3. Auflage

Gerhard Lienemann

TCP/IP

Grundlagen und Praxis

Protokolle, Routing, Dienste, Sicherheit

→ Mit Beiträgen von Dirk Larisch

dpunkt.verlag

Inhalt

4 Routing

Freitagnachmittag, zur Feierabendzeit, auf einem Großstadtbahnhof: Zahlreiche Züge fahren in den Bahnhof ein. Einige Güterzüge durchfahren den Bahnhof, einige Personenzüge halten an. Fahrgäste steigen aus, andere wiederum steigen in die Züge ein und fahren damit weiter. Auf mehreren Gleisen können zur gleichen Zeit unterschiedliche Züge abgefertigt werden. Zur Koordinierung dieses täglich wiederkehrenden Chaos werden ausgeklügelte und durchdachte Fahrpläne entwickelt und Wege festgelegt, die von den einzelnen Güter- und Personenzügen genau eingehalten werden müssen. Dabei lassen sich denkbare Alternativen in der Wegewahl durch eine kombinierbare Anfahrt verschiedener Bahnhöfe und die Benutzung mehrerer Weichensysteme erreichen. Diese vorhandene Infrastruktur muss ggf. verändert oder erweitert werden, wenn sich der Bedarf von weiteren Anbindungspunkten ergibt.

Ein solches Szenario lässt sich durchaus als gedankliche Grundlage für die Auseinandersetzung mit dem Thema *Routing im Netzwerk* verwenden, wobei die Züge hier durch Datenpakete (Datagramme) ersetzt werden. Bevor der eigentliche Transportvorgang relevant wird, muss genau über die Wahl des einzuschlagenden Weges nachgedacht werden. Die Wahl des optimalen Weges ist eine der Hauptaufgaben des *Routings*. An allen Verbindungsknoten, wo eine Änderung der Route vorgenommen werden kann, werden im Netzwerk »Bahnhöfe«, die sogenannten *Router* eingesetzt. Dabei kann es sich um Router handeln, die lediglich ein einziges Protokoll zu verarbeiten haben, oder auch um *Multiprotokoll-Router* (mehrere »Gleise«), die in der Lage sind, mehrere Protokolle gleichzeitig zu routen. Der Begriff »Weiche« ist eher mit einer Bridge bzw. Brücke zu vergleichen, da hier zur Wegesteuerung i.d.R. weitaus weniger Intelligenz erforderlich ist als bei einem Router. Filtermechanismen bei Routern sorgen dafür, dass nur die gewünschten Datenpakete passieren dürfen. Unerwünschte Datenpakete (»Schwarzfahrer«) werden herausgefiltert (bzw. »am Bahnhof hinausgesetzt«).

4.1 Grundlagen

4.1.1 Aufgaben und Funktion

Ein Router oder Internet-Router hat folgende Aufgaben zu erfüllen:

- Anpassung an spezielle Internetprotokolle, einschließlich IP, ICMP oder andere
- Verbindung zweier oder mehrerer paketorientierter Netzwerke

Ein Router muss in seiner Funktionsweise den Anforderungen eines jeden Netzwerks Rechnung tragen, wobei folgende Aufgaben entscheidend sind:

- Ein- und Auspacken (*Encapsulation, Decapsulation*) von Daten-Frames der jeweiligen Netzwerke
- Versand und Empfang von IP-Datagrammen bis zu der maximal möglichen Größe. Diese wird durch die MTU (*Maximum Transfer Unit*) repräsentiert
- Umsetzung der IP-Zieladresse in die entsprechende MAC-Adresse des jeweiligen Netzwerktyps
- Reaktion auf Datenflusssteuerung und Fehlerbedingungen, sofern vorhanden

Ein IP-Router empfängt und versendet IP-Datagramme und benutzt dabei wichtige Mechanismen wie beispielsweise *Speichermanagement* oder *Überlastkontrolle*. Er erkennt Fehlermeldungen und reagiert darauf mit der Erzeugung geeigneter ICMP-Meldungen. Wenn der TTL-Timer (*Time To Live*) eines Datenpakets abgelaufen ist, so muss das Paket aus dem Netzwerk entfernt werden, um unendlich zirkulierende Daten-Frames im Netzwerk zu vermeiden.

Eine weitere sehr wichtige Funktionalität stellt die Fähigkeit dar, Datagramme zu fragmentieren. Sehr große Pakete werden in mehrere, der MTU-Größe entsprechende Teilpakete unterteilt und später wieder zusammengesetzt. Gemäß den ihm in der Routing-Datenbasis vorliegenden Informationen bestimmt der Router den nächsten Ziel-Hop für das zu transportierende Datenpaket.

Über bestimmte Formalismen bzw. unter Verwendung des IGP (*Interior Gateway Protocol*) werden Routing-Informationen zwischen den Routern eines Netzwerks ausgetauscht. Für die Kommunikation mit anderen Netzwerken werden Mechanismen innerhalb von EGPs (*External Gateway Protocol*) eingesetzt (z.B. Austausch von Topologie-Informationen). Für ein umfassendes

Netzwerk- und eigenes Systemmanagement stehen leistungsfähige Funktionen zur Verfügung, wie beispielsweise Debugging, Tracing, Logging oder Monitoring.

4.1.2 Anforderungen

Es bestehen besondere Anforderungen an Router-Systeme, die zunehmend für die Verbindung von LANs über zum Teil weit gestreute WAN-Konstruktionen verantwortlich sind (*Global Interconnect Systems*). Router benötigen dynamische Routing-Algorithmen mit minimierter Prozessor- und Kommunikationslast. Von verschiedenen Router-Herstellern werden sogenannte *Queuing-Modelle* angeboten, die eine optimierte Datenflusssteuerung zulassen.

Router unterstehen normalerweise keiner kontinuierlichen Beobachtung. Sie arbeiten als *Unattended Components*, wobei dafür gesorgt sein muss, dass ein Monitoring und Management dieser Geräte über das Netzwerk realisiert werden kann (z.B. TELNET-Sessions als Konsolenbetrieb zu Installations-, Konfigurations- und Managementzwecken).

Router müssen an die unterschiedlichsten Technologien für WAN- bzw. LAN-Zugriffsgeschwindigkeiten angepasst werden können. Der Betrieb einer relativ langsamen 64-kbit-ISDN-Festverbindung muss ebenso ermöglicht werden wie der Anschluss an ein 100-Mbit-Fast-Ethernet-Segment oder Gigabit-Netzwerke. Für den Einsatz in bereits bestehenden Rechnernetzen muss das Zusammenspiel der Router unterschiedlicher Hersteller (mit natürlich unterschiedlichen Betriebssystemen) ohne nennenswerte Probleme realisiert werden können. Nach Festlegung eines gemeinsamen Routing-Protokolls muss die Verständigung heterogener Router-Systeme untereinander einwandfrei arbeiten.

Ein Router hat die Aufgabe, jeden Header eines IP-Pakets genau zu überprüfen. Er tut dies, bevor irgendeine inhaltsabhängige Aktion vorgenommen werden kann. Dadurch ist er in der Lage, fehlerhafte Pakete vor Weiterleitung an andere Netzwerkressourcen zu verwerfen. In diesem Zusammenhang spielt der TTL-Wert (*Time To Live*) eine große Rolle. Er gibt das aktuelle Alter eines Datagramms an und veranlasst den Router, in folgender Weise zu verfahren:

- Der TTL darf vom Router dann nicht überprüft werden, wenn dieser das entsprechende IP-Datagramm nicht weiterleiten muss.
- Ein Router darf kein Datagramm mit einem TTL-Wert von »0« erzeugen oder weiterleiten.

- Die Tatsache, dass ein TTL-Wert von »0« oder »1« vorliegt, darf einen Router nicht dazu veranlassen, das entsprechende Datagramm zu verwerfen. Wenn es an ihn selbst gerichtet ist oder andere relevante Gründe vorliegen, *muss* er den Versuch unternehmen, es zu empfangen.

HINWEIS

Die wesentliche Funktion des TTL-Felds in einem IP-Datagramm stellt die Vermeidung von endlos im Netzwerk kreisenden IP-Paketen bzw. die Beendigung von Internet-Routing-Schleifen dar. Aus der Praxis zeigt sich, dass der TTL-Wert bei einem großen Router-Netzwerk mit ca. 20 Routern mindestens bei 40 liegen sollte; ein üblicher Default-Wert liegt bei 64.

4.1.3 Funktionsweise

Zur Verbindung mehrerer Netzwerke stellt das in Kapitel 2 beschriebene *Bridging* oder *Switching* eine Alternative dar. Hier werden allerdings alle Transportaktivitäten größtenteils innerhalb des ISO/OSI-Layers 2 (Datensicherungsschicht) durchgeführt; Switching bildet in einigen Fällen eine Ausnahme (Layer-3- und Layer-4-Switching). Das Routing spielt sich hingegen immer auf Layer 3 (Netzwerkschicht) ab.

Dem Transport von IP-Datagrammen liegt ein bestimmter Algorithmus zugrunde, wobei für alle Formen der Weiterleitung von Datenpaketen (*Unicast, Multicast* und *Broadcast*) folgende Vorschriften gelten:

Der Router erhält das IP-Datagramm vom Layer 2 (*Data Link Layer*). Dabei erfolgt eine Auswertung des IP-Headers nach folgenden Gesichtspunkten:

- Die vom Link Layer angegebene Paketgröße muss für die Aufnahme des IP-Datagramms ausreichend dimensioniert sein. Es sind mindestens 20 Bytes erforderlich.
- Die IP-Checksumme muss korrekt sein.
- Das IP-Datagramm-Header-Feld muss für die Aufnahme des IP-Headers ausreichend dimensioniert sein. Dieser Wert umfasst die 20 Bytes Fix-Header und zusätzlich mögliche Optionsfelder.
- Das IP-Datagramm-Total-Length-Feld muss die Größe des *IP-Headers* samt IP-Daten umfassen.

Der Router vollzieht eine erste Paketbehandlung nach den im IP-Header angegebenen Optionen. Die Paketbehandlung für weitere Optionen wird zu

einem späteren Zeitpunkt fortgesetzt, wobei der Router eine Auswertung der Ziel-IP-Adresse nach folgenden Kriterien vornimmt:

- Das IP-Datagramm ist für den Router selbst bestimmt und muss zu *Reassembly*-Zwecken zwischengespeichert werden.
- Das IP-Datagramm ist nicht für den Router bestimmt und muss zwecks Weiterleitung zwischengespeichert werden.
- Das IP-Datagramm muss zwischengespeichert werden, da es einerseits weitergeleitet werden muss und andererseits (eine Kopie) an den Router selbst gerichtet ist.

Unicast

Wenn ein Datenpaket durch einen Router an eine Unicast-Adresse weitergereicht werden soll, muss er den nächsten *IP-Address-Hop* bestimmen. Dabei überprüft der Router die Zieladresse im Datenpaket und versucht zunächst unter Verwendung geeigneter Algorithmen zu ermitteln, ob er das Datenpaket direkt über seine Schnittstelle (*Interface*) im benachbarten (*adjacent*) Netzwerksegment zustellen kann oder ob ein weiterer Router mit dem Transport beauftragt werden muss. Die Wahl der zu verwendenden Netzwerkschnittstelle wird hier ebenfalls vorgenommen.

In einem nächsten Schritt wird überprüft, ob das Datagramm überhaupt weitergeleitet werden darf. Hierzu ist eine Analyse der Quell- und Zieladresse erforderlich. Handelt es sich bei der Zieladresse beispielsweise um eine Broadcast- oder Multicast-Adresse, so darf das Datenpaket nicht transportiert werden. Ähnliches gilt für Pakete mit Adressen, die über Paketfilter oder Access-Listen explizit nicht übertragen werden dürfen. Der Router vermindert nunmehr den TTL-Wert um mindestens 1 und überprüft, ob dieser den Wert 0 angenommen hat. Ist dies der Fall, so muss das IP-Datagramm verworfen werden.

Ein Teil der Paketbehandlung gemäß den im IP-Header angegebenen Optionen wurde bereits vor Festlegung der zuvor erläuterten Routing-Verfahren vorgenommen. An dieser Stelle werden nun die restlichen Optionen »verarbeitet«. Dann erfolgt die *IP-Fragmentierung*. Anschließend führt der Router die Bestimmung der MAC-Adresse des nächsten IP-Hops durch, packt das IP-Datagramm in einen geeigneten LLC-Frame ein (z.B. gemäß IEEE 802.3) und stellt es in die Output-Queue (Zwischenspeicher für den Ausgang) der gewählten Netzwerkschnittstelle.

Multicast

Handelt es sich bei der IP-Zieladresse um eine Multicast-Adresse, so wird anhand der IP-Quell- und -Zieladressen, die dem Datagramm-Header entnommen sind, ermittelt, ob das Datagramm über die für die Weiterleitung vorgesehene Schnittstelle empfangen worden ist. Wenn nicht, wird das Datagramm stillschweigend verworfen. Die Methode zur Ermittlung der korrekten Schnittstelle für den Empfang hängt von den aktiven Multicast-Routing-Algorithmen ab. Eines der einfachsten Verfahren ist das RPF (*Reverse Path Forwarding*), bei dem die geeignete Empfangsschnittstelle dadurch ermittelt wird, dass man per Unicast für eine fiktive Übertragung vom Multicast-Empfänger zum eindeutigen Multicast-Versender die geeignete Schnittstelle zum Versenden festlegt.

Auf Basis der IP-Quell- und -Zieladressen aus dem Datagramm-Header ermittelt der Router die ausgehenden Schnittstellen des Datagramms. Um einen IP-Multicast für eine ausgedehnte Ringsuche zu implementieren, wird für jede ausgehende Schnittstelle ein *Minimum-TTL-Wert* festgelegt. Auf jeder Schnittstelle (*Interface*), deren TTL-Wert kleiner oder gleich dem TTL-Wert des Datagramm-Headers ist, wird eine Kopie des Multicast-Datagramms versendet. Alle weiteren Schritte werden auf jeder Schnittstelle parallel ausgeführt; der Router reduziert den Paket-TTL-Wert um 1. Wie bei dem Unicast-Datagramm erfolgt anschließend die Fortsetzung der Verarbeitung aller restlichen Optionen, die Durchführung der IP-Fragmentierung, die Ermittlung der MAC-Adressen für den nächsten IP-Hop, die entsprechende IP-Encapsulation in den LLC-Frame und die Überstellung in den Zwischenspeicher des jeweiligen *Output-Interface*.

Broadcasts

Es gibt zwei Haupttypen von IP-Broadcast-Adressen: *Limited Broadcasts* und *Directed Broadcasts. Directed Broadcasts* werden in drei weitere Subtypen unterschieden: Broadcasts, die an ein spezifiziertes Netzwerkpräfix (Netz-ID) gerichtet sind, des Weiteren an ein Subnetz gerichtete Broadcasts sowie Broadcasts, die an alle Subnetze eines Netzwerks gerichtet sind. Die Klassifizierung eines Broadcasts hängt stets von seiner Adresse und der Kenntnis des Routers von der Struktur des Zielsubnetzes ab. Von anderen Routern wird derselbe Broadcast möglicherweise anders interpretiert.

Die Wahl einer bestimmten Route, die ein Datenpaket auf seinem Weg durch das Netzwerk verwendet, ist von verschiedenen Kriterien abhängig. Die Bewertung dieser Kriterien und das Bestreben, eine Routenwahl zu optimieren, führen zu einem Routing-Verfahren, das sich durch seine Dynamik (im Routing-Algorithmus) vor allem bei Störungen im Netzwerk auszeichnet. Fest definierte

Wege hingegen lassen nur ein geringes Maß an Flexibilität zu, können jedoch eine relativ gute Überschaubarkeit des Datenflusses gewährleisten.

Ein wichtiges Instrumentarium zur Bestimmung optimaler Routen ist die *Routing-Tabelle*, in der die zu verwaltende Netzwerktopologie abgebildet wird. Zwischen den im Netzwerk eingesetzten Routern werden diese Routing-Tabellen in bestimmten Zeitintervallen als wichtige Informationsquelle einander zugesandt und entsprechend ausgewertet.

4.1.4 Router-Architektur

Wie bereits erwähnt, findet das Routing auf dem Netzwerk-Layer statt. Das dabei verwendete Netzwerkprotokoll ist das *Internet Protocol* (IP), und zur Adressierung von IP-Knoten wird das in Kapitel 3 dargestellte Adressierungsschema eingesetzt.

Network Layer

Gegenüber dem *Data Link Layer* (Schicht 2) verhalten sich Router auf Schicht 3 (*Network Layer*) transparent, d.h., die Zugriffsverfahren auf das physische Medium, wie Ethernet oder Token Ring, spielen im IP-Routing keine Rolle. Für beide Verfahren können daher das Internet Protocol und alle seine übergeordneten höheren Protokolle eingesetzt werden. So bereitet beispielsweise die Dateiübertragung mit dem IP-basierten Anwendungsprotokoll FTP keinerlei Probleme, wenn eine Empfangsstation am Ethernet-Netzwerk angeschlossen ist und die Sendestation in einem Token-Ring-Netzwerk betrieben wird.

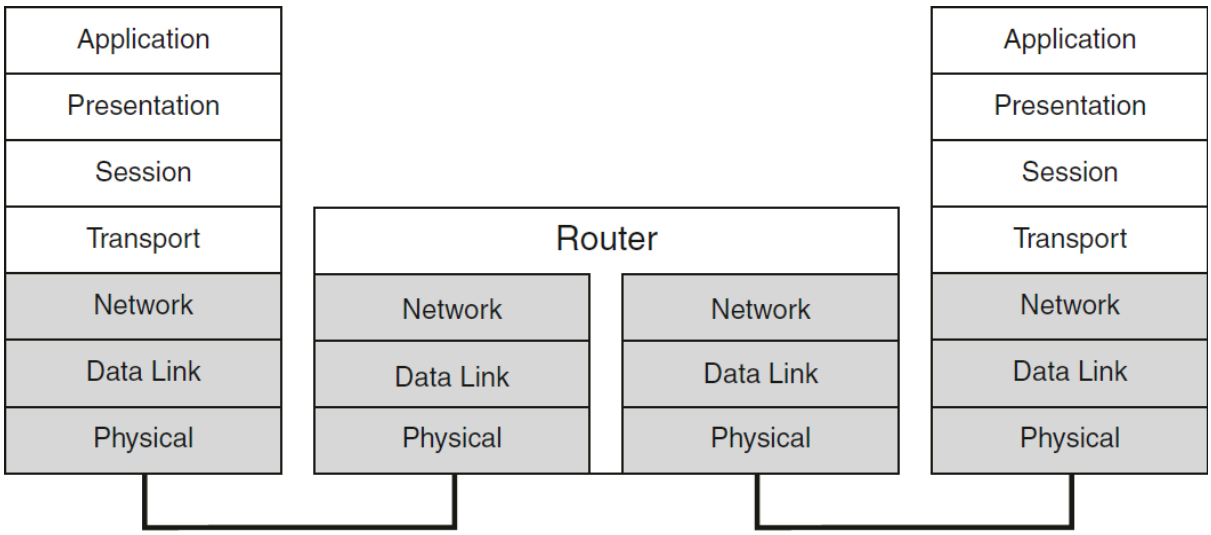

Abb. 4–1 *Router-Einordnung im OSI-Modell auf Schicht 3*

Direct Routing

Befindet sich die adressierte Zielstation im selben IP-Netzwerk, d.h., die Netz-ID der beiden Hosts ist identisch, werden die Dienste eines Routers nicht beansprucht, da eine direkte Adressierung vorgenommen werden kann, das sogenannte *Direct Routing*. Befinden sich zusätzlich Brücken in diesem Netzwerk, so haben diese auf das *Direct Routing* keinerlei Einfluss, da diese auf Layer 2 bekanntlich ein einziges logisches Netzwerk bilden.

Indirect Routing

Zur Adressierung eines Ziel-Hosts außerhalb des eigenen IP-Netzwerks (andere Netz-ID) wird mindestens ein Router-Übergang benötigt. Die Kommunikation wird also über einen Verbindungsknoten geführt, sie erfolgt nicht mehr direkt, sondern indirekt. Hier spricht man vom *Indirect Routing*. Die dazu erforderlichen Mechanismen (Routing-Verfahren, Routing-Tabellen, Routen usw.) werden in den folgenden Abschnitten näher beschrieben.

Default Routing

Das Prinzip des *Default Routing* wird immer dann verwendet, wenn es über die vorhandenen Einträge einer Routing-Tabelle nicht möglich ist, eine Zielstation zu erreichen oder aber noch keine Routing-Einträge (z.B. unmittelbar nach Installation eines Systems) existieren. Das Default Routing kann sowohl direktes als auch indirektes Routing verwenden. Der Default-Routing-Eintrag besteht normalerweise aus der fiktiven IP-Adresse 0.0.0.0 und der Adresse des zu benutzenden Routers.

4.1.5 Routing-Verfahren

Egal, welches Verfahren angewendet wird, die Grundlagen des Routings sind immer die sogenannten *Routing-Tabellen*. Sie enthalten die für eine Erreichbarkeit verschiedener Netzwerke (unterschiedliche Netz-IDs) relevanten Informationen, wobei zwischen zwei Routing-Verfahren unterschieden wird: Das *statische Routing* arbeitet mit festgelegten Routing-Pfaden, die nicht verlassen werden dürfen. Das *dynamische Routing* hingegen basiert auf einer Kommunikation der Router untereinander und verfügt somit über das gesamte Topologiewissen des Netzwerks, wobei sich, je nach Anforderung, die Routing-Pfade ändern können.

Statisches Routing

Beim statischen Routing (siehe Abb. 4–2) werden die notwendigen Routing-Tabellen vom Verwalter des Netzwerks manuell angelegt und die entsprechenden Informationen in einer permanenten Datenbank hinterlegt. Erweiterungen oder Modifikationen müssen manuell in die Tabellen der jeweiligen Router eingetragen werden.

In dem Zusammenhang können Host-Routen oder *Netz-Routen* definiert werden. Ein *Host-Routing-Eintrag* beschreibt die Route zu einem ganz bestimmten Host in einem fremden Netzwerk. Ein anderer Host in diesem Netzwerk kann allerdings dann nicht erreicht werden. Es handelt sich quasi um eine Punkt-zu-Punkt-Verbindung innerhalb eines IP-Netzwerkverbunds. Der Befehl zur Definition lautet beispielhaft:

```
route add host 190.137.23.76 190.136.10.1
```

Damit wird festgelegt, dass der Host 190.137.23.76 im Netzwerk 190.137.0.0 über den Router 190.136.10.1 aus dem Netzwerk 190.136.0.0 erreicht werden kann (als Subnetzmaske wird dabei 255.255.0.0 für Klasse-B-Netzwerke vorausgesetzt).

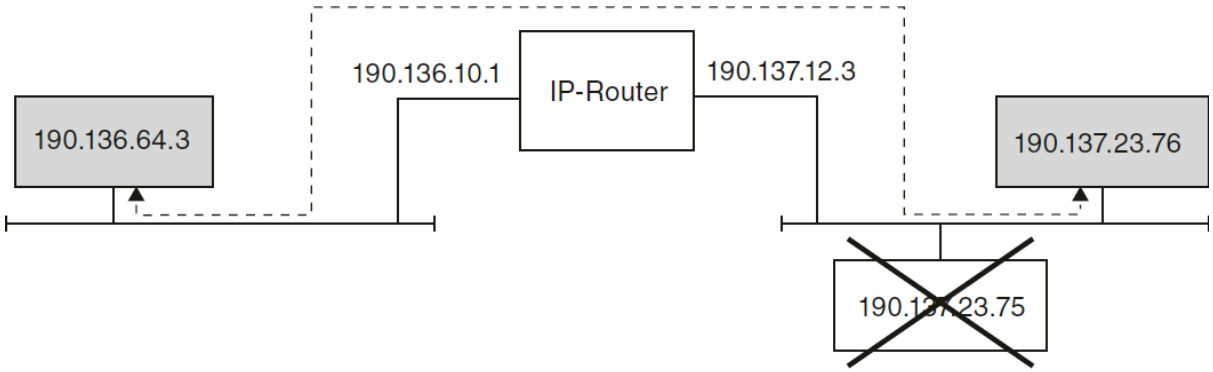

Abb. 4–2 *Beispiel für statisches Routing*

Die Alternative zu festen Einträgen für bestimmte Geräte (Hosts) lautet: *Netz-Routing-Einträge*. Dabei werden diejenigen Router angegeben, die den Übergang in das fremde IP-Netzwerk topologisch ermöglichen. Es wird also nicht nur die Route zu einem bestimmten Host charakterisiert, sondern damit kann ein ganzes Netzwerk adressiert werden (Netzwerk mit einer anderen Netz-ID). Der Befehl zur Definition lautet beispielhaft:

```
route add net 190.137.0.0 190.136.10.1
```

Hier eröffnet der Router mit der IP-Adresse 190.136.10.1 dem Host des lokalen Netzwerks einen Zugang zu allen Hosts innerhalb des Netzwerks 190.137.0.0.

HINWEIS

Das statische Routing wird immer seltener eingesetzt, da die mittlerweile deutlich gewachsenen IP-Netzwerke es nicht mehr zulassen, manuelle Wartungsarbeiten an den Routing-Tabellen durchzuführen. Zudem ist der personelle Aufwand sehr hoch, sodass prinzipiell die Beschränkung auf sehr kleine Netzwerke bzw. für die Realisierung einer eingeschränkten Kommunikation aus Sicherheitsgründen praktikabel ist.

Dynamisches Routing

Das dynamische Routing (auch *Adaptive Routing* genannt) geht von einer umfangreichen Verständigung aller im Netzwerkverbund installierten Router untereinander aus. Um diese Router-Router-Kommunikation zu ermöglichen, werden spezielle Router-Protokolle eingesetzt. Die Dynamik dieses Routing-Verfahrens liegt in seiner Anpassungsfähigkeit gegenüber unvorhersehbaren Ereignissen im Netzwerk. Solche Ereignisse können Router-Ausfälle bzw. -Störungen sein, die bei statischen Routen dazu führen, dass Verbindungen abbrechen und bis zur Beseitigung der Störung nicht wieder etabliert werden können. Das dynamische Routing sorgt durch die eingesetzten Router-Protokolle, die im Grunde die »Intelligenz« der Router darstellen, und die Router-Router-Kommunikation dafür, dass Alternativwege ermittelt werden können und somit eine »Umleitung« um einen defekten Router herum gebildet werden kann. Von einem derartigen Ausfall merkt der Anwender in der Regel überhaupt nichts.

Darüber hinaus lassen sich im Netzwerk neue Hosts hinzunehmen, ohne dass manuelle Eingriffe im Router erforderlich werden. Die Protokollintelligenz erkennt neue Maschinen und fügt sie ihrer dynamisch erzeugten Routing-Tabelle hinzu. Einige Routing-Protokolle bieten zudem Zusatzfunktionen wie Lastverteilung und ermöglichen somit eine dynamische Datenflusssteuerung je nach Datenverkehrsaufkommen.

4.1.6 Routing-Algorithmus

Folgende Objekte bzw. Mechanismen sind zur Beschreibung des Routing-Algorithmus erforderlich:

- *IP-Routing-Table*

  Informationen zur Erreichbarkeit von IP-Hosts

- *Direct Routing (DR)*

Adressierung von Hosts im lokalen Netzwerk

- *Indirect Routing (IR)*

  Adressierung von Hosts außerhalb des lokalen Netzwerks

- *Default Routing*

  Adressierung von Hosts, die über DR und IR nicht erreicht werden können

Zur Veranschaulichung des Routings wird mit der folgenden Anweisung der Aufbau einer TELNET-Verbindung zu einem Zielrechner initiiert:

```
telnet 190.137.23.76
```

Die Zieladresse wird durch den Routing-Algorithmus erfasst und über die Routing-Tabelle geprüft (siehe Abb. 4–3). Dabei erfolgt zunächst die Anfrage, ob die Zieladresse im selben Netzwerk zu finden ist (DR). Ist dies nicht der Fall, so wird der Zielknoten im Routing-Eintrag für fremde Netzwerke gesucht. Lässt er sich dort ebenfalls nicht finden, so bleibt nur noch die Möglichkeit, den Default-Routing-Eintrag zu überprüfen. Enthält dieser eine Routenbeschreibung, die eine Kontaktaufnahme zum Zielrechner ermöglicht, so kann die TELNET-Session etabliert werden. Andernfalls erfolgt die Information des Anwenders durch Ausgabe der Fehlermeldung:

```
network unreachable – no route to host
```

Ziel-Netzwerkadresse	Routenwahl über
190.136.0.0	lokal
190.137.0.0	190.136.10.1
190.138.0.0	190.136.20.1
0.0.0.0 (default)	190.136.1.1

Abb. 4–3 *Muster einer IP-Routing-Tabelle*

Durch Routing-Protokolle werden Router befähigt, ihre Routing-Tabellen mit anderen Routern auszutauschen bzw. Tabellenaktualisierungen (*Table Updates*) durchzuführen, wobei das Zeitintervall für die Updates konfigurierbar ist. Die auf

diesem Wege ermittelten Informationen werden für die Ermittlung der günstigsten Route verwendet. Diese ändert sich ggf. so oft, wie ein Tabellen-Update erfolgt und eine Topologieänderung andere Routen ermöglicht. In dem Zusammenhang ist für die Bewertung einer optimierten Route die Anzahl von *Hops* (Netzübergänge durch Router) wichtig. In einigen Routing-Protokollen (z.B. *Open Shortest Path First* = OSPF) ist neben der Hop-Zahl auch noch eine Bewertung von Verbindungen durch fiktive Kostenwerte möglich. Damit wird die Routenwahl verfeinert und ist nicht nur von zwischengelagerten Routern abhängig. Bei LAN-LAN-, aber vor allem bei LAN-WAN-Verbindungen kann somit zwischen langsamen und schnellen Verbindungen differenziert werden.

Ein Router ist bestrebt, aus der Kenntnis seiner Routing-Informationen heraus die günstigste Route zu wählen (z.B. geringste Anzahl von Hops). Ferner sind Routing-Algorithmen stets bemüht, positive Informationen, also optimierte Routen, schnell im Netzwerk über die Router-Router-Kommunikation (Routing-Tabellen-Updates) zu verbreiten. Negativinformationen – dazu gehören auch Routen, die durch Router-Störungen ausgefallen sind – werden jedoch nur schleppend im Netzwerk verbreitet. Dieser Umstand kann dazu führen, dass bei einem durch zahlreiche Router strukturierten Netzwerk die im Störfall notwendige Ermittlung der Alternativroute extrem lange dauert; eine Session-Unterbrechung bzw. lange Netzlaufzeiten sind die Folge.

Zur Gewährleistung der Kenntnis der aktuellen Netzwerktopologie mit allen möglichen Routen sind permanente Routing-Tabellen-Updates erforderlich, die jedoch aufgrund der damit verbundenen Netzlast nur in bestimmten Zeitintervallen vorgenommen werden können. Wenn also nach dem Ausfall eines Routers dieser keine Updates mehr versenden kann, sind die anderen Router stets auf die Hop-Informationen aus den alten Routing-Tabellen angewiesen. Diese sind allerdings nicht mehr aktuell, denn der defekte Router schickt schließlich keine Updates mehr. Die nun mit jedem Update immer älter werdenden Hop-Informationen führen zu einer kontinuierlichen Erhöhung des *Hop Counts*. Um eine mögliche Endlosschleife bei der Übermittlung über einen defekten Router zu vermeiden, wurde eine Hop-Anzahl von 15 als »nicht erreichbar« deklariert. Die maximale Anzahl von Routern zwischen zwei kommunizierenden IP-Hosts wurde daher auf 14 limitiert, wobei diese Problematik auch als *Slow Convergence Problem* bezeichnet wird.

Die Hop-Informationen als Entfernungsangabe zu den erreichbaren Netzwerken sehen im Normalfall für das in Abbildung 4–4 dargestellte Netzwerk so aus wie in Abbildung 4–5 dargestellt. Daraus geht beispielsweise hervor, dass eine Verbindung von dem Host 190.136.64.3 (*Router Münster* mit Netz-ID 190.136.0.0) zum Host 190.140.17.42 (*Router Ulm* mit Netz-ID 190.140.0.0) über insgesamt zwei Hops (Router) möglich ist.

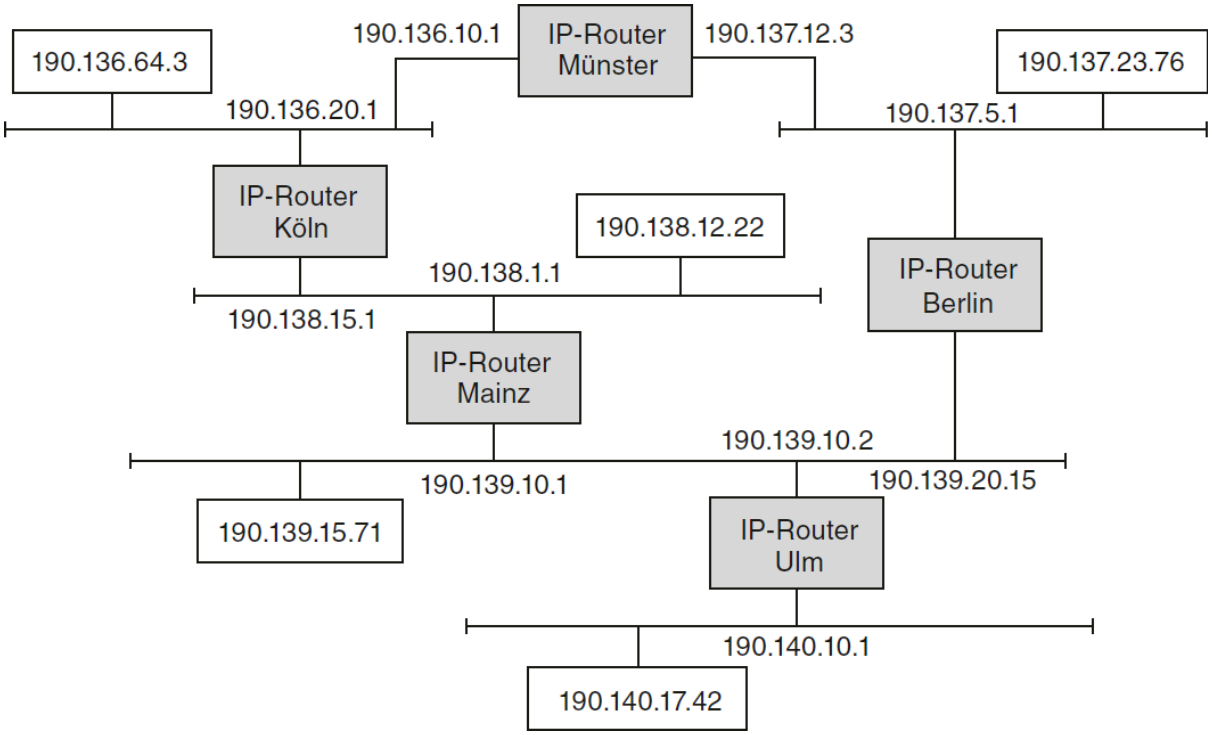

Abb. 4–4 *Beispiel für ein Netzwerk mit mehreren Routern (Hop-Count)*

Router Münster		Router Köln		Router Mainz		Router Berlin		Router Ulm	
190.136	0	190.136	0	190.136	1	190.136	1	190.136	2
190.137	0	190.137	1	190.137	1	190.137	0	190.137	1
190.138	1	190.138	0	190.138	0	190.138	1	190.138	1
190.139	2	190.139	1	190.139	0	190.139	0	190.139	0
190.140	2	190.140	2	190.140	1	190.140	1	190.140	0

Abb. 4–5 *Tabelle mit Informationen zu den einzelnen Routern (Hops)*

4.1.7 Einsatzkriterien für Router

Nicht selten werden Diskussionen über den Einsatzzweck und Sinn von Routern gegenüber der (manchmal) preiswerteren Alternative einer Implementierung von Brücken bzw. Switches geführt. Beides sind Strukturelemente, die zur Gestaltung der Infrastruktur eines Netzwerks eine wichtige Rolle spielen können, die jedoch von ihren Funktionen her nicht vergleichbar sind. Beide leisten einen entscheidenden Beitrag, wenn es um die Steuerung des Datenflusses geht, wobei einige Argumente für den Einsatz von Routern sprechen.

Fragmentierung

Werden zwei gleichartige Netzwerke über Brücken/Switches miteinander verbunden, so sind in der Regel keine Probleme hinsichtlich der Größe der übertragenen Daten-Frames zu erwarten. Handelt es sich bei dem ersten Segment jedoch um ein Ethernet-Netzwerk und bei dem zweiten Segment um ein Token-Ring-Netzwerk, so können sehr schnell Schwierigkeiten auftreten, wenn eine Station im Token Ring einen Frame aussendet, der eine erlaubte Größe von beispielsweise 4 KByte besitzt. Die MTU im Ethernet ist auf maximal 1500 Bytes beschränkt, sodass die verbindende Brücke den Token-Ring-Frame ablehnen muss bzw. ignoriert. Mit Routern ist diese Problematik zu vermeiden, denn sie beherrschen das Fragmentieren von Datenpaketen. Das Internet Protocol bzw. das übergeordnete TCP ermöglicht dem Router als Gerät der Kommunikationsschicht 3, ein Datenpaket zu stückeln und am Zielrouter wieder zusammenzusetzen. Die Gefahr einer Verwerfung von Datenpaketen, die wegen ihrer Größe nicht akzeptiert werden können, besteht beim Einsatz von Routern also nicht.

Error Handling

Durch die Verfügbarkeit eines leistungsfähigen Protokolls wie ICMP (*Internet Control Message Protocol*) lassen sich Fehlersituationen oder Störungen wesentlich besser im Router-Router- oder Router-Host-Datenverkehr übermitteln, und es kann schneller auf derartige Situationen reagiert werden.

Filtering

In den meisten Routern sind bereits umfangreiche Paketfilter implementiert, die den grundsätzlichen Sicherheitsanforderungen für eine einfache Abschottung nach außen genügen. Sie bieten damit auch die Grundlage für die Entwicklung hoch entwickelter Firewall-Systeme, die für eine Anbindung an das öffentliche Internet eine unverzichtbare Voraussetzung sind.

Die verfügbare Filterintelligenz lässt sich auch zur gezielten Protokollsteuerung einsetzen. Sollen nur ausgewählte Protokolle über einen Router geführt werden, um somit die Netzbelastung zu reduzieren, so kann dies durch eine geschickte Filterprogrammierung durchaus realisiert werden. Allerdings stellen umfangreiche und komplexe Filterdefinitionen hohe Anforderungen an die CPU-Leistung und sollten stets mit Bedacht formuliert werden. Für Netzwerkumgebungen mit geringeren Anforderungen gibt es mittlerweile auch Low-Cost-Router, die recht preiswert sind, aber natürlich auch deutlich verminderte Performance-Werte liefern.

HINWEIS

Die Multifunktionalität von Routern und ihre Leistungsfähigkeit sind nur zu erreichen, wenn sie mit qualitativ hochwertiger Software, einem entsprechend großzügig dimensionierten Arbeitsspeicher und einer Hochgeschwindigkeits-CPU ausgestattet werden. Entsprechend hohe Investitionen sind fällig, wenn ein Router-Netzwerk aufgebaut werden soll.

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.

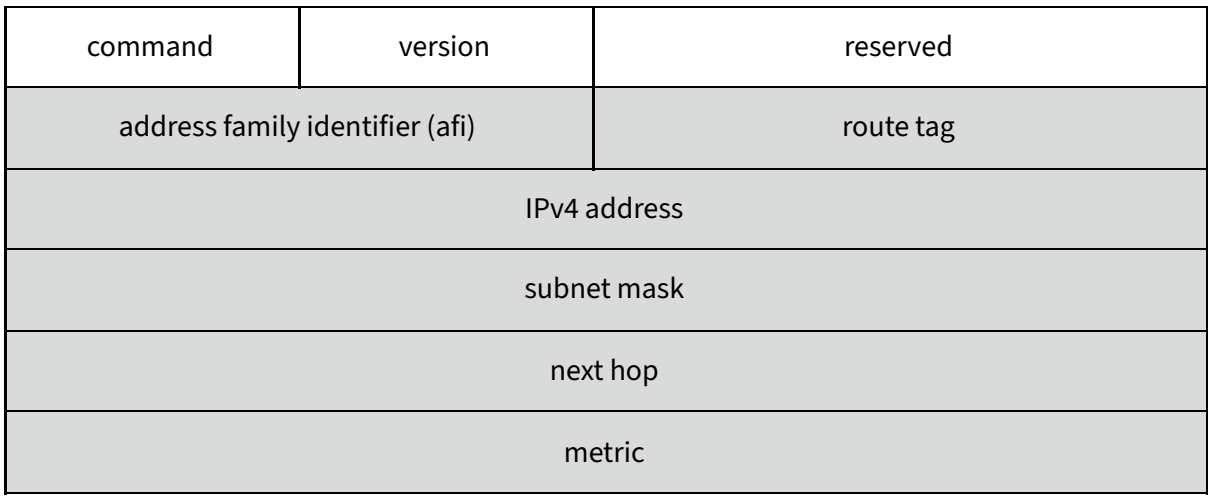

Abb. 4–6 *RIPv2-Message-Format*

- *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.

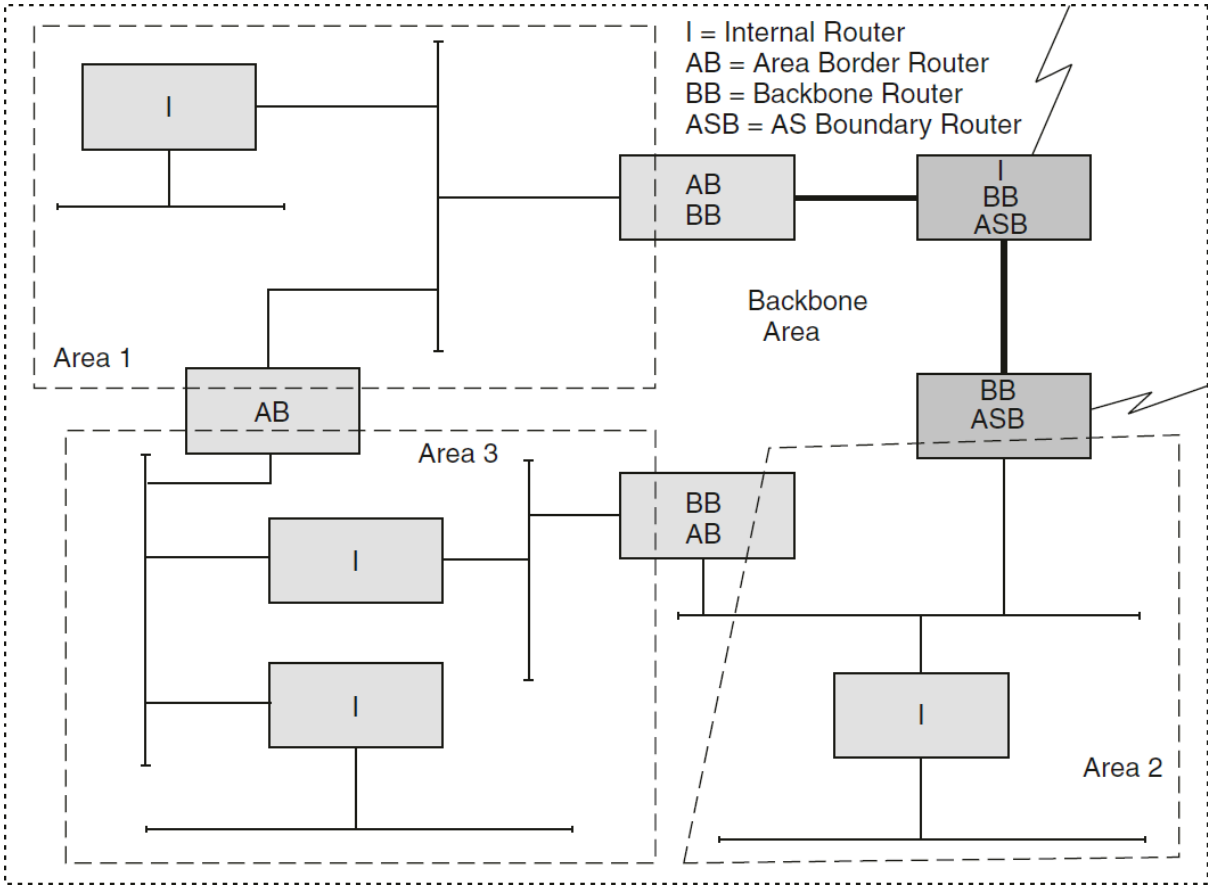

Abb. 4–7 *Struktur der Areas im OSPF*

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 Netzwerkverkehr 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.

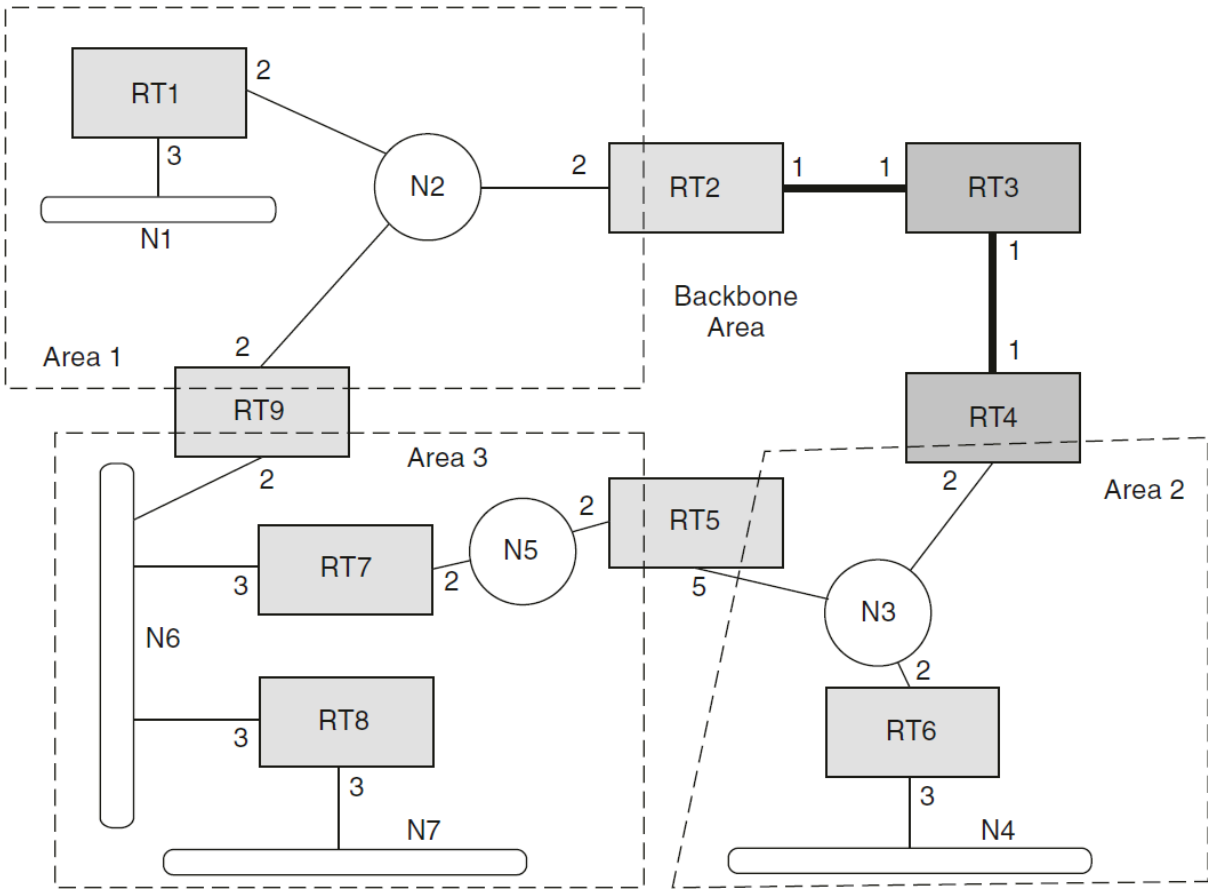

Abb. 4–8 *OSPF-Topologie*

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

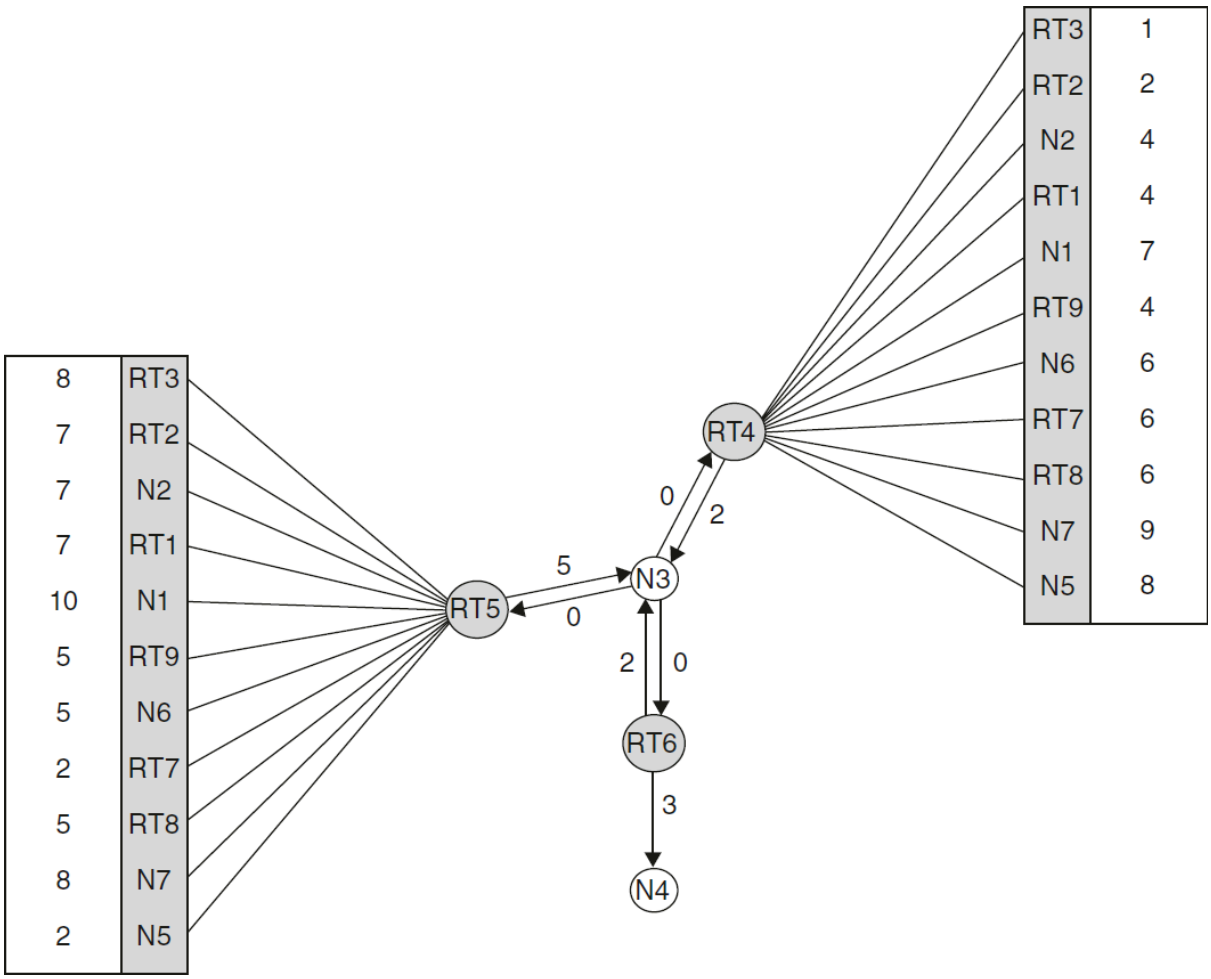

Abb. 4–9 *OSPF-Topologiedatenbasis Router RT4, Area 2*

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.

Version	Type	Packet Length

Router ID	
Area ID	
Checksum	AuType
Authentication	
Authentication	

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 Verzögerungszeiten in einem Netzwerk zugrunde legt und daher als wesentlich realistischer im Vergleich zu RIP eingestuft werden kann. Es entspricht auch eher dem Empfinden der Netzwerkanwender, Antwortzeiten zu berücksichtigen, als einfache *Hop-Counts*, die unterschiedlichen LAN- bzw. Leitungsgeschwindigkeiten keinerlei Beachtung schenken.

Für eine zeitgesteuerte Routing-Konzeption ist allerdings ein exakter Synchronisationsprozess auf allen Routern erforderlich. Dies bedeutet, dass mit einem erhöhten Overhead im Netzwerk und damit mit einer deutlichen Netzwerkbelastung gerechnet werden muss. Jedes Datenpaket wird beim Router-Durchlauf mit einem *Time Stamp* versehen, der vom nächsten Router gelesen und interpretiert wird. Infolge der ermittelten Zeitabweichung zu seiner eigenen Uhrzeit kann der Router das für die optimale Route relevante *Delay* berechnen und entsprechend für seine Auswahl zugrunde legen. Aus der Vielzahl periodisch versendeter bzw. empfangener *Hellos* wird die aktuelle Zeit im Netzwerk kontinuierlich untereinander abgestimmt und dadurch aktualisiert.

Zur Vermeidung eines *Route Hopping* wird eine Schwellenwertzeit beim Delay-Update eingesetzt. Ein unmittelbares Update hätte zur Folge, dass bei einer Routenänderung im Netzwerk *alle* Router die neue, günstigere Route

verwenden und dadurch eine Überlastung dieser Route hervorrufen würden. Die Überlastung führte allerdings dann wieder zu einem Verlassen der Route (sie wird ungünstiger), und anschließend würde diese erneut bevorzugt. Dieser *Hopping*-Vorgang würde sich kontinuierlich wiederholen.

4.2.5 Interior Gateway Routing Protocol (IGRP)

Neben allgemeinen Routing-Protokollen, die nicht aus den Labors bestimmter Hersteller stammen, hat es der Router-Hersteller Cisco geschafft, sein eigenes proprietäres Routing-Protokoll *Interior Gateway Routing Protocol* (IGRP) in seinen Routern auf dem Markt zu platzieren. Als die Komplexität der Netzwerke Mitte bis Ende der 80er Jahre des vorigen Jahrhunderts deutlich zunahm und es lediglich das für diese Zwecke etwas überforderte *Routing Information Protocol* (RIP) gab, empfahl sich IGRP als leistungsfähige Alternative. Während RIP den Hop-Count als einzig relevante Metrik verwendet, benutzt IGRP eine Kombination mehrerer Metriken. So sind beispielsweise das *Internetwork Delay*, also der Verzögerungsfaktor zwischen einzelnen Netzwerken, sowie Überlegungen zur garantierten Bandbreite vom Netzwerksystemverwalter zu bewertende Metriken und dienen ihm daher als Instrumentarien zur gezielten Einflussnahme auf die Wahl der Routen. Der Aufbau alternativer Routen im Falle von Störungen gehört ebenso zum Funktionsumfang wie die Lastverteilung; eine Route, die z.B. nur halb so teuer ist wie andere, wird auch doppelt so oft benutzt.

HINWEIS

Wie im OSPF ist auch im IGRP das Verhalten der einzelnen Router im Netzwerk über verschiedene *Timer* steuerbar. Es gibt *update timer, invalid timer, flush timer* oder auch *hold-time periods*.

Die Weiterentwicklung von IGRP wurde von Cisco in dem unmittelbaren Nachfolger EIGRP (Enhanced IGRP) fortgesetzt; siehe nachfolgender Abschnitt.

4.2.6 Enhanced IGRP

Anfang der 90er Jahre des vorigen Jahrhunderts wurde in den Routern der Firma Cisco die Weiterentwicklung des IGRP implementiert: Enhanced IGRP. Es stellt eine gelungene Mischung aus *Link-State-Protokollen* (wie beispielsweise das OSPF) und *Distance-Vector-Protokollen* (wie RIP oder auch IGRP) dar. Folgende Eigenschaften werden unterstützt:

- Durch einen neuen Algorithmus beim Update von Routing-Informationen (*Diffusing Update Algorithm* = DUAL) werden die Routing-Tabellen der Nachbar-Router ebenfalls gespeichert und stehen somit für eine rasche

Alternativroutenwahl unmittelbar zur Verfügung. Sollte dennoch eine Route nicht zustande kommen, so wird diese vom Nachbarn erfragt.

- Verwendung variabler Subnetzmasken (variabel in ihrer Länge), wodurch eine Bündelung von Subnetzrouten am logischen (Netz-ID des Subnetzes) Netzwerkübergang erfolgen kann
- Durchführung begrenzter Teil-Updates, bei denen Updates nicht periodisch wiederkehrend vorgenommen werden, sondern nur dann, wenn sich der Status der Metrik ändert. Nur diejenigen Router werden mit den relevanten Updates versorgt, die sie auch benötigen. Eine deutlich reduzierte Netzbelastung durch *Enhanced IGRP* gegenüber IGRP ist die Folge.
- Es lassen sich AppleTalk, IP und beispielsweise IPX gemeinsam verwenden. Dabei bezieht AppleTalk seine Routing-Informationen aus dem *Routing Table Maintenance Protocol* (RTMP), IP erhält die Informationen von OSPF, RIP, IS-IS, EGP oder BGP, während schließlich IPX vom *Novell RIP* und dem *Service Advertisement Protocol* (SAP) bedient wird.
- Einführung des *Reliable Transport Protocol* (RTP), bei dem nur speziell gekennzeichnete (Kennzeichen-)Pakete vom Empfänger bestätigt werden, alle übrigen bleiben unbestätigt.

4.2.7 Intermediate System – Intermediate System (IS-IS)

Im Gegensatz zu anderen Routing-Protokollen entstammt das IS-IS (*Intermediate System – Intermediate System*) als OSI-Protokoll den Bestrebungen der *International Standardization Organization* (ISO). Es gehört wie OSPF zur Kategorie der *Link State Protocols*, basiert auf der DECnet-Architektur *Phase V* und wird auf dem ISO-Netzwerk CLNP (*Connectionless Network Protocol*) eingesetzt. Folgende Protokolle sind dabei definiert:

- ISO 9542 – ES-IS
- ISO 10589 – IS-IS Intradomain Routing Exchange Protocol
- ISO 10747 – IS-IS Interdomain Routing Protocol

HINWEIS

Ein ES (*End System*) ist ein Netzwerkknoten, der keine Routing-Aufgaben übernimmt, und mit IS (*Intermediate System*) wird ein Router bezeichnet.

Die erweiterte Terminologie bilden die *Area* (Zusammenschluss mehrerer Hosts in verschiedenen Netzwerken) und die *Domain* (Verknüpfung von Areas). *Level 1 Router* stellen die Router-Verbindungen innerhalb einer Area her, wohingegen für die Area-zu-Area-Verbindung innerhalb einer Domain *Level 2 Router* zuständig sind.

End System to Intermediate System Protocol (ES-IS)

Bei dem Routing-Protokoll ES-IS handelt es sich mehr um ein Protokoll für das *Routing Discovery* als um ein vollwertiges Routing Protocol. Auf beiden beteiligten Systemen stattfindende Lernprozesse führen zur Bildung von beidseitigen Information-Pools. Es werden drei verschiedene Subnetztypen unterschieden:

- *Point-to-Point-Subnetze*

  Punkt-zu-Punkt-Verbindungen zwischen zwei Netzwerken

  - Beispiel: serielle oder ISDN-Verbindungen im WAN

- *Broadcast-Subnetze*

  Nachrichtenverteilung an alle Knoten im Netzwerk

  - Beispiel: Ethernet, IEEE 802.3, IEEE 802.5

- *General-Topology-Subnetz*

  Dieses Subnetz unterstützt eine willkürliche Anzahl von Endsystemen und Routern, ermöglicht jedoch keine Einrichtung zur komfortablen und verbindungslosen Übertragung an mehrere Zielknoten. Man unterscheidet *multipoint links* mit einem Primary-Secondary- bzw. Master-Slave-Kommunikationsverhalten, *permanent point-to-point links* in Form von Standleitungen und *dynamic data links*, die verbindungsorientiert arbeiten, wie beispielsweise X.25, X.21 oder ISDN.

Sowohl ES als auch IS senden sich untereinander *HELLO-Messages* (ESHs und ISHs) zu, um die Konfiguration betreffende Informationen zu übermitteln. Auf Broadcast-Netzwerken geschieht dies unter Verwendung einer Multicast-Adresse. In General-Topology-Netzwerken wird eine Übertragung solcher Konfigurationsdaten vermieden, denn bei (langsamen) WAN-Verbindungen schlägt eine erhöhte Netzlast mit hohen Leitungskosten bzw. einer geringen verbleibenden Bandbreite deutlich zu Buche.

4.2.8 Border Gateway Protocol (BGP)

Beim *Border Gateway Protocol* handelt es sich um ein Protokoll, das nicht zur Kategorie der *Internal Gateway Protocols* (IGP) gehört, sondern auf dem *External Gateway Protocol* (EGP) basiert (siehe RFC 827 vom Oktober 1982).

BGP stellt eine weit flexiblere und leistungsfähigere Alternative zum mittlerweile veralteten EGP dar. Es ermöglicht die Verwendung alternativer Routen zwischen zwei Domänen bzw. Autonomen Systemen (AS) und bietet Mechanismen zur Ermittlung und Vermeidung von Endlosschleifen (*Routing Loops*). Ähnlich wie bei OSPF werden keine vollständigen Routing-Tabellen ausgetauscht, sondern die Aktualität der Tabellen wird durch Updates und *keep alive messages* gewahrt. Während EGP bei überlasteten Netzwerken (*Congestions*) eine sehr schlechte Performance aufweist, arbeitet BGP durch TCP-basierende Retransmissions wesentlich toleranter.

Ein aktuelles Beispiel der auch heute noch betriebenen Weiterentwicklung von BGP (mittlerweile in Version 4 – gemäß RFC 4271 vom Januar 2006) kann dem RFC 6774 vom November 2012 entnommen werden. Hier wird ein relativ einfaches Verfahren zur BGP-Optimierung beschrieben, das im Wesentlichen durch eine Anpassung der BGP-Konfiguration auf Routern erreicht werden kann. Das BGP-Protokoll selbst wird in seiner Spezifikation dabei nicht verändert.

4.3 Betrieb und Wartung

Für den Praxiseinsatz lassen sich beim Betrieb und der Wartung von Routern folgende Schwerpunkte definieren:

- Diagnose von Hardwareproblemen des Router-Prozessors, seiner Netzwerkschnittstellen, seiner angebundenen Netzwerke, Modems oder Kommunikationsleitungen
- Installation neuer Hardware
- Installation neuer Software
- Neustart oder Reboot eines Routers nach erfolgtem Ausfall
- Konfiguration oder Rekonfiguration des Routers
- Ermittlung von IP-Problemen wie Überlast, Routing-Schleifen, fehlerhafte IP-Adressen, Broadcast-Stürme oder Fehlverhalten von Hosts
- Modifikation der Netzwerktopologie, entweder temporär (Aufbau alternativer Routen bei vorübergehenden Leitungsproblemen im Netzwerk) oder permanent

- Erstellung von Netzwerkstatistiken, um eine geeignete Netzwerkplanung zu realisieren
- Koordination vorgenannter Aktivitäten mit geeigneten Herstellern und Spezialisten aus dem Bereich der Telekommunikation

In vielen Unternehmen oder Organisationen erfolgt das Router-Management an zentraler Stelle und ausgelegt von einem gut ausgebildeten Team von Netzwerkspezialisten, die den oder die Router in der Regel über Netzwerkverbindungen installieren, konfigurieren und steuern. Dabei beschränkt sich der Zugang oft nicht auf eine klassische Netzwerkverbindung, sondern es werden separate Wählleitungen installiert, die auch bei Netzwerkstörungen den Router-Zugang ermöglichen. Dabei müssen Hilfsmittel für das Netzwerkmanagement und für die Beobachtung des Netzwerks und seiner Komponenten (Monitoring) verfügbar sein, wobei »überflüssiges« Monitoring immer zu einer zusätzlichen Belastung des Netzwerks führt; es gilt hier also, ein ausgewogenes Verhältnis zu finden.

4.3.1 Router-Initialisierung

Soll ein Router in ein Netzwerk integriert werden, so ist dieser in der Regel mit der Basissoftware bzw. seinem Betriebssystem vorinstalliert. In vielen Fällen ist dann auch bereits eine mit Default-Werten versehene Konfiguration vorhanden, die allerdings immer den eigenen Bedürfnissen angepasst werden muss. Fehlt beispielsweise eine Definition von IP-Adressen oder Subnetzmasken für einzelne Netzwerkschnittstellen, so sind bei einer Inbetriebnahme des Routers keinerlei Probleme zu erwarten. Geht der Router jedoch mit voreingestellten IP-Adressen ins Netz, so kann dies zu nicht vorhersehbaren Problemen führen. Eine individuelle Konfiguration sollte daher immer zu den ersten Aktivitäten vor Inbetriebnahme eines Routers gehören.

Die Funktionsfähigkeit eines Routers lässt sich grundsätzlich auf zwei verschiedenen Wegen herstellen: Entweder erfolgt die Installation bzw. Konfiguration manuell, wobei diese Informationen permanent gespeichert werden, sodass der Router nach Störungen jederzeit wieder rekonfigurierbar ist, oder seine vollständige Systemsoftware wird über das Netzwerk durch einen dedizierten Boot-Rechner unter Verwendung des BootP- und TFTP-Protokolls zur Verfügung gestellt.

Wie in Kapitel 3 (siehe dort) ausführlich dargestellt, ist BootP ein Protokoll, das zur Ermittlung von Rechnern dient, von denen ein Endsystem sein Betriebssystem und Konfigurationsparameter bezieht. Zu diesem Zweck wird vom Router ein *BootP Request* generiert, der die Hardwareadresse der eigenen

Netzwerkschnittstelle enthält. Derjenige BootP-Server, der diese empfangene Hardwareadresse kennt, übermittelt dem Router die ihm bekannt gegebene IP-Adresse des Routers, seine eigene IP-Adresse und den Namen des *Bootfile Image*. Nach Empfang dieser *BootP Response* (und ihrer lokalen permanenten Speicherung) besitzt der Router alle erforderlichen Informationen, um den Boot-Vorgang als vollwertiger IP-Knoten mit seinem Kommunikationspartner durchführen zu können, wozu zusätzlich auch ein File-Transfer-Protokoll benötigt wird; in den meisten Fällen ist dies TFTP (*Trivial File Transfer Protocol*).

HINWEIS

Auch bei einer automatisierten Installation und Konfiguration eines Routers ist es erforderlich, dass ein Router nicht nur direkt steuerbar ist – z.B. über eine angeschlossene Konsole oder über eine lokal bedienbare proprietäre Tastatur –, sondern auch über eine Netzwerkverbindung kontrolliert werden kann. Die erforderliche Kommunikation sollte dann über Standardprotokolle bzw. -anwendungen wie TELNET, FTP oder SNMP möglich sein.

4.3.2 Out-Of-Band Access

Bei anhaltenden Fehlersituationen in einem Netzwerk ist es oft nicht mehr möglich, einen Router über die Netzwerkverbindung (z.B. per *TELNET*) zu erreichen. Eine Fehleranalyse (Protokolldateien) oder ein Absetzen wichtiger Kommandos kann dann nicht mehr vorgenommen werden, sodass ein *direkter* Zugang zum Router notwendig wird. Wenn sich der Router jedoch außerhalb des direkten Einzugsbereichs befindet und möglicherweise in einer anderen Location (viele Kilometer entfernt) untergebracht ist, würde sehr viel Zeit verstreichen, bis man vor Ort ein entsprechendes Operating durchführen könnte.

Für solche Notfälle ist es zu empfehlen, einen *Remote Access* durchzuführen, der vom eigentlichen Netzwerk unabhängig implementiert ist. Dieser *Out-Of-Band Access* (OOB) lässt sich beispielsweise durch eine separate Wählleitung (analog oder digital) über einen ISDN-Controller realisieren, wobei natürlich für diese Art der Fernwartung in jedem Router eine zusätzliche Schnittstelle eingebaut und konfiguriert werden muss (siehe Abb. 4–11).

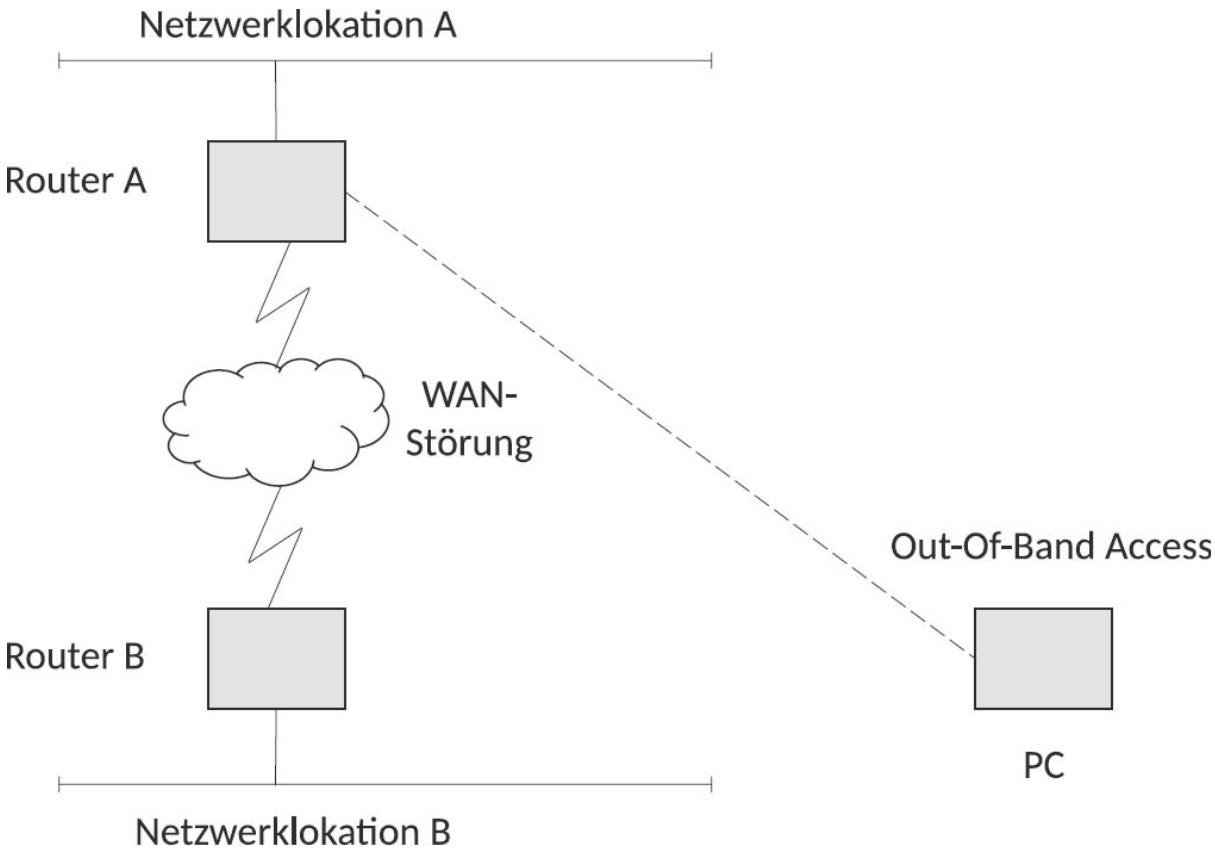

Abb. 4–11 *Out-Of-Band Access*

Heute arbeitet man auch zunehmend mit mobilfunknetzbasierten OOB-Komponenten (GSM-Modems), die in einen Router »eingeschleift« werden können. Man schafft sich somit die Möglichkeit, einen Router im Störungsfall vom Stromnetz zu trennen, und ist nicht nur auf *Software-Resets* beschränkt.

HINWEIS

Beim Aufbau eines (oben beschriebenen) »Notfallzugangs« ist darauf zu achten, dass die OOB-Verbindung keinerlei Einschränkungen in den wesentlichen Funktionen des Router-Managements unterliegt.

4.3.3 Hardwarediagnose

Für die Überprüfung der rudimentären Betriebs- und Funktionsfähigkeit eines Routers müssen in der Basissoftware Programme zur Verfügung stehen, die Aufschluss über den aktuellen Zustand des Geräts geben können. Die Ausführung von Diagnoseprogrammen oder die Durchführung von Selbsttests (einschließlich aller angeschlossenen Schnittstellen) ist obligatorisch. Ferner sollte es die Möglichkeit geben, einen System-Dump (Hauptspeicherauszug) zu erzeugen.

4.3.4 Router-Steuerung

Für die automatische Wiederherstellung (*Recovery*) in Störsituationen ist ein Automatismus erforderlich, der einen *Reboot* oder einen *Restart* des Routers auslöst. Nicht immer ist es sinnvoll, so lange zu warten, bis das Netzwerkteam den Fehler erkennt, analysiert und anschließend die Fehlersituation beseitigt. Wenn der Router automatisch neu startet, ist es allerdings wünschenswert, dass die Fehlersituation nicht nur lokal in einer Berichtsdatei gesichert, sondern möglichst auch ein Speicherauszug (*Memory Dump*) ausgeführt wird, um Fehler nachträglich analysieren zu können.

Änderungen an der Router-Konfiguration erfordern nicht selten einen Systemstopp bzw. einen Neustart; einige der Konfigurationsparameter werden unmittelbar nach der Einrichtung aktiv, einige erfordern einen Neustart (*Reboot*). Die Planung von Konfigurationsänderungen sollte diesen Sachverhalt berücksichtigen, da ein *Reboot* des Routers stets mit einem Ausfall der betroffenen Netzwerkverbindungen einhergeht. Erfahrungsgemäß empfiehlt sich eine Durchführung dieser Wartungsarbeiten in fest eingeplanten Wartungsintervallen oder, sofern es derartige Wartungsfenster nicht gibt, an Wochenenden oder Feiertagen.

4.3.5 Sicherheitsaspekte

Ein äußerst strittiges Thema ist das *Auditing* und das *Accounting*. Es besteht die aus Sicherheitsgründen verständliche Anforderung, wesentliche Konfigurationsänderungen im Router-Profil zu protokollieren, damit jederzeit nachvollzogen werden kann, wer wann welche Änderungen vorgenommen hat. Verletzungen der Filtering-Vorschriften oder Autorisationsmängel (falsche Passwörter, ungültige SNMP-Communities usw.) gehören zu den *Audit-relevanten* Ereignissen. Darüber hinaus sollte jeder Anwender in dem Maße mit anfallenden fixen und vor allem variablen Kosten belastet werden (z.B. Hardware- und Software-Leasing, Leitungskosten), wie er den Router in Anspruch nimmt; in dem Zusammenhang ist auch von *Packet Accounting* die Rede.

Damit die geforderten Informationen zur Verfügung gestellt werden können, bedarf es einer Fülle von Prozessen, die zusätzlich zum »normalen« Datenverkehr auf dem Router betrieben werden müssen. Die Leistungsfähigkeit des Routers wird dadurch natürlich mehr oder weniger stark beeinträchtigt. In diesem Interessenkonflikt muss versucht werden, ein individuelles, aber ausgewogenes Konzept zu entwickeln, das allen Anforderungen in vernünftigem Umfang entsprechen kann.

4.4 Software Defined Networking (SDN)

Heutige Netzwerke verlangen aufgrund des erheblich zugenommenen Datenaufkommens leistungsfähige Routing-Konzepte. Da sich an den eigentlichen Routing-Protokollen in den letzten Jahren nicht viel geändert hat, sind neue Konzepte erforderlich, die eine deutliche Optimierung der Wegewahl innerhalb der Netzwerke ermöglichen. Die Technologie des *Software Defined Networking* (SDN) stellt solch eine Optimierung dar.

Dem SDN liegt formal eine Trennung »der Kontrollebene von der Datenebene« zugrunde. Eine zentrale (Hardware-unabhängige) Instanz übernimmt die vollständige Kontrolle des Netzwerks und all seiner beteiligten Komponenten. Sämtliche erforderliche Kommunikation beispielsweise zur Parameterabstimmung oder Routenoptimierung läuft über diese Instanz. Man reduziert dadurch die Komplexität mehr oder weniger gleichberechtigter Netzwerkkomponenten durch einen »Chef-Kommunikator«, der auch gleichzeitig in einer Hierarchie an oberster Stelle steht.

Mit dieser konzeptionellen Änderung im Netzwerk erhält der Netzwerkadministrator im Unternehmen eine wesentlich bessere Kontrolle über »sein« Netzwerk, da er diese ohne Hardware-Restriktionen bzw. -Spezifikationen der Hersteller ausüben kann. Open-Source-Software zur Administration von Netzwerken spielt in dieser Umgebung eine besondere Rolle; denn sie ist überall verfügbar und unter Berücksichtigung eines allseits akzeptierten Regelwerks sehr flexibel einsetzbar. Die Zukunft wird nicht mehr von z.T. proprietärer »Netzwerk-Intelligenz« der Hersteller bestimmt, sondern die Kontrolle erhält nun das Unternehmen bzw. der Internet-Service-Provider mit eigenen Entwicklungen und der »Selbst-Programmierung« ihrer Netzwerke.

Abb. 4–12 zeigt eine vereinfachte SDN-Architektur, die allerdings nur das Grundprinzip darstellt, nicht aber alle im SDN beheimatete Varianten, wie sie in den folgenden Abschnitten kurz erläutert werden.

HINWEIS

Die Kontrollebene wird auch *Control Plane*, die Hardware-/Infrastrukturebene wird im internationalen Sprachgebrauch auch *Data Plane* genannt.

OpenFlow bezeichnet eine Standard-Schnittstelle zur Kommunikation zwischen Kontroll- und Datentransportebene im SDN. Sie wird mittlerweile von zahlreichen Herstellern der »Data Plane«-Komponenten unterstützt. Der Standard wird von der *Open Network Foundation* (ONF) verwaltet.

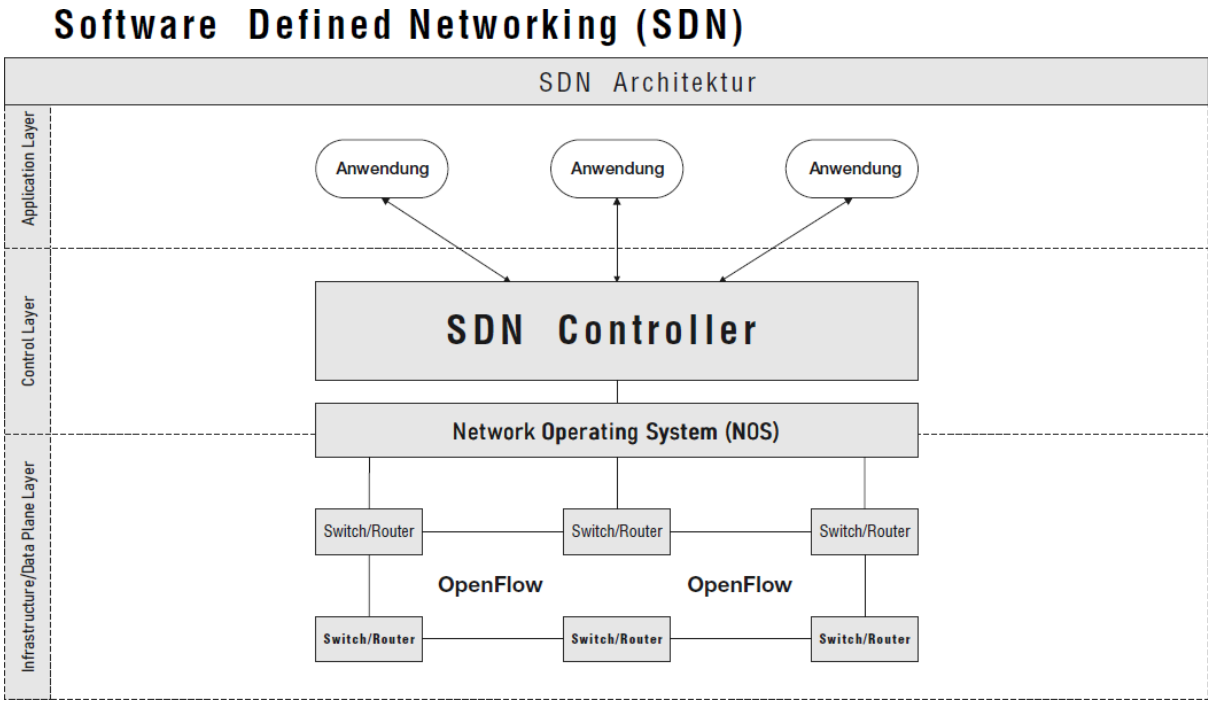

Abb. 4–12 *SDN Architektur*

SDN ist aber kein Allheilmittel. Es schützt das Netzwerk beispielsweise nicht vor Störungen, die wegen nicht vorhandener oder unzureichender Transparenz des Netzwerks entstehen. Daher ist es u.a. von entscheidender Bedeutung, dass der »Controller« sämtliche Statusinformationen oder auch Aktivitäten der Netzwerkadministratoren akribisch protokolliert.

Beispiele für SDN-Implementierungen sind:

4.4.1 Netzwerk Virtualisierung

Sie stellt eine weit umfassendere Virtualisierung von Netzwerk-Ressourcen dar, als diese mit den seit Jahren bereits praktizierten virtuellen privaten Netzwerken (VPNs) oder virtuellen LANs (VLANs) möglich sind.

4.4.2 Switching Fabrics

Sie wird primär bei Cloud-Providern und größeren Unternehmensnetzwerken eingesetzt. Dieses Konzept vermeidet den Einsatz von proprietärer Hardware und verwendet stattdessen einfache switching Hardware mit eigener »Intelligenz« über Softwarelösungen. Switching Fabrics kommen oft im Zusammenhang mit der neuen »Spine-Leaf«-Netzwerkarchitektur zum Einsatz, das zunehmend das ältere hierarchische Modell (*Access – Distribution – Core*) ablöst. Die neue Architektur bietet einige Vorteile wie beispielsweise eine reduzierte Latenz (kürzere Wege in einer vermaschten Zwei-Ebenen-Konzeption)

sowie eine bessere Skalierbarkeit (Komponenten können auf beiden Ebenen problemlos ergänzt oder entfernt werden).

4.4.3 WAN Traffic Engineering

Diese Technologie ist prinzipiell nicht neu, sondern wird bereits seit Jahren in MPLS-Netzwerken im WAN angewendet – allerdings ohne die im SDN-Umfeld nun mögliche zentrale Übersicht des Datenverkehrs und das damit verbundene Optimierungspotenzial (z.B. bei der Re-Kalkulation von Routen im Zuge von Statusänderungen einzelner Verbindungen). Die Priorisierung bestimmter Datenklassen stellt eine weitere Funktion zur Effizienzsteigerung des Netzwerks dar.

4.4.4 SD-WAN

Mit SD-WAN wird die klassische Strukturierung eines MPLS-Netzwerks in CE-Routern (*Customer Edge Router*; beim Kunden) und PE-Routern (*Provider Edge Router*; beim Provider/Netzwerkanbieter) durch eine wesentlich flexiblere Konzeption abgelöst. Die zentrale Konfiguration von Routern in Zweigstellen eines Unternehmensnetzwerks erfolgt automatisch, wenn der Router in der Zweigstelle eingetroffen und mit dem Netzwerk verbunden ist. Separater und individueller Konfigurationsaufwand ist nicht mehr erforderlich. Ferner ermöglichen SD-WAN-Strukturen wesentlich besseres Change Management und reduzieren somit Ausfallzeiten.

4.4.5 Access Networks

Die Implementierung von »Last Mile«-Anbindungen an das Internet werden auch *Access Networks* genannt. So stellt das »Fiber-to-the-Home«-Konzept oder das »radio access network« (4G/5G-Vermittlung) ein solches Access Network dar.

Index

Ziffern

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z