Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung Anwendungen 1

Marco Schneider

Border Gateway Protocoll Monitoring, Fluss-Messungen und -Optimierungen

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Marco Schneider

Thema

Border Gateway Protocol - Monitoring, Fluss-Messungen und -Optimierungen

Stichworte

Border Gateway Protocol, BGP, Monitoring, Flussmessung, Topologieerkennung, Analyse

Kurzzusammenfassung

Diese Ausarbeitung ist eine Zusammenfassung über die Grundlagen des künftigen Projektes, welches im Rahmen der Masterarbeit realisiert werden wird.

Marco Schneider

Title

Border Gateway Protocol - Monitoring, Fluss-Messungen und -Optimierungen

Keywords

Border Gateway Protocol, BGP, monitoring, flowmeasurement, identification of topology, analysis

Abstract

This paper is a summary of the basic knowledge within the master-thesis project.

Inhaltsverzeichnis

1 Einleitung

Fast jeder kennt und benutzt das Internet. Kürzlich gab es die Meldung, dass der IPv4-Adress-Pool aufgebraucht sei - das heißt konkret: 4.3 Milliarden Adressen und somit Geräte. Diese gewaltige Anzahl ist jedoch nicht die Anzahl der aktiven Geräte - dies waren Mitte 2010 weltweit ca. 763 Millionen und Anfang dieses Jahres bereits über 818 Millionen Geräte[1]! Wie schafft man es also, dass zwischen jedem dieser Teilnehmer eine Ende-zu-Ende Kommunikation ermöglicht werden kann? Eine wichtige Grundlage sind die verschiedenen Protokolle wie TCP/IP - doch es bedarf zusätzlich dynamischen Routingprotokollen wie z.B. dem Border Gateway Protocol. Dieses Protokoll muss einfach und performant sein und zudem noch gut skalieren. Um eine gute Skalierbarkeit zu erreichen, hat man die Internet-Struktur geeignet hierarchisiert und jedem IP-Netz eine eindeutige Nummer zugewiesen. Um zwischen diesen verschiedenen IP-Netzen routen zu können, benötigt man ein Routingprotokoll mit genannten Anforderungen - im Backbone-Routing hat sich das Border Gateway Protocol durchgesetzt. Grund genug, sich dieses Thema etwas genauer anzuschauen. . .

1.1 Motivation

Das Internet ist das Resultat einer Idee, Computer mittels einer universellen Abstraktionsschicht zu verbinden und so eine systemorientierte Rechnerkommunikation zu ermöglichen - unabhängig von dem eigentlichen Übertragungsweg bzw. der Übertragungstechnik. Durch den Erfolg und den Wunsch nach einer Vernetzung aller Computer wurde das Internet immer größer und komplexer. Das Internet wächst exponentiell[1] - technologische Neuerungen werden eingeführt und Ideen zur Verbesserung der Performanz sind ein wichtiger Teil der Forschung.

In diesem hoch spannenden Gebiet ist viel Bewegung: Forschung und Wissenschaft suchen ständig nach neuen Methoden, die bisherige Technik zu verbessern oder zu erweitern.

Das Border Gateway Protocol ist der de-facto Standard des Routings zwischen den verschiedenen IP-Netzen. Der erste Entwurf des heutigen BGP4 wurde bereits 1995 als Neuauflage für das BGP3 eingericht. Natürlich gab es viele Veränderungen zur Verbesserung des BGP4,

[1] CIA, ISC

dennoch wird dieses Protokoll nicht in absehbarer Zeit abgelöst werden, wie z.B. IPv4 durch IPv6 - ein weiterer Grund, sich mit dem Thema tiefer auseinanderzusetzen.

Techniken wie der Multicast werden immer wichtiger durch den ressourcenschonenden Umgang mit der zur Verfügung stehenden Infrastruktur, deswegen kann ein Einblick in das Rückgrat des Internet sehr hilfreich sein für die Optimierung dieser Multicast-Ströme. Die iNET-Gruppe[2] der HAW Hamburg forscht auf diesem Gebiet - jedoch gibt es keine praktischen Experimentiermöglichkeiten am Backbone-Routing - also direkt an einem BGP-Router.

Durch eine Kooperation mit dem B-CIX in Berlin ist es möglich, diese Lücke mit Hilfe eines Hardware-BGP-Routers zu schließen...

1.2 Aufbau dieser Arbeit

Diese Arbeit ist eine Zusammenfassung des in „Anwendungen 1“ erarbeiteten Thema. Sie ist neben der Präsentation[3] der zweite Teil der Arbeit, der einen tieferen Einblick in das Thema ermöglicht.

Die Arbeit wurde in logische Blöcke geteilt, um eine möglichst sinnvolle Darstellung zu ermöglichen:

Neben der kurzen Einführung folgt der Schwerpunkt der Arbeit, nämlich eine kurze Erklärung des BGP-Protokolls. Dieses Kapitel ist in vier Sektionen geteilt, die einen groben Einblick in BGP, die Routenverdichtung und in Sicherheitsaspekte bieten.

Das folgende Kapitel ist die Problemstellung, bzw. eine Sammlung von Ideen, die realisiert werden können während des späteren Projektes. Hier gibt es drei Schwerpunkte, die jeweils je nach Ausprägung ausreichend sind, um bis zur Masterarbeit das jeweilige Thema zu vertiefen.

In Kapitel 4 werden mögliche Risiken aufgezeigt und Lösungsansätze angedacht, im darauf folgenden Kapitel wird diese Arbeit zusammengefasst und bewertet.

[2] http://inet.cpt.haw-hamburg.de/
[3] http://users.informatik.haw-hamburg.de/ ubicomp/projekte/master10-11-aw1/schneider/folien.pdf

2 Border Gateway Protocol

In diesem Abschnitt wird das Border Gateway Protokoll erläutert, da es wesentlicher Bestandteil des Projekts ist. Es wird das grundlegende Prinzip sowie die relevanten Details erklärt. Es werden viele Abkürzungen verwendet, die bei der ersten Verwendung ausgeschrieben sind. Diese Abkürzungen sollten präsent sein, um den Sinn dieses Kapitels zu verstehen.

2.1 Was ist BGP?

Das Border Gateway Protocol (BGP) ist das Routingprotokoll des Internet-Backbone. Es ist in RFC 4271 (1) in der aktuellen Version 4 spezifiziert. Es ist ein Protokoll der Anwendungsschicht des OSI-Modells, basiert also auf TCP/IP.

Das Internet ist das Netz mit allen Netzen. Ein Netz ist eine Menge von (Internet-) Teilnehmern, welche logisch zusammengehören. Bis Anfang der 90er Jahre gab es feste Klassen (A, B oder C), die unterschiedlich viele Teilnehmer aufnehmen konnten. Dies wurde jedoch durch das klassenlose Internet-Routing (CIDR) in der RFC 1519 (2) abgelöst. Die maximal mögliche Anzahl der Teilnehmer stieg jedoch bei dieser Änderung nicht.

Damit dieser hierarschische Aufbau funktioniert, bedarf es einer Instanz, welche die einzelnen Netze miteinander verbindet und die Kommunikation untereinander ermöglicht. Dazu ist eine Hierarchisierung erforderlich gewesen, welche alle IP-Netze in sog. Autonome Systeme (AS) umwandelt. Ein AS ist ein solcher Zusammenschluss von einem oder mehreren IP-Netzen, welches einer eindeutigen AS-Nummer (Autonomous System Number - ASN, (3)) zugeordnet werden kann.

Die „Aufgabe“ von BGP ist es, die Zuordnung von IP-Prefixen und ASN zu verwalten, dazu hat jeder BGP-Router (BGP Speaker) eine Tabelle, in der zu einem IP-Prefix der ASN-Pfadvektor genannt wird. Das AS, welches das IP-Netz verwaltet (Orign-AS) steht dabei an letzter Stelle im Pfadvektor. Anhand dieser Tabelle weiß jeder Speaker, zu welcher ASN ein Datenpaket weitergeleitet werden muss, damit der Empfänger erreicht wird.

BGP arbeitet in der sog. „default-free zone[1]“, d.h. jedes AS muss zu jedem IP-Prefix einen Eintrag in seiner Routingtabelle haben (aggregierte Prefixe müssen nicht zwangsläufig einen

[1] Es gibt keinen Default-Gatway, an den das Paket weitergeleitet werden kann

eigenen Eintrag haben!) - jeder Router hat also über 300.000 Einträge[2] in seiner Tabelle. Fehlt ein IP-Prefix, so hat der Router keinen Eintrag und es kann kein Pfad ermittelt werden (4).

2.2 BGP als Protokoll

BGP ist in Bezug auf den Kommunikationsteil ein sehr einfach gehaltenes Protokoll. Es besteht nur aus 4 Nachrichten, welche für die komplette Organisation notwendig sind. Die Kommunikation erfolgt über den Port 179 (TCP) (1).

OPEN	Erstellt eine BGP-Session zwischen zwei BGP-Speakern. Die IP-Adressen der Peering-Partner sind fest konfiguriert auf den Routern und müssen so nicht selber gefunden werden.
UPDATE	Update-Nachrichten sind das Kernstück von BGP. Hier werden die Verfügbarkeits- und Erreichbarkeitsnachrichten zwischen den Routern ausgetauscht. Sie enthalten Vektoren von ASN, welche den Weg zum Zielnetz zeigen.
NOTIFICATION	Ist das Gegenstück zu OPEN - wird also nur benutzt, um eine Verbindung wieder abzubauen. Normalerweise ist dies unüblich (bzw. nicht in der Natur eines Routers), deswegen wird die Notification nur im Fehlerfall gesendet.
KEEPALIVE	Wird von den Routern als „ping“ benutzt um festzustellen, ob die Nachbar-Router erreichbar sind. Dies ist ein wichtiger Bestandteil für die Pflege der Routingtabelle.

2.3 Routenauswahl

Ein wichtiger Bestandteil von BGP ist die Routenauswahl. Bei diesem Prozess wird eine Routingtabelle erstellt, auf die der BGP-Router zurückgreift. Dazu wird ständig die Routing Information Base (RIB_IN) aktualisiert durch fremde Announcements. Diese werden vorher gemäß der lokalen Policy Information Base (PIB) gefiltert. Der Prozess der Routenauswahl hat 3 Phasen (s. Bild 2.1):

1. für jeden Eintrag in der RIB_IN wird eine Bewertung erstellt
2. wird in den Prozess der Phase 1 mit einbezogen. Phase 2 ist verantwortlich für die die Auswahl der besten Route zu jedem einzelnen Prefix. Weiterhin wird aus jeder besten Route die Forwarding Information Base (FIB) gebildet.

[2] http://bgp.potaroo.net

3. wird ausgeführt, nachdem die FIB geändert wurde. Dieser Prozess ist verantwortlich für die Verbreitung der eigenen Routeninformationen an die anderen Router, sowie die Routenverdichtung.

Phase 1 wird immer ausgeführt, sobald ein Announcement von einem anderen Router empfangen wurde, sofern dieses Announcement einen Pfad ändert, löscht oder einen neuen Pfad hinzufügt. In die Bewertung fließen Faktoren wie IP-Hoplänge, AS-Pfadlänge, etc. ein.

In Phase 2 wird nun nun genau ein Pfad pro Prefix ausgewählt. Dieses Auswahlverfahren ist standardisiert und folgt einer gewissen Reihenfolge (höchste lokale Präferenz $\rightarrow$ kürzester AS-Pfad...). Die meisten Operator bzw. Hersteller benutzen jedoch eigene Policies (5). Dies ist notwendig, da die Standard-Policies z.B. nur die reine AS-Pfadlänge berücksichtigen, nicht jedoch die IP-Hoplänge (6). Aus diesem Grund kann durch eigene Policies das Netz optimiert werden, um z.B. ein Loadbalancing zu ermöglichen. Es gibt auch Ansätze, um echte Kosten für die Links zu realisieren, dies ist in BGP allerdings nicht etabliert (7).

Wenn alle Regeln auf die ganze Tabelle angewendet wurden, ist der Prozess abgeschlossen und die FIB wurde erstellt. Die FIB enthält nur genau eine ASN zu jedem IP-Prefix und ist somit die eindeutige Routingentscheidung. Sie wird periodisch neu generiert und ist nicht nur notwendig, damit der Router performant arbeitet, sondern wird auch benötigt, um die Nachbarrouter mit Announcements zu versorgen (1).

Phase 3 sorgt für die Verbreitung der aktuellen Routingtabelle, vorher kann jedoch noch die Routenverdichtung mit einbezogen werden. Auf Grundlage der FIB wird die RIB_OUT erstellt, diese enthält dann die Informationsgrundlage, die an andere Router annonciert werden soll. Dazu wird die RIB_OUT an alle verbundenen BGP-Router, bzw. den Route-Reflector gesendet.

Für den Fall, dass das Peering an einem öffentlichen Internet Exchange & Peering Point (IXP - z.B. AMS-IX, DE-CIX, B-CIX)[3] passiert, wird meistens ein zentraler Route Reflector (RR) gestellt. Dieser RR ist eine zentrale Stelle, mit dem sich alle BGP-Speaker verbinden können um die Updates auszutauschen. Dies hat den Vorteil, dass aus einem Mesh-Netz ein Stern-Netz wird und somit die Last deutlich verringert wird (8).

2.4 Routenverdichtung

Routenverdichtung oder Aggregation bedeutet, dass eine Menge von verschiedenen Announcements zu einem Prefix vorliegen, die jedoch verschiedene AS-Pfade haben. Um diese Menge auf eine Route zu reduzieren, wird nach dem Algorithmus in Phase 2 angewendet. Nun kann der Router diese „fremde“ Route an seine Nachbarn weitergeben (=er annonciert sich

[3] Eine Übersicht der am AMS-IX verbundenen Unternehmen: https://www.ams-ix.net/connected

selber als Hop für dieses Prefix), allerdings muss sichergestellt sein, dass 1. der Router sich nicht als Orign-AS für dieses Prefix ausgibt und 2. dass die Aggregation kenntlich gemacht wird, damit keine Loops entstehen können.

Um dies zu erreichen, annonciert der Router dieses Prefix mit dem gesetzten Aggregationsbit, setzt sich selber als ersten Hop in die Route und hängt einen ungeordneten Pfad hinter sich (AS-SET), die auf dem Weg zum Orign-AS passiert werden. Durch diese Methode werden in transparenter Weise die Routen zusammengelegt.

Dieser Schritt passiert „auf dem Weg“ von FIB zu RIB_OUT, also der Information, die unser Router selber braucht (FIB - geordneter AS-Pfad) und der Information, die andere Router wissen müssen (eigene ASN & AS-SET - ungeordneter AS-Pfad).

In Bild 2.1 ist der Gesamtprozess Beispielhaft dargestellt. Der Router erhält regelmäßig Announcements der anderen Router. Diese werden in der Routing Information Base (RIB_IN) gespeichert und aktualisiert. Dies passiert jedoch nur, wenn das Announcement den Ingress-Filter des Routers passiert hat, der aus verschiedenen Gründen vorhanden sein muss (s. Kapitel 2.5). Wenn die RIB_IN aktualisiert wurde, wird der Vorgang der Routenauswahl ausgeführt. Wenn dieser abgeschlossen ist, wurde die RIB_OUT und die FIB erstellt. Diese beinhalten nun zu jedem IP-Prefix einen eindeutigen Pfadvektor und werden von dem Router genutzt. Die RIB_OUT wird an die anderen Router wieder annonciert und der Vorgang kann erneut beginnen. Sollte allerdings eine Route ungültig werden, kann dies erst nach einem erneuten Aufbau der FIB „repariert“ werden, da die FIB über keine Redundanzen verfügt.

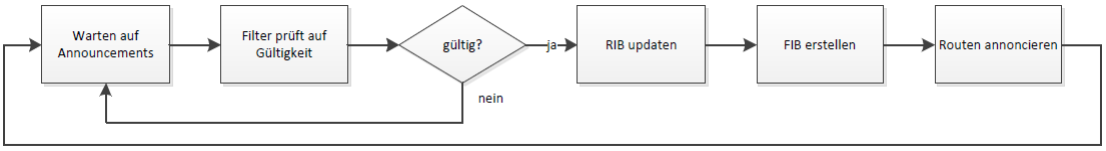

Abbildung 2.1: Grobdarstellung des Update-Mechanismus in BGP

2.5 Sicherheit

Die Sicherheit, die BGP per default bietet, steht in keinem Verhältnis zu der Wichtigkeit im Internet. Aus diesem Grund ist es notwendig, dass man entsprechende Filterregeln auf die ankommenden Updates anwendet. Diese Filterregeln werden i.d.R. von großen zu kleinen Providern immer „schärfer“, da die Erfahrung gezeigt hat, dass ein kleines, lokales Unternehmen öfter Fehlkonfigurationen implementiert, als z.B. eine Deutsche Telekom.

Es gibt viele Ideen, wie diese Probleme gelöst werden kann (9) (10). Die üblichste Variante ist ein Abgleich der Announcements mit der RIPE-Datenbank. Die RIPE ist eine der fünf Regional Internet Registries (RIR), welche die ASN und IP-Prefixe vergibt und somit über eine Datenbank verfügt. Diese Datenbank kann man abrufen und so bei ankommenden Advertisements prüfen, ob das annoncierte IP-Netz auch von der entsprechenden ASN kommt, bzw. ob der ASN das IP-Netz „gehört“ (11). Durch diese Methode wird das sog. Prefix-Hijacking weitesgehend unterbunden. Prefix-Hijacking ist ein Angriff auf ein IP-Prefix, indem man ein falsches Orign-AS annonciert und somit den Verkehr auf sein eigenes AS umleitet. Dieses Phänomen hat Pakistan im Jahre 2008 genutzt, um Youtube lahm zu legen[4]. Dabei wurde eine more-specific-route zu dem Youtube-Server annonciert, die leider auch über die Ländergrenzen von Pakistan hinaus propagiert wurde. . . Als diese „Fehlkonfiguration“ bemerkt wurde, mussten die ISP’s, welche mit der Pakistan Telecom peerten einfach nur diese eine Route löschen und das System heilte sich innerhalb kürzester Zeit selbst.

[4] http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

3 Problemstellung

Nachdem im vorherigen Kapitel das BGP erklärt wurde, wird nun das eigentliche Problem bzw. der künftige Arbeitsansatz vorgestellt. Jedes der Teilgebiete wird kurz erörtert und bewertet, im nächsten Kapitel folgen dann die daraus resultierenden Risiken. Es gibt zwei Teilgebiete zur Analyse: einmal die Control-Plane (die Summe der Routinginformationen) und einmal die Data-Plane (die effektiven Datenweiterleitungen). Im ersten Teil des Kapitels liegt der Schwerpunkt auf der Analyse der Control-Plane, während sich die Flow-Messungen auf die Data-Plane beschränken.

Ziel soll sein, einen Arbeits- und Messplatz zu etablieren, mit dem (je nach Anforderung) Messungen „am offenen Herz des Internets“ durchgeführt werden können. Das Peering wird am B-CIX in Berlin sein - es wird also nicht mit veralteten Dumps gearbeitet, sondern es kann direkt und im Livebetrieb geforscht werden. Dieser Ansatz ermöglicht wertvolle Einblicke in den tatsächlichen Ablauf des (BGP-) Routings und ist eine Grundlage für weiterführende Projekte.

3.1 BGP-Messungen

Es sollen im ersten Schritt Messungen zur Routen- bzw. Pfadstabilität sowie zu dem Updateverhalten auf dem Router realisiert werden. Diese sollen zum besseren Verständnis des gesamten Protokolls aufgearbeitet und somit verstanden werden. Diese Messungen sollen Auskunft darüber geben, wann und in welchem Umfang der Router durch fremde Announcements seine eigenen Routen ändert.

Diese Messungen können z.B. verwendet werden, um die BGP-Updates auf Anomalien zu überprüfen. Es ist z.B. relativ unwahrscheinlich, dass die Deutsche Bank eine Route über Amerika oder China annoncieren würde. Dies kann mit entsprechenden Auswertungen aufgedeckt und analysiert werden.

3.2 Topologieerkennung

Im H∀Mcast[1] Kontext ist eine Topologieerkennung um den Router wünschenswert. Diese hilft neben Ergebnissen aus dem folgenden Punkt die Optimierung der Verteilbäume zu verbessern und so eine möglichst geringe Verkehrslast über den Router zu ermöglichen. Um dieses Ziel zu erreichen ist eine Übersicht der Topologie aus Sicht des Routers hilfreich. Da aber nicht sämtliche Router am Verteilbaum überwacht werden können, wird hier nur ein Ausschnitt der Topologie und nicht der gesamte Verteilbaum dargestellt.

Eine weitere Idee ist es, sich die Topologie des Internets aus mehreren Perspektiven anzusehen. Da das Internet nicht symmetisch ist, werden die Routen wahrscheinlich von einander abweichen. Auch dies ist ein Ansatzpunkt für die bestmögliche Optimierung in Bezug auf das H∀Mcast-Projekt.

3.3 Flow-Messungen, -Auswertung und Optimierung

Das Kernproblem liegt im Bereich der Flussmessung und deren Auswertung. Natürlich ist das Thema Flussmessung im Internet nicht neu, dennoch sollen sich die Auswertungen auf spezielle Anwendungsfälle, z.B. das H∀Mcast Projekt beziehen. Dort ist es wünschenswert, eine genaue Information über die Flussverteilung zum und über den Router zu erhalten.

Das heißt, es soll ein spezieller Multicast-Fluss gefunden und analysiert werden. Dies ist mittels des Tools SFlow realisierbar. Der verwendete Router am B-CIX hat eine Hardwareunterstützung für genau dieses Tool, sodass eine große Datenmenge zuverlässig analysiert werden kann.

SFlow funktioniert im wesentlichen als reine Monitoring-Instanz, welche die Pakete mittels zwei verschiedener Mechanismen analysiert. Das sind die Flow-Samples - hier werden die Datenpakete mit einer vorher festgelegeten „Abtastrate“ zufällig ausgewählt und analysiert, während bei den Counter-Samples das Interface gepollt werden muss.

Die mit SFlow gesammelten Daten werden an einen zentralen Server („SFlow-Collector“) geschickt und dort verarbeitet. So kann eine hohe Verarbeitungsgeschwindigkeit bei einer großen Genauigkeit und geringer CPU-Last zugesichert werden. SFlow kann außerdem über sämtliche OSI-Schichten protokollieren, d.h. von Layer 2 bis Layer 7.

Die so erhaltenen Daten müssen aufbereitet und in geeignete (visuelle) Form gebracht werden, damit sie im H∀Mcast Projekt verwendet werden können. Dort sind die Ergebnisse relevant um die Datenströme besser und effektiver verteilen zu können.

[1] H∀Mcast ist ein Projekt der iNET-Gruppe der HAW Hamburg,http://www.realmv6.org/hamcast.html

4 Risiken

Die im vorigen Kapitel genannten Ideen sind sehr weit gefasst und mit ihnen können einige (möglicherweise massive) Probleme auftreten.

Das größte Problem könnte eine Überschätzung des Aufwandes sein. Dabei geht es nicht rein um die Einrichtung des Messplatzes, sondern viel mehr um den Overhead um auf dem Gebiet up-to-date zu bleiben. Es wird sehr viel geforscht und viele helle und kreative Köpfe bringen neue Ideen zur Verbesserung ein. Wenn man nicht aktuell ist, kann man schnell alte Methoden anwenden, während es schon bessere und/oder einfachere Methoden gibt. Dieses Problem kann nur gelöst werden, indem man ständig auf dem neusten Stand bleibt und ggf. das Projekt in Richtung der neuen Erkenntnisse anpasst.

Ein weiteres Problem ist technischer Natur und könnte das Auffinden der gewünschten Daten sein. Wenn z.B. ein Overlay-Multicast neben anderen, diversen Daten durch den Router geschickt wird, kann es ein Problem geben, diese gewünschten Daten zu finden. Man kann zwar die verschiedenen Ströme durch IP/Port bzw. Flow-Label erkennen, da jedoch das Tool SFlow nicht alle Daten mitloggt, kann es dort zu Problemen kommen.

Ein weiteres Problem in dieser Richtung ist der Datenschutz. Sofern Daten der Data-Plane analysiert wird, dürfen die Daten nur konform zum Datenschutzgesetz analysiert/gespeichert werden. Ein möglicher Missbrauch, bzw. die Identifikation einzelner Personen/Unternehmen muss ausgeschlossen sein!

Viele Probleme werden erst im Laufe des Projekts auftreten, andere lassen sich durch Planung vermeiden. Es sollten auf jeden Fall keine Probleme auftreten, die das Projekt „zu Fall“ bringen - schlimmstenfalls könnte nur ein Teil der Ideen realisiert werden.

5 Zusammenfassung

Es soll ein Messplatz am B-CIX etabliert werden, der für verschiedene experimentelle Messungen der Control-Plane und Data-Plane zur Verfügung stehen soll. Die Ergebnisse der Auswertung können von großer Bedeutung für das H∀Mcast Projekt der iNET-Gruppe der HAW Hamburg sein. Sie ermöglichen einen experimentellen Einblick in das „Routerleben“ und können so die theoretischen Ergebnisse bestätigen oder Differenzen aufzeigen.

Durch Kooperationen (u.a. mit dem B-CIX) sind alle nötigen Voraussetzungen geschaffen, um dieses Projekt in der angedachten Form zu realisieren. Die bisher bekannten Probleme lassen sich umgehen oder minimieren, sodass in 1,5 Jahren verwertbare Ergebnisse zu den Problemstellungen vorliegen können.

Literaturverzeichnis

[1] Y. Rekhter, T. Li, and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” IETF, RFC 4271, January 2006.

[2] V. Fuller, T. Li, J. J. Y. Yu, and K. Varadhan, “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy,” IETF, RFC 1519, September 1993.

[3] J. Hawkinson and T. Bates, “Guidelines for creation, selection, and registration of an Autonomous System (AS),” IETF, RFC 1930, March 1996.

[4] T. Bates and Y. Rekhter, “Scalable Support for Multi-homed Multi-provider Connectivity,” IETF, RFC 2260, January 1998.

[5] M. Caesar and J. Rexford, “Bgp routing policies in isp networks,” *Network, IEEE*, vol. 19, no. 6, pp. 5 – 11, 2005.

[6] R. Asati, “BGP Bestpath Selection Criteria,” IETF, Internet-Draft – work in progress 00, October 2008.

[7] I. Varlashkin and R. Raszuk, “Carrying next-hop cost information in BGP,” IETF, Internet-Draft – work in progress 00, January 2011.

[8] R. Raszuk, C. Cassar, E. Aman, and B. Decraene, “BGP Optimal Route Reflection (BGP-ORR),” IETF, Internet-Draft – work in progress 00, October 2010.

[9] C. Lynn, “Secure BGP (S-BGP),” IETF, Internet-Draft – work in progress 01, July 2003.

[10] S. Murphy, “BGP Security Protections,” IETF, Internet-Draft – work in progress 00, February 2002.

[11] D. Guangming, “BGP UPDATE Advertisement Restriction,” IETF, Internet-Draft – work in progress 00, September 2006.