Broadcast-Reduzierung

Die Entstehung unkontrollierter *Broadcasts* ist zumeist durch Protokollfehler oder Netzwerkstörungen bedingt. Sie werden durch Brücken nicht daran gehindert, das lokale Netzwerksegment zu verlassen und dadurch den gesamten Netzwerkverbund zu überfluten. Diese *Broadcast-Stürme* lassen sich im globalen Netzwerk durch den Einsatz von Routern vermeiden. Sie analysieren die Datenpakete und entscheiden nach Überprüfung, ob ein Broadcast weitergeleitet oder verworfen werden soll. Dadurch lässt sich vermeidbarer Broadcast im lokalen Segment isolieren.

Insbesondere bei LAN-WAN-Verbindungen steht die Broadcast-Problematik an erster Stelle, denn »normale« Broadcast-Situationen oder gar Broadcast-Stürme, die als »Grundrauschen« im Hochgeschwindigkeits-LAN kaum wahrgenommen werden, machen sich im WAN sehr schnell negativ bemerkbar.

4.2 Routing-Protokolle

Die Intelligenz oder Logik des *Routings* ist in speziellen *Routing-Protokollen* implementiert; diese stellen auf verschiedene Art und Weise Verfahren zur Verfügung, um den Routing-Prozess zu realisieren. Je nach Bedarf lässt sich ein Protokoll wählen, das ein fest umschriebenes Spektrum an Funktionalität bietet. Oft hängt die Wahl des Routing-Protokolls auch von der eingesetzten Router-Hardware ab. Dies ist mittlerweile jedoch recht selten geworden, da fast alle Hersteller von Routern auch die wichtigsten Routing-Protokolle in ihren Geräten zur Verfügung stellen.

Neben den Routing-Protokollen gibt es zusätzlich die Bezeichnung der *routbaren* Protokolle. Darunter versteht man ein Protokoll, das auf der Netzwerkschicht (Layer 3) adressiert werden kann. Ein Routing-Protokoll wird hingegen ausschließlich für die Kommunikation zwischen Routern verwendet. Nachfolgend sind die wesentlichen Varianten dieser beiden Protokolltypen aufgeführt:

Routbare Protokolle

- Internet Protocol (IP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Control Message Protocol (ICMP)

Routing-Protokolle

- Border Gateway Protocol (BGP)
- Exterior Gateway Protocol (EGP)
- Open Shortest Path First (OSPF)

- Routing Information Protocol (RIP)
- DECnet Routing Protocol (DRP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- IS-IS
- Integrated IS-IS

Router werden – wie andere Netzwerkkomponenten auch – über ihre MAC-Adresse angesprochen, wodurch diese wiederum über einen *ARP-Reply* bekannt gemacht werden. Handelt es sich um ein Datenpaket, das mittels Ethernet-Protokoll übertragen wird, wird in der Routing-Protokollsoftware derjenige Prozess aktiviert, der für eine Überprüfung des Ethernet-Pakets zuständig ist. Nach erfolgreicher Überprüfung wird der Ethernet-spezifische Teil des Pakets abgetrennt und die IP-Logik aktiviert. Diese überprüft ihrerseits den IP-Teil des Datenpakets. Ist auch diese Überprüfung erfolgreich (fehlerfrei), so können anschließend Mechanismen eingesetzt werden, die über *Access Control Lists* (ACL) das Datenpaket gezielt weiterleiten oder den Weitertransport verhindern. Die Routing-Tabelle liefert dabei die Information, welcher physische Port angesprochen und welcher Router in Anspruch genommen werden muss, um das Datenpaket an das jeweils adressierte Netzwerk (anhand der Netz-ID) zu transportieren. Handelt es sich bei dem nächsten Ziel-Netzwerk beispielsweise um ein Token-Ring-Netzwerk, so wird der vollständige Token-Ring-Frame zusammengebaut und über den entsprechenden Router-Port an das Netzwerk abgegeben.

4.2.1 Routing Information Protocol (RIP)

RIP ist ein schon recht »betagtes« Distance-Vector-Protokoll, das im Verlauf der Zeit einen überaus großen Verbreitungsgrad erfahren hat. Es wird trotz seiner teilweise nicht unerheblichen Mängel gern eingesetzt, nicht zuletzt deshalb, weil es nahezu auf allen Routern verfügbar und sehr leicht implementierbar ist.

Leistungsmerkmale

RIP (*Routing Information Protocol*) hat sich zu einem Zeitpunkt etabliert, als die Netzwerke noch relativ klein und überschaubar waren. Nur selten existierten innerhalb eines Netzwerks verschiedene Leitungsqualitäten mit unterschiedlichen Geschwindigkeiten. Diese Merkmale, die sich infolge der Heterogenität gewachsener Netzwerkstrukturen allmählich herausgebildet haben, stellen heute in den meisten Unternehmen eine Ausgangsbasis dar, die für ein homogenes Routing nicht unerhebliche Probleme aufwirft. Die Verfügbarkeit lediglich einer einzigen Metrik (Hop-Count) führt beim RIP oft zu einer nicht sehr realistischen Routenoptimierung, denn wenn allein die Anzahl der Hops bzw. der zu passierenden

Router für eine Wegewahl entscheidend sein soll, so werden schnelle Netzabschnitte (z.B. Fast Ethernet mit 100 Mbit/s) und deutlich langsamere (z.B. 64-kbit/s-ISDN-Festverbindungen im WAN) unter Umständen gleich gewichtet, was zu einer drastischen Fehleinschätzung der günstigsten Route führt. RIP lässt darüber hinaus die Bildung von Subnetzen nicht zu und schränkt somit seine Routing-Flexibilität deutlich ein.

In Zeitintervallen von 30 Sekunden erfolgt ein vollständiges Update der Routing-Tabellen. Geht man nun von einer Störung zwischen zwei Routern aus, so kann es bis zu 7,5 Minuten (15 Hop-Counts × 30 Sekunden = 7 Minuten 30 Sekunden) dauern, bis RIP diese Störung erkennt und die betreffende Route aus seiner Tabelle streicht; denn erst wenn der nach jedem Tabellen-Update ermittelte neue Hop-Count für die Erreichbarkeit eines Ziels im Netzwerk den Wert 15 erreicht hat, wird die Aussage »nicht erreichbar« getroffen.

Bewertung

Eine Übersicht der Vor- und Nachteile lässt den Schluss zu, dass RIP nicht mehr zeitgemäß ist. Kleine und einfache Netzwerke jedoch können durch RIP-Funktionalität im Großen und Ganzen ausreichend bedient werden.

- Vorteile
  - sehr einfach zu implementieren
  - nahezu überall verfügbar
  - Algorithmus recht einfach und daher leicht zu durchschauen
  - Public Domain
- Nachteile
  - keine Subnetzadressierung
  - lange Reaktionszeit bei Störungen (schlechte Konvergenz)
  - einzige Metrik ist der Hop-Count
  - unterschiedliche LAN/WAN-Geschwindigkeiten lassen sich nicht berücksichtigen
  - hoher LAN/WAN-Traffic durch vollständige Routing-Tabellen-Updates in festen Intervallen

Implementierung

Die Implementierung des RIP erfolgt unter Verwendung des sogenannten *routed* bzw. *route daemons*. Es handelt sich dabei um einen Prozess, der auf allen dedizierten Routern automatisch aktiviert ist und auf Workstations (UNIX-Maschinen oder auch Personalcomputern wie z.B. Windows-Server als Dienst) mit Router-Funktionalität und (mindestens) zwei Netzwerkcontrollern optional gestartet werden kann.

HINWEIS

In vielen Fällen wird beim RIP eine *Default Route* (meist 0.0.0.0) angegeben, mit der die Festlegung von Routen definiert wird, die dann zu benutzen sind, wenn die adressierte Netzwerkadresse vom Router nicht erreicht werden kann.

4.2.2 RIP-Version 2

Die Weiterentwicklung von RIP in der Version 2 stellt grundsätzlich kein völlig neues Routing-Protokoll dar, sondern liefert lediglich einige wichtige Erweiterungen zur alten Version 1. Details hierzu sind im RFC 2453 vom November 1998 nachzulesen. So gibt es einige geringfügige Unterschiede hinsichtlich des *Message-Formats*. Während der *Frame-Header* in beiden Versionen identisch ist, weist der *Frame-Body* Unterschiede auf.

Der RIP-Header besteht aus den Feldern:

- *command (8)*
  Ein in diesem Feld eingetragener Wert von »1« markiert das Datagramm als RIP-Request, der Wert »2« bezeichnet eine RIP-Response.
- *version (8)*
  Dient zur Identifikation der RIP-Version.
- *reserved (16)*
  Dieses zwei Oktette umfassende Feld ist mit binären Nullen belegt.

In der RIP-Version 1 wird dem Header ein sogenannter *RIP entry* angefügt, der aus insgesamt 20 Oktetten besteht. Jeder *RIP entry* umfasst die folgenden Felder:

- *address family identifier (16)*
  Besitzt den Wert »2« in der RIP-Version 1, in RIPv2 kann der AFI unterschiedliche Werte annehmen.
- *reserved (16)*
  Dieses zwei Oktette umfassende Feld ist mit binären Nullen belegt.
- IPv4 address (32)
  Ziel-IP-Adresse
- *reserved (32)*
  Dieses vier Oktette umfassende Feld ist mit binären Nullen belegt.
- *reserved (32)*
  Dieses vier Oktette umfassende Feld ist mit binären Nullen belegt.
- *metric (32)*
  Anzahl der erforderlichen Hops (Metrik) bis zur Erreichung des Zielnetzwerks. Es sind Werte zwischen 1 und 15 definierbar; der Wert 16 wird als »Netzwerk unerreichbar« interpretiert.

Die in RIPv2 erstmals vorgesehene Authentifizierung belegt einen vollständigen (und zwar den ersten) 20-Bytes-Routeneintrag. Allerdings kommt hier lediglich eine einfache Kennwortauthentifizierung zur Anwendung.

- *Identification (16)*
  Zwei Bytes mit dem Inhalt 0xFFFF für die Kennung
- *Authentication type (16)*
  Dieses Feld gibt den Authentifizierungstyp an. Derzeit ist allerdings nur der Typ *Passwort* definiert.
- *Authentication (128)*
  Dieses Feld enthält das Kennwort (maximal 16 Zeichen bzw. Bytes).

Die verbleibenden maximal 24 Routeneinträge können dann gemäß RIPv2-Message-Format (siehe Abb. 4–6) gebildet werden. Hier wird dann im Unterschied zur RIPv1 eine Subnetzmaske eingeführt.

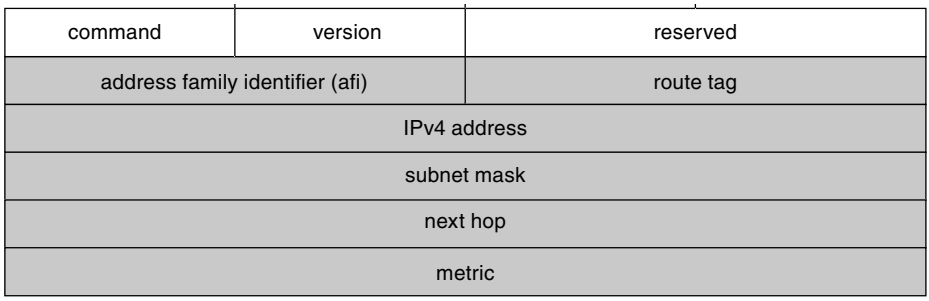

Abb. 4–6 *RIPv2-Message-Format*

- *address family identifier (16)*
  Siehe RIPv1-Frame
- *route tag (16)*
  Kennzeichen zur Differenzierung von internen und externen RIP-Routen
- IPv4 address (32)
  Siehe RIPv1-Frame
- *subnet mask (32)*
  Subnetzmaske der IP-Adresse
- *next hop (32)*
  IP-Adresse des nächsten Hops (innerhalb des lokalen Subnetzes)
- *metric (32)*
  Siehe RIPv1-Frame

4.2.3 Open Shortest Path First (OSPF)

Als ein »Konkurrent« zum *Routing Information Protocol* hat sich *OSPF* (*Open Shortest Path First*) als modernes *Link State Protocol* auf dem Routing-Markt etabliert. Die offiziellen Charakteristika des mittlerweile standardisierten Routing-Protokolls *OSPF Version 2* sind im RFC 2328 vom April 1998 nachzulesen. OSPF wird eigentlich als das Nachfolgeprotokoll des RIP betrachtet. Allerdings ist eine kontinuierliche Entwicklung vom RIP zum OSPF nicht zu erkennen, da beiden Protokollen recht unterschiedliche Philosophien zugrunde liegen. In der Praxis hat OSPF zwischenzeitlich das RIP als Standard für Routing-Protokolle abgelöst. OSPF wartet mit Funktionen auf, die RIP nicht zu bieten hat, als da beispielhaft zu nennen sind:

- Verwendung von Subnetzen und variablen Subnetzmasken
- Authentifizierung
- Einsatz mehrerer Metriken (Hop-Count, Kosten, Zuverlässigkeit)
- Lastverteilung über Routen mit gleicher Kostenbewertung
- Priorisierungsmechanismen über das TOS-Feld des IP
- Bildung von Routing-Tabellen durch Link-Informationen der Router-Nachbarn
- Verwendung *kurzer* Datagramme aus Gründen der Netz-Performance

Netzwerkstruktur

Die übergeordnete Struktur in einem OSPF-Router-Netzwerk ist das *Autonome System* (AS). Es wird normalerweise die gesamte Netzwerkstruktur eines Unternehmens im LAN- und im WAN-Bereich umfassen. Jeder involvierte Router besitzt stets aktuelle Informationen über die Topologie des AS, aus der er seine relevanten Routing-Pfade ermitteln kann. Zur besseren Verwaltung eines solch komplexen Netzwerks bzw. eines AS wird allerdings eine Unterteilung in mehrere *Areas* vorgenommen, die jeweils individuell adressiert werden müssen (siehe Abb. 4–7).

Die Identifikation der *Areas* erfolgt durch eindeutige IDs, wozu in der Regel die jeweilige IP-Adresse der Area verwendet wird. Über eine Datenbank erhält jede Area die Kontrolle über ihre eigenen Topologie-Informationen. Diese werden im Router verwaltet. Router, die zwischen zwei Areas installiert sind, administrieren daher auch zwei verschiedene Topologiedatenbanken, die kontinuierlich abgeglichen werden. Aufgrund dieser Unterteilung spricht man einerseits vom *Intra-Area Routing*, das sich auf Routing-Aktivitäten ausschließlich innerhalb einer Area bezieht, und andererseits vom *Inter-Area Routing*, das sich mit der notwendigen Kommunikation der einzelnen Areas untereinander beschäftigt. Die an den Area-Grenzen befindlichen Inter-Area-Router besitzen einen Zugang zu der sogenannten *Backbone-Area*, die alle einzelnen Areas zu einem AS verbindet. Diese Area wird im OSPF mit der Identifikation 0.0.0.0 versehen.

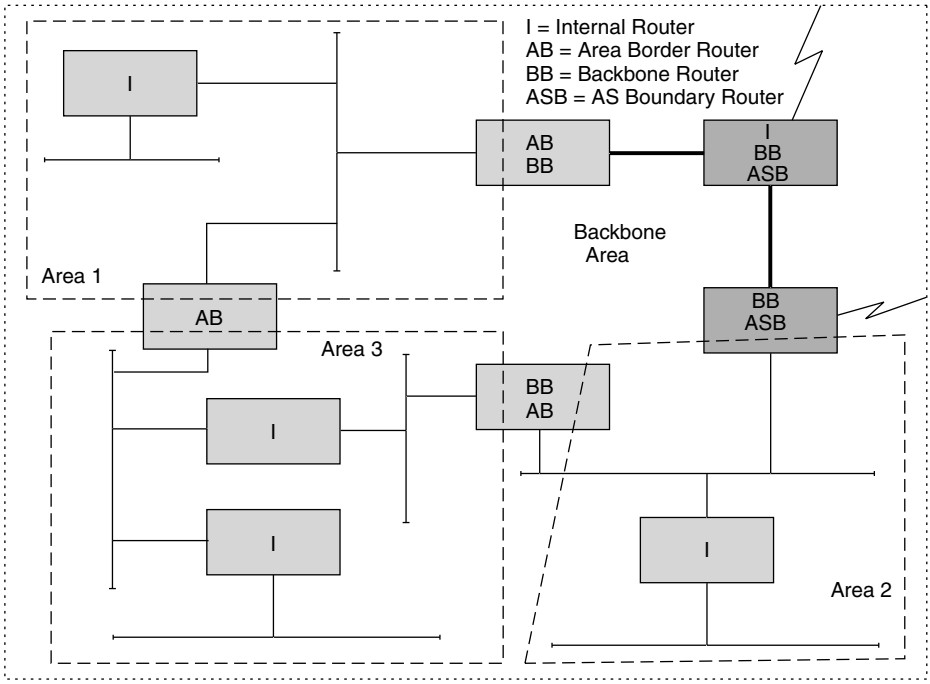

Abb. 4–7 *Struktur der Areas im OSPF*

Als wesentliche Bedingung für die Definition einer Area muss gewährleistet sein, dass jedes Netzwerk innerhalb einer Area erreicht werden kann, ohne diese dabei zu verlassen. Sollte dies aus bestimmten Gründen nicht eingehalten werden können (die Backbone-Area ist beispielsweise in sich nicht geschlossen, sondern zweigeteilt), so müssen »virtuelle Links« definiert werden, die eine zu konfigurierende logische Verbindung bilden, um die Backbone-Area wieder zu schließen. Für die Durchführung von Kommunikation innerhalb und außerhalb eines AS samt seiner Areas werden vier Router-Typen benötigt, die an bestimmten topologischen Schlüsselstellungen im Netzwerk positioniert werden:

- *Internal Router*
  Befinden sich innerhalb einer Area.
- *Area Border Router*
  Befinden sich an den geografischen Grenzen der Areas.
- *Backbone Router*
  Befinden sich mit mindestens einer Schnittstelle in der *Backbone-Area*.
- *AS Boundary Router*
  Befindet sich an der Grenze des AS – zur Verbindung mit weiteren AS.

Der Kommunikationsweg einer Sendestation zu einer Zielstation über Area-Grenzen hinweg lässt sich in folgende Phasen einteilen:

- *Phase 1*
  Sendestation zum Area Border Router 1
- *Phase 2*
  Area Border Router 1 zum Area Border Router 2 (Backbone-Weg)
- *Phase 3*
  Area Border Router 2 zur Zielstation

Netzwerktypen

Folgende Netzwerktypen werden von OSPF unterstützt:

- *Point-to-Point Networks*
  Dabei wird eine Verbindung zwischen zwei Routern über eine direkt angeschlossene Leitung realisiert, wobei es sich nicht ausschließlich um ein physisches Kabel handeln muss, das beide Router verknüpft; die Punkt-zu-Punkt-Verbindung kann auch über ein öffentliches Netzwerk wie beispielsweise über das ISDN (Festverbindungen, Wählverbindungen) hergestellt werden.
- *Broadcast Networks*
  In einem *Broadcast Network* können mehrere Router eingebunden werden. Die Verständigung der einzelnen Netzwerkknoten kann über *Broadcasts* erfolgen, wobei Mitteilungen gleichzeitig an alle (oder an eine Gruppe) Netzwerkteilnehmer verschickt werden.
- *Non-Broadcast Networks*
  Dieser Netzwerktyp ermöglicht mehrere parallele Verbindungen zu verschiedenen Zielen, jedoch ist die Aussendung von *Broadcasts* nicht möglich. X.25-Netzwerke gehören zu diesem Typ, wobei virtuelle Verbindungen als SVC (*Switched Virtual Circuit*) oder PVC (*Permanent Virtual Circuit*) die Grundlage bilden.

> **HINWEIS**
>
> Die beiden zuletzt genannten Typen werden auch als *Multi-Access Networks* bezeichnet, da dabei in der Regel immer mehrere Router zum Einsatz kommen.

Arbeitsweise

Nach Aktivierung eines OSPF-Routers versucht dieser, über *HELLO-Messages* seine Router-Nachbarn zu erreichen. Dies geschieht in *Point-to-Point-Netzwerken* durch feste Adresszuordnungen, in *Multi-Access-Netzwerken* wird dazu die Multicast-Adresse 224.0.0.5 verwendet. Eine solche Adresse der D-Klasse steht für die »normale« Adressierung von IP-Knoten nicht zur Verfügung. Sie dient lediglich dazu, Routing-Informationen an eine Gruppe von Routern zu senden. Dadurch kann die Verwendung von *Broadcasts* verhindert werden, um den Netz-

werkverkehr erheblich zu reduzieren (nicht jeder Knoten erhält – wie bei einem Broadcast – die jeweilige Information, sondern lediglich die Router).

Im *Multi-Access-Netzwerk* wird daraufhin unter den involvierten Routern ein sogenannter *Designated Router* (DR) sowie sein Vertreter, ein *Backup Designated Router*, bestimmt (während dieser Zeit ist das gesamte Netzwerk blockiert). Der DR ist fortan für die gesamte Steuerung des Netzwerks zuständig. Bei einem DR-Ausfall übernimmt der Backup-DR die Rolle des DR. Die Kommunikation zwischen DR und Backup-DR erfolgt über die Multicast-Adresse 224.0.0.6. Sie wird ebenfalls von denjenigen Routern benutzt, die dem DR bzw. dem Backup-DR Informationen zukommen lassen wollen. Eine der Hauptaufgaben des DR ist die Bestimmung von *Adjacencies* (Nachbarschaften). Sie bezeichnen eine Gruppe von Routern, die direkt miteinander kommunizieren. Router in unterschiedlichen *Adjacencies* stehen normalerweise untereinander nicht in Kontakt. Sie kommunizieren lediglich mit den beiden DRs. Würde eine netzwerkweite Kommunikation aller Router untereinander freigegeben, so führte dies zweifelsohne zu einer starken Netzwerkbelastung.

Router versenden in konfigurierbaren Zeitintervallen *Link State Advertisements* (LSA), in denen ihr aktueller Zustand beschrieben wird. Bleibt dieser Zustand konstant, so wird erst nach Ablauf des Zeitintervalls wieder ein LSA geschickt. Ändert sich jedoch sein Zustand, so erfolgt unmittelbar ein zusätzliches *Link-State-Update*. Aus der Vielzahl von LSAs ermittelt ein Router die Netzwerktopologie, für die er zuständig ist. Der *Shortest-Path-Algorithmus* berechnet aus diesen Informationen schließlich den günstigsten Weg.

In Abhängigkeit vom Router-Typ werden unterschiedliche LSA-Typen eingesetzt, um entsprechende Informationen zu versenden:

- *ROUTER LINK ADVERTISEMENT (type 1)*
  In diesem LSA versendet ein normaler Router die Statusinformationen seiner Netzwerkschnittstelle innerhalb seiner eigenen Area.
- *NETWORK LINK ADVERTISEMENT (type 2)*
  Innerhalb einer Area versendet der DR eine Aufstellung aller im Netzwerk installierten Router.
- *SUMMARY LINK ADVERTISEMENT (type 3)*
  Diese LSA enthält Routenbeschreibungen und wird von Area-Border-Routern benutzt, um Ziele außerhalb der Area erreichen zu können.
- *SUMMARY LINK ADVERTISEMENT (type 4)*
  Diese LSA enthält Routenbeschreibungen zu den AS-Boundary-Routern und wird von Area-Border-Routern benutzt, um Ziele außerhalb des Autonomen Systems (AS) erreichen zu können.
- *AS EXTERNAL LINK ADVERTISEMENT (type 5)*
  Alle Router im AS bzw. in der Domäne werden vom AS-Boundary-Router informiert, wie ein Ziel innerhalb eines anderen AS erreicht werden kann.

Die unterschiedlichen Statuswerte, die der Netzwerkcontroller eines Routers annehmen kann, sind nachfolgend kurz beschrieben. Aus ihnen geht der aktuelle Zustand des Routers hervor:

- *Down*
  Initialzustand eines Routers unmittelbar nach seinem Einschalten, jedoch noch vor der Initialisierung des Netzwerkcontrollers
- *Loopback*
  Dieser Zustand verweist auf die Möglichkeit, bereits einfache Netzwerktests durchführen zu können (z.B. *Ping*). Normaler Datenverkehr ist allerdings (noch) nicht möglich.
- *Waiting*
  In diesem Zustand befindet sich ein Router bzw. seine Schnittstelle, wenn er das Netzwerk nach den bereits bekannten *HELLO-Messages* seines DR abhört. Erfolgt innerhalb eines bestimmten Intervalls (*RouterDeadInterval*) kein Empfang einer *HELLO-Message* vom DR, so muss ein neuer DR bestimmt werden.
- *Point-to-Point*
  Der Netzwerkcontroller in einem *Point-to-Point-Netzwerk* oder an einem virtuellen Link befindet sich in einem aktiven Zustand. Es wird versucht, den Aufbau einer *Adjacency* mit dem Nachbar-Router vorzunehmen.
- *DR other*
  Beim Router dieses aktiven Netzwerkcontrollers handelt es sich um keinen DR oder einen Backup-DR. Er baut jedoch *Adjacencies* zu ihnen auf.
- *Backup*
  Beim Router dieses aktiven Netzwerkcontrollers handelt es sich um den Backup-DR.
- *DR*
  Router dieses aktiven Netzwerkcontrollers ist ein *Designated Router*.

Topologiedatenbasis

Ein OSPF-Router erhält über *Link State Advertisements* (LSA) die Topologie-Informationen, die zur Bildung einer entsprechenden Routing- bzw. Topologiedatenbank in einem Router benötigt werden. Der Router selbst betrachtet sich bei Berechnung aller Routen in seiner Area als Root (Wurzel). Von ihm ausgehend werden alle potenziellen Wege über Router und Netzwerke »durchwandert«. Dabei werden Router-Netzwerkübergänge mit Kosten bewertet. Je geringer die Kosten, desto günstiger die Route. Eine solche primäre Route wird nur dann ignoriert, wenn eine Störung auf ihrem Pfad vorliegt. In dem Fall entscheidet sich OSPF für eine nach der Routenberechnung höher bewertete, also kostspieligere Routenalternative.

Abbildung 4–8 zeigt eine Topologie, die als Schaubild die Grundlage für die Bewertung der Routen darstellt. Der System-Manager hat dabei die Aufgabe, nach den ihm vorliegenden Kriterien (z.B. Leitungsqualität, Leitungs- bzw. LAN-Geschwindigkeit) eine kostenorientierte Bewertung einzelner Router-Netzwerkabschnitte vorzunehmen. Dabei wird ein Netzwerkabschnitt stets mit »0« bewertet. Alle übrigen Abschnitte werden mit Kostenwerten versehen. Eine schnelle LAN-Verbindung eines Routers zu einem Gigabit-Ethernet-Netzwerk könnte demnach mit einem geringeren Kostenwert als eine langsame Ethernet-Verbindung mit hoher Kollisionsrate belegt werden.

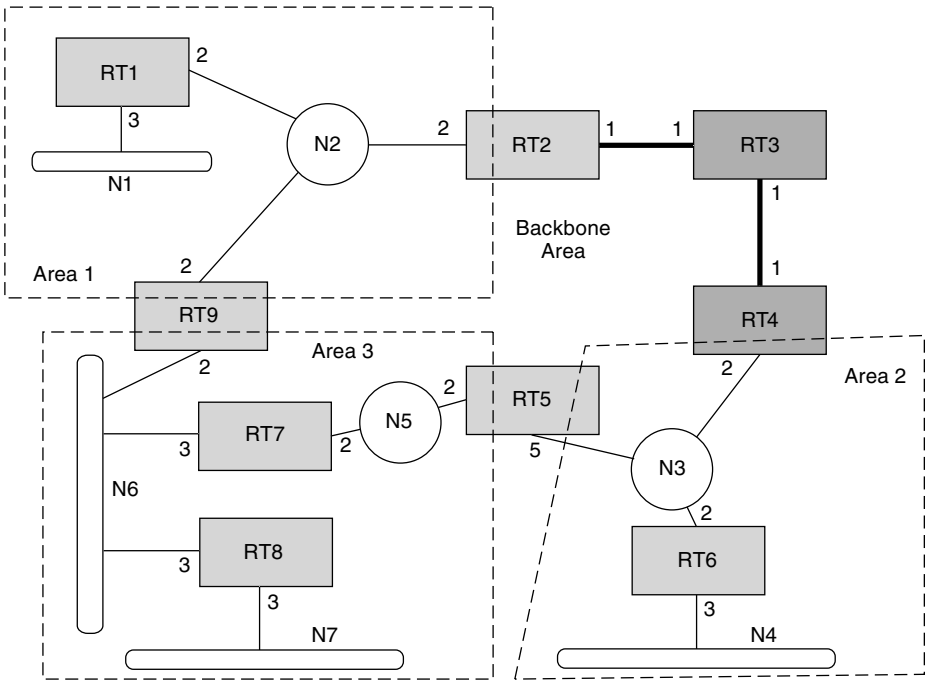

Abb. 4–8 *OSPF-Topologie*

Aus der ermittelten Topologie wird ein *Directed Graph* (gerichteter Graph) erzeugt, aus dem – in diesem Fall für die *Area 2* – die Topologiedatenbasis für den *Area Boundary Router RT4* abgeleitet wird. Aus dem Graphen geht hervor, dass teilweise mehrere Routen zu ein und demselben Ziel existieren, allerdings zu unterschiedlichen Kosten. Routen mit geringeren Kosten werden natürlich bevorzugt. Sind die Kostenwerte jedoch gleich, so werden die Datenpakete zu gleichen Teilen über die gleichwertigen Routen verteilt (*Load Balancing*). Abbildung 4–9 zeigt das Beispiel in anschaulicher Form.

Durch den Lernprozess des Routers *RT4* nach Empfang zahlreicher *Link State Advertisements* lässt sich nicht nur die Topologiedatenbasis seiner *Area 2* bilden, sondern auch eine entsprechende Routing-Tabelle, die auszugsweise wie folgt aussieht:

Zielnetz?	Nächster Hop	Entfernung
N1	RT3	7
N2	RT3	4
N3	–	2
N4	RT6	5
N5	RT5	4
N6	RT3	6
N7	RT3	9

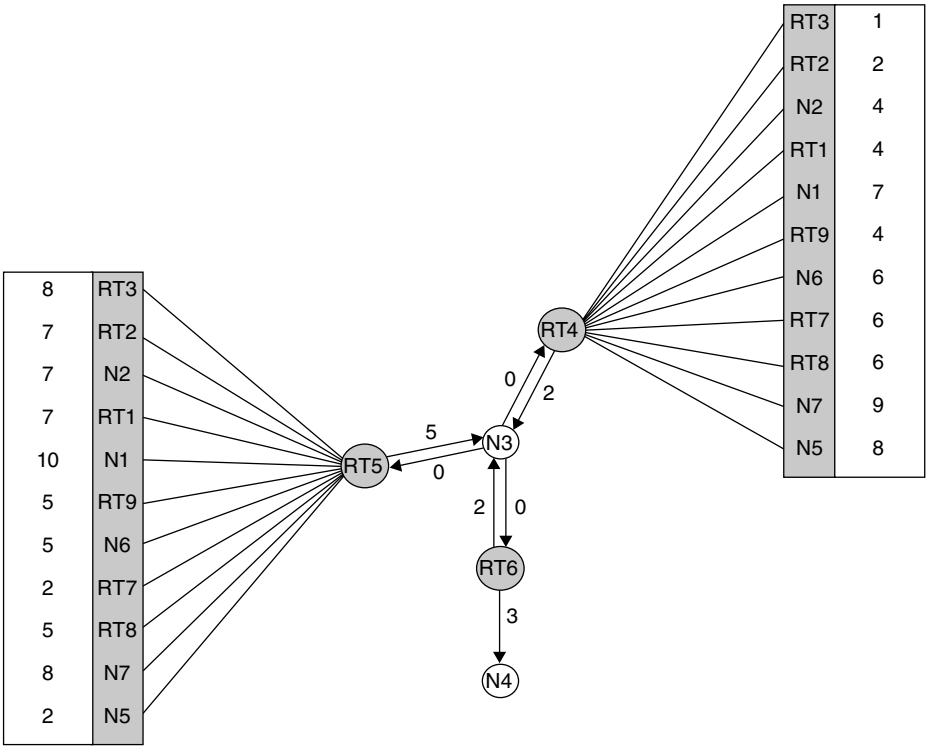

Abb. 4–9 *OSPF-Topologiedatenbasis Router RT4, Area 2*

HINWEIS

Da es sich beim Router RT4 um einen *Area-Border-Router* handelt, verwaltet er mindestens zwei Topologien. In Abhängigkeit vom Feld *Type Of Service* lassen sich separate Routing-Tabellen verwalten. Das aus dem IP-Header verfügbare TOS-Feld ermöglicht ein Routing gemäß den dort hinterlegten Prioritäten.

Parametrisierung

Eine äußerst wichtige, aber auch zeitaufwendige Tätigkeit stellt die Konfiguration eines OSPF-Routers dar. Von den im RFC 2328 zur Verfügung gestellten Parametern sind einige konstant vorgegeben, andere hingegen müssen zunächst einmal in ihrer Bedeutung und Wirkungsweise analysiert werden, bevor man diese modifiziert. In vielen Fällen geben die Router-Hersteller auch Empfehlungen (Default-Werte), die man für die meisten Konfigurationen übernehmen kann.

Die wichtigsten, nachfolgend beschriebenen Parameter sind im Wesentlichen dem RFC 2328 von April 1998 entnommen:

- *LSRefreshTime*
  Maximalzeitintervall, nach dessen Ablauf ein neues *Link State Advertisement* generiert wird, sofern kein anderer Grund vorliegt (z. B. Topologieänderung), ein LSA zu versenden. Dieser Timer besitzt den Wert 30 Minuten. Länger darf ein LSA nicht auf sich warten lassen.
- *MinLSInterval*
  Mindestzeitintervall, nach dessen Ablauf ein neues LSA generiert werden kann. Der Wert dieses Timers lautet auf 5 Sekunden. Kürzere Intervalle sind nicht erlaubt.
- *MinLSArrival*
  Mindestdauer, die zwischen Empfang neuer LSA-Instanzen verstreichen muss. LSAs in kürzeren Intervallen werden ignoriert. Der Default-Wert lautet 1 Sekunde.
- *MaxAge*
  Maximalalter eines LSA. Hat ein LSA den Wert in *MaxAge* (= 60 Minuten) erreicht, so wird es für die Berechnung der Routing-Tabelle nicht mehr herangezogen. *MaxAge* muss immer größer als *LSRefreshTime* sein.
- *CheckAge*
  Sobald das Alter eines in der Datenbank abgelegten LSA ein Vielfaches des Wertes von *CheckAge* erreicht hat, wird eine Überprüfung der LSA-Prüfsumme vorgenommen. Eine fehlerhafte Prüfsumme weist auf einen schweren Fehler hin. Der Wert steht auf 5 Minuten.
- *MaxAgeDiff*
  Maximalzeit, in der ein LSA das AS durchqueren darf. Die meiste Zeit warten LSAs in den Routern bzw. ihren Ausgabepuffern (in dieser Zeit »altern« sie jedoch nicht). Dieser Parameter besitzt den Wert 15 Minuten.
- *LSInfinity*
  Dieser Link-State-Metrikwert gibt an, ob ein Ziel nicht erreichbar ist. Das Metrikfeld wird dann mit binären Einsen gefüllt (16 Bits bei normalen LSAs, 24 Bits bei Summary LSAs und AS External LSAs).

- *DefaultDestination*
  Dieser Parameter enthält die Destination-ID der Default Route. Sie wird verwendet, wenn kein anderer passender Routing-Eintrag gefunden werden kann. Für diese Route werden jedoch nur AS External LSAs und Summary LSAs des Typs 3 benutzt. Der Wert der IP-Adresse lautet 0.0.0.0.
- *InitialSequenceNumber*
  LS-Sequence-Number-Wert, der für die zuerst generierte Instanz jedes LSA verwendet wird; Wert = 0x80000001 (signed 32-bit integer)
- *MaxSequenceNumber*
  Maximalwert, den eine LS Sequence Number annehmen kann; Wert = 0x7fffffff (signed 32-bit integer)
- *Router-ID*
  Eindeutige Router-Kennung. Meist wird hier die niedrigste oder auch höchste IP-Adresse des Routers verwendet. Wird diese geändert, so muss der Router neu gebootet werden, damit die Änderung auch aktiv wird.
- *Area-ID*
  In diesem Parameter wird ein 32-Bit-Wert zur Identifikation der Area abgelegt. Die Area-ID mit dem Wert 0 ist für den Backbone reserviert. Repräsentiert die Area ein Subnetz, so lässt sich die Subnetz-ID verwenden.
- *List of address ranges*
  Eine OSPF-Area ist als Liste von IP-Adress- und -Maskenpaaren definiert. Jedes Paar beschreibt einen IP-Adressbereich. Netzwerke und Hosts werden gemäß ihrer IP-Adresse und dem entsprechenden Bereich einer Area zugeordnet. Router gehören meist mehreren Areas an, je nach zugeordneten Netzwerken.
- *External routing capability*
  Dieser Parameter gibt an, ob *AS External Advertisements* in oder durch die eigene Area transportiert werden dürfen. Ist dies nicht erlaubt, so handelt es sich um eine »Stub Area«. Innerhalb eines solchen Bereichs erfolgt das Routing zu externen Zielen über Default Routes. Die Backbone Area darf niemals Stub Area sein. Virtuelle Links dürfen nicht über Stub Areas definiert werden.
- *StubDefaultCost*
  Bei einer *Stub Area* gibt ein Area-Border-Router dieser Area über einen Parameter die Kosten der Default Route bekannt.
- *IP interface address*
  Hier ist die netzwerkweit eindeutige IP-Adresse der Router-Schnittstelle anzugeben. Serielle Leitungen können als *unnumbered* gekennzeichnet werden und auf die IP-Adresse verzichten.
- *IP interface mask*
  Angabe der Subnetzmaske des angebundenen Netzwerks

- *Interface output cost(s)*
  Es werden die Kosten konfiguriert, die für den Datentransport über diese Router-Schnittstelle berechnet werden sollen. Diese Werte sind Bestandteil der Router-LSAs. Für jeden TOS dürfen verschiedene Kostenwerte angegeben werden.
- *RxmtInterval*
  Gibt die Zeit an, die zwischen zwei LSA-Retransmissions liegen muss. Der Wert sollte deutlich über dem *round trip delay* zwischen zwei beliebigen Routern im Netzwerk liegen. Auf seriellen Leitungen muss dieser Wert entsprechend höher konfiguriert werden. In LANs wird ein Wert von 5 Sekunden empfohlen.
- *InfTransDelay*
  Gibt an, wie lange es dauert (in Sekunden), ein LS-Update-Paket über diese Schnittstelle zu versenden. LSAs, die in dem Update-Paket enthalten sind, müssen den Wert für ihr »Alter« um diesen Wert erhöhen, bevor sie übertragen werden. Dieser Wert sollte die Verzögerungszeiten der Schnittstelle berücksichtigen. Der Wert muss größer als 0 sein. Der Wert 1 wird empfohlen.
- *Router priority*
  Dieser Wert wird für die Bestimmung des *Designated Router* herangezogen. Der Router mit dem höchsten Wert »gewinnt«. Bei gleichem Wert entscheidet die höhere Router-ID. Ein Router mit der Router Priority von 0 kann niemals *Designated Router* werden.
- *HELLOInterval*
  Zeitintervall, in dem *HELLO*-Pakete vom Router über die Schnittstelle versendet werden. Innerhalb eines Netzwerks muss dieser Parameter auf allen Routern identisch sein. Je kleiner das Intervall, desto schneller werden topologische Änderungen ermittelt, umso höher ist jedoch auch die Netzbelastung. Empfohlene Werte für ein X.25-Netzwerk sind 30 Sekunden, für ein LAN 10 Sekunden.
- *RouterDeadInterval*
  Gibt die Zeit (in Sekunden) an, die seit dem letzten *Hello* dieses Routers verstrichen ist, bevor die Nachbar-Router ihn als *down* bzw. inaktiv deklarieren. Das Vierfache des *HELLOInterval* wird empfohlen. Es ist darauf zu achten, dass dieser Wert für alle im Netzwerk involvierten Router identisch ist.
- *Autype*
  Jeder Area kann ein separater Authentifizierungstyp zugeordnet werden. Über diesen Mechanismus müssen sich Router identifizieren, wenn sie am OSPF-Routing teilnehmen wollen. Drei mögliche Werte sind implementierbar: 0 = keine Authentifizierung, 1 = 64-Bit-Kennwort muss angegeben werden, 2 = Paket-Verschlüsselung (Einzelheiten siehe RFC 2328, Anhang D).

- *Authentication key*
  Jeder am OSPF teilnehmende Router weist seine Berechtigung durch dieses Kennwort nach.
- *List of all other attached routers*
  Beschreibt eine Liste aller übrigen im Non-Broadcast-Netzwerk integrierten Router. Sie werden mit ihrer IP-Adresse angegeben. Ferner ist ersichtlich, ob der entsprechende Router *Designated Router* werden kann.
- *PollInterval*
  Wenn ein Nachbar-Router inaktiv wird (*RouteDeadInterval* abgelaufen), ist es ggf. erforderlich, *HELLO*-Messages an ihn zu verschicken. Diese *Hellos* werden jedoch in einem verringerten Poll-Intervall gesendet, das erheblich größer sein soll als das *HELLOInterval*. Für X.25-Netzwerke wird ein Wert von 2 Minuten empfohlen.
- *Host IP address*
  IP-Adresse des direkt erreichbaren Hosts
- *Cost of link to host*
  Kostenwert für den Versand eines Datenpakets vom Router zu diesem Host (auch hier darf für jeden TOS ein entsprechender Wert vergeben werden)
- *Area-ID*
  Angabe der OSPF-Area, zu der dieser Host gehört

Datagramme

Das OSPF-Datagramm setzt unmittelbar auf das Internet Protocol auf, d.h., dem *IP-Header* folgt unmittelbar das OSPF-Datenpaket. Da im OSPF eine Fragmentierung nicht vorgesehen ist, übernimmt entweder IP diese Funktionalität oder aber es werden von vornherein kleine OSPF-Datenpakete generiert, die ein Fragmentieren überflüssig machen. Die Adressierung der OSPF-Pakete erfolgt über die bereits mehrfach erwähnten Multicast-Adressen aus der IP-Adressklasse D (reserviert). Für das Multicasting werden zwei IP-Adressen verwendet. Die Adresse 224.0.0.5 richtet sich an alle Router. Die über diese Adresse verschickten Multicast-Datenpakete müssen von allen Routern bearbeitet werden (z.B. *HELLO-Messages*). Alle *Designated Router* mit ihren Backups werden über die Adresse 224.0.0.6 angesprochen. Der *OSPF-Header* setzt sich aus den in Abbildung 4–10 dargestellten Feldern zusammen.

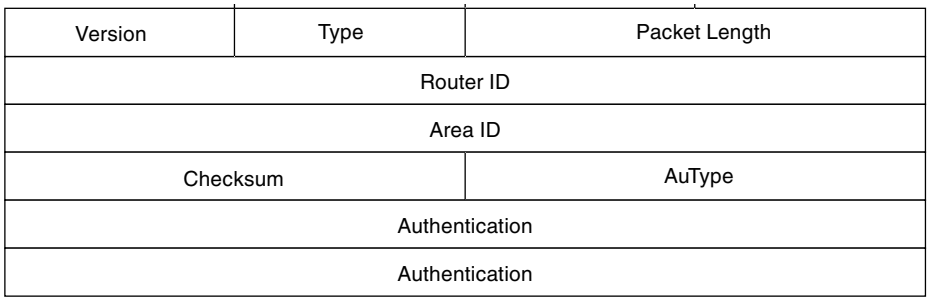

Abb. 4–10 *OSPF-Header*

- *Version* (8)
  Enthält die OSPF-Versionsnummer.
- *Type* (8)
  Hier wird der Typ des OSPF-Datenpakets angegeben, wobei folgende Typen definierbar sind: *HELLO-Paket* (type 1), *Database Description* (type 2), *Link State Request* (type 3), *Link State Update* (type 4), *Link State Acknowledgement* (type 5).
  - *HELLO-Paket (type 1)*
    Das periodisch generierte *HELLO*-Paket sorgt für den Aufbau und die »Pflege der Nachbarschaft« mit anderen Routern. Es werden bestimmte Parameter abgeglichen, die im Netzwerk in allen Routern identisch sein müssen. Unterschiede können dazu führen, dass bei der »Nachbarschaftspflege« Probleme auftreten oder ein Aufbau der Nachbarschaften (*Adjacencies*) erst gar nicht zustande kommt.
  - *DATABASE DESCRIPTION (type 2)*
    Die DD-Pakete werden zum Aufbau einer Topologiedatenbank benötigt. Im Master-Slave-Verhältnis werden im Polling-Verfahren entsprechende *Link State Advertisements* (LSA) ausgetauscht. Alle fünf LSA-Typen besitzen einen Header, der aus den Feldern *LSAge*, *Options*, *LSType*, *LinkStateID*, *Advertising Router*, *LSsequence number*, *LSchecksum* und der Länge des gesamten LSA besteht. Anschließend werden die fünf unterschiedlichen »Bodies« der LSAs angehängt.
  - *LINK STATE REQUEST (type 3)*
    Sollte nach mehrfachem Austausch von Database-Description-Paketen festgestellt werden, dass ein anderer Router aktuellere Informationen besitzt, werden zur Aktualisierung gezielte Link State Requests verschickt. Diese bestehen aus dem *LSType*, der Link State ID und dem Advertising Router.
  - *LINK STATE UPDATE (type 4)*
    Mit einem *Link State Update* werden die *Link State Advertisements* (LSAs) übertragen. Innerhalb eines LSU können mehrere LSAs übertragen werden. Die genaue Anzahl geht aus dem Feld *number of advertisements* hervor.

- *LINK STATE ACKNOWLEDGEMENT (type 5)*
  Zur Sicherung des Datenflusses wird für die *Link State Updates* ein Bestätigungsverfahren eingeführt, das jedes einzelne oder auch mehrere LSAs gemeinsam über Multicasts bestätigt.

- *Packet Length* (16)
  Länge des OSPF-Pakets in Oktetten (Bytes)
- *Router ID* (32)
  Gibt die eindeutige Identifikation (IP-Adresse) des sendenden Routers an.
- *Area ID* (32)
  Gibt die *Area* an (meist Subnetzadresse), zu der das Paket gehört. Alle OSPF-Pakete sind einer bestimmten Area zugeordnet, die zumeist höchstens einen Hop vornehmen. Pakete, die über einen virtuellen Link übertragen werden, erhalten die Backbone-Area-ID 0.
- *Checksum* (16)
  Prüfsumme, die aus dem gesamten Paket mit Ausnahme des Authentifizierungsfelds berechnet wird
- *AuType* (16)
  Hier wird der Authentifizierungstyp abgebildet, der aktuell verwendet werden soll. Zwei Werte sind zurzeit definiert: Ein *AuType* von 0 gibt an, dass keine Authentifizierung erfolgt, ein *AuType* von 1 weist auf die Benutzung eines maximal acht Oktette umfassenden Kennworts hin, ein *AuType* von 2 ermöglicht Verschlüsselung.
- *Authentication* (64)
  Hier wird, entsprechend dem *AuType*, das Kennwort hinterlegt.

OSPF-Weiterentwicklung

Auch wenn OSPF in der Version 2 heute noch überwiegend in Netzwerken anzutreffen ist, so lohnt doch ein Blick auf die Weiterentwicklung des populären Routing-Protokolls der letzten Jahre. Diese sind dem öffentlich verfügbaren RFC-Index zu entnehmen.

Hieraus ist ersichtlich, dass es mittlerweile eine OSPFv3 gibt, die sich grundsätzlich von OSPFv2 dahin gehend unterscheidet, dass sie der IPv6-Technologie Rechnung trägt.

4.2.4 HELLO

Basierend auf einer Implementierung von PDP-11-Software wird *HELLO* innerhalb des *Distributed Computer Network* (DCN) als Routing-Protokoll verwendet. Es ist dem RIP-Protokoll verwandt, benutzt allerdings keine *Hop-Counts* zur Routenoptimierung, sondern arbeitet nach dem Delay-Konzept, das primär die