Border Gateway Protocol

Tim Wegner, *Student im Master Elektrotechnik/Informationstechnik*

***Zusammenfassung*—Zu Beginn wird eine Einführung in die Anwendung des BGP gegeben. Danach werden die speziellen Aspekte des BGP erläutert. Zum Schluss werden die Vor- und Nachteile des Protokolls gegenübergestellt und ein Ausblick gegeben.**

***Index Terms*—Internet, Kommdunikationsprotokoll, Anwendungsschicht, IP-Routing.**

I. Übersicht

Das Internet besteht aus einer Vielzahl verschiedener Autonomer Systeme (AS) (vergleiche Abbildung 1). Um diese AS miteinander verbinden zu können, benötigt man ein einheitliches Inter-Domain-Routing-Protokoll. Im heutigen Internet hat sich das Border Gateway Protocol (BGP) durchgesetzt.
Das BGP ist ein Anwendungschichtsprotokoll (siehe Abbildung 2), dass nach dem Pfadvektorprinzip arbeitet. Im BGP entsprechen die Routen dem Pfad zu den anderen AS wobei keine internen Details der Autonomen Systeme bekannt sind. Ein BGP-Router führt eine Routingtabelle mit aggregierten Pfaden zu allen anderen AS.
Der Routing Allgorithmus ist im BGP nicht festgelegt, sondern kann durch Routing Policies bestimmt werden. Dies ist im Abschnitt Pfadauswahl genauer erläutert.
Das BGP in der aktuellen Version ist im RFC 4271 beschrieben (RLH06).

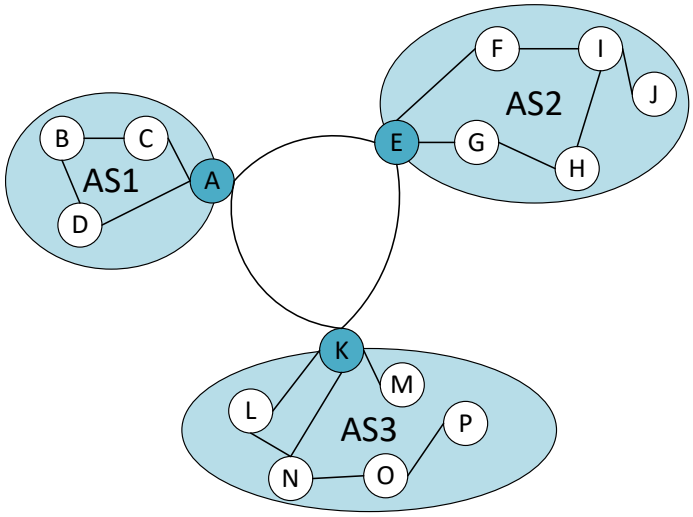

Abbildung 1. Beispielnetzwerk Autonomer Systeme (AS)

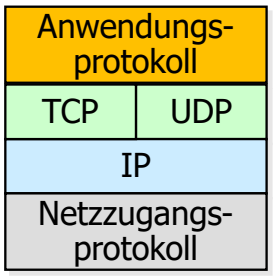

Abbildung 2. Das Internet-Schichtenmodell

II. Protokollmechanismen

Nachdem im vorherigen Abschnitt die grundsätzliche Idee hinter BGP aufgezeigt wurde, sollen hier die speziellen Aspekte näher gebracht werden.
Das BGP ist auf allen beteiligten Routern verteilt und enthält die Anzahl der AS als Metrik. Der Austausch der Routing-Informationen erfolgt nicht periodisch sondern ereignisbasiert.
BGP kann außerhalb und innerhalb der AS verwendet werden. Externes BGP (eBGP) wird für die Kommunikation zwischen zwei Peer-Routern zweier AS verwendet. Internes BGP (iBGP) dient der Kommunikation zwischen BGP-Routern eines AS. Es ist in der Lage mit Protokollen innerhalb eines AS wie Open Shortest Path First (OSPF) zusammenzuarbeiten. Das iBGP wird unter anderem dafür verwendet um den Datenverkehr durch ein AS zu schleusen.

A. Ablauf einer BGP-Sitzung

Das BGP nutzt kein eigenes Protokoll um eine Verbindung aufzubauen, sondern verwendet das Transmission Control Protocol (TCP) am Port 179 um einen sicheren Datenaustausch zu gewährleisten.
Zur Kommunikation zwischen zwei BGP-Routern sind in (RLH06) vier Nachrichtentypen definiert.
Nachdem eine TCP-Verbindung hergestellt wurde, wird von den einzelnen Routern eine OPEN-Message geschickt. Wenn die OPEN-Message akzeptiert wird, wird sie mit einer KEEPALIVE-Message bestätigt. Die KEEPALIVE-Message wird periodisch neu geschickt um die Verbindung beizubehalten. Tritt ein Fehler in der Verbindung auf oder die Verbindung soll abgebaut

werden, wird eine NOTIFICATION-Message geschickt. Das Kernstück von BGP ist die UPDATE-Message. Über diese Nachricht werden die Routing-Informationen ausgetauscht. Um die zu übertragenden Routing-Informationen zu minimieren werden im Normalfall nur die Änderungen des besten Pfades gesendet.
Auf die verschiedenen Nachrichtentypen wird im Abschnitt C nochmal genauer eingegangen.

B. Paketaufbau

Der BGP-Paketkopf ist bei jedem Nachrichtentyp gleich (siehe Abbildung 3).
Der **Marker** besteht aus Kompatibilitätsgründen nur aus Einsen und gibt den Start einer neuen Nachricht an. Die **Message Length** gibt die Gesamtlänge der Nachricht an. Sieht hilft dabei den Beginn des Markers der nächsten Nachricht im TCP-Datenstrom zu identifizieren. Die Länge einer Nachricht ist mindestens 19 und maximal 4096 Bytes.
Der gesendete Nachrichtentyp ist im Feld **Message Type** angegeben.

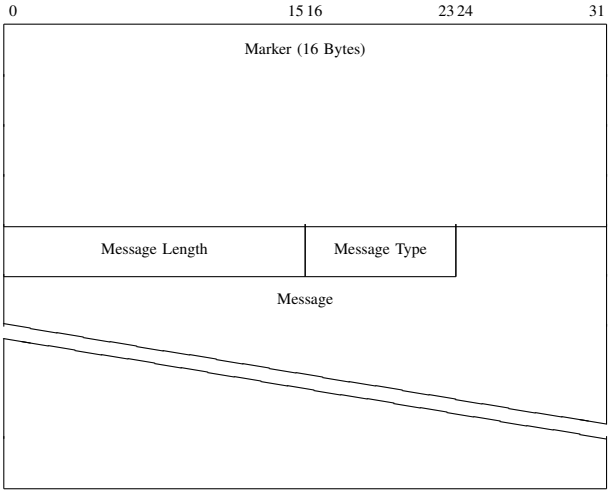

Abbildung 3. Der Paketkopf des BGP. (RLH06)

C. Nachrichtentypen

Wie bereits erwähnt erfolgt die Kommunikation zwischen BGP-Routern über unterschiedliche Nachrichten. Ziel dieses Abschnittes ist es die verschiedenen Nachrichtentypen und deren Aufbau näher zu erläutern.

1) OPEN-MESSAGE: Zusätzlich zum Message-Header besitzt die OPEN-Message die folgenden Felder (siehe Abbildung 4).
Das **Version** Feld gibt die verwendete BGP Version

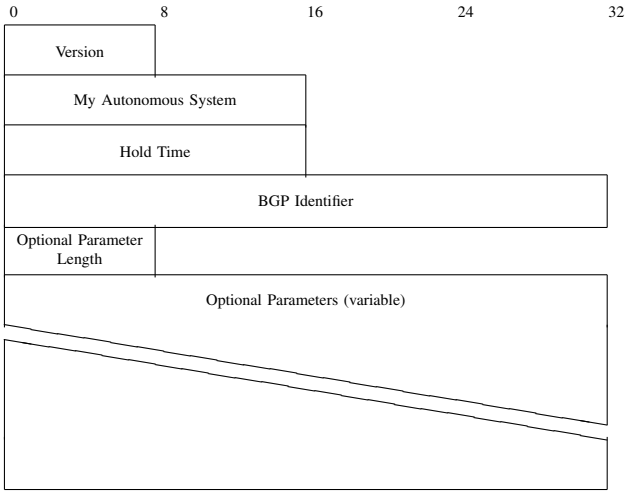

Abbildung 4. OPEN-Message (RLH06)

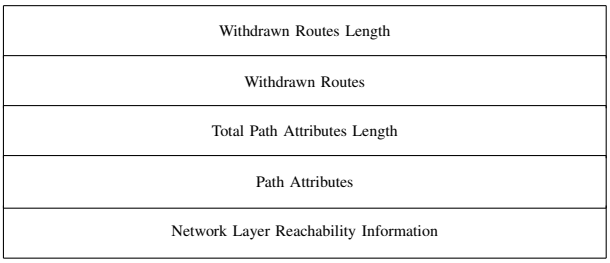

Abbildung 5. UPDATE-Message (RLH06)

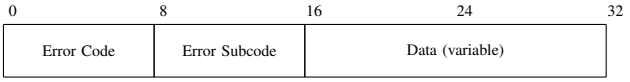

Abbildung 6. NOTIFICATION-Message (RLH06)

an. Die aktuelle Version ist die Nummer 4. **My Autonomous System** gibt die AS-Nummer des Senders an. Die **Hold Time** gibt die maximale Zeit in Sekunden an bis eine vom Sender geschickte KEEPALIVE oder UPDATE-Message ankommen kann. Wird diese Zeit überschritten, wird der Sender als unereichbar angesehen und der Empfänger verschickt keine weiteren Daten. Der **BGP Identifier** enthält die IP-Adresse des Senders der Nachricht über die er erreicht werden kann. Der Wert des BGP Identifiers muss bei allen Verbindungen des Senders gleich sein. Die **Optional Parameter Length** zeigt die Länge des **Optional Parameters** Feldes. Mögliche optionale Parameter sind im RFC 5492 beschrieben (SC09).

2) UPDATE-MESSAGE: Wie oben bereits erwähnt, werden UPDATE-Messages gesendet um die Routinginformationen zu übertragen. Die Information in dieser Nachricht kann dafür verwendet werden um eine

Tabelle aufzustellen, die die Verbindungen zwischen den autonomen Systemen zu beschreiben. Es kann eine neue Route übertragen werden und gleichzeitig mehrere Routen abgelegt werden. Abgelegt werden Routen zum Beispiel wenn ein Pfad seine Routing Policy ändert und sie somit ungültig macht.
Den Aufbau dieses Nachrichtentypes kann man in Abbildung 5 nachverfolgen. Die **Witdhdrawn Routes Length** beschreibt die Länge des **Withdrawn Routes** Feldes, welches die Routen angibt, die abgelegt werden sollen. Eine 0 in dem Length Feld bedeutet, dass keine Route abgelegt wird. Die **Total Path Attribute Length** gibt die Gesamtlänge der folgenden Felder an. Das **Path Attributes** Feld beinhaltet mehrere Eigenschaften der übertragenen Pfade. Wird keine neue Route übertragen ist dieses Feld leer. Im **Network Layer Reachability Information** Feld steht die neue Adresse die verbreitet wird. Diese Adresse ist verschlüsselt um klassenlose Adressierung zu gewährleisten.

3) NOTIFICATION-MESSAGE: Die NOTIFICATION-Message wird gesendet, wenn ein Fehler auftritt oder die Verbindung abgebaut werden soll. Sie besteht aus dem Message-Header und drei weiteren Feldern (siehe Abbildung 6).
Der **Error Code** gibt an, um welchen Fehlertyp es sich handelt. Die möglichen Fehlerarten sind hier aufgelistet:

- *Message Header Error*
- *OPEN Message Error*
- *UPDATE Message Error*
- *HOLD Timer Expired*
- *Finite State Machine Error*
- *Cease*

Um den Fehler genauer spezifizieren zu können, gibt es für jeden Fehlercode mehrere Subcodes. Der passende Subcode wird durch den Wert des **Error Subcode** Feldes angegeben.

4) KEEPALIVE-MESSAGE: Das BGP verwendet keine der TCP-basierten Mechanismen um eine Verbindung aufrecht zu erhalten. Stattdessen werden periodisch KEEPALIVE-Messages zwischen den BGP-Partnern ausgetauscht. Diese Nachrichten werden oft genug gesendet, damit die **Hold Time** der OPEN-Message nicht überschritten wird was zum Beenden der Verbindung führen würde. Ein empfohlener Wert für dieses Intervall ist Eindrittel der Hold Time.
Eine KEEPALIVE-Message besteht nur aus dem Message-Header wie in Abbildung 2.

D. Pfadauswahl

Wie oben bereits erwähnt ist der Routing-Allgorithmus in BGP nicht direkt festgelegt sondern ist durch die Routing Policies einstellbar. Das BGP ermöglicht es die Pfadattribute manuell einstellen zu können. So kann jeder Router unabhängig von den anderen BGP-Routern im System den besten Pfad bestimmen.
Die Priorität anhand der ein BGP-Router seinen besten Pfad bestimmt ist als *BGP Path Selection Process* (Cis16) beschrieben.
Die Regeln nachdem die Pfadattribute eingestellt werden sind Teil der Routing Policies. Für das Aufstellen der Routing Policy werden sowohl technisch-metrische als auch stragische Aspekte herangezogen. In der Praxis spielen in der Regel insbesondere die wirtschaftlichen Aspekte eine große Rolle.
Anhand der Attribute kann man die unterschiedlichsten Routing Allgorithmen einstellen, zum Beispiel Hot-Potato oder Cold-Potato (MP06). Auf diese wird in dieser Ausarbeitung nicht genauer eingegangen.
Es gibt eine Vielzahl von Pfadattributen. Für den *BGP Path Selection Process* sind die hier aufgelisteten Attribute von besonderer Bedeutung.

- *AS Path*
- *Weight*
- *Local Preference*
- *Origin*
- *Multi-Exit Discriminator*
- *Next Hop*

Diese Attribute sind im RFC 4271 beschrieben. Um zu verdeutlichen wie man den Entscheidungsprozess beeinflussen kann, soll hier beispielhaft das Attribut **AS Path** näher erläutert werden.
AS Path gibt an über welche AS das angegebene Ziel erreicht werden kann. Es ist erlaubt, dass sich ein AS mehrmals hintereinander einträgt. So gilt man zwar als erreichbar aber der Pfad wird künstlich verlängert und somit unattraktiv gemacht. Dadurch kann man verhindern, dass der eigene Pfad genommen wird. Dies ist auch unter dem Begriff *AS Path Prepending* bekannt (TVG15).
Zusätzlich werden Routingschleifen durch dieses Attribut wie folgt vermieden. Im AS Path steht das eigene AS immer an erster und das Ziel-AS an letzter Stelle. Wenn das eigene AS mehrfach im AS Path auftaucht wird eine Routingschleife erkannt und kann somit vermieden werden.

E. Erweiterungen und Ergänzungen

Die Struktur des BGP wie es im RFC 4271 beschrieben ist hat zahlreiche Ergänzungen bzw. Erweiterungen, die ohne Anspruch auf Vollständigkeit im Folgenden kurz aufgelistet sind. Interessierte können sich unter der jeweils genannten Literaturangabe näher über die Erweiterungen informieren.

- RFC 4456: *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)* wurde definiert um das Problem der vollständigen Vermaschung zu lösen (BCC06).
- RFC 4760: *Multiprotocol Extensions for BGP-4* beschreibt Erweiterungen um das Transportieren von Routing-Informationen für mehrere Internet-Schicht Protokolle zu ermöglichen (BCKR07).
- RFC 5065: *Autonomous System Confederations for BGP* beschreibt die Möglichkeit mehrere AS als ein Verband von AS zusammenzufassen (TMS07).
- RFC 5492: *Capabilities Advertisement with BGP-4* definiert einen neuen optionalen Parameter namens Capabilities (SC09).
- RFC 6286: *Autonomous-System-Wide Unique BGP Identifier for BGP-4* beschäftigt sich damit die Definition des *BGP Identifier* als 4 Byte großes Feld zu entschärfen (CY11).
- RFC 6608: *Subcodes for BGP Finite State Machine Error* beinhaltet mehrere Subcodes um den Netzbetreibern mehr Informationen zur Fehlerdiagnose liefern zu können (DCS12).
- RFC 7606: *Revised Error Handling for BGP UPDATE Messages* befasst sich mit der Überarbeitung der UPDATE-Message Fehlerbehandlung, damit eine BGP-Verbindung bei einem Fehler nicht unbedingt unterbrochen wird (CSMP15).
- RFC 7705: *Autonomous System Migration Mechanisms and Their Effects on the BGP AS PATH Attribute* beschreibt bestehende BGP-Mechanismen für die Migration der AS-Nummer, die nicht direkt Teil der BGP-4 Spezifikation sind (GA15).

III. Bewertung

In seiner Grundkonfiguration weist das BGP einige Schwächen auf. Diese können in der Regel aber durch definiertes Lenken des richtigen Pfades mittels der Routing Policies minimiert werden (Wik). Im Folgenden sollen einige Schwächen erläutert werden.

Eine große Herausforderung des BGP ist der stetige Wachstum des Internets und den daraus folgenden sehr großen Routingtabellen. Den Verlauf der Größe dieser Tabelle kan man unter (CID) nachverfolgen. Der aktuelle Stand liegt bei etwas 645982 Einträgen. Dieses Problem wurde unter anderem bei der Entwicklung von IPv6 mit berücksichtigt, daher werden hier weniger Einträge benötigt.

Ein weiterer Nachteil ist, dass es keine Lastverteilung vorsieht. Es wird immer nur ein möglicher Pfad gewählt. Es bestehen hier allerdings bereits unternehmenseigene Erweiterungen (Cis16), die eine Lastverteilung erlauben.

Auch sicherheitstechnisch gibt es in der Grundstruktur des BGP einige Schwächen. Insbesondere das Manipulieren von Routinginformationen spielt hier eine große Rolle. Allerdings wird viel versucht um diese Angriffe zu erschweren. So wurde zum Beispiel mit dem RFC 6480 (LK12) eine Spezifikation veröffentlicht, die einem BGP-Router ermöglicht die Echtheit einer UPDATE-Nachricht zu überprüfen (Hen11).

Der große Vorteil des BGP liegt darin, dass viele optionale Pfade in einer einzigen Routingtabelle vereint werden. Dazu kann das BGP mit Protokollen wie OSPF, die innerhalb eines eines AS eingesetzt werden, zusammenarbeiten.

Ein weiterer großer Vorteil liegt im Prinzip des BGP. Das BGP ist ein Path-Vector Protokoll. Seine Funktionsweise orientiert sich an Distance-Vector Protokolle wie das Routing Information Protocol (RIP). Diese haben allerdings das Problem von Routingschleifen. Diesen wird bei BGP wie bereits erwähnt durch dem Pfadattribut AS Path vorgebeugt.

Bis heute basiert die Kommunikation autonomer Systeme im Internet auf dem BGP. Eine ausreichend dokumentierte mögliche Alternative ist bisher nicht bekannt. Dies wird sich in naher Zukunft mit großer Wahrscheinlichkeit aus Kompatibilitätsgründen nicht ändern. Wie man beim Übergang von IPv4 zu IPv6 sehen kann, ist das Ersetzen eines so weitreichenden Protokolls sehr langwierig (Ris08).

IV. Zusammenfassung und Ausblick

Mit dem BGP wurde ein Protokoll entwickelt, dass die Verbindung zwischen den vielen AS des Internets ermöglicht. Dank des Informationsaustausches zwischen den BGP-Routern ist die Verbreitung neuer und das Entfernen nicht mehr genutzter Routen gewährleistet.

Obwohl das Protokoll einige Schwächen aufweist ist es der Grundstein für die Kommunikation im Internet.

Zukünftig wird es mit Sicherheit noch mehrere Erweiterungen geben um das Protokoll zu verbessern.

Literatur

[BCC06] Bates, T. ; Chen, E. ; Chandra, R.: *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP).* RFC

4456 (Draft Standard). http://www.ietf.org/rfc/rfc4456.txt. Version: April 2006 (Request for Comments). – Updated by RFC 7606

[BCKR07] BATES, T. ; CHANDRA, R. ; KATZ, D. ; REKHTER, Y.: *Multiprotocol Extensions for BGP-4*. RFC 4760 (Draft Standard). http://www.ietf.org/rfc/rfc4760.txt. Version: Januar 2007 (Request for Comments). – Updated by RFC 7606

[CID] *CIDR REPORT*. http://www.cidr-report.org/as2.0/, . – Accessed: 2017-01-17

[Cis16] CISCO: BGP Best Path Selection Algorithms. Version: September 2016. http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html. 2016 (13753). – Forschungsbericht

[CSMP15] CHEN, E. ; SCUDDER, J. ; MOHAPATRA, P. ; PATEL, K.: *Revised Error Handling for BGP UPDATE Messages*. RFC 7606 (Proposed Standard). http://www.ietf.org/rfc/rfc7606.txt. Version: August 2015 (Request for Comments)

[CY11] CHEN, Enke ; YUAN, Jenny: Autonomous-System-Wide Unique BGP Identifier for BGP-4 / Internet Engineering Task Force (IETF). Version: June 2011. http://www.rfc-editor.org/pdfrfc/rfc6286.txt.pdf. 2011 (6286). – Request for Comments

[DCS12] DONG, J. ; CHEN, M. ; SURYANARAYANA, A.: *Subcodes for BGP Finite State Machine Error*. RFC 6608 (Proposed Standard). http://www.ietf.org/rfc/rfc6608.txt. Version: Mai 2012 (Request for Comments)

[GA15] GEORGE, Wesley ; AMANTE, Shane: Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute / Internet Engineering Task Force (IETF). Version: November 2015. http://www.rfc-editor.org/pdfrfc/rfc7705.txt.pdf. 2015 (7705). – Request for Comments

[Hen11] HENKE, Jan: Sicherheit im Internet Backbone. (2011). https://inet.haw-hamburg.de/teaching/ws-2011-12/master-projects/henke_aw1.pdf

[LK12] LEPINSKI, M. ; KENT, S.: *An Infrastructure to Support Secure Internet Routing*. RFC 6480 (Informational). http://www.ietf.org/rfc/rfc6480.txt. Version: Februar 2012 (Request for Comments)

[MP06] MCPHERSON, D. ; PATEL, K.: *Experience with the BGP-4 Protocol*. RFC 4277 (Informational). http://www.ietf.org/rfc/rfc4277.txt. Version: Januar 2006 (Request for Comments)

[Ris08] RIST, Michael: Border Gateway Protocol. (2008). https://pdfs.semanticscholar.org/3712/ec1a3ff1b9ac063efaec12d473ee3d6575cf.pdf

[RLH06] REKHTER, Yakov ; LI, Tony ; HARES, Susan: A Border Gateway Protocol 4 (BGP-4) / Internet Engineering Task Force (IETF). Version: January 2006. http://www.rfc-editor.org/rfc/pdfrfc/rfc4271.txt.pdf. 2006 (4271). – Request for Comments

[SC09] SCUDDER, J. ; CHANDRA, R.: *Capabilities Advertisement with BGP-4*. RFC 5492 (Draft Standard). http://www.ietf.org/rfc/rfc5492.txt. Version: Februar 2009 (Request for Comments)

[TMS07] TRAINA, P. ; MCPHERSON, D. ; SCUDDER, J.: *Autonomous System Confederations for BGP*. RFC 5065 (Draft Standard). http://www.ietf.org/rfc/rfc5065.txt. Version: August 2007 (Request for Comments)

[TVG15] TEARE, Diane ; VACHON, Bob ; GRAZIANI, Rick: *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: (CCNP ROUTE 300-101) (Foundation Learning Guides)*. Indianapolis, USA : Cisco Systems, 2015. – ISBN 978–1–58720–456–2

[Wik] *Border Gateway Protocol*. https://de.wikipedia.org/wiki/Border_Gateway_Protocol, . – Accessed: 2017-01-17