche Implementierung aufzeigen. Dabei würde die Verteilung der Information komplexer werden und mehr Bandbreite aufgewendet. Die Information an den Frame zu binden, ist sehr nahe am 802.1Q-Standard, aber womöglich nicht optimal für drahtlose Netzwerke.

## 2.5 Einschränkungen der Implementierung

Aufgrund der an 802.1Q-orientierten Lösung ist es für einen Knoten nicht möglich festzustellen, ob das Ziel in dem VLAN des Absenders ist. Deshalb kommt es zu Übertragungen im Netzwerk, die vom letzten Hop verworfen werden, weil erst dieser in der Lage ist, zu entscheiden, ob das Ziel im passenden VLAN ist. Es ist aber nicht zu erwarten, dass allzu viele Pakete unnötig übertragen werden. Da der Sender keine Antwort auf seine Pakete erhält, wird er nach einer gewissen Zeit den Versuch aufgeben.

Ließe sich der *ARP-Response* des ARP-Dienstes unterbinden, so wäre dies eine Möglichkeit nutzlose Übertragungen für IP-basierte Protokolle zu vermeiden. Aber auch dazu ist es notwendig festzustellen, ob eine Ziel-Station im selben VLAN wie die Quell-Station ist ohne den Frame zu übertragen. In der aktuellen Implementierung beantwortet der ARP-Dienst Anfragen für Stationen, die nicht im selben VLAN sind. Ebenso ist es nicht möglich IP-Adressen aus unterschiedlichen Adressräumen für unterschiedliche VLANs zu verteilen, da der DHCP-Dienst die VLANs nicht kennt.

In VLANs werden normalerweise Broadcasts nicht über VLAN-Grenzen hinweg an Stationen zugestellt. Im BRN kommt es aber dazu, da eine Station anhand der BSSID und anhand der Destination Address (DA) eines 802.11-Frame entscheidet, ob der Frame an sie adressiert ist. Im Falle eines Broadcasts ist die DA gleich der Broadcast-MAC-Adresse also 'FF:FF:FF:FF:FF:FF'. Da jedes VLAN dieselbe BSSID hat, wird der Frame von jeder Station unabhängig vom VLAN angenommen. Um das Problem zu beheben, muss der BSSID für jedes VLAN unterschiedlich sein. Wäre dies der Fall, so würde der Treiber lediglich Broadcasts für das passende VLAN weiterverarbeiten. In dieser Variante hat jedes VLAN eindeutig einen BSSID zugeordnet, der beim aktiven Scan einer Station über den *Probe Response* mitgeteilt wird. Der BSSID muss dabei nur lokal eindeutig sein. Es muss nicht einmal jedes VLAN an jedem Knoten im Netzwerk denselben BSSID haben. Wichtig ist nur, dass eine Station lokal unterscheiden kann, ob der Frame für sie ist. Dabei ist zu beachten, dass die Station nicht einen anderen AP mit dem selben BSSID sieht, denn dann wäre unklar mit welchem AP sie nun assoziiert ist. Beide würden sich für sich für die Station zuständig fühlen.

Bei der Verwendung eines BSSID pro VLAN muss zudem der bereits implementierte Handover und das damit verbundene Inter-Access-Point Protokoll angepasst werden, da nun bei einem Handover dem neuen AP ein BSSID mitgeteilt werden kann, der nicht bekannt sein muss. Denn bisher ist der BSSID die MAC-Adresse der drahtlosen Netzwerkkarte des Knotens. Zudem benötigt man einen Mechanismus der neue BSSIDs generieren kann und dabei Konflikte mit bestehenden anderen APs unterbindet.

Weiterhin wird das Problem Broadcast-basierter Protokolle für drahtlose Netzwerke meist separat gelöst, da ein naiv implementierter netzweiter Broadcast zum *Broadcast-Storm-Problem* [NTCS99] führt. Gerade deshalb wird das Broadcast-basierte ARP im BRN über eine DHT implementiert. Broadcast-basierte Protokolle sollten ohne besondere Vorkehrungen gemieden werden. Aus diesem Grund sind Broadcasts im BRN (außer für die erwähnten Dienste DHCP und ARP) derzeit abgeschaltet.

Für VLANs ist aber eine Unterstützung von VLAN-weiten Broadcasts z.B. per Multicast denkbar. Derzeit wird im BRN nur Unicast-Routing via DSR unterstützt.

Vom Standpunkt der Sicherheit ist die Implementierung einer sicheren Verschlüsselung eventuell in Verbindung mit einer Erweiterung auf netzwerkweite VLANs wünschenswert. Eine brauchbare Lösung sollte auf Wi-Fi Protected Access (WPA) basieren. Dabei ist es unter Umständen sogar möglich, die Ver- und Entschlüsselung lediglich auf den Stationen durchführen zu lassen. So würden die Knoten von aufwendigen kryptographischen Berechnungen verschont. Hierbei muss sich besonders Gedanken über die Verteilung der Schlüssel, sowie der gesamten Sicherheitsarchitektur gemacht werden.

Um die Konfiguration der VLANs zu vereinfachen, könnte das Anlegen eines VLAN schon beim aktiven Scannen nach einem SSID, die der Konvention genügt, angelegt werden. Zudem würde ein verbessertes Entfernen der VLANs den Konfigurationsaufwand verringern. Insgesamt würde sich die Verbesserung von der derzeit manuellen hin zu einer automatisierten Konfiguration bewegen.

## 2.6 Unterschiede zu 802.11s

Der Entwurf von 802.11s vom November 2006 befasst sich im Abschnitt 11A.3.5.3 unter dem Titel „VLAN support in a WLAN Mesh“ mit der Unterstützung von VLANs in 802.11s. Es wird vorgeschlagen 802.1Q durch den Subnetwork Access Protocol (SNAP)-Header, einer Erweiterung des Logical Link Control (LLC)-Header, zu unterstützen. Anstatt VLAN-Tags in den Ethernet-Header zu kodieren, wird der Tag in dem SNAP-Header verpackt, wie es nach 802.1Q ebenfalls möglich ist. Die Begründung dafür ist, dass so das Format des 802.11-MAC-Header nicht angepasst werden muss. Insgesamt können dann mit 802.11s VLAN-getaggte Frames durch ein WLAN Mesh transportiert werden. Der Standard beschreibt nur, dass die VLAN-Tags von einem MP zu einem MPP erhalten bleiben. Das MPP konvertiert den 802.11s-Frame in einen 802.3-Frame. Dabei bleibt der SNAP-Header unberührt und kann von nachfolgenden Geräten ausgewertet werden. Wird ein VLAN-Frame von einer drahtlosen Station zu einer anderen verschickt, so bleiben die Tags ebenfalls durch obiges Schema erhalten. Das Setzen so-

wie die Kontrolle der VLAN-Tags wird nicht vom Standard behandelt und ist damit nur durch 802.1Q für drahtgebundene Stationen erklärt. Für eine drahtlose Station wird nicht erklärt, wie sie sich mit einem VLAN verbindet und wie sichergestellt wird, dass nur Stationen des selben VLAN Frames austauschen können. Somit werden nur die VLANs drahtgebundener Stationen über ein WLAN Mesh verbunden. Es gibt in diesem Sinne keine drahtlosen VLANs. Der Fokus von 802.11s liegt in der Erhaltung der Information für drahtgebundene VLANs. Die vorgestellte Lösung ordnet drahtlosen Stationen ein VLAN zu und stellt sicher, dass die Frames einer Station in ihrem VLAN bleiben und dieses nicht verlassen. Im Unterschied zu 802.11s entscheidet nicht die Station selbst über ihre Zugehörigkeit zu einem VLAN. Durch den Ausbau der Authentifikation nach 802.11 oder der Verschlüsselung kann sichergestellt werden, dass sich Stationen nicht mit beliebigen VLANs verbinden. Für das lokale VLAN wurde dies exemplarisch durchgeführt.

## 2.7 Zusammenfassung

Mit der vorliegenden Implementierung von VLANs im BRN ist ein Vorschlag für drahtlose VLANs vorgelegt worden, der sich an 802.1Q orientiert. Dies ist aus technischen Gründen nicht notwendig. Vorteilhaft ist aber die mögliche Integration mit Ethernet durch eine Anpassung der Ermittlung von VIDs eines VLAN. Die Bestimmung einer VID muss in Einklang mit der Vergabe von VIDs für das Ethernet erfolgen. Der Vorschlag erlaubt es drahtlose Stationen einem VLAN über virtuelle SSIDs zu zuordnen. In 802.11s ist eine solche Funktionalität nicht vorgesehen. Für den Benutzer ist das Verbinden mit einem drahtlosen VLAN mit der Standardsoftware zum Verbinden mit 802.11-basierten Netzwerken möglich und Bedarf keiner weiteren Software. Er kann seine „gewohnte“ Software verwenden. Zur Verwaltung der drahtlosen VLANs wurden einfache Mechanismen zum Anlegen und Löschen von VLANs auf Basis der vorhandenen DHT entwickelt. In Bezug auf die Sicherheit eines VLAN wurde wenig Aufwand betrieben. Den Schutz von Vertraulichkeit und Integrität von drahtlosen VLANs sollte in Einklang mit 802.11i erfolgen, geht allerdings über den Rahmen dieser Arbeit hinaus.

## Literatur


[80206] *IEEE P802.11s/D1.00*. November 2006

[BABM05] Bicket, John ; Aguayo, Daniel ; Biswas, Sanjit ; Morris, Robert: Architecture and Evaluation of an Unplanned 802.11b Mesh Network. In: *Mobicom*, 2005

[BRN] *Berlin RoofNet*. `http://www.berlinroofnet.de`

[CABM03] Couto, Douglas S. J. D. ; Aguayo, Daniel ; Bicket, John ; Morris, Robert: A high-throughput path metric for multi-hop wireless routing. In: *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*. New York, NY, USA : ACM Press, 2003. – ISBN 1–58113–753–2, S. 134–146

[FC] Freifunk-Community: *The OLSR.org story*. `https://www.open-mesh.net/misc/optimized-link-state-routing-deamon/olsr-story.txt`

[FON] *FON Community*. `http://www.fon.com`

[Gas05] Gast, Matthew S.: *802.11 wireless networks*. 2. Auflage. O'Reilly, 2005

[GHP+04] Ghassemian, Mona ; Hofmann, Philipp ; Prehofer, Christian ; Friderikos, Vasilis ; Aghvami, Hamid: Performance Analysis of Internet Gateway Discrovery Protocols in Ad Hoc Networks. In: *Wireless Communications and Networking Conference (WCNC)*, IEEE, 2004, S. 120–125

[JMB01] Johnson, David B. ; Maltz, David A. ; Broch, Josh ; Perkins, Charles E. (Hrsg.): Addison-Wesley, 2001. – 139–172 S. `http://www.monarch.cs.rice.edu/monarch-papers/dsr-chapter00.ps`. – DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks

[KMC+00] Kohler, Eddie ; Morris, Robert ; Chen, Benjie ; Jannotti, John ; Kaashoek, M. F.: The Click modular router. In: *ACM Transactions on Computer Systems* Bd. 18(3), 2000, 263–297

[Koh06] Kohler, Eddie: Click for measurement / UCLA Computer Science Department. Version: February 2006. `http://www.cs.ucla.edu/~kohler/pubs/kohler06click.pdf`. 2006. – Forschungsbericht

[Mad] *MadWifi*. `http://www.madwifi.org`

[MIT] *MIT Roofnet*. `http://pdos.csail.mit.edu/roofnet`

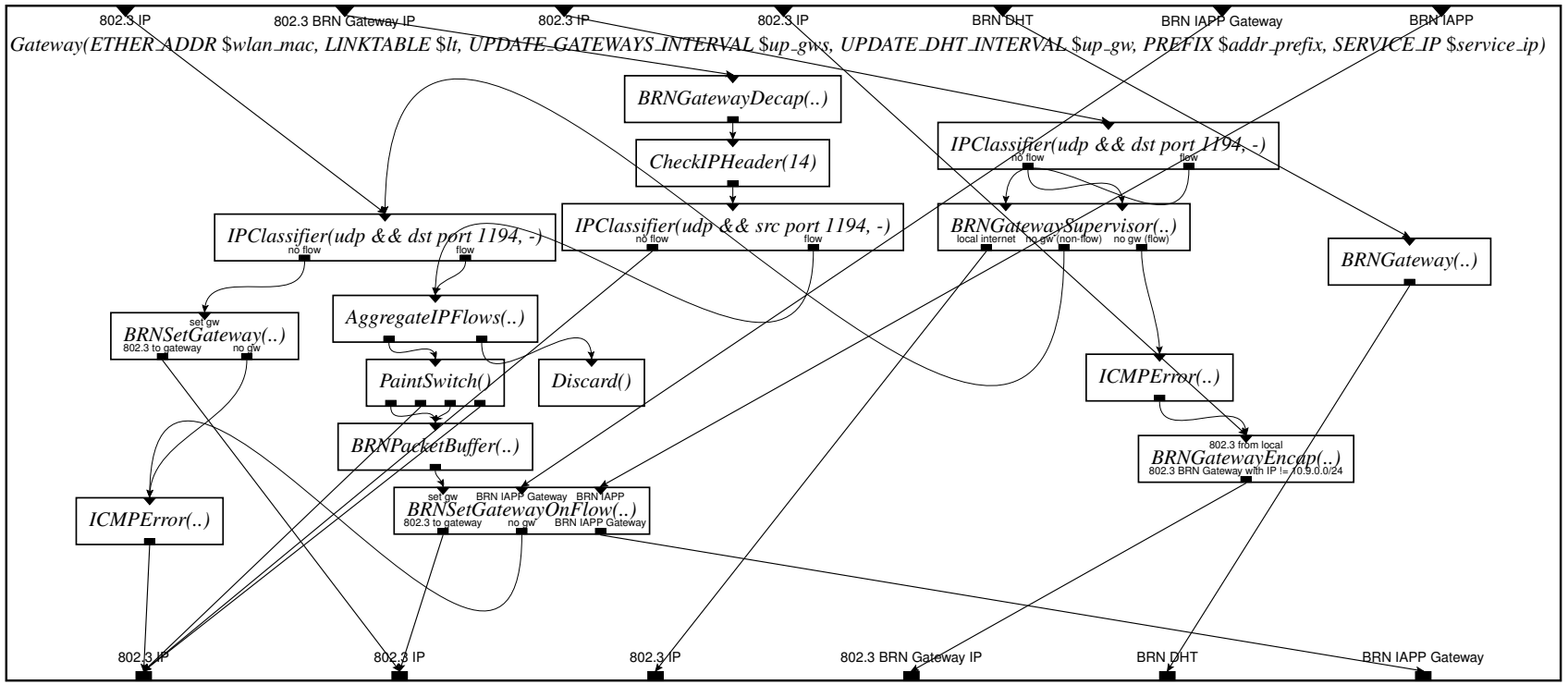
[NTCS99] Ni, Sze-Yao ; Tseng, Yu-Chee ; Chen, Yuh-Shyan ; Sheu, Jang-Ping: The broadcast storm problem in a mobile ad hoc network. In: *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, 1999, S. 151–162

[OLS] *OLSR Daemon.* `http://www.olsr.org`

[SMLN+03] Stoica, Ion ; Morris, Robert ; Liben-Nowell, David ; Karger, David R. ; Kaashoek, M. F. ; Dabek, Frank ; Balakrishnan, Hari: Chord: a scalable peer-to-peer lookup protocol for internet applications. In: *IEEE/ACM Trans. Netw.* 11 (2003), Nr. 1, S. 17–32. – ISSN 1063–6692

[TWP07] Tews, Erik ; Weinmann, Ralf-Philipp ; Pyshkin, Andrei: Breaking 104 bit WEP in less than 60 seconds, TU Darmstadt, 2007

[Tø] Tønnesen, Andreas: *Mobile Ad-Hoc Networks.* `http://www.olsr.org/docs/wos3-olsr.pdf`


802.3 IP
802.3 BRN Gateway IP
802.3 IP
802.3 IP
BRN DHT
BRN IAPP Gateway
BRN IAPP
Gateway(ETHER_ADDR $wlan_mac, LINKTABLE $lt, UPDATE_GATEWAYS_INTERVAL $up_gws, UPDATE_DHT_INTERVAL $up_gw, PREFIX $addr_prefix, SERVICE_IP $service_ip)
BRNGatewayDecap(..)
CheckIPHeader(14)
IPClassifier(udp && dst port 1194, -)
no flow
flow
IPClassifier(udp && dst port 1194, -)
no flow
flow
IPClassifier(udp && src port 1194, -)
no flow
flow
BRNGatewaySupervisor(..)
local internet
no gw (non-flow)
no gw (flow)
BRNGateway(..)
set gw
BRNSetGateway(..)
802.3 to gateway
no gw
AggregateIPFlows(..)
PaintSwitch()
Discard()
ICMPError(..)
BRNPacketBuffer(..)
802.3 from local
BRNGatewayEncap(..)
802.3 BRN Gateway with IP != 10.9.0.0/24
ICMPError(..)
set gw
BRN IAPP Gateway
BRN IAPP
BRNSetGatewayOnFlow(..)
802.3 to gateway
no gw
BRN IAPP Gateway
802.3 IP
802.3 IP
802.3 IP
802.3 BRN Gateway IP
BRN DHT
BRN IAPP Gateway

## Eidesstattliche Erklärung

Ich versichere an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht.

Berlin, den 26. Juli 2007 _____

Jens Müller

Reports published by Humboldt University Berlin, Computer Science Department, Systems Architecture Group.

1. SAR-PR-2005-01: Linux-Hardwaretreiber für die HHI CineCard-Familie. Robert Sperling. 37 Seiten.
2. SAR-PR-2005-02, NLE-PR-2005-59: State-of-the-Art in Self-Organizing Platforms and Corresponding Security Considerations. Jens-Peter Redlich, Wolf Müller. 10 pages.
3. SAR-PR-2005-03: Hacking the Netgear wgt634u. Jens-Peter Redlich, Anatolij Zubow, Wolf Müller, Mathias Jeschke, Jens Müller. 16 pages.
4. SAR-PR-2005-04: Sicherheit in selbstorganisierenden drahtlosen Netzen. Ein Überblick über typische Fragestellungen und Lösungsansätze. Torsten Dänicke. 48 Seiten.
5. SAR-PR-2005-05: Multi Channel Opportunistic Routing in Multi-Hop Wireless Networks using a Single Transceiver. Jens-Peter Redlich, Anatolij Zubow, Jens Müller. 13 pages.
6. SAR-PR-2005-06, NLE-PR-2005-81: Access Control for off-line Beamer – An Example for Secure PAN and FMC. Jens-Peter Redlich, Wolf Müller. 18 pages.
7. SAR-PR-2005-07: Software Distribution Platform for Ad-Hoc Wireless Mesh Networks. Jens-Peter Redlich, Bernhard Wiedemann. 10 pages.
8. SAR-PR-2005-08, NLE-PR-2005-106: Access Control for off-line Beamer Demo Description. Jens Peter Redlich, Wolf Müller, Henryk Plötz, Martin Stigge. 18 pages.
9. SAR-PR-2006-01: Development of a Software Distribution Platform for the Berlin Roof Net (Diplomarbeit / Masters Thesis). Bernhard Wiedemann. 73 pages.
10. SAR-PR-2006-02: Multi-Channel Link-level Measurements in 802.11 Mesh Networks. Mathias Kurth, Anatolij Zubow, Jens Peter Redlich. 15 pages.
11. SAR-PR-2006-03, NLE-PR-2006-22: Architecture Proposal for Anonymous Reputation Management for File Sharing (ARM4FS). Jens Peter Redlich, Wolf Müller, Henryk Plötz, Martin Stigge, Torsten Dänicke. 20 pages.
12. SAR-PR-2006-04: Self-Replication in J2me Midlets. Henryk Plötz, Martin Stigge, Wolf Müller, Jens-Peter Redlich. 13 pages.
13. SAR-PR-2006-05: Reversing CRC – Theory and Practice. Martin Stigge, Henryk Plötz, Wolf Müller, Jens-Peter Redlich. 24 pages.
14. SAR-PR-2006-06: Heat Waves, Urban Climate and Human Health. W. Endlicher, G. Jendritzky, J. Fischer, J.-P. Redlich. In: Kraas, F., Th. Krafft & Wang Wuyi (Eds.): Global Change, Urbanisation and Health. Beijing, Chinese Meteorological Press.
15. SAR-PR-2006-07: □□□□□□□□□□□□ (State of the Art in Wireless Sensor Networks). □□ (Li Gang), □□□•□□•□□□□ (Jens Peter Redlich)

16. SAR-PR-2006-08, NLE-PR-2006-58: Detailed Design: Anonymous Reputation Management for File Sharing (ARM4FS). Jens-Peter Redlich, Wolf Müller, Henryk Plötz, Martin Stigge, Christian Carstensen, Torsten Dänicke. 16 pages.
17. SAR-PR-2006-09, NLE-SR-2006-66: Mobile Social Networking Services Market Trends and Technologies. Anett Schülke, Miquel Martin, Jens-Peter Redlich, Wolf Müller. 37 pages.
18. SAR-PR-2006-10: Self-Organization in Community Mesh Networks: The Berlin RoofNet. Robert Sombrutzki, Anatolij Zubow, Mathias Kurth, Jens-Peter Redlich, 11 pages.
19. SAR-PR-2006-11: Multi-Channel Opportunistic Routing in Multi-Hop Wireless Networks. Anatolij Zubow, Mathias Kurth, Jens-Peter Redlich, 20 pages.
20. SAR-PR-2006-12, NLE-PR-2006-95 Demonstration: Anonymous Reputation Management for File Sharing (ARM4FS). Jens-Peter Redlich, Wolf Müller, Henryk Plötz, Christian Carstensen, Torsten Dänicke. 23 pages.
21. SAR-PR-2006-13, NLE-PR-2006-140 Building Blocks for Mobile Social Networks Services. Jens-Peter Redlich, Wolf Müller. 25 pages.
22. SAR-PR-2006-14 Interrupt-Behandlungskonzepte für die HHI CineCard-Familie. Robert Sperling. 83 Seiten.
23. SAR-PR-2007-01 Multi-Channel Opportunistic Routing. Anatolij Zubow, Mathias Kurth, Jens-Peter Redlich, 10 pages. IEEE European Wireless Conference, Paris, April 2007.
24. SAR-PR-2007-02 ARM4FS: Anonymous Reputation Management for File Sharing. Jens-Peter Redlich, Wolf Müller, Henryk Plötz, Christian Carstensen, 10 15 pages.
25. SAR-PR-2007-03 DistSim: Eine verteilte Umgebung zur Durchführung von parametrisierten Simulationen. Ulf Hermann. 26 Seiten.
26. SAR-SR-2007-04 Architecture for applying ARM in optimized pre-caching for Recommendation Services. Jens-Peter Redlich, Wolf Müller, Henryk Plötz, Christian Carstensen. 29 pages.