Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

WS 2007/2008

Seminararbeit

IP-Multicast

Die Funktionsweise von IP-Multicast

Marcel Tschöpe

22. Januar 2008

Betreut durch Prof. Dr. Christian Schindelhauer

Abstract

Mit IP-Multicast existiert eine funktionsfähige Lösung zur Auslieferung von Paketen an mehreren Teilnehmern einer Multicastgruppe. Um dies verwirklichen zu können, werden spezielle Protokolle benötigt, die erstens Funktionen beinhalten zur Netzlastreduzierung, und zweitens Funktionen um Hostcomputer zu Gruppen zusammenzufassen. Mit diesem Dokument, möchte ich ein grundlegendes Multicastverfahren dar- beziehungsweise vorstellen.

Inhaltsverzeichnis

1 Einleitung

IP-Multicast soll eine zuverläsige und effiziente Möglichkeit bieten, Daten über ein Netzwerk, an mehrere Teilnehmer senden zu können. Hilfreich kann dies beispielsweise für Mediendienste, wie dem immer populärer werdenden IPTV, oder auch für Parallelinstallation von Betriebssystemen sein. Die Einsatzpunkte sind vielfältig. Die Frage ist jedoch, wie funktioniert IP-Multicast? Warum benutzt man nicht Broadcast? Diese Ausarbeitung verfolgt dabei das Ziel, die Funktionsweise von IP-Multicast näher zu bringen, indem es auf grundlegende Punkte, wie beispielsweise der Gruppenverwaltung oder in welcher Weise Multicast-Pakete über Netzwerke verschickt werden, versucht einzugehen.

2 Grundlagen Netzübertragung

Zunächst möchte ich ich diesem Kapitel die grundlegenden Nachrichtenübertragungsarten in einem Computernetzwerk vorstellen. Diese sind notwendig, um das Thema Multicast im weiteren Verlauf verstehen zu können.

2.1 Unicast

Als Unicast wird eine Punkt-zu-Punkt-Verbindung bezeichnet, also eine Verbindung zwischen 2 Teilnehmern in einem Netzwerk. Unicast-Verbindungen kommen beispielsweise

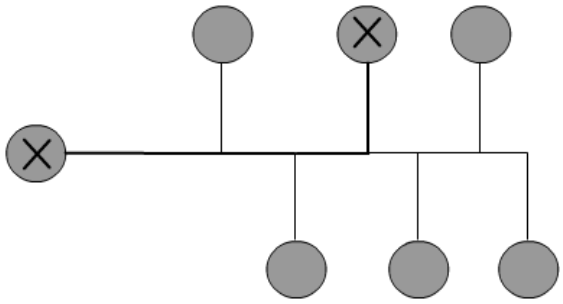

Abbildung 1: Modell für Unicast

beim Übertragen einer Datei,über das Netzerk zu einem anderen Computer, zustande. So bestehen die meisten Verbindungen im Internet aus Unicast-Verbindungen. Will man allerdings nicht nur an einen Clienten eine Nachricht schicken, ist Unicast ungeeignet,

da nun für jeden Empfänger eine Kopie der Nachricht verschickt werden muss, was die Netzlast unnötig erhöhen würde.

2.2 Broadcast

Broadcast, oder auch Rundruf auf Deutsch, bezeichnet eine Nachricht von einem Teilnehmer eines Netzwerkes an alle anderen Teilnehmer des selben Netzwerkes. Diese Art der Nachrichtenübertragung wird vorwiegend für Verwaltungszwecke verwenden, um beispielsweise MAC-Adressen[1] mit IP-Adressen[2] zu verbinden (siehe ARP). Hierbei wird, wie schon erwähnt, eine Nachricht an alle PCs eines Netwerkes gesendet, Rechner die nicht für diese gesendeten Pakete zuständig sind verwerfen diese Pakete automatisch.

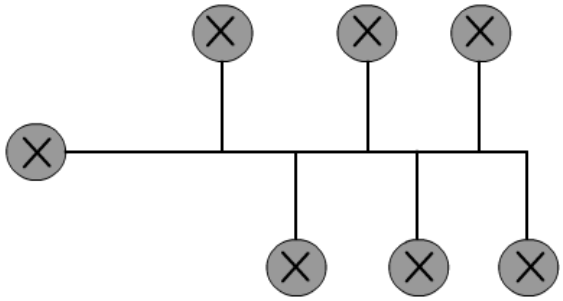

Abbildung 2: Modell für Broadcasting

Ein anderes Beispiel für Broadcast, ist das SMB-Protokoll[3] , welches per Broadcast versucht Drucker- und Netzwerkfreigaben zu finden. Das Problem bei Broadcast ist allerdings, dass es eine hohe Netzlast verursachen kann. Existiert beispielsweise ein hoher Broadcastanteil in einem Netzerk, so werden die Rechner in der Bearbeitung der Pakete ausgebremst und somit auch in der Bearbeitung der Applikation.

[1] Media-Access-Control, ist die Hardware-Adresse eines Netzwerkadapters, das diesen weltweit eindeutig identifiziert. Dient meistens zur Filterung von Paketen.

[2] **I**nternet **P**rotocol ist ein Netzwerkprotokoll, welches in der Vermittlungsschicht des ISO/OSI Modells angesiedelt ist und für die Übertragung von Paketen zustaändig ist.

[3] Das **S**erver **M**essage **B**lock - Protokoll wird hauptsächlich in Windows Netzwerken zur Steuerung von Netzwerkfreigaben verwendet.

2.3 Multicast

Multicast hingegen, stellt eine Verbindung von einem Host zu einer Gruppe von Rechnern da, deshalb wird Multicast auch als Gruppenruf bezeichnet. Der Vorteil von Multicast besteht darin, das jediglich eine Kopie der Nachricht verschickt wird, diese wird dann von Verteilern wie beispielsweise Router an alle Teilnehmer dieser Gruppe weitergeleitet.

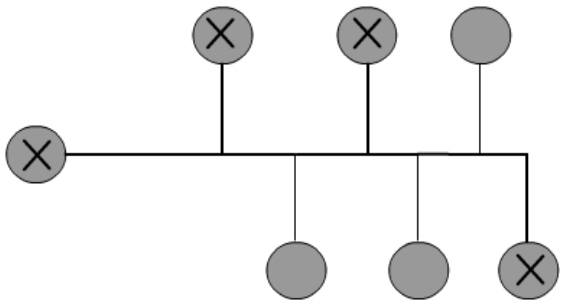

Abbildung 3: Modell für Multicast

Hierdurch wird die Bandbreite auf Seiten des Senders nicht mit der Anzahl der Empfänger multipliziert, was zur Folge hat, dass der Sender, im Gegensatz zu Unicast, die gleiche Bandbreite wie der Empfänger benötigt.

3 Funktionsweise von IP-Multicast

Es stellt sich nun die Frage,wie die erwähnten Gruppen verwaltet werden, Hostcomputer[4] zu Gruppen beitreteten können, und wie Pakete weitergeleitet und verteilt werden. Diese Fragen möchte ich in diesem Kapitel klären.

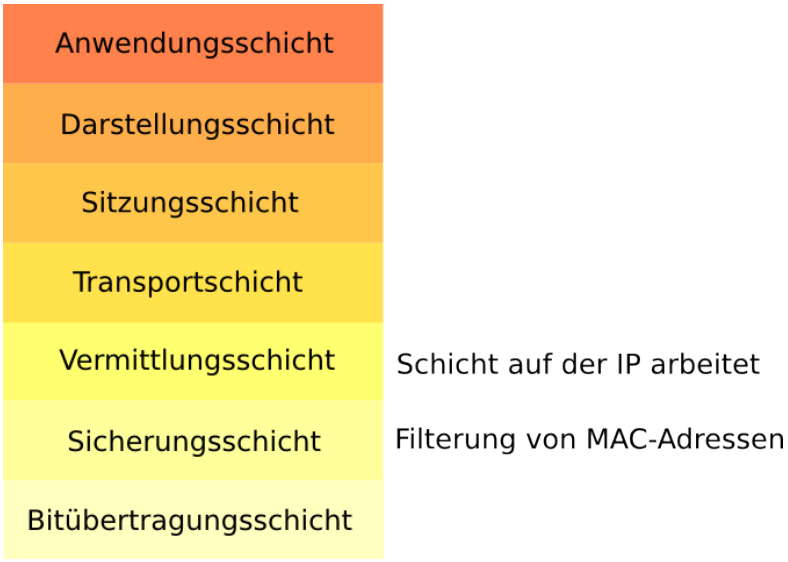

Abbildung 4: Das ISO/OSI Modell, Für IP-Multicast arbeitet auf der Vermittlungsschicht, IP unter anderem in Verbindung mit IGMP. Filterung gibt es allerdings schon in der Bitübertragungsschicht

3.1 Multicast auf Hardwareebene

Auf der Hardware-Ebene im ISO/OSI Modell, ist Multicast direkt realisiert. Ich möchte allerdings hierauf weniger eingehen, da sich diese Arbeit auf IP-Multicast konzentrieren sollte, und den Rahmen sprengen würde, der diese Arbeit umfasst. Daher möchte ich hierbei nur auf die Filtermechanismen der entsprechenden Hardware eingehen, welche für Multicast von Relevanz sind. So werden bei der Übertragung über Ethernet, IP-Multicast-Adressen auf sogenannte Pseudo-MAC-Adressen abgebildet, um somit die

[4] hier: ein Rechner, der Teil eines Netzwerkes, beispielsweise des Internets, ist und DIenste, hier Multicast, in Anspruch nimmt.

vorhin erwähnte Filterung durch die Netzwerkkarte zu ermöglichen. Dies hat den Vorteil, dass die Netzlast reduziert wird und somit auch der jeweilige Rechner weniger Daten verarbeiten muss, wobei die IP-Software entlastet wird, die ansonsten überprüfen muss ob die entsprechenden Pakete für sie bestimmt sind. Um dies zu erreichen, ist die Hälfte der Ethernet-Adressen für Multicast reserviert, indem im ersten Oktett ein Bit gesetzte wird. Somit sieht die Darstellung einer Multicastadresse folgendermaßen aus: $01-00-00-00-00-00_{16}$.
Wie man sehen kann ist das Bit im ersten Oktett gesetzt worden, wodurch diese Adresse eine Multicast-Adresse repräsentiert. IP setzt nun die untersten 23 Bit der IP-Adresse in die MAC-Adresse $01-00-5e-00-00-00_{16}$ ein.
Da allerdings 28 Bit für die Multicastgruppen zur Verfügung stehen und nur 23 Bit für die MAC-Adresse, ist das Mapping der IP-Adresse auf die Hardwareadresse nicht eindeutig, kann allerdings auf Grund der Tastsache, dass es relativ unwahrscheinlich ist 2 gleiche MAC-Adressen im selben Subnet zu haben, vernächlässigt werden. Ebenso hat dieses Verfahren den Vorteil Probleme mit anderen Protokollen welche Ethernet benutzen zu vermeiden, wodurch Fehleranalyse leichter wird.

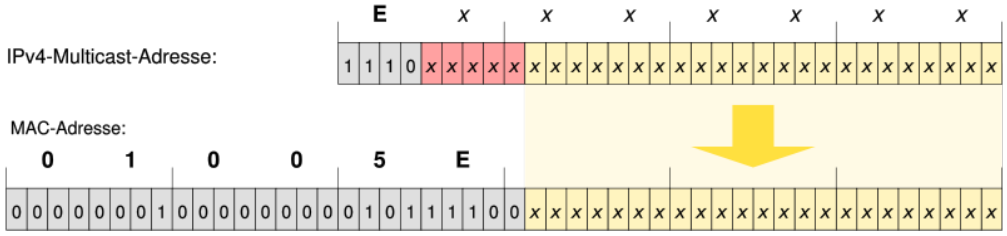

Abbildung 5: Das Abbilden der Multicastadresse auf eine MAC-Adresse aus [1]

Hierdurch ergibt sich ein Bereich von
$01-00-5e-00-00-00_{16}$ bis maximal $01-00-5e-7f-ff-ff_{16}$.
Durch dieses Verfahren, akzeptiert die Netzwerkkarte nur noch Multicast-Pakete, die an ihre MAC-Adresse gerichtet sind.

3.2 Multicast auf Netzwerkebene

Bei IP-Multicast ist eine Adressierung notwendig, die entweder statisch, um beispielsweise zu einem Multicast-Server verbinden zu können welcher zum Beispiel Streaming-Dienste anbietet, oder dynamisch ist, um zu einer besagten Multicast-Gruppe beizutreten. Dynamisch deshalb, weil Multicast-Gruppen nicht immer existent sein müssen,

so können private Gruppen entstehen und ebenso leicht wieder aufgelöst werden. IP-Multicast Adressen müssen sich hierbei von gewöhnlichen IP-Adressen unterscheiden, um festzulegen, dass ein Paket per Multicast versendet werden muss. Das IP-Protokoll hat hierzu den sogenannten **D-Class** Adressraum reserviert, welcher neben den Klassen **A**,**B**,**C** die für Unicast bestimmt sind, eingeführt wurde. Hierzu werden die ersten 4 Bits der IP-Adresse auf 1110 gesetzt, wodurch 4 der 32 Bit einer IP-Adresse benutzt werden und somit maximal 2^{28} IP-Adressen für IP-Multicast zur Vefügung stehen. In Dezimalnotation ergibt sich somit der Adressbereich, 224.0.0.0 bis 239.255.255.255, wovon allerdings einige Adressen für besondere Zwecke reserviert sind, dazu jedoch später. Dieser gesamte Adressbereich steht für benutzerdefinierte Gruppen zur Verfügung, wobei

Abbildung 6: Bildung einer Multicast-IP-Adresse nach [4]

jede Adresse eine Host-Gruppe repräsentiert. Will ein Host nun eine Nachricht zu einer Gruppe senden, trägt er diese entsprechend als Empfängergruppe ein, worauf jeder Client dieser Host-Gruppe die Nachricht empfängt. Die Aufgabe wie diese Nachricht die Empfänger erreicht, wird gewöhnlicherweise Routern in einem Netzwerk überlassen. Hierzu wird ein Multicast-Baum aufgebaut, welcher bestimmt wie die Knoten, in diesem Fall die Router, miteinander verbunden sind, und zwar immer nur auf einem möglichen Weg die verschiedenen Hostcomputer zu erreichen. Dazu möchte ich allerdings, der Übersicht halber, erst in einem späteren Kapitel eingehen.

3.3 Der Begriff Datengramm

Um die Folgenden Kapitel verstehen zu können, muss eine grundlegende Frage geklärt werden. Was sind Datengramme? Ein Datengramm, ist im Prinzip das Paketformat, bestehend aus einem Header und den eigendlichen Daten.

3.4 Reservierte Adressbereiche / Scope-Netze

Wie schon erwähnt gibt es auch bei IP-Multicast reservierte Adressbereiche, welche zum Teil für die verwendeten Protokolle notwenig sind. So ist der Adressraum 224.0.0.0 bis 224.255.255.255 für Routingprotokolle reserviert, hier sendet der Host keine Multicast Datengramme.
In Tabelle2, kann man einige Beispiele zu den reservierten Adressen erkennen.

Adresse	Bedeutung
224.0.0.1	Alle Computer in einem Subnet werden angesprochen
224.0.0.2	Alle Router in einem Subnet werden angesprochen
224.0.0.12	Alle DHCP-Server werden angesprochen
224.0.0.4	Adresse wird vom **D**istance **V**ector **R**outing **P**rotokoll benutzt
224.0.0.22	Adresse wird vom **I**nternet **G**roup **M**anagment **P**rotokoll benutzt

Weiterhin ist der Bereich 239.0.0.0 bis 239.255.255.255 für sogenannte Scope-Netze reserviert. Scope Netze, sind Multicast Netzwerke, dessen Pakete ein bestimmtes lokales Netzwerk nicht verlassen. Diese Netzwerke sind also nicht öffentlich zugänglich und Datagramme werden von Router und Switches nicht zu anderen Routern weitergeleitet. Meistens wird auch noch ein TTL-Wert in den Header der Pakete geschrieben, welcher die Sprünge über Router begrenzt. Scope-Netzwerke sind beispielsweise für Firmen sehr interessant, da man so ein internes Multicastnetzwerk aufbauen kann.

4 IGMP, das Internet Group Management Protocol

Das **I**nternet **G**roup **M**anagement **P**rotocol, kurz *IGMP*, wird dazu genutzt, damit Hostcomputer zu Multicastgruppen beitreten. Hierzu verfährt *IGMP* auf zwei unterschiedlichten Wegen. Zum Einen, teilen die entsprechenden Hosts ihre Gruppenmitgliedschaft durch das Senden von *IGMP* Nachrichten an den entsprechenden lokalen Router mit. Zum Andern, senden die Router nach einer bestimmten Zeit Abfragen an Hostcomputer einer Gruppe, um festzustellen ob die entsprechende Gruppe existiert oder ob diese aufgelöst wurde. *IGMP* selber ist dabei Bestandteil von IP, und benutzt dessen Datengramme um die erwähnten Nachrichten zu versenden. Von *IGMP* selber gibt es zur Zeit drei verschiedene Versionen, welche sich geringfügig unterschieden.

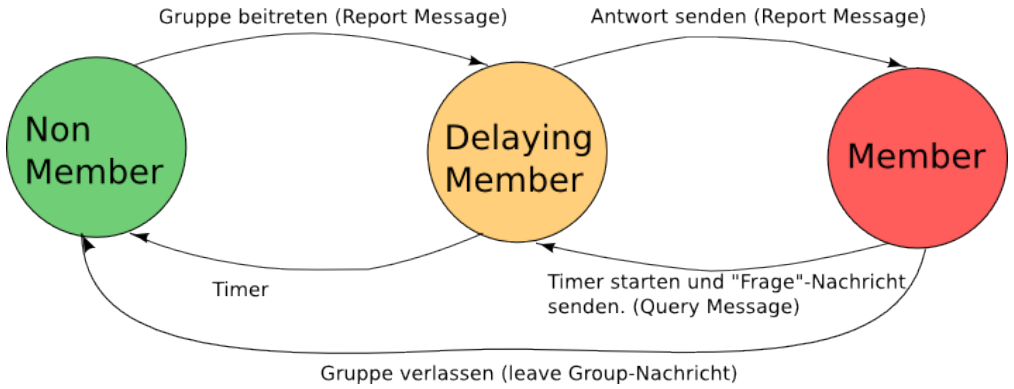

Abbildung 7: Das Prinzip, welches zu Grunde liegt, wie Hosts einer Gruppe teilnehmen nach [4]

In dem folgenden Kapitel werde ich kurz auf die verschiedenen Versionen eingehen und deren Funktionsweise erklären.

4.1 IGMPv1

In *IGMPv*1 existieren nur 2 Arten von Nachrichten, *Membership-Query*-Nachrichten und *Membership-Report*-Nachrichten. *Membership-Query*-Nachrichten sind dabei solche, die von dem Router zur Überprüfung der Gruppenaktivität, wie schon vorhin erwähnt, benutzt werden. *Membership-Report*-Nachrichten werden hingegen von einem Hostcomputer versendet, wenn dieser Zu einer Gruppe beitreten will. Mit *IGMPv1* verläuft das Beitreten einer Gruppe folgendermaßen: Will ein Hostcomputer zu einer bestimmten Mul-

ticastgruppe beitreten, so sendet der Host durch IP, eine *Membership-Report*-Nachricht, sobald ein Programm auf dem Host eine Verbindung zu einer Multicastgruppe herstellen möchte.

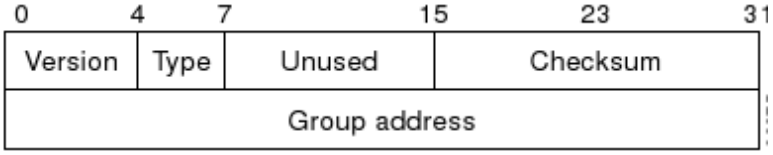

Abbildung 8: Der Header einer IGMPv1 Nachricht aus [5] und [?]

Der Router hingegen überprüft mit Hilfe von *Membership query*-Nachrichten, die ebenfalls über IP versendet werden, ob mindestens ein Host in dieser Multicastgruppe existiert. Werden drei Nachrichten von keinem Gruppenmitglied beantwortet, wird der Router das Weiterleiten der Pakete stoppen, und somit die Gruppe in seinem Netz auflösen.

4.2 IGMPv2

Im Prinzip arbeitet *IGMPv2* genauso wie *IGMPv1*, allerdings bietet es nun vier Arten von Nachrichten, die versendet werden können, wobei der Hauptunterschied zu Version 1, die *leave Group*-Nachricht ist. Mit dieser können Hosts, einem Router mitteilen, dass sie aus einer Multicastgruppe austreten möchten, dies verringert die Netzlast. Ist ein Host-

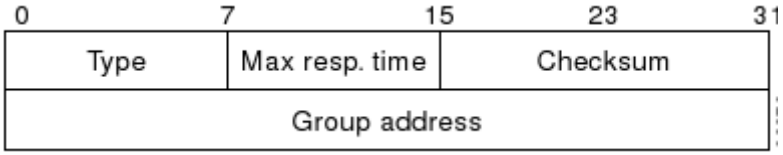

Abbildung 9: Der Header einer IGMPv2 Nachricht aus [5] und [2]

computer nun aus einer Gruppe ausgetreten, so sendet der Router, wie auch zuvor, eine *Membership-Query*-Nachricht, um festzustellen ob die Multicast Gruppe noch benutzt wird. *IGMPv2* ist dabei zu *IGMPv1* abwärtskompatibel, weshalb es nun die besagten vier Nachrichtentypen in *IGMPv2* gibt:

- *Membership-Reportv1*-Nachricht
- *Membership-Reportv2*-Nachricht

- *Membership-Query*-Nachricht
- *Leave-Group*-Nachricht

4.3 IGMPv3

Mit *IGMPv3* wurde nun Adressenfilterung hinzugefügt. Hierdurch kann ein Host, einem Router signalisieren, von welcher Multicastgruppe er Pakete empfangen will und von welcher nicht. Hierzu wird das Feld *REC TYPE* in einer *Membership-Report-Nachricht*, entweder auf *MODE IS INCLUDE* oder auf *MODE IS EXCLUDE* gesetzt.
Ist ersteres gesetzt, wird der Router alle nachfolgenden im IP-Header unter *SOURCE ADRESS[n]*(siehe unten) stehenden Adressen, entsprechende Multicast-Pakete schicken. Ist letztere Option gesetzt, so werden die enthaltenden Adressen in der Tabelle des Routers gelöscht, und somit ausgeschlossen, was bedeutet, dass die Hostcomputer mit den entsprechenden Adressen keine Multicast-Pakete aus der Gruppe mehr empfangen werden. Dieses Verfahren hat wieder einmal den Vorteil, weniger Netzlast zu verbrauchen. *IGMPv3* benutzt hierbei wieder zwei Arten von Nachrichtentypen:

- *Membership-Report*-Nachricht
- *Membership-Query*-Nachricht

, wobei sich der IP-Header, der entsprechenden Nachrichtentypen, im Gegensatz zu Version 1 und 2, wesentlich vergrößert hat. Im folgenden möchte ich den IP-Header für *IGMPv3-Membership-Query*-Nachrichten beschreiben.

4.4 IGMP Membership Query Message Format

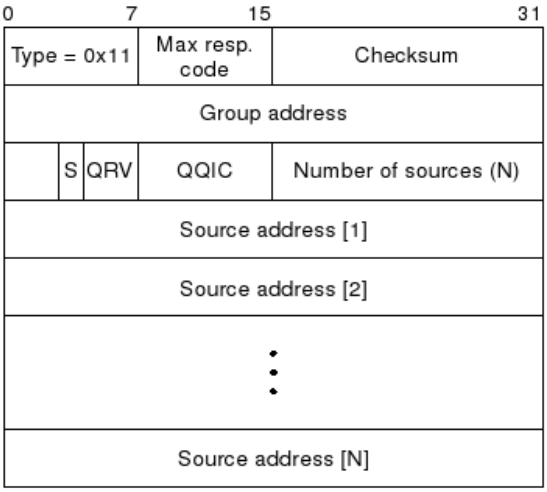

Abbildung 10: Der Header einer IGMPv3 Membership-Query-Nachricht aus [5] und [3]

Feld	Beschreibung
TYPE	Gibt die Art der Nachricht an $TYPE = 0x22$ steht hierbei für Membership Report Messages, $TYPE = 0x11$ steht dabei für Membership Query Messages
RESP CODE	Dieses Feld definiert die maximale Wartezeit, bevor eine Antwortnachricht gesendet wird
Group Adress	Die Adresse der Multicast Gruppe
S	Beim setzen dieses Feldes auf 1 Bit, wird das Timerupdate unterdrückt.
QVR	dieses Feld beinflusst wie oft Pakete versendet werden, nützlich für Netze mit hoher Verlustrate
QQIC	**Q**uerier's **Q**uery **I**nterval **C**ode, es bestimmt die Zeit , in Sekunden, in der Query Messages gesendet werden.
NUMBER OF SOURCES	Bestimmt Anzahl der Quell-Adressen in der Anfrage.

Für das *IGMP*v3-Membership-Report-Message-Format werden die gleichen Felder bis auf ein paar Ausnahmen benutzt, diese sind wie folgt beschrieben:

4.5 IGMP Membership Report Message Format

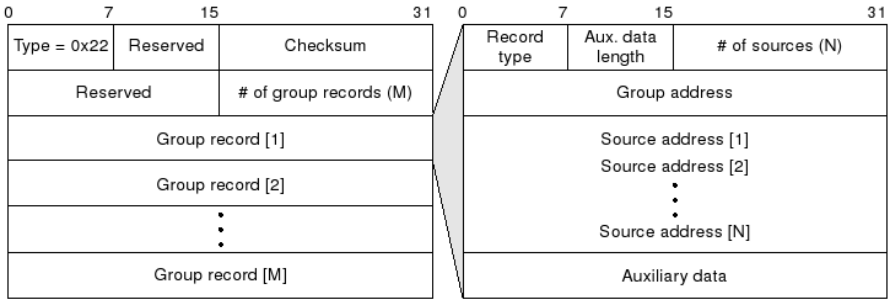

Abbildung 11: Der Header einer IGMPv3 Membership-Report-Nachricht aus [5] und [3]

Feld	Beschreibung
NUM Group Records	Anzahl der Gruppen die in den nachfolgenden Feldern angegeben werden
GROUP RECORD	Dieses Feld besteht nun aus weiteren Informationen, siehe folgende Felder
REC TYPE	gibt an ob Adressen ausgeschlossen oder eingebunden werden sollen (e.g., **MODE IS INCLUDE**, **MODE IS EXCLUDE**).
NUM OF SOURCES	Anzahl der Quell-Adressen
SOURCE ADRESS[N]	Adressangabe

5 Multicast- Forwarding und Routing

IGMP ist, wie wir in vorherigen Kapitel erfahren haben, für die Gruppenverwaltung zuständig ist. Allerdings muss es noch ebenso ein Verfahren geben, welches die Pakete über lokale Netzwerke, beispielsweise über mehrere Router, hinweg transportiert, wenn Hostcomputer über mehrere Netzwerke verteilt sind. Diese Aufgabe werden hierbei von speziellen Routingprotokollen erfüllt. Da es kein Standard-Protokoll für das Packet-Forwarding in Multicastnetzwerken gibt, werde ich in diesem Kapitel auf die grundlegenden Algorithmen eingehen, welche von Routingprotokollen verwendet werden. Zum Abschluss des Kapitels, werde ich noch eine kleine Aufzählung von Protokollen abdrucken. Der Grund dieser Protokollvielfalt liegt darin, dass jedes Protokoll für eine andere Aufgabe erstellt wurde. So gibt es Protokolle die sich besonders gut eignen, wenn Gruppenmitglieder in großen Netzwerken nah bei einander befinden. Andere Protokolle hingegen eignen sich gut für weit auseinander liegende Gruppen.

5.1 RPF - Reverse Path Forwarding

Wenn eine Host eine Nachricht an eine Multicastgruppe sendet, so muss der Router wissen, wohin Pakete weitergeleitet werden müssen. RPF ist hierbei ein grundlegendes

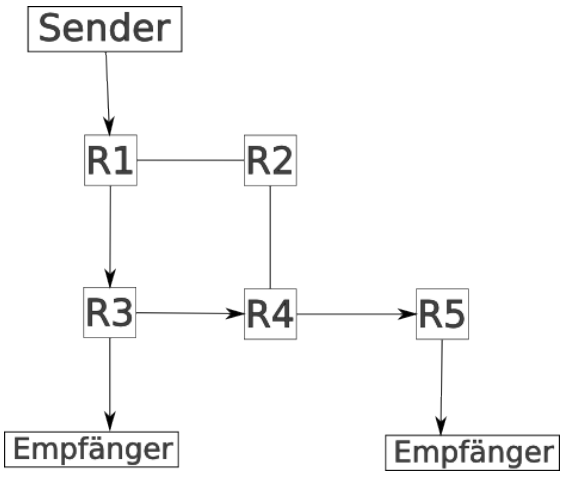

Abbildung 12: Ein Distributiontree gibt den Weg von Sender bis zu den Empfängern an nach

Prinzip, welches dafür sorgt wie Pakete über Router hinweg zu ihrem Ziel kommen. Hierzu

wird zu aller erst, von RPF, win Broadcast an alle Router durchgeführt. Diese überprüfen nun auf welchem Wege die Pakete angekommen sind, und leitet diese auch nur dann weiter, falls das Paket von einer anderen Schnittstelle kommt, als es der Router versendet hat. Durch dieses Verfahren, welche alle Router erreicht, bildet sich ein sogenannter Multicastbaum, den jeder Router durch RPF erstellt. Bei dem Multicastbaum ist der Ausgangspunkt, oder die Wurzel, immer der Sender (in diesem Fall also der Router). Über diesen Multicastbaum sind die Router nun auf dem kürzesten Weg erreichbar.(siehe Abbildung 12). Hierzu verwendet Reverse Path Forwarding dabei folgendes Verfahren, welches ich kurz Erläutern möchte.
Kommt ein Paket an einer Schnittstelle eines Routers an, überprüft der Router mittels RPF, ob das Paket weitergeleitet oder verworfen wird. Dabei arbeitet RPF wie folgt:

- Als erstes vergleicht der Router die Source-Adresse aus dem Header des empfangenen Pakets, mit dem Eintrag aus der Routing-Tabelle.
- Ist das Paket, wie in Abbildung 13, auf einer anderen Schnittstelle angekommen, als von der Schnittstelle, die in der Routing-Tabelle eingetragen ist, um das Paket weiterzuleiten. So wird das Paket verworfen.

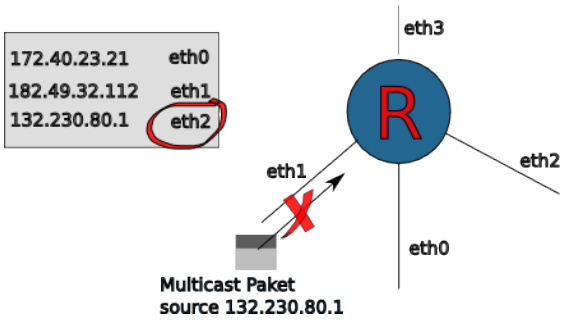

Abbildung 13: Das Paket von der Quelle 132.230.80.1 kommt auf dem falschen Interface an, denn Pakete von dieser Adresse, sollten laut der Routing-Tabelle (links oben) auf Interface eth2 ankommen nach [5]

- Kommt das Paket von der Schnittstelle, dessen Source-Adresse mit der Netzwerkschnittstelle aus der Routing-Tabelle übereinstimmt, so wird das Paket weitergeleitet.(siehe Abbildung 14)

Durch das Überprüfen auf welchen Schnittstellen ein Paket ankommt, wird sichergestellt, dass Router auf dem kürzesten Weg miteinander verbunden werden.

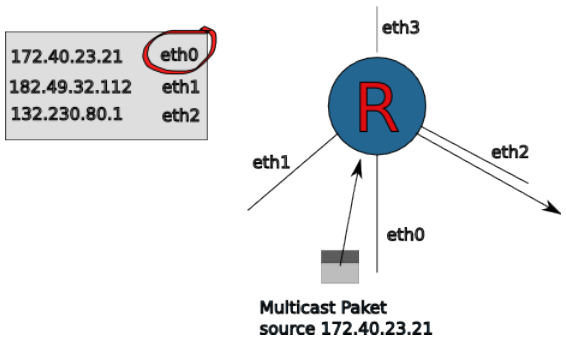

Abbildung 14: Das Paket von der Quelle 172.40.23.21 kommt laut Routing Tabelle auf dem richtigen Interface an und wird weitergeleitet nach [5]

Auf Reverse Path Forwarding bauen zahlreiche Multicast-Routing-Protokolle, wie beispielsweise PIM [5] auf.

5.2 TRPF - Truncated Reverse Path Forwarding - eine Verbesserung von RPF

TRPF unterscheidet sich kaum von RPF, allerdings bietet es einen Unterschied: es sendet keine Pakete an Router, welche keine Multicastgruppenmitglieder besitzen. Hierfür werden allerdings auch 2 Informationen benötigt, die ein Router beherrschen muss.

1. ,wird wieder eine Routing Tabelle benötigt und
2. ,wird ausserdem eine Liste der Gruppen, welche durch ein Netzwerkinterface erreichbar sind benötigt.

Das weitere Verfahren beschreibt sich wie folgt: Erreicht ein Mutlicast-Paket den Router, so wird erst das Verfahren., welches von RPF bekannt ist durchgegangen. Wird das Paket durch RPF zum weitersenden spezifiziert, so tritt allerdings eine neue Regel von TRPF in Kraft. TRPF überprüft nun ob sich mindestens ein Gruppenmitglied, von der Zieladresse des Paketheaders, auf der zu versendende Netzwerkschnittstelle befindet. Ist kein Gruppenmitglied über diese Schnittstelle erreichbar, so wird die nächste Schnittstelle überprüft.

[5] Protocol Independent Multicast, ein Multicast-Routingprotokoll

5.3 RPM - Reverse Path Multicast

Reverse **P**ath **M**ulticast implementiert nun TRPF und macht dieses dadurch einsetzbar. RPM geht in zwei Schritten vor. Der erste Schritt, wie auch von RPF bekannt, sendet einen Broadcast an alle Router des Netzwerkes. Nun verfahren die Router nach dem Prinzip von RPF, tauschen allerdings ebenso Informationen gegenseitig aus, auf welchen Pfaden sich Multicastgruppenmitglieder befinden. Da die lokalen Router durch IGMP jeweils Gruppenmitglieder aus ihren lokalen Netzwerken kennen, wird dies möglich. Befinden sich nun keine Gruppenmitglieder auf einem Pfad, so wird diese Information an den nächsthöheren Router geschickt. Besitzt dieser Gruppenmitglieder in seinem Netzwerk, so wird der Pfad zu den Gruppenmitgliederlosen Routern aus der Routingtabelle ausgetragen, wodurch der Zweig sozusagen abgeschnitten wird. Dies nennt man deshalb auch "pruning". Besitzt dieser Router jedoch ebenfalls keine Gruppenmitglieder in seinem Netzwerk, so gibt er diese Information an seinen ihm übergeordnetem Router in seiner Routingtabelle weiter. Angenommen ein Router hat in seinem lokalen Netzwerk einen Hostcomputer, der an einer Gruppe teilnehmen will, allerdings der Router mittels "pruningäus dem Multicastbaum "herausgeschnitten"wurde. So muss der Router eine sogenannte *"graft request"* senden, welche den Multicastbaum, durch das selbe Verfahren, neu aufbauen lässt. Dadurch wird der abgeschnittene Zweig wieder hinzugefügt.

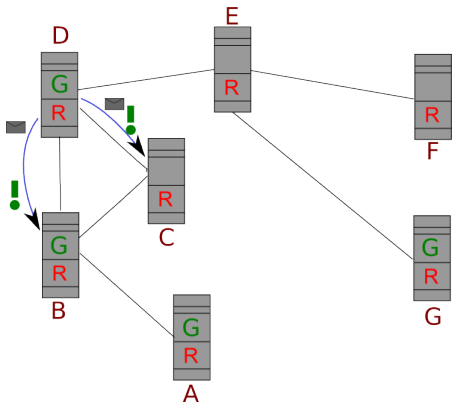

Abbildung 15: Angenommen Router A,B,D und G besitzen in ihren jeweiligen lokalen Netzwerken Gruppenmitglieder, so zeigt Abbildung 16 den dazugehörigen Multicastbaum von Router B. Das grüne Ausrufezeichen-Symbol bedeutet, dass Informationen über Gruppenmitgliedschaften ausgetauscht werden, während das kleine Briefsymbol eine Broadcastnachricht repräsentiert.

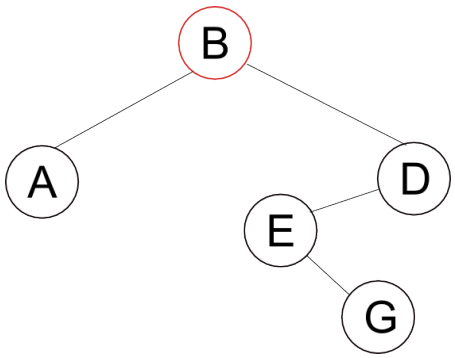

Abbildung 16: Der zu Abbildung 15 gehörende Multicastbaum von Router B

5.4 Und die Routingprotokolle ?

Wie schon vorher erwähnt, gibt es kein Standard-Protokoll für Mlticast-Routing. Allerdings greifen diese Protokolle auf die vorgestellten Algorithmen, wie RPF oder RPM, zurück. Der Grund, weshalb es eventuell keinen Standard geben darf, ist die Tatsache, dass sich Multicastnetzwerke im Aufbau unterschieden können. So ist ein Netzwerk zwar eher kleiner, allerdings sind die Gruppenmitglieder weit verteilt. Ein anderes hat eine große Ausdehnung, die Gruppenmitglieder sind allerdings gleichmäßig verteilt. Hierdurch wurden unterschiedliche Protokolle für bestimmte Einsatzzwecke entwickelt.

- Distance Routing Vector Multicast Protocol (DVMRP), basiert beispielsweise auf RPF
- Protocol Multicast Independent Multicast (PIM)
- Multicast extensions to OSPF (MOSPF)
- Core Based Trees (CBT)

Abbildungsverzeichnis

Literatur

[1] Wikipedia: The Free Enzyklopedia. http://de.wikipedia.org, 2007-08-15.

[2] Multicast- IGMPv2. http://www.faqs.org/rfcs/rfc2236.html, 2007-08-15, 1997.

[3] Multicast- IGMPv3. http://www.ietf.org/rfc/rfc3376.txt, 2002-10, 2002.

[4] Douglas E. Comer. *Internetworking with TCP/IP 5th Edition, ISBN 0-13-187671-6.* Prentice Hall, 2006.

[5] Cisco Systems. *IP Multicast - Technology Overview.* http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mcstsol/mcstovr.pdf, 2002.