

Webcode - Übungsdateien

CD1D-C5DF-C350

Berufsbildende Schule I Mainz



In Kooperation mit dem HERDT-Verlag stellen wir Ihnen eine PDF inkl. Zusatzmedien für Ihre persönliche Weiterbildung zur Verfügung. In Verbindung mit dem Programm HERDT|Campus ALL YOU CAN READ stehen diese PDFs nur Lehrkräften und Schüler*innen der oben genannten Lehranstalt zur Verfügung. Eine Nutzung oder Weitergabe für andere Zwecke ist ausdrücklich verboten und unterliegt dem Urheberrecht. Jeglicher Verstoß kann zivil- und strafrechtliche Konsequenzen nach sich ziehen.

Netzwerke

Protokolle und Dienste

(Stand 2017)

Andreas Dittfurth

9. Ausgabe, 1. Aktualisierung, Januar 2020

ISBN 978-3-86249-753-9

NWPD



1 Informationen zu diesem Buch	4	6.3 TCP-Header	65
1.1 Voraussetzungen und Ziele	4	6.4 UDP	66
1.2 Aufbau und Konventionen	4	6.5 Übung	68
2 Übersicht über gängige Kommunikationsprotokolle	6	7 Network Address Translation	70
2.1 Die Aufgaben von Protokollen und Diensten in der EDV	6	7.1 Datenaustausch mit dem Internet über NAT	70
2.2 Protokolle in lokalen Netzwerken	8	7.2 Praktische Einsatzgebiete	74
2.3 Namensauflösende Dienste	10	7.3 Vergleich mit Proxy- und Routerlösungen	76
2.4 Protokolle aus dem Weitverkehrsbereich	13	7.4 Übung	77
2.5 Neue Protokolle an der Grenze zwischen WAN und LAN	14	8 Routing	78
3 Netzwerkmodelle	18	8.1 Statisches Routing	78
3.1 Überblick Netzwerkmodelle	18	8.2 Dynamisches Routing	82
3.2 Das OSI-Modell	19	8.3 Distance-Vector-Protokolle	85
3.3 Sieben Schichten des OSI-Modells	22	8.4 Linkstate-Protokolle	87
3.4 Das DoD-Modell	27	8.5 Übung	87
3.5 Das TCP/IP-Modell	27	9 Namensdienst DNS	90
3.6 Kapselung und Entkapselung	28	9.1 Konzept	90
3.7 Übung	29	9.2 Forward Lookup	92
		9.3 Reverse Lookup	103
		9.4 Primäre und sekundäre Zone	104
4 Die TCP/IP-Protokollsammlung	30	9.5 Dynamisches DNS	106
4.1 Die Protokolle und ihre Aufgaben	30	9.6 Round Robin	107
4.2 Interaktion zwischen Protokollen und Diensten	33	9.7 GlobalNames	108
4.3 Die MAC-Adresse	35	9.8 DNSSEC	109
4.4 Übung	36	9.9 Übung	110
5 Das Internet-Protokoll IP	38	10 Namensdienst WINS	112
5.1 Bestandteile und Aufgaben von IP	38	10.1 NetBIOS	112
5.2 Mathematische Grundlagen für die Arbeit mit IP	40	10.2 WINS	114
5.3 IP-Adressen und Subnetzmasken	43	11 Netzwerkkonfigurationsdienste	116
5.4 IP-Pakete	45	11.1 Aufgabe und Funktion von Netzwerkkonfigurationsdiensten	116
5.5 Internet-Control-Message-Protokoll	49	11.2 BootP	116
5.6 IPv6	50	11.3 DHCP	119
5.7 IPv6-Übergangsmechanismen	54	11.4 DHCP-Optionen	125
5.8 Übung	56	11.5 Ausfallsicherheit unter DHCP/BootP	128
6 TCP und UDP	60	11.6 APIPA in kleinen Netzwerken	129
6.1 Funktion und Aufbau von TCP und UDP	60	11.7 Übung	131
6.2 Arbeitsweise von TCP	61		

12 ATM und LANE	132	16 Virtual Private Network	156
12.1 ATM	132	16.1 Zielsetzung	156
12.2 ATM im Vergleich zu LAN	134	16.2 PPTP	157
12.3 LAN-Emulation (LANE)	136	16.3 L2TP/IPSEC	158
12.4 Übung	137	16.4 OpenVPN	162
		16.5 Abgrenzung zu anderen VPN-Arten	162
13 DSL	138		
13.1 Grundlagen zu DSL	138	17 WLAN	164
		17.1 WLAN	164
14 Frame Relay	144	17.2 Sicherheit	167
14.1 Grundlagen zu Frame Relay	144		
14.2 Frame Relay in der Praxis	146	18 Firewall und DMZ	170
14.3 Frame Relay im Vergleich zu ATM und X.25	147	18.1 Wie Firewalls arbeiten	170
		18.2 Paketfilter-Firewall	173
15 RAS und NPS	148	18.3 Stateful Inspection Firewall	174
15.1 Remote Access Service	148	18.4 Proxy Level/Application Level Firewall	175
15.2 Arten von RAS-Anbindungen	148	18.5 NAT	176
15.3 RAS-Authentifizierung	151	18.6 Personal Firewall	177
15.4 Network Policy Server (NPS)	154	18.7 Sicherheitskonzept Firewall	177
		Stichwortverzeichnis	178

1 Informationen zu diesem Buch

In diesem Kapitel erfahren Sie

- ✓ wie Sie dieses Buch einsetzen können
- ✓ welche Vorkenntnisse Sie mitbringen sollten
- ✓ welche Konventionen für dieses Buch gelten

1.1 Voraussetzungen und Ziele

Zielgruppe

- ✓ Netzwerkspezialisten
- ✓ Studierende der Informatik
- ✓ Telekommunikationstechniker
- ✓ Auszubildende in IT-Berufen

Empfohlene Vorkenntnisse

Bei den Kursteilnehmern werden folgende Kenntnisse vorausgesetzt:

- ✓ Grundwissen zu Computer-Netzwerken
- ✓ Grundwissen zu Betriebssystemen (Linux, Windows)
- ✓ Grundwissen über Hardware (PC, Netzwerkkomponenten)

Lernziele

Nach dem Durcharbeiten des Buchs kennt der Leser die wichtigsten Protokolle in IT-Netzwerken: TCP/IP-Protokoll-Familie, ATM, DSL, Frame Relay, WLAN. Er kann sie in Aufgaben und Funktionen unterscheiden und ist vertraut mit der Ansiedlung im OSI-Schichtenmodell. Neben den Protokollen an sich werden auch die Dienste beschrieben, die diese Protokolle verwenden. Dazu gehören die Namensauflösung (DNS, WINS), das Routing, RAS und VPN. Auch sicherheitsrelevante Themen werden dargestellt (Firewall und DMZ).

Hinweise zu Soft- und Hardware

Zum besseren Verständnis der Protokolle empfiehlt sich der Einsatz eines Netzwerkanalysators (auch „Netzwerk-sniffer“ genannt) wie Wireshark (siehe: <https://www.wireshark.org/>), um selbst die Funktionen und Kommunikationsabläufe bestimmter Protokolle und Dienste nachvollziehen zu können. Das Programm sollte auf einem Rechner mit Netzwerkzugang installiert werden. Sollen darüber hinaus Dienstkonfigurationen nachvollzogen werden, wird ein Server mit installierten Netzwerkdiensten wie DNS, DHCP und RAS/VPN benötigt.

1.2 Aufbau und Konventionen

Aufbau des Buchs

- ✓ Am Anfang eines jeden Kapitels finden Sie die Lernziele.
- ✓ Am Ende einiger Kapitel finden Sie Übungen zur Vertiefung und zur Lernkontrolle.
- ✓ Notizseiten in diesem Buch ermöglichen es Ihnen, eigene Anmerkungen und Ergänzungen vorzunehmen.

Inhaltliche Gliederung

In diesem Buch werden nach einer allgemeinen Einführung die wichtigsten Protokolle mit ihren Funktionen, ihrem Aufbau und ihren Einsatzgebieten vorgestellt. Zum besseren Verständnis sind dabei auch die verschiedenen Netzwerkmodelle erklärt. Bei der Beschreibung der einzelnen LAN- und WAN-Protokolle wird teilweise der schematische Aufbau erläutert, teilweise werden auch anhand von Netzwerkanalysatoren die Details der Kommunikationsvorgänge bei bestimmten Protokollen erläutert. Daneben sind Beispiele aus der Praxis aufgeführt, die dem Leser die Einsatzmöglichkeiten der Protokolle und Dienste näher bringen sollen. Dabei werden verschiedene Betriebssysteme verwendet, um die herstellerübergreifende Funktionalität aufzuzeigen.

Typografische Konventionen

Damit Sie bestimmte Elemente auf einen Blick erkennen und zuordnen können, werden diese im Text durch eine besondere Formatierung hervorgehoben. So werden beispielsweise Bezeichnungen für Programmelemente wie Register oder Schaltflächen immer *kursiv* geschrieben und wichtige Begriffe **fett** hervorgehoben.

- | | |
|----------------------|---|
| Kursivschrift | kennzeichnen alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten etc., Menüs bzw. Menüpunkte (z. B. <i>Datei - Schließen</i>), Internetadressen und vom Benutzer angelegte Namen (z. B. Rechner-, Domänen-, Benutzernamen). |
| Courier | wird für Systembefehle sowie für Datei- und Verzeichnisnamen verwendet.
In Syntaxangaben werden Parameter kursiv ausgezeichnet (z. B. <code>cd Verzeichnisname</code>).
Eckige Klammern [] kennzeichnen optionale Elemente. Alternative Eingaben sind durch einen senkrechten Strich getrennt. Benutzereingaben auf der Konsole werden fett hervorgehoben. |

Symbole



Hilfreiche Zusatzinformation



Praxistipp



Warnhinweis

HERDT BuchPlus - unser Konzept:

Problemlos einsteigen - Effizient lernen - Zielgerichtet nachschlagen

(weitere Infos unter www.herdt.com/BuchPlus)

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



- Rufen Sie im Browser die Internetadresse www.herdt.com auf.

1 Wählen Sie Codes.

2 Geben Sie den folgenden Matchcode ein: **NWPD.**

2 Übersicht über gängige Kommunikationsprotokolle

In diesem Kapitel erfahren Sie

- ✓ was Protokolle sind
- ✓ was Dienste sind
- ✓ wie Protokolle und Dienste eingesetzt werden

Voraussetzungen

- ✓ Netzwerkgrundlagen

2.1 Die Aufgaben von Protokollen und Diensten in der EDV

Protokolle und Dienste

Protokolle dienen in der IT dazu, den Transport von Daten zu gewährleisten. Sie stellen die „Sprachen“ dar, mit denen verschiedene Systeme miteinander kommunizieren. An jedem Kommunikationsprozess sind mehrere Protokolle beteiligt.

Dienste stellen den Protokollen eine Umgebung zur Verfügung, in der Aufgaben, wie etwa die Konfiguration von Netzwerkinformationen oder die Bereitstellung von Daten auf entfernten Systemen, bewältigt werden können. Die Trennlinie zwischen Diensten und Protokollen zu finden ist nicht immer ganz einfach. So basiert der Dienst des Internets (WWW) auf einem eigenen Protokoll (HTTP), der namensauflösende Dienst DNS (Domain Name System) jedoch verwendet das Protokoll DNS.

Generell gilt, dass kein Dienst ohne ein geeignetes Protokoll seine Aufgaben erledigen kann. Denn jede Kommunikation basiert in der IT auf einer Vielzahl von unterschiedlichen Möglichkeiten, die jeweils eine genaue Anpassung der Umgebung erfordern. Diese Anpassungen werden als Regelsätze von exakt für diese Aufgaben entworfenen Protokollen beschrieben.

Protokolle für die physikalische Datenübertragung

Eine Gruppe von Protokollen beschreibt das Verfahren, wie Daten über ein bestimmtes Medium transportiert werden müssen. So wird etwa im Ethernet-Protokoll die Art des Zugriffs auf das Übertragungsmedium (CSMA/CD = Carrier Sense, Multiple Access with Collision Detection; etwa: Leitungsabfrage bei vielfachem Zugriff mit Kollisionserkennung) festgelegt; es werden aber auch Definitionen der Ströme, Adernbelegungen, Spannungen, die eine Null oder eine Eins darstellen, usw. beschrieben.

Andere Protokolle dienen dazu, die Daten aus einem Netzwerk in die Daten einer Telefonverbindung einzubinden, um so den Transport zwischen den Netzwerken zu ermöglichen. Die Definitionen dessen, was dabei die Telefonverbindung selber betrifft, fallen hierbei in den Grenzbereich der Netzwerkprotokolle. Zwar kann eine WAN-Verbindung mittels ISDN aufgebaut werden, dabei handelt es sich jedoch um die Nutzung eines netzwurfremden Dienstes.

Der Einsatz von hardwarenahen Protokollen wird durch die verwendete Hardware bestimmt und lässt keinen Spielraum für individuelle Anpassungen.

Protokolle für die Wegermittlung und den Pakettransport

Eine weitere Gruppe von Protokollen hat die Aufgabe, den Transport von Datenpaketen zwischen Netzen zu gewährleisten. Diese Protokolle lassen sich in zwei Gruppen fassen:

- ✓ Protokolle zur Ermittlung der möglichen Wege zwischen Netzwerken (Routing-Protokolle)
- ✓ Protokolle zum Transport von Paketen zwischen Netzwerken (geroutete Protokolle)

Protokolle für den Datentransport

Auf einem Computer nehmen meist mehrere Anwendungen gleichzeitig Dienste des Netzwerkes in Anspruch. Zwischen diesen Anwendungen und dem Netzwerk müssen vermittelnde Protokolle eingesetzt werden, die die Daten in transportgerechte Segmente unterteilen und beim Zusammensetzen an die jeweils richtige Anwendung weiterleiten. Die Datensegmente, die von den Transportprotokollen an die Netzwerkprotokolle weitergereicht werden, bezeichnet man als Datagramme.

Da Datagramme auf unterschiedlichen Pfaden durch das Netzwerk transportiert werden können, muss darauf geachtet werden, dass sie in der richtigen Reihenfolge zusammengesetzt und an die Anwendungen weitergereicht werden.

Einer der Gründe, warum Daten in Segmenten und nicht im Ganzen übertragen werden, ist dabei, dass bei einer Beschädigung oder einer teilweise fehlerhaften Übertragung nicht das gesamte Datenpaket neu gesendet werden muss. Das beteiligte Protokoll nimmt bei jedem zusätzlichen Verarbeitungsprozess zu diesem Zweck eine weitere Unterteilung der Daten in kleinere Stücke vor. Viele Protokolle können dann bei einer Beschädigung oder einem Datenverlust geeignete Reaktionen in die Wege leiten, um die Daten erneut zu übertragen. Andere Protokolle verlassen sich darauf, dass weitere am Kommunikationsprozess beteiligte Protokolle oder Dienste die Datenintegrität sicherstellen.

Generell benötigt jede zusätzliche Funktionalität beim Datentransport auch die Bandbreite des Netzwerkes und die Verarbeitungskapazität der CPU. Daher gilt es immer, einen Kompromiss zwischen Sicherheit der Übertragung und Effektivität der Ressourcen-Nutzung zu finden.

Dienste

Aktuelle Dienste umfassen unterschiedlichste Aufgaben. Viele dieser Aufgaben werden nicht von einem einzelnen Dienst gewährleistet, sondern werden durch mehrere unterschiedliche Dienste abgedeckt. Dies ist teilweise auf sich verändernde Ansprüche und Leistungsfähigkeiten von Netzwerken, Betriebssystemen, Benutzern und Anwendungen zurückzuführen, zum Teil handelt es sich bei alternativen Diensten um Produkte verschiedener Hersteller.

Dienste in Netzwerken lassen sich grob in drei Gruppen unterteilen:

- ✓ Dienste für den Netzwerkbetrieb
- ✓ Dienste für Betriebssysteme
- ✓ Dienste für Anwender und Anwendungen

Dienste für den Netzwerkbetrieb

Dienste für den Netzwerkbetrieb haben die Aufgabe, den einwandfreien und benutzerfreundlichen Betrieb von Netzwerken sicherzustellen. Sie übernehmen Dienste wie Adressauflösung und -zuweisung, Zeitsynchronisation, Sicherheitsfilterung von Daten und Paketen oder die Bereitstellung zwischengespeicherter Informationen zur Entlastung von Weitverkehrsverbindungen.

Teilweise ist dabei die Grenze zu den anderen Gruppen von Netzwerkdiensten eine fließende. So kann etwa die Zeitsynchronisation sowohl von Netzwerkkomponenten als auch von Betriebssystemen oder Benutzern verwendet werden.

Dienste für Betriebssysteme

Es gibt eine ganze Reihe von Diensten, die betriebssystemspezifische Aufgaben erfüllen. In der Folge finden Sie eine Übersicht über gängige Betriebssystemaufgaben, die von Netzwerkdiensten gewährleistet werden:

- ✓ **Benutzeroauthentifizierung:** Die Anmeldeinformationen von Benutzern werden bei modernen Netzwerken nicht mehr von lokalen Systemen abgelegt. Die Verwaltung erfolgt in einer zentralen Datenbank für das gesamte Netzwerk, die Authentifizierung übernimmt ein zentraler Server.
- ✓ **Bereitstellung verteilter Dienst:** Um Systemressourcen effizienter zu nutzen, können beispielsweise Datenbanken auf mehrere Rechner verteilt werden. Auch Anwendungen laufen nicht immer auf dem lokalen System, sondern werden zunehmend auf sogenannten Anwendungsservern ausgeführt. Dies bietet Einsparungspotenzial für Hardware und Lizenzen. Zudem kann der administrative Aufwand für die Netzwerkwartung deutlich verringert werden.
- ✓ **Ausfallsicherheit:** Indem beispielsweise Dokumentationen mittels verteilter Dateisysteme auf mehreren Servern im Netzwerk gespeichert werden, kann erreicht werden, dass bei Ausfall kompletter Systeme das Netzwerk einsatzbereit bleibt. Durch geografische Verteilung von Systemen – z. B. Clusterung über Weitverkehrsleitungen – kann ein wirksamer Schutz vor Datenverlust bei Katastrophen wie Erdbeben, Flugzeugabstürzen oder Bränden errichtet werden.
- ✓ **Lastenverteilung:** Neben der Ausfallsicherheit bieten Cluster den Vorteil, die Leistungsfähigkeit von Systemen zu erhöhen. Werden Dienste auf mehrere Systeme verteilt, kann dem Entstehen von Ressourcenengpässen (sog. „Flaschenhälse“) vorgebeugt werden.

Dienste für Anwender und Anwendungen

Diese Gruppe von Netzwerkdiensten stellt Benutzern und Anwendungen Dienste wie das World Wide Web, Newsgroups oder E-Mail zur Verfügung. In Firmennetzwerken bieten die Dienste Zugriff von Programmen auf Remote-Drucker oder das Speichern von Daten auf Datei-Servern.

Dienste sorgen dafür, dass beim Einkaufen über das Internet Informationen verschlüsselt werden, um sie vor dem Zugriff durch Dritte zu schützen. Bei einem einzigen Zugriff auf eine Website kommen neben HTTP etwa Cookies, Skripten, Active-X-Steuerdaten usw. zum Tragen, die größtenteils wiederum auf eigene Netzwerkdienste zurückgreifen.

2.2 Protokolle in lokalen Netzwerken

Netzwerkprotokolle

Eine ganze Reihe von Protokollen, die in lokalen Netzwerken Verwendung finden, soll hier kurz vorgestellt werden. Diese sind aus Gründen der Übersichtlichkeit in folgende Gruppen unterteilt:

- ✓ Übertragungsprotokolle
- ✓ Übermittlungsprotokolle

Die Gruppe der Übertragungsprotokolle bezieht sich dabei auf die physikalische Übertragung von Daten und betrifft den hardwarenahen Bereich.

Die Übermittlungsprotokolle beschäftigen sich mit der korrekten Zustellung von Daten über das Netzwerk. Sie gewährleisten, dass Daten vom korrekten Empfänger ausgewertet werden, dass die Weiterverarbeitung im System fehlerfrei und effizient vollzogen wird und dass beschädigte oder verloren gegangene Daten erneut übertragen werden.

Übertragungsprotokolle

Die Gruppe der verwendeten Übertragungsprotokolle in modernen Netzwerken ist nicht mehr so groß, wie noch vor wenigen Jahren. Neben Ethernet kommt heutzutage kaum ein kabelbasiertes Protokoll mehr zum Einsatz. Nachdem IBM Anfang 2002 die Produktion von Komponenten für Token-Ring-Netzwerke eingestellt hat, war dessen Verschwinden aus modernen Netzwerken absehbar.

Auch Verfahren wie VG-AnyLAN findet man in kaum einem Netzwerk mehr vor. Gründe hierfür sind neben den Kosten vor allem eine Tendenz des Marktes zur Vereinheitlichung. Dabei muss sich nicht das beste Verfahren durchsetzen, sondern vielleicht das mit der breitesten Unterstützung durch die Hersteller.

Ethernet

Ethernet spezifiziert Software (u. a. Protokolle) und Hardware (u. a. Kabel, Verteiler, Netzwerkkarten) für kabelgebundene Datennetze. Ursprünglich war Ethernet für lokale Datennetze (LANs) gedacht, wird daher auch als LAN-Technik bezeichnet. Daten werden in Form von Datenframes zwischen den im lokalen Netzwerk verbundenen Geräten ausgetauscht. Derzeit sind Übertragungsraten von 10 Mbit/s, 100 Mbit/s (Fast Ethernet), 1000 Mbit/s (Gigabit-Ethernet), 10, 40 und 100 Gbit/s spezifiziert. In seiner ursprünglichen Form erstreckt sich das LAN dabei nur über ein Gebäude; Ethernet über Glasfaser hat eine Reichweite von 10 km und mehr.

Die Ethernet-Protokolle umfassen Festlegungen für Kabeltypen und Stecker sowie für Übertragungsformen. Im OSI-Modell (siehe Kapitel 3) ist mit Ethernet sowohl OSI-Schicht 1 und 2 festgelegt. Ethernet entspricht weitestgehend der IEEE-Norm 802.3. Es wurde ab den 90er Jahren zur meistverwendeten LAN-Technik und hat andere LAN-Standards wie Token Ring verdrängt. Ethernet kann die Basis für Netzwerkprotokolle, z. B. AppleTalk, DECnet, IPX/SPX oder TCP/IP, bilden.

Eine ausführliche, stets aktuelle Übersicht über die vielen verschiedenen Ethernet-Spezifikationen finden Sie unter der Adresse <https://de.wikipedia.org/wiki/Ethernet>.

Übermittlungsprotokolle

Übermittlungsprotokolle stellen sicher, dass Daten auf einem geeigneten Weg vom Sender zum Empfänger übermittelt werden. Sie sind generell in zwei Gruppen zu fassen:

- ✓ routingfähige Protokolle
- ✓ nicht routingfähige Protokolle

Routingfähige Protokolle enthalten Informationen über logische Strukturen von Netzwerken. Diese Strukturen werden in Form von Netzen und Subnetzen gebildet, die über Router miteinander in Verbindung stehen. Sie dienen dazu, eine Hierarchie im Netzwerk zu implementieren, und können dabei Broadcast-Domänen segmentieren. Werden Daten innerhalb eines logischen Netzes übermittelt, spielt die Hierarchie keine große Rolle. Soll Datenverkehr aber die Grenzen eines Netzes überschreiten, muss im routingfähigen Protokoll eine Information über das Zielnetzwerk enthalten sein, die es den vermittelnden Geräten (Routern) erlaubt, einen geeigneten Weg zu wählen.

In der Vergangenheit wurden verschiedene routingfähige Protokolle verwendet, heutzutage spielen nur noch IPv4 und IPv6 eine Rolle.

Nicht routingfähige Protokolle spielen keine Rolle für den Datenverkehr zwischen Netzwerken. Sie unterstützen keine Untergliederung in logische Netze, sondern gehen davon aus, dass sich alle physikalisch ansprechbaren Knoten eines Netzwerkes im selben logischen Verbund befinden. Daher können sie auch nicht eingesetzt werden, um Datenverkehr zwischen Netzen zu ermöglichen.

Diesem Nachteil steht auf der anderen Seite gegenüber, dass der Konfigurationsaufwand des Protokolls und sein Overhead (der Anteil an zusätzlich zu den Nutzdaten zu übermittelnden Informationen des Protokolls) deutlich geringer ausfallen, als wenn eine Differenzierung von Knoten und Netzen in jedem Header mit enthalten sein muss.

2.3 Namensauflösende Dienste

Rechnernamen und Domänen

Je größer ein Netzwerkverbund ist, desto wichtiger ist es, dass Systeme von den Benutzern in einer nachvollziehbaren Art und Weise adressiert werden können. Darum kommt einer sauberen Nomenklatur (Namensgebungsregel) eine bedeutende Rolle zu.

Es fällt Benutzern und Administratoren deutlich leichter, sich im Netzwerk zurechtzufinden, wenn etwa der Druckserver der Hauptverwaltung in Berlin B-HV-DrSrv01 heißt, als wenn das Gerät als 24Bv27Ssr254 oder über seine IP-Adresse angesprochen werden muss. Hierfür sollten im gesamten Netzwerkverbund eindeutige Regeln verwendet werden, die möglichst in entsprechenden Pflichtenheften definiert und zur Information der Benutzer in öffentlich zugänglichen Dateien dokumentiert werden.

Wird das Netz größer und umfasst es möglicherweise sogar mehrere Länder oder Firmen eines Konsortiums, kommt als weiterer Namensbestandteil die Domäne hinzu. Domänen stellen für Gruppen von Rechnern und Benutzern zentrale Authentifizierungsinstanzen zur Verfügung. So kann etwa die Standortinformation BERLIN als Unterdomäne von FIRMA im Namen enthalten sein. Für den Druckserver der Hauptverwaltungsstelle ergäbe dies einen Namen wie HV-DrSrv01.Berlin.Firma.de.

Namensauflösende Protokolle

Der Wichtigkeit von Namen für Benutzer steht auf Netzwerkseite die Übermittlung von Informationen zwischen logischen Netzen gegenüber. Die Adressierung der Systeme erfolgt über eindeutige Adressen, die sich aus Netzwerkadresse und Knotenadresse zusammensetzen. Damit das Netzwerk in der Lage ist, auf Anforderung eines Benutzers Daten von Forschung-Wks215.Hamburg.Firma.de (Wks steht hier für Workstation) an Produktion-Filer02.Berlin.Firma.de zu übermitteln, muss das System den Namen einer Adresse zuordnen.

Dies kann generell auf mehrere Arten erfolgen. Die Arten der Namensauflösung sind einerseits vom eingesetzten Netzwerkprotokoll abhängig und betreffen andererseits die Betriebssystemumgebung. Die folgende Aufzählung gibt einen Überblick über die gängigen Arten der Namensauflösung:

- ✓ namensauflösende Broadcast-Anfragen
- ✓ namenspublizierende Broadcasts
- ✓ Namenszuordnungen über Dateien
- ✓ statische oder dynamische Datenbanken auf Servern

Dienste veröffentlichen

Neben Namen werden in Netzwerken auch Informationen über die Verfügbarkeit von Diensten benötigt. Auch diese Informationen werden über Mechanismen der Namensauflösung publiziert und sollen hier nicht getrennt betrachtet werden, da sie im Prinzip nur eine Sonderform der Namensauflösung darstellen.

Namensauflösende Broadcasts

Innerhalb kleiner Netzwerkverbunde ist es möglich, die Namensauflösung über Broadcasts zu regeln. Gibt ein Benutzer oder eine Anwendung einem System den Auftrag, eine Datenübermittlung mit einem anderen System zu initialisieren, sendet das System als Erstes eine Anfrage an alle anderen Systeme, in der der Empfänger aufgefordert wird, seine Adresse bekannt zu geben.

Diese Art der Namensauflösung belastet das Netzwerk, da die gesamte zur Verfügung stehende Bandbreite durch die Broadcasts nicht mehr für die eigentliche Datenübermittlung genutzt werden kann, und führt dazu, dass alle Netzwerkkarten stets mit der Auswertung von Paketen belastet werden, auch wenn sie in der Regel nicht für sie bestimmt sind. Broadcasts können nur innerhalb logischer und physikalischer Netze oder Subnetze verwendet werden, da diese nicht geroutet werden können, da sonst alle Netze von Broadcasts geflutet würden (sog. Broadcast-Sturm).

Broadcasts zur Namensauflösung werden von NetBIOS, einem proprietären namensauflösenden Dienst von Microsoft, verwendet. Sie unterstützen neben gerouteten Netzwerken auch keine hierarchischen Domänen-Konzepte und werden daher kaum noch eingesetzt.

Namenspublizierende Broadcasts

Ein weiterer Ansatz für die Namensauflösung in Netzen beruht darauf, dass Systeme, die bestimmte Dienste für das Netz bereitstellen, sogenannte Dienstpublikationen als Broadcast senden, wodurch das Netzwerk deutlich weniger belastet wird.

In einem Netzwerk werden in der Regel wenige Server von vielen Arbeitsplatzrechnern angesprochen. Dass Arbeitsplatzrechner sich gegenseitig ansprechen, ist eher die Ausnahme und in den meisten Fällen auch gar nicht wünschenswert. (Dies erschwert beispielsweise die Verwaltung einer zentralen Backup-Struktur, bei der Daten nur auf den Servern gesichert werden.) Wenn die Arbeitsplatzrechner Broadcasts senden, um die Dienste der Server zu finden, so ist die Netzlast bedeutend höher, als wenn die Server in bestimmten Intervallen das Netz darüber informieren, welche Dienste wo im Netz verfügbar sind. Denn in den meisten Netzwerken gibt es deutlich mehr Arbeitsplatzrechner als Server.

Ein System, das einen bestimmten Dienst benötigt, kann nun entweder direkt auf die Information zurückgreifen oder es fragt bei einem dafür dedizierten Server nach, welcher Dienst von welchem System angeboten wird. So können Dienstpublikationslisten zwischen Routern ausgetauscht werden und so ohne zusätzliche Netzwerkbelaustung durch Broadcasts Dienste in entfernten Netzen erreicht werden.

Die IPX/SPX-Protokollfamilie von Novell verwendete das Service Advertisement Protocol (SAP = Dienstveröffentlichungsprotokoll), um die Verfügbarkeit von Diensten im Netzwerk zu publizieren. Kennt ein Client noch keine Adresse eines Servers für einen benötigten Dienst, sendet er einen GNS-Request als Broadcast (Get Nearest Server). Dieser wird dann entweder von einem entsprechenden Server oder von einem Router mit der entsprechenden Information beantwortet.

Da die Anzahl der SAPs eine deutliche Netzwerklast generieren kann (sie werden standardmäßig alle 60 Sekunden gesendet), belasteten IPX/SPX das Netz erheblich. Dies ist neben der fehlenden Internetfähigkeit einer der Hauptgründe dafür, dass IPX/SPX nicht mehr verwendet wird.

Namenszuordnungen über Dateien

Eine weitere Möglichkeit der Zuordnung von Rechner-Namen oder Diensten zu Adressen besteht in der Verwendung vorkonfigurierter Dateien, die entsprechende Einträge enthalten. Durch die lokale Verfügbarkeit von Netzwerkinformationen wird die Bandbreite deutlich entlastet, aber es werden andererseits erhebliche manuelle Wartungsarbeiten für das administrative Personal fällig. Daher bietet sich die Arbeit mit Zuordnungsdateien nur dann an, wenn etwa einzelne entfernte Ressourcen in einer gerouteten Umgebung angesprochen werden sollen, in der lokale Rechner-Namen über Broadcasts aufgelöst werden können. Ein weiterer Einsatzbereich von Dateien zur Namenszuordnung ergibt sich, wenn Dienste wie DNS (Domain Name System) verwendet werden, die keine Broadcasts unterstützen.

Die Textdateien **Hosts** und **LMHosts**

Die Informationen werden als Adress-Namenspaare in Textdateien festgehalten und können vom System nur ausgewertet werden, wenn sie an bestimmten Orten im Dateisystem unter einem festen Namen gespeichert sind. Dieser Name ist für NetBIOS-Informationen *LMHosts* und für DNS-Informationen *Hosts*. Der Speicherort ist betriebssystemabhängig. Bei aktuellen Microsoft-Betriebssystemen und UNIX-Systemen ist dies in der Regel das Verzeichnis *etc/*. Bei der Größe aktueller Netzwerke haben diese Dateien stark an Bedeutung verloren und werden nur in Ausnahmefällen verwendet. Server übernehmen an zentraler Stelle komplett die dynamische Verwaltung der Daten für das gesamte Netzwerk.

Alle NetBIOS-Namensdienste haben durch fehlende IPv6-Unterstützung stark an Bedeutung verloren.

Statische oder dynamische Datenbanken auf Servern

In großen Netzwerken lassen sich die Informationen über Namens-Adress-Paare nur dann verwalten, wenn diese an zentraler Stelle für das gesamte Netzwerk bereitgestellt werden. Diese Datenbanken können entweder dynamisch von den Betriebssystemen oder weiteren Netzwerkdiensten aktualisiert werden oder sie müssen als statische Einträge von Serveroperatoren gepflegt werden.

Domain Name System (DNS)

Das weltweit am weitesten verbreitete System zur Auflösung von Namens-Adress-Paaren ist das **Domain Name System**. DNS-Server unterstützen dabei ein hierarchisches Namenssystem, das auf Namensräumen mit Domänen und Unterdomänen basiert.

Im Beispiel

Server3.buchhaltung.herdt.de

steht der Rechner *server3* in der Unterdomäne *buchhaltung* der Domäne *herdt* im Namensraum *DE*. Dieser Namensraum wird auch als „Top-Level-Domain“ bezeichnet.

Adressen in DNS können entweder für lokale Systeme genutzt werden oder im Internet eingebunden sein und so zur weltweiten Adressauflösung verwendet werden. Im Internet sind unterhalb des Stammes ROOT (der bei DNS-Namen durch einen finalen Punkt gekennzeichnet ist) die Namensräume von Staaten und Organisationen angelegt. Diese werden von InterNIC (International Network Information Center), der internationalen Verwaltung für das Internet, oder den nationalen Unterorganisationen (für Deutschland DeNIC; genauer: für alle Domains mit der Länderendung .de) verwaltet. Bei diesen – oder stellvertretend bei Internetseviceproviders – können sich dann Firmen oder auch Privatpersonen einen Namensraum zuweisen lassen, dessen Verwaltung ihnen dann selbst obliegt.

DNS basiert ursprünglich auf einer statischen Adressdatenbank, in der Zonen für bestimmte Namensräume eingerichtet werden. Diese enthalten untergeordnete Einträge für Rechnernamen, Dienste und Unterdomänen. Insgesamt gibt es etwa 20 unterstützte Eintragstypen. Neben Namen können z. B. auch Diensteinträge (SRV) verwendet werden, die angeben, welche Server bestimmte Dienste für das Netz bereitstellen.

Ein weiteres Merkmal von DNS ist, dass die Datenbank an weitere Server repliziert werden kann. Somit kann in Netzen mit mehreren Standorten die Namensauflösung lokal erfolgen, und WAN-Verbindungen werden entlastet. Allerdings ist es in den meisten Implementierungen von DNS nicht möglich, an den Replikaten Änderungen vorzunehmen. Diese Replikate (sog. sekundäre Zonen) sind schreibgeschützte Kopien der originalen, aktiven Datenbank (der primären Zone). Es handelt sich hierbei um eine Master/Slave-Konfiguration.

Aktuelle Implementierungen des DNS-Serverdienstes erlauben darüber hinaus die Errichtung von Zonen im Multi-Master-Modell, bei denen mehrere aktive DNS-Server die Konfigurationsinformationen zu einer einzelnen Zone gegenseitig aktualisieren können und Änderungen der Zone auf jedem beliebigen beteiligten Server erfolgen können.

Dynamisches DNS (D-DNS)

Zwar basiert DNS ursprünglich auf statischen Datenbanken, aktuelle Implementierungen unterstützen aber auch dynamische Einträge. Zusätzlich kann ein dynamischer DNS-Server von einem DHCP-Server Informationen über die dynamische Vergabe von Adressen an Clients erhalten. Damit wird der Verwaltungsaufwand von DNS deutlich verringert. D-DNS wird beispielsweise von Microsoft-Betriebssystemen ab Windows 2000 oder den aktuellen Linux-Versionen unterstützt.

Einer der Vorteile von dynamischem DNS ist dabei, dass die Daten nicht über eine Datenbankdatei repliziert werden müssen, sondern in einer Datenbank mit Einzelattributreplikation verwaltet werden. Dadurch ist die Belastung des Netzwerkes für die DNS-Replikation deutlich reduziert.

Domain Name System Security Extensions (DNSSEC)

Mit DNSSEC werden die Authentizität und Integrität von Antworten auf DNS-Abfragen gesichert. Übermittelte DNS-Zonendaten werden überprüft, ob sie vom erwarteten, vertrauenswürdigen Absender stammen und ob sie inhaltlich identisch sind mit den Daten, die der Ersteller der Zone autorisiert hat. Zur Erfüllung dieser Aufgaben kommen asymmetrische Verschlüsselungstechniken und Zertifikate zum Einsatz.

Asymmetrische Verschlüsselung bedeutet, dass zwei unterschiedliche Schlüssel verwendet werden: ein privater Schlüssel des Eigentümers, der für die Verschlüsselung oder Echtheitsbestätigung (im Fall von DNSSEC) verwendet wird, und ein zweiter (öffentlicher) Schlüssel, mit dem die Echtheit bestätigt werden kann oder die Daten entschlüsselt werden können. Im Gegensatz dazu stehen symmetrische Verschlüsselungen, bei denen beide Parts den identischen Schlüssel für Ver- und Entschlüsselung verwenden.

Windows Internet Name Service (WINS)

Der Windows Internet Name Service von Microsoft dient dazu, NetBIOS-Namen und -Dienste in einem lokalen Netzwerk für Clients verfügbar zu machen, indem die Namens-Adress-Zuordnung in einer zentralen Datenbank gehalten wird. Jeder WINS-Client ist einem primären WINS-Server zugeordnet, dem er beim Start des Netzwerkadapters seine IP-Adresse, seinen Systemnamen sowie eine Vielzahl weiterer NetBIOS-Informationen mitteilt. Allerdings unterstützt WINS im Gegensatz zu DNS keine hierarchischen Konzepte und ist damit für den Einsatz in sehr großen Systemen nur bedingt geeignet.

WINS wird schon länger als veraltet angesehen. Microsoft empfiehlt – sofern möglich – eine Umstellung auf DNS. Mit der Entdeckung sicherheitsrelevanter Lücken in der WINS-Implementierung aktueller Windows-Versionen im Juni 2017 und der Tatsache, dass Microsoft diese Lücke nicht patchen wird, verbietet sich ein Einsatz von WINS in Produktivumgebungen.

2.4 Protokolle aus dem Weitverkehrsbereich

Übersicht

Im Weitverkehrsbereich unterliegt Netzwerkkommunikation grundsätzlich anderen Regeln als in lokalen Netzwerken. Dies hat vor allem damit zu tun, dass im Weitverkehrsbereich hauptsächlich verbindungsorientierte Kommunikation auftritt, die sich deutlich von der auf dem Medium konkurrierenden Kommunikation in lokalen Netzen unterscheidet. Entsprechend bestehen auch andere Anforderungen an WAN-Protokolle als an LAN-Protokolle.

Auf logischer Ebene dagegen ähnelt die Kommunikation im WAN der in komplexen LAN-Umgebungen. Auch im WAN muss üblicherweise zwischen diversen Netzen vermittelt werden und entsprechend kommen hier auch bekannte Netzwerkprotokolle wie IP und IPX (bis etwa 2010) zum Einsatz.

Im Folgenden werden WAN-Dienste kurz vorgestellt. Hier soll nur ein genereller Überblick gegeben werden. Eine Auflistung der einzelnen Protokolle, die diverse Aufgaben im Hintergrund der Dienste erfüllen, würde den Rahmen dieser Übersicht sprengen.

Gängige WAN-Protokoll-Familien

Protokoll	Beschreibung
Asynchronous Transfer Mode (ATM)	Bei ATM handelt es sich um ein Hochgeschwindigkeits-Datenübertragungsverfahren, das im LAN-Backbone-Bereich, in Telefonnetzen und im Internet sowie bei dedizierten Standortanbindungen zum Einsatz kommt. Im ATM-Netzwerk wird eine virtuelle Verbindung zwischen Endsystemen aufgebaut, über die in einem konstanten Strom von 53 Byte großen Zellen Daten verschiedener Anwendungen übertragen werden können. Dabei kommen unterschiedliche Übertragungsgeschwindigkeiten zum Einsatz.
Frame Relay	Frame Relay wurde als Zubringerdienst für ISDN entwickelt und ist ebenfalls ein Hochgeschwindigkeits-Datenübertragungsverfahren im WAN-Bereich. Es ist ein Packet-Switching-Verfahren, d. h., Daten werden entsprechend ihrer Zieladresse über virtuelle Leitungen vermittelt. Die Größe der übertragenen Daten ist dabei unterschiedlich.
Integrated Services Digital Network (ISDN)	Der gängige digitale Telefondienst ISDN spielt auch in Netzwerken eine bedeutende Rolle für Weitverkehrsverbindungen. Hier kommen neben Wählleitungen auch Standleitungen infrage. Im Gegensatz zu den zuvor genannten Diensten werden nur geringe Geschwindigkeiten unterstützt. ISDN war lange Zeit der am weitesten verbreitete WAN-Dienst. Inzwischen ist er weitgehend durch DSL verdrängt worden. Die Daten, die über ISDN übertragen werden, müssen allerdings in der Regel gekapselt werden. Diese Kapselung kann mittels unterschiedlicher Protokolle wie etwa PPP, L2TP oder PPTP erfolgen.
Digital Subscriber Line (DSL)	DSL erfreut sich zunehmender Beliebtheit. Dies ist vor allem auf die wachsende Beliebtheit des Internets im Heimbereich zurückzuführen. Hier kommt vor allem das Asymetric DSL (ADSL) zum Einsatz, bei dem eine hohe Download-Rate einer niedrigen Upload-Rate gegenüber steht. Bei der Anbindung von Firmennetzen dagegen kommt vor allem symmetrisches DSL (SDSL) zum Einsatz. Neuere Technologien mit höheren Übertragungsraten sind unter den Kürzeln ADSL2+, HDSL oder VHDSL bekannt. Einer der Hauptgründe für die weite Verbreitung von DSL-Verfahren ist, dass bestehende Vernetzungen für die Hochgeschwindigkeits-Datenübertragung genutzt werden können und damit die Kosten für den Umstieg relativ niedrig ausfallen können. Im Zusammenhang mit DSL kommt es häufig zu einer fehlerhaften Namensgebung, wenn von DSL-Modems die Rede ist. In Wirklichkeit handelt es sich bei einem DSL-Modem üblicherweise um eine ATM-Bridge.

2.5 Neue Protokolle an der Grenze zwischen WAN und LAN

Steigender Bandbreitenbedarf im LAN

Mit dem stetigen steigenden Bandbreitenbedarf in lokalen Netzwerken drängen immer mehr Techniken aus dem Weitverkehrsbereich in lokale Netze. Dies verursacht Probleme, da sich Kommunikation zwischen Netzen generell anders verhält als konkurrierende Kommunikation im LAN. Grund für den wachsenden Bandbreitenbedarf sind vor allem die immer größer werdenden Datenmengen, die für heutige Applikationen benötigt werden, und dabei besonders der Trend zu multimedialer Ausschmückung von Dokumenten. Beim Vergleich der Dateigröße eines reinen Textdokumentes mit einer PowerPoint-Folie wird deutlich, warum heute im Netzwerk Übertragungsgeschwindigkeiten von 10 Mbit/s oder auch 100 Mbit/s oft nicht mehr ausreichen.

Eine Vielzahl von Clients greift z. B. auf wenige Fileserver zu, was bei guter Anbindung (etwa mit Gigabit-Ethernet) für den Einzelnen ausreichend wäre. Da sich aber alle Beteiligten bei erhöhtem individuellen Bedarf die Bandbreite des Servers teilen müssen, kann am Server u. U. keine ausreichende Bandbreite gewährleistet werden.

LANE

Eine der Techniken, die heute zunehmend Einzug ins LAN gefunden hat, ist die ATM-LAN-Emulation (ATM-LANE). Dabei geht es um die Aufgabe, auf einem verbindungsorientierten Medium den quasi verbindungslosen Verkehr und die Namensauflösungsstrategien lokaler Netzwerke zu simulieren.

Die Umsetzung dieser Problematik erfordert vollkommen neue Netzwerkfunktionalitäten, die das LAN im ATM-Netz abbilden. Dazu gehören neue Servertechnologien wie etwa Broadcast-Emulatoren über ATM.

Steigender Adressbedarf

Ein weiteres Problem, das sowohl lokale Netze als auch den WAN-Bereich (und dabei besonders das Internet) betrifft, ist der stetig steigende Bedarf an gültigen IP-Adressen. Durch die Umstellung der Adressen von 32 Bit (IPv4) auf 128 Bit (IPv6) ist dieses Problem prinzipiell gelöst.

Allerdings ist nach wie vor der Einsatz von IPv6 im LAN mit Mehrkosten für neue Hardware (Router und Layer-3-Switches) verbunden. Da außerdem der Verwaltungsaufwand steigt und IPv4 intern nach wie vor funktioniert, wird in den meisten Netzwerken intern nach wie vor IPv4 eingesetzt. Für den internen Netzwerkbetrieb stehen mit den privaten Netzwerkadressen fast 17 Millionen Adressen bereit, die eine Adressierung aller Systeme ermöglichen. IPv6 bedingt seinerseits steigende Bandbreiten, denn der Header von IPv6 ist deutlich größer als der von IPv4.

An IPv6 führt kein Weg vorbei, auch wenn die Ablösung von IPv4 nach wie vor recht schleppend voranschreitet. Im August 2017 fanden etwa 20 % aller Zugriffe auf Google über IPv6 statt. Zu erwarten ist wohl, dass IPv4 und IPv6 häufig parallel eingesetzt werden, wie das in modernen Betriebssystemen unterstützt wird.

Sicherheitsbedarf

Da firmenkritische Daten für den Zugriff über Weitverkehrsverbindungen verfügbar gemacht werden und ein großer Teil der Korrespondenz über Mail stattfindet, kommt dem Thema der Sicherheit eine große Bedeutung zu.

Im Bereich der Zugangskontrolle über WAN-Verbindungen finden Authentifizierungsmechanismen wie etwa RADIUS (Remote Authentication Dial-In User Service) in Verbindung mit Zertifikaten und hardwarebasierten Einmal-Passwortgeneratoren Einsatz. Mit der schnellen Verbreitung von WLANs gewinnen die Verschlüsselung von Daten sowie die geschützte und gesicherte Übertragung an Einfluss. Verschlüsselungen sind durch eine Vielzahl von Faktoren – wie etwa Schlüssellängen, verwendete Algorithmen und Lebensdauer der Schlüssel – für den normalen Anwender meist schwer nachvollziehbar. Gleichzeitig werden auch die Angriffsmethoden immer ausgefeilter, was zu einer Art Wettrüsten zwischen angreifenden und abwehrenden Instanzen führt. Neben Firmenrechnern müssen auch Privatanwender der stetig wachsenden Problematik der Kriminalität im Netz begegnen, indem sie ihre Rechner mit aktueller Schutzsoftware ausstatten.

Der umfangreiche Bereich der Netzwerksicherheit kann in diesem Buch nur gestreift werden, doch sollte sich jeder der Brisanz des Themas bewusst sein und entsprechend handeln. Mails können verschlüsselt versendet werden, Einkäufe im Internet sollten nur über SSL-Verschlüsselung erledigt werden, Vorsicht ist bei Dateidownload und Mailanhängen geboten u.v.m. Diese Maßnahmen erhöhen die Sicherheit, eliminieren aber nicht vollständig die Gefahren. Weiterführende Informationen finden Sie u. a. im HERDT-Buch *Netzwerke – Sicherheit*.



Funkübertragung

In heutigen LANs kommt es vermehrt zum vermischten Einsatz von kabelbasierten Übertragungstechniken und kabellosem Netzwerkverkehr. Waren Richtfunkverfahren noch vor wenigen Jahren vor allem für die Vernetzung von Gebäuden im Einsatz, werden heutzutage oft Notebooks mit WLAN-Adaptoren ausgestattet, und auch Bluetooth findet eine immer stärkere Verbreitung. Zusätzlich werden zunehmend tragbare Computer, Tablets und Smartphones eingesetzt, die sich über die Mobiltelefonnetze mittels Hochgeschwindigkeitsverbindungen (z. B. UMTS, HSDPA, LTE) mit dem Internet oder Firmennetzwerken verbinden.

Da immer mehr mobile Geräte mit Computern synchronisiert werden sowie eine stetige Verfügbarkeit von Netzwerken (z. B. Internet) vom Benutzer mittlerweile als selbstverständlich angesehen wird, wird die Funkkommunikation nach und nach zum erwarteten Standard. Da die Frequenzbänder, die zur Datenübertragung verwendet werden können, beschränkt sind, kann es zu Konflikten zwischen Geräten kommen. In größeren Firmen können aus diesem Grund Funknetze überlastet sein, so dass sich Benutzer z. B. zu Hauptgeschäftszeiten nicht mehr einloggen können.

Ausblick

Die Implementierung von IP in lokalen Netzen oder DNS im Intranet ist genau genommen eine Portierung von Weitverkehrstechniken aus dem Internet in den Einsatzbereich lokaler Netze. Klassische, mittlerweile veraltete LAN-Techniken wie etwa NetBEUI oder NetBIOS, die für den Einsatz in kleinen Netzen deutlich effizienter waren, wurden verdrängt. Diese Tendenz – Einsatz eines Standards für alle Bereiche – wird sich in der Zukunft weiter verstärken.

3 Netzwerkmodelle

In diesem Kapitel erfahren Sie

- ✓ was Netzwerkmodelle sind
- ✓ wie Sie mit Netzwerkmodellen arbeiten können
- ✓ was das OSI-Modell, das DoD-Modell und das TCP/IP-Modell ist

Voraussetzungen

- ✓ Netzwerkgrundlagen

3.1 Überblick Netzwerkmodelle

Einleitung

Nehmen Sie an, jemand möchte über das Internet auf die HTML-Seite eines Hardwareherstellers zugreifen, um dort einen Treiber für seine Grafikkarte mittels FTP herunterzuladen. Das Betriebssystem des Downloadrechners unterscheidet sich deutlich von dem des Hardwareherstellers. Vielleicht sind auch noch ein altes Modem und ein Webbrower eines anderen Herstellers im Spiel.

Im Internet wird seine Anfrage über ATM-Leitungen, Frame-Relay-Verbindungen oder ISDN-Leitungen bis zum Rechner des Herstellers übermittelt, wobei unter Umständen diverse Protokolle zum Einsatz kommen.

Aufgrund der Vielzahl an beteiligten Hard- und Softwarekomponenten wird eine klare Strukturierung der Kommunikation über das Netzwerk benötigt. Nur so kann gewährleistet sein, dass die diversen Produkte an den Schnittstellen zwischen Netzhardware, Kommunikationsprotokollen und Software fehlerfrei miteinander kommunizieren.

Schichten

Um die Schnittstellen zwischen Komponenten der Kommunikation zu vereinheitlichen, wird ein theoretisches Modell verwendet, das die einzelnen Komponenten und Aufgaben bestimmten Schichten zuordnet. Diese Schichten weisen standardisierte Schnittstellen zu den benachbarten Schichten auf. Im Einzelfall können bestimmte Pakete von Schichten zusammengefasst werden, wenn es z. B. nur um Hardware geht oder nur Softwareanwendungen betroffen sind. Es ist jedoch aus Kompatibilitätsgründen notwendig, ein generelles Modell zur Standardisierung zu verwenden.

Heute werden vor allem drei Modelle zur Darstellung von Netzwerkkommunikation verwendet. Sie unterscheiden sich vor allem durch die Genauigkeit, mit der dabei die einzelnen Schichten definiert sind. Außerdem gibt es Unterschiede in der Generalisierung der Modelle. Dabei gilt: Je allgemein gültiger ein Modell sein soll, desto exakter muss jede einzelne Funktion beschrieben werden, die auf einer Schicht liegt.

Die drei gängigsten Modelle sind:

- ✓ das ISO/OSI-Modell
- ✓ das DoD-Modell
- ✓ das TCP/IP-Modell

3.2 Das OSI-Modell

Geschichte

Das OSI-Modell (auch ISO/OSI-Modell) wurde 1984 von der International Organization for Standardization (ISO), einem Zusammenschluss von Normungsorganisationen, entwickelt, um Kommunikationsabläufe in Computernetzen in einem normierenden, theoretischen Modell (auch Referenzmodell genannt) abzubilden. Der Modellname OSI (Open Systems Interconnection) weist auf den Ansatz hin, mit dem Modell die Kommunikation über unterschiedlichste technische Systeme zu ermöglichen.

Beschreibung

Das OSI-Modell umfasst sieben Schichten, die von Informationen auf dem Weg zwischen zwei Systemen zweimal durchlaufen werden müssen – auf Senderseite von der obersten bis zur untersten Schicht, auf Empfängerseite in umgekehrter Reihenfolge. Dies lässt sich mit am einfachsten mittels eines Modells aus der menschlichen Kommunikation darstellen.

Im Folgenden wird sehr detailliert auf die einzelnen Komponenten des OSI-Modells eingegangen. Je besser Sie verstehen, was auf den einzelnen Schichten passiert, umso leichter fällt es Ihnen, in der Praxis mögliche Ursachen für Probleme in Netzen zu identifizieren. Auch wenn es sich bei dem OSI-Modell um einen theoretischen Ansatz handelt, sollten Sie es so weit verinnerlichen, dass Sie beliebige Protokolle und Dienste sofort ihren Schichten zuordnen können.



Beispieldaten

Angenommen, ein Mitarbeiter A einer Firma befindet sich im Außendienst. Er muss einem Kunden Informationen zu einem Produkt geben, die sich in einer Unterlage auf seinem Schreibtisch befinden. Also ruft er seinen Kollegen B in der Hauptstelle an, der ihm die Informationen vorliest. Anschließend kann Mitarbeiter A mit dem Kundengespräch fortfahren.

Was aber sind die einzelnen Schritte, die nötig sind, damit der Außendienstmitarbeiter die Information erhält?

Bitübertragungsschicht

Erst einmal muss A auf ein Medium zugreifen, das auch B zur Verfügung steht. In diesem Fall ist dies das Telefon. Würde A stattdessen zu einem Funkgerät greifen, würde die Kommunikationsaufnahme scheitern. Es werden also auf physikalischer Ebene kompatible Medien benötigt.

Sicherungsschicht

Nun muss A die richtige Telefonnummer wählen, um im Netz der Telekom mit dem korrekten Hausanschluss verbunden zu werden. Nur wenn die richtige NTBA ein Signal erhält, kann auch eine Verbindung stattfinden. Auch auf der Verbindungsschicht muss also eine korrekte Adressierung stattfinden.

Vermittlungsschicht

Innerhalb des Firmennetzes wird über die Telefonanlage eine logische Unterteilung vorgenommen. So kann z. B. mit der 1xx die erste Etage und mit der 2xx die zweite Etage gekennzeichnet werden. Auf der Netzwerkschicht muss entsprechend der richtige Anschluss angesprochen werden.

Transportschicht

Die Informationen von A müssen für B in verständlicher Form ankommen. Dazu müssen beide dieselbe Sprache verstehen und es müssen bestimmte Konventionen eingehalten werden. Spricht A zu leise oder zu schnell oder knackt es in der Leitung, muss B nachfragen, was gemeint war. Auf der Transportschicht wird sichergestellt, dass alle Informationen korrekt ankommen und von beiden Seiten in derselben Art und Weise verarbeitet werden können.

Sitzungsschicht

Wenn A zu sprechen beginnt, ohne dass B den Hörer abgenommen hat, wird die Kommunikation nicht erfolgreich sein. Erst wenn Kommunikationsaufbau (und evtl. -kontrolle durch eine Begrüßung) stattgefunden haben, kann A eine Handlungsanweisung an B weiterleiten. A muss sich bei B identifizieren. B wird nicht jedem beliebigen Anrufer Zugriff auf Informationen von As Schreibtisch gewähren. Auf der Sitzungsschicht werden Regeln des Zugriffs und der Kommunikationsaufbau überprüft.

Darstellungsschicht

A kann in diesem Beispiel die Informationen nicht selbst lesen. Wenn B die Information liest, kann A sie noch nicht verwenden. Erst indem B die Information laut wiedergibt, kann sie A erreichen. Die Information muss für den Transport über das Telefon aufbereitet werden. Auf der Präsentationsschicht erfolgt quasi eine Umleitung von der nicht netzwerkauglichen Verarbeitungsform „Lesen“ zur für den Transport geeigneten Verarbeitungsform „Sprechen“.

Anwendungsschicht

Und damit schließlich der eigentliche Zugriff auf die Informationen erfolgen kann, muss B wissen, in welcher Unterlage die benötigten Daten stehen, er muss seine Lesebrille holen, die Unterlage öffnen usw. Erst wenn dies erfolgt ist, kann er mit dem eigentlichen Lesen der Informationen beginnen. Auf der Anwendungsschicht wird also das Umfeld für die Verarbeitungsform „Lesen“ vorbereitet.

Anwendung

Die Aktion des Lesens als solche ist nicht mehr Bestandteil des Kommunikationsmodells, sie könnte auch ohne Telefonat stattfinden und spielt deswegen hier keine Rolle. Entsprechend wird sie auch nicht im Modell berücksichtigt.

Das OSI-Modell

In der Tabelle finden Sie die Schichten dieses Beispiels der Nomenklatur des OSI-Modells gegenübergestellt:

	Beispiel	OSI-Modell (Deutsch)	OSI-Modell (Englisch)
Schicht 7	Informationsauswahl	Anwendungsschicht	Application Layer
Schicht 6	Lesen/Sprechen	Darstellungsschicht	Presentation Layer
Schicht 5	Begrüßung/Identifizierung	Sitzungsschicht	Session Layer
Schicht 4	Verständniskontrolle	Transportschicht	Transport Layer
Schicht 3	Interne Durchwahl	Vermittlungsschicht	Network Layer
Schicht 2	Anschlussnummer	Sicherungsschicht	Data Link Layer
Schicht 1	Auswahl des Mediums	Bitübertragungsschicht	Physical Layer

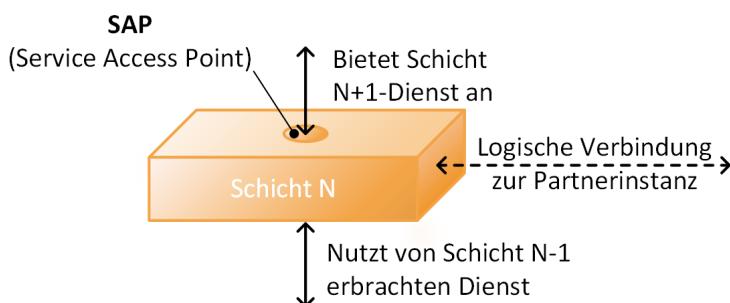


Merken Sie sich die englischen Begriffe, denn in der Fachliteratur werden auf Deutsch unterschiedliche Übersetzungen der Begriffe verwendet. Die englischen Begriffe werden in der Regel dort auch angegeben.

Funktionsprinzip des OSI-Referenz-Modells

Die Funktionsweise des OSI-Referenz-Modells entspricht der Kommunikation zwischen den einzelnen OSI-Schichten.

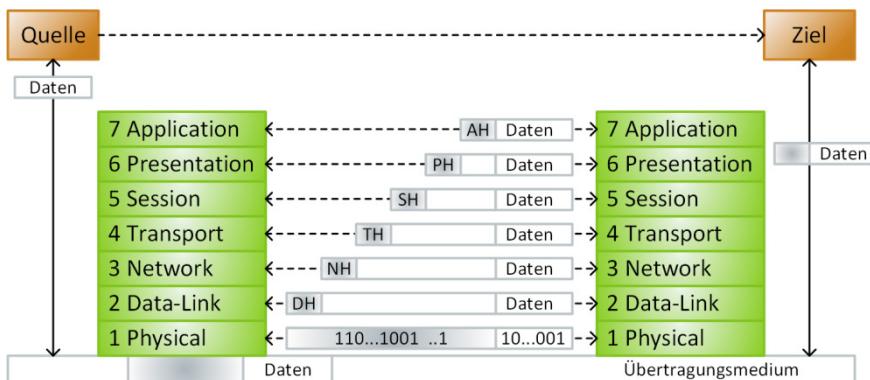
- ✓ Über eine definierte Schnittstelle, den sogenannten **Service Access Point (SAP)**, stellt jede Schicht der nächsthöheren eine Gruppe von Methoden (Dienste) zur Verfügung. Diese Dienste ermöglichen den Zugriff auf die Datenstrukturen.
- ✓ Mit steigender Schicht nimmt die Komplexität der Aufgaben zu. Die Funktionalität jeder Schicht baut auf die Standards der darunter liegenden auf.
- ✓ Bei Datenverkehr agieren die einzelnen Schichten des Senders/Empfängers so, als ob sie mit der jeweiligen Schicht des Kommunikationspartners direkt kommunizieren würden (horizontale Kommunikation über eine logische Verbindung). Tatsächlich aber durchlaufen alle Daten immer alle Schichten (vertikale Kommunikation): beim Sender von Schicht 7 abwärts nach Schicht 1 auf das Übertragungsmedium und beim Empfänger dann vom Übertragungsmedium zur Schicht 1 aufwärts zu Schicht 7.
- ✓ Es interagieren immer nur benachbarte Schichten, einzelne Schichten können nicht übersprungen werden.



Kommunikation zwischen Schichten

Die zwischen den Schichten weitergereichten Daten werden als Protokolldateneinheiten (**PDU** für **Protocol Data Unit**) bezeichnet. Sie setzen sich zusammen aus einem Programmkopf (**Header**), in dem sich Protokoll-Kontrollinformationen (**PCI** für **Protocol Control Information**) der jeweiligen Schicht befinden, sowie den eigentlichen Nutzdaten (**SDU** für **Service Data Unit**).

Beim Weiterreichen stellt jede einzelne Schicht des Senders den erhaltenen Daten einen Header voran, der von der entsprechenden Schicht auf der Seite des Empfängers interpretiert und wieder entfernt wird.



Schichtenmodell

Vorteile des Schichtenkonzepts

Obwohl das Schichtenmodell sehr abstrakt ist, ergeben sich daraus für Hersteller und Entwickler etliche Vorteile.

Unabhängigkeit der einzelnen Schichten voneinander

Die eigentliche Umsetzung des Inhalts einer Schicht ist unerheblich. Wichtig sind nur die Dienste, die an den Schnittstellen zur Verfügung stehen. So können einzelne Schichten unabhängig voneinander entwickelt werden.

Flexibilität

Änderungen an einzelnen Schichten wirken sich nicht auf benachbarte Schichten aus, solange die definierten Schnittstellen erhalten bleiben.

Physikalische Trennung der Schichten

Jede Schicht kann in der für ihre Aufgabenstellung günstigsten Technik entwickelt werden, als Hard- oder Softwarelösung.

Vereinfachte Standardisierung

Die genaue Festlegung der Funktion einer Schicht erlaubt es, Standardschichten zu entwickeln.

Einfache Wartung und Implementation

Die Entwicklung komplexer Systeme wird durch die Modularität mit klar definierten Schnittstellen vereinfacht.

Nachteil

Der Nachteil dieses Schichtenkonzepts besteht in dem immensen Aufwand an Steuerinformationen (jede Schicht schreibt ihren eigenen Header), wodurch die Übertragung der Daten länger dauert.

3.3 Sieben Schichten des OSI-Modells

1. Bitübertragungsschicht (Physical Layer)

Die Bitübertragungsschicht definiert alles, was für den direkten Übertrag und Empfang einzelner Bits auf bzw. von einem Medium notwendig ist.

Im **mechanischen** Teil werden die Verbindungselemente (Stecker, Art des Übertragungsmediums) spezifiziert.

Der **elektrische** Bereich definiert z. B. die zu verwendenden Spannungspegel, den Widerstand der Kabel, die Zeitspanne von Signalelementen und Spannungswechseln, die zu verwendenden Codierungsverfahren (wie ein Bit dargestellt wird). Aus diesen Spezifikationen ergibt sich die maximal erreichbare Datenübertragungsrate.

Die **funktionalen** Spezifikationen befassen sich mit der Funktion von Verbindungen, wie z. B. der Unterscheidung Datenleitung - Steuerungsleitung, der Taktgebung oder der Pin-Belegung.

Die **verfahrenstechnischen** Spezifikationen definieren z. B. den Übertragungsmodus (Halb-, Vollduplex) oder wie lange welcher Spannungspegel anliegen muss, um eine 1 bzw. 0 zu definieren.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

2. Sicherungsschicht (Data Link Layer)

Die Sicherungsschicht bereitet die Daten der Vermittlungsschicht in sogenannte Frames (Datenrahmen definierter Größe) auf und reicht sie an die Bitübertragungsschicht weiter. Dazu werden größere Datenpakete gegebenenfalls in kleinere aufgelöst. Das Zerlegen von Frames in einzelne Bits für die Bitübertragungsschicht bzw. das Zusammensetzen einzelner Bits zu Frames (aus Schicht 1) gehört ebenfalls zu den Aufgaben der Sicherungsschicht.

Ein einfacher Frame besteht aus einem **Header** (den Adressen von Empfänger und Sender sowie Steuerinformationen), den eigentlichen **Daten** sowie einem angehängten **Trailer** (FCS für Frame Check Sequence), um zu erkennen, ob die Daten fehlerfrei übertragen wurden. Für die Berechnung einer Prüfsumme wird in der Regel der CRC-Algorithmus (Cyclic Redundancy Check) verwendet.

Anhand der FCS kann der Empfänger beurteilen, ob die Daten während des Transports verändert wurden. Protokolle der Sicherungsschicht stellen durch Fehlerüberwachungsmethoden sicher, dass beschädigte oder bei der Übertragung verloren gegangene Rahmen erneut gesendet werden.

Letzte Aufgabe der Sicherungsschicht ist die **Flusssteuerung**. Hierbei geht es darum, einen schnellen Sender daran zu hindern, einen langsamen Empfänger mit Daten zu überschwemmen.

Fehlerüberwachung und Flusssteuerung werden häufig so realisiert, dass der Sender wartet, bis er eine Bestätigung des gesendeten Rahmens erhält. Nicht bestätigte Frames werden erneut gesendet.



3. Vermittlungsschicht (Network Layer)

Die Vermittlungsschicht legt den optimalen Verbindungsweg im Netz fest. Sie realisiert eine Ende-zu-Ende-Verbindung zwischen den beiden kommunizierenden Stationen über verschiedene Netzwerkknoten hinweg.

Hierzu gehören die Adressierung und Adressinterpretation, die Festlegung des Übertragungswegs (Routing) und die Kopplung verschiedener Transportnetze.

Wenn Router die ankommenden Pakete nicht in der gewünschten Größe übertragen können, erfolgt in dieser Schicht eine weitere Fragmentierung der Datenpakete.



4. Transportschicht (Transport Layer)

Die Transportschicht realisiert eine „feste“ Verbindung zwischen zwei Prozessen und liefert den darüber liegenden Schichten einen transparenten Datenkanal.

Die Transportschicht vermittelt zwischen den anwendungsorientierten (7.–5.) und den transportorientierten Schichten (3.–1.) und bereitet die Daten entsprechend auf. Da verschiedene Protokolle unterschiedlich große Daten-Pakete für die Datenübertragung benötigen, werden die Daten in der Transportschicht in entsprechende Pakete unterteilt und durchnummeriert. Der Empfang eines Pakets wird bestätigt.



Hier erfolgt eine weitere Flusskontrolle und Fehlerbehandlung. Es wird überprüft, ob die Pakete vollständig, korrekt, in der richtigen Reihenfolge und ohne Duplikate ankommen.

5. Sitzungsschicht (Session Layer)

Die Sitzungsschicht sorgt für die Prozesskommunikation zwischen den Systemen. Sie ist zuständig für den Aufbau einer Sitzung, die Verwendung und den Abbau von Verbindungen zwischen Netzwerkressourcen. Hierzu gehören die Namensauflösung von Netzwerkressourcen sowie das Aushandeln von Flusskontroll-Parametern (wer wann wie lange wie viele Daten auf einmal senden darf usw.). Sie stellt einen universalen Transportservice (Prozess-zu-Prozess-Verbindung) dar.

Zur Sitzungsverwaltung gehört auch die Synchronisation. Bei kurzfristigen Netzausfällen muss es möglich sein, fehlende Daten erneut zu übertragen. Um dies zu gewährleisten, werden entsprechende Prüfpunkte in die Daten eingefügt. Reißt der Datenstrom ab, müssen nur die Daten nach dem letzten übertragenen Prüfpunkt erneut übertragen werden.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

6. Darstellungsschicht (Presentation Layer)

Die Darstellungsschicht konvertiert die Daten in ein allgemeines, vereinbartes und für die beteiligten Systeme verständliches Datenformat (ASN.1 Abstract Syntax Notation One). Das ist nötig, da sich die interne Darstellung von Daten (z. B. in den Zeichencodes ASCII, ANSI, EBCDIC) je nach eingesetztem System unterscheidet.

Weitere Aufgaben dieser Schicht sind die Protokollumwandlung, die Datenverschlüsselung sowie die Datenkomprimierung zur Reduzierung der zu übertragenden Datenmenge.

Der sogenannte Redirector, der Ein-/Auszabeoperationen zwischen lokalen Festplatten und Netzwerkressourcen verteilt, ist ebenfalls hier angesiedelt.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

7. Anwendungsschicht (Application Layer)

Die Anwendungs-Schicht stellt die Schnittstelle zwischen Anwendungen (Programme und Benutzer) und Netzwerkdiensten dar. Hier sind Netzwerkzugang, Flusskontrolle und Fehlerbehebung sowie Anwendungsdienste (Services) angesiedelt, z. B. Dateitransfer, Datenbankzugriffe, E-Mail oder Freigaben. In dieser Schicht werden Funktionen für die Anwendungen zur Verfügung gestellt; die Anwendungen selbst gehören nicht zur Schicht.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

Mehrfache Kontrolle

Verschiedene Mechanismen, wie z. B. Fehler- oder Flusskontrolle sind mehrfach auf verschiedenen Ebenen aufgeführt. Jede Schicht regelt dabei "ihren" Teil der Kontrolle. Erst wenn diese Schicht nicht mehr weiter kommt, wird eine entsprechende Meldung nach "oben" zur nächsten Schicht gegeben. Dort setzen dann andere Mechanismen an, um das Problem zu beseitigen.

Merksätze



Folgende zwei Sätze erleichtern es, sich die Reihenfolge der Schichten anhand der englischen Bezeichnung einzuprägen:

Von Schicht 1 bis 7:

Please Do Not Throw Sausage Pizza Away

Von Schicht 7 bis 1:

All People Seem To Need Data Processing

Überblick über die Aufgaben

So weit zur reinen Darstellung des OSI-Modells. Die folgende Tabelle gibt eine kurze Zusammenfassung:

Nr.	OSI-Schicht	Aufgaben
7	Application	Anwendungen
6	Presentation	Datenformate, Darstellungs-, Verschlüsselungsinformationen
5	Session	Verbindungen, Flusskontrolle (Kommunikationsparameter), Datenfluss-Prüfpunkte
4	Transport	Pakete, Flusskontrolle, Fehlerbehandlung und Empfangsbestätigung
3	Network	Adressinformationen, Routing
2	Data Link	Frames, Fehlerbehandlung
1	Physical	Definition physikalischer Werte

Schichtengruppen

Häufig werden die Schichten in zwei Gruppen von generell unterschiedlichem Charakter zusammengefasst.

Schichten-gruppe	Nr.	OSI-Schicht	Beispiele		
			Anwendungsnahe Protokolle	Systemspezifische Protokolle	Netzwerk-Protokolle
Anwendungs-schichten	7	Application	Dateübertragung, Post, WWW		
	6	Presentation	FTP, SMTP, HTTP		
	5	Session		SMB, WinSocket	
Netzwerk-schichten	4	Transport			TCP, UDP, SPX
	3	Network			IP, IPX, ARP
	2	Data Link			MAC
	1	Physical			ETH0, TokenRing

Einerseits befassen sich die Schichten 1 bis 4 mit den netzwerkspezifischen Aufgaben der Kommunikation. Andererseits werden in den Schichten 5 bis 7 betriebssystemspezifische Dienste, Datenaufbereitungen und Anwendungsunterstützungen bereitgestellt.

Unterschichten der Datensicherungsschicht

In der Praxis hat sich gezeigt, dass es einer weiteren theoretischen Unterteilung der Datensicherungsschicht (Data Link Layer) bedarf, da sie auf zwei sehr unterschiedliche Weisen Funktionen übernimmt.

Unterschicht der Sicherungsschicht	Aufgaben
Logical Link Control (LLC)	SAPs Die LLC stellt der MAC-Unterschicht SAPs zur Verfügung, sodass die Daten von der MAC-Unterschicht an die korrekten Dienste in Schicht 3 gesendet werden können (z. B. wird ein ICMP Packet anders verarbeitet als ein ARP-Paket).
	Trennung von Netz und Protokoll Die LLC ermöglicht es, die Protokolle der höheren Schichten unabhängig von der Art des Netzwerkes zu betreiben. So kann z. B. IP durch IPX ersetzt werden oder Eth0 durch TokenRing, ohne dass dies sich jeweils beeinflusst.
	Flusskontrolle Kontrolliert die Geschwindigkeit, mit der die oberen Schichten Daten erreichen. So wird vermieden, dass vom Netzwerk Daten einen Host überfluten.
	Sequenzierung der Frames In der LLC werden die Frames, die von der Karte empfangen werden, wieder in die richtige Reihenfolge gebracht.
Media Access Control (MAC)	Physikalische Adressierung Über die MAC-Adresse wird jede Netzwerkkarte weltweit eindeutig identifiziert. Die MAC-Adresse setzt sich aus der Unique ID (UID) des Herstellers und der herstellerspezifischen Adresse zusammen. Beide sind jeweils sechsstellige, hexadezimale Werte. Wenn ein Frame auf der physikalischen Schicht empfangen wird, überprüft die MAC-Schicht, ob er für die Karte bestimmt ist, und leitet gegebenenfalls die Verarbeitung ein.
	Framing Die Pakete, die von der Netzwerkschicht verarbeitet werden, werden als Frames über das Netzwerk transportiert. Hierzu verwaltet sie Header und Trailer und führt eine Fehlerprüfung durch.

Das OSI-Modell in der Praxis

Mit dem OSI-Modell wurde eine Definition von Kommunikationsmerkmalen geschaffen, die von Gremien (wie etwa IEEE) genutzt werden kann, um Standards zu schaffen, die sich auf einzelne oder mehrere Schichten des Modells beziehen.

Aufgrund der Allgemeingültigkeit des OSI-Modells ist es außerordentlich komplex. Wird diese Komplexität nicht gebraucht, kommen häufig andere, simplere Modelle zu Einsatz, die sich auf für das Einsatzgebiet wesentliche Faktoren der Netzwerktheorie beschränken. Die gebräuchlichsten vereinfachten Modelle sind das DoD-Modell und das TCP-Modell.

Da sie aber stets auf das OSI-Modell zurückgehen müssen und diesem nicht widersprechen dürfen, sollen sie nur als Detailergänzungen für bestimmte Anwendungen verstanden werden. Sie können niemals das OSI-Modell ersetzen, denn erst eine genaue Kenntnis vom OSI-Modell erlaubt eine exakte Bewertung von Problemen oder Lösungsansätzen in der Netzwerkkommunikation.

3.4 Das DoD-Modell

Ursprung

Das US-Verteidigungsministerium (Department of Defense = DoD) ist maßgeblich an vielen Entwicklungen im Bereich der Netzwerke beteiligt. Das DoD entwickelte ein eigenes Netzwerkmodell Jahre vor der Entwicklung des OSI-Modells. Es dient in erster Linie der Beschreibung von Kommunikation im Internet und ist weniger auf lokale Netzwerke ausgerichtet. Im Zusammenhang mit der Entwicklung des ARPANET (dem Vorgänger des Internets) ging es beim DoD-Modell um eine rein militärische Anwendung.

Einige Jahre später wurde das OSI-Modell mit einem ähnlichen Aufbau, aber sieben statt vier Schichten, entwickelt. Große Computerfirmen und auch die US-Regierung (seit 1988) unterstützen das OSI-Modell. Anhand des DoD-Modells werden häufig Kommunikationsabläufe im Internet beschrieben.

Vergleich zwischen OSI- und DoD-Modell

Die vier Schichten des DoD-Modells lassen sich genau den sieben Schichten des OSI-Modells zuordnen.

OSI-Schicht	OSI-Modell	DoD-Modell	Beispiele	DoD-Schicht
7	Application Layer			
6	Presentation Layer	Process Layer	Telnet, SMTP, FTP	4
5	Session Layer			
4	Transport Layer	Host-to-Host Layer	TCP, UDP	3
3	Network Layer	Internet Layer	IP, IPX	2
2	Data Link Layer	Network Access Layer	Ethernet	1
1	Physical Layer		Token Ring	

3.5 Das TCP/IP-Modell

Konzentration auf das Internet-Protokoll

Ähnlich wie das DoD-Modell versucht auch das TCP/IP-Modell eine Vereinfachung des logischen Ansatzes, um so der Kommunikationspraxis gerecht zu werden. TCP/IP ist heute die am weitesten verbreitete Protokollfamilie. Dabei sind die zentralen Komponenten auf den OSI-Schichten 3 und 4 angesiedelt. Was auf den Schichten darunter und darüber vorgeht, spielt erst einmal eine untergeordnete Rolle.

Daraus ergibt sich, dass ein Modell, das zur Beschreibung der Kommunikation mittels TCP/IP eingesetzt wird, auch nicht beschreiben muss, was auf den Anwendungsschichten oder den Netzwerzugangsschichten passiert. Sie sehen also wieder ein vierstichtiges Modell, das im Prinzip mit dem DoD-Modell übereinstimmt und sich nur in Details der Nomenklatur von diesem unterscheidet.

OSI-Modell	TCP/IP-Modell
Application Layer	
Presentation Layer	Application Layer (Anwendungsschicht)
Session Layer	
Transport Layer	Transport Layer (Transportschicht)
Network Layer	Internet Layer (Internetschicht)

OSI-Modell	TCP/IP-Modell
Data Link Layer	
Physical Layer	Link Layer (Netzzugangsschicht)

Um Probleme der Netzwerkkommunikation im Allgemeinen zu betrachten, empfiehlt es sich, auf das detaillierteste Modell (OSI) zurückzugreifen.

3.6 Kapselung und Entkapselung

Segmentierung

Wenn höhere Schichten Daten an die unteren Schichten weiterreichen, geschieht zweierlei mit den Daten. Einerseits werden diese in immer kleinere Pakete unterteilt, um bei Bedarf ein kleineres Datenpaket erneut übertragen zu können. Andererseits werden den Daten Steuerinformationen hinzugefügt, um so Informationen zu Datenintegrität und -reihenfolge bereitzustellen.

Dieser Vorgang wird Kapselung genannt und muss beim Entpacken der Daten umgekehrt werden. Die folgende Tabelle zeigt, wie der Vorgang Daten aus den Anwendungsschichten aufteilt. Dabei werden die oberen Schichten nicht unterschieden, da sie für die Kapselung und Entkapselung keine Rolle spielen.

System 1		System 2
Application		Application
Presentation	Datagramm: Daten	Presentation
Session		Session
Transport	Segment: Header Daten	Transport
Network	Packet: Header Daten	Network
Data Link	Frame: Header Daten	Data Link
Physical	Bits: Daten	Physical

Aus Sicht einer untergeordneten Schicht handelt es sich beim Header der höheren Schicht um Daten, die von der eigentlichen Nutzlast nicht zu unterscheiden sind. Dies erklärt sich dadurch, dass Header-Informationen auch nur auf der eigenen Schicht ausgewertet werden können.

Durch das Zusammenfassen von Daten und Headern kann es nötig werden, etwa ein Segment auf zwei Pakete zu verteilen, da die maximale Größe (Maximal Transmission Unit, MTU) nicht überschritten werden darf.

Entkapselung

Werden die Informationen schließlich beim Empfänger wieder einer Anwendung zugänglich gemacht, muss dieser Prozess umgekehrt werden:

- ✓ Die Header-Informationen und die Informationen aus dem Trailer werden ausgewertet.
- ✓ Der Header und der Trailer werden vom Paket entfernt.
- ✓ Gegebenenfalls werden Segmente gesammelt und wieder zusammengefügt.
- ✓ Die Daten werden an die nächsthöhere Schicht weitergeleitet.
- ✓ Auf der nächsthöheren Schicht wird entsprechend verfahren.

3.7 Übung

Fragen zum OSI-Modell

Übungsdatei: --

Ergebnisdatei: uebung03.pdf

1. Wählen Sie aus der folgenden Aufzählung die korrekten deutschen Begriffe der Schichten des OSI-Modells aus:
Transportschicht, Verkehrsschicht, Leitungsschicht, Abbildungsschicht, Darstellungsschicht, Tagungsschicht, Sitzungsschicht, Umleitungsschicht, Speicherungsschicht, Datensicherungsschicht, Verbindungsschicht, Vermittlungsschicht, Binärschicht, Byteübertragungsschicht, Bitübertragungsschicht, Programmsschicht, Anwendungsschicht, Dienstschicht
2. Wählen Sie die korrekten englischen Begriffe der Schichten des OSI-Modells aus:
Theoretical Layer, Application Layer, Connection Layer, Transport Layer, Binary Layer, Data Link Layer, Session Layer, Backup Layer, Tunneling Layer, Program Layer, Presentation Layer, Streaming Layer, Conversation Layer, Physical Layer, Infrastructure Layer, Network Layer, Communication Layer, Service Layer
3. Ordnen Sie den Schichten die Begriffe aus ① und ② in der richtigen Reihenfolge zu:

	OSI-Modell (Deutsch)	OSI-Modell (Englisch)
Schicht 7		
Schicht 6		
Schicht 5		
Schicht 4		
Schicht 3		
Schicht 2		
Schicht 1		

4. Wie werden die Verbindungspunkte zwischen den Schichten bezeichnet?
5. Welche Schicht hat die Aufgabe, logische Wege in Netzwerken zu ermitteln?
6. Welche Schicht bereitet Daten von der Festplatte für den Transport über das Netzwerk auf?
7. Welche Schicht übernimmt die physikalische Adressierung innerhalb eines Netzwerksegments?

4 Die TCP/IP-Protokollsammlung

In diesem Kapitel erfahren Sie

- ✓ welche Protokolle zur TCP/IP-Protokollsammlung gehören
- ✓ welche grundlegenden Aufgaben Protokolle erfüllen
- ✓ welchen Schichten die einzelnen Protokolle zugeordnet werden

Voraussetzungen

- ✓ Verständnis der gängigen Netzwerkmodelle

4.1 Die Protokolle und ihre Aufgaben

Der TCP/IP-Protokoll-Stapel

Der TCP/IP-Protokoll-Stapel umfasst eine Sammlung an Protokollen, die unterschiedliche Aufgaben in Netzwerken erfüllen. Der gemeinsame Nenner dieser Protokolle ist, dass sie alle das Internet-Protokoll (IPv4 oder IPv6) auf der Netzwerkschicht des OSI-Modells verwenden, um Datenpakete zu transportieren. Die folgende Tabelle vermittelt einen Überblick über die wichtigsten Protokolle des Protokoll-Stapels (engl. protocol stack).

Anwendungsschicht	Telnet, FTP, TFTP, HTTP, HTTPS, LDAP, DHCP, BOOTP, DNS, NETBIOS, SMTP ...				
Transportschicht	TCP	UDP	GRE	AH	ESP ...
Internetschicht	ICMP				
Netzzugangsschicht	IPv4				
	IPv6				

 Die Zuordnung von ICMP zur Internetschicht ergibt sich aus den Aufgaben der Protokolle. Auch wenn ICMP über einen eigenen IP-SAP angesprochen wird, befindet es sich auf der Internetschicht. Die Zuordnung von ARP/RARP im Schichtenmodell ist nicht ganz einfach, da die Protokolle eine Zuordnung von Informationen der Netzwerkschicht zu Informationen der Datenverbindungsschicht vornehmen. Aufgerufen werden sie als Subprotokolle der LLC und sind somit in der Netzwerk-Interface-Schicht anzusiedeln.

Internet-Protokoll (IP)

Schicht 3: Vermittlungsschicht (Network Layer)	IP
--	----

Das wichtigste Protokoll der TCP/IP-Protokollfamilie ist das Internet Protocol in den Versionen 4 und 6. Es ist für die Übermittlung der TCP oder UDP-Datagramme in Paketen zuständig (Paketswitching) und kümmert sich um die Pfadermittlung im Netzwerk. Anhand des Netzwerkanteils der IP-Adresse wird der beste Weg vom Sendernetz zum Zielnetz gefunden, und innerhalb des Netzes wird mittels der Hostadresse das Zielsystem adressiert.

ARP/RARP

Schicht 2: Sicherungsschicht (Data Link Layer)	ARP/RARP
--	----------

Das Address Resolution Protocol (ARP) dient zur Ermittlung der Hardware-Adresse eines bekannten IP-Hosts, mit Reverse ARP(RARP) wird einer bekannten Hardware-Adresse die zugehörige IP-Adresse zugeordnet.

Dazu sendet ein System einen MAC Broadcast auf der Sicherungsschicht und eine ARP-Anfrage auf der Vermittlungsschicht. Die ARP-Anfrage (ARP Request) ist dabei eine zielgerichtete Sendung an die IP-Adresse des Hosts, dessen MAC-Adresse aufgelöst werden soll. In diesem wird das mit der IP-Adresse angesprochene System aufgefordert, seine MAC-Adresse dem anfragenden System mitzuteilen.

ICMP

Schicht 3: Vermittlungsschicht (Network Layer)	ICMP
--	------

Das Internet Control Message Protocol (ICMP) dient zur Ermittlung von Fehlern, die bei der Übertragung von IP-Paketen auftreten. Hierzu wird ein sogenannter Echo Request an das Zielsystem gesendet. Dabei handelt es sich um einen acht Byte langen Header mit Informationen zum ICMP Type (1 Byte), ICMP Code (1 Byte), einer Checksumme (2 Byte) und einem Operationsfeld (4 Byte), das je nach ICMP-Typ unterschiedliche Informationen enthalten kann, wie etwa den Fehlerstatus oder Zeitstempel des Pakets.

Als Nutzlast verwendet ICMP eine festlegbare Menge an Buchstaben von A bis W. Die bekannteste Anwendung, die auf ICMP zurückgreift, ist der Befehl PING.

Transmission Control Protocol (TCP)

Schicht 4: Transportschicht (Transport Layer)	TCP
---	-----

Das Transmission Control Protocol (TCP) ist für den verbindungsorientierten Datentransport im Netzwerk zuständig. Es steuert unter anderem den Sitzungsaufbau und -abbau, das Multiplexing zwischen verschiedenen Anwendungen der oberen Schichten und die Fehlerkontrolle für empfangene Segmente.

Wenn sich die Empfangsreihenfolge der Datagramme verschiebt, wird z. B. anhand der Sequenznummern die Reihenfolge wieder korrigiert. Und falls für gesendete Datagramme keine Empfangsbestätigung erfolgt, werden diese nochmals gesendet.

User Datagram Protocol (UDP)

Schicht 4: Transportschicht (Transport Layer)	UDP
---	-----

Auch das User Datagram Protocol (UDP) ist für den Datentransport zuständig, allerdings ist es ein verbindungsloses Protokoll, das keine Empfangskontrolle durchführt. Daher kommt es nicht so häufig bei der Übertragung größerer Datenmengen zum Einsatz, sondern wird vor allem mit Diensten verwendet, die selbstständig eine Fehlerkontrolle durchführen. Beispiele dafür sind der Domain Name Service (DNS) oder das Dynamic Host Configuration Protocol (DHCP).

Daneben kann es für den schnellen und einfachen Datentransport in Umgebungen mit hoher Übertragungssicherheit verwendet werden. TFTP (Trivial File Transfer Protocol) verlässt sich beispielsweise auf die Kontrollmechanismen anderer Schichten und kann mittels UDP deutlich höhere Geschwindigkeiten erreichen als FTP. Für den Einsatz im Weitverkehrsbereich ist es aber ungeeignet.

GRE, AH und ESP

Die Protokolle GRE (Generic Routing Encapsulation), AH (Authentication Header) und ESP (Encapsulating Security Payload) stehen beispielhaft für weitere Protokolle auf der Transportschicht. Obwohl der meiste Datenverkehr mit den Protokollen TCP und UDP abgewickelt wird, gibt es Situationen, die besondere Transportprotokolle erfordern. So wird GRE nicht nur in der Kapselung von Daten von Router zu Router, sondern auch beim Erstellen von VPNs benutzt. AH und ESP sind zwei Protokolle, die aus der Familie der IPSec-Protokolle eine authentifizierte und verschlüsselte Datenübertragung in IP-Netzwerken ermöglichen.

Protokolle höherer Schichten

Schicht 7: Anwendungsschicht (Application Layer)	HTTP, FTP, TFTP, POP, SMTP ...
Schicht 6: Darstellungsschicht (Presentation Layer)	JPEG, MIDI, ASCII, MPEG ...
Schicht 5: Sitzungsschicht (Session Layer)	NFS, NetBIOS, DNS ...

Auf den Anwendungsschichten des TCP/IP-Modells findet sich eine ganze Reihe von Protokollen und Diensten mit den verschiedensten Aufgaben. Da die Protokollfamilie in allen heute gängigen Netzwerksituationen zum Einsatz kommt, müssen auch für alle gängigen Applikationen Protokolle bereitgestellt werden.

Protokolle der Sitzungsschicht

TCP/IP unterstützt eine ganze Reihe von Protokollen und Diensten der Sitzungsschicht. Manche von diesen erfüllen generelle Aufgaben in Netzwerken, wie etwa die Namensauflösung, während andere betriebssystem-spezifische Dienste wie etwa die Benutzerauthentifizierung oder den Dateizugriff über das Netzwerk bereit stellen.

Beispiele hierfür sind DNS und WINS, NetBIOS, NIS und Kerberos oder NFS und CIFS.

Protokolle der Darstellungsschicht

Auf die diversen Dateiformate soll an dieser Stelle wegen mangelnder Praxisnähe nicht detailliert eingegangen werden. Es sei nur erwähnt, dass sich in einigen Sonderfällen die Formen der Implementierung (etwa von ASCII bei UNIX- und Microsoft-Systemen) unterscheiden und eine Detailanpassung erfordern.

Die folgende Tabelle soll nur eine beispielhafte Übersicht über Protokolle auf Schicht 7 geben, sie kann jedoch bei Weitem nicht alle Protokolle darstellen, die unterstützt werden.

Text, Daten	ASCII, EBCDIC, Unicode
Musik	MIDI, Wave
Grafik	JPEG, GIF, PICT, TIFF
Video	MPEG, DivX, QuickTime

Die Daten dieser verschiedenen Protokolle werden von der Darstellungsschicht für den Transport über das Netzwerk aufbereitet. Dazu erfolgen eine Datenkompression, Sitzungssteuerung und Verschlüsselung. Die Art der Aufbereitung ist dabei betriebssystemabhängig. So können etwa 8-Bit-ASCII-Zeichen oder 16-Bit-ASCII-Zeichen Verwendung finden.

Protokolle der Anwendungsschicht

Die Protokolle der Anwendungsschicht, die in die TCP/IP-Familie integriert sind, haben die Aufgabe, Dienste für Programme bereitzustellen. So werden mit FTP Daten über das Netzwerk übertragen, während etwa SMTP für das Übermitteln von Mails zuständig ist. In der folgenden Tabelle sind einige der gängigen Dienste und Protokolle der Anwendungsschicht aufgeführt, die von TCP/IP angesprochen werden können.

Datenübertragung	FTP, TFTP
E-Mail	SMTP, POP2, POP3
Remotesitzungen	Telnet, Rlogin
WWW	HTTP, HTTPS
Netzwerkdienste	DHCP, WINS, DNS

Zwar werden nicht alle der hier angeführten Netzwerkdienste von Anwendungen außerhalb des Netzwerkes benötigt, doch sind sie als Dienste nicht mit den Aufgaben der niedrigeren Schichten zu vereinbaren und sollten deshalb (soweit sie überhaupt in ein Netzwerkmodell integrierbar sind) der Anwendungsschicht zugeordnet werden.

4.2 Interaktion zwischen Protokollen und Diensten

Service Access Points

Jede Netzwerkkommunikation benötigt den Einsatz mehrerer Protokolle, um den fehlerfreien Transport von Daten über das Netzwerk sicherzustellen. Damit die Daten von einer Schicht an den richtigen Dienst der darüber liegenden Schicht weitergereicht werden, müssen sie über bestimmte Ports adressiert werden. Diese werden auch als Service Access Points (SAP) bezeichnet.

Die Ports der Schichten 2 und 3 (Sicherung und Vermittlung) sind dabei kaum von Bedeutung, hier können von Netzwerkadministratoren keine Eingriffe vorgenommen werden. So spielt es etwa keine Rolle, dass TCP z. B. von IP über Port 6 adressiert wird, außer man möchte jeglichen TCP-Verkehr unterbinden.

Anders verhält sich die Sache bei den Ports der Schicht 4 (Transportschicht). Hier ist eine genaue Kenntnis der Ports insbesondere dann nötig, wenn der Datenverkehr analysiert werden soll oder wenn die Konfiguration einer Firewall für bestimmte Protokolle vorgenommen werden soll.

Standardisierte Ports

Bei den Portnummern unterscheidet man drei Gruppen: Well known Ports (0-1023), registrierte Ports (1024-49151) und private Ports (ab 49152).

Die Ports können entweder über TCP, per UDP oder über beide Protokolle angesprochen werden. Wenn ein Protokoll verbindungsorientierte Dienste benötigt (wie etwa FTP), kann es auch nur über TCP adressiert werden. Hat ein Protokoll dagegen einfache Aufgaben, die eine verbindungsorientierte Kommunikation nicht erforderlich machen (wie etwa DNS), kann auch auf das schlankere und bandbreiteneffizientere UDP zugegriffen werden. Dies ist vor allem dann der Fall, wenn die zu übermittelnden Daten eine Frage beinhalten, deren Beantwortung selbst eine Art Transportkontrolle darstellt.

Die Textdatei `etc/services`

Die Zuordnung der Protokolle zu Diensten erfolgt in der Datei `services`. Bei Windowsystemen befindet sich die Datei im Pfad `%systemroot%\System32\drivers\etc`.

`%systemroot%` ist eine Umgebungsvariable für den Installationspfad von Windows. Hier können bei Bedarf Veränderungen vorgenommen werden, sollten bestimmte Anwendungen ein Protokoll über einen anderen als den üblichen Port ansprechen wollen.

Das Format der Datei `services` ist generalisiert und unterscheidet sich bei unterschiedlichen Betriebssystemen wie LINUX oder der Windows-Familie nicht, auch wenn einzelne Ports in unterschiedlichen Systemen nicht definiert sind. Dies ist lediglich darauf zurückzuführen, dass nicht alle Dienste auf allen Betriebssystemen eingesetzt werden.

Die Informationen in der Datei sind recht einfach aufgebaut und werden zu Beginn der Datei erläutert. Hier ein Beispiel, wie Informationen:

Name des Dienstes	Port/Protokollzuordnung	Aliase	#Kommentar
www	80/tcp	http	# WorldWideWeb HTTP
www	80/udp		# Hyper Text Transfer Protocol

Wie in dem Beispiel ersichtlich, gibt es für den Dienst `www` einen Eintrag für TCP und einen weiteren für denselben Port für UDP. Dies entspricht RFC 1340, auch wenn die meisten Protokolle keine Operation unter UDP unterstützen.

Nachfolgend sehen Sie die ersten Zeilen der Datei `services` (die Originaldatei besitzt eine Länge von knapp 300 Zeilen):

```
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
echo                7/tcp
echo                7/udp
discard            9/tcp    sink null
discard            9/udp    sink null
systat             11/tcp   users          #Active users
systat             11/udp   users          #Active users
daytime            13/tcp
daytime            13/udp
qotd               17/tcp   quote          #Quote of the day
qotd               17/udp   quote          #Quote of the day
chargen            19/tcp   ttyst source   #Character generator
chargen            19/udp   ttyst source   #Character generator
ftp-data           20/tcp
ftp                 21/tcp
ssh                22/tcp
Protocol
```

Wenn Sie die Datei verändern wollen, halten Sie das vorgegebene Format ein. Anstatt z. B. eine vorhandene Zeile zu löschen, empfiehlt es sich, am Beginn der Zeile ein Kommentarzeichen (#) einzufügen.

Die offizielle Zuordnung der Ports lässt sich unter <http://www.iana.org/assignments/port-numbers> abrufen und in verschiedenen Formaten herunterladen. Diese von der IANA (Internet Assigned Numbers Authority) verwaltete Liste erhebt Anspruch auf Vollständigkeit, während die Datei `services` nur die well known Portnummern enthält („This file contains port numbers for well-known services defined by IANA“).

4.3 Die MAC-Adresse

Ziel: Zuordnung MAC – IP

Unterhalb der TCP/IP-Protokoll-Sammlung kann eine ganze Reihe unterschiedlicher Protokolle eingesetzt werden. Diese sind in erster Linie von der Art der Netzwerkkomponenten und nicht vom Protokoll-Stack abhängig. Allerdings müssen sie eine Zuordnung der physikalischen Adresse (Media Access Control, MAC) zur IP-Adresse erlauben.

Format der MAC-Adresse

Die MAC-Adresse ist eine 48-Bit-Adresse, die der Netzwerkkarte vom Hersteller zugewiesen wird. Sie besteht aus einem von InterNIC an den Hersteller vergebenen Anteil von drei Byte und einer Seriennummer von ebenfalls drei Byte, die der Hersteller der Karte zuweist. Die Angabe erfolgt in der Regel als 12-stelliger Hexadezimal-Wert vom Format 00:3C:DE:12:34:56.

MAC-Adress-Konflikte

In der Regel sollte dieser Wert weltweit eindeutig sein. Doch ist es in der Vergangenheit immer wieder vorgekommen, dass baugleiche Karten eines Herstellers über identische MAC-Adressen verfügen. In diesem Fall muss einer der Karten von Hand eine andere MAC-Adresse zugewiesen werden oder es muss darauf geachtet werden, dass die Karte in einem anderen Netzwerksegment eingesetzt wird, das auch mit einem anderen Switch verbunden ist.

Es ist nicht empfehlenswert, solche Karten einzusetzen. Insbesondere bei Verwendung von DHCP kann es aufgrund der Datenbankinformationen zu Konflikten kommen und Adressreservierungen könnten falsch vergeben werden.

Ein weiteres mögliches Problem stellen virtualisierte Rechner im Netzwerk dar, da bei deren Verwaltung im Hypervisor eine MAC-Adresse manuell frei eingetragen werden kann. Verwaltet ein Hypervisor die beteiligten virtualisierten Netzwerkkarten seiner Virtuellen Maschinen selbst, sind Dopplungen nicht zu erwarten.

ARP

Das Address Resolution Protocol (ARP) dient zur Ermittlung von MAC-Adressen in direkt verbundenen Netzwerken. Über den Vorgang der Adressbindung werden der MAC-Adresse eine oder mehrere IP-Adressen zugewiesen, an die eingehende Pakete weitergereicht werden müssen. Sendende Systeme müssen diese Adressbindung ermitteln, indem sie einen sog. ARP-Request senden. Über einen MAC-Broadcast wird dabei das System auf IP-Ebene aufgefordert, seine MAC-Adress-Information an das nachfragende System zu übermitteln. Anschließend können Pakete an das Zielsystem als gerichtete Sendungen übermittelt werden und werden nur noch von der Ziel-Netzwerkkarte ausgewertet, ohne alle Systeme im Netzwerk zu belasten.

Da ARP von IPv6 nicht unterstützt wird, wird diese Funktionalität bei Verwendung von IPv6 durch das Neighbor Discovery Protocol (NDP) bereitgestellt.

RARP

Sollte ein System die MAC-Adresse kennen und die dazugehörige IP-Adresse ermitteln müssen, kommt bei Verwendung von IPv4 mit dem Reverse Address Resolution Protocol (RARP, umgekehrtes ARP) eine Variation von ARP zum Einsatz.

4.4 Übung

Fragen zur TCP/IP-Protokollsammlung

Übungsdatei: --

Ergebnisdatei: uebung04.pdf

1. Ordnen Sie die folgenden Protokolle den Schichten des ISO/OSI-Modells zu:

Protokoll	Schicht
TCP	
IPv4	
HTTP	
ARP	
NetBIOS	
MIDI	
UDP	
RARP	
ICMP	
DNS	
IPv6	

2. Was ist die Aufgabe von ARP im Netzwerk?
3. Welcher bekannte Befehl verwendet das Protokoll ICMP?
4. Erläutern Sie knapp den Unterschied zwischen UDP und TCP.
5. Was ist die Aufgabe von Ports?
6. Wo sind die Zuordnungen von Protokollen zu Ports hinterlegt?
7. Besuchen Sie die Website <http://www.iana.org/assignments/port-numbers> und orientieren Sie sich, welche aktuellen Definitionen die IANA zur Verfügung stellt. Schauen Sie zusätzlich in die Datei `services` und orientieren sich an einem verfügbaren Linux- oder Windows-System.
8. In der folgenden Tabelle finden Sie eine Übersicht häufig benötigter Ports. Ordnen Sie diesen bitte die Standardprotokolle zu:

Port	Protokoll
20 und 21	
23	
25	
53	
67 und 68	
69	
80	
110	
443	

9. Vergleichen Sie die Einträge für FTP und TFTP. Welcher Unterschied fällt Ihnen hierbei auf? Erläutern Sie die Auswirkung auf Netzwerkverkehr und Übertragungssicherheit.

5 Das Internet-Protokoll IP

In diesem Kapitel erfahren Sie

- ✓ welche Bestandteile das Internet-Protokoll IP umfasst
- ✓ wodurch sich IP- und Netzwerkadresse unterscheiden
- ✓ wie Sie Subnetzmasken und IP-Adressen berechnen können
- ✓ welche Neuerungen IPv6 bringt

Voraussetzungen

- ✓ Grundlagen binären Rechnens

5.1 Bestandteile und Aufgaben von IP

Internet-Protokoll

Schicht 3: Vermittlungsschicht (Network Layer)	IP
--	----

Das Internet-Protokoll (IP) ist das am weitesten verbreitete Protokoll auf OSI-Schicht 3. Es spielt einerseits eine wesentliche Rolle im Internet: Ohne IP lässt sich kein Zugang zum Internet bereitstellen. Andererseits ist das IP auch für alle anderen Netze von Bedeutung, seit TCP/IP in modernen Betriebssystemen zum Standard erklärt wurde.

Verschiedene Dienste werden mittels IP über dasselbe Netz betrieben. Beispiele sind die Übermittlung von Sprache und Videos im Netz, Onlinekonferenzen oder der gesicherte Transport von Informationen für Dienste wie Onlinebanking.

Bei all diesen Kommunikationsformen findet sich IP mit seinen vielfältigen Charakteristiken wieder. Daher müssen im Folgenden der Aufbau und die Verwendung von IP-Adressen sowie ihre Verarbeitung im Netz detailliert beleuchtet werden. Dies soll zunächst am Beispiel von IPv4 dargestellt werden.

Netz-, Subnetz- und Hostadresse

Um Ihnen das Verständnis der Strukturen in der IP-Adressierung zu erleichtern, wird im Folgenden ein Beispiel aus der Telefonie verwendet. Dies wird anschließend mit dem Aufbau von IP-Netzwerken verglichen.

Aufbau einer Telefonnummer

Eine Telefonnummer, die **0049-30-123456** lautet, besteht aus drei Bestandteilen:

- ✓ der Landeskennung **0049**
- ✓ der Ortskennung **30**
- ✓ der Anschlusskennung **123456**

Die Landeskennung wird von einer internationalen Konvention festgelegt, sie darf nicht geändert werden und muss international eindeutig sein.

Die Ortskennung dagegen unterliegt der Telekommunikationsbehörde des nationalen Netzes, sie wird von ihr vergeben und dient dazu, interne Vermittlungen zwischen den eigenen Schaltzentralen des nationalen Netzes zu ermöglichen. Dabei dürfen in verschiedenen Ländern durchaus identische Ortskennungen vorkommen.

Die Anschlusskennung schließlich unterliegt der lokalen Verwaltungsstelle. Sie muss innerhalb eines Ortsnetzes eindeutig sein. Es ist aber legitim, wenn in mehreren Ortsnetzen identische Anschlusskennungen vorkommen.

Eine Untergliederung des Landesnetzes in einzelne Ortsbereiche ist nicht immer notwendig. Vatikanstadt benötigt z. B. keine Untergruppierung in Ortsnetze, sondern ist international unter 00379 erreichbar. Dagegen werden ländliche Bereiche statt einer zweistelligen Vorwahl und einer siebenstelligen Anschlussnummer eher eine fünfstellige Vorwahl und eine vierstellige Anschlussnummer verwenden. Wenn Sie nun die komplette Nummer wählen, werden Sie garantiert auch nur mit der richtigen Gegenstelle verbunden.

Vergleich mit dem Aufbau einer IP-Adresse:

Eine IPv4-Adresse lautet z. B. **73.152.132.197**

Dies ist die dezimale Schreibweise für die binäre Adresse:

0100 1001 . 1001 1000 . 1000 0100 . 1100 0101.

Auch sie kann (muss aber nicht) aus drei Bestandteilen zusammengesetzt sein:

- ✓ der Netzadresse **73. (0100 1001)**
- ✓ der Subnetzadresse **152. 132 (1001 1000 . 1000 0100)**
- ✓ der Hostadresse **197**

Die Netzadresse ist eine über InterNIC (Internet Network Information Center) und deren Unterstellen, den nationalen Regulierungsbehörden, vergebene weltweit eindeutige Adresse. Sie darf vom Netzbetreiber nicht verändert werden.

Die Subnetzadresse dagegen wird vom Betreiber des gemieteten Netzes – je nach Bedarf – verwendet, um eine Untergliederung des Netzes in kleinere Bereiche vorzunehmen. Die Subnetzadressen müssen dabei nur innerhalb des eigenen Netzes eindeutig sein, der Betreiber des Netzes mit der Adresse 75 dürfte aber durchaus ebenfalls ein Subnetz mit der Adresse 152.132 verwenden.

Es bleibt allein ihm überlassen, ob er (wie in diesem Fall) 16 Bit für die Subnetzadressierung verwendet oder mehr oder weniger Bit für Subnetze respektive Hostadressen verwenden möchte. Hat eine Firma beispielsweise viele kleine Außenstellen, wird sie eine der beschriebenen ähnlichen Lösungen anstreben, die eine große Zahl von Netzen (65 534) erlaubt, in denen jeweils relativ wenig Hosts (254) Platz finden.

Hat eine Firma dagegen wenige, dafür aber umso größere Außenstellen, wird sie ihr Netz entsprechend anders strukturieren. Allerdings sollte ein Netz nicht zu viele Hosts beinhalten, da diese extreme Netzwerklästen erzeugen können. (Stellen Sie sich vor, alle Telefonapparate in Deutschland würden eine einzige Vermittlungsstelle verwenden.) Auch ist dann die Adressverwaltung nicht mehr übersichtlich zu gewährleisten. (Stellen Sie sich vor, Sie müssten Hans Müller im Telefonbuch von ganz Deutschland finden.)

Router

Innerhalb eines Ortsnetzes werden die Vorwahlen zwar nicht gewählt, sind aber logisch vorhanden, da sie durch die Vermittlungsstelle bekannt sind. Möchte man dagegen mit einem Anschluss in einem anderen Ortsnetz verbunden werden, ist es nötig, dass die Nummer inklusive der Vorwahl angegeben wird. Dabei spielt es jedoch für den Benutzer keine Rolle, welcher Bestandteil der gesamten Telefonnummer Vorwahl und welcher Anteil Anschlusskennung ist. Diese Informationen müssen nur in der Vermittlungsstelle vorliegen, die entscheidet, wohin ein Anruf weitergeleitet werden soll. Kennt die Vermittlungsstelle keinen Weg zum angerufenen Ortsnetz, kann sie die Verbindung auch nicht herstellen.

In IP-Netzen ist die Situation eine andere. Die Rechner innerhalb eines Netzwerkes werden nicht durch eine zentrale Instanz verbunden, die mit einer Vermittlungsstelle vergleichbar wäre, sondern kommunizieren über ein gemeinsames Medium.



Zwar werden heute meist Switches zur Verbindung von Rechnern verwendet, doch arbeiten diese nur auf den OSI-Schichten 1 und 2 und vermögen von daher nicht das Kommunikationsmedium auf Schicht 3 logisch zu unterteilen. Für die Netzwerkarten ist es so, als kommunizierten sie miteinander über ein einziges Kabel.

Wenn ein Host also mit einer Adresse in einem anderen Netzwerk kommunizieren soll, muss er selbstständig eine Instanz ansprechen, die für ihn die Vermittlung des Paketes an die Gegenstelle übernimmt. Dieses Gerät kennt den Weg (Route) zu beiden beteiligten Netzwerken, es wird entsprechend als Router bezeichnet.

Damit ein Host nun aber erkennen kann, ob er mit einer Gegenstelle im eigenen oder in einem anderen Netzwerk kommunizieren soll, muss er stets zusätzlich zur Hostadresse die Netzwerkadresse und die Subnetzadresse mit verwenden.

Unterscheidung zwischen Netz-, Subnetz- und Hostadresse

Eine IP-Adresse besteht aus vier binären Oktetten, die aus Gründen der Übersichtlichkeit dezimal als vier Zahlen zwischen 0 und 255 dargestellt werden. Zur Trennung der Oktette werden Punkte verwendet. Für das System muss kenntlich gemacht werden, was als Netz-, Subnetz- oder Hostadresse zu interpretieren ist. Hierzu verwendet man die Subnetzmaske.

Subnetzmaske

Eine Subnetzmaske besteht aus einer Reihe von binären Einsen gefolgt von einer Reihe von binären Nullen. Sie ist – wie jede IP-Adresse – 32 Bit lang und wird in vier Oktette aufgeteilt, die wiederum mittels Punkten voneinander getrennt sind, z. B.:

1111 1111 . 1111 1111 . 0000 0000 . 0000 0000 bzw. dezimal **255.255.0.0**

Indem eine Subnetzmaske auf eine IP-Adresse angewendet wird, kann ermittelt werden, wo die Grenze zwischen Netzwerk-Anteil der Adresse und dem Hostbereich liegt. Dazu wird eine logische UND-Verknüpfung verwendet (binär ergeben nur zwei Einsen als Ergebnis 1, alle anderen Kombinationen [10, 01, 00] ergeben 0).

Eine andere Form der Notation ist die CIDR-Notation (Classless Internet Domain Routing), bei der nur die Anzahl der Einsen der Subnetmask nach dem Trennzeichen / direkt nach einer IP-Adresse angegeben werden. So stehen beispielsweise die Angaben 192.168.0.0/16 die die IP-Adresse 192.168.0.0 mit der Subnetmask 255.255.0.0 oder 55.0.3.22/26 für eine IP-Adresse 53.0.3.22 mit der Subnetmask 255.255.255.192.

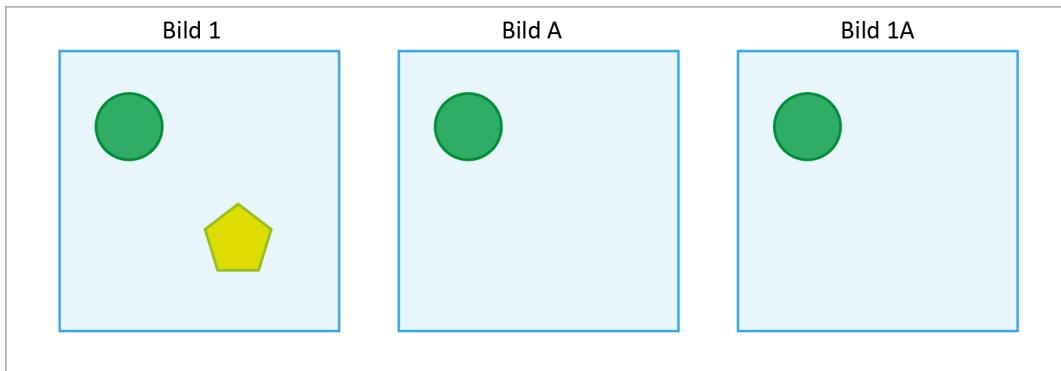
5.2 Mathematische Grundlagen für die Arbeit mit IP

Logisches UND

Bei einer logischen UND-Verknüpfung handelt es sich um einen Vorgang, mit dem sich Unterschiede zwischen zwei binären Informationssätzen filtern lassen. Dieser Vergleich dient dazu, gleiche Informationen von veränderten Informationen zu unterscheiden.

Um dies zu erläutern, werden Sie in drei Schritten arbeiten: In Schritt 1 werden Bilder miteinander verglichen, im zweiten Schritt werden Sie einfache Zahlen „undieren“ und in Schritt 3 schließlich echte IP-Adressen mit Subnetzmasken.

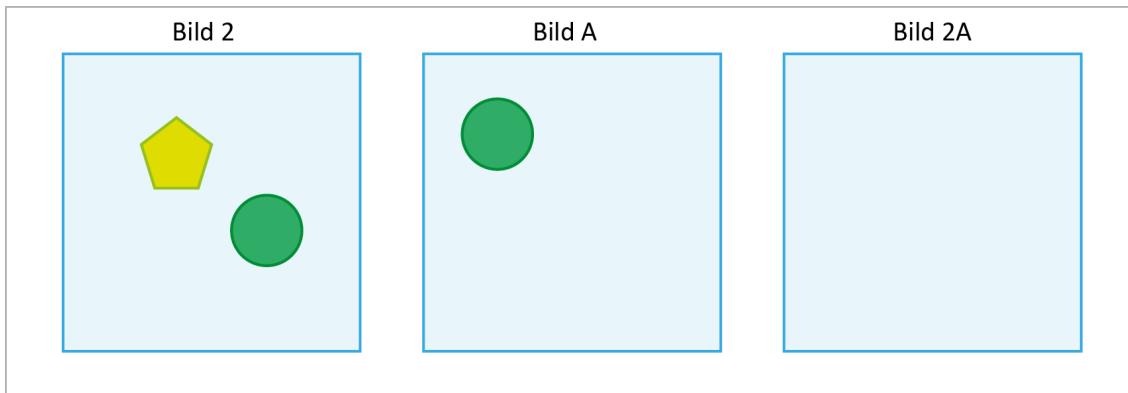
Zur Verdeutlichung vergleichen Sie Bild 1 mit Bild A:



Nur identische Informationen bleiben erhalten. Jede Information, die sich unterscheidet, ist nur einmal vorhanden, wird also von der anderen Information überblendet. Vergleichbar ist dieser Vorgang mit der Doppelbelichtung eines Positivs mit zwei Negativen. Nur Bildinformationen, die auf beiden Negativen gleich sind, werden kein Licht auf das Fotopapier lassen, an den anderen Stellen wird das Licht auf das Fotopapier fallen und die Bildinformation wird verschwinden.

Nehmen Sie nun an, dass Bild 1 die IP-Adresse eines Rechners ist und Bild A seine Subnetzmaske darstellt. Der grüne Kreis markiert den Netzwerkanteil der Adresse und diese bleibt auch nach dem Vergleichen auf Bild 1A erhalten. Das gelbe Fünfeck dagegen war der Hostanteil. Dieser verschwindet nach der Operation.

Vergleichen Sie nun die IP-Adresse eines Remote-Hosts (Bild 2) mit der Subnetzmaske (Bild A):



Hier stimmt die Information zur Netzwerkadresse nicht mit der in der Subnetzmaske überein. Daher wird das System Rechner 2 auch nicht direkt erreichen können, sondern IP-Pakete für diesen an ein Gateway senden.

Sie nehmen eine logische UND-Verknüpfung des vierstelligen binären Informationssatzes 0011 mit dem Informationssatz 0101 vor:

	Erste Stelle	Zweite Stelle	Dritte Stelle	Vierte Stelle
Informationssatz 1	0	0	1	1
Informationssatz 2	0	1	0	1
Resultat	0	0	0	1

Nur an der vierten Stelle ist jeweils eine binäre 1 zu finden. Damit ergibt sich das Resultat 0001.

Vergleichen Sie die IP-Adresse 192.168.0.51 mit der Subnetzmaske 255.255.255.0, erhalten Sie als Resultat die IP-Adresse des Netzwerks:

IP-Adresse	192.168.0.1	1100 0000 . 1010 1000 . 0000 0000 . 0011 0011
Subnetzmaske	255.255.255.0	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
Resultat	192.168.0.0	1100 0000 . 1010 1000 . 0000 0000 . 0000 0000

Soll ein Rechner mit einem zweiten System Kontakt aufnehmen, wird auf diese Weise ermittelt, ob beide Host-adressen im selben Netzwerk liegen.

Netzwerkklassen

Als IP in den 70er Jahren des 20. Jahrhunderts entwickelt wurde, ging man davon aus, dass mittels vier Oktetten eine weltweit ausreichende Zahl an Adressen zur Verfügung stünde, und man legte sich auf sogenannte Netzwerkklassen fest. Eine Netzwerkkategorie ist durch die Anzahl der Bytes gekennzeichnet, in denen sich Subnetze und/oder Hostadressen bilden lassen. Auch legt die Klasse fest, wie das erste Oktett binär beginnen muss. Daraus ergibt sich, dass die höchste dezimale Adresse einer Klasse einen Wert nicht überschreiten darf.

Es gibt die folgenden fünf Klassen:

Netzwerk-Klasse	Adressbereich der Netzadressen	Erstes Oktett	Maximale Host-Adressen	Einsatzzweck
Klasse A (Oktett 1=Netz)	1.0.0.0 bis 127.0.0.0	0*** ****	16. 777. 214	Sehr große Netzwerke
Klasse B (Oktett 1+2=Netz)	128.0.0.0 bis 191.255.0.0	10** ****	65.534	Mittlere Netzwerke
Klasse C (Oktett 1,2+3=Netz)	192.0.0.0 bis 223.255.255.0	110* ****	254	Kleine Netzwerke
Klasse D (speziell)	224.0.0.0 bis 239.255.255.255	1110 ****	Nicht verfügbar	Multicast-Gruppen
Klasse E (speziell)	240.0.0.0 bis 255.255.255.255	1111 ****	Nicht Verfügbar	Experimentelle Adressen

Private Netze

In den Bereichen der Klasse-A-, Klasse-B und Klasse-C-Netze sind jeweils Bereiche für den privaten Einsatz in LANs reserviert. Diese Adressen zeichnen sich dadurch aus, dass sie im Internet nicht geroutet werden.

Privates Klasse-A-Netzwerk	10.0.0.0 mit der Subnetzmaske 255.0.0.0 = ein Klasse-A-Netz
Privates Klasse-B-Netzwerk	172.16.0.0 (bis 172.31.255.255) mit der Subnetzmaske 255.240.0.0 = 16 Klasse-B-Netze
Privates Klasse-C-Netzwerk	192.168.0.0 (bis 192.168.255.255) mit der Subnetzmaske 255.255.0.0 = 255 Klasse-C-Netze

Netzwerkklassen hatten nur Relevanz zu Zeiten, als hinreichend IPv4-Adressen weltweit zur Verfügung standen. Mittlerweile – durch IPv6 und viele Konzepte, mit den knappen IPv4-Adressen nicht so verschwenderisch umzugehen – gilt das Konzept der Netzwerkklassen seit mehr als 20 Jahren als veraltet und nicht praxisrelevant.

5.3 IP-Adressen und Subnetzmasken

Broadcast-Domänen

Je größer ein Netzwerk ist, desto größer ist auch die Anzahl der Systeme, die von einem Broadcast angesprochen werden. Dies bezeichnet man als Broadcast-Domäne. Da Broadcasts verschiedene Aufgaben in Systemen erfüllen, kann auf sie nicht verzichtet werden. Wenn ein Netzwerk zu viele Rechner enthält, erhöht dies die Netzwerklast (im Extremfall führt dies zu einem Erliegen der Kommunikation). Um das zu verhindern, werden Netzwerke in Subnetze unterteilt, die durch Router miteinander verbunden sind. Da Broadcasts von Routern nicht weitergeleitet werden, wird dies auch als Broadcast-Segmentierung bezeichnet.

Subnetting

Man unterteilt das bestehende Netzwerk in diverse logische Bereiche, die die benötigte Anzahl an Adressen enthalten, indem man eine Adresse mit einer erweiterten Subnetzmaske ausstattet. So kann z. B. das Netz mit der Adresse 192.168.1.0 Subnetzmaske 255.255.255.0 mittels der Subnetzmaske 255.255.255.192 in die vier Netze 192.168.1.0, 192.168.1.64, 192.168.1.128 und 192.168.1.192 unterteilt werden.

Netzwerkadresse	Hostadressen	Broadcastadressen
192.168.1.0	192.168.1.1 bis 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 bis 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 bis 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 bis 192.168.1.254	192.168.1.255

Subnetzadressen

Die Subnetzadressen sind dadurch gekennzeichnet, dass sie im Hostbereich nur aus binären Nullen bestehen. Der Hostbereich ist der Bereich, der in der Subnetzmaske ebenfalls nur aus binären Nullen besteht. Hier ist das Subnetz 192.168.1.0 mit der Subnetzmaske 255.255.255.192 dargestellt:

Erstes Oktett	Zweites Oktett	Drittes Oktett	Viertes Oktett
192	168	1	0
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 1	0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1.1 0 0 0 0 0 0

Broadcast-Adresse

Die Broadcast-Adresse ist dadurch gekennzeichnet, dass im Hostbereich alle Bits auf Eins gesetzt sind. Mit ihr werden alle Systeme des Netzwerks angesprochen:

Erstes Oktett	Zweites Oktett	Drittes Oktett	Viertes Oktett
192	168	1	63
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 1	0 0 1 1 1 1 1 1
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1.1 0 0 0 0 0 0

Verwendet wird die Broadcast-Adresse des Subnetzes z. B. zur Namensauflösung von NetBIOS-Namen mit Broadcasts.

Hostbereich

Der Hostbereich umfasst alle Adressen, die sich zwischen der Netzwerkadresse (**X. X. X. x x 0 0 0 0 0 0**) und der Broadcast-Adresse (**X. X. X. x x 1 1 1 1 1 1**) befinden, also X. X. X. 1 bis X. X. X. 62.

Erste Hostadresse

Erstes Oktett	Zweites Oktett	Drittes Oktett	Viertes Oktett
192	168	1	1
1100 0000	1010 1000	0000 0001	0000 0001
1111 1111	1111 1111	1111 1111	1.100 0000

Letzte Hostadresse

Erstes Oktett	Zweites Oktett	Drittes Oktett	Viertes Oktett
192	168	1	62
1100 0000	1010 1000	0000 0001	0011 1110
1111 1111	1111 1111	1111 1111	1.100 0000

Folgenetze

In den weiteren Subnetzen des gleichen Netzes gelten die identischen Bestimmungen für die Netzwerkadresse, die Broadcast-Adresse und den Hostbereich. Auch die eigentliche Netzwerkadresse darf nicht geändert werden. Das Einzige, was sich ändern darf, sind die Bits des Subnetzes; im angegebenen Beispiel das erste und das zweite Bit des vierten Oktetts.

Erstes Netz	192. 168. 1. 0 0 xx xxxx
Zweites Netz	192. 168. 1. 0 1 xx xxxx
Drittes Netz	192. 168. 1. 1 0 xx xxxx
Viertes Netz	192. 168. 1. 1 1 xx xxxx

Tipps für den Umgang mit IP



Die folgenden Ratschläge stellen keine neuen Erkenntnisse dar, können aber helfen, Fehler beim Rechnen mit IP schneller zu erkennen. So können etwa 50 % aller falsch errechneten Netzwerkadressen erkannt werden, da sie ungerade sind, eine ungerade Zahl aber immer bedeutet, dass das letzte Bit gesetzt (= 1) ist. Das letzte Bit muss im Hostbereich liegen.

- ✓ Eine Netzwerkadresse muss immer eine Potenz von eins sein.
- ✓ Eine Broadcast-Adresse ist nie gerade, sondern immer eine ungerade Zahl, die eins kleiner ist als eine Einserpotenz.
- ✓ Die höchste Netzwerkadresse und die Subnetzmaske auf dem Host-Oktett müssen identisch sein, z. B. 165.34.224.0 mit der Maske 255.255.224.0.

Supernetting

Neben der Möglichkeit, ein großes Netz in kleinere Einheiten zu unterteilen, gibt es auch die Möglichkeit, mehrere Netze durch Erweiterung des Hostbereiches zu einem größeren zusammenzufassen.

Netzwerkadresse	Subnetzmaske	Hostadressen	Broadcast-Adressen
192.168.0. 0	255.255.255.0	192.168.0. 1 bis 192.168.0. 254	192.168.0. 255
192.168.1. 0	255.255.255.0	192.168.1. 1 bis 192.168.1. 254	192.168.1. 255
Zusammengefasst zu 192.168.0.0	Mit Subnetzmaske 255.255.254.0	Ergibt gemeinsamen Hostbereich 192.168.0. 1 bis 192.168.1.254	Neue Broadcast-Adresse 192.168.1. 255

Eine besondere Rolle spielt das Supernetting bei der Routenzusammenfassung. Betrachtet man das Szenario, dass ein Unternehmensnetzwerk aus zwei Gebäuden mit jeweils zwei Etagen besteht. In Gebäude Eins befinden sich im ersten Stock die Rechner des Netzwerkes 192.168.0.0 und im zweiten Stock die des Netzwerkes 192.168.1.0, die jeweils über einen Etagen-Router verfügen. Der Zugang zu Gebäude Zwei wird über den Gebäude-Router GB1 gewährleistet. Der Gebäude-Router von Gebäude Zwei muss nun alle Pakete für die Netzwerke 192.168.0.0/24 und 192.168.1.0/24 an GB1 schicken, ohne sich um die einzelne Verteilung der Pakete zu kümmern. Um bei ihm die Anzahl der Routen zu vereinfachen, kann man für das Netzwerkziel 192.168.0.0/23 das Gateway GB1 einsetzen, und erst GB1 muss sich um die Verteilung der Pakete auf die einzelnen Router der Etagen kümmern.

Der Fachausdruck für das Zusammenfassen von Routen lautet Routenaggregation, und dieses Verfahren ist nur möglich, wenn auf klassenloses Interdomänenrouting (Classless Interdomain Routing, CIDR) zurückgegriffen wird.

5.4 IP-Pakete

Arbeitsweise des IP-Protokolls

Im ersten Teil dieses Kapitels wurden der Aufbau und die Funktion der IP-Adressen untersucht. Im Folgenden geht es um die Arbeitsweise des Protokolls. Dazu gehören das Unterteilen der Daten in geeignete Pakete und das Versehen mit einem Header (Encapsulation).

Encapsulation

Daten einer Anwendung werden von der Anwendungsschicht an die Transportschicht weitergegeben. Dort werden sie mit einem TCP- oder UDP-Header versehen und in Datagramme unterteilt. Daraufhin reicht die Transportschicht die Datagramme an die Netzwerkschicht weiter, die sie in Pakete unterteilt und diese mit Headern versieht:

Anwendungsschichten:	Daten	Daten
Transportschicht:	Datagramm	TCP-Header DATEN
Vermittlungsschicht:	Paket	IP-Header TCP-HEADER DATEN
Sicherungsschicht:	Frame	Eth-Header IP-HEADER TCP-HEADER Trailer
Bitübertragungsschicht:	Bits	1 0 0 0 1 0 1 0 1 1 0 0 0 1 0 1 1 1 0 0 1.....

IP-Paket

Ein IP-Paket setzt sich aus einem Header und dem segmentierten Datagramm der Transportschicht mit dessen Header zusammen. Die theoretische Maximalgröße eines IP-Paketes beträgt 64 Kilobyte, in der Praxis werden IP-Pakete allerdings auf rund 1500 Byte begrenzt, da sonst die maximale Größe der Ethernet-Frames überschritten würde.

IPv4-Header

Der Header eines IP-Paketes hat bei IPv4 in der Regel eine Größe von 20 Byte. Diese kann allerdings zwischen 20 Byte und 60 Byte variieren. Bei IPv6 erreicht der Header die doppelte Größe.

In der folgenden Tabelle steht jede Zeile für einen 32-Bit-Block.

1. Byte		2. Byte		3. Byte		4. Byte													
Version	Headerlänge	Diensttyp				Gesamtlänge													
Identifikationsnummer				Flags	Fragmentabstand														
TTL	Protokoll			Header-Prüfsumme															
Quelladresse																			
Zieladresse																			
Optionsfeld						Füllbits													
Daten ...																			

Version

Im Versionsfeld (Version) steht die IP-Protokollversion, die verwendet wird. Dies ist in der Regel noch IPv4, allerdings ist davon auszugehen, dass sich IPv6 in der nächsten Zeit immer weiter durchsetzen wird.

Header-Länge

Die Header-Länge (Length) muss angegeben werden, da IPv4 mit einer variablen Header-Länge arbeitet, abhängig davon, welche Optionen verwendet werden. Die Angabe erfolgt in 32-Bit-Worten. Die maximale Länge des Feldes von vier Bit bestimmt dabei den Maximalwert von sechzehn 32-Bit-Worten=60 Byte.

Diensttyp

0	1	2	3	4	5	6	7
Priorität			D	T	R		

Unter Diensttyp lassen sich Prioritäten (Precedence) von 0 (Normal) bis 7 (Steuerungspaket) definieren. Mit diesen lassen sich Pakete vorrangig bearbeiten. Mit den Flags D (Delay = Verzögerung), T (Throughput = Durchsatz) und R (Reliability = Zuverlässigkeit) kann der Host definieren, worauf er bei der Übertragung am meisten Wert legt.

Ein Beispiel für den Einsatz von Prioritäten ist etwa die Datenübertragung während einer Telnetsitzung. Normalerweise würden zur effizienten Bandbreitennutzung Daten gesammelt, bis sich ein Paket von ausreichender Größe ergäbe. Somit wäre die Telnetsitzung nicht mehr durchführbar, da eine übermäßige Anzahl von Zeicheneingaben erfolgen müsste. Stattdessen ist es hier nötig, die Übertragung von einzelnen Eingaben sofort durchzuführen, auch wenn dadurch mehr Headerdaten als Nutzdaten transportiert werden. Um dabei die Mindestübertragungsgröße (Minimum transfer Unit) nicht zu unterschreiten, werden die Pakete aufgefüllt.

Gesamtlänge

Im Feld für die Gesamtlänge ist definiert, wie groß das Paket maximal sein kann. Da hier maximal 65.535 Byte angegeben werden können, ergibt sich die theoretische Gesamtgröße für IP-Pakete von 64 Kilobyte. Hosts müssen laut Spezifikationen (RFC 791) mindestens IP-Pakete von 576 Byte Länge verarbeiten können, in der Regel werden aber Pakete von ca. 1500 Byte verwendet.

Identifikation

Alle Fragmente eines Datagramms weisen dieselbe Identifikationsnummer (Identification) auf. Damit wird sicher gestellt, dass sie richtig zusammengesetzt werden, um sie an die höheren Schichten weiterzureichen. Die Identifikationsnummer wird vom Absender vergeben und zusammen mit der Quelladresse ausgewertet.

Flags

Die Flags (Zeiger) dienen zur Steuerung der Fragmente. Das erste Bit ist nicht in Gebrauch. Das zweite Bit steht für DF (Don't Fragment = Nicht fragmentieren), das dritte Flag steht für MF (More Fragments = Mehr Fragmente).

Fragmentabstand

Über den Wert im Feld für den Fragmentabstand (Fragment Offset) ist definiert, an welche Stelle ein Fragment relativ zur Gesamtlänge des Datagramms gehört. Die Feldlänge von 13 Bit bedeutet, dass ein Datagramm maximal in 8192 Fragmenten übertragen werden kann.

Time To Live (TTL)

Die TTL (Time To Live = Maximale Lebensdauer) eines Paketes definiert die Lebenserwartung eines IP-Paketes auf 255 Sekunden (UNIX, gemäß RFC 791) oder 128 Sekunden (Microsoft-Betriebssysteme). In der Praxis wird hier aber keine Zeitbegrenzung vorgenommen, sondern die TTL von jedem verarbeitenden Knoten um eins reduziert. Wenn ein Router das Paket länger zwischenspeichern muss, muss er den Wert mehrmals verringern. Erreicht der Wert null, wird das Paket verworfen. Auf diese Weise wird verhindert, dass Pakete endlos im Netz kreisen.

Protokoll

Im Feld mit dem Protokoll (Protocol) steht die Nummer des Service Access Points (SAP) für die Transportschicht. Hier ist definiert, welches Protokoll der höheren Schicht die Weiterverarbeitung des Pakets erledigen soll. Man spricht auch von ULP-Nummern (Upper-Layer-Protocol) oder Protokollnummern – nicht zu verwechseln mit der bei TCP und UDP gebräuchlichen Portnummer.

Diese Tabelle stellt einen Auszug aus der Zuteilung der Protokollnummern dar:

Protokoll	ULP-Nummer	Name	Beschreibung
ip	0	IP	Internet-Protokoll, Pseudoport für die Eigenadressierung
icmp	1	ICMP	Internet-Control-Message-Protokoll
igmp	2	IGMP	Internet-Group-Multicast-Protokoll
ggp	3	GGP	Gateway-to-Gateway-Protokoll
tcp	6	TCP	Transport-Control-Protokoll
egp	8	EGP	Exterior-Gateway-Protokoll
udp	17	UDP	Universal-Datagramm-Protokoll
gre	47	GRE	Generic Routing Encapsulation
esp	50	ESP	Encapsulating Security Payload
ah	51	AH	Authentication Header

Protokoll	ULP-Nummer	Name	Beschreibung
I2tp	115	L2TP	Layer 2 Tunneling Protocol
raw	255	RAW	RAW IP Interface

Header-Prüfsumme

In der Header-Prüfsumme steht eine Prüfsumme für den gesamten IP-Header. Sie wird als 16-Bit-Längsparität ermittelt und muss von jedem verarbeitenden System neu berechnet werden, da sich die TTL bei jeder Verarbeitung ändert.

Quelladresse, Zieladresse

An dieser Stelle stehen die IP-Quelladresse (Source Address) des Absenders und die IP-Zieladresse (Destination Address) des Paketes.

Optionen

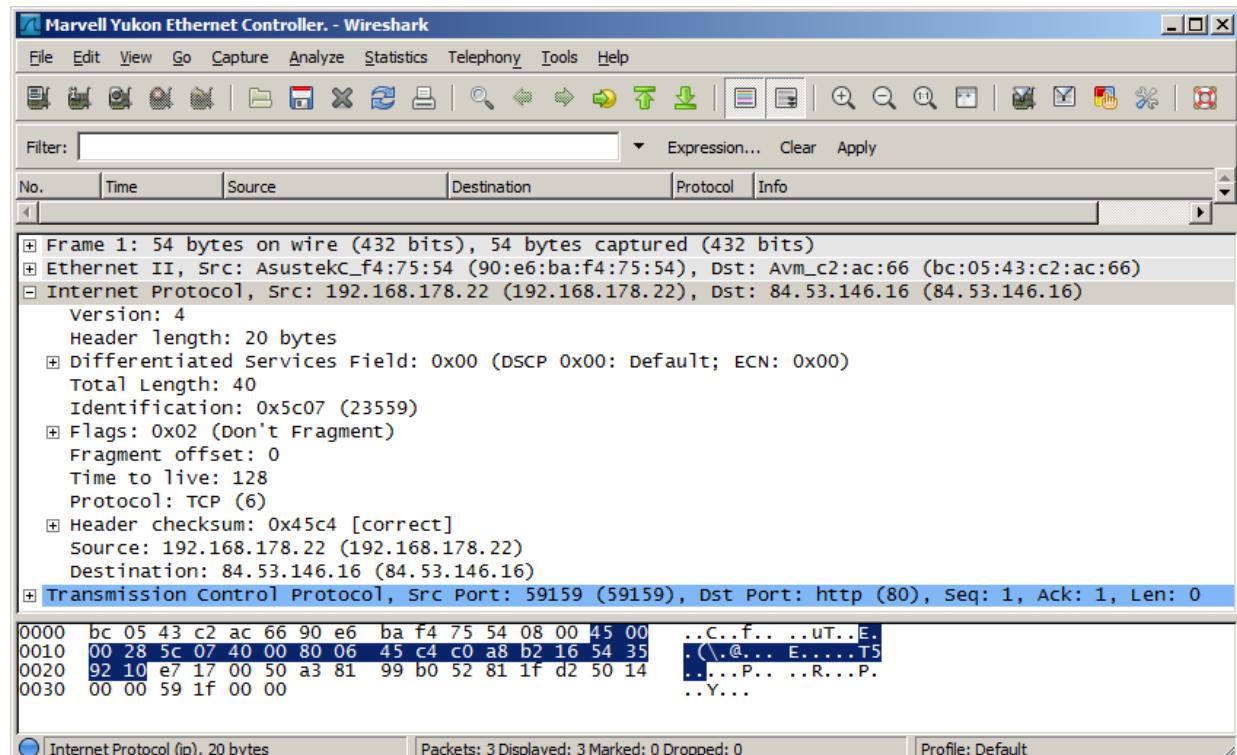
Es sind eine ganze Reihe optionaler Informationen im Paket-Header verankerbar, die etwa der Routen-Ermittlung und der erweiterten Fehlerbehebung dienen. Diese sollen an dieser Stelle aber nicht weiter behandelt werden. Lesen Sie RFC 791, falls Sie mehr dazu erfahren möchten.

Füllbits

Damit die Längeninformation korrekt ausgewertet werden kann, muss das Paket aus kompletten 32-Bit-Wörtern bestehen. Mit den Füllbits (Padding) werden die fehlenden Bits durch Nullen aufgefüllt.

IP-Header im Protokollanalysator

Hier sehen Sie einen Screenshot eines IP-Paketes, das mit einem Protokollanalysator aufgefangen wurde:



Wireshark im Einsatz, Download der aktuellen Version unter <http://www.wireshark.org/>

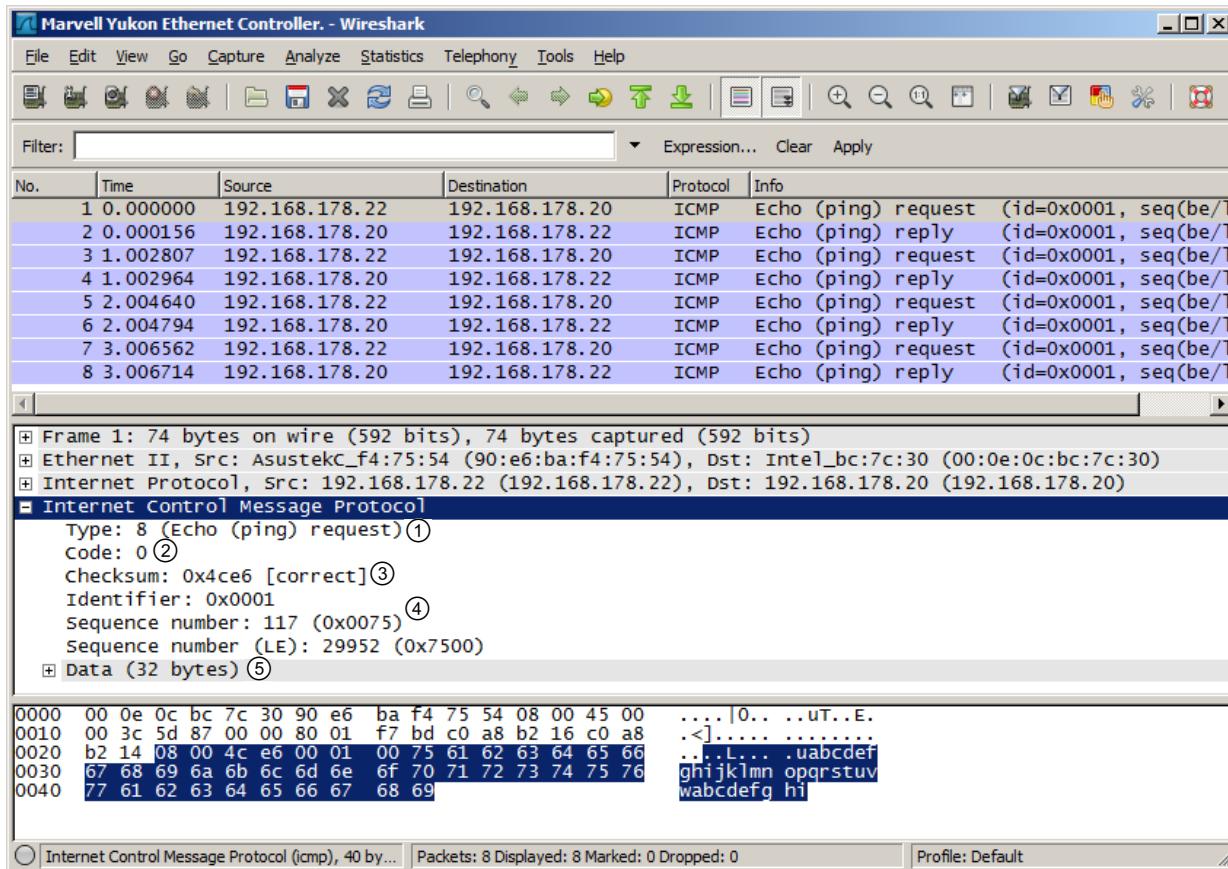
5.5 Internet-Control-Message-Protokoll

ICMP

Das Internet-Control-Message-Protokoll (ICMP) dient zum Austausch von Fehlermeldungen und Kontrollnachrichten zwischen Geräten auf IP-Ebene. Es wird als Protokoll von IP aufgerufen (ULP 1), ist jedoch selbst ebenfalls ein Protokoll auf Schicht 3. ICMP-Nachrichten werden als Nutzlast im Daten-Bereich von IP-Paketen transportiert.

PING

Der wichtigste Befehl, der für die ICMP-Steuerung verwendet wird, ist der Befehl PING. Mit PING wird ein ICMP-Echo-Request an ein System geschickt, das daraufhin seinerseits ein ICMP-Echo-Reply sendet, sofern die Systemeinstellungen eine Antwort zulassen. Ein ICMP-Echo-Request entspricht dem ICMP-Typ 8, ein ICMP-Echo-Reply dem Typ 0. In der Standardeinstellung von PING wird eine Sequenz von vier Requests und vier Replies gesendet.



Type ①

Die Type-Information gibt Aufschluss darüber, welche Art von ICMP-Nachricht versendet wird:

0 Echo Reply	Antwort auf eine Ping-Anfrage eines Remotesystems
3 Destination Unreachable	Ein Netzwerkziel ist nicht erreichbar. Die Ursache steht im Code-Feld: <ul style="list-style-type: none"> ✓ 0 = Netzwerk nicht erreichbar ✓ 1 = Host nicht erreichbar ✓ 2 = Protokoll nicht erreichbar ✓ 3 = Port nicht erreichbar ✓ 4 = Fragmentierung nötig 5 = Quellroute nicht intakt

4	Source Quench	Pufferüberlauf; es kommen mehr Datagramme an, als das System verarbeiten kann.
5	Redirect	Ein Gateway informiert Systeme darüber, dass eine bessere Route zu einem Ziel verfügbar ist, und sendet die IP-Adresse des neuen Gateways.
8	Echo request	Anfrage nach einem Echo Reply
11	Time Exceeded for Datagram	Ein Datagramm ist verfallen. Die Ursache wird im Code-Feld mitgeteilt: ✓ 0 = Die TTL ist abgelaufen. 1 = Die maximale Zeitspanne für das Zusammenfügen der Fragmente wurde überschritten.
12	Parameter Problem on Datagram	Der IP-Header konnte nicht interpretiert werden. Im Code steht ein Verweis auf die entsprechende Stelle des Headers.
13	Timestamp Request	Anfrage nach einer Zeitmessung in Millisekunden
14	Timestamp Reply	Antwort auf einen Timestamp Request
15	Information Request	Anfrage nach einer Netzwerk-ID
16	Information Reply	Antwort auf eine Netzwerk-ID-Anfrage
17	Address Mask Request	Anfrage nach einer Subnetzmaske
18	Address Mask Reply	Antwort auf einen Address Mask Request

Code ②

Hier können Details zum Nachrichtentyp festgehalten werden.

Checksum ③

In dem Feld für die Checksum steht eine Prüfsumme zum ICMP-Feld. Diese ist nötig, da IP ja nur den eigenen Header überprüft, den Dateninhalt aber unberücksichtigt lässt.

Identifier oder Sequence Number ④

Dieses Feld wird ausgewertet, um eine einwandfreie Zuordnung eines Paketes zu einem Kommunikationsstrang vornehmen zu können. In der Darstellung sehen Sie die Sequenznummer 3, da es sich um den dritten Request einer Ping-Sequenz handelt.

Data ⑤

Im Datenfeld des Ping-Paketes befinden sich Buchstaben von "a" bis "w". Mit diesen wird Datenlast erzeugt, um so möglichen Fragmentierungsfehlern auf die Schliche zu kommen.

5.6 IPv6

Internet Protokoll Version 6

Mit Internet Protokoll Version 6 (IPv6, IP-Next Generation oder IPng) soll der Mangel an IP-Adressen im Internet bekämpft werden. Zusätzlich benötigen neue Anwendungen im Multimediacbereich festgelegte Datendurchsatzraten, die in IPv4 nicht bestimmt werden können, weil viele routende Systeme das eigentlich für QoS-Dienste vorgesehene Header-Feld nicht auswerten. Werden z. B. bei der Videoübertragung nicht gewisse Übertragungsgeschwindigkeiten eingehalten, können Bewegungen nicht mehr flüssig dargestellt werden.

Eigenschaften von IPv6

Adressformat	IPv6-Adressen bestehen nicht mehr aus 32, sondern aus 128 Bit. Somit stehen nun rund $3,4 * 10^{38}$ Adressen zur Verfügung.
Neues Header-Format	Der Header von IPv6 ist komplett verändert. Zu Gunsten der deutlich längeren Adressen wurde auf einige der alten Informationen verzichtet. Stattdessen werden nun Verkehrsklassen und Extension Header unterstützt.
Neue Optionen	Mit neuen Optionen können teilweise alte IPv4-Optionen je nach Bedarf mit transportiert oder ausgelassen werden. Dies vereinfacht die Verarbeitung der Pakete durch Router, die entsprechend Optionen überspringen können.
Quality of Service	Um besonders zeitkritische Anwendungen zu unterstützen, müssen Dienstqualitäten definiert werden.
Datensicherheit	IPv6 ist für den Einsatz im Internet entwickelt worden und enthält Mechanismen, die die Authentizität und Integrität der Daten während des Transportes gewährleisten. Die in IPv4 bekannten Protokolle AH und ESP – auch IPSec genannt – gehören standardmäßig schon zum Funktionsumfang von IPv6.
Zukunftssicherheit	IPv6 wurde von vornherein als erweiterbarer Standard implementiert, um so seine Einsetzbarkeit auch bei veränderten Ansprüchen zu gewährleisten.

Der Umstieg auf 128-Bit-Netzwerkadressen erhöht die Anzahl verfügbarer IP-Adressen drastisch. Im Gegensatz zu den in IPv4 theoretisch verfügbaren 4,2 Milliarden Adressen sind es bei IPv6 $3,4 * 10^{38}$. Diese Anzahl würde ausreichen, um jeden Quadratmeter der Erdoberfläche (Wasserflächen mitgerechnet) mit $6,7 * 10^{23}$ IP-Adressen zu versorgen.

Im Vergleich zum v4-Header wurde der v6-Header um einige Informationen abgespeckt. So finden sich zum Beispiel keine Headerchecksumme und keine Fragmentierungsinformationen mehr. Das Fehlen einer Headerchecksumme entlastet routende Systeme, die jetzt viele Datenpakete ohne CPU-lastige Prüfsummenberechnungen weiterleiten können. Die Fehlerfreiheit der Datenübertragungen wird jedoch weiterhin sichergestellt, wenn Protokolle auf höheren Übertragungsschichten (wie zum Beispiel TCP) eine eigene Überprüfung durchführen und gegebenenfalls eine Neuübertragung von fehlerhaften Datenpaketen veranlassen. Fragmentierungsinformationen und andere Steuerinformationen wurden in die Extension Headers ausgelagert - optionale Headerelemente, die nur zwischen zwei routenden Systemen übertragen werden und so den Overhead für die gesamte Verbindung niedrig halten.

Theoretisch ist es in IPv6 möglich, jedem einzelnen an das Internet angeschlossenen Rechner wieder eine öffentliche IP-Adresse zuzuweisen, sodass Notlösungen gegen die IP-Adressknappheit wie z. B. die Network Address Translation (NAT) wieder überflüssig werden. Viele Probleme der vergangenen Jahre, in denen NAT notwendig geworden war, lösen sich bei der direkten Adressierbarkeit einzelner Rechner von selbst. Dazu gehört das bisher notwendige Mappen bzw. Freischalten von Ports an der NAT-Firewall, wenn hinter der NAT-Firewall ein Serverdienst betrieben werden soll. Auch der Betrieb eines ALG (Application Layer Gateway), um NAT-unfreundliche Protokolle wie FTP oder SIP dennoch durch NAT hindurch verwenden zu können, würde entfallen.

Andererseits bietet aber gerade die Verwendung von NAT sicherheitsrelevante Vorteile, da so ein zentraler Zugangspunkt verwaltet wird und das interne Netzwerk nach außen unsichtbar bleibt. Der Einsatz einer DMZ (Demilitarisierte Zone - ein eigenes Netzwerk zwischen zwei Firewalls, das das interne Netz vom Internet trennt) macht die Verwendung von IPv6 im LAN überflüssig, und die Beschränkung des Internetzugangs über Proxy-Server erübrigts ebenfalls den Einsatz von IPv6 im internen Firmennetzwerk.

Moderne Netzwerkbetriebssysteme wie aktuelle Linux-Versionen, Windows Clients und Server unterstützen genuin die Verwendung von IPv6-Adressen. Windows 10 oder Windows Server 2016 besitzen einen vollwertigen IPv6-Stack, der bei einer Standardinstallation gleich mit eingerichtet wird und neben IPv4 läuft.

In der Praxis wird aber vor allem im europäischen und nordamerikanischen Bereich nach wie vor überwiegend IPv4 eingesetzt. Europa und Amerika wurden bei der Zuteilung von IPv4-Adressräumen sehr großzügig bedacht, sodass momentan wenig Motivation für einen Umstieg besteht. In Asien oder Afrika hingegen, wo sehr wenige öffentliche IPv4-Adressen verfügbar sind, es aber eine wachsende Anzahl an Nutzern gibt, schreitet der Einsatz von IPv6 sehr schnell voran.

Ein Umstieg auf IPv6 bedarf neben der veränderten Netzwerksoftware auch Änderungen im Hardware-Bereich. Dies sind Änderungen, die oft auf die lange Bank geschoben werden. So sind viele billigere Router und Schicht-3-Switches nicht in der Lage, mit dem IPv6-Protokoll zu arbeiten, was einen Umstieg auf die modernere Technologie unmöglich macht. Die Angebote von IPv6 durch die Internetprovider unterscheiden sich je nach Land teilweise stark. So ist das Angebot in Nordamerika relativ gering, in Rumänien und Frankreich dagegen weit verbreitet, die Schweiz und Österreich nehmen vor Deutschland mittlere Plätze ein. Viele Internetprovider bieten IPv6-Internetanschlüsse erst auf Nachfrage an, da sie von Kunden selten erwartet werden. Immerhin lässt sich in den letzten Jahren beobachten, dass IPv4 und IPv6 im öffentlichen Raum und in einer wachsenden Anzahl von Firmennetzwerken koexistieren.

IPv6 Header

1. Byte		2. Byte		3. Byte	4. Byte
Version	Traffic Class	Flow Label			
Payload Length			Next Header	Hop Limit	
Source Address					
Destination Address					

Version

Gibt die Versionsnummer dieses IP-Headers an. Diese ist im Fall von IPv6 auf 6 gesetzt (binär 0110). Version 5 wurde nur experimentell verwendet.

Traffic Class (Verkehrsklasse)

Die Einteilung von IP-Paketen in verschiedene Verkehrsklassen erlaubt eine Unterstützung für Quality-of-Service-Funktionen.

Flow Label (Datenflussfeld)

Das Flow Label wird ebenfalls für QoS-Dienste in Applikationen benutzt, die Echtzeitdienste anbieten. Pakete mit einem bestimmten Flow Label werden alle gleich behandelt.

Payload Length (Nutzlastlänge)

Die Länge des Paketinhaltes. Aus der verwendeten 16-Bit-Feldbreite ergibt sich somit eine maximale Paketgröße von 64 Kilobytes. Jedoch ist es mit einem IPv6 Extension Header möglich, sogenannte Jumbogramme zu senden. Ipv6-Jumbogramme können bis zu 4 Gigabytes lang sein, da diese Extension Headers eine 32-bittige Nutzlastlänge ermöglichen.

Next Header (nächster Header)

Dieser Eintrag identifiziert den Typ des nächsten verwendeten Headers. Dieses Datenfeld wird zum Beispiel benutzt, um auf vorhandene Extension Headers hinzuweisen.

Hop Limit

Die maximale Anzahl an Hops wird ähnlich wie in IPv4 oder anderen Protokollen angegeben, um ein endloses Kreisen von Paketen in Netzwerken zu verhindern, falls eine fehlerhafte Routerkonfiguration vorliegt. Jeder Router muss das Hop Limit beim Empfang um den Wert 1 verringern. Sinkt das Hop Limit auf 0, muss das Paket verworfen werden und der Absender des Paketes wird per ICMP-Nachricht darüber informiert.

Extension Header

Derzeit gibt es in IPv6 folgende Extension Header:

Hop-by-Hop Options Header	Dient dazu, Informationen zu übertragen, die nur für das Routing von einem zum nächsten Router interessant sind und anschließend verworfen werden. Hier befindet sich auch die Möglichkeit, auf Jumbogramme hinzuweisen.
Routing Header	Der Routing Header erlaubt es, einem Paket einen vorgegebenen Routingweg vorzuschreiben. Es kann eine Liste von 1 bis 127 IP-Adressen angegeben werden, die dieses Paket auf seinem Weg zum Empfänger passieren muss.
Fragment Header	Der Fragment Header regelt die Fragmentierung und die Reassemblierung von Paketen, wenn diese aufgrund einer kleinen MTU (Maximum Transmission Unit) auf der Strecke ansonsten nicht weitergeleitet werden könnten.
Destination Options Header	Dieser Header transportiert Optionen, die das Ziel auswerten sollte.
Authentication Header	Der Authentication Header sorgt durch eine digitale Signatur dafür, dass der Empfänger des Paketes die Gewissheit hat, unveränderte Originaldaten vom echten Absender erhalten zu haben. Dieser Header wurde, um die Funktionalität auch in IPv4 zur Verfügung stellen zu können, im Rahmen des IPSec Standards entsprechend adaptiert.
Encapsulating Security Payload Header	Der ESP Header verschlüsselt die transportierten Inhalte und sorgt somit dafür, dass nur der Absender und der Empfänger die Nutzdaten einsehen können. Auch dieser Header wurde im Zuge von IPSec für IPv4 adaptiert.

IPv6-Adressen

Gleichzeitig mit der deutlich längeren Adresse in IPv6 ändert sich auch die Darstellungsweise. Anstatt der auf IPv4 gewohnten gepunkteten Dezimalschreibweise (wie zum Beispiel 192.168.0.1) wird die Doppelpunkt-Hexadezimal-Notation verwendet. Im englischen Sprachraum wird diese Schreibweise als „colon hex“ bezeichnet.

Jeweils 2 Bytes werden zu einem 4-stelligen Block hexadezimaler Werte zusammengefasst, die durch einen Doppelpunkt getrennt sind. Eine IPv6-Adresse sieht zum Beispiel so aus:

2001:0db8:85a3:08d3:1319:8a2e:0005:7344

Führende Nullen eines Blockes dürfen zur Verkürzung der Schreibweise weggelassen werden. Das ergibt für die obige Adresse:

2001:db8:85a3:8d3:1319:8a2e:5:7344

In Adressen, in denen zusammenhängende Blöcke vorkommen, die komplett aus Nullen bestehen, dürfen die „Nuller-Blöcke“ **einmalig** durch zwei Doppelpunkte (::) ersetzt werden.

Aus der Beispieldresse 2001:0db8:0000:0000:0000:1428:57ab wird verkürzt
2001:0db8::1428:57ab.

Eine mehrfache Verwendung von :: ist nicht eindeutig und aus diesem Grund unzulässig. So lässt sich z. B. nicht eindeutig rekonstruieren, welche Adresse mit der Angabe 1 :: 4 :: F gemeint ist.

Eine Aufteilung in verschiedene Netzwerkklassen, wie sie aus den Anfangszeiten von IPv4 bekannt ist, gibt es in IPv6 nicht mehr. Üblicherweise stellen die ersten 64 Bit die Netzwerk-ID und die letzten 64 Bit die Host-ID dar. Es gibt jedoch, ähnlich wie in IPv4, spezielle Adressen mit Sonderfunktionen:

- ✓ :: oder ::0 ist eine undefinierte IPv6 Adresse – entspricht der IPv4-Adresse 0.0.0.0
- ✓ ::1 ist das lokale Interface – entspricht der IPv4-Adresse 127.0.0.1 (Loopbackadresse)
- ✓ ff... stellen Multicast-Adressen dar
- ✓ 0:0:0:0:0:ffff:: sind „IPv4 mapped“ IPv6-Adressen. Die letzten 32 Bit enthalten die IPv4-Adressen. Auf diese Weise können geeignete Router zwischen IPv4 und IPv6 konvertieren und beide Welten miteinander verbinden.
- ✓ fc00:: bis fdfff:: steht für eine Unique Local Address (ULA). Adressen mit dem Präfix fc sind global zugewiesene, eindeutige Adressen, während Adressen mit dem Präfix fd lokal generierte ULAs anzeigen. Auf das Präfix folgen die eindeutige Site-ID (40 bit) für den Standort und die Subnet-ID (16 bit). Die letzten 64 Bit sind die Host-ID. Dieses System tritt die funktionale Nachfolge der privaten IP-Adressen aus dem IPv4-Bereich an. Im Gegensatz zum IPv4 sind diese IP-Adressen aus den öffentlichen Netzwerken ohne NAT-Probleme direkt adressierbar.

URL-Schreibweise von IPv6-Adressen

Bei IPv4 werden URL-Adressen mit Portangabe in der folgenden Schreibweise angegeben:

`http://192.168.0.1:8080`

Diese Schreibweise lässt sich für IPv6 nicht übernehmen, da ein Doppelpunkt als Abgrenzungszeichen zwischen Adresse und Portnummer interpretiert wird. Bei IPv6 wird die Adresse in eckige Klammern gesetzt und die Portnummer anschließend durch Doppelpunkt getrennt hinzugefügt:

`http://[2001:0db8::1428:57ab]:8080`

Auf diese Weise werden die Doppelpunkte nicht fehlinterpretiert, sondern als Teil der Adresse akzeptiert.

5.7 IPv6-Übergangsmechanismen

In den USA und Europa ist man bei ausgebauter Infrastruktur hervorragend mit IPv4-Adressen ausgestattet, der Umstieg auf IPv6 erscheint nicht so zwingend. In anderen Regionen der Welt (Asien, Afrika), in denen der Bedarf an IP-Adressen sprunghaft gestiegen ist, weil die IPv4-Adressen nicht mehr ausreichen und sich die Infrastruktur teilweise erst entwickelt, sieht das anders aus. Netzbetreiber und Provider betreiben ihre Server ausschließlich mit IPv6 („IPv6-only“).

Eine Angleichung bzw. der Wechsel auf IPv6 erfolgt schleppend und über Jahrzehnte. Solange IPv4 und IPv6 nebeneinander existieren und parallel betrieben werden, werden Mechanismen verwendet, um IPv6-Kommunikation in einer IPv4-Welt – oder umgekehrt – zu ermöglichen und zu regeln (IPv6-Übergangsmechanismus; IPv6 transition mechanism). In der Regel werden also keine neuen Leitungen, Geräte oder Netzwerkkarten benötigt.

Generell sollten alle Übergangsmechanismen als technische Zwischenlösungen auf dem Weg zur ausschließlichen Verwendung von IPv6 gesehen werden. Grundlegend werden folgende Mechanismen unterschieden:

- ✓ *Parallelbetrieb von IPv4 und IPv6 (Dual-Stack)*
Allen beteiligte Schnittstellen werden IPv4- und IPv6-Adressen und -Routinginformationen zugewiesen. Die Kommunikation kann somit unabhängig über beide Protokolle erfolgen.

✓ **Tunnelmechanismen**

Tunnelmechanismen werden auf dem Weg zum IPv6-Internet dazu verwendet, um Router zu überbrücken, die IPv6 nicht weiterleiten. Dabei werden IPv6-Datenpakete direkt in IPv4-Pakete gepackt, genauer in die Nutzdaten von IPv4-Paketen. In einem speziellen Tunnelserver auf der empfangenden Seite werden die IPv6-Pakete herausgelöst und mittels IPv6-Routing übertragen. Der Rückweg funktioniert analog.

✓ **Übersetzungsverfahren**

Ist IPv6 nicht aktiviert oder stehen nicht genügend IPv4-Adressen zur Verfügung, kann eine Übersetzung zwischen beiden Protokollen mittels Verfahren wie Transport Relay Translation (TRT, siehe RFC 3142) erfolgen.

Folgende Übergangsmechanismen stehen zur Verfügung:

- ✓ **4in6:** IPv4 in IPv6-Tunnelung
- ✓ **6in4:** IPv6 in IPv4-Tunnelung
- ✓ **6over4:** Transport von IPv6-Datenpaketen zwischen Dual-Stack Knoten über ein IPv4-Netzwerk
- ✓ **6to4:** Transport von IPv6-Datenpaketen über ein IPv4-Netzwerk
- ✓ **AYIYA:** Anything In Anything
- ✓ **Dual-Stack:** Netzknoten mit IPv4 und IPv6 im Parallelbetrieb
- ✓ **Dual-Stack Lite:** Wie Dual-Stack, jedoch mit globaler IPv6 und Carrier-NAT IPv4
- ✓ **6rd:** IPv6 rapid deployment
- ✓ **ISATAP:** Intra-Site Automatic Tunnel Addressing Protocol
- ✓ **Teredo:** Kapselung von IPv6-Datenpaketen in IPv4-UDP-Datenpaketen
- ✓ **NAT64:** Übersetzung von IPv4-Adressen in IPv6-Adressen
- ✓ **464XLAT:** Übersetzung von IPv4- in IPv6- in IPv4-Adressen
- ✓ **SIIT:** Stateless IP/ICMP Translation

Manche Tunnelmechanismen sind automatisch mit an Bord. Z.B. haben moderne Windows-Betriebssysteme nach Standardinstallation sowohl IPv4 als auch IPv6 aktiviert. Sie erhalten nach Eingabe des Befehls Get-NetAdapter-IncludeHidden in der PowerShell (oder ipconfig in der Eingabeaufforderung) eine Liste installierter Netzwerkadapter. Darunter befinden sich die ISATAP- und Teredoadapter, wie Sie in der folgenden Abbildung sehen:

```
PS C:\Users\Administrator> Get-NetAdapter -IncludeHidden | select Name, InterfaceDescription | Format-List

Name : Ethernet1
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection #2

Name : Ethernet0
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection

Name : LAN-Verbindung* 1
InterfaceDescription : Microsoft Kernel Debug Network Adapter

Name : Reusable ISATAP Interface
{8200DB83-7285-4245-A518-D009C1E3E839}
InterfaceDescription : Microsoft ISATAP Adapter #3

Name : isatap.localdomain
InterfaceDescription : Microsoft ISATAP Adapter

Name : Teredo Tunneling Pseudo-Interface
InterfaceDescription : Teredo Tunneling Pseudo-Interface
```

Windows Server 2016 (PowerShell) Anzeige der Netzwerkadapter, inkl. Teredo- und ISATAP-Adapter

5.8 Übung

Fragen zum Internetprotokoll

Übungsdatei: --

Ergebnisdatei: uebung05.pdf

- In der folgenden Tabelle sehen Sie einige IPv4-Adressen. Ordnen Sie diese ihren Klassen zu und bestimmen Sie, ob es öffentliche oder private Adressen sind (soweit möglich):

Adresse	Klasse	Privat/Öffentlich
20.0.0.1		
10.11.217.133		
230.22.115.213		
192.168.199.218		
129.0.100.211		
172.31.254.253		
223.224.242.232		
169.254.245.69		
254.245.252.225		
255.255.255.255		

- Wie viele Hosts können die folgenden IPv4-Netzwerke jeweils enthalten?

Netzwerkadresse	Subnetzmaske	Anzahl der möglichen Hosts
10.0.0.0	255.0.0.0	
172.19.160.0	255.255.224.0	
159.18.255.248	255.255.255.248	
192.168.4.0	255.255.252.0	
192.168.4.0	255.255.255.192	
117.192.0.0	255.248.0.0	
213.99.182.160	255.255.255.240	
129.128.127.126	255.255.255.254	
169.254.1.0	255.255.0.0	

3. Die folgende Tabelle enthält verschiedene Adressen, manche mit Angabe der Bit-Anzahl, manche mit ausgeschriebenen Subnetzmasken. Ergänzen Sie die jeweils fehlende Information:

Adresse mit Bit-Anzahl	Subnetzmaske
192.168.0.0/24	
10.50.64.0/	255.255.224.0
89.71.16.128/	255.255.255.240
117.215.96.0/20	
150.213.119.208/	255.255.255.248
15.64.0.0/11	
80.88.240.0/	255.255.252.0

4. In den folgenden Tabellen finden Sie einige Adressen unter Angabe der zugehörigen Subnetzmaske. Tragen Sie die zugehörige Netzwerkadresse, den ersten und den letzten Host und die Broadcast-Adresse ein:

Beispiel:

vorgegebene Adresse:	192.168.68.217/20
Netzwerkadresse:	192.168.64.0
erster Host	192.168.64.1
letzter Host	192.168.79.254
Broadcast-Adresse:	192.168.79.255

vorgegebene Adresse:	10.51.219.35/27
Netzwerkadresse:	
erster Host	
letzter Host	
Broadcast-Adresse:	

vorgegebene Adresse:	172.16.66.219/13
Netzwerkadresse:	
erster Host	
letzter Host	
Broadcast-Adresse:	

vorgegebene Adresse:	223.198.252.253/18
Netzwerkadresse:	
erster Host	
letzter Host	
Broadcast-Adresse:	

5. Ihr Netzwerk war bisher auf zwei Gebäude verteilt. Diese hatten die Adressen 192.168.1.0/24 und 192.168.2.0/24. Nach dem Umzug in ein neues Gebäude möchten Sie, dass jeder Computer dieselbe IP-Adresse wie vorher verwendet. Gleichzeitig sollen aber die Netze zusammengelegt werden, um Router zu sparen. Wie lauten die neue Netzwerkadresse und die Subnetzmaske?
6. Sie verwenden das Netzwerk 192.168.5.0/24. Nach einem Umzug in die neuen Firmengebäude müssen Sie den vorhandenen Adressraum so unterteilen, dass für Haus 1 mindestens 100 Hostadressen zur Verfügung stehen und Haus 2 und 3 jeweils mindestens 50 Adressen verwenden können. Den vorgegebenen Adressraum dürfen Sie nicht verlassen.
7. Sie sind Netzwerkadministrator eines multinationalen Konzerns und verantwortlich für die IP-Konfiguration innerhalb Deutschlands. Der Konzern gibt Ihnen den Adressbereich 10.168.0.0/14 vor. Sie müssen für Ihre sechzehn Niederlassungen jeweils eine geeignete Netzwerkadresse festlegen. Dabei müssen so viele Hostadressen wie möglich erhalten bleiben. Definieren Sie die daraus resultierenden Netzwerke mit jeweils erstem und letztem Host:

Netz/Bit	1. Host	letzter Host	Broadcast

8. In der folgenden Tabelle sehen Sie einige IPv6-Adressen. Manche sind ausgeschrieben, andere in Kurzschreibweise. Ergänzen Sie jeweils die alternative Schreibweise. (Möglichlicherweise sind manche Adressen nicht eindeutig. Welche beiden Lesarten gibt es für diese? Ist eine Schreibweise falsch?)

IPv6 ausgeschrieben	IPv6 Kurzschreibweise
fe80:00aa:0016:b001:0151:23f3:005a:0613	
	fe80:127:0:33:5:200:0:1b2c:
2001:0000:0000:0000:f121:2134:a001:1513	
	ff31:1200::2034:1424
	fe82::ff:1:2
0000:0000:0000:ffff:0192:0168:0001:0152	
fe80:0000:0000:0001:0000:0000:0010:1000	
	fe80::55:e::169
	::ffff:192.168.1.172
	::1

9. Finden Sie heraus, worum es sich bei dem vorletzten Eintrag handelt. Was ist hier die Besonderheit?

6 TCP und UDP

In diesem Kapitel erfahren Sie

- ✓ wie TCP und UDP funktionieren
- ✓ wie die Header aufgebaut sind
- ✓ wie ein Three-Way-Handshake funktioniert
- ✓ wie TCP mit Sliding Window Size das Netzwerk effizienter nutzt

Voraussetzungen

- ✓ Verständnis von Netzwerkgrundlagen
- ✓ TCP/IP-Protokoll-Stack
- ✓ Internet-Protokoll IP

6.1 Funktion und Aufbau von TCP und UDP

Transportprotokolle TCP und UDP

Sowohl das Transport Control Protocol (TCP) als auch das User Datagram Protocol (UDP) haben die Aufgabe, innerhalb der TCP/IP-Protokoll-Familie den Transport von Datagrammen zu gewährleisten. Dies bewältigen die beiden Protokolle auf sehr unterschiedliche Art und Weise.

TCP

Das Transport Control Protocol zeichnet sich gegenüber UDP durch eine Reihe komplexer Eigenschaften aus, die den Datagramm-Transport einerseits absichern, andererseits aber auch einen deutlichen Protokoll-Overhead bewirken. Diese sind insbesondere:

- ✓ Verbindungsorientiertheit
- ✓ Zuverlässigkeit
- ✓ Flexibilität in der Bandbreitennutzung

UDP

Demgegenüber wurde das User Datagram Protocol vor allem im Hinblick auf folgende Eigenschaften entwickelt:

- ✓ Geschwindigkeit
- ✓ geringer Overhead
- ✓ Vermeiden redundanter Transportkontrolle

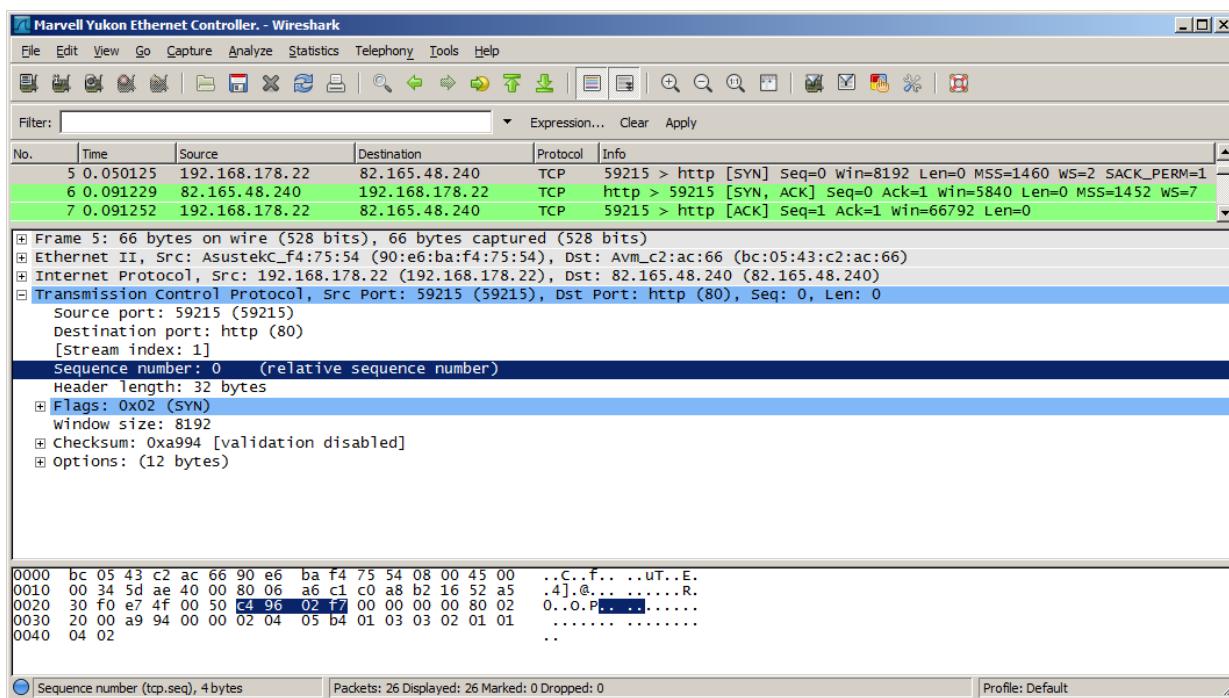
6.2 Arbeitsweise von TCP

Verbindungsorientiertheit

TCP verwendet für den Verbindungsaufbau zwischen zwei kommunizierenden Systemen den Three-Way-Handshake. Dabei handelt es sich um ein Verfahren, bei dem zwei Systeme zu Beginn einer Datenaustauschsequenz eine Synchronisation des TCP-Dienstes durchführen. Dieses Verfahren basiert auf drei Schritten.

- ✓ Im ersten Paket übermittelt der Sender eine Synchronisationsanforderung (SYN) mit einer Sequenznummer "Seq = X".
- ✓ Im zweiten Schritt schickt der Empfänger eine Synchronisationsbestätigung (Acknowledgment, ACK). Dazu wird die empfangene Synchronisationsnummer um 1 erhöht und als "Ack = X + 1" mitgesendet. Gleichzeitig fordert der Empfänger seinerseits eine Synchronisation (SYN) an, die ebenfalls eine Synchronisationsnummer enthält ("Seq = Y").
- ✓ Im dritten und letzten Schritt übermittelt der Sender eine Bestätigung (ACK). Dieses Paket enthält die eigene Synchronisationsnummer ("Seq = X+1") und eine Bestätigungsnummer ("Ack = Y+1").

Um diesen Prozess zu verdeutlichen, wurde ein Three-Way-Handshake mithilfe eines Paketfilters verfolgt und im Folgenden dargestellt. Im oberen Bereich des folgenden Screenshots sind dabei die drei Pakete zwischen dem Sender (192.168.178.22) und dem Empfänger (82.165.48.240), das Kommunikationsprotokoll der höchsten beteiligten Schicht (TCP) sowie die Information über den Inhalt der Pakete abgebildet. Das mittlere Fenster zeigt den Inhalt des oben markierten Paketes und der untere Bereich stellt den Inhalt des Paketes in hexadezimalem Format dar.



TCP-Three-Way-Handshake zwischen zwei Systemen

Der Umgang mit Netzwerküberwachungswerkzeugen wie Paketanalysatoren (auch „Netzwerk-Sniffer“ genannt) ist nicht ganz einfach und erfordert einiges an Übung. Allerdings ist er ein ausgezeichnetes Mittel, um ein tieferes Verständnis für die Netzwerkkommunikation zu entwickeln. Auch bei der Fehlersuche und Ressourcenverwaltung sind solche Werkzeuge hilfreich.



Es muss darauf hingewiesen werden, dass der Einsatz solcher Programme im Firmenumfeld aus Gründen des Datenschutzes nur nach Absprache mit Betriebsleitung und Betriebsrat erfolgen darf. Fragen Sie im Zweifelsfall immer erst einen Vorgesetzten, bevor Sie solche Werkzeuge verwenden, und lassen Sie sich die Genehmigung der Verwendung idealerweise schriftlich bestätigen. Ein verbotener Einsatz von Spionagesoftware kann durchaus arbeitsrechtliche oder sogar strafrechtliche Folgen haben.

Verbindungsabbau

Als verbindungsorientiertes Protokoll muss TCP am Ende eines Kommunikationsstranges auch die Verbindung wieder beenden. Dazu wird mit der letzten Empfangsbestätigung eines Paketes auch eine Anforderung zum Verbindungsabbau übermittelt, die von der Gegenseite bestätigt wird.

Synchronisationsanforderung

Das Paket mit der Synchronisationsanforderung wurde von Port 59215 an den HTTP-Dienst (Port 80) gesendet und hat die relative Sequenznummer 0.

Die Flags, die gesetzt sind, zeigen, dass es sich um das erste Datagramm des Handshakes handelt. Andernfalls würde der Header auch ein Acknowledgment enthalten. So ist nur das Synchronisations-Flag gesetzt.

```

Transmission Control Protocol, Src Port: 59215 (59215), Dst Port: http (80),
Source port: 59215 (59215)
Destination port: http (80)
[Stream index: 1]
Sequence number: 0      (relative sequence number)
Header length: 32 bytes
Flags: 0x02 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0. .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgement: Not set
    .... .... 0... = Push: Not set
    .... ..... 0.. = Reset: Not set
    +.... ..... 1. = Syn: Set
    .... ..... 0 = Fin: Not set
window size: 8192

```

SYN-Request eines TCP-Three-Way-Handshake

SYN/ACK-Datagramm

Im folgenden Datagramm schickt der Empfänger die Antwort auf die Synchronisationsanforderung des Senders. Dazu wird das Acknowledgment Flag gesetzt und die Acknowledgment Number mitgeteilt. Diese Nummer entspricht der um den Wert 1 erhöhten Sequenz-Nummer des vorher empfangenen Datagramms und ist die Sequenz-Nummer, die im nächsten Datagramm erwartet wird. Sollten nun in der Folge Datagramme in der falschen Reihenfolge eintreffen, so erkennt das System dies und kann sie wieder in die richtige Reihenfolge bringen.

```

Transmission Control Protocol, src Port: http (80), Dst Port: 59215 (59215)
Source port: http (80)
Destination port: 59215 (59215)
[Stream index: 1]
Sequence number: 0      (relative sequence number)
Acknowledgement number: 1      (relative ack number)
Header Length: 28 bytes
Flags: 0x12 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ....0 .... .... = Nonce: Not set
    ....0.... .... = Congestion Window Reduced (CWR): Not set
    ....0.... .... = ECN-Echo: Not set
    ....0.... .... = Urgent: Not set
    ....1.... .... = Acknowledgement: Set
    ....0.... .... = Push: Not set
    ....0.... .... = Reset: Not set
    +.... .... .1. = Syn: Set
    .... .... ....0 = Fin: Not set
window size: 5840

```

TCP-Header des zweiten Datagramms eines Three-Way-Handshakes

Gleichzeitig wird auch vom Empfänger eine Synchronisation durchgeführt. Auf diese Weise ist sichergestellt, dass beide Systeme eine lückenlose Informationsübertragung gewährleisten können.

Sicherheit gegen Datenverlust

Mithilfe der Sequenz-Nummern können Datagramme in die korrekte Reihenfolge gebracht werden. Außerdem kann ein Sender erkennen, wenn innerhalb einer bestimmten Zeit kein Acknowledgment für ein gesendetes Datagramm eintrifft. Dieses Datagramm wird dann erneut gesendet, um so Datenverlusten bei der Übermittlung vorzubeugen.

Flusskontrolle

Bei der Informationsübermittlung kann es vorkommen, dass ein Sender einem Empfänger mehr Daten übermittelt, als dieser zu einem gegebenen Zeitpunkt verarbeiten kann. In diesem Fall werden die Daten in einem Puffer zwischengespeichert. Da dieser Puffer nur eine begrenzte Größe hat, kann es zu einem Pufferüberlauf kommen. Um dies zu verhindern, schickt ein System, dessen Verarbeitungspuffer voll ist, ein ECN-Echo (Explicit Congestion Notification Echo, auf Deutsch etwa: ausdrückliche Datenstau-Information). Daraufhin halbiert das sendende System seine Sendegeschwindigkeit, bis das empfangende System durch das CWR-Flag (Congestion Window Reduced, auf Deutsch etwa: reduziertes Übertragungsfenster wegen Datenstau) signalisiert, dass die Übertragung wieder in normaler Geschwindigkeit erfolgen kann.

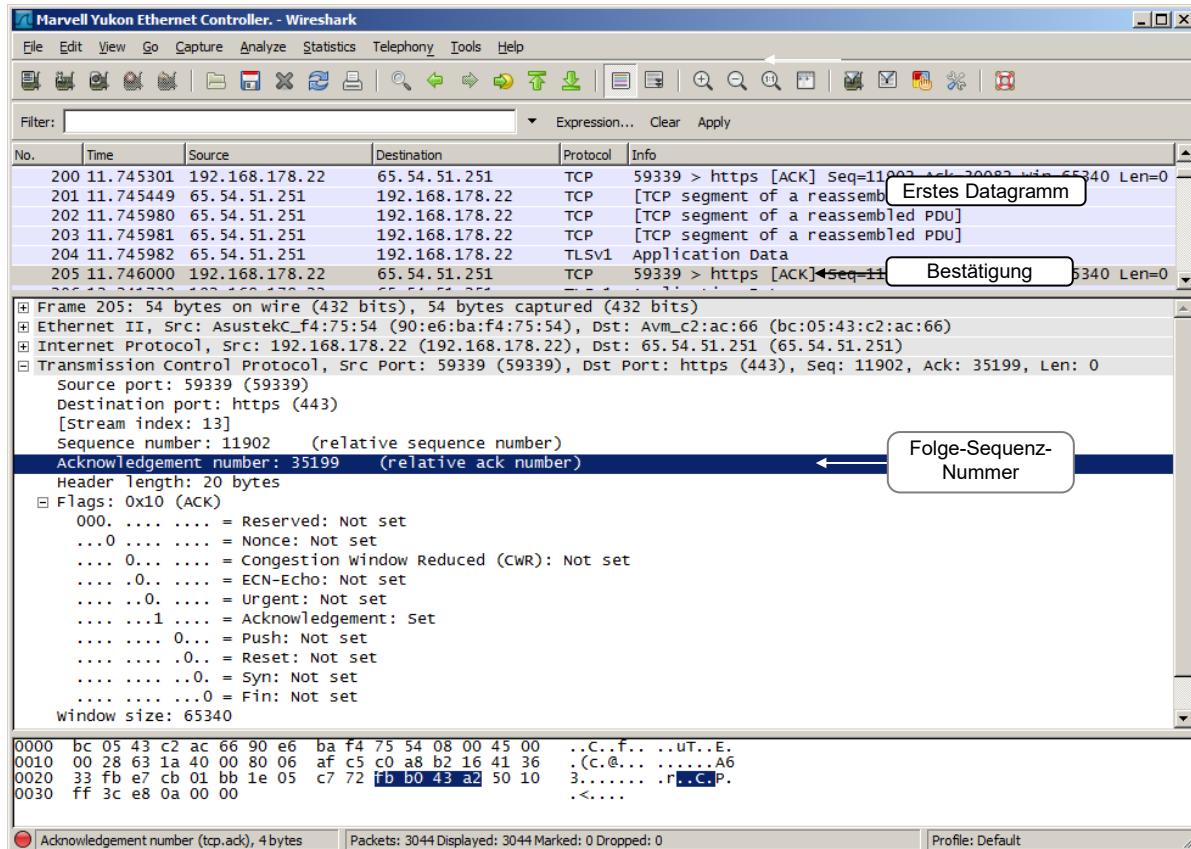
Sliding Window Size

In der Regel wird in einem TCP-Netzwerk für jedes gesendete Datagramm eine Empfangsbestätigung übertragen. Dieses Verhältnis von Nutzdaten und Quittungen belastet die Netzwerkbандbreite deutlich. Durch den Einsatz der Sliding Window Size (fließende Fenstergröße) können aber auch mehrere Datagramme übermittelt werden, bevor eine Empfangsbestätigung erfolgt.

Üblicherweise folgt auf eine gegebene Sequenz-Nummer direkt die erwartete Acknowledgment Number. Sollen jedoch mehrere Datagramme nacheinander gesendet werden, arbeitet das System folgendermaßen:

Nach der Sequenz-Nummer wird die nächste Sequenz-Nummer des Folge-Datagramms angegeben, während die erwartete Acknowledgment Number für den ganzen Datagramm-Strang gleich bleibt. Nur wenn der Empfänger sämtliche Datagramme des Strangs empfängt, sendet er das entsprechende Acknowledgment-Paket.

Dies können Sie in der folgenden Darstellung einer Sendung von vier Datagrammen und einer Empfangsbestätigung ersehen.



Weitere Aufgaben

Neben den transportorientierten Aufgaben ist TCP auch an der Verwaltung des Datenstromes zwischen den Protokollen der Anwendungsschicht und der Netzwerkschicht beteiligt. Dazu gehören die Segmentierung des Datenstromes der Anwendungsschichten, die Pufferung der Daten sowie die Parallelisierung.

Segmentierung

Bei der Segmentierung des Datenstromes werden die Daten der Anwendungsschicht gesammelt und aus ihnen werden die für die Übertragung geeigneten Pakete geschnürt, die dann mit Header versehen an die Netzwerkschicht gereicht werden.

Pufferung

Damit Daten zu Segmenten zusammengefasst werden können und die Segmente nach Erhalt in der richtigen Reihenfolge an die Anwendungsschicht weitergereicht werden können, muss die Transportschicht auf einen eigenen Speicher (Puffer) zugreifen.

Parallelisierung

Wenn eine Anwendung schnellere Datenübertragung benötigt wird, als von einem einzelnen Kanal zur Verfügung gestellt werden kann, ist TCP in der Lage, mehrere Verbindungen gleichzeitig zu nutzen. Durch diese Kanalbündelung können z. B. zeitkritische Datenübertragungen über mehrere ISDN-Kanäle gleichzeitig versendet werden.

Parallelisierung ist kein fester Bestandteil von TCP, sondern ein zusätzliches Feature, das von modernen Betriebssystemen wie den meisten UNIX-Implementierungen oder den aktuellen Microsoft-Betriebssystemen bereitgestellt wird.

6.3 TCP-Header

Beschreibung

Der Header (Protokoll-Kopf) eines TCP-Paketes enthält die zuvor aufgeführten Informationen sowie eine Reihe weiterer optionaler Felder, die bei Bedarf ebenfalls zur Steuerung der Kommunikation eingesetzt werden können. Die Informationen des Headers sind dabei in Blöcken zu 32 Bit (vier Byte) zusammengefasst. Auch wenn ein Header länger wird, beträgt die Länge immer ein Vielfaches von vier Byte. Die eigentlichen Header-Informationen sind dabei zwanzig Byte lang.

Im Folgenden sehen Sie eine schematische Darstellung des Headers.

1. Byte	2. Byte	3. Byte	4. Byte		
Source Port		Destination Port			
Sequence Number					
Acknowledgment Number					
Header Länge	Flags		Fenstergröße		
Prüfsumme		Dringlichkeitszeiger			
Optionen	Auffüllende Nullen bis zum Erreichen eines Vielfachen von 32 Bit				
Daten					

Source Port (16 Bit)

Der Source Port (Quellport) gibt an, von welchem Port auf Schicht 5 die Daten stammen, die (in Datagramme zerlegt) übermittelt werden. Die maximale Länge von zwei Byte entspricht dem Höchstwert eines Ports (65.535).

Destination Port (16 Bit)

Der Destination Port (Zielport) gibt an, an welchen Port auf Schicht 5 die zusammengesetzten Daten der Datagramme weitergereicht werden sollen.

Sequence Number (32 Bit)

Die Sequenz-Nummer dient dazu, die empfangenen Datagramme in die richtige Reihenfolge zu bringen, den Kommunikationsfluss zu kontrollieren und etwaige Fehler zu erkennen.

Acknowledgment Number (32 Bit)

Die Acknowledgment Number (Bestätigungsnummer) gibt an, welche Sequenznummer das empfangende System zur Bestätigung des einwandfreien Erhalts des oder der Datagramme verwenden soll.

Header Length (4 Bit)

Die Längeninformation des Headers gibt an, wie viele 32-Bit-Wörter dieser umfasst. Dies ist notwendig, weil sich die Länge des Headers verändern kann, z. B. wenn zusätzliche Optionen für die Flusskontrolle vereinbart werden müssen.

Flags (12 Bit)

Auch wenn im Moment erst acht Bit = acht Flags definiert sind, ist das System an dieser Stelle bereits für Erweiterungen vorbereitet. So können etwa Sonderformen von TCP für den Satellitentransfer spezielle Informationen enthalten, welche die erhebliche Verzögerung bei globalen Übertragungen berücksichtigen.

Fenstergröße

Hier ist festgelegt, wie viele Bits ein Gerät maximal auf einmal empfangen kann.

Prüfsumme

Anhand der Prüfsumme kann ein Empfänger bestimmen, ob Daten während des Transportes verändert worden sind.

Dringlichkeitszeiger

Wenn bei den Flags eine Kennzeichnung des URGENT-Flags (Dringend-Kennzeichen) vorliegt, werden die Daten nicht in den Puffer gelegt, sondern es wird sofort mit der Verarbeitung begonnen. Der Dringlichkeitszeiger verweist auf das Ende der dringend zu verarbeitenden Daten. Dieser kommt beispielsweise zum Einsatz, wenn bei einer Telnetsitzung einzelne Zeichen an den Kommunikationspartner übertragen werden sollen.

Optionen

Hier ist derzeit in der Standardversion von TCP nur die maximale Größe für TCP-Segmente definiert. Der Rest des 32-Bit-Wortes muss mit Nullen aufgefüllt werden, um so der Längeninformation zu entsprechen.

6.4 UDP

Vorteile und Einsatzgebiete

Das User Datagram Protocol (UDP) stellt ebenfalls Dienste der Transportschicht bereit, ohne allerdings die Fehler-toleranz und die Verbindungsorientiertheit von TCP aufzuweisen. Daher kommt UDP vor allem dann zum Einsatz, wenn Dienste anderer Schichten die Verbindungskontrolle und die Fehlerkorrektur übernehmen.

Der Vorteil von UDP liegt in dem gegenüber TCP deutlich verringerten Overhead. So kommt der Protokoll-Header von UDP mit der festen Größe von acht Byte aus und durch den Wegfall der Acknowledgment-Sendungen wird zusätzliche Bandbreite gespart.

Ein weiterer Vorteil besteht dabei im Wegfall von Verbindungsaufbau und -abbau. Im Vergleich zu TCP werden so drei Pakete für den Three-Way-Handshake und eines für das Sitzungsende eingespart.

Damit ist UDP vor allem für die Übertragungen geeignet, bei denen es zu wenig oder keinen Datenverlusten kommt. Dies gilt insbesondere für Netzwerk-Dienste. So ist etwa bei einem DNS-Request keine Flusskontrolle nötig. Wenn der Server antwortet, ist die Information in einem einzigen Datagramm enthalten, wenn der Server nicht antwortet, wird die Information erneut übertragen.

Ein weiteres Einsatzgebiet von UDP sind reine Datenübertragungen. So wird die Übertragung von NFS-Daten (Network File System, ein verteiltes Netzwerk-Dateisystem von SUN) über UDP abgewickelt. Sollte es zu einem Datenverlust kommen, erledigt NFS auf der Anwendungsschicht die erneute Anforderung der Daten. Hier steht die Geschwindigkeit der reinen Datenübertragung im Vordergrund.

Gegenüberstellung von TCP und UDP

Die folgende Tabelle soll eine Übersicht über die Unterschiede zwischen TCP und UDP geben.

Aufgabe	TCP	UDP
Übertragungs-methode	Verbindungsorientierte Datenübertragung, Three-Way-Handshake, Empfangsbestätigungen, Sequenznummern	So gut wie möglich („As good as possible“), verbindungslos
Datensegment- und Header-Größe	Datensegmentgröße wird dynamisch zwischen den Systemen ausgehandelt, der Header ist zwischen 20 und 28 Byte lang.	Der Header ist immer 8 Byte lang, die Datensegmente können unterschiedlich groß sein.
Flusskontrolle	Pufferverwaltung, Sliding Window Size	Keine

UDP-Header

Aufbau des UDP-Headers:

1. Byte	2. Byte	3. Byte	4. Byte
Source Port		Destination Port	
UDP-Header-Längeninformation		Prüfsumme	
Daten			

Source Port

Die Adresse des Dienstes auf einer höheren Schicht, der die Daten an die Transportschicht gereicht hat, wird in einer 16 Bit langen Port-Nummer angegeben.

Destination Port

Die Adresse des Dienstes auf einer höheren Schicht, an den die Datagramme der Transportschicht gereicht werden sollen, wird in einer 16 Bit langen Port-Nummer angegeben.

UDP-Header-Längeninformation

An dieser Stelle wird angegeben, dass der Header acht Byte lang ist. Diese Information ist an sich überflüssig, sie wurde jedoch aus Gründen der Erweiterbarkeit des Protokolls mit eingeführt.

Prüfsumme

In einer 16 Bit langen Information wird die Prüfsumme für die Daten und den Header geliefert, um Veränderungen der Daten während des Transportes zu erkennen.

6.5 Übung

Fragen zu TCP und UDP

Übungsdatei: --

Ergebnisdatei: uebung06.pdf

1. Warum muss jeder TCP-Datenverkehr mit einem Three-Way-Handshake beginnen?
2. Was passiert, wenn der Sender kein Ack-Paket erhält?
3. Wie reduziert die Sliding Windows Size die Netzwerklast?
4. Wie kann der Einsatz von UDP die Netzwerklast verringern?
5. Welche Rolle spielen die Port-Nummern in den Headern von TCP und UDP?
6. Vergleichen Sie die beiden Dienste FTP und TFTP. Analysieren Sie, welche Transportschicht-Protokolle diesen beiden Diensten zugeordnet sind. Welche Unterschiede ergeben sich daraus? Welcher Dienst ist zu bevorzugen, wenn Sie ein unzuverlässiges Netzwerk verwenden? Welcher Dienst sollte vor allem für die Übertragung von großen Dateien verwendet werden? Welcher Dienst bietet sich an, wenn in einem zuverlässigen Netzwerk kleine Dateien übertragen werden sollen?
7. Der Dienst DNS erlaubt die Verwendung mit TCP und UDP. Vergleichen Sie, wie viele Datagramme transportiert werden müssen, wenn Sie eine Abfrage an einen DNS-Server unter Verwendung von TCP senden würden, und wie viele Datagramme für UDP benötigt werden. Welches Protokoll kommt bei den meisten Implementierungen von DNS zum Einsatz?
8. Weshalb kommt bei den Übertragungen im Internet vorrangig TCP zum Einsatz?
9. In der folgenden Tabelle finden Sie eine Reihe von häufig verwendeten Diensten. Überprüfen Sie, welche davon auf TCP und welche auf UDP zurückgreifen. Denken Sie über Parameter wie Verbindungsaufbau und zu übertragende Datenmenge nach:

Dienst	Transportprotokoll
smtp	
bootps/bootpc	
http	
pop3	
ntp	
snmp	
phone	
pptp	

7 Network Address Translation

In diesem Kapitel erfahren Sie

- ✓ wie NAT funktioniert
- ✓ welche Arten von NAT Sie einsetzen können
- ✓ die Vor- und Nachteile des Einsatzes von NAT

Voraussetzungen

- ✓ Kenntnisse der TCP/IP-Protokollfamilie
- ✓ Kenntnisse im IP-Routing

7.1 Datenaustausch mit dem Internet über NAT

Der Mangel an IP-Adressen (bei IPv4)

In der großen Mehrzahl heutiger Firmennetzwerke besteht die Notwendigkeit, allen Arbeitsstationen einen Zugang zum Internet zu verschaffen. Spätestens ab einer Anzahl von zehn Clientcomputern macht es keinen Sinn mehr, jedes einzelne System mit einem Modem oder ISDN-Adapter auszustatten und so den Zugang zum Internet anzubieten. Da die einzelnen Computer zumeist bereits über ein LAN miteinander verbunden sind, ist es naheliegend, den Zugang über einen Router einzurichten.

In IP-Netzwerken können zunächst nur die Computer direkt miteinander Verbindung aufnehmen, die sich im gleichen logischen Netzwerksegment befinden. Wenn mehrere Segmente miteinander verbunden werden sollen, werden an den Verbindungspunkten Router angeschlossen. Router müssen in der Lage sein, IP-Pakete von einem Netzwerksegment in ein anderes zu leiten, wenn das Paket an einen Netzwerknoten adressiert ist, der nicht im Segment des Absenders liegt. Damit der Router entscheiden kann, ob er das Paket weiterleiten muss oder es ignorieren kann, ist eine eindeutige Adressierung aller Hosts im gesamten Netzwerk notwendig. Sobald über einen Router eine Verbindung zum Internet hergestellt wird, müssen also alle IP-Adressen weltweit eindeutig sein.

Wegen der relativ begrenzten Anzahl an Adressen sind registrierte (öffentliche) IP-Adressen aber ein knappes Wirtschaftsgut und haben einen entsprechend hohen Preis. Aus diesem Grund werden in LANs normalerweise private IP-Adressen aus den von der IANA (Internet Assigned Numbers Authority) nach RFC 1918 reservierten Bereichen 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 vergeben. Im Internet werden Pakete mit Zieladressen aus diesen Bereichen nicht weitergeleitet. Wenn ein Host mit einer solchen Adresse aus dem LAN ein Paket ins Internet schicken würde, könnte das Paket (theoretisch) beim Zielhost ankommen, die Antwort des Empfängers würde allerdings niemals zurückgehen.

Die Idee hinter Network Address Translation

Einem Computer oder Router aus dem LAN, der sich ins Internet einwählt, wird vom Internet Service Provider (ISP) eine von diesem registrierte, öffentliche IP-Adresse für die Dauer der Verbindung zugewiesen. Dieser mit dem Internet und dem LAN verbundene Computer oder der Router müsste nun nur noch dafür sorgen, dass alle ausgehenden Pakete mit der öffentlichen IP-Adresse als Absender versehen werden und die Antworten aus dem Internet wieder an den richtigen Client im LAN gesendet werden. Er muss sich also aus dem IP-Header eines an das Internet gerichteten Paketes die ursprüngliche LAN-Adresse des Absenders merken, durch seine eigene öffentliche Adresse ersetzen und das Paket ins Internet an die Zieladresse weiterleiten. Anschließend muss er bei eingehenden, an ihn gerichteten Datenpaketen aus dem Internet die Zieladresse wieder durch die des LAN-Clients ersetzen.

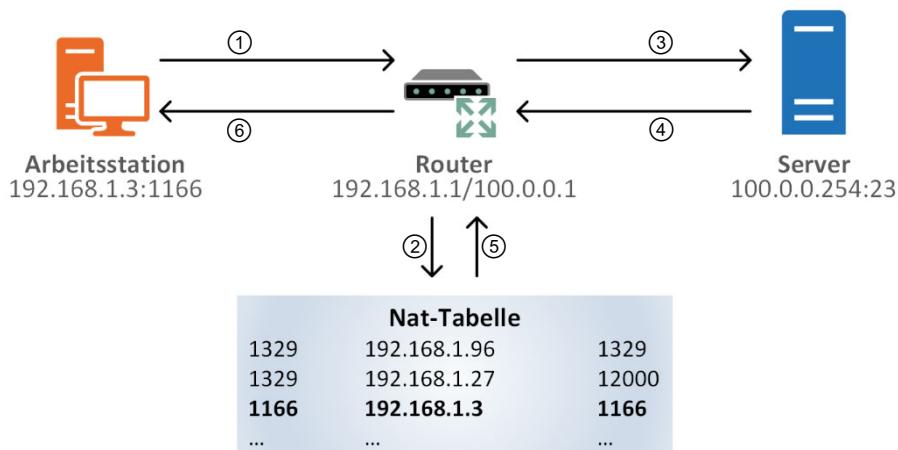
Die gerade beschriebene Funktionalität wird mit Network Address Translation (NAT) bezeichnet und ist für ICMP-Echo-Request und -Response (Ping) bereits ausreichend. Doch was passiert, wenn beispielsweise zwei unterschiedliche LAN-Clients auf ein und denselben Telnet-Server im Internet gleichzeitig zugreifen? Der NAT-Router wüsste nicht, für welchen der beiden Rechner im LAN ein Antwortpaket vom abgefragten Server bestimmt ist. Die Lösung dieses Problems liegt in den sogenannten Ports. Bei der Network Address Port Translation (NAPT) werden nicht nur die IP-Adressen, sondern auch die TCP/UDP-Portnummern übersetzt.

Ports

Ein TCP-Datagramm und ein UDP-Datagramm enthalten unter anderem Quell- und Zielportnummern des Dienstes der oberen Schichten, der die Weiterverarbeitung der Informationen gewährleisten soll. Da unterschiedliche Dienste, wie z. B. FTP, Telnet, SMTP oder HTTP, bei einem per TCP erreichbaren Rechner unter derselben IP-Adresse abgerufen werden können, muss über eine zusätzliche Kennung deutlich gemacht werden, welcher dieser Dienste konkret gewünscht wird. Dies geschieht über sogenannte Portnummern. Während die IP-Adresse eindeutig einen Rechner identifiziert, bestimmt die Portnummer, welcher Dienst auf dem Rechner angesprochen wird. Beide Informationen zusammen (IP-Adresse und Portnummer) werden auch als Socket bezeichnet. Die Ports werden von 0–65535 durchnummeriert. Die Ports unterhalb von 1023 werden als well known Ports bezeichnet.

Ablauf der Adressübersetzung

Zur Veranschaulichung anhand eines praktischen Beispiels finden Sie im Folgenden eine Schemadarstellung und zwei Mitschnitte eines auf dem NAPT-Router laufenden Protokollanalysators. (Hinweis: Die Ziffernkreise ① - ⑥ korrespondieren in allen drei Abbildungen.)



Client-Server-Kommunikation über einen NAPT-Router und dessen NAT-Tabelle

Die Arbeitsstation mit der privaten IP-Adresse 192.168.1.3 möchte eine Telnet-Verbindung zum Server mit der öffentlichen IP-Adresse 100.0.0.254 aufbauen. Dazu sucht sie einen beliebigen unbelegten lokalen Port aus (hier: 1166), auf dem sie die Antworten des Servers erwartet. Durch ihre services-Datei weiß sie, dass sie den Telnet-dienst des Servers über TCP auf seinem Port 23 erreicht. Die Arbeitsstation weiß anhand ihrer IP-Konfiguration (IP-Adresse und Subnetzmaske) auch, dass sie den Server nur über das für sie zuständige Gateway 192.168.1.1 erreichen kann. Also wird mit TCP und IP ein Paket mit der Quell-Socket-Adresse 192.168.1.3:1166 und der Ziel-Socket-Adresse 100.0.0.254:23 über das Ethernet an die MAC-Adresse des Routers geschickt ①.

Socketwahl auf dem Router

Der Router sieht in seiner NAT-Tabelle nach, ob bereits eine solche Quell-Socket-Adresse existiert ②. Ist dies der Fall, wird ermittelt, welche Portnummer er seiner öffentlichen Schnittstelle dafür belegt hat. Ist dagegen noch kein passender Eintrag vorhanden, sucht der Router einen unbelegten Port auf seiner öffentlichen Schnittstelle und belegt diesen. Wenn er die Portnummer noch nicht belegt hat, die der Client verwendet (in diesem Beispiel 1166), wird er diese für die Kommunikation belegen.

In der NAT-Tabelle wird ein Eintrag (Mapping) mit der privaten IP-Adresse und der Portnummer des Absenders sowie der öffentlichen Portnummer des Routers angelegt. Da im Beispiel der öffentliche Port 1166 noch frei ist, kann er ihn belegen und die Portnummer im ausgehenden IP-Paket unverändert lassen. Im ausgehenden Paket wird vor dem Versenden die in der NAT-Tabelle abgelegte, private Quell-Socket-Adresse durch die öffentliche Adresse (100.0.0.1:1166) ersetzt ③. Die TCP- ⑦ und die IP-Prüfsummen des Paketes werden ebenfalls aktualisiert.

Der Server 100.0.0.254 erhält das Paket auf seinem TCP-Port 23 und möchte die Telnet-Verbindung mit dem Router aufbauen (da dieser aus seiner Sicht Absender des Verbindungswunsches ist). Der Server schickt sein Antwortpaket also an die Socket 100.0.0.1:1166 ④.

Der NAT-Router empfängt das Paket und sucht dessen Ziel-Port-Adresse in seiner NAT-Tabelle ⑤. Ist diese Adresse nicht in der NAT-Tabelle enthalten und auch nicht für eigene Verbindungen des Routers belegt, wird das Paket verworfen. Ist diese Adresse in der NAT-Tabelle enthalten, findet eine Rückübersetzung statt. In diesem Beispiel werden also die Ziel-Socket-Adresse 100.0.0.1:1166 durch 192.168.1.3:1166 ersetzt und die entsprechenden Prüfsummen aktualisiert ⑥. Das Paket wird anschließend an das interne Netz weitergeleitet und der Host 192.168.1.3 erhält die vom Telnetserver erwartete Antwort auf Port 1166.

Time .	Source	Src port	Destination	Dest port	Protocol	
19:21:32.4580	192.168.1.3	1166	100.0.0.254	23	TCP	①
19:21:32.4594	100.0.0.254	23	192.168.1.3	1166	TCP	⑥

Frame 39 (62 on wire, 62 captured)

Ethernet II

Internet Protocol, Src Addr: xppro1.matrix.de (192.168.1.3), Dst Addr: NT4W (100.0.0.254)

Transmission Control Protocol, Src Port: 1166 (1166), Dst Port: telnet (23), Seq: 2496184586, Source port: 1166 (1166)

Destination port: telnet (23)

Sequence number: 2496184586

Header length: 28 bytes

Flags: 0x0002 (SYN)

window size: 64240

Checksum: 0x070d (correct)

Options: (8 bytes) ⑦

0000 00 e0 7d d2 07 12 00 06 7b 01 46 84 08 00 45 00 ..}.... {.F...E.
0010 00 30 b7 e6 40 00 80 06 1c 38 c0 a8 01 03 64 00 .0..@... .8....d.
0020 00 fe 04 8e 00 17 94 c8 c1 0a 00 00 00 00 70 02p.
0030 fa f0 07 0d 00 00 02 04 05 b4 01 01 04 02

Analyse der beiden IP-Pakete Dienstanfrage und Serverantwort im internen LAN

Time .	Source	Src port	Destination	Dest port	Protocol	
19:21:32.4592	100.0.0.1	1166	100.0.0.254	23	TCP	③
19:21:32.4597	100.0.0.254	23	100.0.0.1	1166	TCP	④

Frame 4 (62 on wire, 62 captured)

Ethernet II

Internet Protocol, Src Addr: 100.0.0.1 (100.0.0.1), Dst Addr: 100.0.0.254 (100.0.0.254)

Transmission Control Protocol, Src Port: 1166 (1166), Dst Port: telnet (23), Seq: 2496184586, Source port: 1166 (1166)

Destination port: telnet (23)

Sequence number: 2496184586

Header length: 28 bytes

Flags: 0x0002 (SYN)

window size: 64240

Checksum: 0x64b7 (correct)

Options: (8 bytes)

0000 00 aa 00 ac 85 61 00 e0 7d 8a 1a cd 08 00 45 00a... }....E.
0010 00 30 b7 e6 40 00 7f 06 7a e2 64 00 00 01 64 00 :0..@.. z.d...d.
0020 00 fe 04 8e 00 17 94 c8 c1 0a 00 00 00 00 70 02p.
0030 fa f0 64 b7 00 00 02 04 05 b4 01 01 04 02 ..d.....

Analyse der beiden IP-Pakete Dienstanfrage und Serverantwort im externen Netz

Transparenz

Die Adressübersetzung ist in diesem Beispiel für die beteiligten Netzwerkendknoten völlig transparent. Der NAT-Router stellt sich für den Client als ganz normaler Router dar. Für den Telnetserver ist der NAT-Router ein ganz normaler Client. Das heißt, sowohl der Host im privaten Netzwerksegment als auch der Host im externen Netzwerk können ohne spezielle Konfiguration störungsfrei miteinander kommunizieren. Die Hosts im privaten Netz sind vom externen Netz aus nicht sichtbar und somit gegen Angriffe aus dem externen Netz wenigstens grundlegend geschützt.

Sollte eine Verbindung nicht explizit durch einen Three-Way-Handshake wieder beendet werden, kann ein NAT im Allgemeinen nicht wissen, wann eine Verbindung beendet ist. Deshalb wird in den NAT-Tabelleneinträgen ein Zeitstempel der letzten Benutzung gesetzt. Nach einstellbarer Zeit wird die Session als beendet angesehen, und der Eintrag wird entfernt (Leerlaufzeit, z. B. TCP 24 h, UDP 5 min). Ein anderer Ansatz ist, erst bei Bedarf den Eintrag mit der längsten Leerlaufzeit zu entfernen.

NETENT - Sitzungszuordnungstabelle für Netzwerkadressübersetzung								
Protokoll	Richtung	Private Adresse	Privater Port	Öffentliche Adresse	Öffentlicher Port	Remoteadresse	Remoteport	Leerlaufzeit
TCP	Ausgehend	192.168.1.3	1.257	100.0.0.1	1.257	100.0.0.254	445	3.086
TCP	Ausgehend	192.168.1.3	1.290	100.0.0.1	1.290	100.0.0.254	23	7

NAPT-Tabelle mit zwei eingetragenen Mappings

Mappings können nicht nur dynamisch (bei Verbindungsaufbau) in die Tabelle eingetragen werden. Ein Administrator kann von Hand statische Einträge vornehmen.



7.2 Praktische Einsatzgebiete

Arten von NAT

Traditional NAT (Outbound NAT, Source NAT)	<p>Verbindungen können nur von Hosts des internen Netzes initiiert werden. Im internen Netz dürfen nur private Adressen nach RFC 1918 verwendet werden. Die Übersetzung der Adressen erfolgt nach dem Routing, da NAT auf der externen Schnittstelle aufsetzt. Man unterscheidet Basic NAT und NAPT.</p> <p>Basic NAT: Je externer Adresse ist maximal eine interne Adresse zugeordnet; Zuordnung n interner IP-Adressen zu m externen Adressen ($n:m$-NAT). Maximal m interne Clients können Verbindungen in das externe Netz aufbauen.</p> <p>Bei Outbound-Paketen wird die Quell-IP-Adresse, bei Inbound-Paketen die Ziel-IP-Adresse angepasst. IP-, TCP-, UDP- und ICMP-Headerchecksum werden immer angepasst.</p> <p>NAPT (IP-Masquerading, NAT mit Single User Account Feature (SUA)): Zusätzlich werden Quell- und Zielport und ICMP-Queries angepasst. Die einzige externe Adresse kann mehreren internen Adressen zugeordnet sein ($n:1$-NAT).</p> <p>Basic NAT und NAPT können kombiniert werden. Dies ermöglicht die Verwendung mehrerer öffentlicher Adressen und die gleichzeitige Verwendung einer öffentlichen Adresse mit mehreren internen Adressen.</p>
Destination NAT (Inbound NAT, Load Share NAT (LSNAT))	<p>Externe Hosts können Verbindungen ins interne Netz initiieren. Im Gegensatz zu Source NAT werden bei Destination NAT die Adressen vor dem Routing geändert, da auch hier NAT auf der externen Schnittstelle aufsetzt.</p> <p>Eine Einsatzmöglichkeit ist das Veröffentlichen von Servern (exposed server) aus dem internen Netzwerk. Anfragen von extern werden auf eine interne Adresse (Port redirection, forwarding, mapping) übersetzt. Mehrere vom externen Netz kommende Verbindungsanfragen können damit auch zum Lastenausgleich auf mehrere Server oder Proxies verteilt werden (Load Sharing, LSNAT).</p>
Bi-directional NAT (Two-Way NAT)	<p>Verbindungen können auch von Hosts des externen Netzes aufgebaut werden. Dazu wird auf dem NAT-Router ein DNS-ALG (Application Layer Gateway) benötigt, das DNS-Abfragen und -Antworten mithilfe der NAT-Tabelle anpasst. Voraussetzung ist, dass der DNS-Namensraum für interne und externe Netzwerke eindeutig ist.</p>
Twice NAT	<p>In jedem Paket werden Quell- und Zieladresse geändert. Twice NAT kann eine Lösung sein, wenn im internen Netz öffentliche IP-Adressen verwendet werden, die durch eine andere Organisation im externen Netz offiziell registriert sind. Dies kann z. B. durch einen Providerwechsel passieren, wenn die vom alten Provider vergebenen öffentlichen Adressen nicht auf den neuen Provider übertragen werden können.</p>
Multihomed NAT	<p>Um Ausfallsicherheit und/oder Lastenausgleich zu schaffen, können ein oder mehrere NAT-Router mit einem oder mehreren Providern verbunden werden. In all diesen Fällen muss gewährleistet werden, dass die einzelnen NAT-Tabellen stets miteinander abgeglichen sind, um eine eindeutige Zuordnung von Quellen und Zielen zu gewährleisten.</p>

NAT wird im Allgemeinen nur auf dem stub border router an der Grenze zwischen LAN/WAN verwendet. Existieren mehrere stub border router mit NAT, müssen diese ihre NAT-Tabellen stets abgleichen. NAT wird häufig auf Internet Access Routern und auf Computern, die den Internetzugang für andere Rechner in einem kleinen LAN anbieten, eingesetzt.

Application Layer Gateways

In der Regel wird NAT als Dienst ausreichen, um den Zugriff auf Daten in externen Netzwerken für die Clients transparent zu übersetzen, es gibt jedoch auch Fälle, in denen NAT alleine dieser Aufgabe nicht gerecht werden kann und entsprechend erweitert werden muss.

Solange die Network Address Translation nur auf den OSI-Schichten 3 und 4 ansetzt, bleiben die mithilfe von TCP/IP transportierten Nutzdaten (payload) unverändert. Sobald ein Protokoll in den Nutzdaten die Quell- oder Ziel-Socket-Adresse überträgt, wird diese vom NAT-Router nicht angepasst und die Kommunikation scheitert.

Ein Beispiel für ein solch problembehaftetes Protokoll ist das File Transfer Protocol (FTP), das Socket-Adressen ASCII-codiert in der payload überträgt. Dies ist aber nicht das einzige Problem von FTP im Zusammenhang mit NAT. FTP verwendet mehrere Verbindungen (control session und data session), und die Portnummer der Datenverbindung kann sogar während der laufenden Kommunikation durch entsprechende Kommandos in der Steuerverbindung geändert werden.

Ein Application Layer Gateway (ALG, auch NAT-Editor genannt) ist eine auf dem NAT laufende Software, die den Datenstrom eines bestimmten Protokolls untersucht und notwendige Anpassungen daran vornimmt. Dazu ist ein Decodieren des Datenstroms mitunter bis auf die Anwendungsschicht des OSI-Modells nötig. In einem solchen Fall spricht man deshalb nicht mehr von einem NAT-Router, sondern von einem NAT-Gateway. Immer wenn ein NAT-Gateway ein Paket bearbeitet, bestimmt es das verwendete Protokoll und bindet die passende ALG-Software (sofern installiert) in den Übersetzungsprozess mit ein.

Application Layer Gateways existieren unter anderem für die folgenden Protokolle:

- ✓ FTP
- ✓ NetBIOS over TCP/IP
- ✓ PPTP (Point-to-point Tunneling Protocol)
- ✓ SMTP (Simple Mail Transfer Protocol)
- ✓ DNS (Domain Name Service)
- ✓ SNMP (Simple Network Management Protocol)
- ✓ Realaudio
- ✓ H.323 (ITU: Packet-based Multimedia Communication Systems, z. B. Internet-Telefonie)
- ✓ SIP (IETF: Session Initiation Protocol, z. B. Internet-Telefonie)
- ✓ RSVP (Resource Reservation Protocol)
- ✓ manche ICMP-Nachrichten (echo, timestamp und redirect messages laufen problemlos über NAT)

Ein Anwendungs-Gateway oder Application Layer Gateway wird in der Regel auch als Firewall eingesetzt. Dazu werden bestimmten Anwendungen nur bestimmte Netzwerkziele erlaubt. Auch die Auswahl der Benutzer, die die Anwendungen einsetzen, kann mit einem Application Layer Gateway sehr fein skaliert werden. Allerdings haben Application Layer Gateways eine recht hohe Verzögerung aufzuweisen, da sie die komplette Sitzung mit dem Client übernehmen müssen.

Nicht unterstützte Protokolle

Einige Protokolle sind praktisch nicht mit NAT zu vereinbaren. Dazu zählen einerseits Protokolle, die Verschlüsselung in den TCP/IP-Headern verwenden und somit z. B. ein Update der Checksums verhindern. (Solange nur die Nutzdaten verschlüsselt sind und kein ALG verwendet werden muss, steht dem Einsatz von NAT nichts im Wege.)

Andererseits gibt es Protokolle, die eine Änderung der Adressen aus konzeptionellen Gründen nicht zulassen. Ein von einem Server im externen Netz ausgestelltes Kerberos-4-Ticket wäre für alle Clients im internen Netz gültig. Aus einem ähnlichen Grund lassen sich keine Sessions zwischen X-Windows-Servern und -Clients über NAT etablieren. In diesen Fällen kann auch der Einsatz von ALGs nicht abhelfen.

Protokolle, die die Verwendung von NAT ausschließen, sind unter anderem:

- ✓ Kerberos V4 und V5
- ✓ X-Windows
- ✓ IPSec (Internet Protocol Security)
- ✓ RSh (Remote Shell) und RLogin (Remote Login)
- ✓ IKE (Internet Key Exchange Protocol)

7.3 Vergleich mit Proxy- und Routerlösungen

Vergleich

Um ein lokales Netz an das Internet anzubinden, können auch Proxies oder Router ohne NAT verwendet werden. Im Folgenden soll kurz auf die Unterschiede eingegangen werden.

Art der Anbindung	Vorteile	Nachteile
NAT	<ul style="list-style-type: none"> ✓ Transparent für Endknoten ✓ Spart registrierte IP-Adressen ✓ Geringer Konfigurationsaufwand, keine Änderungen auf den Hosts nötig ✓ Erhöhung der Sicherheit gegen Angriffe von außen 	<ul style="list-style-type: none"> ✓ Adresskonflikte möglich ✓ Nicht alle Protokolle möglich, insbesondere kein IPSec ✓ Verbindungen können von außen nicht oder nur mit Einschränkungen aufgebaut werden ✓ Gegenüber Proxy-Lösungen erhöhter Netzwerkverkehr, da auch statische Inhalte mehrfach übertragen werden müssen
Router ohne NAT	<ul style="list-style-type: none"> ✓ Höchstmögliche Kompatibilität ✓ Höchstmögliche Geschwindigkeit 	<ul style="list-style-type: none"> ✓ Benötigt registrierte IP-Adressen ✓ Kein Schutz gegen Angriffe ✓ Gegenüber Proxy-Lösungen erhöhter Netzwerkverkehr, da auch statische Inhalte mehrfach übertragen werden müssen
Proxy	<ul style="list-style-type: none"> ✓ Zwischenspeicherung (Caching) möglich ✓ Erhöhung der Sicherheit gegen Angriffe von außen ✓ Zentrale Überwachung und Filterung des Internetverkehrs möglich 	<ul style="list-style-type: none"> ✓ Clients müssen konfiguriert werden ✓ Alle Protokolle müssen extra eingerichtet werden ✓ Nicht alle Protokolle möglich

In der Praxis werden häufig alle drei Techniken miteinander kombiniert.

7.4 Übung

Fragen zu Network Address Translation

Übungsdatei: --

Ergebnisdatei: uebung07.pdf

1. Was ist NAPT und wofür wird es verwendet?
2. Was sind Sockets?
3. Können Sie eine Kerberos-Authentifizierung über NAT durchführen? Warum?
4. Können Sie über einen Proxy einen IPSec-Tunnel aufbauen? Warum?
5. Können Sie über NAT auf einen FTP-Server zugreifen? Warum?
6. Welche Vor- und Nachteile haben Proxy- und NAT-Lösungen für kleine respektive große Netzwerke?

8 Routing

In diesem Kapitel erfahren Sie

- ✓ wofür Routen verwendet werden
- ✓ was statische und dynamische Routen kennzeichnet
- ✓ was interne und externe Routing-Protokolle sind
- ✓ was Distance-Vector-Protokolle und Linkstate-Protokolle sind
- ✓ wie Routing-Schleifen verhindert werden

Voraussetzungen

- ✓ Fundierte IP-Kenntnisse
- ✓ Verständnis logischer Konjunktionen

8.1 Statisches Routing

Routing

Routing ist das Vermitteln von Paketen eines Rechners in ein anderes Netzwerk. Dabei wird das routende System (egal, ob es sich um einen Rechner mit aktiviertem Routing-Dienst oder einen Hardware-Router handelt) von dem sendenden System adressiert, indem dieses mittels seiner Hardware-Adresse angesprochen wird.

Um zu ermitteln, ob ein Router eingesetzt werden muss, um ein Remotesystem anzusprechen, kommt ein logischer UND-Vergleich zum Einsatz. Der gesamte Vorgang soll anhand des folgenden Beispiels erläutert werden:

Ein Rechner hat die IPv4-Adresse 192.168.0.1 und die Subnetzmaske 255.255.255.0. Er soll ein ICMP-Paket an das System mit der Adresse 172.16.0.1 schicken.

Anhand der Subnetzmaske findet das System heraus, ob sich die Zieladresse im eigenen Netzwerksegment befindet. Ist dies der Fall, kann das Paket direkt übermittelt werden. Andernfalls muss das Paket an einen Router übermittelt werden, der den Weg bzw. einen Teil des Weges zum Ziel kennt. Der angesprochene Router ist im einfachsten Fall das in der Routing-Tabelle aufgeführte Gateway.

Routing-Tabelle

In der Routing-Tabelle sind die logischen Verknüpfungen für die Adresszuordnung gespeichert. Hier werden den Adapters die passenden Adressen, Netzwerke, Broadcasts und Routen zugeordnet. In der folgenden Darstellung ist ein Ausdruck der Routing-Tabelle eines Microsoft Windows 2016-Servers mit zwei Netzwerkadapters dargestellt:

```

Administrator: Eingabeaufforderung

C:\Users\Administrator>route print
=====
Schnittstellenliste
 5...00 0c 29 f9 98 a6 .....Intel(R) 82574L Gigabit Network Connection
 6...00 0c 29 f9 98 b0 .....Intel(R) 82574L Gigabit Network Connection #2
 1.....Software Loopback Interface 1
 4...00 00 00 00 00 e0 Microsoft ISATAP Adapter
 2...00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 8...00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel  Netzwerkmaske      Gateway      Schnittstelle Metrik
    0.0.0.0        0.0.0.0   192.168.178.1  192.168.178.127    25
    0.0.0.0        0.0.0.0   192.168.142.2  192.168.142.144    25
    127.0.0.0      255.0.0.0 Auf Verbindung  127.0.0.1       331
    127.0.0.1      255.255.255.255 Auf Verbindung  127.0.0.1       331
 127.255.255.255 255.255.255.255 Auf Verbindung  127.0.0.1       331
  192.168.142.0   255.255.255.0 Auf Verbindung  192.168.142.144    281
 192.168.142.144 255.255.255.255 Auf Verbindung  192.168.142.144    281
 192.168.142.255 255.255.255.255 Auf Verbindung  192.168.142.144    281
  192.168.178.0   255.255.255.0 Auf Verbindung  192.168.178.127    281
 192.168.178.127 255.255.255.255 Auf Verbindung  192.168.178.127    281
 192.168.178.255 255.255.255.255 Auf Verbindung  192.168.178.127    281
    224.0.0.0       240.0.0.0 Auf Verbindung  127.0.0.1       331
    224.0.0.0       240.0.0.0 Auf Verbindung  192.168.142.144    281
    224.0.0.0       240.0.0.0 Auf Verbindung  192.168.178.127    281
 255.255.255.255 255.255.255.255 Auf Verbindung  127.0.0.1       331
 255.255.255.255 255.255.255.255 Auf Verbindung  192.168.142.144    281
 255.255.255.255 255.255.255.255 Auf Verbindung  192.168.178.127    281
=====

Ständige Routen:
  Keine

IPv6-Routentabelle
=====
Aktive Routen:
  If Metrik Netzwerkziel          Gateway
  1   331 ::1/128                 Auf Verbindung
  5   281 fe80::/64               Auf Verbindung
  6   281 fe80::/64               Auf Verbindung
  6   281 fe80::dcdc:5ba8:2eae:58fa/128
                                Auf Verbindung
  5   281 fe80::ecbc:5a88:c95:bb9a/128
                                Auf Verbindung
  1   331 ff00::/8                Auf Verbindung
  5   281 ff00::/8                Auf Verbindung
  6   281 ff00::/8                Auf Verbindung
=====

Ständige Routen:
  Keine

```

Routing-Tabelle eines Microsoft Windows 2016-Servers mit zwei Netzwerkkarten

Schnittstellenliste

```
C:\Users\Administrator>route print
=====
Schnittstellenliste
5...00 0c 29 f9 98 a6 .....Intel(R) 82574L Gigabit Network Connection ①
6...00 0c 29 f9 98 b0 .....Intel(R) 82574L Gigabit Network Connection #2
1........................Software Loopback Interface 1②
4...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter③
2...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
8...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====
```

In der Schnittstellenliste sind die logischen und physikalischen Geräte aufgeführt. Die ersten zwei Zeilen ① verweisen auf die eingebauten Netzwerkkarten. Dabei folgen auf die Schnittstellennummer die MAC-Adresse und schließlich eine Beschreibung des Gerätes. Der folgende Eintrag ② steht für das Loopback-Interface. Hierbei handelt es sich um die interne Bindung des TCP/IP-Stacks. In der vierten und fünften Zeile ③ ist die Bindung der Adapter für die Übermittlung von IPv6 über IPv4 über virtuelle MAC-Adressen zu erkennen.

Aktive Routen

Die aktiven Routen sind nach folgendem Schema dargestellt:

In der ersten Spalte stehen die Zieladressen. Dabei kann es sich um eine Host-, eine Netz- oder um eine Broadcast-Adresse handeln.

In der zweiten Spalte ist die anzulegende Netzwerkmaske dargestellt. Dabei markieren binäre Einsen den Bereich, der nicht geändert werden darf. So steht 192.168.0.255 255.255.255.255 etwa für die Netbios-Broadcast-Adresse im Netz mit der Adresse 192.168.0.0.

Die dritte Spalte gibt Auskunft darüber, ob dieses Ziel über eine eigene Adresse oder ein Fremdsystem angesprochen werden soll. Handelt es sich bei diesem Eintrag um ein Fremdsystem, wird vor dem Senden des Frames die MAC-Adresse des entsprechenden Rechners ermittelt und als MAC-Ziel in den Header des Frames eingetragen.

An der vierten Stelle steht, über welche Adresse der Gateway-Partner angesprochen werden soll. Steht hier ein Remote-Gateway, wird dieses über einen der Netzwerkadapter adressiert, handelt es sich dabei um eine eigene Adresse, wird diese über Loopback angesprochen.

Und in der letzten Spalte steht die Metrik einer Verbindung. Unter Metrik versteht man einen Wert, der einer Route zugeordnet ist. Ein niedriger Wert führt dazu, dass die Route vom System bevorzugt wird, falls zwei Routen zu demselben Ziel existieren. Metriken können etwa Kosten darstellen oder sie weisen auf Faktoren wie Bandbreite, Geschwindigkeit, Zuverlässigkeit, Pfadlänge oder Verzögerung von Routen hin.

Default Gateway und Loopback-Zuordnung

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik
0.0.0.0	0.0.0.0	192.168.178.1	192.168.178.127	25
0.0.0.0	0.0.0.0	192.168.142.2	192.168.142.144	25
127.0.0.0	255.0.0.0	Auf Verbindung	127.0.0.1	331
127.0.0.1	255.255.255.255	Auf Verbindung	127.0.0.1	331
127.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	331

Die ersten zwei Zeilen in diesem Beispiel führen zu dem Netzwerkziel 0.0.0.0 mit der Netzwerkmaske 0.0.0.0. Dieses Ziel ist das Default Gateway. Jedes Bit kann umgeschrieben werden. Wenn nun das System zu einem Ziel keine konkrete Adresse kennt, wird das Paket dem Default Gateway übergeben. Wenn mehrere Default-Gateway-Einträge vorliegen, wird der mit der geringeren Metrik bevorzugt (geringere Kosten).

In den nächsten Zeilen ist das Loopback-Netz der Loopback-Adresse zugeordnet. Dadurch kann das System jedes an das Netz 127.0.0.0 gerichtete Paket über das interne Loopback-Interface (auch als *localhost* bezeichnet) übermitteln. Weiterhin werden hier Loopback-Interface und Loopback-Broadcast definiert.

Adressbindung

Administrator: Eingabeaufforderung					
①	192.168.178.0	255.255.255.0	Auf Verbindung	192.168.178.127	281
②	192.168.178.127	255.255.255.255	Auf Verbindung	192.168.178.127	281
③	192.168.178.255	255.255.255.255	Auf Verbindung	192.168.178.127	281

In der nächsten Zeile ① wird beschrieben, dass das eigene Netz über die eigene Adresse anzusprechen ist. In der darauf folgenden Zeile ② steht die Zuordnung der eigenen Adresse zur Loopback-Adresse. In der nächsten Zeile ③ wird die Broadcast-Adresse für namensauflösende NetBIOS-Broadcasts der eigenen Adresse zugeordnet.

Dezidierte Route zu einem Remote-Netzwerk

```
192.168.111.0 255.255.255.255 192.168.178.222 192.168.178.127      26
```

In der hier abgebildeten Zeile ist eine Netzwerkroute über einen Router explizit angegeben. Um das Netzwerk mit der Adresse 192.168.111.0 anzusprechen, müssen Pakete an den Router mit der Adresse 192.168.178.222 geleitet werden, der über den Adapter 192.168.178.127 angesprochen wird.

Multicast-Bereiche

Administrator: Eingabeaufforderung					
	224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	331
	224.0.0.0	240.0.0.0	Auf Verbindung	192.168.142.144	281
	224.0.0.0	240.0.0.0	Auf Verbindung	192.168.178.127	281

In den Zeilen, die mit der Adresse 224.0.0.0 beginnen, ist die Zuordnung der Multicast-Bereiche zu den diversen Netzwerkadressen vorgenommen. Jedem Netzwerk können somit bei Bedarf eine oder mehrere Multicast-Gruppen zugeordnet werden. Die Identifikation des physikalischen Adapters erfolgt in diesem Fall über die Zuordnung einer zusätzlichen temporären MAC-Adresse. So wird der Multicast-Adresse 224.0.0.1 die MAC-Adresse 0000 0000 0001 zugeordnet.

Broadcastbindung

Administrator: Eingabeaufforderung					
	255.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	331
	255.255.255.255	255.255.255.255	Auf Verbindung	192.168.142.144	281
	255.255.255.255	255.255.255.255	Auf Verbindung	192.168.178.127	281

In den letzten Zeilen findet schließlich die Bindung der Adapter an die Adresse für Broadcasts statt. Broadcasts an die Adresse 255.255.255.255 werden z. B. von DHCP verwendet, um alle DHCP-Server zu adressieren und so eine Netzwerkadresse anzufordern.

Manuelle Routen

Wenn Sie eigene statische Routen zu einem speziellen Netzwerk hinzufügen wollen, geben Sie bei Windows in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `route add <Zielnetzwerk> MASK <Subnetzmase> <Gateway-IP>` ein, z. B. `route ADD 192.168.35.0 MASK 255.255.255.0 192.168.0.2`.

Soll die Route permanent verfügbar bleiben und nicht nur für die aktuelle Sitzung gelten, ergänzen Sie den Befehl um den Parameter `-p`.

Um eine Route aus der Routingtabelle manuell zu entfernen, verwenden Sie den Befehl `route delete <Zielnetzwerk>`, also z. B. `route delete 192.168.35.0`.

Zum Anzeigen verfügbarer Routen verwenden Sie den Befehl `route print` oder `netstat -r`.

8.2 Dynamisches Routing

Einsatzgebiet

In kleinen Netzwerken mag es sinnvoll sein, die Routing-Tabellen von Hand zu editieren, denn dies hat den Vorteil, dass das Netzwerk nicht durch das Versenden von Paketen zur Routenermittlung und -überwachung belastet wird.

Eine veränderte Situation tritt jedoch auf, wenn die Netzwerkumgebung auf häufig wechselnde Gegebenheiten reagieren muss. In Netzwerken, die über mehrere Teilnetze verfügen, welche über redundante Routen angeprochen können werden sollen, benötigt man entsprechende Mechanismen, um das Erstellen und Verwalten der Routen zu automatisieren. Dafür verwendet man Routing-Protokolle.



Routing-Protokolle sind für das Ermitteln der Routen in Netzwerken und ihre Überwachung zuständig. Geroutete Protokolle sind für die eigentliche Übermittlung von Paketen zwischen den Netzwerken (Paket-Switching) zuständig.

Routing-Protokolle und ihre Ziele

Routing-Protokolle verwenden – je nach Einsatzgebiet – unterschiedliche Algorithmen, um die Qualität von Pfaden im Netzwerk zu beschreiben. Dabei sind verschiedene Faktoren zur Beurteilung heranzuziehen.

Routen-optimierung	Ein Routing-Protokoll sollte in der Lage sein, die Qualität von redundanten Routen zu vergleichen, um der schnelleren oder sichereren Route den Vorzug geben zu können oder bei redundanten Routen gleicher Qualität eine Lastenverteilung vornehmen zu können.
Eigenständige Flexibilität	Nur wenn das Routing-Protokoll ohne Eingriffe durch den Administrator selbstständig auf veränderte Bedingungen reagieren kann, lässt es sich zur Automatisierung des Netzwerkbetriebs einsetzen. So muss etwa der Ausfall einer Route vom Protokoll selbstständig erkannt werden und das Finden der Ersatzroute sollte ohne weitere Eingriffe vom System selbst gehandelt werden.
Konvergenz	Ein wichtiger Faktor bei der Beurteilung von Routing-Protokollen ist die Geschwindigkeit, mit der die Informationen der Router in einem Netzwerk konvergieren. Nur wenn innerhalb einer kurzen Zeitspanne alle Router über dieselben Informationen verfügen, kann ein effizienter Netzwerk-Betrieb sichergestellt werden. Sonst könnte es vorkommen, dass Router versuchen, bereits nicht mehr verfügbare Routen zu verwenden oder auf neuere, bessere Routen erst nach längerer Zeit ausweichen.

Effektivität	Ein Routing-Protokoll sollte möglichst wenig Bandbreiten beanspruchen und trotzdem seine eigentlichen Aufgaben schnell und zuverlässig erfüllen. Dazu muss genau abgewogen werden, welche Informationen ein Router an die anderen übermittelt und wie diese darauf reagieren. Replikationsintervalle, Fehlerbehandlungsroutinen und Ressourcenverwaltung spielen hier die zentrale Rolle.
---------------------	---

Arten von Routing-Protokollen

Routing-Protokolle können sich in einer Reihe von Faktoren unterscheiden.

Statische oder dynamische Routen	Statische Routen können von Administratoren angelegt werden, um die Arbeit des Netzwerkes zu beeinflussen. Diese sollten von einem Routing-Protokoll mit berücksichtigt werden. Dem Vorteil der Vorhersehbarkeit und der Bandbreiten-Ersparnis steht hierbei allerdings der Mangel an Flexibilität gegenüber. Dynamische Routing-Protokolle verwenden andererseits nicht unbeträchtliche Ressourcen für die Aktualisierung und Übermittlung der Netzwerk-Informationen.
Flache oder hierarchische Protokolle	<p>Ein Routing-Protokoll kann in der Lage sein, eine hierarchische Router-Struktur abzubilden, indem verschiedene Ebenen erkannt werden und Router sich entsprechend nur um die für sie relevanten Informationen kümmern.</p> <p>So kann das Routen zwischen Standorten, die über ein Backbone verbunden sind, insofern eingegrenzt werden, als dass für die Router innerhalb eines Standortes nur wichtig ist, über welches Gateway sie das Remote-Netzwerk erreichen können. Die Struktur innerhalb des Remote-Netzwerkes dagegen ist ohne Bedeutung. Um dies zu erreichen, finden autonome Gruppen von Routern Verwendung, die für andere Gruppen wie ein einziges Gerät erscheinen.</p> <p>Andererseits sollte in einem einfachen Netzwerk mit flacher Struktur auch auf die Verwaltung von Gruppen verzichtet werden, da diese nur eine zusätzliche Belastung des Systems bewirken. Hier ist es wichtiger, dass jeder Router jedes Nachbargerät kennt, um so Redundanzen schnell und effizient auswerten zu können.</p>
Singlepath-Protokolle versus Multipath-Protokolle	<p>Kann ein Routing-Protokoll zwischen parallelen Pfaden gleicher Wertigkeit (Metrik) zu einem Netzwerk unterscheiden und dynamisch zwischen diesen wechseln, so sprechen wir von einem Multipath-Protokoll. Dies ist unter anderem Voraussetzung für das Multiplexing zur Lastenverteilung.</p> <p>Wird dagegen nur ein "bester" Pfad erkannt, während andere Pfade gleicher Metrik verworfen werden, handelt es sich um ein Singlepath-Protokoll.</p>
Linkstate-Verfahren versus Distance-Vector-Protokolle	<p>Bei den Linkstate-Verfahren benachrichtigt ein Router alle anderen Router im Netzwerk über den Status seiner Schnittstellen. Er informiert also darüber, welche Netzwerke er direkt ansprechen kann. Und indem er die identischen Informationen der anderen Router erhält, kann er sich ein Bild des gesamten Netzwerks aufbauen.</p> <p>Bei Distance-Vector-Protokollen (Entfernungsvektorprotokollen) dagegen übermittelt jeder Router nur den benachbarten Routern seine komplette Routing-Tabelle. So erfahren die Geräte, über welche Nachbar-Router sie welche Netzwerke erreichen können. Zur Bewertung der Routen kommt der Distance-Vector zum Einsatz. Je kürzer eine Route ist, desto geringer ist die Metrik, die ihr zugeordnet wird.</p>
Multiprotokoll-Fähigkeit	<p>Routing-Protokolle können unterschiedliche geroutete Protokolle unterstützen oder auf den Einsatz mit einem einzigen gerouteten Protokoll beschränkt sein. So ist etwa in einem LAN durchaus der Einsatz von IPX/SPX neben TCP/IP möglich und durch Verwendung eines multiprotokollfähigen Routing-Protokolls kann der Aufwand der Routen-Ermittlung gesenkt werden.</p> <p>Im Internet andererseits kommt nur ein Netzwerkprotokoll zum Einsatz. Hier ist es wichtiger, ein spezialisierteres Routing-Protokoll einzusetzen, als eine zusätzliche Unterstützung für zusätzliche Netzwerkprotokolle zur Verfügung zu stellen.</p>

Interne und externe Protokolle	Ist ein Routing-Protokoll vor allem für den Einsatz im LAN gedacht, spricht man von einem internen Routing-Protokoll. Innerhalb eines LANs ist die Netzwerkumgebung von weniger Veränderungen betroffen, als dies in großen, komplexen Umgebungen der Fall ist. Externe Protokolle müssen dagegen in der Lage sein, zwischen verschiedenen Router-Hierarchien zu unterscheiden. Würde etwa im Internet ein Router versuchen, sich einen kompletten Überblick über alle Geräte zu verschaffen, um redundante Routen zu bewerten, käme der Datenverkehr zum Erliegen. Hier ist „weniger“ tatsächlich „mehr“. Ein effizienter Betrieb ist nur durch die Filterung von Informationen möglich.
--------------------------------	--

Gängige Routing-Protokolle im Überblick

Protokoll	Statisch/ Dynamisch	Flach/ Hierarchisch	Singlepath-/ Multipath- Fähigkeit	Linkstate/ Distance- Vector	Multiprotokoll- Fähigkeit	Intern/ Extern
Routing Information- Protokoll Version 1 (RIPv1)	Dynamisch	Flach	Singlepath	Distance- Vector	Multiprotokoll	Intern
Routing Information- Protokoll Version 2 (RIPv2)	Dynamisch	Flach	Multipath	Distance- Vector	Multiprotokoll	Intern
Open Shortest Path First (OSPF)	Dynamisch	Hierarchisch	Multipath	Linkstate	Multiprotokoll	Intern
Border-Gateway-Protokoll (BGP)	Dynamisch	Hierarchisch	Multipath	Speziell	Singleprotokoll	Extern
Exterior-Gateway-Protokoll (EGP)	Dynamisch	Hierarchisch	Multipath	Speziell	Singleprotokoll	Extern
Interior-Gateway-Routing Protokoll (IGRP)	Dynamisch	Flach	Multipath	Distance Vektor	Multiprotokoll	Intern



Da es sich bei BGP und EGP um externe Routing-Protokolle handelt, die über besondere Mechanismen verfügen müssen, um Routing-Tabellen mit derzeit mehr als 100.000 Einträgen zu verwalten, sollen sie hier nur kurz gestreift werden. Sie finden im Internet und in sehr großen WANs Verwendung und benutzen zur Informationsermittlung eine ganze Reihe von speziellen Attributen, um den Aufbau der hierarchischen Gruppen zu automatisieren.

Metrik

Im Netzwerkbereich definiert die Metrik ein numerisches Maß für die Güte einer Verbindung bei Verwendung einer bestimmten Route. Metriken werden immer dann ausgewertet, wenn mehrere Wege zu einem Ziel führen können, um zu ermitteln, welchem Weg der Vorrang gegeben werden soll. Bei der Vergabe von Metriken können verschiedene Faktoren berücksichtigt werden. Die häufigsten sind dabei in der folgenden Tabelle erfasst.

Kosten	Die Kosten einer Verbindung müssen von Administratoren eingetragen werden. So kann etwa einer Standleitung der Vorrang vor einer bei Bedarf aufzubauenden Wählverbindung (Dial-on-Demand Routing, DDR) gegeben werden.
Entfernung	Die Entfernung zwischen Netzwerken wird üblicherweise durch die Anzahl der verarbeitenden Knoten beschrieben (Sprungzähler, Hop Count). Da jede Verarbeitung von Paketen Zeit in Anspruch nimmt, ist die geografische Entfernung hier weniger bedeutend als die logische Entfernung. Hops werden von Systemen ermittelt, indem von einer maximalen Lebensdauer (Time To Live, TTL) bei jeder Verarbeitung 1 abgezogen wird. Je niedriger der Hop-Wert, desto mehr Verarbeitungen haben stattgefunden.

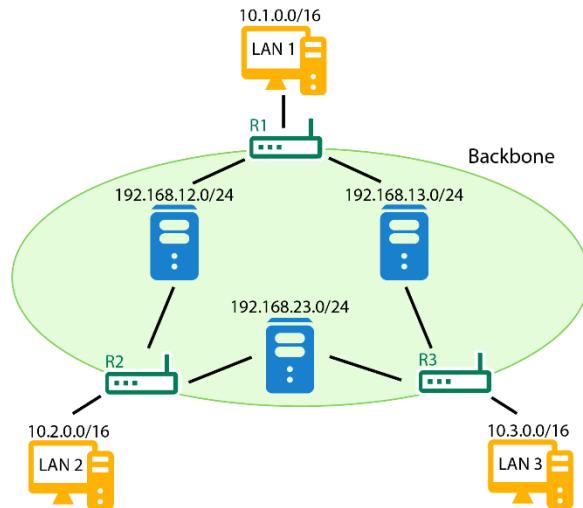
Verzögerung (Delay)	Bei der Verzögerung handelt es sich um die Summe verschiedener Faktoren. So spielen neben der Entfernung auch Bandbreiten, Geschwindigkeit verarbeitender Geräte oder Netzwerklasten eine Rolle. Zusammen ergeben diese einen Zeitwert, der für die Übermittlung eines Paketes benötigt wird.
Bandbreite	Als einer der Teilstücke, die für die Verzögerung ausgewertet werden können, ist die Bandbreite einer Verbindung von Bedeutung. So kann eine langsamere Verbindung, die über mehr Bandbreite verfügt, in letzter Konsequenz zu einer effizienteren Datenübertragung führen. Denn jedes Überschreiten der Bandbreite führt zu einer Warteschlange, die letztendlich den Datentransport bremst.
Ausfallsicherheit (Mean Time Between Failures, MTBF)	Schließlich ist auch noch zu berücksichtigen, wie hoch die Wahrscheinlichkeit eines Leitungsausfalls ist. So kann eine Funkverbindung, auch wenn sie geringere Kosten verursacht als die Wählverbindung, von vielerlei Störungen betroffen werden. Damit ist sie für bestimmte Datenübertragungen nicht geeignet. Die Berücksichtigung der Ausfallsicherheit bedarf wieder eines Eingriffs durch den Administrator. Und jeder statische Eingriff in die Routing-Informationen schränkt die Automatisierbarkeit des Netzwerkes ein.

8.3 Distance-Vector-Protokolle

Funktionsweise

Für die Erklärung der Arbeitsweise von Distance-Vector-Protokollen wird das folgende Beispielnetzwerk verwendet, bei dem die drei Netzwerke 10.X.0.0/16 über drei Router verbunden sind. Diese kommunizieren miteinander über die drei Netzwerke 192.168.X.0/24.

Distance-Vector-Protokolle übermitteln benachbarten Routern ihre gesamte Routing-Tabelle. Diese setzen im Anschluss die Hop Counts (Sprungzähler) um den Wert 1 hoch und vergleichen die Ergebnisse mit der eigenen Routing-Tabelle. Ergibt sich nun ein kürzerer Weg zu einem Netzwerkziel als zuvor in der Tabelle vorhanden, wird der neue Weg als besser erkannt und in die Routing-Tabelle übertragen. Dies ist in dem folgenden Beispiel systematisch dargestellt. Die Tabelle bezieht sich dabei auf das Beispiel-Netzwerk und beschreibt die Übermittlung der Routing-Tabelle von Router R1 zu Router R2, nachdem das Netzwerk 10.1.0.0/16 neu verbunden wurde.



Empfangene Routing-Tabelle +1	Eigene Routing-Tabelle	Ergebnis
10.1.0.0/16 Hop 1	-----	10.1.0.0/16 Hop1 GW [IP-R1]
10.2.0.0/16 Hop 2	10.2.0.0/16 Hop 0 GW [Eigene IP]	10.2.0.0/16 Hop 0 GW [Eigene IP]
10.3.0.0/16 Hop 2	10.3.0.0/16 Hop 1 GW [IP-R3]	10.3.0.0/16 Hop 1 GW [IP-R3]
192.168.12.0/24 Hop 1	192.168.12.0/24 Hop 0 GW [Eigene IP]	192.168.12.0/24 Hop 0 GW [Eigene IP]
192.168.13.0/24 Hop 1	192.168.13.0/24 Hop 1 GW [IP-R3]	192.168.13.0/24 Hop 1 GW [IP-R1] + 192.168.13.0/24 Hop 1 GW [IP-R3]
192.168.23.0/24 Hop 2 + 192.168.23.0/24 Hop 2	192.168.23.0/24 Hop 0 GW [Eigene IP]	192.168.23.0/24 Hop 0 GW [Eigene IP]

Wie in dem Beispiel ersichtlich, sind zu zwei Netzwerkzielen damit Routen hinzugekommen: einmal zum Netz 10.1.0.0/16, das vorher nicht erreichbar war, und einmal zum Netz 192.168.13.0/24, für welches damit eine zweite, gleichwertige Route zur Verfügung steht.

Routing-Schleifen

Fällt die Netzwerkverbindung von Router R1 zu Netz 10.1.0.0 aus, ergibt sich folgende Situation: R2 erfährt von R1, dass dieser Netz 10.1.0.0 nicht erreichen kann. R3 übermittelt, dass er in einer Entfernung von 2 Hops Netz 10.1.0.0 erreichen kann, Router R2 übernimmt diesen Eintrag (der schon veraltet ist) und übermittelt in der Folge an R1, dass er Netz 10.1.0.0 über drei Hops erreichen kann usw. Pakete kreisen nun endlos auf der Verbindung.

Mechanismen zur Vermeidung von Routing-Schleifen

Um Routing-Schleifen zu verhindern, kommt eine Vielzahl unterschiedlicher Mechanismen zum Einsatz, die sich vor allem hinsichtlich der Routing-Protokolle unterscheiden, bei denen sie zum Einsatz kommen.

Maximum Hop Count

Der sogenannte Maximum Hop Count (Maximaler Sprungzähler) soll verhindern, dass ein Paket endlos lange im Netz kreist (Counting-to-Infinity). Bei jeder Verarbeitung eines Paketes durch einen Router wird der Sprungzähler um eins hochgesetzt. Dieser Wert lässt sich verwenden, um die Dauer, die ein Paket bereits durch das Netzwerk transportiert wurde, zu messen. Indem man die maximale Distanz im Netzwerk ermittelt, lässt sich verhindern, dass ein Paket über Schleifen weitertransportiert wird. Dabei wird der Sprungzähler allerdings schon beim Konfigurieren der Routing-Tabelle ausgewertet, sodass der eigentliche Transport der Pakete über Schleifen im Vorfeld verhindert werden kann.

Dies bewirkt jedoch, dass Routingprotokolle wie RIP nur in kleinen Netzwerken verwendet werden können. Der Maximum Hop Count bei RIP ist auf 15 Sprünge limitiert, was den Einsatz in größeren Netzwerken unmöglich macht.

Route Poisoning und Hold Down Timer

Wenn ein Router bemerkt, dass ein Netzwerk nicht mehr erreichbar ist, kann er es als unerreichbar markieren und diese Information im Netzwerk verteilen. Gleichzeitig akzeptiert er für dieses Netzwerkziel keine Aktualisierungen, bis die Router im Netz konvergiert sind. Man spricht bei diesem Verfahren von Route Poisoning (Pfade vergiften).

Route Poisoning kommt in der Regel gemeinsam mit einem Hold Down Timer zum Einsatz. Ein Router, der eine Network-Unreachable-Nachricht (Netzwerk nicht erreichbar) von einem anderen Router erhält, akzeptiert für einen gewissen Zeitraum keine weiteren Aktualisierungen für diese Route, es sei denn, sie kämen vom Gerät, das ursprünglich das Ziel als nicht erreichbar markiert hat.

Split Horizon

Split Horizon (geteilter Horizont) ist ein Verfahren, das verhindert, dass ein Router Routing-Informationen an das Gerät zurückschickt, von dem diese ursprünglich generiert wurden. Kann etwa Router R1 Netzwerk 10.1.0.0 erreichen, wird diese Information von Router R2 nicht zurückübermittelt.

8.4 Linkstate-Protokolle

Funktionsweise

Linkstate-Protokolle verwenden ein grundsätzlich anderes Verfahren, um Routing-Informationen zu übermitteln. Sie übermitteln nicht die komplette Routing-Tabelle, sondern nur die direkt angeschlossenen Netzwerke. Dafür werden diese Informationen aber nicht nur an die benachbarten Geräte übermittelt, sondern an alle Router des Netzwerkes oder der autonomen Verwaltungseinheit. Auf diese Weise lernen alle Router das gesamte Netzwerk kennen und können so die idealen Routen zu jedem Netzwerkziel ermitteln.

Bei diesem Verfahren können Routing-Schleifen nicht auftreten, da die Systeme diese selbstständig erkennen würden. Andererseits werden die Gerätressourcen (Speicher und CPU-Leistung) erheblich belastet. Dies lässt sich am besten durch eine sinnvolle hierarchische Strukturierung des Netzwerkes in autonome Verwaltungseinheiten begrenzen.

So wäre es etwa sinnvoll, dass zwischen Standorten nicht jedes Mal die kompletten Routing-Informationen übermittelt werden, sondern die Standorte als autonome Einheiten definiert werden. So kann die Verarbeitungslast deutlich gesenkt werden.

8.5 Übung

Fragen zum Routing

Übungsdatei: --

Ergebnisdatei: uebung08.pdf

1. Welche Information muss ein Betriebssystem auswerten, um zu erkennen, ob ein Netzwerkziel im eigenen Netz liegt oder über einen Router adressiert werden muss?
2. In einem Ethernet-Segment soll ein Computer, der gerade erst gestartet wurde, ein Paket an sein Default-Gateway übermitteln. Was sendet dieser Computer als Erstes?
3. In der Routing-Tabelle eines Computers finden sich die folgenden zwei Zeilen. Was stellen sie dar?

224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	306
224.0.0.0	240.0.0.0	Auf Verbindung	192.168.1.2	266

4. Was bedeutet diese Zeile?

=====				
Ständige Routen:				
Netzwerkadresse	Netzmaske	Gatewayadresse	Metrik	
0.0.0.0	0.0.0.0	192.168.178.1	Standard	
1.2.3.4	255.255.255.0	192.168.1.100	1	

5. Welcher Router wird bevorzugt?

=====				
Ständige Routen:				
Netzwerkadresse	Netzmaske	Gatewayadresse	Metrik	
0.0.0.0	0.0.0.0	192.168.178.1	Standard	
1.2.3.4	255.255.255.0	192.168.1.100	1	
1.2.3.4	255.255.255.0	192.168.1.200	100	

6. Fügen Sie von Hand einen Eintrag in der Routing-Tabelle Ihres Computers hinzu, der eine dezidierte Route zu dem Netzwerkziel 10.0.0.0/19 über den Router 172.16.55.178 erzeugt.
7. Überprüfen Sie, was mit dem Eintrag geschieht, wenn Sie die Netzwerkschnittstelle deaktivieren und anschließend wieder aktivieren.
8. Wie können Sie den Eintrag dauerhaft hinzufügen?
9. Löschen Sie den Eintrag gezielt.
10. Definieren Sie Konvergenz bei Routingprotokollen.
11. Ist eine höhere oder eine niedrige Metrik besser?
12. Was bedeutet MTBF?
13. Bei welcher Art von Routingprotokollen können Schleifen entstehen?
14. Welche Verfahren kennen Sie, mit denen Schleifen verhindert werden können?
15. Welche Nachteile haben Linkstate-Protokolle?
16. Kreuzen Sie in der folgenden Tabelle an, um welchen Protokoll-Typ es sich jeweils handelt:

Protokoll	Distance-Vector	Linkstate
RIP		
OSPF		
IGRP		

17. Bei welchem Protokoll-Typ ist die Konvergenz niedriger?

9 Namensdienst DNS

In diesem Kapitel erfahren Sie

- ✓ was der Domain Name Service ist
- ✓ was ein FQDN ist
- ✓ wie iterative Namensaauflösungen funktionieren
- ✓ wie DNS-Replikation arbeitet
- ✓ wie D-DNS arbeitet
- ✓ was Round Robin ist und wie Round Robin mit lokalen Netzwerkadressen verfährt

Voraussetzungen

- ✓ Netzwerkgrundlagen
- ✓ TCP/IP

9.1 Konzept

Hierarchisches Konzept

Der Domain Name Service (DNS) ist ein Dienst zur Namens- und Adressauflösung in großen Netzwerken. So wie innerhalb einer Familie der Vorname jede Person ausreichend identifiziert, ist auch ein Rechnername in einer kleinen Umgebung ausreichend, um jeden Rechner anzusprechen.

Muss die Person aber in einem größeren Kontext angesprochen werden, wird dem Vornamen ein Familienname hinzugefügt. Damit lässt sich die Person einer Gruppe zuordnen. Genauso wird der Rechner in einem größeren Netzwerk einer Domäne (= seiner Familie) zugeordnet. Und bei steigender Komplexität der Netzwerkstruktur kann es erforderlich werden, dass diese Organisation wiederum einer anderen Organisation, einem Land oder einem Organisationstyp zugeordnet wird.

Beispiel

FTPServer01.Institut-für-Festkörperphysik.Fraunhofer.de.

Dies entspricht einer Organisation der Informationen nach folgendem Prinzip:

HOSTNAME.SUBDOMAIN.SECONDLEVELDOMAIN.TOLEVELDOMAIN.ROOT

Hostname am Beispiel des FTP-Servers

Der Hostname ist ein innerhalb der Subdomain eindeutiger Name. Auch wenn es weltweit unzählige FTP-Server gibt, kann durch die hierarchische Struktur der DNS-Namen eine eindeutige Zuordnung eines Gerätes zu einer weltweit eindeutigen IP-Adresse vorgenommen werden. Entsprechend ist für die relative Eindeutigkeit des Hostnamens auch die Institution zuständig (in dem vorliegenden Beispiel das Fraunhofer-Institut), die den Namensraum (in dem Beispiel „Fraunhofer“) verwaltet.

Subdomain

Die Subdomain (Unterdomäne) kann dazu verwendet werden, innerhalb eines komplexen Unternehmens Untergruppierungen zu organisieren. Sie ist ein optionaler Namensbestandteil und ihre Verwaltung obliegt ebenfalls der Domain.

Second-Level-Domain/Sublevel Domain

Die Second-Level-Domain (Domäne) entspricht der Basis des Namensraumes. Sie ist die Schnittstelle zwischen dem weltweiten Netz und der Verantwortlichkeit eines Unternehmens. Alles, was innerhalb des Unternehmens-Namensraumes an Namen verwendet wird, muss auch vom Unternehmen verwaltet werden. Die Domänennamen dagegen werden von zentralen Institutionen verwaltet, die als nationale Unterabteilungen von InterNIC (Internet Network Information Center) fungieren.

Der Begriff Subdomain bezeichnet allgemeiner eine Domain, die in der Hierarchie unterhalb einer anderen Domain liegt. Zumeist werden damit Domains mindestens der dritten Ebene bezeichnet. Subdomains werden in der Regel zur besseren logischen Gliederung eines Verwaltungsraums verwendet.

Top-Level-Domain

Die Top-Level-Domain (hier „de“) beschreibt entweder eine nationale Organisationseinheit (zwei Buchstaben) oder stellt die Art eines Unternehmens dar (drei oder mehr Buchstaben). Die Letzteren werden auch als generische Top-Level-Domains bezeichnet. Die Verwaltungsstelle der Top-Level-Domain ist für alle Domänennamen innerhalb ihres Namensraumes zuständig. Die folgende Übersicht erläutert die generischen Top-Level-Domains:

- ✓ *com* internationale Firmen
- ✓ *edu* Forschungseinrichtungen und Hochschulen
- ✓ *gov* US-Regierungseinrichtungen
- ✓ *int* international
- ✓ *mil* militärische Einrichtungen
- ✓ *net* Netzwerk und Netzwerkmanagement-Organisationen
- ✓ *org* nicht kommerzielle Einrichtungen, Vereine etc.
- ✓ *biz* geschäftliche Domains
- ✓ *name* Privatnamen
- ✓ *eu* europäische Domains

Die nationalen Top-Level-Domains entsprechen den ISO-3166-Codes für die nationalen Abkürzungen.

Root

Root (die Wurzel) kann als Punkt am Ende eines jeden DNS-Namens dargestellt werden. Die meisten Anwendungen, die DNS auswerten, ergänzen diesen Punkt jedoch selbstständig. Root ist die Verwaltungsdatenbank der Top-Level-Domains. Die Root-Namensserver halten entsprechend die Adressen der Top-Level-Domain-Namensserver bereit, die wiederum die Adressen für die Domain-Namensserver auflösen können.

FQDN

Der Fully Qualified Domain Name (vollständig qualifizierte Domänenname, FQDN) eines Rechners ist also die weltweit eindeutige Kombination eines Gerätenamens, Angaben zu Subdomains und der Top-Level-Domain, in der diese registriert ist.

DNS-Server

Die Informationen für die FQDNs werden von einer Reihe von Servern verwaltet, die jeweils ihren Teil der DNS-Datenbank halten. Zusätzlich können sie aber aus Gründen der Effizienz auch Kopien von Datenbanken anderer DNS-Server enthalten. An diesen dürfen aber keine Änderungen vorgenommen werden. Eine Ausnahme stellen dabei Active-Directory-integrierte Zonen unter Windows-Server-Betriebssystemen ab Server 2000 dar. Diese werden nach dem Multimaster-Prinzip verwaltet und verwenden die Einzelattributreplikation anstelle der Datenbankdateiübertragung.

9.2 Forward Lookup

Auflösung von DNS-Namen

Möchte ein Client mittels eines DNS-Namens auf ein Remotesystem zugreifen, kann eine von drei Möglichkeiten eintreten:

- ✓ Die Zuordnung des DNS-Namens zur IP-Adresse ist bereits vorgenommen worden und die Information befindet sich im Cache für den DNS-Auflösungsdienst.
- ✓ Der Name kann in der DNS-Host-Datei des Systems aufgelöst werden.
- ✓ Der Client schickt eine Forward-Lookup-Anfrage an einen DNS-Server, der in seiner IP-Konfiguration aufgeführt ist.

DNS-Cache

Der DNS-Cache hält Informationen zu den DNS-Abfragen, die in der letzten Zeit (z. B. der letzten Stunde) vom System erfolgreich vorgenommenen wurden. Diese Informationen lassen sich unter den meisten Systemen nicht beeinflussen. So lässt sich etwa die Größe des DNS-Cache unter Linux-/UNIX-Systemen nicht beschränken. Unter Microsoft-Betriebssystemen kann der Wert für die Gültigkeitsdauer von Namensauflösungen in der Registrierdatenbank beeinflusst werden. Darüber hinaus lässt sich unter Microsoft-Betriebssystemen der komplette lokale DNS-Cache löschen oder anzeigen, indem die Befehle `ipconfig /flushdns` und `ipconfig /displaydns` verwendet werden.

Hosts-Datei

Bei der Hosts-Datei handelt es sich um eine simple Text-Datei, in der IP-Adressen FQDNs zugeordnet sind. Die Datei lässt sich mit einem beliebigen Texteditor erstellen und bearbeiten. Üblicherweise wird sie im Verzeichnis `etc` (z. B. `%Systemroot%\System32\Drivers\etc` bei Microsoft) gespeichert. Wichtig ist allerdings, dass die Hosts-Datei exakt und ohne Dateiendung als „Hosts“ bezeichnet wird.

Das Format eines Eintrags in der Hosts-Datei ist:

`[IP-Adresse] [Mindestens ein Leerzeichen] [FQDN], optional #[Kommentar]`

Beispiel: `192.168.0.1 server01.testnetz.int`



Achten Sie beim Erstellen einer Hosts-Datei unter Microsoft-Betriebssystemen darauf, dass im Explorer die Ansichtsoption für das Ausblenden bekannter Dateinamenserweiterungen deaktiviert ist. Ansonsten kann es Ihnen passieren, dass Sie Ihre Datei `Hosts.txt` oder ähnlich benennen, sodass diese anschließend vom System nicht ausgewertet werden kann.

DNS-Server

In der Regel wird die Auflösung von DNS-Namen nicht durch eine Host-Datei gewährleistet, sondern erfolgt mittels eines DNS-Servers. Damit dieser eine Abfrage bedienen kann, muss auf ihm eine sogenannte Zone eingerichtet werden.

Forward-Lookupzone

The screenshot shows the Windows 2016 DNS Manager interface. On the left, the navigation pane displays the following structure:

- DNS
- 2016-FINAL
 - Forward-Lookupzonen
 - _msdcs.final.test
 - final.test
 - Schulungsnetz.intern
 - Reverse-Lookupzonen
 - 200.168.192.in-addr.arpa
 - 0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e
 - Vertrauenspunkte
 - Bedingte Weiterleitungen

The right pane lists the records for the 'Schulungsnetz.intern' zone:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[17] 2016-final.final.test., ...	Static
(identisch mit übergeordne...	Namenserver (NS)	2016-final.final.test.	Static
Cisco-Schulungsrouter	Host (A)	192.168.200.254	Static
Client-01	Host (A)	192.168.200.21	Static
Client-01	IPv6 Host (AAAA)	fe80:0000:0000:0000:0000:0...	Static
Client-02	Host (A)	192.168.200.22	Static
Client-02	IPv6 Host (AAAA)	fe80:0000:0000:0000:0000:0...	Static
Client-03	Host (A)	192.168.200.23	Static
Client-03	IPv6 Host (AAAA)	fe80:0000:0000:0000:0000:0...	Static
Client-04	Host (A)	192.168.200.24	Static
Client-04	IPv6 Host (AAAA)	fe80:0000:0000:0000:0000:0...	Static
Client-05	Host (A)	192.168.200.25	Static
Client-05	IPv6 Host (AAAA)	fe80:0000:0000:0000:0000:0...	Static

Im Beispiel sehen Sie eine Forward-Lookupzone auf einem Windows 2016 DNS-Server. Hier wurde die Zone *Schulungsnetz.intern* eingerichtet. Sie finden in dieser Zone Einträge für z. B. einen Router und diverse Clientrechner mit ihren zugeordneten IPv4-Host-Einträgen (A) und IPv6-Host-Einträgen (AAAA).

Zonendatei

Eine Zone ist eine als Datenbank gespeicherte Verwaltungseinheit, die in der Verantwortung eines Servers liegt. In der Regel handelt es sich hierbei um eine Domäne, es kann aber auch die Verwaltung einer Subdomäne an einen anderen Server delegiert werden. Wenn Sie Ihre Zonen nicht ins Active Directory integrieren, sondern primäre Standardzonen oder sekundäre Zonen verwenden, lassen sich die Informationen auch als Textdateien mit einem Editor bearbeiten und zwischen Systemen migrieren.

Damit ein Server die Zonendatei auswerten kann, muss diese im DNS-Verzeichnis liegen (bei Windowssystemen ist das der Pfad %systemroot%\System32\dns) und den Namen der Zone mit der Dateityp-Endung .dns tragen. Das folgende Beispiel zeigt eine einfache DNS-Datei:

```

Schulungsnetz.intern.dns - Editor
Datei Bearbeiten Format Ansicht ?

;①Database file Schulungsnetz.intern.dns for Default zone scope in zone Schulungsnetz.intern.
;      Zone version: 17

@          ② IN SOA 2016-final.final.test. hostmaster.final.test. (
                17           ; serial number
                900           ; refresh
                600           ; retry
                86400          ; expire
                3600          ) ; default TTL

;
; Zone NS records
;

@          ③ NS      2016-final.final.test.

;
; Zone records
;

Cisco-Schulungsrouter A      192.168.200.254
Client-01             A      192.168.200.21
                      AAAA fe80::c1
Client-02             A      192.168.200.22
                      AAAA fe80::c2      ④
Client-03             A      192.168.200.23
                      AAAA fe80::c3
Client-04             A      192.168.200.24
                      AAAA fe80::c4
Client-05             A      192.168.200.25
                      AAAA fe80::c5

```

DNS-Datei von „Schulungsnetz.intern“

Unter ① finden Sie die Zoneninformation inklusive der aktuellen Versionsnummer der Zone. Diese dient nur der Übersichtlichkeit bei der Bearbeitung, wird vom System jedoch nicht ausgewertet. Das Semikolon dient in einer DNS-Datei als Kommentarzeichen für den Rest der Zeile.

Unter ② steht die Source of Authority (SOA, autorisierte Quelle) der Name des DNS-Servers, auf dem der Eintrag vorgenommen wurde und der autorisiert für die Zone ist

Der Eintrag für die verantwortliche Person der Zone stellt eine E-Mail-Adresse in DNS-Schreibweise dar, bei der das @ durch einen Punkt ersetzt wird. *hostmaster.testnetz.intern* wird also als *hostmaster@testnetz.intern* interpretiert.

Die Seriennummer (serial number) bezeichnet die Revisionsnummer der Datei, die sich bei jeder Änderung um den Wert eins erhöht. Auf diese Weise ist sichergestellt, dass bei der Replikation andere Server die aktuellen Informationen erhalten.

Das Aktualisierungsintervall (refresh) bezeichnet die Anzahl an Sekunden, die vergehen sollen, bevor ein sekundärer (untergeordneter) DNS-Server versucht, die Zonendaten des Quell-Servers zu replizieren.

Das Wiederholungsintervall (retry) bezeichnet die Anzahl an Sekunden, die vergehen sollen, bevor ein sekundärer Server eine fehlgeschlagene Replikation erneut versucht.

Das Verfallsdatum (expire) gibt an, wann ein sekundärer Server die Daten als veraltet verwerfen soll, falls keine Replikation stattfinden konnte.

Wenn ein Eintrag keine eigene Time To Live (TTL) hat, wird davon ausgegangen, dass der Eintrag mindestens so lange gültig ist, bis die Minimum-TTL abgelaufen ist.

Unter ③ Zone NS Records (Namensserver-Einträge der Zone) steht eine Liste aller Namensserver, die Kopien dieser Zone erhalten dürfen.

Unter ④ schließlich finden Sie eine Liste sämtlicher Einträge, die auf dem System vorgenommen wurden.

Eintragstypen

In der DNS-Datenbank finden sich diverse Typen von Einträgen. Diese können nicht nur Rechner identifizieren, sondern daneben auch Dienste im Netz auffindbar machen. So ist beispielsweise der Betrieb von Windows-Domänen ohne DNS nicht mehr durchführbar, da sämtliche Domänen-dienste über SRV-Einträge (Service, Diensteinträge) in der DNS bereitgehalten werden müssen. Im Folgenden finden Sie eine Tabelle mit einigen wichtigen Eintragstypen, die in DNS-Zonen verwendet werden:

Eintragstyp	Abkürzung	Erklärung
Hostadresse	A	IPv4-Standardeintrag für den Hostnamen eines Rechners
IPv6-Hostadresse	AAAA	IPv6-Standardeintrag für den Hostnamen eines Rechners
ATM-Adresse	ATMA	ATM-Eintrag eines Hosts; ermöglicht es, in ATM-LAN-Emulationsumgebungen (LANE) Rechneradressen mittels DNS aufzulösen
Alias	CNAME	Kanonischer Name eines Rechnernamens (ein Pseudonym, über das das System ebenfalls angesprochen werden kann)
Mailbox	MB	Ordnet eine Domänenmailbox einem Hostnamen zu, auf dem die Mailbox läuft
Mail-Exchanger	MX	Ermöglicht dem angegeben Host des Mail-Exchangers Nachrichtenrouting, wodurch dieser als Mail-Exchanger für einen DNS-Domänen-namen verwendet werden kann
Pointer	PTR	Weist eine Adresse einem bestimmten, bekannten Host zu. Dieser Eintragstyp steht nicht in Forward-Lookup-Zonen, sondern dient dem Reverse Lookup, bei dem der FQDN einer bekannten IP-Adresse ermittelt wird.
Service	SRV	Weist einen Dienst einem FQDN zu

Abfragevorgang

Möchte ein Client auf eine unbekannte Adresse über einen DNS-Namen zugreifen, muss er als Erstes diesen Namen zu einer IP-Adresse auflösen. Dazu wird dem DNS-Server des Clients ein DNS-Query-Request geschickt. Der DNS-Server hat drei Möglichkeiten, die Information für die Antwort zu erlangen:

- ✓ **Cache;** wenn der DNS-Server diese Anfrage bereits einmal bearbeitet hat, kann sich die Antwort noch in seinem Cache befinden.
- ✓ **Zonendatei;** wenn der DNS-Server selbst die Zone verwaltet, kann er den Namen in der Zonendatei suchen und die zugehörige Adresse an den Client übermitteln.
- ✓ **Weiterleitung;** wenn der DNS-Server als weiterleitender Server konfiguriert ist, fragt er einen anderen DNS-Server. Dies wird vor allem dann gemacht, wenn nur einzelne DNS-Server in der Lage sind, auf das Internet zuzugreifen. Er verhält sich diesem gegenüber wie ein ganz normaler Client.
- ✓ **Iterative Abfrage;** um einen Namen in einer fremden Zone zu ermitteln, löst der Server Schritt für Schritt jeden Namensanteil auf.

Weiterleitung

Eine weiterleitende Anfrage wird verwendet, wenn ein DNS-Server selbst keinen Zugang zum Zielnetzwerk besitzt. Er kann dann als stellvertretender Client auftreten und einem DNS-Server mit Verbindung zum Zielnetzwerk die Abfrage übergeben. Dieser kann anschließend eine iterative Abfrage starten. Dadurch, dass nur ein einziger DNS-Server Namen im Zielnetzwerk auflöst, kann die WAN-Anbindung eines Netzwerkes entlastet werden. So können mehrere DNS-Server auf einen zugreifen, der entsprechend mit höherer Wahrscheinlichkeit bereits über die Information verfügt oder zumindest bereits weiß, welcher DNS-Server für die Top-Level-Domäne oder die Sublevel-Domänen verantwortlich ist.

Die iterative Namensauflösung stellt die Standardmethode dar, um Namen außerhalb der eigenen Zone aufzulösen. Daher wird im Folgenden detailliert auf diese Vorgänge eingegangen. Dazu wird die Arbeitsweise beschrieben und anschließend anhand eines Beispiels dargestellt.

Seit Windows Server 2003 ist die dezidierte Weiterleitung von Abfragen an bestimmte Server möglich. So kann etwa in einem Konzern der DNS-Server von Unternehmen A die Abfragen für Unternehmen B an den dafür zuständigen DNS-Server weiterleiten, generelle Abfragen dagegen iterativ auflösen. In großen Netzwerken lässt sich auf diese Weise die Belastung der einzelnen DNS-Server senken.

Iterative Namensauflösung, Theorie

Ein Client, der eine Adresse von einem Server auflösen lassen möchte, stellt diesem eine rekursive Abfrage. Daraufhin führt der Server folgende Operationen durch:

Zonen-Prüfung	Wenn die Adresse zu einer Zone gehört, die der Server verwaltet, wird die Adresse gesucht. Wenn sie aufgelöst werden kann, wird die Information an den Client weitergegeben.
Cache-Prüfung	Wenn die Adresse nicht in einer vom Server verwalteten Zone liegt, wird überprüft, ob im Cache die Information bereits vorliegt, wenn dies der Fall ist, wird die Information übermittelt. Wenn die Adresse nicht im Cache gespeichert ist, überprüft der Server, ob er die Adresse des für die Zone verantwortlichen DNS-Servers bereits kennt. Ist dies der Fall, wird dieser direkt nach der Adresse gefragt.
Iterative Auflösung	Ist der verantwortliche Server nicht bekannt, sendet der Server eine Anfrage nach dem Ziel an einen der Root-Server. Der Root-Server übermittelt die Adressen der für die Top-Level-Domäne verantwortlichen DNS-Server. Der Server fragt bei einem der verantwortlichen Top-Level-Domänen-Server nach dem Ziel. Der Top-Level-Domänen-Server sendet eine Liste der für die Domäne verantwortlichen Server. Der Server fragt bei dem DNS-Server der Zone nach. Der DNS-Server der Ziel-Domäne sendet die Antwort. <i>oder</i> Der DNS-Server sendet die Adresse des Servers, an den die Verwaltung der Unterdomäne delegiert worden ist, und dieser wird gefragt und beantwortet die Anfrage. Der Server übermittelt die Antwort an den Client.

Beispiel für iterative Namensauflösung

Der Client 192.168.178.26 möchte auf www.regensburger-it-akademie.de zugreifen. Dazu muss er eine rekursive DNS-Abfrage an seinen DNS-Server senden. Sein DNS-Server hat die IP-Adresse 192.168.178.22.

Standard DNS-Query-Request

The screenshot shows a Wireshark capture of network traffic. The packet list pane shows 24 DNS requests from various clients to a single destination IP 192.168.178.22. The details pane shows the structure of a DNS query for the domain `www.regensburger-it-akademie.de`. The query field contains the question `www.regensburger-it-akademie.de type A, class IN`. The bytes pane displays the raw hex and ASCII data of the DNS message, including the question section.

No.	Time	Source	Destination	Protocol	Info
9	0.001181	192.168.178.26	192.168.178.22	DNS	Standard query A www.regensburger-it-akademie.de
10	0.001289	192.168.178.22	199.7.83.42	DNS	Standard query A www.regensburger-it-akademie.de
11	0.134113	199.7.83.42	192.168.178.22	DNS	Standard query response
12	0.134229	192.168.178.22	195.243.137.26	DNS	Standard query A www.regensburger-it-akademie.de
13	0.174723	195.243.137.26	192.168.178.22	DNS	Standard query response
14	0.174927	192.168.178.22	194.0.0.53	DNS	Standard query A ns65.1und1.de
15	0.220263	194.0.0.53	192.168.178.22	DNS	Standard query response
16	0.220354	192.168.178.22	195.20.224.98	DNS	Standard query A ns65.1und1.de
17	0.260440	195.20.224.98	192.168.178.22	DNS	Standard query response A 217.160.82.171
18	0.260516	192.168.178.22	217.160.82.171	DNS	Standard query A www.regensburger-it-akademie.de
19	0.300879	217.160.82.171	192.168.178.22	DNS	Standard query response A 82.165.48.240
20	0.300925	192.168.178.22	192.168.178.26	DNS	Standard query response A 82.165.48.240
21	0.301459	192.168.178.26	192.168.178.22	DNS	Standard query AAAA www.regensburger-it-akademie.de
22	0.301542	192.168.178.22	217.160.82.171	DNS	Standard query AAAA www.regensburger-it-akademie.de
23	0.342408	217.160.82.171	192.168.178.22	DNS	Standard query response
24	0.342461	192.168.178.22	192.168.178.26	DNS	Standard query response

Frame 9: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
 Ethernet II, Src: IBM_1e:5c:af (00:14:5e:1e:5c:af), Dst: AsustekC_f4:75:54 (90:e6:ba:f4:75:54)
 Internet Protocol Version 4, Src: 192.168.178.26 (192.168.178.26), Dst: 192.168.178.22 (192.168.178.22)
 User Datagram Protocol, Src Port: 60547 (60547), Dst Port: domain (53)
 Domain Name System (query)
 Response In: 201
 Transaction ID: 0x0005
 Flags: 0x0100 (Standard query)
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.regensburger-it-akademie.de: type A, class IN
 Name: www.regensburger-it-akademie.de
 Type: A (Host address)
 Class: IN (0x0001)

Query-Feld

```

0000  90 e6 ba f4 75 54 00 14  5e 1e 5c af 08 00 45 00  ....uT.. ^.\...E.
0010  00 4d 03 c2 00 00 80 11  51 5c c0 a8 b2 1a c0 a8  .M.....Q>.....
0020  b2 16 ec 83 00 35 00 39  6c 2f 00 05 01 00 00 01  ....5.9 1.....
0030  00 00 00 00 00 00 03 77  77 77 18 72 65 67 65 6e  ....w ww.regen
0040  73 62 75 72 67 65 72 2d  69 74 2d 61 6b 61 64 65  sburger- it-akade
0050  6d 69 65 02 64 65 00 00  01 00 01 .....mie.de... ...

```

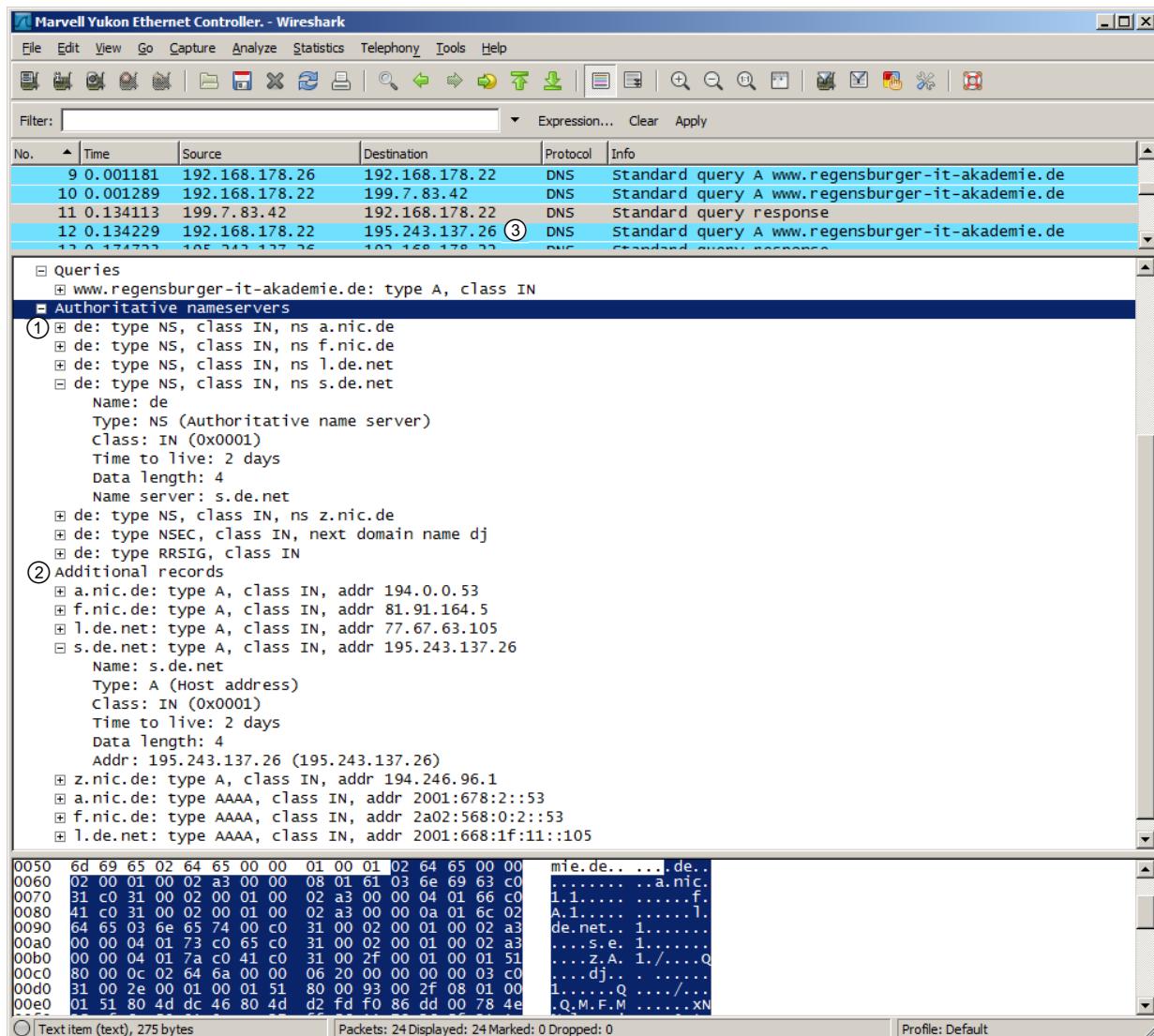
Text item (text), 37 bytes | Packets: 24 Displayed: 24 Marked: 0 Dropped: 0 | Profile: Default

Der Client schickt ein Standard DNS-Query-Request. Dieses beinhaltet im Query-Feld die Frage nach dem Host-eintrag (Type A) für `www.regensburger-it-akademie.de`. Benötigt wird die IN-Information. Diese entspricht unter DNS der IP-Adresse.

Iterative DNS-Namensaüflösung

Da der DNS-Server vorher noch keine DNS-Anfragen für die Top-Level-Domäne `.DE` erhalten hat, muss er nun zuerst bei einem der Stammserver (Root-Server) anfragen.

Dazu wird eine Standardanfrage an einen zufällig gewählten Stammserver gesendet, der in der Liste der Stammserver auf dem DNS-Server hinterlegt ist. In diesem Beispiel wird der Server mit der IP-Adresse 199.7.83.42 (`l.root-servers.net`) abgefragt.



Als Antwort wird eine Liste mit den Namensservern der Top-Level-Domäne *.DE* übermittelt ①. Dabei ist auffällig, dass die Top-Level-Domäne *.DE* auch von Servern verwaltet wird, die selbst in der Top-Level-Domäne *.NET* sind.

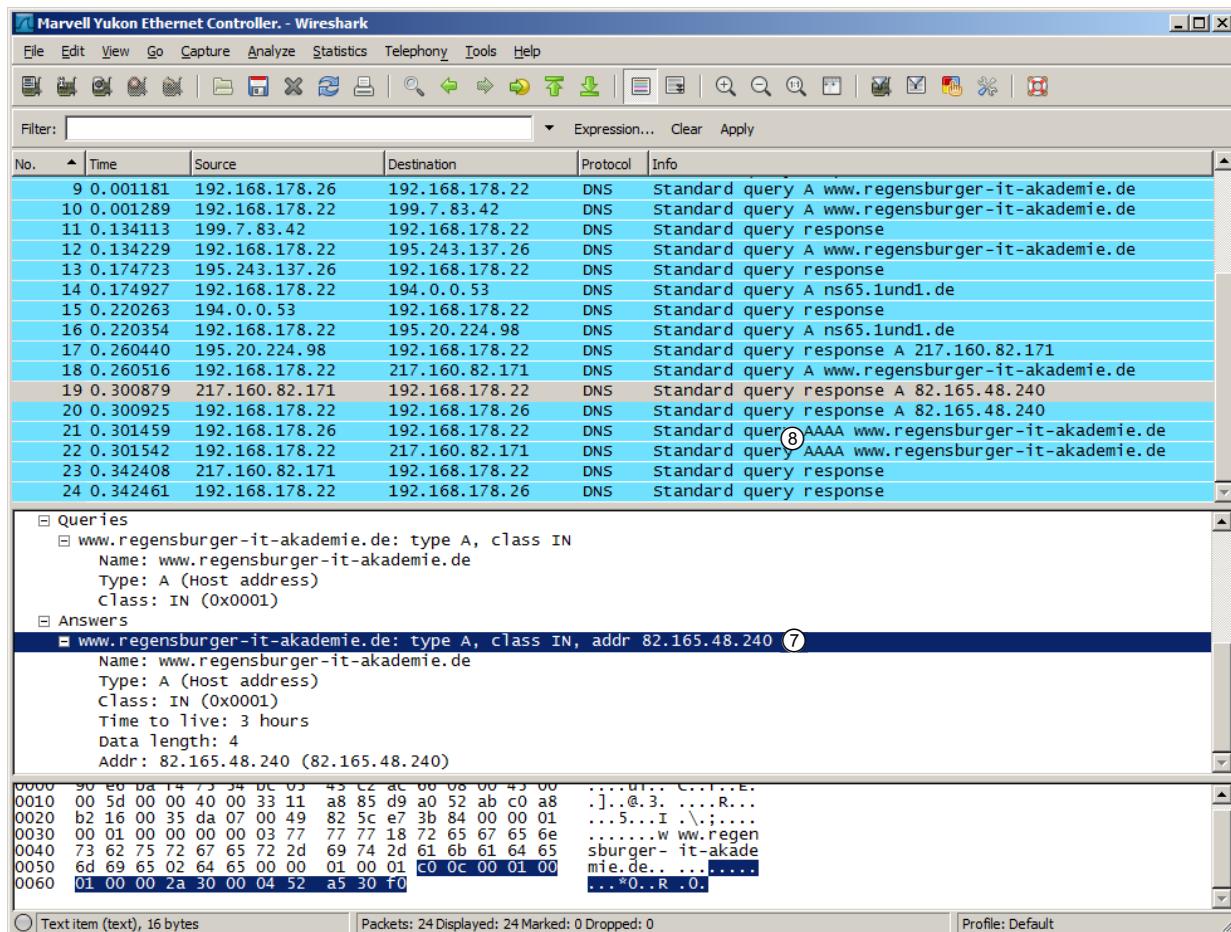
Darüber hinaus werden unter Additional records (zusätzliche Einträge) ② die IP-Adressen der verantwortlichen Namensserver übermittelt. Diese Zusatzinformation wird aber nicht obligatorisch von jedem DNS-Server hinzugefügt.

Aus der Liste der autoritativen Namensserver (Authoritative Nameservers) wird wiederum zufällig ein Server ausgewählt und erhält entsprechend eine Abfrage ③. In diesem Beispiel wird Server *S.DE.NET* mit der IP-Adresse *195.243.137.26* ausgewählt.

The screenshot shows a Wireshark capture of DNS traffic. The packet list pane shows 24 DNS packets. The details pane shows the following information for the selected packet (number 4):

- [Time: 0.040494000 seconds]
- Transaction ID: 0x419d
- Flags: 0x8010 (Standard query response, No error)
- Questions: 1
- Answer RRs: 0
- Authority RRs: 2
- Additional RRs: 1
- Queries**
 - www.regensburger-it-akademie.de: type A, class IN
 - Name: www.regensburger-it-akademie.de
 - Type: A (Host address)
 - Class: IN (0x0001)
- Authoritative nameservers**
 - regensburger-it-akademie.de: type NS, class IN, ns ns65.1und1.de
 - Name: regensburger-it-akademie.de
 - Type: NS (Authoritative name server)
 - Class: IN (0x0001)
 - Time to live: 1 day
 - Data length: 13
 - Name server: ns65.1und1.de
 - regensburger-it-akademie.de: type NS, class IN, ns ns66.1und1.de
- Additional records**
 - <Root>: type OPT

Als Antwort wird eine Liste mit den Namenssäfern der Zone übermittelt ④. Dabei kann eine Zone von Servern verwaltet werden, die selbst in einer anderen Zone (z. B. .NET) sind. Daneben zeigt sich in dem Beispiel, dass die zusätzlichen Einträge nicht immer übermittelt werden ⑤. Darum ist vor der eigentlichen Anfrage erst eine Auflösung der IP-Adresse von NS65.1UND1.DE nötig ⑥.



An diese wird nun eine Anfrage nach der Adresse des Zielsystems www.regensburger-it-akademie.de gesendet und die Antwort übermittelt ⑦:

www.regensburger-it-akademie.de = 82.165.48.240



Da der DNS-Client unter Windows 7 läuft, wird anschließend auch noch eine IPv6-Auflösung initiiert ⑧. Diese ist jedoch optional.

DNS Standard Query Response

The screenshot shows a Wireshark capture window titled "Marvell Yukon Ethernet Controller - Wireshark". The main pane displays a list of network packets. A specific packet, number 20, is highlighted in blue and has a circled '1' next to it. The details pane shows the DNS query for "www.regensburger-it-akademie.de" and its response. The bytes pane at the bottom shows the raw hex and ASCII data of the selected packet.

No.	Time	Source	Destination	Protocol	Info
9	0.001181	192.168.178.26	192.168.178.22	DNS	Standard query A www.regensburger-it-akademie.de
10	0.001289	192.168.178.22	199.7.83.42	DNS	Standard query A www.regensburger-it-akademie.de
11	0.134113	199.7.83.42	192.168.178.22	DNS	Standard query response
12	0.134229	192.168.178.22	195.243.137.26	DNS	Standard query A www.regensburger-it-akademie.de
13	0.174723	195.243.137.26	192.168.178.22	DNS	Standard query response
14	0.174927	192.168.178.22	194.0.0.53	DNS	Standard query A ns65.1und1.de
15	0.220263	194.0.0.53	192.168.178.22	DNS	Standard query response
16	0.220354	192.168.178.22	195.20.224.98	DNS	Standard query A ns65.1und1.de
17	0.260440	195.20.224.98	192.168.178.22	DNS	Standard query response A 217.160.82.171
18	0.260516	192.168.178.22	217.160.82.171	DNS	Standard query A www.regensburger-it-akademie.de
19	0.300879	217.160.82.171	192.168.178.22	DNS	Standard query response A 82.165.48.240
20	0.300925	192.168.178.22	192.168.178.26	DNS	Standard query response A 82.165.48.240 ①

Queries:

- www.regensburger-it-akademie.de: type A, class IN
 - Name: www.regensburger-it-akademie.de
 - Type: A (Host address)
 - Class: IN (0x0001)

Answers:

- www.regensburger-it-akademie.de: type A, class IN, addr 82.165.48.240
 - Name: www.regensburger-it-akademie.de
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Time to Live: 3 hours ③
 - Data length: 4 ④
 - Addr: 82.165.48.240 (82.165.48.240) ②

```

0000 00 14 5e 1e 5c af 90 e6 ba f4 75 54 08 00 45 00 ..^.\... .UT..E.
0010 00 5d 3a 34 00 00 80 11 1a da c0 a8 b2 16 c0 a8 .]:4.....
0020 b2 1a 00 35 ec 83 00 49 e5 dc 00 05 84 00 00 01 ..5...I .....
0030 00 01 00 00 00 00 03 77 77 77 18 72 65 67 65 6e .....w ww.regen
0040 73 62 75 72 67 65 72 2d 69 74 2d 61 6b 61 64 65 sburger- it-akade
0050 6d 69 65 02 64 65 00 00 01 00 01 c0 0c 00 01 00 mie.de.. .....
0060 01 00 00 2a 30 00 04 52 a5 30 f0 ...*0..R .0.

```

Der Client 192.168.178.26 erhält ein DNS Standard Query Response ① mit der Information ②:

`www.regensburger-it-akademie.de = 82.165.48.240`

Des Weiteren erfährt der Client noch, dass dieser Eintrag eine TTL von drei Stunden hat ③ und vier Byte lang ist ④.

Voraussetzungen für iterative Abfragen

Die iterative Abfrage stellt die Standardauflösungsmethode für Namen außerhalb der eigenen Zone eines DNS-Servers dar. Damit iterative Abfragen funktionieren können, müssen zwei Voraussetzungen gegeben sein:

- ✓ Internetzugang
- ✓ Aktuelle Datei `named.root`

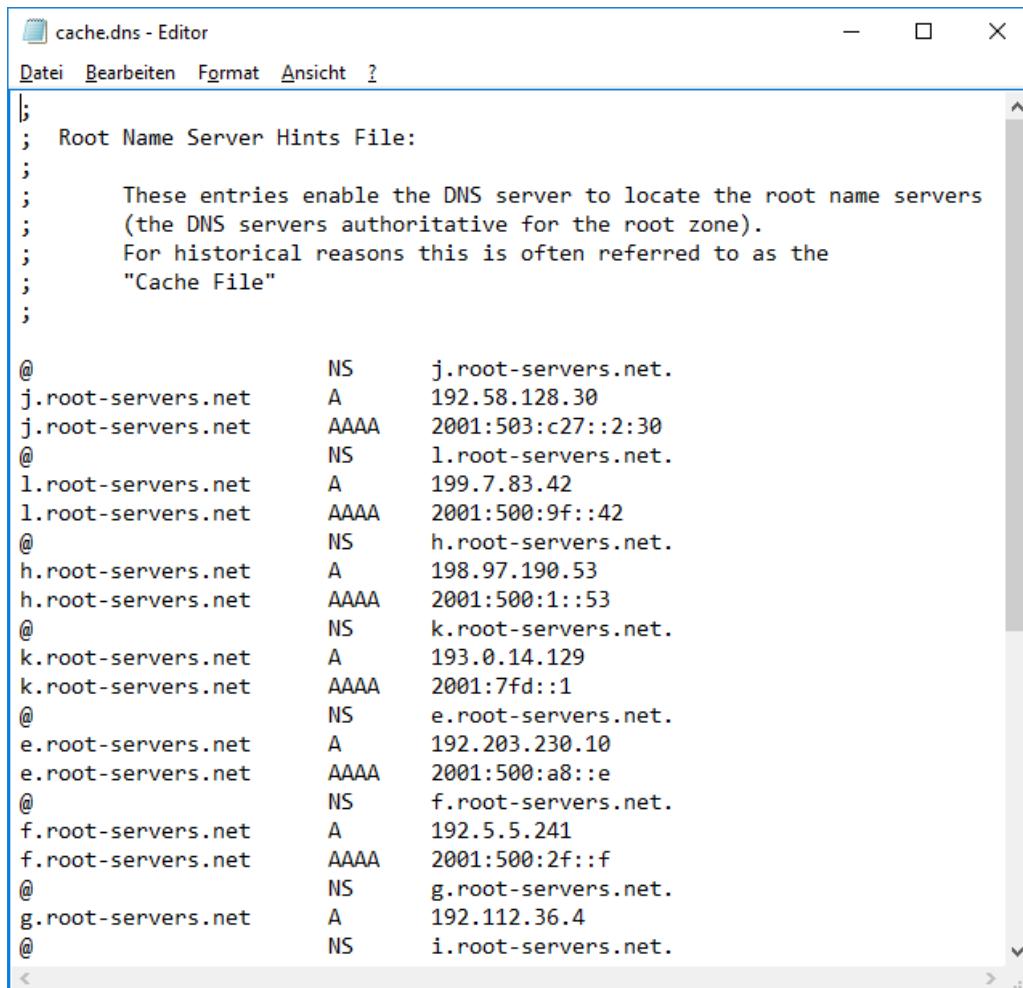
Datei `named.root`

Die Datei `named.root` ist eine Standarddatei, in der die Adressen der ROOT-Server des Internets festgehalten sind. Sie muss an der für das Betriebssystem spezifisch richtigen Stelle unter dem richtigen Namen abgelegt sein, um beim Start des DNS-Dienstes in den Cache geladen werden zu können.

Unter Microsoft und BIND-DNS-Servern ist der korrekte Name für die Datei `cache.dns` im Verzeichnis DNS (Pfad für Windowssysteme: `%systemroot%\System32\dns\`).

Soll ein DNS-Server dagegen nicht in der Lage sein, Namen im Internet aufzulösen, können Sie die Beispieldatei mit den Root-Server-Adressen löschen – oder besser – umbenennen. Durch eine Umbenennung verlieren Sie nicht die Einträge, die Sie vielleicht später noch einmal brauchen. Das System ist in beiden Fällen nicht mehr in der Lage, die DNS-Server-Adressen von Top-Level-Domänen aufzulösen. Falls Sie einzelne Domänen oder Top-Level-Domänen dennoch auflösen möchten, müssen Sie die Adressen der verantwortlichen Server nun von Hand in einer eigenen cache.dns-Datei konfigurieren. Dies kann z. B. dann sinnvoll sein, wenn Clients nur auf bestimmte Informationen im Internet oder anderen Netzwerken zugreifen sollen.

 Benutzen Sie eine derartige Konfiguration nicht, wenn Sie zum Beispiel in einem Firmennetzwerk verhindern wollen, dass am Arbeitsplatz privat gesurft wird – findige Benutzer könnten an ihrem Arbeitsplatz die IP-Adresse eines ihnen bekannten DNS-Servers konfigurieren und somit diese Sperre umgehen. Besser ist hier, die IT-Richtlinien einer Firma durch eine entsprechende Firewallkonfiguration oder andere Mechanismen wie Gruppenrichtlinien sicherzustellen.



```
cache.dns - Editor
Datei Bearbeiten Format Ansicht ?
; Root Name Server Hints File:
;
; These entries enable the DNS server to locate the root name servers
; (the DNS servers authoritative for the root zone).
; For historical reasons this is often referred to as the
; "Cache File"
;

@ NS j.root-servers.net.
j.root-servers.net A 192.58.128.30
j.root-servers.net AAAA 2001:503:c27::2:30
@ NS l.root-servers.net.
l.root-servers.net A 199.7.83.42
l.root-servers.net AAAA 2001:500:9f::42
@ NS h.root-servers.net.
h.root-servers.net A 198.97.190.53
h.root-servers.net AAAA 2001:500:1::53
@ NS k.root-servers.net.
k.root-servers.net A 193.0.14.129
k.root-servers.net AAAA 2001:7fd::1
@ NS e.root-servers.net.
e.root-servers.net A 192.203.230.10
e.root-servers.net AAAA 2001:500:a8::e
@ NS f.root-servers.net.
f.root-servers.net A 192.5.5.241
f.root-servers.net AAAA 2001:500:2f::f
@ NS g.root-servers.net.
g.root-servers.net A 192.112.36.4
@ NS i.root-servers.net.
```

Die Datei cache.dns mit Einträgen zu Root Name Servern auf einem Windows Server 2016 DNS-Server

9.3 Reverse Lookup

In der Regel kennt der Benutzer einen Rechnernamen, und das System muss die dazugehörige IP-Adresse ermitteln. Es kann jedoch auch vorkommen, dass einem Benutzer oder einer Anwendung eine IP-Adresse bekannt ist, aber der Name des dazugehörigen Systems ermittelt werden soll. In diesem Fall wird ein Reverse Lookup (etwa: umgekehrtes Nachschauen) benötigt.

In einer IPv4-Reverse-Lookup-Zone werden IPv4-Adressen FQDNs zugeordnet, indem für sie PTR-Einträge (Pointer = Zeiger) vorgenommen werden. Die Einträge sind in einer Reverse-Lookup-Zone gespeichert, die der Netzwerkadresse der Hosts zugeordnet ist. So steht z. B. für *Client-04.schulungsnetz.intern* mit der IPv4-Adresse 192.168.200.24 der PTR-Eintrag

192.168.200.24 PTR Client-04.schulungsnetz.intern

in der Reverse-Lookup-Zone 200.168.192.in-addr.arpa. Der Zonenname entspricht dabei der umgekehrten Reihenfolge der Dezimalwerte des Netzwerkteils der IP-Netzwerkadresse. Sofern es sich hierbei um eine Standardzone ohne die Integration in Active Directory handelt, finden Sie die Informationen auch in einer Textdatei namens 200.168.192.in-addr.arpa.dns.

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordneter Ordner)	Autoritätsursprung (SOA)	[12], 2016-final.final.test, ...	Static
(identisch mit übergeordneter Ordner)	Namenserver (NS)	2016-final.final.test.	Static
192.168.200.21	Zeiger (PTR)	Client-01.schulungsnetz.i...	Static
192.168.200.22	Zeiger (PTR)	Client-02.schulungsnetz.i...	Static
192.168.200.23	Zeiger (PTR)	Client-03.schulungsnetz.i...	Static
192.168.200.24	Zeiger (PTR)	Client-04.schulungsnetz.i...	Static
192.168.200.25	Zeiger (PTR)	Client-05.schulungsnetz.i...	Static
192.168.200.254	Zeiger (PTR)	Cisco-Schulungsrouter.sc...	Static

In einer IPv6-Reverse-Lookup-Zone werden IPv6-Adressen FQDNs zugeordnet, indem für sie PTR-Einträge (Pointer = Zeiger) vorgenommen werden. So steht z. B. für *Client-04.schulungsnetz.intern* der PTR-Eintrag

fe80:0000:0000:0000:0000:0000:00c3 PTR Client-04.schulungsnetz.intern

in der Reverse-Lookup-Zonendatei für 0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. Der Zonenname entspricht dabei der umgekehrten IPv6-Netzwerkadresse in zerlegter Schreibweise.

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordnetem Ordner)	Autoritätsursprung (SOA)	[10], 2016-final.final.test, ...	Static
(identisch mit übergeordnetem Ordner)	Namenserver (NS)	2016-final.final.test.	Static
fe80:0000:0000:0000:0000:0000:00c1	Zeiger (PTR)	Client-01.schulungsnetz.i...	Static
fe80:0000:0000:0000:0000:0000:00c2	Zeiger (PTR)	Client-02.schulungsnetz.i...	Static
fe80:0000:0000:0000:0000:0000:00c3	Zeiger (PTR)	Client-03.schulungsnetz.i...	Static
fe80:0000:0000:0000:0000:0000:00c4	Zeiger (PTR)	Client-04.schulungsnetz.i...	Static
fe80:0000:0000:0000:0000:0000:00c5	Zeiger (PTR)	Client-05.schulungsnetz.i...	Static

9.4 Primäre und sekundäre Zone

Arten von Zonen

Es kann auf einem DNS-Server unterschiedliche Arten von Zonen geben, die sich dadurch unterscheiden, welche Eintragsarten mit anderen DNS-Servern derselben Zone ausgetauscht werden. Diese unterscheiden sich einerseits durch die Art der ausgetauschten Informationen und andererseits durch die Art, wie mit den ausgetauschten Daten umgegangen werden darf. Zusätzlich unterscheiden sie sich durch den Speicherort der Daten. Die gängigen Zonentypen sind:

- ✓ primäre Zonen
- ✓ sekundäre Zonen
- ✓ Active-Directory-integrierte Zonen
- ✓ delegierte Zonen
- ✓ Stubzonen

Primäre Standardzonen

Unter einer primären Zone versteht man eine Zone, die auf einem Master-Server geführt wird. Auf einem DNS-Server, der für eine Zone autorisiert ist, können Änderungen an der Zone vorgenommen werden. Die Zone kann auf andere Server repliziert werden. Sie liegt dann bei diesen als sekundäre Zone (= schreibgeschützte Kopie) vor.

Sekundäre Zonen

Die sekundäre Zone dient der Ausfallsicherheit und der Lastenverteilung. An ihr können keine Änderungen der Einträge vorgenommen werden.

Die Replikation zwischen primären und sekundären Zonen wird in erster Linie durch die Eigenschaften der Zone bestimmt. In der Zonendatei ist ein Alterungsstempel für die Zonenübertragung angegeben und hier wird auch festgelegt, in welchem Intervall eine erneute Übertragung versucht werden soll, falls die erste Übertragung scheitert. Des Weiteren ist in der Zonendatei eine Versionsnummer hinterlegt. Nur wenn die Version auf dem primären Zonen-Server höher ist als auf dem sekundären Server, wird die DNS-Datei angefordert. Die Übertragung der DNS-Datei erfolgt immer komplett, es ist also nicht möglich, einzelne Einträge zu aktualisieren und somit Netzwerkbandbreite zu sparen.

Active-Directory-integrierte Zone

Seit Microsoft Windows 2000 ist erstmalig ein weiterer Typ von DNS-Zonen eingeführt worden, die Active-Directory-integrierte Zone (Active Directory ist der Verzeichnisdienst in Windows-Domänen seit Windows 2000). Er basiert auf einer LDAP-fähigen Datenbank. LDAP ist das Lightweight-Directory-Access-Protokoll, ein herstellerübergreifender Standard zur Datenbankabfrage von X.500-Datenbanken.

Durch die Integration in das verteilte Datenbanksystem von Windows 2000 oder höher ist es möglich, Änderungen an der DNS-Datenbank auf mehreren Servern gleichberechtigt vorzunehmen. Diese werden dann über den Active Directory-Replikationsmechanismus mit jeweils eigenen Versionsnummern übertragen. Somit ist auch nicht mehr jedes Mal eine komplette Zonenübertragung nötig, sondern es können einzelne Einträge übertragen werden. Dies entlastet das Netzwerk beträchtlich. Voraussetzung dafür ist allerdings, dass der DNS-Server, der eine beschreibbare Kopie der Datenbank enthalten soll, zugleich Domänencontroller ist, denn nur diese verfügen über Kopien der Active-Directory-Datenbank. Die Daten der Active-Directory-Datenbank werden dabei in sogenannten Verzeichnisdienstpartitionen gespeichert.

Die Active Directory-Integration von DNS stellt eine große Erleichterung für die Arbeit von Administratoren dar. DNS ist zum wartungsarmen Dienst geworden.

Verzeichnisdienstpartitionen

Bei einer Verzeichnisdienstpartition handelt es sich um einen zu Replikationszwecken definierten Teil der Active Directory-Datenbank. Um diese zu verstehen, muss die Organisation einer Active Directory-Struktur kurz beleuchtet werden. Die Rechner und Benutzer einer Active Directory-Umgebung sind nach unterschiedlichen Kontexten in Domänen zusammengefasst. Diese Domänen werden als Domänenstruktur (Englisch: tree) bezeichnet und können innerhalb einer DNS-Namensstruktur hierarchisch angeordnet sein, wobei diese dem Modell *subdomain.domain.top-level-domain* folgt.

Alle Domänenstrukturen eines Active Directory befinden sich in derselben Gesamtstruktur (Englisch: forest), die über eine gemeinsame Definition der möglichen Datensätze verfügt. Diese Definition wird als das Schema bezeichnet und muss in allen Domänen gleich sein, damit Objekttypen von allen beteiligten Teilen des Verzeichnisdienstes verstanden werden können. Organisiert sind die Domänen innerhalb einer Gesamtstruktur nach dem Modell *domain1.top-level-domain1* und *domain2.top-level-domain2*.

Je nach Aufgabe eines Domänencontrollers muss dieser bestimmte Teile der gesamten Active Directory-Datenbank zur Verfügung haben. So müssen etwa die Schema-Konventionen auf allen Domänencontrollern verfügbar sein, bestimmte Eigenschaften von Benutzern dagegen werden nur innerhalb einer Domäne repliziert. Je nach Zugriffsbedarf auf Teile der DNS-Informationen kann entschieden werden, in welchem Teil der Active Directory-Datenbank die DNS-Informationen abgelegt werden sollen, um so die Replikation zwischen den DNS-Servern zu optimieren und WAN-Leitungen zu schonen. Folgende Verzeichnisdienstpartitionen sind standardmäßig auf einem Domänencontroller unter Windows Server vorhanden oder werden von Anwendungen oder Administratoren angelegt:

- ✓ Schemapartition
- ✓ Konfigurationspartition
- ✓ Domänenpartition
- ✓ Globaler-Katalog-Partition
- ✓ Anwendungspartitionen

Administratoren können für die Replikation ausgewählter Daten bestimmte Anwendungspartitionen erstellen und so die DNS-Daten segmentieren, um sie auf ausgewählte DNS-Server zu verteilen. Neben der Optimierung der Replikation können hierfür auch Sicherheitsaspekte von Bedeutung sein, da die Bekanntmachung von DNS-Daten nicht immer gewünscht ist.

Zonendelegierungen

Bei einer Zonendelegierung wird der DNS-Namensraum in Bereiche unterteilt, die von unterschiedlichen DNS-Servern verwaltet werden. Dies geschieht, um die Datenbankgröße zu verringern und so die Verarbeitungsgeschwindigkeit der DNS-Server zu erhöhen oder um eine verteilte Verwaltung der DNS-Zonen zu ermöglichen. Bei der Verteilung der Datenbank ohne Delegierungen tritt folgende Problematik zutage: Wenn Server DNS-1 Master von *domain.de* ist und eine Abfrage für *delegierung.domain.de* erhält, geht er davon aus, dass diese Daten in seiner Datenbank verfügbar sind und löst diese nicht weiter auf. Erst wenn der Server über einen NS-Eintrag und SOA-Verweis für den mit der Delegierung betrauten Server verfügt, kann er die Abfrage an diesen Server weiterleiten. Der Nachteil ist dabei, dass eine Zonendelegierung nur als statische Konfiguration mit den Informationen zu einem einzigen Server eingerichtet werden kann und daher auch keine Redundanz ermöglicht.

Stubzonen

Die Stubzone ist ein Zonentyp, bei dem ein Server nicht nur einen NS-Eintrag einer anderen Zone bereitstellt, sondern über die Replikation regelmäßig alle NS-Einträge einer anderen Zone erhält und somit in der Lage ist, auch bei Ausfall einzelner Server oder Leitungen DNS-Informationen einer geteilten Datenbank abzurufen. Stubzonen sind seit Windows Server 2003 verfügbar.

9.5 Dynamisches DNS

Erweiterung von DNS

Heutige Netzwerke zeichnen sich durch Größe und Flexibilität aus. An einem Standort können mehr als 10.000 verteilte Systeme vorhanden sein, die mittels DHCP (Dynamic Host Configuration Protocol) dynamisch konfiguriert werden. In einem solchen Netzwerk ist die Verwendung statischer DNS-Datenbanken, die von Administratoren von Hand gepflegt werden, nicht denkbar. Andererseits kann aber in heterogenen Netzen nicht auf einen standardisierten, herstellerübergreifenden Dienst zur Namensauflösung verzichtet werden.

Dies macht die Einführung einer dynamischen Version von DNS-Datenbanken nötig. Dynamisches DNS (D-DNS) ermöglicht es Clients, sich bei der Aktivierung des Netzwerkadapters bei einem DNS-Server anzumelden, der daraufhin diesen Host in seiner Datenbank registriert.

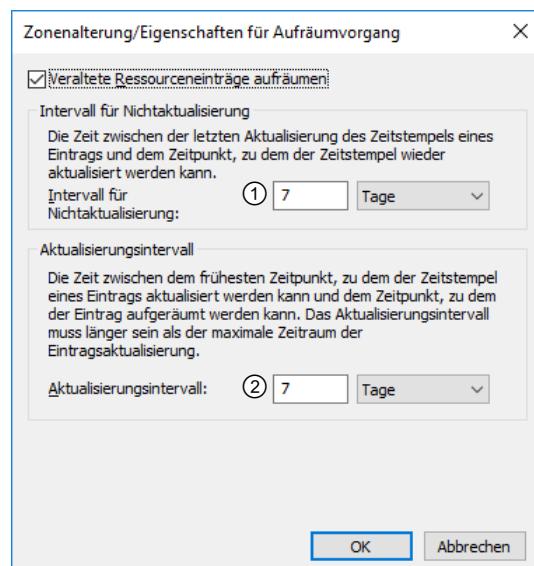
Dadurch werden nicht nur die DNS-Administratoren eines Netzes deutlich entlastet, sondern auch die DHCP-Verwaltung wird weniger aufwändig, da auf Reservierungen von DHCP-Adressen bei Clients weitestgehend verzichtet werden kann. Sonst müssen DHCP-Adressen über Reservierungen an MAC-Adressen gebunden werden, damit eine Übereinstimmung zwischen dem DNS-Eintrag und der tatsächlichen IP-Adresse des Clients jederzeit gewährleistet ist.

Zonenalterung

Wenn ein DHCP-Server die Informationen an den D-DNS-Server weiterleitet, können möglicherweise falsche Informationen abgelegt werden. Um dies zu verhindern, werden den DNS-Einträgen Alterungsinformationen hinzugefügt: Diese bestehen aus der Aktualisierungs-Sperrung und der Aktualisierungsfrist.

Ein DHCP-Bereich hat beispielsweise eine Leasedauer von acht Tagen. Hier wird normalerweise kein Client während der ersten vier Tage seine IP-Adresse verändern. Entsprechend sollte der Eintrag auf dem DNS-Server geschützt werden. In den folgenden vier Tagen dagegen ist die Adresskonfiguration zwar noch gültig, kann aber jederzeit überschrieben werden. Auch dies sollte in der DNS-Datenbank Berücksichtigung finden. Nach Ablauf der acht Tage dagegen ist davon auszugehen, dass der Eintrag nicht mehr gültig ist, und er sollte aus der Datenbank des DNS-Servers entfernt werden. Unter Windows Server-Betriebssystemen können Sie die Konfiguration der Aktualisierungssperrung und der Alterung wie folgt anpassen:

- ▶ Rufen Sie die Eigenschaften der Zone auf, für die Sie die D-DNS-Zonenalterung konfigurieren möchten.
- ▶ Wählen Sie im Register *Allgemein* die Schaltfläche *Alterung*.
- ▶ Geben Sie unter *Intervall für Nichtaktualisierung* ① an, wie lange die Einträge für die Aktualisierung gesperrt sein sollen.
- ▶ Geben Sie unter *Aktualisierungsintervall* ② an, wie lange die Einträge für die Aktualisierung freigestellt sein sollen.
- ▶ Bestätigen Sie Ihre Änderungen und verlassen Sie das Fenster mit *OK*.



D-DNS-fähige Betriebssysteme

Dynamisches DNS (D-DNS) wird bei den Microsoft-Betriebssystemen seit Windows 2000 unterstützt, in der Linux-/UNIX-Welt sind die neueren Versionen D-DNS-fähig. Andere DNS-Server können zwar die dynamisch vorgenommenen Einträge als sekundäre Zonen übernehmen, lassen jedoch selbst keine dynamischen Einträge zu.

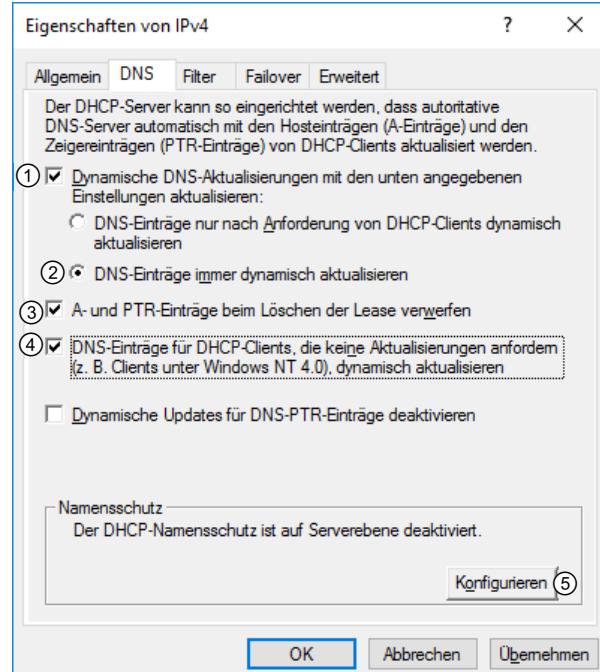
Clients, die DNS nicht dynamisch aktualisieren können

Auch wenn DHCP-Clients nicht D-DNS-fähig sind, können sie in die dynamische Datenbank eingetragen werden. Und zwar kann der DHCP-Server diese Aufgabe übernehmen. Er kennt ja die aktualisierten Informationen sämtlicher Clients und kann diese entsprechend an den DNS-Server weiterleiten.

Konfiguration von DHCP für D-DNS

Um auf einem DHCP-Server unter Microsoft-Server-Betriebssystemen ab Windows Server 2000 die Unterstützung für Clients, die DNS nicht dynamisch aktualisieren können, zu aktivieren, gehen Sie folgendermaßen vor:

- ▶ Rufen Sie die Eigenschaften des Bereichs oder des Servers auf, für den Sie die D-DNS-Unterstützung konfigurieren möchten.
- ▶ Wählen Sie das Register *DNS*.
- ▶ Markieren Sie das Kontrollfeld ①, damit der DHCP-Server die Aktualisierung von Reverse-Lookup-Einträgen (PTR) für den Client im D-DNS durchführt.
- ▶ Wählen Sie hier *DNS-A- und -PTR-Einträge immer dynamisch aktualisieren* ②, damit auch die Einträge von nicht-D-DNS-fähigen Clients aktualisiert werden.
- ▶ Markieren Sie das Kontrollfeld ③, damit veraltete Einträge automatisch aus der Datenbank entfernt werden können.
- ▶ Aktivieren Sie das Kontrollfeld ④, damit die Forward-Lookup-Einträge für nicht D-DNS-fähige Clients vom DHCP-Server vorgenommen werden können.



- ▶ Betätigen Sie die Schaltfläche *Konfigurieren* ⑤, wenn Sie die Funktion *Namensschutz* aktivieren möchten. Diese bewirkt, dass bereits vorliegende Einträge nicht vom DHCP-Server überschrieben werden können. Darüber hinaus wird dieser Standard automatisch auf neue Bereiche des DHCP-Servers angewendet.
- ▶ Bestätigen Sie Ihre Änderungen, indem Sie das Fenster mit *OK* verlassen.

9.6 Round Robin

Lastenverteilung und Ausfallsicherheit

Round Robin ist ein Mechanismus, der für eine einfache Art der Lastenverteilung und Ausfallsicherheit verwendet wird.

Ein Client, der nach einem Namen fragt, bekommt mehrere IP-Adressen mitgeteilt. Der nächste Client erhält dieselben Adressen in anderer Reihenfolge. Da jeder Client als Erstes versucht, die erste Adresse, die er erhalten hat, anzusprechen, werden so die Verbindungen abwechselnd zu den unterschiedlichen Systemen geleitet. Sollte aber eines der Systeme ausfallen, werden die Clients automatisch auf die nächste Adresse, die sie erhalten haben, zugreifen.

Voraussetzungen für Round Robin

Voraussetzung für Round Robin ist, dass einem Host-Namen mehrere IP-Adressen zugeordnet werden. Die Hostnamen müssen dabei nicht wirklich die Namen der Systeme sein, sondern dienen lediglich dazu, dass Clients auf einen Dienst zugreifen können.

Round Robin kann mit DNS-Servern ab BIND-Version 4.9.3 und Kompatiblen verwendet werden.

Priorität lokaler Netze

In einigen Versionen von DNS werden Prioritäten für lokale Netze vergeben. Ein Client erhält damit bei Abfragen immer als Erstes die Adressen, die er direkt erreichen kann, und nur die entfernten Adressen werden mittels Round Robin getauscht.

Auf diese Weise werden Zugriffe über WAN-Leitungen minimiert. Allerdings geht DNS dabei von der Verwendung echter Netze aus. Subnetze werden nicht erkannt, sondern die Masken werden anhand der IP-Klasse vom System errechnet.

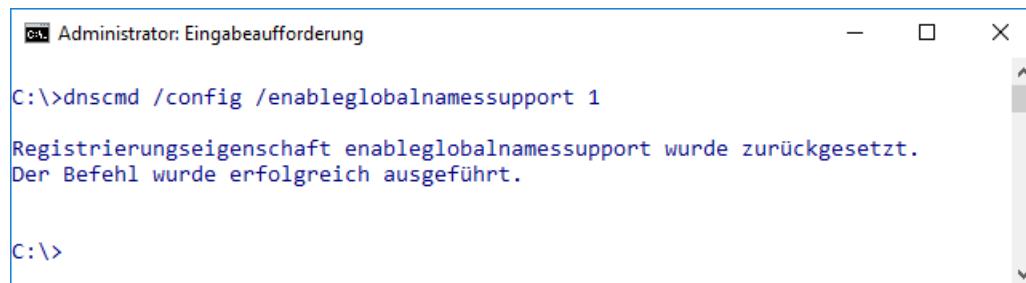
9.7 GlobalNames

Seit Microsoft Windows Server 2008 steht die DNS-Zone GlobalNames zur Verfügung. Mit dieser wird dem folgenden Problem begegnet: Wenn ein DNS-Client eine Anfrage an einen DNS-Server sendet, wird dem Hostnamen der eigene Domänenname angehängt, um einen FQDN zu bilden. Wenn nun aber in einem Unternehmensnetz mehrere Domänen verwendet werden, kann es sein, dass der gesuchte Host in einer anderen Domäne ist. In diesem Fall wird eine Fehlermeldung an den anfragenden Host zurückgegeben.

Damit diese Namen auch ohne Eingabe des FQDN aufgelöst werden können, kann DNS für die Verwendung von GlobalNames eingerichtet werden. Mit aktivierten GlobalNames versucht der DNS-Server bei einer negativen Überprüfung der Datenbank, ob er durch Weglassen der Domäneninformation einen Treffer in der Zone GlobalNames erzielen kann. Wenn nun ein Alias für einen Hosteintrag in GlobalNames eingerichtet wurde, gibt der Server eine entsprechende Antwort an den Client, als habe er den Eintrag in der Domäne des Clients gefunden.

Gehen Sie folgendermaßen vor, um GlobalNames einzurichten:

- ▶ Öffnen Sie die Eingabeaufforderung auf dem DNS-Server und geben Sie den Befehl `dnscmd /config /enableglobalnamessupport 1` ein.



```
C:\>dnscmd /config /enableglobalnamessupport 1
Registrierungseigenschaft enableglobalnamessupport wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>
```

- ▶ Richten Sie nun eine neue primäre Forward-Lookupzone namens GlobalNames ein (der Name muss exakt so lauten!).

The screenshot shows the Windows DNS Manager interface. On the left, there's a tree view of zones: 'DNS', '2016-FINAL' (expanded), 'Forward-Lookupzonen' (expanded), and 'GlobalNames' (selected). Under 'GlobalNames', there are entries for '_msdcf.final.test', 'final.test', 'Schulungsnetz.intern', and 'GlobalNames'. On the right, a table lists four entries under the 'GlobalNames' zone:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordnetem Ordner)	Autoritätsursprun...	[1], 2016-final.final.test, hostma...	Static
(identisch mit übergeordnetem Ordner)	Namenserver (NS)	2016-final.final.test.	Static
mail	Alias (CNAME)	2016-final.final.test	
superclient	Alias (CNAME)	Client-03.Schulungsnetz.intern	

GlobalNames-Zone mit mehreren Einträgen aus unterschiedlichen Zonen

- Erstellen Sie in dieser einen Alias für den Host, der über Domänengrenzen hinweg auffindbar sein soll.

Sendet ein Host eine DNS-Anfrage nach einem der vorgenommenen Einträge, erhält er eine Antwort, die den Eintrag als Alias kennzeichnet und die zusätzlich den echten FQDN und die IP-Adresse enthält.

```
C:\>nslookup mail
Server: localhost
Address: ::1

Name: 2016-final.final.test
Addresses: 192.168.178.127
          192.168.142.144
Aliases: mail.final.test

C:\>nslookup superclient
Server: localhost
Address: ::1

Name: Client-03.Schulungsnetz.intern
Addresses: fe80::c3
          192.168.200.23
Aliases: superclient.final.test
```

9.8 DNSSEC

Angriffe auf DNS

Eines der gängigen Angriffsszenarien im Internet basiert auf dem Vortäuschen falscher Identitäten. Zum Beispiel gaukelt jemand vor, legaler Betreiber der Website einer Bank zu sein. Clients, die sich mit dieser Website verbinden, geben möglicherweise wertvolle Informationen wie PIN, TAN, Kontoinformationen oder Kreditkartendaten weiter. Eine Art, diese kriminellen Ziele zu erreichen, ist die Korruption von DNS-Antworten eines DNS-Servers, um Clients auf gefälschte Websites umzuleiten (sog. „Man-in-the-Middle-Attack“).

DNSSEC

Um diesem Missbrauch vorzubeugen, wurde DNSSEC entwickelt. Es basiert auf dem Prinzip der hierarchischen DNS-Pyramide und verwendet digitale Signaturen, um die Echtheit von Informationen zu bestätigen. Dabei kommt eine asymmetrische Verschlüsselung ähnlich der Public Key Infrastructure zum Einsatz.

Bei dieser verwendet der autoritative Namensserver einer Zone seinen privaten Schlüssel, um die Echtheit der übertragenen Informationen zu bestätigen. Diese kann von jedem empfangenden Server mittels eines passenden öffentlichen Schlüssels auf ihre Richtigkeit hin überprüft werden. Voraussetzung für DNSSEC ist dabei, dass die Vertrauenskette (Chain of trust) von der verantwortlichen Zone bis zum letztendlichen Client durchgängig erhalten bleibt, getreu dem Prinzip: Wenn X gesagt hat, dass Y vertrauenswürdig ist, dann vertraue ich auch denen, denen Y vertraut.

Seit 2010 wurde DNSSEC auf allen 13 DNS-Rootservern im Internet eingeführt. Etwa 70% aller Top-Level-Domains sind mit DNSSEC signiert.

9.9 Übung

Fragen zu DNS

Übungsdatei: --

Ergebnisdatei: uebung09.pdf

1. DNS verwendet ein hierarchisches Prinzip. Welche Namensbestandteile muss ein FQDN dabei verwenden? Welche weiteren sind optional?
2. Wie viele Buchstaben darf ein einzelner DNS-Namensbestandteil maximal enthalten?
3. Wie lang darf ein FQDN maximal sein?
4. Was ist root und wie wird root in DNS-Namen dargestellt?
5. Was muss ein Client bei einem Forward Lookup kennen?
6. Was muss ein Client bei einem Reverse Lookup kennen?
7. Welche Art von DNS-Abfrage wird häufiger benötigt?
8. Wie bezeichnet man die schreibgeschützte Kopie einer Zone, die aus Redundanz- oder Leistungsgründen auf einem zusätzlichen DNS-Server liegt?
9. Was enthält die Datei named.root?
10. Wofür kann die Hosts-Datei verwendet werden?
11. Was unterscheidet Standard-Zonen von Active-Directory-integrierten Zonen?
12. Wofür können Weiterleitungen verwendet werden?
13. Wann können Zonendelegierungen verwendet werden?
14. Was sind Stubzonen?
15. Überlegen Sie sich aussagekräftige Beispiele für die Gegenüberstellung von Weiterleitung und Stubzone. Welche Voraussetzungen müssen jeweils erfüllt sein?
16. Welchen Vorteil hat D-DNS?
17. Kann D-DNS auch effektiv mit sekundären Servern verwendet werden? Unter welchen Voraussetzungen?
18. Inwiefern hängen D-DNS und DHCP miteinander zusammen?
19. Was ist Round Robin?
20. Was sind die Voraussetzungen für einen effektiven Einsatz von GlobalNames?

10 Namensdienst WINS

In diesem Kapitel erfahren Sie

- ✓ wie Ressourcen mit NetBIOS im Netzwerk bekannt gemacht werden
- ✓ wie WINS den Einsatz von NetBIOS in großen Netzen ermöglicht

Voraussetzungen

- ✓ Verständnis der Browser-Dienste in Microsoft-Netzwerken

10.1 NetBIOS

Nutzen

Das Network Basic Input/Output System ist eine Programmierschnittstelle (API), die das Programmieren von Netzwerkanwendungen vereinfacht. So gesehen ist NetBIOS weder ein Clientdienst noch ein Netzwerkprotokoll. NetBIOS ermöglicht es Netzwerkanwendungen, unabhängig vom verwendeten Transportprotokoll Ressourcen im Netzwerk zu lokalisieren (Name-Service), Verbindungen zu den Ressourcen auf- und abzubauen (Session-Service) und mit ihnen Daten auszutauschen (Datagram-Service).

Die älteren Microsoft-Windows-Betriebssysteme (vor Version 2000) benötigen NetBIOS für den „Client für Microsoft-Netzwerke“, also für den Arbeitsstationsdienst, Serverdienst, Computersuchdienst (Browser) und für Datei- und Druckerfreigaben.

Relevanz hat NetBIOS seit den Tagen der Orientierung moderner Betriebssysteme zu TCP/IP nicht mehr.

Transportprotokolle für NetBIOS

IBM ließ NetBIOS für broadcastbasierte PC-Netzwerke in den 80er-Jahren entwickeln. Ursprünglich wurde als zu Grunde liegendes Transportprotokoll NetBEUI (NetBIOS Enhanced User Interface) verwendet. Da NetBEUI broadcastbasiert und nicht routingfähig ist, wurde NetBIOS um Schnittstellen zu anderen Protokollstapeln wie TCP/IP erweitert. Somit können auf NetBIOS basierende Anwendungen auch in anderen Netzwerken verwendet werden.

Die Schnittstelle von NetBIOS zu TCP/IP wurde von der IETF unter dem Namen TcpBEUI standardisiert. Microsoft nennt diesen Standard NetBT (NetBIOS over TCP/IP, manchmal auch mit NBT abgekürzt). Microsoft Windows installiert NBT automatisch mit dem TCP/IP-Protokollstack.

NetBT verwendet folgende TCP/UDP-Ports:

- ✓ 137/TCP NetBIOS Name Service
- ✓ 137/UDP NetBIOS Name Service
- ✓ 138/UDP NetBIOS Datagram Service
- ✓ 139/TCP NetBIOS Session Service



IBM unterscheidet in der Nomenklatur nicht zwischen NetBIOS und NetBEUI, sondern bezeichnet beides mit NetBIOS. Microsoft nennt NetBEUI auch NBF (NetBIOS Frame). Seit Windows Vista ist NetBEUI nicht mehr verfügbar und gilt heute als historisch.

NetBIOS-Namen

NetBIOS-Ressourcen werden über NetBIOS-Namen angesprochen, welche genau 16 Byte lang sind. Von Benutzern vergebene Namen können die Zeichen A–Z, a–z und 0–9 enthalten und werden nötigenfalls vom System mit Leerzeichen auf 15 Zeichen aufgefüllt. Das 16. Byte spezifiziert den Ressourcentyp, z. B. Computer, Benutzer, Domäne und Domänencontroller. NetBIOS-Namen sind entweder eindeutig (eine Netzknodenadresse) oder stehen für eine Gruppe von Ressourcen gleichen Typs (mehrere Netzknodenadressen).

Die Auflösung der Namen zu Netzwerkadressen kann mithilfe folgender Techniken erfolgen:

- ✓ lokaler NetBIOS-Namenscache
- ✓ lokale LMHOSTS-Datei
- ✓ Netzwerkbroadcasts
- ✓ NetBIOS-Namensserver (z. B. WINS)
- ✓ lokale HOSTS-Datei (Aufruf von `gethostbyname()` der WinSockets)
- ✓ DNS-Namensserver (Aufruf von `gethostbyname()` der WinSockets)

Der lokale Namenscache wird zuerst abgefragt. Die Reihenfolge der anschließend eingesetzten Techniken hängt vom sogenannten Knotentypen (Node type) ab:

Knotentyp	Reihenfolge
B-Knoten (Broadcast)	Netzwerkbroadcasts
P-Knoten (Peer-to-Peer)	NetBIOS-Namensserver
M-Knoten (mixed)	Registrierung: Broadcasts Auflösung: 1.) Broadcasts 2.) NetBIOS-Namensserver
H-Knoten (hybrid)	1.) NetBIOS-Namensserver 2.) Netzwerkbroadcasts

Kann der Name dann immer noch nicht aufgelöst werden, wird die LMHOSTS-Datei (sofern aktiviert) abgefragt. Sogenannte Microsoft-enhanced-Knoten versuchen als Letztes eine Auflösung mittels des Funktionsaufrufes `gethostbyname()` über die HOSTS-Datei und DNS-Server.

Bei den LMHOSTS-Dateien handelt es sich um lokale, statische Textdateien, in denen eine tabellarische Zuordnung von NetBIOS-Namen zu IP-Adressen vorgenommen wird. Analog enthalten HOSTS-Dateien Hostnamen, FQDNs und die zugehörigen IP-Adressen.

LANA-Nummern

Ein anderes Konzept von NetBIOS stellen die LAN Adapter Numbers dar. Jedes Protokoll an jeder Netzwerkkarte bekommt eine LANA-Nummer zugewiesen. Stecken in einem Rechner zwei Netzwerkkarten und ist an jede Netzwerkkarte sowohl TCP/IP als auch NetBEUI gebunden, existieren in diesem Rechner vier LANA-Nummern. Anhand dieser Zahl gibt eine NetBIOS-Anwendung an, über welches spezielle Protokoll auf welcher Netzwerkkarte sie angesprochen werden kann.

Der Einsatz von Microsoft Active Directory und DNS ermöglicht den Verzicht auf NetBIOS in Windows-Netzwerken.



10.2 WINS

Einführung in den WINS-Dienst

WINS (Windows Internet Name Service) ist der Verzeichnisdienst von Microsoft, der NetBIOS-Namen und -Diensten IP-Adressen mithilfe einer dynamischen Datenbank zuordnet. Er soll hier stellvertretend für andere Produkte vorgestellt werden, da er wohl der verbreitetste NetBIOS-Namensserverdienst ist und um viele zusätzliche Funktionen erweitert wurde. WINS ermöglicht zusammen mit NetBT den Einsatz von NetBIOS über die Grenzen von physikalischen Netzwerksegmenten hinweg und verringert gleichzeitig den störenden IP-Broadcastverkehr in den einzelnen Netzwerksegmenten. Der Administrationsaufwand sinkt durch die zentrale Verwaltung, da auf LMHOSTS-Dateien verzichtet werden kann. Sie sollten WINS in einem NetBIOS-Netzwerk implementieren, falls es aus mehreren physikalischen Segmenten oder mehr als 50 Clients besteht.

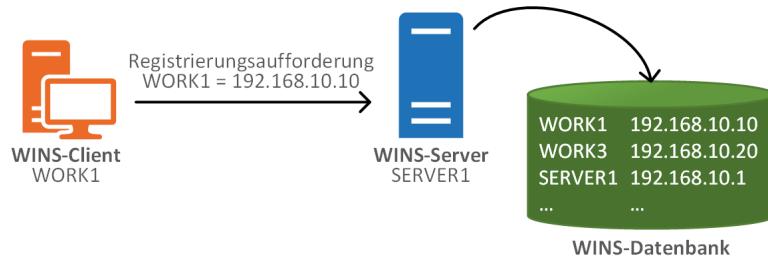
WINS besteht aus den folgenden vier Komponenten:

- ✓ WINS-Clients
- ✓ WINS-Server
- ✓ WINS-Datenbank
- ✓ WINS-Proxies und WINS-Proxy-Clients

Funktion und Konfiguration von WINS-Clients

WINS-Clients können Ressourceneinträge in der Datenbank registrieren, aktualisieren, freigeben oder abfragen. Wenn WINS-Clients gestartet werden, versuchen sie, die Namen ihrer NetBIOS-Ressourcen und ihre IP-Adresse beim WINS-Server zu registrieren. Der Server sieht in seiner Datenbank nach, ob bereits ein Eintrag mit diesem Namen vorhanden ist. Ist dies nicht der Fall, wird der Eintrag (mit Versionsnummer, TTL und einer Besitzerkennung des Servers) mit dem Attribut „aktiv“ erstellt und eine positive Antwort an den Client gesendet.

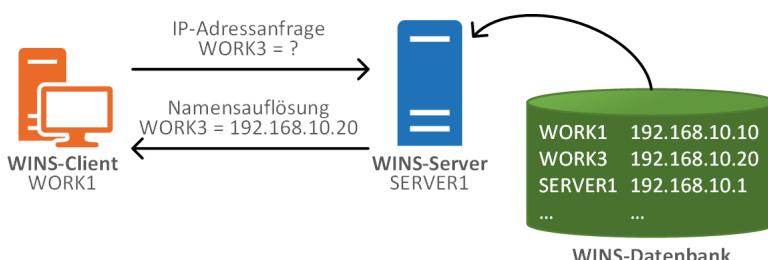
Ist bereits ein Eintrag vorhanden, wird geprüft, ob dieser als „aktiv“ gekennzeichnet ist und eine andere IP-Adresse als der anfragende Client hat. In diesem Fall wird versucht, die angegebene Ressource im Netzwerk zu erreichen. Antwortet sie nicht, wird der Eintrag an den anfragenden Client vergeben, ansonsten erhält der anfragende Client eine negative Antwort und die Registrierung wird abgelehnt. Ist der bereits vorhandene Eintrag mit „freigegeben“ oder „veralter“ gekennzeichnet, wird er sofort an den neuen Client vergeben.



Registrierung eines WINS-Clients in der WINS-Datenbank

Registrierte WINS-Clients versuchen, ihre Registrierungen nach der halben TTL-Zeit zu erneuern. Schaffen sie dies nicht, wird nach Ablauf der ganzen TTL-Zeit (Standard 6 Tage) der Eintrag als „freigegeben“ markiert. Wenn WINS-Clients herunterfahren werden, melden sie sich beim Server ab und der Eintrag wird als „freigegeben“ markiert.

Die Namensauflösung mithilfe eines WINS-Servers erfolgt wie in nebenstehender Abbildung skizziert. Der WINS-Server beantwortet Namensabfragen von Clients mit den zum NetBIOS-Namen gehörenden IP-Adressen.



Namensauflösung durch den WINS-Server

Zur Konfiguration von WINS-Clients genügt es bei neueren Windows-Installationen, in den erweiterten TCP/IP-Einstellungen eine oder mehrere IP-Adressen von WINS-Servern anzugeben und NetBT zu aktivieren. Die Konfiguration bezieht sich immer auf einzelne NICs. Samba-Clients (Linux, UNIX ...) werden entsprechend über `/etc/smb.conf` konfiguriert.

Die Begriffe **primäre und sekundäre WINS-Server** bezeichnen lediglich die Reihenfolge, in der Clients die Server abfragen. Die Server selbst unterscheiden sich nicht voneinander. Jeder Client hat also genau einen primären WINS-Server konfiguriert, den er zuerst anfragt. Ist der primäre WINS-Server nicht erreichbar, wird der sekundäre WINS-Server abgefragt. Es ist möglich, bis zu 11 sekundäre WINS-Server einzutragen. Die WINS-Server werden einer nach dem anderen in der angegebenen Reihenfolge angefragt, bis die Namensregistrierung oder -abfrage erfolgreich verläuft. Erhält der Client von keinem der Server eine positive Antwort, wechselt er zur nächsten Abfragetechnik entsprechend seinem NetBIOS-Knotentyp.

WINS-Server

Unter Windows Server 2008/R2 muss im Server-Manager die entsprechende Funktion hinzugefügt werden. Der WINS-Server kann anschließend dort auch konfiguriert werden. An dieser Stelle können Sie wichtige Parameter wie Erneuerungs-, Alterungs- und Überprüfungsintervall, Alterungszeitüberschreitung, Replikationspartner und -intervalle festlegen. Des Weiteren können Sie beispielsweise statische Einträge in der Datenbank vornehmen, dynamische Einträge unerwünschter NetBIOS-Ressourcen blockieren und die Datenbank prüfen, aufräumen oder sichern.

Wenn mehrere WINS-Server in einem Netzwerk existieren, können diese ihre Datenbanken gegenseitig replizieren. Die Replikation sorgt für einen einheitlichen Datenbestand im gesamten Netzwerk und schafft eine höhere Ausfallsicherheit der WINS-Dienste. Die Replikation erfolgt inkrementell, d. h., es werden nur die Änderungen an der Datenbank repliziert. Ein WINS-Server kann sowohl als Push- als auch als Pullpartner konfiguriert werden. Ein Pushpartner verständigt nach einer einstellbaren Anzahl geänderter Datensätze seinen Partner, und dieser fordert die Daten bei nächster Gelegenheit an. Ein Pullpartner fordert nach Ablauf einer einstellbaren Zeitspanne seinen Partner dazu auf, die geänderten Datensätze zu übertragen.

Die WINS-Datenbank

Die WINS-Datenbank (Jet-Format) besteht aus mehreren Protokoll-, Prüfpunkt- und Datenbankdateien im Ordner `%systemroot%\system32\Wins\` auf dem WINS-Server und wird von dessen WINS-Serverdienst verwaltet. Die Datenbankdateien bestehen aus zwei Tabellen. In der ersten Tabelle sind IP-Adressen Besitzer-IDs und in der zweiten NetBIOS-Namen IP-Adressen zugeordnet.

WINS-Proxies und WINS-Proxy-Clients

WINS-Proxies (WINS-Proxy-Agenten) sind normale WINS-Clients mit aktiver WINS-Proxyfunktion. Sie reagieren auf NetBIOS-Broadcasts von Nicht-WINS-Clients in ihrem Netzwerksegment. Namensanfragen werden direkt aus dem Namenscache beantwortet oder stellvertretend vom WINS-Server abgefragt und an die Nicht-WINS-Clients weitergeleitet. Auch Namensregistrierungen und -freigaben werden von den Proxies an den WINS-Server weitergegeben.

Mehr oder weniger historisch

Die in diesem Kapitel angesprochenen NetBIOS, NetBEUI und mittlerweile auch WINS sind eher von historischer Bedeutung als von aktuellem Nutzen. TCP/IP hat in modernen Betriebssystemen NetBEUI und NetBIOS vollständig abgelöst, auch wegen fehlender Kompatibilität zu IPv6. Das noch bislang neben DNS in einer Nischenrolle verwendete WINS sollte zukünftig vollständig von DNS abgelöst werden. Im Juni 2017 wurden sicherheitsrelevante Lücken in der WINS-Implementierung aktueller Windows-Versionen entdeckt, die Microsoft nicht mehr beheben wird. Microsoft sieht WINS seit langem als veraltet an und empfiehlt schon länger die Umstellung interner Namenslösungen auf DNS.

11 Netzwerkkonfigurationsdienste

In diesem Kapitel erfahren Sie

- ✓ wie das Bootstrap-Protokoll arbeitet
- ✓ wie DHCP-Clients mit dem Server kommunizieren
- ✓ welche Einstellungen Sie mit DHCP auf Clients vornehmen können
- ✓ wie Windows seine Einstellungen mit APIPA konfiguriert

Voraussetzungen

- ✓ Tiefer gehende Kenntnisse des TCP/IP-Protokollstapels

11.1 Aufgabe und Funktion von Netzwerkkonfigurationsdiensten

Grundlagen zu Netzwerkkonfigurationsdiensten

Mit zunehmender Verbreitung des Protokoll-Stacks TCP/IP auch in Intranets entstand der Wunsch, den administrativen Aufwand zur Konfiguration von TCP/IP zu reduzieren. Deshalb wurden verschiedene Verfahren entwickelt, mit denen Hosts automatisch eine IP-Adresse, die zugehörige Subnetzmaske und alle übrigen Konfigurationsdaten erhalten können:

- ✓ BootP: Bootstrap Protocol
- ✓ DHCP: Dynamic Host Configuration Protocol, eine Erweiterung von BootP
- ✓ APIPA: Automatic Private IP-Addressing

All diese Verfahren gehen davon aus, dass miteinander verbundene Knoten in einem Netzwerk bereits auf unterster Ebene durch Broadcasts miteinander kommunizieren können und über eindeutige Hardwareadressen (MAC-Adressen) verfügen.

APIPA ist ein Verfahren, das ohne Verwendung eines speziell dafür entwickelten Protokolls und ohne eine zentrale Instanz zur Verwaltung auskommt. Bei den anderen Verfahren dagegen handelt es sich um Protokolle, mit deren Hilfe eine Kommunikation zwischen einem Client und einem Server ermöglicht wird, der die Host-Adressen im Netzwerk verwaltet.

11.2 BootP

Grundlagen von BootP

Das Bootstrap-Protokoll war eines der ersten Remotekonfigurationsprotokolle. Es wurde Mitte der 80er-Jahre für sogenannte Diskless Clients entwickelt. Dabei handelt es sich um Systeme, die über keinerlei Plattsensystem, aber einen Netzwerkanschluss verfügen, zum Beispiel Workstations oder Router.

Beim Einschalten eines solchen Clients wird die eingebaute Hardware vom BIOS initialisiert. Anschließend wird aus einem PROM-Speicher ein minimales Betriebssystem gestartet, das grundlegende Systemfunktionen bietet und u. a. auch die Netzwerkschnittstelle mit einem minimalen IP-Stack ausstattet. Über Broadcasts wird ein BootP-Server gesucht und um Übermittlung einer gültigen IP-Konfiguration und Dateiname sowie Speicherort eines passenden Bootimages gebeten. Dieses Bootimage kann anschließend z. B. mit TFTP (Trivial File Transfer Protocol) in den RAM-Speicher des Clients geladen und gestartet werden.

Das BootP-Protokoll wird häufig auch nur dazu verwendet, einen noch nicht konfigurierten Client mit einer passenden IP-Konfiguration zu versorgen, ohne dass ein Bootimage übertragen wird.

BootP wird in den RFCs 951 und 1542 beschrieben und standardisiert. Es ist auf der OSI-Schicht 6 angesiedelt.

Eine aktuelle Anwendungsmöglichkeit für BootP findet sich in der Bereitstellung von Installationsmedien über das Netzwerk. Dabei werden Installationsabbilder mittels BootP von Installationsservern abgerufen. Neben blanken Installationen von Betriebssystemen können auch Abbilder mit bereits installierten Softwarepaketen bereitgestellt werden.

Aufbau von BootP-Nachrichten

BootP verwendet UDP-Datagramme mit den Portnummern 67 (Zielport für die Anfrage) und 68 (Port, auf dem gelauscht wird, ob eine Antwort eingeht). In der folgenden Skizze ist ein BootP-Datagramm mit der Position der einzelnen Bytes dargestellt.

Bit 0-7	Bit 8-15	Bit 16-23	Bit 24-31		
Code (1 Request, 2 Reply)	Hardwaretyp (z. B. 1 Ethernet)	Länge der HW-Adressen (z. B. Ethernet oder Token-Ring 6 Byte)	Hops (Zähler zur Vermeidung von Schleifen, anfangs 0, jeder Router inkrementiert +1)		
Transaktions-ID: beim ersten Datagramm zufällig generiert, dient der Zuordnung von Request zu Reply					
Sec: Zeit in Sekunden seit Client-Start		Flags: MSB 1: Broadcast-Antwort erwünscht MSB 0: Unicast-Antwort erwünscht Andere Bits unbelegt, für zukünftige Verwendung			
Client IP-Adresse: Vom Client auf 0.0.0.0 oder auf seine bekannte Adresse gesetzt					
"Deine" IP-Adresse: Vom Server vergebene Client-Adresse					
Server IP-Adresse: Beim BootP-Reply trägt der Server seine eigene Adresse hier ein.					
Router IP-Adresse: Adresse eines BootP-Relay-Agents, von diesem beim BootP-Forwarding eingetragen					
Client HW-Adresse (16 Byte): Vom Client eingetragen; anhand dieser bestimmt der Server die zu übertragende Konfiguration aus seiner Konfigurationsdatei.					
Server Host-Name (64 Byte): Optional, Hostname des BootP-Servers, nullterminiert					
Dateiname Bootimage (128 Byte): Vom Client leer gelassen oder mit dem <i>GenericName</i> belegt Vom Server belegt mit Pfad- und Dateiname des Images; nullterminiert					
Herstellerspezifisch (64 Byte): Kann zusätzliche Informationen für den Client enthalten, z. B. Standardgateway, DNS-Serveradresse, Subnetzmaske					

Ablauf der BootP-Client-Server-Kommunikation

Der BootP-Vorgang läuft in folgenden drei Schritten ab:

- ✓ **BootP-Request:** Der Client sendet ein UDP-Datagramm an Port 67 eines BootP-Servers. Das Datagramm enthält außer der Client-MAC-Adresse ein Feld für die IP-Adresse des Clients. Hat dieser noch keine Adresse, trägt er 0.0.0.0 ein. In ein weiteres Feld wird die IP-Adresse des BootP-Servers eingetragen; ist sie noch unbekannt, wird die IP-Broadcast-Adresse 255.255.255.255 eingetragen. In den meisten Fällen sind beide Adressen anfangs unbekannt. Falls nicht rechtzeitig vom Server eine Antwort erfolgt, wird der BootP-Request nach kurzer Zeit wiederholt.

- ✓ **BootP-Reply:** Der Server erhält das BootP-Request-Datagramm. Aus seiner Konfigurationsdatei ermittelt er die zugehörige Konfiguration für die angegebene MAC-Adresse des Clients und trägt sie in das Datagramm ein, das er an die Portnummer 68 zurücksendet.

Hierzu gibt es für den Server zwei Möglichkeiten:

1. Wenn der Client seine eigene IP-Adresse bereits hatte, kann diese über den ARP-Cache oder einen ARP-Request aufgelöst werden.
2. Wenn der Client noch keine IP-Adresse hatte (0.0.0.0), kann die Hardware-Adresse auch nicht mit ARP herausgefunden werden. In diesem Fall gibt es wiederum zwei Möglichkeiten: Entweder wird die Hardware-/IP-Adressen-Kombination extra vor dem Versenden des BootP-Reply in den ARP-Cache geschrieben oder die Antwort erfolgt an die IP-Broadcast-Adresse.

- ✓ Wenn der Client die BootP-Reply erhält, kann er seine IP-Konfiguration vervollständigen und ist anschließend auch in der Lage, auf ARP-Requests zu antworten. Falls ein Bootimage geladen werden soll, kann jetzt der entsprechende Fileserver über TFTP (meistens verwendet) zum Übertragen dieser Datei aufgefordert werden. Im Allgemeinen wird nach dem Starten des Bootimages der minimale IP-Stack durch einen vollwertigen TCP/IP-Stack ersetzt. Die IP-Konfiguration wird unverändert übernommen.

Die BootP-Datenbank des BootP-Servers

Ein BootP-Server hält eine Datenbankdatei vor, die in zwei Abschnitte unterteilt ist. Im ersten Abschnitt werden der Standardpfad zu den Bootimages und danach die Namen der Bootimages angegeben. Im zweiten Abschnitt, der mit einem "%" am Zeilenanfang eingeleitet wird, ist je Client eine Zeile mit den folgenden Informationen gespeichert:

Hostname Hardwaretyp Hardwareadresse IP-Adresse GenerischerName Suffix

Über den einem Client zugeordneten generischen Namen wird ein Imagetyp ausgewählt. Ein danach zusätzlich angegebenes Suffix kann eine speziell angepasste Version des Images spezifizieren.

Beispiel für eine BootP-Datenbank:

```
/usr/bootimg
vmlinuz      vmlinuz
cad          hpcad
fetest       /usr/fe/bootptestl
gway         gway.

% end of generic names, start of address mappings

pluto        1 00.e0.7d.13.a7.09    172.16.8.20
neptun       1 00.e0.7d.27.3d.93    172.16.8.12
inet-gw      1 00.50.da.73.ce.b7    172.16.8.1        gway inet
itmgmt-gw   1 00.50.da.d6.44.2c    172.16.12.1      gway itmgmt
cadwsl       1 00.50.da.44.62.5a    172.16.15.27     cad
cadws2      1 00.50.da.4d.48.9e    172.16.15.65     cad
```

Wenn beispielsweise der Client `itmgmt-gw` in seinem BootP-Request im Feld *Dateiname Bootimage* keine Angabe gemacht hat, erhält er im BootP-Reply im Feld *Dateiname Bootimage* die Angabe `/usr/bootimg/gway.itmgmt` für das zu ladende Image zurück.

BootP Forwarding

Da BootP-Requests an die Broadcast-Adresse geschickt werden, können diese zunächst nur von BootP-Servern im gleichen physikalischen Netzwerksegment empfangen werden. Ein normaler Router leitet weder Pakete mit der IP-Absenderadresse 0.0.0.0 noch Datagramme mit der Broadcast-Zieladresse 255.255.255.255. weiter. Um diese Begrenzung zu überwinden, kann auf RFC-1542-kompatiblen Routern das sogenannte Forwarding für BootP aktiviert werden. Ein solcher Router fungiert dann als BootP-Relay-Agent. Er bearbeitet die Datagramme für Port 67 und leitet sie in andere Subnetze weiter.

Ein als BootP-Relay-Agent konfigurierter Router entscheidet anhand der Hop-Zahl des BootP-Requests, ob er das Datagramm weiterleitet. Die Schwelle dafür ist auf dem Router einstellbar. Falls das Datagramm weitergeleitet wird, wird die Hop-Zahl um eins inkrementiert. Anschließend wird das Feld *Router-IP-Adresse* geprüft. Ist es gleich 0.0.0.0, wird es durch die Adresse der empfangenden Schnittstelle ersetzt. Das Datagramm wird anschließend (normalerweise per Unicast) an BootP-Server, deren Adressen in der Router-Konfiguration eingetragen sind, weitergeleitet.

Der empfangende BootP-Server sendet das BootP-Reply per Unicast an Port 67 an die im Feld *Router-IP-Adresse* angegebene Adresse, wenn diese nicht gleich 0.0.0.0 ist.

Der empfangende BootP-Router prüft im Feld *Flags*, ob das Broadcastbit gesetzt ist. Wenn ja, leitet er den BootP-Reply per Broadcast weiter, ansonsten an die IP-Adresse im Feld *DEINE-IP-Adresse*, die dem Client bereits bekannt ist.

Die Vor- und Nachteile von BootP

Vorteile	Nachteile
✓ Zentrale Vergabe von IP-Adressen	✓ Umfangreiche statische Datenbank, die von Hand administriert werden muss
✓ Erhöhung der Sicherheit, da IP-Adressen nur an Clients mit bekannter Hardware-Adresse vergeben werden	✓ Sicherheitsprobleme durch falsche BootP-Server und -Relay-Agents; Denial-of-service durch BootP-Clients möglich
	✓ Für jeden Client, der mit BootP konfiguriert werden soll, muss eine IP-Adresse vergeben werden. Deshalb ist kein Einsparen von IP-Adressen durch nicht aktive Clients möglich.

11.3 DHCP

Dynamic-Host-Configuration-Protokoll

Das Dynamic-Host-Configuration-Protokoll baut auf dem BootP-Protokoll auf und wurde zu Anfang der 90er-Jahre spezifiziert (RFC 2131 für DHCP; RFCs 1534 und 2132 für DHCP-Optionen). Es dient wie BootP dazu, Knoten in IP-Netzwerken zu konfigurieren. Es bietet aber zusätzlich die Möglichkeit, IP-Adressen dynamisch zu verteilen, also nicht mehr fest an eine bestimmte Hardwareadresse zu binden. Damit ist es möglich, IP-Adressen, die gerade nicht mehr verwendet werden (weil z. B. eine Arbeitsstation heruntergefahren wurde), an andere Clients zu vergeben. Es ist also ein Einsparen von IP-Adressen möglich.

Ein weiterer Vorteil von DHCP gegenüber BootP ist die deutlich erhöhte Anzahl an Parametern (Optionen) zur Netzwerkkonfiguration von Clients.

Ein DHCP-Server verfügt über eine Datenbank, in der unter anderem ein Pool von IP-Adressen (z. B. mehrere Subnetze) verwaltet wird. Die Vergabe der einzelnen Adressen an einen Client kann auf drei Arten erfolgen:

- ✓ **Permanent:** Sobald ein Client eine IP-Adresse anfordert, wird ihm eine freie Adresse aus dem Adress-Pool zugeteilt. Der Client kann die Adresse für eine unbegrenzte Zeit nutzen.
- ✓ **Dynamisch:** Sobald ein Client eine IP-Adresse anfordert, wird ihm eine freie Adresse aus dem Adress-Pool für eine bestimmte Zeitdauer zugeteilt.
- ✓ **Statisch:** Sobald ein bestimmter Client eine IP-Adresse anfordert, wird ihm eine vom Administrator extra für ihn reservierte Adresse aus dem Adress-Pool zugeteilt. Der Client erhält immer dieselbe Adresse, muss seine Adress-Reservierung aber regelmäßig erneuern.

DHCP-Leases

Eine von einem DHCP-Server vergebene dynamische IP-Adresse ist nur begrenzte Zeit gültig. Dieses Zeitintervall wird mit **Lease** (Lease-Dauer) bezeichnet und in Sekunden berechnet. Die Dauer des Leases wird vom DHCP-Server vorgegeben und der Client hat selbst keinen Einfluss darauf. (Er kann höchstens ablehnen.)

Die Lease-Dauer ist also die maximale Zeit, während der die IP-Adresse von einem Client verwendet werden darf. Während dieser Zeit ist die Lease gültig, danach abgelaufen.

Zwei weitere Zeitintervalle spielen eine Rolle: die **Renewal Time** (T_1) und die **Rebinding Time** (T_2). Beide Intervalle werden als Prozentwerte definiert und auf die Lease-Dauer bezogen. Standardmäßig sind T_1 auf 50 % und T_2 auf 87,5 % eingestellt.

Nach Ablauf der Renewal Time (T_1) versucht der Client immer wieder, sein Lease bei dem DHCP-Server zu erneuern, an den er gebunden ist. Gelingt ihm dies, wird der Timer für die Lease-Dauer zurückgesetzt. Erhält er keine neue Lease, versucht er nach Ablauf der Rebinding Time (T_2) immer wieder, auch von anderen DHCP-Servern seine Lease zu erneuern. Kann der Client auch auf diesem Wege keine neue Lease erhalten, wird nach Ablauf der Lease der Netzwerkverkehr eingestellt und die IP-Adresse auf 0.0.0.0 gesetzt.



Die Zeiten werden in Sekunden angegeben. Die dazu verwendeten 32 Bits ermöglichen Lease-Dauern von länger als einem Jahrhundert. Der Wert ff:ff:ff:ff steht für unendlich und ermöglicht eine permanente Zuweisung einer IP-Adresse.

Aspekte der Lease-Dauer

Eine sinnvolle Einstellung der Lease-Dauer hängt von vielen Faktoren ab, insbesondere ...

- ✓ von dem Verhältnis Anzahl IP-Adressen im Pool zur Anzahl belegter Adressen (die Lease-Dauer muss verkürzt werden, wenn die freien Adressen knapp werden);
- ✓ von der Anzahl der Clients pro DHCP-Server (die Lease-Dauer muss verlängert werden, wenn der Server oder das Netzwerk durch zu viele Anfragen überlastet wird);
- ✓ von der Art der Arbeitsstationen im Netzwerk (z. B. Desktoprechner sind permanent im Netzwerk – Standardlease-Dauer: 8 Tage, Notebooks von Außendienstmitarbeitern, die sich eher selten im Firmennetz anmelden – Standardlease-Dauer: 8 Stunden);
- ✓ von der Häufigkeit der Änderungen wichtiger DHCP-Optionen (z. B. DNS-Serveradresse) (die Optionen werden den Clients erst bekannt, wenn sie von sich aus den Server kontaktieren);
- ✓ von der Zeitspanne, die es dauert, bis Störungen, die zu Nichterreichbarkeit von DHCP-Servern führen, zu beseitigen (eine zu kurze Lease-Dauer führt dann zum Ausfall der Netzwerkanbindung von Clients durch Ablauf der Lease).

Beispiele für Lease-Dauern

Lease-Dauer	Besondere Vorteile
20 min.	IP-Adressen, die nicht mehr benötigt werden, können sehr schnell wieder vergeben werden (aber hohe Netzlast alle 10 min. je Client = Renewal Time)
12 h	Verteilung neuer IP-Adressen und DHCP-Optionen über Nacht
1 d	Clients können tagsüber noch arbeiten, falls der DHCP-Server über Nacht ausfällt
3 d	Standardeinstellung auf vielen DHCP-Servern
6 d	Clients können montags noch arbeiten, falls der DHCP-Server am Wochenende ausfällt
1 a	ist einer permanenten Vergabe vorzuziehen

Bei modernen DHCP-Servern gibt es die Möglichkeit, bestimmten Geräteklassen (z. B. mobilen Geräten) die Option bereitzustellen, den Lease beim Herunterfahren zu verwerfen. So kann sichergestellt werden, dass mobile Benutzer stets einen zu der Standortkonfiguration passenden DHCP-Lease verwenden. Voraussetzung ist, dass die Geräte zwischen den Verwendungen heruntergefahren werden.



DHCP-Client-Zustände während der Lease-Dauer

Ein DHCP-Client befindet sich in Abhängigkeit vom Vorhandensein einer Lease und deren bereits abgelaufener Zeit in einem der nachfolgend tabellarisch aufgelisteten Zustände. Vom jeweiligen Zustand hängt nicht nur das Verhalten des Clients, sondern auch das des DHCP-Servers ab.

Zustandsbezeichnung	Beschreibung des Clients
INIT	Der Client hat noch keine Lease und ist auf der Suche nach einem DHCP-Server.
INIT-REBOOT	Der Client hat eine Lease und startet seine Netzwerkschnittstelle neu.
SELECTING	Der Client hat von einem oder mehreren DHCP-Servern ein Lease-Angebot erhalten und entscheidet, ob und welche Lease er annimmt.
BOUND	Der Client wurde erfolgreich konfiguriert und besitzt eine gültige Lease. Er ist an einen bestimmten Server gebunden.
RENEWING	Der Client versucht, seine Lease bei dem Server, an den er gebunden ist, zu erneuern.
REBINDING	Der Client konnte seine Lease bei dem Server, an den er gebunden ist, nicht erneuern und sucht nach einem neuen Angebot eines Servers.

Aufbau von DHCP-Nachrichten

DHCP-Nachrichten sind bis auf zwei Unterschiede genauso aufgebaut wie herkömmliche BootP-Nachrichten:

- ✓ Bei einem DHCP-Discover ist das Feld *Dateiname Bootimage* auf NULL gesetzt.
- ✓ Das letzte Feld heißt nicht mehr *Herstellerspezifisch*, sondern *Optionen* und wurde von 64 Byte auf 312 Byte vergrößert.

Es werden insgesamt acht DHCP-Nachrichtentypen unterschieden. Diese sind in der folgenden Tabelle aufgeführt.

Nachrichtentyp	Absender	Bedeutung
DHCP-Discover	Client	Aufforderung per Broadcast an alle DHCP-Server, eine Konfiguration anzubieten
DHCP-Offer	Server	Antwort auf DHCP-Discover mit Angebot einer IP-Adresse und zusätzlichen Optionen
DHCP-Request	Client	Annehmen des DHCP-Offers eines Servers und gleichzeitiges Ablehnen der Angebote anderer Server <i>oder</i> Anfrage an den Server nach einem Reboot oder Ortswechsel, ob die bisherige Konfiguration beibehalten werden kann <i>oder</i> Anfrage an den Server, ob eine Lease verlängert wird
DHCP-Ack	Server	Bestätigung eines Servers, dass Konfiguration verwendet werden kann; beinhaltet alle Konfigurationsparameter
DHCP-NAck	Server	Negative Bestätigung eines Servers, weil beantragte IP-Adresse falsch oder Lease abgelaufen ist

Nachrichtentyp	Absender	Bedeutung
DHCP-Release	Client	Mitteilung an Server, dass Lease und IP-Adresse nicht mehr benötigt werden
DHCP-Inform	Client	Mitteilung an Server, dass bereits eine IP-Adresse vorhanden ist (z. B. durch manuelle Konfiguration), aber noch andere Informationen (Optionen) gewünscht werden.
DHCP-Decline	Client	Mitteilung an Server, dass eine angebotene IP-Adresse bereits von einem anderen Knoten verwendet wird. Der Server wird diese Adresse dann nicht an andere Clients vergeben.

Der Typ der DHCP-Nachricht ist in BootP-Datagrammen im Feld *Optionen* in der Option 53 angegeben.

Ablauf der Kommunikation zwischen DHCP-Client und -Server

Die drei wichtigsten Gründe, die zu einem Austausch von DHCP-Nachrichten führen, sind:

- ✓ Ein Client möchte eine neue Lease erhalten (Zustand INIT).
- ✓ Ein Client möchte eine Lease verlängern (Zustand RENEWING).
- ✓ Ein Client war schon einmal durch DHCP konfiguriert und möchte dieselbe IP-Adresse erneut verwenden (Zustand INIT-REBOOT).

Beantragen einer neuen Lease

Ausgehend von einem noch nicht über DHCP konfigurierten Client (Zustand INIT) und einem im selben Subnetz erreichbaren DHCP-Server soll im Folgenden der Ablauf der Kommunikation zwischen beiden dargestellt werden. Der DHCP-Server verfüge über freie IP-Adressen in seiner Datenbank, die auch die belegten IP-Adressen und Leases enthält.

Zusätzlich zu folgender Abbildung finden Sie in diesem Abschnitt auch die Abbildung der Ausgaben eines Protokollanalysators, der den Nachrichtenfluss aufzeichnet hat. Die Bezeichner ① – ④ korrespondieren in beiden Abbildungen.



Kommunikation zwischen einem noch nicht konfigurierten DHCP-Client und einem DHCP-Server

DHCP-Discover

Ein BootP-Request-Datagramm wird an die Broadcast-Adresse gesendet ①. Da der Client bisher noch keine IP-Adresse hat, lautet die IP-Absenderadresse 0.0.0.0. Das Datagramm enthält unter anderem die MAC-Adresse des Absenders, den Host-Namen und – sofern vorhanden – die zuletzt vom Client verwendete IP-Adresse. Im Feld *Optionen* werden mit DHCP-Option 55 die in der Antwort von DHCP-Servern erwarteten Parameternamen aufgelistet. Dies sind insbesondere die Subnetzmaske, die Gateway-, DNS-Server- und Domänen-Controller-IP-Adressen. Der Client erwartet anschließend DHCP-Offer-Nachrichten.

DHCP-Offer

Ein DHCP-Server antwortet mit einem BootP-Reply-Datagramm an die Broadcast-Adresse ②, wenn er eine Lease anbieten kann, und nimmt eine vorläufige Belegung dieser IP-Adresse in seiner Datenbank vor. Im Feld *Deine IP-Adresse* ⑤ wird dem Client eine IP-Adresse angeboten. Im Feld *Optionen* ⑥ werden weitere Parameter wie Subnetz-Maske, Lease-Zeiten, Domänenname, Gateway- und DNS-Server-IP-Adresse und insbesondere auch die IP-Adresse (Server Identifier) ⑦ des antwortenden DHCP-Servers übergeben.

Nach Erhalt einer DHCP-Offer wechselt der Client in den Zustand SELECTING.

DHCP-Request

Sobald der DHCP-Client sich für ein Lease-Angebot entschieden hat, sendet er ein BootP-Request an die Broadcast-Adresse ③. Im Feld *Optionen* werden die gewünschte IP-Adresse (entsprechend der vorher ausgewählten DHCP-Offer), Clienthostname, Client-FQDN und der Server Identifier übertragen.

Weil der DHCP-Request an die Broadcast-Adresse gerichtet ist und den Server Identifier enthält, erfahren dadurch alle DHCP-Server, ob ihre eigene DHCP-Offer angenommen oder abgelehnt wurde.

DHCP-Ack

Der dem Server Identifier entsprechende DHCP-Server antwortet mit einem BootP-Reply-Datagramm an die Broadcast-Adresse ④, wenn er den erhaltenen DHCP-Request erfüllen kann. Die Client-IP-Adresse wird in der Datenbank als benutzt markiert.

Der DHCP-Client broadcastet nach dem Empfang des DHCP-Ack drei ARP-Requests ⑧, um herauszufinden, ob die an ihn vom DHCP-Server vergebene IP-Adresse tatsächlich frei ist. Falls er darauf keine Antwort erhält, richtet er nun seine Netzwerkschnittstelle mit der ihm übergebenen Konfiguration ein und wechselt in den Zustand BOUND. Erhält er wider Erwarten Antwort auf seine ARP-Requests, sendet er eine DHCP-Decline-Message an den DHCP-Server, um diesen darüber zu informieren, dass die Konfiguration wegen eines IP-Adresskonfliktes nicht übernommen werden konnte. Der Client wechselt dann wieder in den INIT-Zustand.

No.	Time	Source	Destination	Protocol	Info
①	35 19.205997	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x91f771a
②	36 19.210784	192.168.1.1	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x91f771a
③	37 19.211505	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x91f771a
④	38 19.216404	192.168.1.1	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x91f771a
⑤	39 19.236384	xppro1.matrix.de	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.2? Tell 192.168.1.2
⑥	40 20.194501	xppro1.matrix.de	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.2? Tell 192.168.1.2
	41 21.195835	xppro1.matrix.de	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.2? Tell 192.168.1.2

Internet Protocol, Src Addr: 192.168.1.1 (192.168.1.1), Dst Addr: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x091f771a
Seconds elapsed: 0
Broadcast flag: 0x0000
Client IP address: 0.0.0.0 (0.0.0.0)
⑤ Your (client) IP address: 192.168.1.2 (192.168.1.2)
Next server IP address: 100.0.0.1 (100.0.0.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client hardware address: 00:06:7b:01:46:84
Server host name not given
Boot file name not given
⑥ Magic cookie: (OK)
Option 53: DHCP Message Type = DHCP Offer
Option 1: Subnet Mask = 255.255.255.0
option 58: Renewal Time value = 4 days
option 59: Rebinding Time value = 7 days
option 51: IP Address Lease Time = 8 days
⑦ option 54: Server Identifier = 192.168.1.1
Option 15: Domain Name = "matrix.de"
Option 3: Router = 192.168.1.1
Option 6: Domain Name Server = 192.168.1.1
End Option

0000 ff ff ff ff ff ff 00 e0 7d d2 07 12 08 00 45 00 .:..... }......E.
0010 01 48 33 5c 00 00 80 11 44 a0 c0 a8 01 01 ff ff .H3\.... D.....
0020 ff ff 00 43 00 44 01 34 6d d7 02 01 06 00 09 1f ...C.D.4 m.....
0030 77 1a 00 00 00 00 00 00 00 c0 a8 01 02 64 00 w..... .d.
0040 00 01 00 00 00 00 00 06 7b 01 46 84 00 00 00 00{.F.....

Mitschnitt eines Protokollanalyzers der zwischen DHCP-Client und -Server ausgetauschten Nachrichten

Verlängerung einer Lease

Nach Ablauf der Renewal Time (T_1) wechselt der Client vom BOUND- in den RENEWING-Zustand. Er sendet dann per Unicast einen DHCP-Request an die IP-Adresse des DHCP-Servers, an den er gebunden ist. Der Server kann dann mit DHCP-Ack an die IP-Adresse des Clients eine Verlängerung der Lease zustimmen. Nach Erhalt des DHCP-Ack setzt der Client seinen Leasetime zurück und wechselt in den Zustand BOUND.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.1	DHCP	DHCP Request - Transaction ID 0x8147a71b
2	0.006010	192.168.1.1	192.168.1.2	DHCP	DHCP ACK - Transaction ID 0x8147a71b

Unicast-DHCP-Nachrichten bei der Verlängerung einer Lease

Hat der DHCP-Client keine Verlängerung seiner Lease vom gebundenen DHCP-Server erhalten und ist auch die Rebinding Time (T_2) abgelaufen, wechselt er in den Zustand REBINDING. Er sendet dann die DHCP-Requests an die Broadcast-Adresse und lässt den Server Identifier (Option 54) weg, um alle erreichbaren DHCP-Server abzufragen.

Wiederverwenden einer IP-Adresse

Wenn ein Client bei einem Reaktivieren seiner Netzwerkschnittstelle (z. B. Neustart) eine ihm früher durch DHCP zugewiesene IP-Adresse wieder zugewiesen bekommen möchte, wechselt er in den Client-Zustand INIT-REBOOT. Der Client broadcastet dann einen DHCP-Request, in dem das Feld *Client-IP-Adresse* mit 0.0.0.0 und die Option 50 *Requested IP-Address* mit der früheren Adresse belegt ist.

Der DHCP-Server überprüft anhand des Client Identifier, ob die beantragte IP-Adresse an diesen Client vergeben war. Ist dies der Fall und ist die IP-Adresse frei, antwortet er mit einem DHCP-Ack und der Client übernimmt die Konfiguration (BOUND). Kann die IP-Adresse nicht vergeben werden, antwortet der Server mit einem DHCP-NAck und der Client begibt sich in den INIT-Zustand.

Konfiguration der Clients

Bei allen modernen Betriebssystemen genügt es, die Verwendung von DHCP in der IP-Konfiguration an entsprechender Stelle zu aktivieren und eventuell einen Neustart durchzuführen. Eine weitergehende Konfiguration ist nicht notwendig.

Dynamische DNS-Registrierung

DHCP-Clients können bei der Kommunikation mit DHCP-Servern ihren voll qualifizierten Domänennamen mitteilen. Die DHCP-Server können dann automatisch die Einträge auf DNS-Servern aktualisieren (D-DNS). Dies kann auf drei Arten geschehen:

- ✓ Der DHCP-Server registriert alle Clients beim DNS-Server. Es werden A-Einträge (forward lookup) und PTR-Einträge (reverse lookup) getätigert.
- ✓ Der DHCP-Server registriert alle Clients beim DNS-Server. Es werden nur PTR-Einträge (reverse lookup) getätigert.
- ✓ Der DHCP-Server registriert nur für Clients, die dies ausdrücklich wünschen, A- und PTR-Einträge.

11.4 DHCP-Optionen

Struktur der Optionen

DHCP-Optionen sind zusätzliche Konfigurationsparameter und Informationen über das Netzwerk, die einem Client zur Konfiguration angeboten werden können. Sie werden im Feld *Optionen* der DHCP-Nachrichten übermittelt. RFC 2132 beschreibt die DHCP-Optionen. Darin enthalten sind die in RFC 1497 beschriebenen *Herstellererweiterungen* des Feldes *Herstellerspezifisch* aus den BootP-Nachrichten.

Die DHCP-Optionen sind nummeriert von 0 bis 255 und in zwei Bereiche unterteilt:

- ✓ 1–127: öffentliche Optionen; diese sind in allen Netzwerken gültig.
- ✓ 128–254: private Optionen; diese können vom Betreiber eines Netzwerkes definiert und verwendet werden.

Die nicht in RFC 2132 aufgeführten Optionen im Bereich 1–127 gelten als *inoffiziell*. Einige davon sind dennoch sehr verbreitet. Genaue Informationen finden Sie unter www.iana.org/assignments/bootp-dhcp-parameters und www.iana.org/assignments/bootp-dhcp-extensions/index.htm.



Die Optionen 0 und 255 haben besondere Funktionen. DHCP-Optionen werden innerhalb des Feldes *Optionen* im Datagramm durch ihre Nummer (Länge: 8 bit (=1 Oktett)) voneinander getrennt. Die Optionen 0 und 255 dienen zur Formatierung des Feldes *Optionen*. Ist die Option 0 vorhanden, werden alle Optionen an Byte-Grenzen ausgerichtet (Padding). Die Option 255 beendet das Feld *Optionen*.

Nach der Optionsnummer wird im nächsten Oktett die Länge der Option in Bytes angegeben. Darauf folgt der Wert der Option in entsprechender Länge.

Beispiel: Die Option 69 gibt die IP-Adressen von SMTP-Servern an. Im Beispiel wird die IP-Adresse eines Servers übermittelt:

Bit 0 - 7	8 - 15	16 - 23	24 - 31	32 - 39	40 - 47
Optionsnummer	Länge	Wert	Wert	Wert	Wert
69	4	115	23	180	250

Die Optionen im Einzelnen

Im Folgenden sind die wichtigsten Optionen tabellarisch aufgelistet. Da DHCP eine Erweiterung von BootP ist, sind BootP-Optionen auch für DHCP gültig. Die anderen Optionen können nur mit DHCP verwendet werden.



Nicht alle DHCP-Optionen dienen zur Konfiguration. So dient zum Beispiel die Option 53 zur Unterscheidung des DHCP-Nachrichtentyps.

Optionen für BootP und DHCP

Nummer	Überschrift	Verwendung
0	Padding	Ausrichtung der Optionen
Herstellererweiterungen nach RFC 1497		
1	Subnet Mask	Subnetzmaske
2	Time Offset	Abweichung in Sekunden von der Coordinated Universal Time (UTC)
3	Router Option	IP-Adressen von Routern im Subnetz des Clients
4	Time Server	Adressliste von Zeitservern nach RFC 868
Herstellererweiterungen nach RFC 1498		
6	Domain Name Server	Adressen von DNS-Servern, die für den Client zuständig sind
9	LPR Server	Adressliste von LPR-Druck-Servern
12	Host Name	Name des Clients, mit oder ohne lokalen Domänennamen
13	Boot File Size	Größe des Bootimages
15	Domain Name	Standard-Domänenname, den Clients bei der Auflösung von Namen verwenden sollen
IP Layer Parameter		
19	IP Forwarding	Packet Forwarding (0: aus, 1: ein)
23	IP Time to Live	Standard-TTL-Zeit für ausgehende Datagramme
35	ARP Cache Timeout	Zeit in Sekunden, bis Einträge aus dem ARP-Cache gelöscht werden
36	Ethernet Encapsulation	0: Ethernet Version 2 (RFC 894), 1: IEEE 802.3 (RFC 1042)
46	NetBIOS over TCP/IP Node Type Option	Zum Einstellen des Knotentyps der Client-Schnittstelle (B-, P-, M- oder H-Knoten)
70	POP3 Server	Adressen von POP3-Servern (Post Office Protocol)
255	End	Zum Markieren des Endes des Feldes <i>Optionen</i>

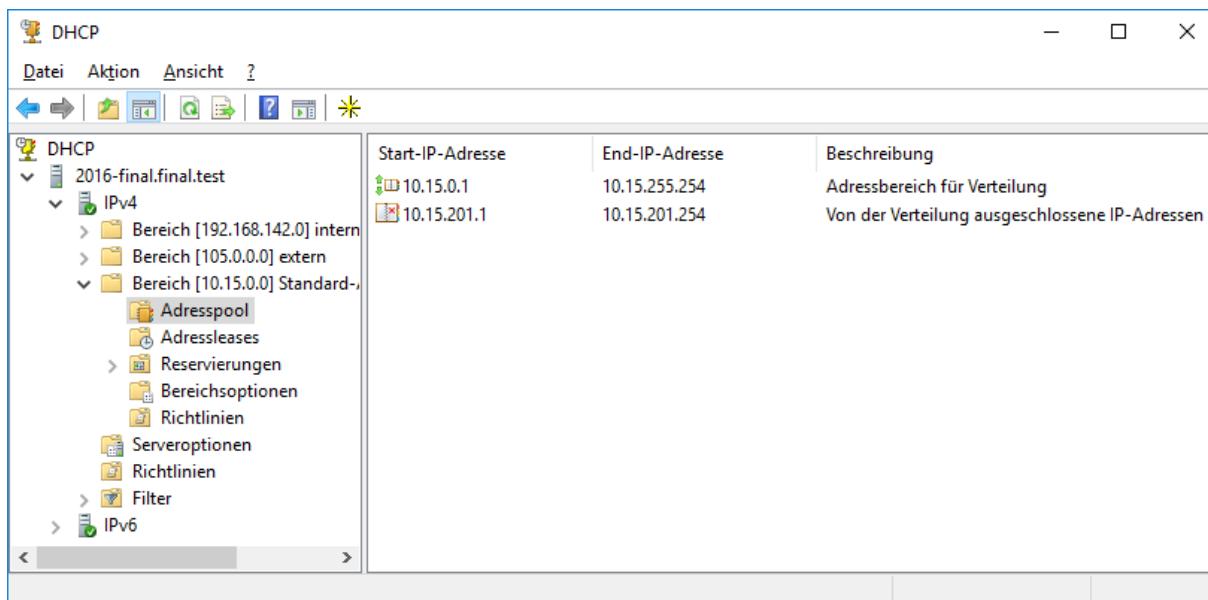
Optionen nur für DHCP

Nummer	Optionsname	Verwendung
50	Requested IP Address	IP-Adresswunsch eines DHCP-Clients
51	IP Address Lease Time	Gewünschte (Client) oder angebotene (Server) Lease-Dauer in Sekunden
53	DHCP Message Type	1: Discover, 2: Offer, 3: Request, 4: Decline, 5: Ack, 6: Nack, 7: Release, 8: Inform
54	Server Identifier	IP-Adresse zur Unterscheidung der DHCP-Server voneinander
55	Parameter Request List	DHCP-Optionsnummern zur Angabe der gewünschten Optionen durch den Client
58	Renewal (T1) Time Value	Renewal Time in Sekunden
59	Rebinding (T2) Time Value	Rebinding Time in Sekunden
61	Client Identifier	Eindeutige ID des Clients

Server-, Bereichs- und Reservierungsoptionen

Auf einem DHCP-Server können mehrere Bereiche (Scopes) eingerichtet werden, die jeweils über einen IP-Adresspool verfügen, eingerichtet werden. Auf vielen DHCP-Servern können mehrere Bereiche zu einer Bereichsgruppierung (Super scope) zusammengefasst werden. In einem Bereich können Reservierungen definiert werden, sodass vorher bestimmte Clients immer dieselbe statische IP-Adresse erhalten.

Aus welchem Bereich eine Lease anzubieten ist, kann anhand der im BootP-Datagramm angegebenen Router-IP-Adresse bzw. der IP-Adresse der Schnittstelle, auf der die Anfrage erhalten wurde, bestimmt werden. Die Router-IP-Adresse gibt entweder die IP-Adresse eines Relay Agent an, der aus dem auszuwählenden Bereich stammt, oder sie ist 0.0.0.0. Im letzteren Fall bestimmt die IP-Adresse der empfangenden Schnittstelle des DHCP-Servers den auszuwählenden Bereich.



Struktur der DHCP-Server-Verwaltungskonsole auf einem Microsoft Windows Server mit mehreren Bereichen

Bei der Konfiguration von DHCP-Optionen kann angegeben werden, für welche Clients diese Optionen gelten sollen. Die DHCP-Optionen werden deshalb in Server-, Bereichs- oder Reservierungsoptionen unterteilt.

Serveroptionen

Als Serveroptionen definierte DHCP-Optionen gelten für alle von einem DHCP-Server verwalteten Clients.

Beispiel: Die DHCP-Option 6 (Domain Name Server) enthält die IP-Adressen von DNS-Servern und wird häufig als Serveroption konfiguriert.

Bereichsoptionen

Sollen DHCP-Optionen nur für einen Bereich gelten, werden sie als Bereichsoptionen konfiguriert. Diese haben Vorrang gegenüber den Serveroptionen und überschreiben sie.

Beispiel: Gateway-Adressen sind nur für das jeweilige Subnetz gültig und werden deshalb als Bereichsoption eingestellt.

Reservierungsoptionen

DHCP-Optionen, die nur für einen bestimmten Client gelten sollen, werden in der für den Client vorgesehenen Reservierung konfiguriert.

Beispiel: Host-Namen werden eindeutig vergeben und deswegen als Reservierungsoption eingestellt.

11.5 Ausfallsicherheit unter DHCP/BootP

Warum DHCP-Server gegen Ausfälle geschützt werden müssen

Die Verwendung von DHCP vereinfacht die Verwaltung eines Netzwerkes und kann somit auch viele Fehler verhindern, die zu einem (Teil-)Ausfall eines Netzwerks führen können. Dabei darf aber nicht übersehen werden, dass DHCP auch neue Fehlerquellen eröffnet. So kann der Ausfall von DHCP-Servern und Relay Agents innerhalb relativ kurzer Zeit dazu führen, dass DHCP-Clients nicht mehr kommunizieren können, weil sie keine gültige IP-Konfiguration mehr haben. Eine solche Situation kann im Extremfall zum Ausfall ganzer Netzwerke führen.

Eine Möglichkeit, die negativen Auswirkungen des Ausfalls eines DHCP-Servers zu minimieren, ist die Redundanz von DHCP-Servern. Die Benutzung zweier oder mehr DHCP-Server kann **kooperativ** oder **nicht kooperativ** erfolgen. In der Windowswelt kann seit der Version Windows Server 2012 das neue Feature DHCP-Failover dazu eingesetzt werden, hohe Verfügbarkeit von DHCP zu ermöglichen. Zu diesem Zweck tauschen zwei DHCP-Server Verfügbarkeitsinformationen miteinander aus. Durch die Replikation von IP-Addressleases und Einstellungen der DHCP-Bereiche fungieren die Server als Failover-Partnerserver.

Kooperative Redundanz von DHCP-Servern

Bei kooperativen DHCP-Servern verfügen alle Server über denselben IP-Adresspool, dessen Verwendung sie stets miteinander abgleichen müssen. Es können entweder alle Server auf Client-Anfragen antworten oder die Server werden in **primäre Server** und **Standbyserver** unterteilt, wobei die Standbyserver nur darauf warten, dass ein primärer Server ausfällt, um dann dessen Rolle übernehmen zu können.

Als Folge eines Kabel- oder Router-Defektes könnte es zu der Situation kommen, dass das Netzwerk in zwei Bereiche (mit DHCP-Clients) unterteilt wird, in denen jeweils einer der DHCP-Server aktiv ist. Dann können drei Zustände eintreten:

- ✓ Beide Server nehmen an, dass ihr Partner ausgefallen ist, und verteilen weiterhin IP-Adressen. Solange die Netzwerke voneinander getrennt sind, können dann beide Teile ohne Konflikte weiterarbeiten. Sobald der Netzwerkfehler behoben wird, kann es (mitunter massiv) zu Adresskonflikten kommen, da beide Server eventuell die gleiche IP-Adresse an unterschiedliche Clients vergeben haben.

- ✓ Weil die Server nicht mehr miteinander kommunizieren können, stellen beide die Arbeit ein, um Adresskonflikte zu vermeiden. Das gesamte Netzwerk ist betroffen.
- ✓ Nur ein dazu vorher bestimmter Server bietet weiterhin seine Dienste an. Alle anderen stellen ihren Dienst ein. Ein Teil des Netzes funktioniert problemlos weiter. Werden die Netze wieder miteinander verbunden, können sich die DHCP-Server wieder abgleichen und die Arbeit wieder aufnehmen.

Sollte es sich bei einem der Server um einen Standby-Server handeln, wird dieser nun seine Dienste auch den Clients in seinem Bereich anbieten.

Nicht kooperative Redundanz von DHCP-Servern

Bei nicht kooperativen DHCP-Servern verwaltet jeder Server seinen eigenen IP-Adresspool. Um im Bedarfsfall auch diejenigen Clients, die normalerweise von anderen DHCP-Servern konfiguriert werden, mit IP-Adressen versorgen zu können, müssen die Adress-Pools entsprechend größer dimensioniert werden. Solange der Adress-Pool nicht erschöpft ist, gibt es für die Clients kein Problem.

Bei dieser nicht kooperativen Redundanz ist ein deutlich höherer Bedarf an IP-Adressen die Folge. Solange kein Ausfall eines DHCP-Servers auftritt, bleiben viele Adressen ungenutzt. Falls es sich um teure registrierte Adressen handelt, kann dieses Verfahren deshalb unwirtschaftlich sein.

Um die Anzahl der benötigten IP-Adressen zu berechnen, multiplizieren Sie die Anzahl der maximal gleichzeitig vergebenen Adressen mit [Anzahl DHCP-Server/(Anzahl DHCP-Server - 1)]. Wenn beispielsweise vier DHCP-Server maximal 150 Adressen vergeben können sollen, benötigen Sie 200 IP-Adressen, um gegen den Ausfall eines Servers gewappnet zu sein.



Andere Möglichkeiten zur Erhöhung der Ausfallsicherheit:

- ✓ Installieren von virtuellen DHCP-Servern in einem Servercluster
- ✓ Relay Agents vermeiden; das BootP-Forwarding auf Routern ist in der Praxis weniger fehleranfällig.

11.6 APIPA in kleinen Netzwerken

Grundlagen von APIPA

Microsoft entwickelte für kleine TCP/IP-Netze ein Verfahren zur automatischen Vergabe privater IP-Adressen (Automatic Private IP-Addressing). Diese Funktionalität ist bei allen Microsoft-Windows-Betriebssystemen implementiert. APIPA konfiguriert lediglich eine IP-Adresse und die passende Subnetzmaske. Adresseinträge für Gateways oder namensauflösende Dienste (DNS und WINS) werden nicht getätigt. Mit APIPA konfigurierte Clients können deshalb keine direkte Verbindung zu anderen Netzwerken oder dem Internet über ein Gateway aufnehmen.

APIPA wird dann verwendet, wenn ein Client für die automatische Adressvergabe konfiguriert wurde, aber die Vergabe einer Konfiguration über DHCP fehlschlägt. Dies kann passieren, wenn der DHCP-Server nicht erreichbar ist oder auch, wenn keine freien Adressen im verwendeten Bereich des DHCP-Servers zur Verfügung stehen.

APIPA eignen sich nur dann zur Verwendung in kleinen Netzwerken im SOHO-Bereich (Small Office/Home Office), wenn sie aus einem einzelnen logischen Netzwerk bestehen und keinerlei Kontakt zur „Außenwelt“ benötigen. Dies trifft allenfalls auf Testumgebungen zu. Zu bedenken gilt, dass bei einer beabsichtigten Konfiguration mit APIPA alle derart konfigurierten Clients etwa alle fünf Minuten erneut versuchen, sich über DHCP konfigurieren zu lassen. Rechtfertigt die Größe eines Netzwerks nicht den Einsatz eines DHCP-Servers, sollten IP-Adressen manuell vergeben werden. Letztlich kann man in der überwiegenden Mehrzahl der Fälle von einem Fehler ausgehen, wenn man auf APIPA-Adressen trifft.

Bei der IANA (Internet Assigned Numbers Authority) ist für die Verwendung von APIPA der IP-Adressbereich 169.254/16 reserviert. Genauso wie bei den nach RFC 1918 reservierten Bereichen 10/8, 172.16/12 und 192.168/16 werden Pakete mit Zieladressen aus diesem Bereich im Internet nicht weitergeleitet.

APIPA ist standardmäßig eingeschaltet, wenn das TCP/IP-Protokoll der entsprechenden Schnittstelle auf automatische Konfiguration eingestellt ist.

Der Suchprozess von APIPA

In der folgenden Abbildung sehen Sie die Auswertung eines Protokollanalyse-Tools, der den Vorgang der automatischen Konfiguration eines Interfaces verdeutlicht.

Bei Aktivierung der Netzwerkschnittstelle wird zuerst versucht, diese mithilfe von DHCP zu konfigurieren ①. Wenn der Host von einem DHCP-Server eine Lease erhält und die Konfiguration der Netzwerkschnittstelle mit diesem erfolgreich durchgeführt werden kann, ist die Konfiguration des TCP/IP-Protokolls für diese Schnittstelle beendet.

Erhält der Host keine Antwort von einem DHCP-Server oder ist die Konfiguration der Netzwerkschnittstelle mit den Parametern der erhaltenen Lease nicht möglich, wird versucht, das Interface durch APIPA zu konfigurieren.

APIPA wählt zunächst zufällig eine IP-Adresse aus dem Bereich 169.254/16 und weist diese der zu konfigurierenden Schnittstelle zu. Danach wird mithilfe von ARP versucht, genau diese IP-Adresse aufzulösen. Damit soll herausgefunden werden, ob diese Adresse nicht etwa schon von einem anderen Netzwerkknoten verwendet wird. Ist die gewählte Adresse im ARP-Cache vorhanden, gilt sie als bereits belegt und der Vorgang beginnt wieder von vorn.

Ist andererseits die Adresse nicht ARP-Cache eingetragen, werden über einen ARP-Request (an die Broadcast-MAC-Adresse ff:ff:ff:ff:ff:ff) alle in diesem Netzwerksegment erreichbaren Knoten aufgefordert, mit einem ARP-Reply zu antworten, falls sie mit dieser IP-Adresse konfiguriert sind ②. Falls ein anderer Knoten antwortet, werden dessen IP- und MAC-Adressen in den ARP-Cache eingetragen und der Vorgang beginnt mit der zufälligen Auswahl einer IP-Adresse von vorne.

Wenn andererseits auch nach drei ARP-Requests mit der gleichen IP-Adresse kein anderer Host antwortet, wird das lokale Netzwerkinterface mit dieser Adresse konfiguriert und der APIPA-Vorgang ist beendet ③. Es wird allerdings auch weiterhin in regelmäßigen Zeitabständen (ca. 5 min.) versucht, eine Konfiguration mit DHCP zu erreichen ④. Im Erfolgsfall wird das Interface dann neu konfiguriert.

No. .	Time	Source	Destination	Protocol	Info
①	1 0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85550773
	2 4.006048	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85550773
	3 11.006008	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85550773
	4 27.009022	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85550773
②	5 58.024446	Toplink_01:46:84	ff:ff:ff:ff:ff:ff	ARP	who has 169.254.168.78? Tell 169.254.168.78
	6 58.053487	Toplink_01:46:84	ff:ff:ff:ff:ff:ff	ARP	who has 169.254.168.78? Tell 169.254.168.78
	7 59.054940	Toplink_01:46:84	ff:ff:ff:ff:ff:ff	ARP	who has 169.254.168.78? Tell 169.254.168.78
③	8 60.076901	169.254.168.78	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
	9 60.081268	169.254.168.78	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
	10 60.103554	169.254.168.78	224.0.0.22	IGMP	V3 Membership Report
	11 60.637243	169.254.168.78	224.0.0.22	IGMP	V3 Membership Report
④	12 62.069830	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x671c929

Ablauf der automatischen IP-Konfiguration auf einem Windows-Rechner

Deaktivieren von APIPA

Wenn Sie Clients über DHCP konfigurieren und die Verwendung von APIPA bei einem Nichterreichen des DHCP-Servers ausschließen wollen, können Sie APIPA über einen neu zu erstellenden Registry-Eintrag deaktivieren.

Deaktivierung von APIPA auf einer Schnittstelle bei Betriebssystemen ab der Windows-2000-Familie	► Erstellen Sie im Registrierungsschlüssel <i>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\Adaptername</i> den DWORD-Eintrag <i>IPAutoconfigurationEnabled</i> und belegen Sie ihn mit dem Wert 0x0.
Deaktivierung von APIPA auf allen Schnittstellen bei Betriebssystemen ab der Windows-2000-Familie	► Erstellen Sie im Registrierungsschlüssel <i>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters</i> den DWORD- Eintrag <i>IPAutoconfigurationEnabled</i> und belegen Sie ihn mit dem Wert 0x0.

11.7 Übung

Fragen zu Netzwerkkonfigurationsdiensten

Übungsdatei: --

Ergebnisdatei: uebung11.pdf

1. Welche drei Möglichkeiten der automatischen Netzwerkkonfiguration kennen Sie?
2. Wofür wurde BootP ursprünglich entwickelt? Wofür wird es heute vermehrt eingesetzt?
3. Nach wie viel Prozent der Leasedauer versucht ein DHCP-Client erstmalig, seinen Lease zu erneuern (Renewal-Time)?
4. Welche Adresse fordert ein DHCP-Client an, wenn er während des Ablaufs seines Lease ausgeschaltet war?
5. Haben DHCP-Clients in der Regel unterschiedliche Adressen? Welche Rolle spielt dabei die Größe des Adresspools?
6. Wie viele Pakete werden zwischen DHCP-Server und -Client getauscht, bevor eine initiale Adressvergabe erfolgt?
7. Welche DHCP-Optionen sollten in der Regel als Serveroptionen, als Bereichsoptionen oder als Reservierungsoptionen vergeben werden?
8. Welche grundlegenden Mechanismen der Ausfallsicherheit kennen Sie zwischen DHCP-Servern?
9. Welchen Adressbereich verwendet APIPA?

12 ATM und LANE

In diesem Kapitel erfahren Sie

- ✓ was Asynchronous Transfer Mode ist
- ✓ wie ATM arbeitet
- ✓ was die Problematik bei der ATM-LAN-Emulation ist
- ✓ wie LANE eingesetzt werden kann

Voraussetzungen

- ✓ Netzwerkgrundlagen
- ✓ WAN-Grundlagen

12.1 ATM

Einordnung im OSI-Modell

Schicht 2: Sicherungsschicht (Data Link Layer)	ATM
Schicht 1: Bitübertragungsschicht (Physical Layer)	

ATM

Asynchronous Transfer Mode ist eine verbindungsorientierte Switching-Technologie für hohe Bandbreiten. Heute wird die ATM-Technik zur Unterstützung von Anwendungen von den globalen Internet- und Telefonie-Backbones über die DSL-Technik bis zum privaten LAN genutzt. Die Normung wurde nicht allein von der ITU (International Telecommunication Union; Internationale Fernmeldeunion) vorgenommen, sondern maßgeblich vom 1991 gegründeten ATM-Forum. Dies ging 2005 in das Broadband Forum (<http://www.broadband-forum.org>) über, dem auch andere herstellerübergreifende Foren für Hochgeschwindigkeitskommunikation wie das FrameRelay-Forum angehören.

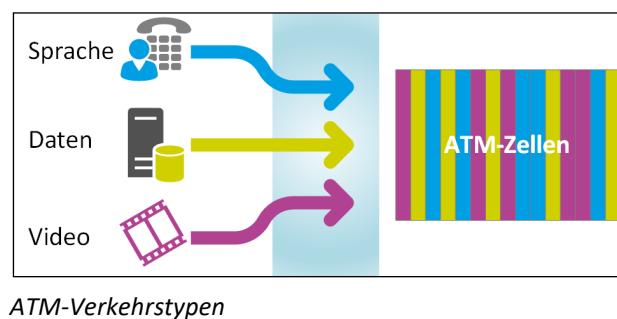
ATM wurde vom CCITT z. B. als Standard für B-ISDN vorgeschlagen. Unter dem Namen T-ATM bietet z. B. die Deutsche Telekom AG dazu einen Dienst an.

B-ISDN

Broadband Integrated Services Digital Network ist ein Vorschlag für einen Standard, der das vorhandene ISDN mit größerer Bandbreite beschreibt. B-ISDN ist dabei ein Versuch, Fernnetzdienste weltweit zu vereinheitlichen (ITU, 1990). Siehe auch <http://de.wikipedia.org/wiki/B-ISDN>.

Die ITU-T-Empfehlung I.121 gibt einen Überblick über die geplante Ausstattung von B-ISDN. Die Dienste werden auf der Basis von ATM realisiert.

ATM wurde ursprünglich für die moderne Telefonvermittlung und den WAN-Bereich entwickelt. Es kann für echtzeitfähige Anwendungen dienen (unter anderem Sprach- und Videoübertragung) und ist sehr gut für Multimedia-Anwendungen geeignet.

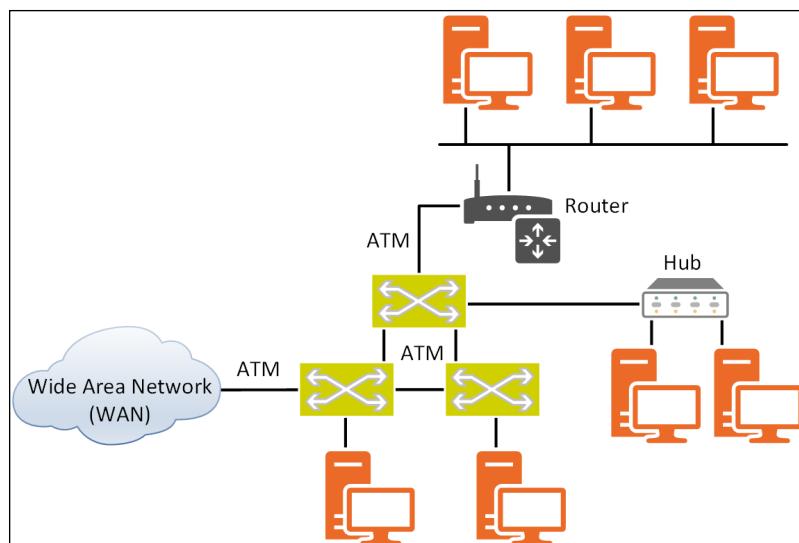


Beschreibung

B-ISDN und ATM benutzen ein eigenes Referenzmodell, das sich vom OSI-Modell unterscheidet. Es besteht im Kern aus drei Schichten, auf denen die Anwendungen aufbauen können:

- ✓ AAL (ATM Adaption Layer, ATM-Anpassungsschicht)
- ✓ ATM
- ✓ Physical

ATM ist weder an ein einzelnes Protokoll noch an ein bestimmtes Medium gebunden. Es können also Lichtwellenleiter genauso verwendet werden wie UTP verschiedener Kategorien. Im Vergleich zu herkömmlichen LANs, die eine Variation der Geschwindigkeit, Ausdehnung und Übertragungsmedien nur beschränkt zulassen, ist ATM deutlich besser geeignet für die verschiedensten Anforderungen, die an ein modernes Netz gestellt werden.



ATM-Netzwerk

Geschwindigkeit

Typische Arbeitsgeschwindigkeiten von ATM sind 25,6 Mbps, 34 Mbps, 155 Mbps oder 622 Mbps.

Übertragungskonzept

Die ATM-Übertragung basiert auf dem Konzept „virtueller Pfade“ (VP) und „virtueller Kanäle“ (VC), die jeweils durch eine Nummer (Identifier) eindeutig gekennzeichnet sind.

- ✓ VPI: Virtual Path Identifier
- ✓ VCI: Virtual Channel Identifier

Die gesamte Verbindung zwischen zwei ATM-Endgeräten kann daher als Folge von VPI/VCI-Paaren beschrieben werden oder als VCC (Virtual Channel Connection).

Die Trennung in Path und Channel lässt sich durchaus mit einem Vergleich zum Telefon erläutern, der bei ATM aufgrund seiner Entstehungsgeschichte nicht weit hergeholt ist. Für Vermittlungsstellen erscheint es sinnvoll, alle Gespräche mit der gleichen Vorwahl gebündelt an die Vermittlungsstelle dieser Vorwahl zu übertragen. Erst wenn der gesamte Übertragungsstrom dort angekommen ist, wird die Rufnummer des einzelnen Teilnehmers wieder wichtig. Für ATM könnte, um bei der Analogie zu bleiben, der VPI die Rolle der Vorwahl übernehmen und der VCI die der Rufnummer.



Verbindungstypen

Da ATM verbindungsorientiert arbeitet, benutzen alle Zellen einer Übertragung einen einmal festgelegten Übertragungsweg, den sogenannten "Virtual Circuit". Beim Aufbau dieses Weges lassen sich zwei Typen unterscheiden:

- ✓ **PVC:** Permanent Virtual Circuit bedeutet eine auf unbestimmte Zeit über eine zentrale Netzwerk-management-Station aufgebaute Verbindung.
- ✓ **SVC:** Switched Virtual Circuit bedeutet, dass die Verbindung nur für die Dauer der Übertragung bestehen bleibt.

Da bei PVC die Verbindung über einen langen Zeitraum bestehen bleibt, gibt es, im Unterschied zu SVC, keine explizite Verbindungsaufbauprozedur vor Beginn der Übertragung.

Vorteile

- ✓ Ein langfristiger Vorteil von ATM wird die einheitliche Verwendung im LAN, WAN und in den öffentlichen Netzen sein.
- ✓ Skalierbarkeit
- ✓ Optimale Ausnutzung der Bandbreite: Wenn eine Anwendung 2 Mbps braucht, wird dies garantiert. Andere weniger „zeitkritische“ Anwendungen erhalten die restliche Bandbreite.

12.2 ATM im Vergleich zu LAN

Starke Unterschiede zwischen ATM und herkömmlichen LAN-Technologien

Vor allem durch Arbeiten des ATM-Forums wurden die entscheidenden Standards zum Einsatz von ATM im LAN definiert. Diese Standards sind auch dringend notwendig, da sich ATM von herkömmlichen LAN-Technologien zum Teil gravierend unterscheidet.

Zugriff

Bei ATM ist jeder Benutzer grundsätzlich direkt mit einem Switch verbunden, über den mehrere Verbindungen simultan abgewickelt werden können. In einem herkömmlichen LAN müssen sich die Benutzer das Übertragungsmedium teilen (shared) und es kann pro Zeitpunkt nur eine Übertragung stattfinden.

Verbindung

ATM arbeitet verbindungsorientiert, d. h., bei einem Verbindungsaufbau wird geprüft, ob die gewünschte Übertragungskapazität im Netz verfügbar ist. Bevor Daten von der Quell- zur Zielstation übertragen werden, wird der genaue Übertragungsweg festgelegt. Ein herkömmliches LAN arbeitet verbindungslos, d. h., die Daten werden nach dem Broadcast-Verfahren an alle Teilnehmer des Netzwerks geschickt.

Paketlänge

ATM verwendet kleine Datenpakete mit fester Länge, sogenannte Zellen. Eine ATM-Zelle besteht aus 53 Byte, die sich aus 5 Byte (Header) für Steuerinformationen und 48 Byte (payload) für Daten zusammensetzen. Die Länge von Paketen in herkömmlichen LANs ist variabel und reicht von einigen wenigen Bytes bis weit über 1 Kilobyte.

Geschichte

Die Anzahl 48 ergab sich als Kompromiss zwischen amerikanischen Interessen (dort sind 64 Byte Nutzdaten und 5 Byte große Header weit verbreitet) und europäischen Gewohnheiten (hier werden häufig 32 Byte für Informationen und 4 Byte für Steuerdaten verwendet).

Übertragungsverzögerung

Die Zeit zwischen zwei zusammengehörigen Zellen ist definiert. Dadurch ist ATM für Multimedia-Anwendungen (insbesondere Sprachübertragung) besser geeignet als z. B. Ethernet. Dort können aufgrund der variablen Länge der Pakete keine Angaben über Verzögerungen gemacht werden. Durch das Zugriffsverfahren CSMA/CD kommt noch die Zufälligkeit der Zugriffszeit hinzu.

Priorität

Bei ATM ist es möglich, Serviceklassen bezüglich der Dienstgüte einzurichten. Das bedeutet z. B., dass je nach Art der gewünschten Übertragung (Sprache, Daten, Video) bestimmte Bandbreiten garantiert werden können oder dass je nach Bedarf ein kontinuierlicher oder sporadischer Übertragungsprozess stattfindet. In einem herkömmlichen LAN (mit einer kleinen Ausnahme bei Token Ring) werden alle Daten von der Bedeutung her gleichgestellt. Die Priorisierung ist eine wichtige Voraussetzung für QoS (Quality of Service, Dienstqualität).

Zusammenfassung

Zum Abschluss finden Sie nun eine Gegenüberstellung der einzelnen Punkte in Tabellenform:

LAN-Techniken	ATM
Broadcast/Filterung	Virtuelle Verbindungen
Nur ein aktiver Sender gleichzeitig	Mehrere aktive Sender gleichzeitig
Ein Medium – eine Geschwindigkeit	Verschiedene Medien – verschiedene Geschwindigkeiten
Verbindungslos	Verbindungsorientiert
Bus- und Ringtopologie	Sterntopologie mit ATM-Switch

Aktuelles bzw. Zukünftiges

Obwohl beispielsweise die klassischen Telekommunikationsnetzbetreiber enorme Summen in ATM-Infrastruktur investierten, kam ab etwa dem Jahr 2000 für immer mehr Anwendungen andere, oft Ethernet-basierte Technik statt ATM (aus Preisgründen und wegen des einfacher zugänglichen Know-hows) zum Einsatz.

ATM wird auch im Backbonebereich der Internet Service Provider in Zukunft keine große Rolle mehr spielen, sondern durch Ethernet-basierte Technik und IP-basierende VPNs abgelöst.

Obwohl ATM als Technik damit wohl nicht mehr zukunftsträchtig ist, werden einige der mit ATM gewonnenen Forschungserkenntnisse in anderen Netztechnologien weitergenutzt, wie etwa bei MPLS (Multiprotocol Label Switching).

12.3 LAN-Emulation (LANE)

LANE

Aufgrund dieser grundsätzlichen konzeptionellen Unterschiede zwischen ATM und herkömmlichen LANs sind mehrere Mechanismen nötig, um z. B. ein Ethernet-Netz und ein ATM-Netz miteinander zu verbinden. Die vom ATM-Forum spezifizierte LAN-Emulation ist ein Verfahren, um verbindungslose LAN-Protokolle in ATM-Netzen zu nutzen.



Das im Jahr 1991 gegründete ATM-Forum ist inzwischen Teil des IP/MPLS-Forums (Internet-Protokoll/Multi-protocol Label Switching), einer Non-Profit-Organisation, der u. a. viele Hersteller von Netzwerkkomponenten angehören (<http://www.broadband-forum.org/>).

Das Prinzip baut auf der Abbildung von MAC-Adressen auf ATM-Adressen auf. Dadurch ist dieses Verfahren für die höheren Schichten transparent. Als Schnittstelle wurde LUNI (LAN Emulation User to Network Interface) geschaffen. Dazu gehören z. B.:

- ✓ LEC: LAN Emulation Client
- ✓ LECS: LAN Emulation Configuration Server
- ✓ LES: LAN Emulation Server
- ✓ BUS: Broadcast and Unknown Server

LAN Emulation Client

Der LAN Emulation Client (LEC) stellt die Schnittstelle zwischen LAN und ATM-Netz dar. Jedes Gerät, das über das ATM-Netzwerk kommunizieren möchte, muss einen LEC implementiert haben. Aufgabe des LEC ist es dabei, die Netzwerkadresse (MAC) auf eine ATM-Adresse abzubilden. Jedes ATM-Endsystem muss eine MAC-Adresse und eine ATM-Adresse aufweisen, um so zwischen den beiden Netzwerktypen vermitteln zu können.

LAN Emulation Configuration Server

Die Verwaltung des emulierten LANs wird von dem LECS erfüllt. Er steuert die Vergabe von ATM-Adressen, von E-LANs und informiert den BUS über die vorhandenen Adressen von LECs und LESs.

LAN Emulation Server

Der LAN Emulation Server (LES) hat die Aufgabe, zwischen MAC und ATM-Adressen zu vermitteln. In jedem emulierten LAN muss ein LES Anfragen mittels LE-ARP (LAN-Emulation-Address-Resolution-Protokoll) beantworten, um die beiden Welten miteinander zu verbinden.

Broadcast and Unknown Server

Der BUS muss alle Knoten im LANE kennen und Broadcasts als zielgerichtete Sendungen weitervermitteln, da ATM als verbindungsorientiertes Protokoll keine Broadcasts kennt.

Weitere Möglichkeiten

Neben dem Ansatz LANE gibt es noch zwei weitere Ansätze, um ATM und LAN näher zusammenzubringen:

- ✓ Classical IP over ATM
- ✓ MPOA (Multi-Protocol over ATM)

12.4 Übung

Fragen zu ATM und LANE

Übungsdatei: --

Ergebnisdatei: uebung12.pdf

1. Ist ATM eine verbindungsorientierte oder eine verbindungslose Technik?
2. Lässt sich ATM im ISO/OSI-Modell einbinden?
3. Welche Arten von Daten können mithilfe von ATM übertragen werden?
4. Wie groß sind die ATM-Zellen?
5. Beschreiben Sie den Vorteil der festgelegten Zellgröße.
6. Was sind VPI und VCI?
7. Erläutern Sie die Konzepte von PVC und SVC.
8. Was sind die grundlegenden Unterschiede zwischen einem Ethernet und einem ATM-Netzwerk?
9. Welche Auswirkungen hat dies auf Broadcasts und Multicasts?
10. Die folgende Tabelle enthält die Abkürzungen der wichtigsten Komponenten für LANE. Schreiben Sie diese aus und erläutern Sie ihre Aufgaben:

Abkürzung	LANE-Komponente	Beschreibung
LEC		
LECS		
LES		
BUS		

13 DSL

In diesem Kapitel erfahren Sie

- ✓ welche DSL-Technologien es gibt
- ✓ welche Geräte Sie dafür benötigen
- ✓ welche Netzwerkprotokolle eingesetzt werden

Voraussetzungen

- ✓ Verständnis der verwendeten Netzwerkprotokolle

13.1 Grundlagen zu DSL

Entwicklung

Der immer stärker wachsende Bedarf an Übertragungsbandbreite in Weitverkehrsnetzwerken führte bereits in den 80er-Jahren zu Überlegungen, wie man diesem Anspruch auch im Massenmarkt flächendeckend, kostengünstig und kurzfristig gerecht werden kann. Vor allem die analogen Teilnehmeranschlüsse zum Kernnetz erwiesen sich diesbezüglich als Nadelöhr. DSL bedeutet Digital Subscriber Line (digitale Teilnehmeranschlussleitung) und bezeichnet die Digitalisierung der sogenannten „letzten Meile“, also des Telefonkabels bis zum Endkunden. Mithilfe der DSL-Technologien ist eine digitale Nutzung des flächendeckend auf Basis von Kupferleitungen vorhandenen Telefonnetzes möglich geworden.

Mit POTS (Plain Old Telephone Service) wird das herkömmliche analoge Telefonnetz bezeichnet. Es belegt lediglich einen Frequenzbereich von 300 Hz – 3,5 kHz auf den Kupferkabeln und kann mithilfe von Modems bis zu 56 kbit/s Rohdaten übertragen. ISDN war die erste DSL-Technik und erreicht durch eine Ausdehnung des verwendeten Frequenzbereiches auf 0 Hz – 50 kHz eine Bruttodatenrate von 160 kbit/s in Sende- und Empfangsrichtung (Verwendung eines BRI, Basic Rate Interface).

Damit ist die Übertragungskapazität der verwendeten Kupferdoppeladern aber noch nicht ausgereizt. Die Verwendung moderner Modulationstechniken und eine Erhöhung der verwendeten Bandbreite bis in den MHz-Bereich hinein ermöglicht Datenraten von bis zu 1000 Mbit/s.

Einteilung der DSL-Technologien

Die einzelnen DSL-Technologien werden unter dem Begriff xDSL subsumiert und unterscheiden sich vor allem durch die Anzahl der benutzten Adernpaare, die belegten Frequenzbänder und die Modulationsarten:

Dienst		Modula-tion	Frequenzband von ... bis	Datenrate bis	Distanz bis	Adern-paar
POTS	Plain Old Telephone Service		300 Hz - 3,4 kHz	56 kbit/s		2
ISDN	Integrated Services Digital Network		0 Hz - 120 kHz	144 kbit/s (2 x 64 + 16)		1
HDSL	High Data Rate DSL	CAP	0 Hz - 292 kHz	2 Mbit/s	5 km	2 - 3

Dienst		Modula-tion	Frequenzband von ... bis			Datenrate bis	Distanz bis	Adern-paar
SDSL	Symmetrical DSL	PAM	0 Hz	-	387 kHz	2 Mbit/s	3,5 km	1
ADSL up	Asymmetric DSL	CAP oder DMT	25 kHz	-	138 kHz	640 kbit/s	5,5 km	1
ADSL down			138 kHz	-	1,1 MHz	8 Mbit/s		
ADSL2+	Asymmetric DSL2+	DMT, RE-ADSL2	138 kHz	-	2,2 MHz	25 Mbit/s	5,5 km	1
VDSL	Very High Data Rate DSL	CAP, DMT, DWMT und SLC möglich	200 kHz	-	30 Mhz	52 Mbit/s	1,5 km	1
VDSL2	Very High Data Rate DSL2	CAP, DMT, DWMT und SLC möglich	300 kHz	-	30 Mhz	100 Mbit/s	3 km	1

Wenig verbreitete Varianten sind BDSL (Broadband DSL) und UDSL (Universal DSL).

Deutschland, die Schweiz und Österreich im Vergleich

Besonders in ländlichen Gebieten Deutschlands ist ADSL immer noch nicht flächendeckend verfügbar. Da dort die Leitungen zur nächsten Vermittlungsstelle oft sehr lang sind, ist die Mindest-Übertragungsrate von 768 Kbit/s meist nicht erreichbar. Deshalb wird dort mitunter eine Sparversion mit 384 Kbit/s mit Namen „DSL-Light“ angeboten. Eine andere Lösung, die mit DSL nichts zu tun hat, bieten Schmalbandtarife, also Zeittarife oder Flatrates für die Einwahl über ISDN oder ein analoges Modem.

In Österreich dagegen können schon heute 97 % aller Haushalte mit DSL angebunden werden (Quelle: Telekom Austria).

In der Schweiz ist ein gesetzlich garantiertes Recht auf schnelle Anbindung mit mindestens einem Mbit/s downstream festgelegt worden (1. März 2012). Dies wird zurzeit zu 98 % gewährleistet (laut Swisscom, dem beauftragten Universaldienstanbieter), für die verbleibenden 2 % sollen u. U. Satellitenanbindungen genutzt werden.

T-DSL, M-DSL und Q-DSL sind Produktbezeichnungen für ADSL. Sky-DSL bezeichnet einen Teilnehmeranschluss per Satellit (downstream) und eine herkömmliche Modem-/ISDN-Verbindung (upstream). 

Eine Besonderheit von ADSL ist die asymmetrische Aufteilung der Gesamtbandbreite. Insbesondere Privatkunden empfangen im Allgemeinen deutlich mehr Daten, als sie senden. Die Sendedatenrate (upstream) wurde deshalb zu Gunsten einer höheren Empfangsdatenrate (downstream) begrenzt. Der überwiegende Teil von DSL-Anschlüssen, die heute geschaltet werden, sind ADSL- oder die schnelleren ADSL2+-Anschlüsse.



ADSL-Beispiel über FRITZ!Box mit 25Mbit/s Download- und 5 Mbit/s Uploadgeschwindigkeit

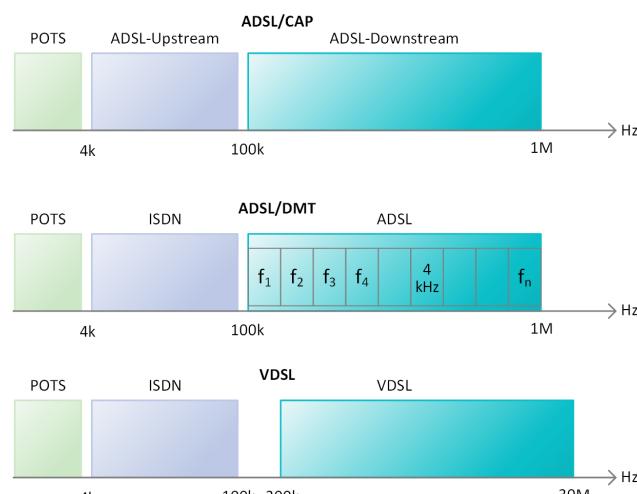
Modulationsarten

- ✓ **PAM:** Pulsed Amplitude Modulation
- ✓ **DMT:** Discrete Multitone Modulation
- ✓ **DWMT:** Discrete Wavelet Multitone Modulation, Variante von DMT
- ✓ **CAP:** Carrierless Amplitude/Phase Modulation, Variante von Quadratur Amplitude Modulation QAM
- ✓ **SLC:** Simple Line Code

Die CAP-Modulation erzeugt ein trägerloses Signal, bei dem Up- und Downstream in voneinander getrennten Frequenzbereichen stattfinden.

Die DMT-Modulation teilt das verwendete Frequenzband in 32 Upstream- und 256 Downstream-Kanäle mit jeweils 4kHz Bandbreite auf, deren Qualität überwacht wird. Bei Störungen in einzelnen Frequenzbändern kann dann die Bitrate in diesen Bändern abgesenkt oder ganz auf alternative Kanäle umgeschaltet werden. Die DMT-Modulation wird vor allem bei ADSL immer häufiger verwendet und scheint sich auch auf Dauer durchzusetzen.

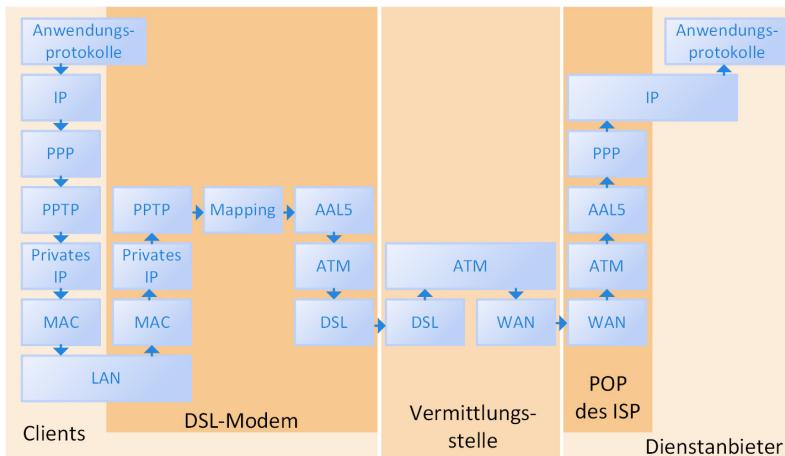
VDSL verwendet verschiedene Modulationsarten (vgl. vorhergehende Tabelle).



Die überbrückbare Distanz bei gegebener Datenrate hängt in erster Linie von Übersprechdämpfung, Dämpfung, Querschnitt und Reflexionsverhalten des Kabels ab. Sogenannte ratenadaptive Systeme können zugunsten einer höheren Reichweite die Datenrate absenken.

Protokolle

PPP wird zwischen Client und ISP eingesetzt, um die Konfiguration von IP, eine Authentifizierung des Users und die Abrechnung der Verbindung beim ISP zu ermöglichen. Somit ist die Verwendung von DSL einer klassischen Einwahl über analoge Modems sehr ähnlich und die Internet-Provider können weiterhin z. B. RRAS und RADIUS verwenden. Um im LAN des Teilnehmers PPP-Verbindungen verwenden zu können, ist ein Treiber für PPPoE (PPP over Ethernet) oder PPPoA (PPP over ATM) nötig.



Protokollstapel zwischen Client und Server bei Verwendung von PPP und PPTP

Beim Mapping im Modem wird das Point-to-Point-Tunneling beendet und die PPP-Verbindung über eine Virtual Circuit in ATM weitergeführt. Bei Standleitungen ist das PPP normalerweise überflüssig und wird deshalb meist nicht verwendet.

POTS, ISDN und xDSL auf einem Adernpaar

Die gleichzeitige Verwendung von HDSL und POTS oder ISDN auf einer Leitung ist nicht möglich, da diese DSL-Technik den gesamten verfügbaren Frequenzbereich benutzt. SDSL kann POTS oder ISDN in DSL integrieren und stellt dann zusätzlich analoge a/b-Anschlüsse oder eine S₀-Schnittstelle zur Verfügung, ein NTBA ist überflüssig.

Bei ADSL ist eine gleichzeitige Verwendung des POTS durch Verwendung eines sogenannten POTS-Splitters (Telekomname NTBBA, Network-Termination-Breitbandanschluss) möglich. Dieser Splitter arbeitet wie eine Frequenzweiche und stellt jeweils Anschlüsse für DSL-Verbindungen und analoge Telefonie zur Verfügung.

Bezüglich ISDN gibt es zwei Möglichkeiten: Je nach DSL-Anbieter kann die untere Grenze des von DSL genutzten Frequenzbandes so niedrig sein, dass ISDN gestört wird. Digitale ISDN-Dienste müssen dann in die Datenpakete, die per DSL übertragen werden, eingekapselt werden (wie bei SDSL). Wenn die untere Grenzfrequenz des ADSL-Bandes hoch genug liegt, wird das ISDN-Signal nicht gestört und kann dann mit einem ISDN-Splitter (NTBBA) vom ADSL-Signal getrennt werden. VDSL erfordert einen Splitter für POTS und ISDN.

Normen und Standards

Standard	Gremium/Institut	Norm
HDSL	ETSI (European Telecommunications Standards Institute)	ETR152
SDSL	ETSI, ITU	G.shdsl
ADSL	ANSI (American National Standards Institute) ITU (International Telecommunication Union)	T1.413 G.992.1, G.992.2
ADSL2	ITU	G.992.3, G.992.4
ADSL2+	ITU	G.992.5
VDSL	ITU	G.993.1
VDSL2	ITU	G.993.2

Der U-R2-Schnittstellenstandard für ADSL

2001 entwickelte die Deutsche Telekom den Standard 1TR112 für ADSL-Schnittstellen, der besser bekannt ist unter dem Namen U-R2. In diesem Standard wurden verschiedene Parameter der bisherigen ADSL-Standards präzisiert, um ADSL-Modems und DSLAMs verschiedener Hersteller miteinander kompatibel zu machen. Die einzelnen ADSL-Technologien unterschieden sich bisher so sehr, dass meist nur ADSL-Modems und ADSL-Access-Multiplexer eines Herstellers miteinander funktionierten.

U-R2 standardisiert nun neben DMT als Modulationsverfahren und 130 kHz Trennfrequenz für die Splitter (ADSL over ISDN) auch Pinbelegung und Bauform der verwendeten Steckverbinder. Auch der Ablauf des Handshakes beim Aufbau der Verbindung und wichtige Parameter des ATM-Protokolls werden spezifiziert (Adressformat von VCI und VPI, Zellformat, Flusskontrolle). Dem U-R2-Standard entsprechende Geräte müssen bei einer Reichweite von minimal 2800 m eine Bruttodatenrate von mindestens 160 kBit/s upstream und 864 kBit/s downstream erzielen, nach oben sind bei den Übertragungsraten jedoch keine Grenzen gesetzt, sodass auch moderne ADSL2+-Modems mit 25 Mbit/s-Downstreamrate einen U-R2-Anschluss haben können.

Seit Oktober 2001 sind alle in Deutschland verkauften DSL-Modems (bzw. Router mit integrierten DSL-Modems und ähnliche Geräte) mit dieser Schnittstelle ausgestattet und erleichtern die Interoperabilität der DSL-Komponenten um ein Vielfaches.

14 Frame Relay

In diesem Kapitel erfahren Sie

- ✓ was Frame Relay ist
- ✓ wie Frame Relay arbeitet
- ✓ welche Leistungsmerkmale Frame Relay von X.25 und ATM unterscheiden

Voraussetzungen

- ✓ Netzwerkgrundlagen
- ✓ OSI-Modell
- ✓ X.25

14.1 Grundlagen zu Frame Relay

Frame Relay, ein Nachfolger von X.25

Bei Frame Relay handelt es sich um eine schnelle Paketvermittlung, die in der Folge von X.25 entwickelt wurde. Einsatzgebiete von Frame Relay sind vor allem im Bereich der Weitverkehrsnetze, es wird aber auch als Zubringerdienst für andere Netzwerkdienste verwendet (z. B. B-ISDN).

Entstehung

Frame Relay wurde Mitte der 80er-Jahre in den USA entwickelt. Die erste RFC zu Frame Relay stammt vom Januar 1992 und ist inzwischen durch RFC 2427 ersetzt worden. Basierend auf den Mechanismen von X.25 wurde ein schnellerer paketorientierter Dienst benötigt, bei dem - zugunsten einer höheren Geschwindigkeit – auf Mechanismen der Fehlererkennung und -beseitigung gegenüber X.25 verzichtet werden konnte. Die Hauptgründe für die Einführung von Frame Relay waren:

- ✓ neue Anwendungen benötigen große Datenmengen in kurzer Zeit (z. B. Bilddaten),
- ✓ die Verbreitung zuverlässiger und schneller Leitungen (Glasfaser),
- ✓ zunehmende Verbreitung von Datenendgeräten (PCs, Server und Hostrechner).

Frame Relay Forum

Gefördert wird die Entwicklung von Frame Relay maßgeblich durch das Frame Relay Forum, einen Zusammenschluss von Firmen und Institutionen, die dieser Technologie auf diese Weise weiteren Rückhalt gewähren. Zu den Mitgliedern gehören alle wichtigen Telekommunikationsunternehmen der Welt sowie Entwickler von Kernkomponenten wie etwa Cisco, Bell oder Lucent.

Wie auch das ATM-Forum ist das Frame Relay Forum in das Broadband Forum übergegangen (www.broadband-forum.org). Dort können Sie sich über die Technologie informieren und zahlreiche Beschreibungen, Handbücher und Whitepapers zu der Thematik herunterladen.

OSI-Einordnung

Schicht 2: Sicherungsschicht (Data Link Layer)	Frame Relay
Schicht 1: Bitübertragungsschicht (Physical Layer)	

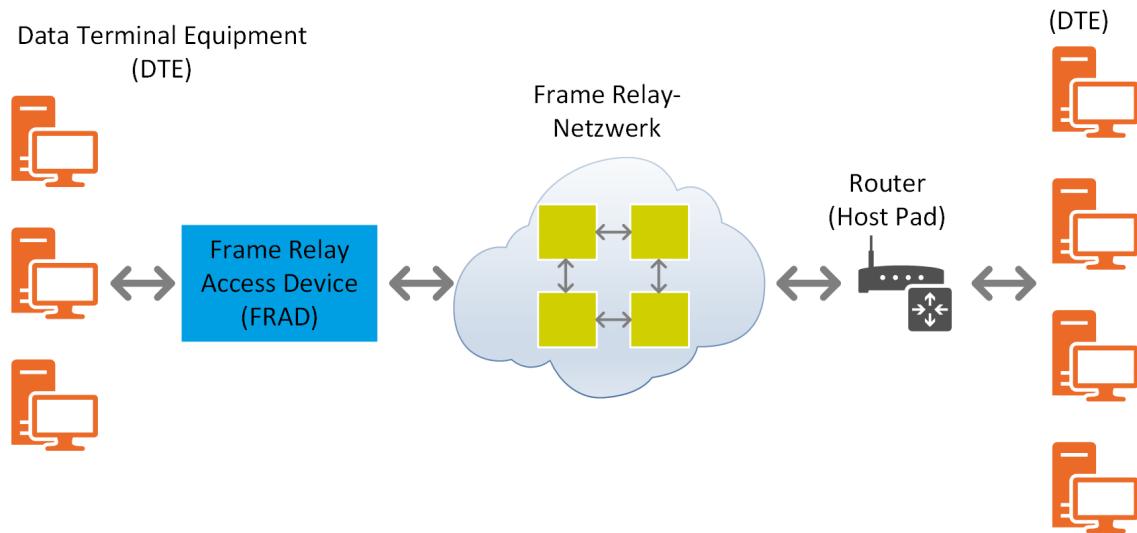
Begriffe

Im Zusammenhang mit Frame Relay finden sich viele Begriffe wieder, die vom X.25-Protokoll stammen. Der Übersichtlichkeit halber sollen auch diese hier noch einmal vollständig erläutert werden.



EUD	End User Device Endpunkt	EUDs sind z. B. Workstations, Server oder Hostrechner, also die Geräte, von denen oder auf die ein Benutzer über das Netz zugreift.
DTE DEE	Data Terminal Equipment Datenendeinrichtung	Bei DTEs kann es sich um Geräte wie eine Bridge, einen Router oder ein Gateway handeln, der ein LAN mit einem Remote-Netzwerk oder WAN verbindet, es kann jedoch auch ein Hostrechner sein, der direkt auf ein Remote-Netzwerk zugreift. Man könnte z. B. ein Modem als DTE eines Hostrechners verstehen.
FRAD	Frame Relay Access Device Frame-Relay-Zugangseinrichtungen	Das Frame Relay Forum bezeichnet ein DTE zum Zugriff auf ein Frame-Relay-Netzwerk als FRAD. Vergleichbar ist dies etwa mit einem Multiprotokoll-Router, der IP, IPX oder SNA-Pakete in Frame-Relay-Pakete umwandelt.
PAD	Packet Assembler/Disassembler	Übersetzt bei Bedarf die Daten der DTEs in Pakete für das Netzwerk
PDN	Public Data Network	Öffentliches Datennetz
PVC	Permanent Virtual Circuit Feste virtuelle Verbindung	In einer Netzwerkwolke werden Wege zwischen zwei Stationen konstant eingerichtet. Der Weg, den ein Datenpaket nimmt, ist im Voraus bekannt. Erfolgt eine Unterbrechung, wird die Verbindung automatisch wieder hergestellt. Der virtuelle Charakter kommt durch das Simulieren einer Verbindung in einer Wolke zustande.
SVC	Switched Virtual Circuit Geschaltete virtuelle Verbindung	Eine virtuelle Verbindung, die bei Bedarf aufgebaut und nach Beendigung der Kommunikation wieder abgebaut wird, vergleichbar mit einer Telefonverbindung, bei der auch nur für die Dauer der Verbindung eine Leitung geschaltet wird.

Frame-Relay-Netzwerk



Daten aus diversen Netzwerken werden über Host-PADs, FRADs oder andere DTEs in ein Frame-Relay-Netzwerk eingespeist. Das Frame-Relay-Netzwerk ist dabei als Wolke strukturiert. Es sind also keine festen Wege vorgegeben, sondern diese können bei Bedarf generiert werden.

14.2 Frame Relay in der Praxis

Weltweite Verfügbarkeit

Frame Relay ist heute ein weltweit verbreiteter Dienst, der im WAN-Bereich dazu dient, LANs zu koppeln. Da Frame Relay multiprotokollfähig ist, können so auch unterschiedliche Netze zusammenarbeiten. Beispielsweise ist es durchaus möglich, heterogene WAN-Netze zu betreiben, in denen neben Frame Relay auch B-ISDN oder ATM eingesetzt werden.

Multiprotokollfähigkeit

Die Multiprotokollfähigkeit von Frame Relay ist (neben der Qualität heutiger Glasfasernetze) der Hauptgrund, warum auf eine zeitintensive Fehlerkennung verzichtet werden kann. Denn indem Protokolle wie TCP, das eine eigene Fehlerkennung auf Schicht 4 benutzt, über Frame Relay verwendet werden, kann die Effizienz gegenüber X.25 deutlich gesteigert werden. Auch für Neuentwicklungen wie etwa IPv6 gilt, dass diese in Anpassung an Frame Relay zur Verfügung stehen müssen.

Verzicht auf Netzwerkschicht

Während X.25 noch mit einem eigenen Netzwerkprotokoll auf Schicht 3 (Network) arbeitet, arbeitet Frame Relay ohne Layer-3-Protokoll. Dadurch lässt sich eine wesentliche Beschleunigung der Kommunikation erreichen.

Arbeitsweise

Jedem Frame Relay Paket wird im Header eine Adresse beigefügt, die das Ziel kennzeichnet. Diese wird als DLCI (Data Link Connection Identifier = Datenstrecken-Verbindungskennung) bezeichnet. Wenn nun ein Paket an eine bestimmte DLCI geschickt werden soll, kann die Übermittlung dadurch erfolgen, dass alle möglichen DLCIs im Netzwerk bekannt sind und entsprechend an die richtigen Netzwerkkomponenten versandt werden.

Dabei erfolgt allerdings keine Reservierung der benötigten Bandbreite wie etwa unter ATM. Es kann also auch zu Fehlern aufgrund von Leistungsüberlastungen kommen. Entweder können die Eingangs-Buffer eines Frame Relay-Switches überlaufen oder ein Engpass auf der folgenden Leitung kann zu einem Überlauf des Ausgangs-Buffers führen.

Kann einmal ein Paket nicht weiterbefördert werden, weil es beschädigt ist oder die Leitung oder ein Switch überlastet ist, wird dieses ohne weitere Beachtung verworfen. Korrekturen (etwa das erneute Anfordern eines verworfenen Paketes) übernehmen dann höhere Protokolle (etwa TCP).

Ergebnis

Es ergibt sich, dass Frame Relay eine sehr effiziente und relativ schnelle Kommunikationsform darstellt, solange die zur Verfügung stehenden Leitungen entsprechend hochwertig und großzügig dimensioniert sind. Werden aber zeitkritische Daten transportiert (etwa moderne Multimediadaten), kann Frame Relay nicht eingesetzt werden. Hier liegen die Einsatzgebiete von ATM und anderen Diensten, die für die Dauer einer Verbindung Bandbreiten garantieren können.

Frame Relay wird zunehmend von Produkten ersetzt, die auf IP basieren. Vor allem übernehmen Virtuelle Private Netze als preiswertere und MPLS-Netze als Breitbandalternative das Marktsegment von Frame Relay.

14.3 Frame Relay im Vergleich zu ATM und X.25

Gegenüberstellung

Abschließend können Sie hier die Vor- und Nachteile von ATM (Time-Division-Multiplexing-Verfahren), X.25 und Frame Relay im Vergleich sehen.

	Frame Relay	X.25-Paketvermittlung	ATM
Multiplexing-Verfahren	Statisches Multiplexing	Statisches Multiplexing	Zeitmultiplexing
Portnutzung	Gemeinsam	Gemeinsam	Getrennt
Leitungsqualität	Hoch	Niedrig	Hoch
Geeignet für zeitkritische Datenübertragung	Nein	Nein	Ja
Geschwindigkeit	Hoch	Niedrig	Hoch
Verzögerung	Niedrig	Hoch	Sehr niedrig

15 RAS und NPS

In diesem Kapitel erfahren Sie

- ✓ was den Remote Access Dienst vom RAS-Protokoll (H.323) unterscheidet
- ✓ was Remote Access Service für Aufgaben hat und wozu RAS eingesetzt wird
- ✓ was Network Policy Server sind
- ✓ wie Sie den Netzwerkzugriff mit NPS steuern können
- ✓ welche Arten von Authentifizierung verwendet werden

Voraussetzungen

- ✓ Netzwerkgrundlagen
- ✓ IP-Grundlagen
- ✓ WAN-Protokolle

15.1 Remote Access Service

Remote Access Service

Remote Access Service (Fernzugriffsdiest, RAS) ist eine Sammlung von Protokollen und Anwendungen, die die Aufgabe haben, Benutzern den Fernzugriff auf Daten und Dienste eines LANs zu gewähren. Mit der zunehmenden Verbreitung von Telearbeitsplätzen, verteilten Netzen und dem Bedarf an ständiger Aktualisierung von Daten kommt dem Fernzugriff eine immer größere Bedeutung zu.

Zum Beispiel müssen Außendienstmitarbeiter heutzutage ständig mit dem Firmennetz in Verbindung stehen, um Preislisten, Lagerbestände und Produktinformationen abzulegen. Hier kann eine zeitliche Verzögerung von wenigen Stunden bereits finanzielle Einbußen zur Folge haben, wenn etwa Lieferzeiten nicht mehr eingehalten werden können.

Auch die Fernwartung von Rechnersystemen gewinnt immer mehr an Bedeutung. Ein Administrator kann Netzwerkkomponenten von der Hauptstelle aus (oder auch problemlos aus dem Homeoffice) verwalten, spart so Fahrtkosten und -zeiten und kann schneller auf Probleme in Außenstellen reagieren.

Begriffliche Abgrenzung: RAS ungleich RAS-Protokoll

Das eigentliche RAS-Protokoll stellt ein Unterprotokoll von H.323, einer Protokollsammlung für Multimedia-Anwendungen und Konferenzübertragungen dar. Hier steht RAS für Registration, Admission and Status. Es dient zur Sitzungssteuerung zwischen dem Terminal (Endgerät) und dem Gatekeeper (zentrale Steuerungseinheit). Auf H.323 kann an dieser Stelle nicht eingegangen werden. Es soll nur der Vollständigkeit halber erwähnt werden.

15.2 Arten von RAS-Anbindungen

Vorüberlegung

Die Öffnung eines Netzwerks nach außen bringt deutliche Vorteile mit sich und ist heute aus einer modernen Netzwerkplanung nicht mehr wegzudenken. Gleichzeitig bringt aber jede Öffnung eines Netzwerks nach außen auch erhebliche Sicherheitsrisiken mit sich. Die Entscheidungsträger müssen im Vorfeld die Risiken gegen die Vorteile abwägen. In diese Abwägung muss die Art der Netzwerkverbindung einbezogen werden, da verschiedene Verbindungstypen auch ganz unterschiedliche Risiken mit sich bringen.

Verschiedene Arten von Netzwerkanbindungen

Der Fernzugriff auf Netzwerke kann über unterschiedliche Verbindungen realisiert werden. Dabei spielt vor allem die Art der Verbindung eine Rolle.

- ✓ Standleitung
- ✓ Wählverbindungen
- ✓ Virtuelle Verbindung über ein offenes Netzwerk (z. B. VPN über das Internet, vgl. Kapitel 16)

Einige der Faktoren, durch die sich verschiedene Verbindungstypen unterscheiden sind:

- ✓ Kosten
- ✓ Sicherheit
- ✓ Verfügbarkeit
- ✓ Bandbreite
- ✓ übertragbare Datentypen

Standleitungen

Standleitungen sind vor allem für die Anbindung entfernter Standorte an Firmennetze geeignet. Sie bieten meistens den Vorteil einer fest verfügbaren Bandbreite, die zu jedem beliebigen Zeitpunkt ohne zusätzliche Kosten genutzt werden kann, es gibt aber auch Lösungen, die flexible Bandbreitennutzung erlauben.

Standleitungen werden vor allem dann genutzt, wenn zu jedem Zeitpunkt eine vergleichbare Menge an Daten übertragen werden muss. Es macht wenig Sinn, eine Standleitung einzurichten, wenn nur einmal am Tag ein Datenbankabgleich erfolgen muss. In diesem Fall wäre eine Wählleitung zu bevorzugen. Müssten dagegen zu jeder Zeit Anmeldeinformationen zwischen Domänencontrollern ausgetauscht werden, empfiehlt sich der Einsatz einer Standleitung.

Die folgende Tabelle zeigt die wichtigsten Eigenschaften von Standleitungen auf:

Bandbreite	Mit Standleitungen können beliebige Bandbreiten unterstützt werden. Dies reicht von einer X.25-Standleitung für die Anbindung von Alarmanlagen oder Kreditkartenautomaten mit wenigen kbps bis zu großen ATM-Anbindungen mit 622 Mbps.
Übertragungs-sicherheit	Da Standleitungen auf verschiedenen Medien betrieben werden können, ist die primäre Sicherheit von diesen abhängig. Wird etwa eine Standleitung als Richtfunkverbindung eingerichtet, kann sie nicht als sicher betrachtet werden, da das Abhören von Funksignalen in der Regel keine Schwierigkeit für potenzielle Angreifer darstellt. Werden dagegen Lichtwellenleiter (LWL) verwendet, ist die Übertragungssicherheit als hoch anzusehen.
Zugangs-sicherheit	Die Zugangssicherheit ist bei Standleitungen nur dann gewährleistet, wenn die Übertragungssicherheit ausreichend gegeben ist. Ist dieses der Fall, stellen Standleitungen einen relativ sicheren Zugang zu Netzen dar. Voraussetzung für eine Verbindung ist, dass der Kommunikationspartner sich von der korrekten Stelle aus mit dem Netz verbindet. Und wenn ein Angreifer erst einmal physikalischen Zugang zu den Rechnersystemen einer Gegenstelle hat, ist ohnehin jegliche Sicherheit korrumptiert.
Übertragbare Datentypen	Da Standleitungen auf den unterschiedlichsten Medien betrieben werden können, können sie auch für die Übertragung jedes Datentyps genutzt werden. So erlaubt der Einsatz von ATM etwa auch die Übermittlung von Voice-Over-IP-Daten oder Multimedia-Anwendungen.

Kosten für Standleitungen

Kosten für Standleitungen sind je nach Art der Leitung und des Anbieters ganz unterschiedlich. Die Berechnung der Kosten für eine Standleitung kann auf dreierlei Art erfolgen:

- ✓ Entfernung
- ✓ Bandbreite
- ✓ übertragenes Datenvolumen

In der Regel wird eine Kombination dieser Faktoren für die letztendlichen Kosten ausschlaggebend sein. So wird etwa bei Satelliten-Verbindungen in der Regel ein fester Grundpreis für die Bereitstellung der Leistung erhoben und zusätzlich werden Gebühren für jede Übertragung fällig. Eine Rolle spielt bei den Kosten auch stets, ob Bandbreiten garantiert werden müssen oder nur nach Möglichkeit verfügbar sein sollen.

Wählverbindungen

Wählleitungen bieten den Vorteil, dass sie nur Kosten verursachen, wenn sie auch tatsächlich benötigt werden. Dafür bieten sie im Allgemeinen nur relativ geringe Bandbreiten und werden entfernungsabhängig berechnet. Sie bieten sich in erster Linie für den Fernzugriff von Einzelsystemen auf Netzwerke an. Hierbei können sie ihren größten Vorteil ausspielen, nämlich die Nutzung vorhandener Informationsinfrastrukturen, wie etwa des Telefonnetzes.

Sicherheit für Wählverbindungen

Wählverbindungen erfordern besondere Arten der Benutzeroauthentifizierung und der Sicherung der Daten während der Übertragung. Bei der Benutzeroauthentifizierung sind zwei Faktoren zu unterscheiden:

- ✓ Darf diese Leitung für eine Einwahl verwendet werden?
- ✓ Darf dieser Benutzer den Dienst nutzen?

Verbindungssicherheit bei Wählverbindungen

Die Absicherung einer Wählverbindung auf Verbindungsebene kann auf drei Arten erfolgen:

Erlaubte Nummer	Eine Einwahl in das Netz ist für einen bestimmten Benutzer nur von einer bestimmten Telefonnummer aus erlaubt. Wenn die Rufnummernübermittlung aktiviert ist, kann der Einwahlserver überprüfen, ob der Benutzer sich z. B. zu Hause befindet, und nur dann die Einwahl erlauben. Ein potenzieller Angreifer müsste in diesem Fall neben den Zugangsdaten des Benutzers auch dessen Wohnung benutzen, um sich in das Netz einzuhören zu können. Damit ist ein Angriff sehr schwierig. Voraussetzung ist allerdings, dass die Rufnummernübermittlung nicht unterdrückt wird.
Rückruf-sicherheit	Bei der Konfiguration eines Einwahlservers mit Rückrufsicherheit wird bei Anruf eines bestimmten Benutzers automatisch dessen eingespeicherte Telefonnummer gewählt. Das Ergebnis ist mit der Verifizierung durch erlaubte Nummern vergleichbar, allerdings trägt hier der Betreiber des Einwahlservers die Kosten für die Verbindung. Rückrufsicherheit kann auch eingerichtet werden, falls die Rufnummernübermittlung unterdrückt ist.
Beliebige Einwahl	Diese Option beinhaltet keinerlei Sicherheitsmerkmale und sollte nur verwendet werden, wenn z. B. ein Außendienstmitarbeiter sich von unterschiedlichen Orten aus mit dem Firmennetzwerk verbinden muss.

Übertragungssicherheit bei Wählverbindungen

Übertragungssicherheit ist vor allem gefragt, wenn die genutzten Telefonleitungen über Territorien von Staaten verlaufen, bei denen mit Spionage gerechnet werden muss. In diesem Fall sollten die Daten während der Übertragung mit einer starken Verschlüsselung gesichert werden. Im deutschen Telefonnetz muss derzeit nicht davon ausgegangen werden, dass Daten abgehört werden. Allerdings ist dies bei Verwendung von Mobiltelefonen für die Datenübertragung nur begrenzt gültig. Hier kann erst ab dem Übergabepunkt zur Erdleitung von einer ausreichenden Übertragungssicherheit ausgegangen werden.

Wenn Sie Daten während der Übertragung schützen möchten, sollten Sie Verschlüsselungstechniken wie IPSec verwenden. Bei besonders sensiblen Daten kann auch der Einsatz von Hardwareverschlüsselung ratsam sein.

Virtuelle Verbindungen

Mittels virtueller Verbindungen kann eine Einwahl über ein offenes Medium wie das Internet eingerichtet werden. Zwar ist Kommunikation über das Internet verbindungsorientiert, aber der Weg, den Informationen nehmen, ist nicht bekannt. Daher muss die Kommunikation getunnelt werden, um sie bei der Übertragung vor Angriffen zu schützen.

Bevor nun aber virtuelle private Netzwerke näher erläutert werden, sollten die Authentifizierungsmethoden für RAS erörtert werden.

15.3 RAS-Authentifizierung

Authentifizierung

Ziel jeder Authentifizierung muss sein, die einwandfreie Identität eines Benutzers zu bestätigen. Dazu bedarf es zweierlei Informationen:

- ✓ Wer behauptet, der Benutzer zu sein?
- ✓ Ist er auch wirklich diese Person?

Die Information, wer denn ein Benutzer zu sein behauptet, wird über den Benutzernamen abgefragt, die Bestätigung dieser Identität erfolgt über das Kennwort. Darüber hinaus erlauben bestimmte Authentifizierungsverfahren noch den Einsatz weiterer Merkmale zur Identitätsbestimmung, wie Smartcards, Einmal-Passwort-Generatoren oder biometrische Verfahren.

Damit die Authentifizierungsinformationen während des Transportes vor Angriffen geschützt sind, sollten sie unbedingt verschlüsselt werden. Das Authentifizierungsprotokoll bestimmt dabei den Grad und den Mechanismus der Verschlüsselung. Je unsicherer die Übertragungsart der Daten ist, desto stärker muss der Schutz der übertragenen Daten sein.

Im Folgenden sind einige der gängigen Authentifizierungsprotokolle und Verschlüsselungstechniken aufgeführt und beschrieben. An dieser Stelle kann aber auf die angewandten Verschlüsselungstechniken nicht detailliert eingegangen werden, dies ist nicht Inhalt dieses Buches.

Protokoll	Eigenschaften
Password-Authentication-Protokoll (PAP)	<p>PAP ist eines der ältesten Verfahren zur Benutzeroauthentifizierung. Mit PAP werden Benutzername und Kennwort im Klartext übermittelt. Sie können ohne jeden Aufwand von einem beliebigen Angreifer ausgewertet werden.</p> <p>Andererseits ist PAP das am weitesten verbreitete Authentifizierungsprotokoll und wird herstellerübergreifend von den meisten Plattformen unterstützt. Dies ist unter anderem darauf zurückzuführen, dass es durch das Fehlen jeder Verschlüsselung sehr schnell ist und ohne administrativen Aufwand eingerichtet werden kann.</p> <p>PAP mag vielleicht noch für den Einsatz von RAS-Verbindungen mit Rufnummernüberprüfung oder Rückrufsicherheit gerade noch akzeptabel sein, empfiehlt sich aber auch hier nicht. Wenn Sie die Möglichkeit haben, sollten Sie PAP für eingehende und ausgehende Verbindungen deaktivieren.</p> <p>Das Verbot für ausgehende Verbindungen ergibt sich daraus, dass PAP die Identität des Gegenübers nicht überprüft und Sie so möglicherweise Ihre Verbindungsdaten einem unbefugten Dritten mitteilen.</p>
Shiva-Password-Authentication-Protokoll (SPAP)	<p>SPAP verwendet eine symmetrische umkehrbare Verschlüsselung. Zwar werden die Kennwörter nicht wie unter PAP ohne jeden Schutz übertragen, aber dennoch kann hier nicht von einem ernsthaften Schutz die Rede sein.</p> <p>Shiva Password Authentication wird hauptsächlich verwendet, um Shiva-Clients die Verbindung mit Shiva LAN-Rover zu erlauben. Außerhalb dieser proprietären Umgebung sollten Sie SPAP nur verwenden, wenn Sie es benötigen. Dabei dürfen SPAP-Informationen niemals über öffentlich zugängliche Netzwerke übermittelt werden.</p>
Challenge-Handshake-Authentication-Protokoll (CHAP)	<p>CHAP verwendet einen Three-Way-Handshake zur Authentifizierung. Dieser verwendet einen MD5-Hash (Message Digest 5) zum Hashen der übertragenen Authentifizierungsdaten. Der hierbei eingesetzte Schlüssel und der zugehörige 40-Bit-Hash können heutzutage nicht mehr als ausreichend angesehen werden. Zusätzlich hasht CHAP nur das Kennwort in einem 128-Bit-Hash-Code, der Benutzername aber wird unverschlüsselt übertragen.</p> <p>Ein CHAP-Passwort unterstützt in der Regel Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen. Es muss mindestens acht Zeichen lang sein, sonst funktioniert der Hash-Algorithmus nicht. Daher werden kürzere Kennwörter von CHAP mit Nullen aufgefüllt.</p> <p>Des Weiteren basiert CHAP auf einer einseitigen Authentifizierung, es erfolgt also keine Kontrolle, ob an der Gegenstelle auch derjenige ist, der er zu sein behauptet.</p>
Terminal Access Controller Access Control System (TACACS)	<p>TACACS ist ein Authentifizierungsprotokoll von 1993, das in seiner ursprünglichen Variante kaum noch eingesetzt wird. Lediglich der Nachfolger TACACS+ wird hauptsächlich noch von CISCO verwendet. Bei TACACS wird eine Authentifizierungsanforderung von dem Einwahlgerät an einen externen Authentifizierungsserver weitergeleitet, der entscheidet, ob der Host Einwahlrechte erhält oder nicht.</p> <p>TACACS unterstützt Benutzernamen von bis zu 128 Zeichen, die sich aus den ASCII-Zeichen von "!" (Dezimal 33) bis "~" (Dezimal 126) zusammensetzen dürfen. Dieselbe Beschränkung gilt für die Kennwörter.</p> <p>TACACS dient nicht zur eigentlichen Authentifizierung, sondern stellt Autorisierungsmechanismen für bestimmte Zugriffe auf bestimmte Ressourcen zur Verfügung. Zur Authentifizierung können gängige Protokolle wie PAP, CHAP oder EAP verwendet werden.</p> <p>TACACS verwendet eine eigene Verschlüsselung.</p>

Protokoll	Eigenschaften
Extensible-Authentification-Protokoll (EAP)	Bei EAP-Authentifizierung wird eine RAS-Verbindung durch einen zufällig ausgewählten Authentifizierungsmechanismus bewerkstelligt, den der Server vom Client anfordert. Dabei kommen etwa Smartcards oder MD-5 Challenge zum Einsatz, sodass die Authentifizierung als sehr sicher betrachtet werden kann. EAP kann zusätzlich noch auf einen RADIUS-Server zugreifen, der eine weitere Verbesserung der Sicherheit gewährleistet.
Microsoft CHAP (MS-CHAP)	MS-CHAP verwendet eine modifizierte Version von CHAP, bei der die Kennwörter mit einem irreversiblen 40-Bit-Hash geschützt werden. Dies stellt eine deutliche Verbesserung dar, ist aber aufgrund der zu schwachen Hashfunktionen nicht ausreichend, um echte Sicherheit zu gewährleisten. Darüber hinaus wird dasselbe Kennwort stets denselben verschlüsselten Wert aufweisen und kann damit für Angriffe ausgewertet werden. Die Authentifizierung mittels MS-CHAP ist unidirektional und damit nicht ausreichend sicher, um zu gewährleisten, dass nicht der falsche Empfänger die Anmeldeinformationen erhält.
Microsoft CHAP Version 2 (MS-CHAPv2)	MS-CHAPv2 stellt eine RAS-Authentifizierung unter Microsoft ab Windows 2000 zur Verfügung. Hierbei wurde die Hashfunktion verstärkt. Es wird nun ein 128-Bit-Hashcode unterstützt und stattdessen auf Abwärtskompatibilität zu früheren Microsoft-Betriebssystemen verzichtet. Zusätzlich wird nun eine bidirektionale Authentifizierung vorgenommen, um zu verhindern, dass ein unberechtigter Einwahlserver Anmeldeinformationen erhält.
Remote Authentication Dial In User Service (RADIUS)	RADIUS wurde von Livingston Enterprises inc. entwickelt und dient zur Authentifizierung und Autorisierung von Benutzern auf Einwahlservern. Unterstützt werden diverse Authentifizierungsprotokolle wie etwa PAP, CHAP, UNIX-Login u. a. Allerdings verwendet RADIUS eigene Verschlüsselungen der Passwörter mit Geheiminformationen, die auf dem Server und dem Client hinterlegt sind, sodass Benutzerkennwörter niemals im Klartext übermittelt werden. RADIUS gilt als sehr sicher und ist für Netzwerke geeignet, in denen sensible Daten transportiert werden.
RSA SecureID	SecureID ist ein Beispiel für eine Hardware-Authentifizierung mit Einmal-Passwort-Generatoren. Dabei wird zu einem Zeitpunkt X aus einer geheimen Information eine Zahl generiert. Diese muss zusammen mit einer PIN und dem Benutzernamen an den Anmeldeserver übermittelt werden. Dieser überprüft dann in seiner Datenbank, ob die Informationen zu diesem Zeitpunkt richtig sein können. Wenn dies der Fall ist, erhält der Benutzer den Zugriff und der Wert wird aus der Liste der zu dem Zeitpunkt möglichen Ergebnisse gestrichen. Selbst wenn es einem Angreifer gelänge, die verschlüsselten Passwortinformationen zu erlangen, könnte er sich keinen Zugriff auf das Netz verschaffen, da die Informationen nun als ungültig in der Datenbank hinterlegt sind. SecureID stellt damit eine Lösung für Hochsicherheitsnetzwerke dar, da es nicht ausreicht, im Besitz zweier Informationen zu sein (Benutzername und PIN), sondern Sie zusätzlich den Passwortgenerator benötigen. Und dessen Diebstahl kann umgehend gemeldet werden, was eine Sperrung zur Folge hat.

Unter Microsoft-Betriebssystemen (seit Windows 2000 Server) ist die Möglichkeit gegeben, bestimmten Benutzern bei Remotezugriff eine reservierte IP-Adresse zuzuweisen. Dadurch kann die Zugriffssicherheit etwas erhöht werden, da aufgrund von Zugriffslisten bestimmte Netzwerkbereiche für Benutzer gesperrt werden können.



15.4 Network Policy Server (NPS)

Network Policy Server (NPS) erlauben die Steuerung des RAS-Zugriffs in Abhängigkeit von installierten Softwareprodukten wie Firewalls, Virenschutzprogrammen oder Updates. Der Mechanismus hierfür wird auch als Netzwerkzugriffs-Richtlinie (Network Access Policy, NAP) bezeichnet. Mit NAP kann z. B. festgelegt werden, dass eine Einwahl ins Netzwerk erst gestattet ist, wenn eine bestimmte Virenschutzanwendung mit aktuellen Virensignaturen installiert ist, um das Netzwerk vor der Verbreitung von Viren zu schützen. Zusätzlich kann auch die automatische Installation der aktuellen Virensignaturen bereitgestellt werden.

NPS unter Windows

Microsoft hat NPS mit Windows Server 2008 eingeführt und unterstützt damit Clients seit Windows Vista und Windows XP. Mit den neueren Windows Server-Betriebssystemen kam die Unterstützung aller neueren Clientbetriebssystem-Versionen hinzu. Für diese Clientbetriebssysteme ermöglicht NPS die Überprüfung einer ganzen Reihe von Sicherheitsmerkmalen (wie z. B. Aktivierung einer Firewall, Einstellungen zu Antivirenanwendungen und Spywareschutz oder Einstellungen für automatische Updates).

SHA und SHV

Die Überprüfung erfolgt mittels eines Dienstes auf dem Clientrechner, dem Systemintegritäts-Agenten (System Health Agent, SHA), die die Informationen zum Status einer Software auf dem Client an den zuständigen Server übermittelt. Dort prüft der zugehörige Systemintegritätsprüfer (System Health Validator, SHV) die Angaben des Berichts des SHA und gewährt Zugriff oder nicht.

16 Virtual Private Network

In diesem Kapitel erfahren Sie

- ✓ was ein Virtual Private Network (VPN) ist
- ✓ wie VPNs eingesetzt werden können
- ✓ mit welchen Protokollen ein VPN betrieben werden kann
- ✓ etwas über OpenVPN

Voraussetzungen

- ✓ Gute TCP/IP-Kenntnisse
- ✓ Netzwerkkenntnisse

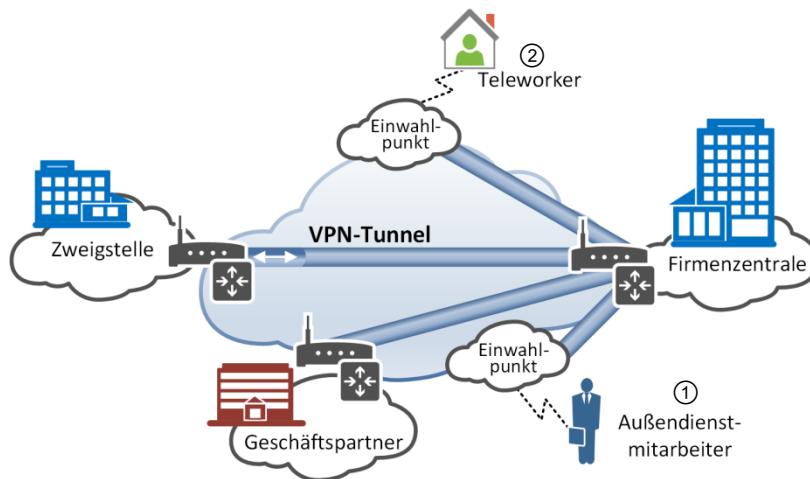
16.1 Zielsetzung

Gründe für ein Virtual Private Network

In Unternehmen, bei denen Zweigstellen oder Außendienstmitarbeiter Zugang zu Ressourcen in der Firmenzentrale benötigen, mussten früher ein Einwahlserver (Remote Access Server, RAS) und eine angemessene Anzahl an Modems bzw. ISDN-Geräten installiert werden. Für eine Datenverbindung zwischen Firmensitz und Zweigstelle, die mehr Bandbreite benötigte, war unter Umständen sogar das Einrichten einer permanenten oder semi-permanenten Standleitung nötig.

Der Remote-Zugang zu Firmenressourcen ist auf diese Weise allerdings nicht nur in der Anschaffung der Hardware, sondern auch bei den laufenden Kosten relativ hoch. So müssen bei der Einwahl von Außendienstmitarbeitern die entsprechend anfallenden Telefongebühren bezahlt werden, die meist als Ferngespräche abgerechnet werden.

Die Idee eines Virtual Private Network (VPN) besteht nun darin, den meist lokal günstig zu nutzenden Internetzugang dazu zu gebrauchen, um den Kontakt zur Firmenzentrale herzustellen. Ein Außendienstmitarbeiter ① könnte also über die Einwahl bei einem Internetprovider über das Internet Zugang zu Ressourcen in der Firmenzentrale bekommen, oder ein Teleworker ② könnte per Internet-Flatrate angebunden sein.

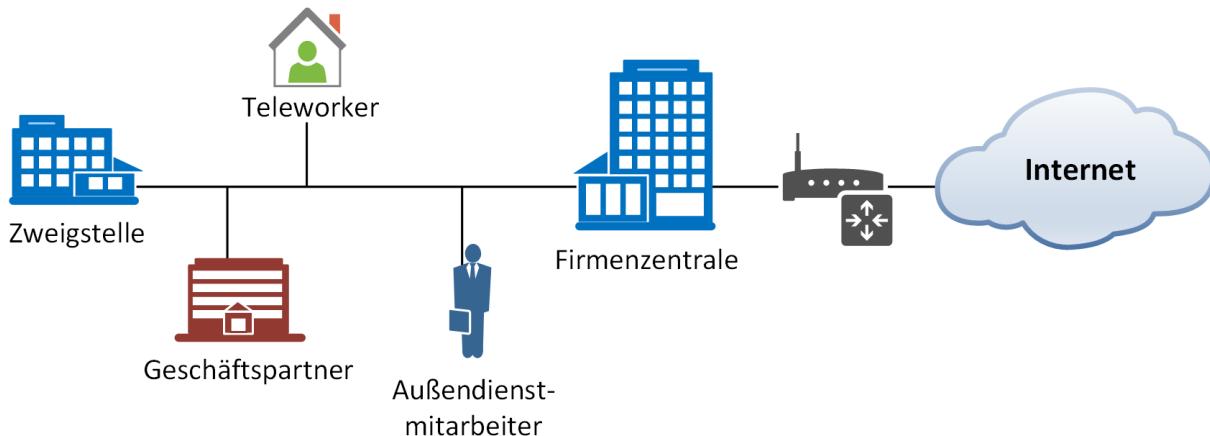


VPN, reelle Verbindungen über Internet

Da das Internet jedoch ein öffentliches Netz ist und so theoretisch jeder die übertragenen Daten an den Knotenpunkten abfangen oder sogar manipulieren kann, müssen Möglichkeiten gefunden werden, dies zu verhindern. Hier bieten sich die Methoden der Kryptografie als Lösung an.

Mit einer VPN-Verbindung werden die Datenpakete des externen Rechners kryptografisch gesichert über das Internet in das Firmennetz weitergeleitet. Umgekehrt werden Datenpakete aus dem Firmennetzwerk über die gesicherte Verbindung an den Client weitergeleitet, wenn es sich um Broadcasts oder direkt an den Client adressierte Pakete handelt.

Aus der Sicht des Clients sieht es also so aus, als würde er sich im LAN der Firmenzentrale befinden.



VPN, logisches Netzwerk aus Sicht der Teilnehmer

Auch eine Kopplung von zwei LANs (z. B. Firmenzentrale und Zweigstelle) ist mit einem VPN realisierbar. In diesem Fall müssen Pakete, je nach Bedarf, von der einen auf die andere Seite geschickt werden. Als Transportmedium kommt hier wieder eine Internetverbindung zum Einsatz.

Da in VPNs die Datenpakete, die ausgetauscht werden sollen, meist als Ganzes gesichert innerhalb neuer Datenpakete verschickt werden, werden die Verbindungsstrecken zwischen zwei VPN-Übergabepunkten auch als VPN-Tunnel bezeichnet.

Kostenvorteil

VPNs haben heute die RAS-Installationen nahezu komplett abgelöst, da die Investitions- und Betriebskosten für den Internetzugang plus VPN-Lösung deutlich unter den Anforderungen für RAS-Hardware plus Telefonverbindungsnetze liegen. Weitere Gründe für die Verwendung von VPNs sind die höhere Geschwindigkeit gegenüber Wählverbindungen und die allgemeine Verfügbarkeit von Internetzugängen, auch z. B. per Hotspot oder Mobilfunkverbindung.

16.2 PPTP

Aufbau von PPTP

Das Point-to-Point Tunneling Protocol ist eine von einem Herstellerkonsortium (mit 3Com und Microsoft) entwickelte Erweiterung des Point-to-Point Protocol (PPP). PPTP ist in der Lage, PPP-Pakete in IP-Paketen so einzupacken, dass Protokolle wie IP, IPX oder NetBEUI damit transportiert werden können. Für die Zugangskontrolle sind beim PPTP mehrere Verfahren implementiert. Dazu gehören die Optionen einer simplen, ungeschützten Passwortabfrage (PAP), eines verschlüsselten Challenge-Response-Verfahrens (CHAP) sowie einer Authentifizierung des Benutzers durch eine Smartcard (z. B. mit EAP).

Die zu übertragenden Daten selbst werden entweder per Microsoft Point-to-Point-Encryption (MPPE) mit der Stromchiffre RC4 verschlüsselt, wobei die Länge des Schlüssels zwischen 40 und 128 Bit variieren kann.

Zur Steuerung der Verbindung benutzt PPTP eine sogenannte Kontrollverbindung (PPTP Control Connection). Über diese Kontrollverbindung auf TCP Port 1723 werden der Aufbau, die Verwaltung und der Abbau der Tunnelverbindung mit den eigentlichen Daten bewerkstelligt.

Die zu tunnelnden Daten werden nach der Verschlüsselung in Pakete nach GREv2 (Generic Routing Encapsulation) gepackt und an die Zieladresse (den VPN-Server) geschickt. GRE trägt die IP-Protokollnummer 47.

Da die Userdaten bei PPTP per GRE übertragen werden und dieses Protokoll anders als TCP oder UDP keine Portnummern hat, stellen NAT/PAT-Gateways im Kommunikationspfad Problemquellen dar.

Die in PPTP verwendete Kryptografie hat bei neuerer Sicherheitsforschung so viele Mängel gezeigt, dass vom Einsatz von PPTP dringend abgeraten wird.

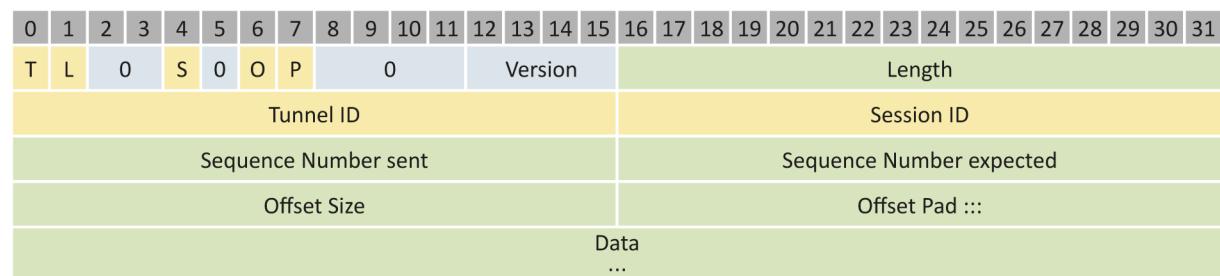
16.3 L2TP/IPSEC

Layer 2 Tunneling Protocol

Das L2TP ist eine Weiterentwicklung des ursprünglich von Cisco entwickelten L2F (Layer 2 Forwarding). Die Angabe einer Tunnel-ID im L2TP Header ermöglicht es, mehrere Tunnel auf einer Verbindungsstrecke zu betreiben. NAT wird ebenfalls unterstützt. Obwohl L2TP eine Authentisierung mithilfe von CHAP oder PAP erlaubt, werden die Datenpakete der bestehenden Verbindung später nicht weiter überprüft. L2TP verschlüsselt die zu übertragenden Daten nicht.

L2TP Header

Ein L2TP Header ist wie folgt aufgebaut:



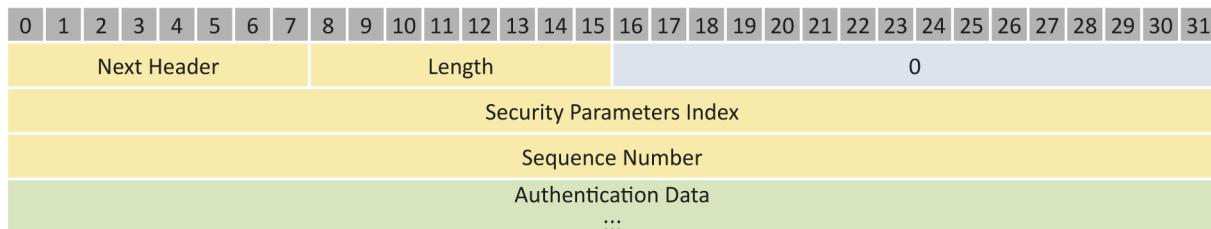
Abkürzungen: T = Message Type, L = Length present, S = Sequence present, O = Offset present, P = Priority

IP Security

Das IPSec-Protokoll war ursprünglich zur Verwendung im IPv6-Standard vorgesehen. Es wurde letztendlich jedoch auch für das bestehende IPv4 implementiert und kann im Zusammenspiel mit L2TP dieses sinnvoll um Verschlüsselung und paketweise Authentifizierung ergänzen. Weiterhin hat sich IPSec (ohne L2TP) als Standard bei LAN-to-LAN-VPNs und auch bei Remote-Access-VPNs durchgesetzt.

Authentication Header

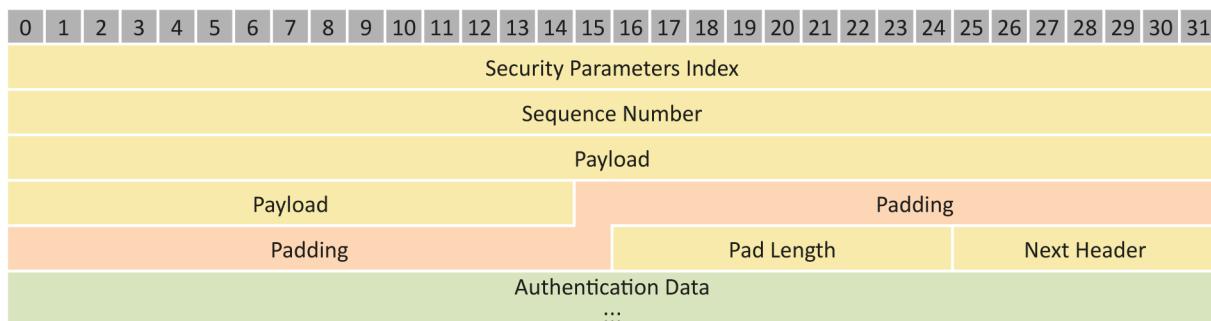
Zum Schutz der Daten vor Veränderungen ist in IPSec der sogenannte AH (Authentication Header) definiert. Dieser garantiert durch eine Prüfsumme (z. B. auf Basis des nicht mehr empfohlenen MD5 oder einer Version der SHA-Familie wie SHA-1 oder SHA-256) die Korrektheit der übertragenen Daten sowie wichtiger Header-informationen. Der Authentication-Header findet bei VPNs kaum Anwendung.



ESP Header

Die Vertraulichkeit wird in IPSec mit dem ESP Header (Encapsulating Security Payload) sichergestellt. In ESP wird als kleinster gemeinsamer Verschlüsselungsstandard DES gefordert. Da DES schon länger keine ausreichende Sicherheit mehr liefert, bieten nahezu alle am Markt befindlichen Lösungen die Verwendung stärkerer Algorithmen wie das inzwischen auch als veraltet geltende 3DES oder den aktuellen Standard AES mit seinen Schlüssellängen von 128, 192 oder 256 Bit.

Bei der Verwendung von ESP können die Nutzdaten sowohl verschlüsselt als auch deren Integrität gesichert werden. Damit ist ESP das typischerweise bei IPSec eingesetzte Verfahren.



Security Parameters Index, SPI

Um den Inhalt von Paketen ordnungsgemäß authentifizieren oder entschlüsseln zu können, wird mit dem SPI angegeben, zu welcher **Security Association (SA)** dieses Paket gehört. In einer SA wird in einem Computer für jedes Ziel (d. h. jede Ziel-IP-Adresse) festgelegt (assoziiert), welche Schlüssel und Sicherheitseinstellungen für dieses Ziel gelten sollen.

Dies kann zum Beispiel auch die erlaubten Algorithmen, die verwendeten Schlüssellängen oder die Zeitdauer bis zum Wechsel des Verschlüsselungsschlüssels beinhalten.

Schlüsselmanagement

Damit SAs gebildet werden können, müssen die Rechner in der Lage sein, sich gegenseitig zu identifizieren und einen gemeinsamen Verschlüsselungsschlüssel zu wählen. Dieser Vorgang wird unter IKE (Internet Key Exchange) zusammengefasst. Das **Internet Security Association and Key Management Protocol**, abgekürzt ISAKMP, ist dafür verantwortlich, über das unsichere Internet zunächst die Kommunikationspartner sicher zu identifizieren und dann eine SA inklusive kryptografischer Schlüssel zu erstellen.

Beim Erstellen der Schlüssel wird vom Diffie-Hellman-Protokoll Gebrauch gemacht. Zwei Kommunikationspartner können mittels Public-Key-Verfahren über Zertifikate gemäß X.509 authentifiziert werden. Alternativ können die Partner auch über einen Kerberos-Trust einen gemeinsamen geheimen Schlüssel erhalten. In diesem Fall ist das Kerberos-Key-Distribution-Center (KDC) der gemeinsame Dritte, dem beide Kommunikationspartner vertrauen müssen und der beide gegenseitig authentifiziert.

Als letzte Notfall-Möglichkeit kann eine Authentifizierung auch über sogenannte Preshared-Keys vorgenommen werden. Hierzu stellt der Systemverwalter auf beiden Systemen, die miteinander über IPSec kommunizieren sollen, denselben Identifikationsschlüssel per Hand ein. Von dieser Methode ist jedoch verwaltungstechnisch abzuraten, da dies für große Netze einen immensen Aufwand bei der Verteilung und Erneuerung von Schlüsseln bedeuten würde. Für eine kleinere Anzahl von VPNs hat sich die Verwendung von Pre-Shared-Keys durchgesetzt, was bei der Verwendung von langen und komplexen Schlüsseln auch sicherheitstechnisch akzeptabel ist.

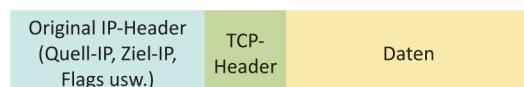
Transportmodus

Soll ein einzelner Client eine Verbindung zu einem Server aufbauen, so kommt üblicherweise der sogenannte Transportmodus zur Anwendung. Dies ist einer der beiden Arbeitsmodi, die von IPSec unterstützt werden.

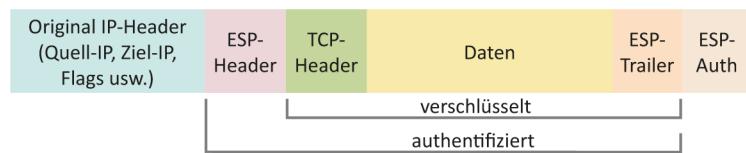
Im Transportmodus werden nur die zu übertragenden Daten durch IPSec verschlüsselt und geschützt. Der Original-IP-Header des Paketes bleibt erhalten.

In der Abbildung rechts sehen Sie oben ein normales IP-Paket ①, in dem die TCP-Daten einer Verbindung transportiert werden.

IPv4-Paket, normal ①



IPv4-Paket mit ESP, Transportmodus ②



IPSec-Transportmodus

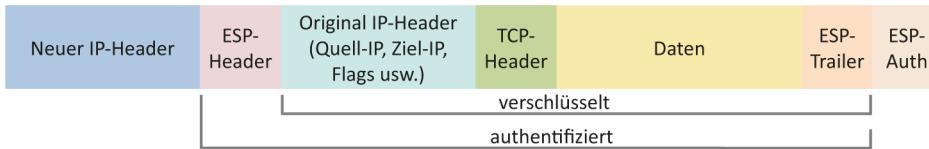
Im Transportmodus ② wird der originale IP-Header dieses Paketes abgetrennt und bleibt erhalten. Vor dem TCP Header und den Daten wird der ESP Header eingefügt. Am Ende des neuen Paketes befinden sich der ESP Trailer und die ESP Authentication.

In diesem Fall ist der Bereich vom TCP Header bis zum ESP Trailer verschlüsselt, und der Bereich vom ESP Header bis zum ESP Trailer wird durch die Authentifizierung geschützt.

Obwohl für einen Lauscher die Verbindungsdaten selbst nicht mehr einsehbar sind, da sie im verschlüsselten TCP- bzw. Datenteil liegen, können durch Auslesen der Informationen im IP-Header zumindest die Absender- und die Empfänger-IP-Adresse ermittelt werden.

Tunnelmodus

Der zweite Modus von IPSec, der Tunnelmodus, eignet sich besonders, wenn zwei LANs über ein VPN gekoppelt werden sollen. Im Tunnelmodus werden an einem Gateway alle Pakete aus dem eigenen Netz, die für das jeweils andere Netz bestimmt sind, komplett verschlüsselt, signiert und neue IP-Pakete erzeugt, die an das Remote-Gateway geschickt werden. Dort werden die derart getunnelten Pakete wieder ausgepackt und den Empfängern im Remote-LAN zugestellt.

IPv4-Paket mit ESP, Tunnelmodus**IPSec-Tunnelmodus**

Die Verschlüsselung umfasst in diesem Fall das komplette ursprüngliche IP-Paket vom Header bis zu den Daten. Die Authentifizierung reicht, ähnlich wie beim Transportmodus, wieder vom ESP Header bis zum ESP Trailer.

Auf diese Weise besteht ein vollständig geschützter VPN-Tunnel zwischen den beiden Gateway-Systemen. Der Datenverkehr, der über das öffentliche Netz abgewickelt wird, ist vollständig verschlüsselt. Ein Lauschangriff würde nur die IP-Adressen der beiden Gateway-Systeme offenbaren. Die Daten sowie die IP-Adressen der Clients, die innerhalb der beiden gekoppelten LANs miteinander kommunizieren, bleiben dem Angreifer wegen der Verschlüsselung verborgen.

Wenn IPSec mit Security-Gateways implementiert wird, kommt fast immer der Tunnel-Mode zum Einsatz.

IPSec und Firewalls

Für den Schlüsseltausch nach IKE wird in IPSec der UDP-Port 500 benutzt. Falls Zertifikate ausgetauscht werden (beispielsweise über LDAP), so werden auch die für den Zertifikatstausch benötigten Portnummern benutzt.

ESP bzw. AH benutzen die IP-Protokolle mit den Nummern 50 und 51. Um eine IPSec-Verbindung erfolgreich durch eine Firewall betreiben zu können, muss diese in der Lage sein, die betroffenen IP-Protokolle weiterzuleiten, und zusätzlich müssen die benötigten Ports konfiguriert werden.

Beachten Sie, dass vor allem günstigere Firewalls unter Umständen keine Möglichkeit anbieten, andere Firewallregeln zu erstellen als eine Freigabe von TCP- oder UDP-Ports. Dies verleitet vor allem Administratoren mit weniger umfangreichen TCP/IP-Kenntnissen zu der falschen Annahme, dass man mit der Freigabe von TCP/UDP-Port 50 und 51 bzw. 47 einen VPN-Betrieb ermöglichen könnte. Bei ESP, AH und dem für PPTP-VPN benötigten GRE handelt es sich aber um IP-Protokolle, die auf derselben OSI-Schicht angesiedelt sind wie TCP und UDP und die deswegen eine **Protokollnummer** und **keine Portnummer** tragen.



Das Vorhandensein einer NAT-Firewall auf der Strecke zwischen den beiden VPN-Partnern unterbindet den Einsatz von AH vollständig. Würden die übertragenen IP-Headerinformationen im Zuge der Network Address Translation von intern auf extern (oder umgekehrt) von der Firewall ersetzt, so würde dies die in AH enthaltene Signatur brechen und das Paket ungültig werden lassen. Abhilfe: für den Transportmodus statt AH ESP mit NAT-T (NAT-transversal) einsetzen.

Problematisch für den verantwortlichen Administrator eines Netzwerkes ist beim Einsatz von ESP die Verschlüsselung der TCP-Informationen, die somit nicht durch die Firewall einseh- oder veränderbar sind und damit ein erhebliches Sicherheitsrisiko darstellen, beispielsweise, wenn ein Nutzer aus dem Intranet (LAN) eigenmächtig einen Tunnel zu einem Remote-VPN-Server eines anderen Netzwerkes aufbaut. Mögliche Gegenmaßnahmen sind, an der Firewall den Aufbau verschlüsselter Verbindungen von Clients aus dem internen LAN Richtung Internet zu blocken oder Web-Security-Appliances (z. B. von Blue Coat) einzusetzen.

Enden VPN-Tunnel bei der Firewall, kann diese die Pakete entschlüsseln, Headerinformationen anpassen und je nach Bedarf einen weiteren Tunnel zum Empfänger aufbauen oder die Daten unverschlüsselt weiterleiten. Alternativ kann das VPN-Gateway auch vor der Firewall (in Richtung Internet) platziert werden.

16.4 OpenVPN

OpenVPN verwendet für die Sicherung der Daten kein IPSec, sondern es basiert auf den Sicherheitsfunktionen, die OpenSSL bietet. Die Verwendung von SSL-basierten VPNs hat sich heute als zweite Technologie neben IPSec durchgesetzt, wobei manche Hersteller SSL/TLS-basierte VPNs nur für Remote-Access-VPNs verwenden.

OpenVPN ist unter der GNU GPL lizenziert und steht unter <http://openvpn.net/> zum Download für u. a.

- ✓ Microsoft Windows (ab 2000),
- ✓ verschiedene Linux-Distributionen und
- ✓ FreeBSD zur Verfügung.

16.5 Abgrenzung zu anderen VPN-Arten

Dieses Kapitel beinhaltet nur sogenannte Security-VPNs. Diese werden verwendet, um Daten über ein potenziell unsicheres Netzwerk wie z. B. das Internet zu transportieren, wobei die Daten kryptografisch gesichert werden.

Im Gegensatz dazu gibt es auch VPNs, die keinen kryptografischen Hintergrund haben. Bei diesen geht es hauptsächlich um die Separierung verschiedener Datenströme, um z. B. verschiedene Kundendaten zu trennen. Das wichtigste Beispiel dafür ist MPLS (Multiprotocol Label Switching), bei dem die Daten standardmäßig ungesichert übertragen werden.

17 WLAN

In diesem Kapitel erfahren Sie

- ✓ was ein WLAN ist
- ✓ wozu Sie WLANs verwenden können

Voraussetzungen

- ✓ WAN-Protokolle
- ✓ Netzwerkgrundlagen

17.1 WLAN

Wireless LAN – Vor- und Nachteile

Bei Wireless LANs (WLANs) handelt es sich um Netzwerke, in denen statt kabelgebundener Übertragungsmedien aus Kupfer oder Glasfaser auf Funksignale in frei verfügbaren Frequenzbändern zurückgegriffen wird. Die Übertragung von Informationen ohne Kabel ist in vielen Lebensbereichen eine praktische Alternative. Von Smartphone und Smart-TV bis hin zur Steuerung diverser Geräte in den eigenen vier Wänden gibt es zahlreiche Beispiele für die Umsetzung dieser Technik.

Die Funkübertragung bringt im Vergleich zur kabelgebundenen Übertragung einige grundlegende Vorteile mit sich:

- ✓ Innerhalb der Reichweite der Signale kann der Netzwerkzugriff von einem beliebigen Ort aus erfolgen.
- ✓ Für eine Vernetzung müssen keine baulichen Veränderungen vorgenommen werden.
- ✓ Flexible Skalierbarkeit
- ✓ Öffentlicher Raum (etwa Straßen oder Gewässer) lässt sich überwinden.

Daneben bringt der Einsatz von WLAN allerdings auch eine Reihe von Problemen mit sich, die bei leitergebundenen Übertragungsverfahren nicht auftreten:

- ✓ hohe Störanfälligkeit
- ✓ keine Abhörsicherheit
- ✓ geringe Portdichte
- ✓ oftmals geringere Übertragungsgeschwindigkeit
- ✓ komplexer Anmeldevorgang auf Schicht Zwei nötig
- ✓ Leistungseinbußen bei vielen gleichzeitigen Benutzern

Um diese Nachteile auszugleichen, müssen zusätzliche Faktoren bei der Einrichtung von WLANs berücksichtigt werden. So müssen die Distanzen zwischen Sendern und Empfängern gering gehalten werden, um die Störanfälligkeit zu kompensieren. Da die Signale innerhalb eines bestimmten Radius von jedem empfangen werden können, muss auf Verschlüsselungsverfahren zurückgegriffen werden. Um die Portdichte ausreichend zu gestalten, müssen größere Frequenzbereiche und komplexe Frequenzmodulationsverfahren eingesetzt werden, und für die Synchronisation zwischen Sendern und Empfängern werden eigene Protokolle benötigt.

WLAN-Topologien

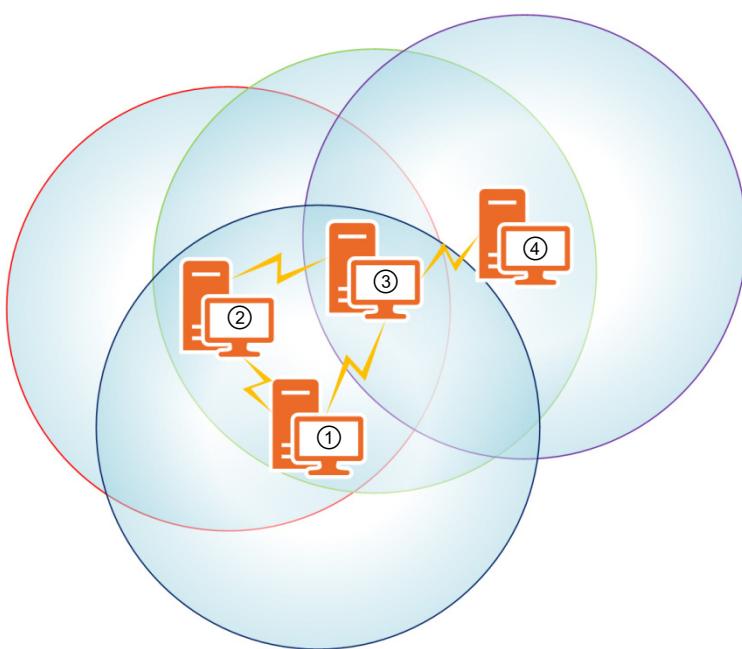
Da in einem WLAN ein Zugriff auf das Übertragungsmedium nicht auf eine einzelne Netzwerkdose beschränkt ist, ergibt sich die Möglichkeit unterschiedlicher Topologien. Unter Topologie versteht man die Weise, in der der physikalische Zugriff auf das Übertragungsmedium organisiert ist. Die beiden gängigen Topologien für WLANs sind:

- ✓ Ad-hoc-Netzwerke
- ✓ Infrastruktur-Netzwerke

Ad-hoc-Netzwerke

Bei einem Ad-hoc-Netzwerk kommunizieren zwei oder mehr Netzwerkgeräte direkt miteinander, sobald sie in Empfangsreichweite sind. Die Empfangsreichweite wird dabei als Basic Service Area (BSA) bezeichnet. In diesem Fall wird auch von einem Peer-to-Peer-Netzwerk gesprochen. Dabei sind alle beteiligten Geräte gleichrangige Partner. Wenn sich nun weitere Geräte innerhalb der BSA befinden, so können auch diese direkt kommunizieren. Ist Host A aber nur in der BSA von Host B und Host B in der BSA von Host C, so können A und C nicht miteinander kommunizieren, in einem Ad-hoc-Netzwerk ist kein Knoten Vermittler für andere.

Ad-hoc-Netzwerke werden in erster Linie im Privatbereich und in sehr kleinen Firmennetzen eingesetzt. Sie sind einfach zu konfigurieren und erlauben auch dem wenig versierten Nutzer den Aufbau einer WLAN-Umgebung. Dies geht jedoch meist zulasten der Skalierbarkeit und der Sicherheit des Netzes.



Ad-hoc-Netzwerk

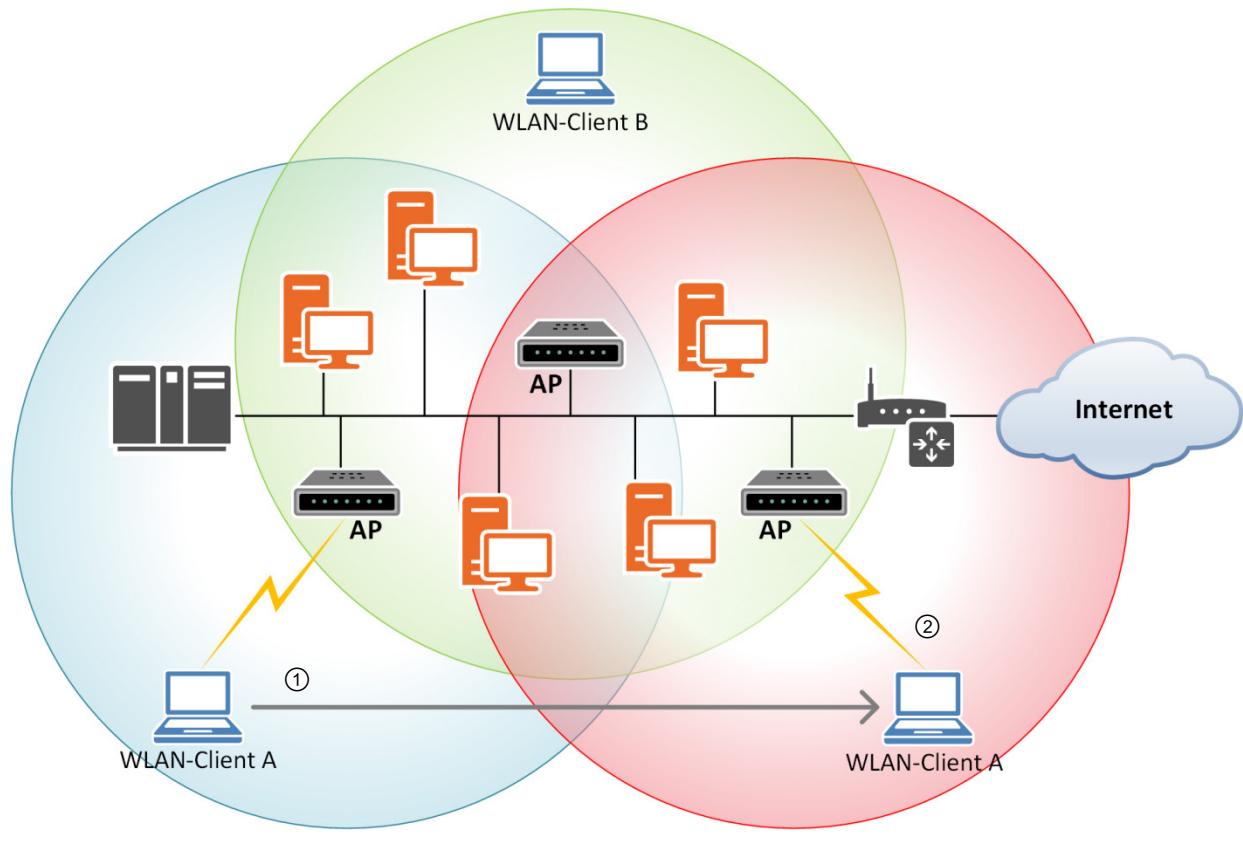
Die vorangehende Abbildung zeigt eine Situation, in der vier Rechner über ein Ad-hoc-Netzwerk verbunden sind. Die Rechner ①, ② und ③ stehen nahe genug zusammen, um alle gegenseitig in Reichweite zu sein. Rechner ④ ist jedoch so weit entfernt, dass er nur noch zu einem der drei anderen Rechner eine Verbindung herstellen kann (Rechner ③).

Infrastruktur-Netzwerke

Ein Infrastruktur-Netzwerk ist um einen zentralen Zugriffsknoten herum aufgebaut. Dieser wird als Access-Point (AP) bezeichnet und stellt die Schnittstelle zwischen dem kabelgebundenen Netz und dem Funknetz dar. Alle Knoten, die an der Netzwerkkommunikation teilnehmen möchten, müssen sich beim AP anmelden, ehe sie mit anderen Netzwerkgeräten kommunizieren können. Auch wenn Host A und Host B in derselben BSA liegen, müssen sie doch über den AP miteinander in Kontakt treten, können dafür aber auch mit anderen Geräten kommunizieren, die nicht innerhalb ihrer eigenen Reichweite liegen.

Infrastruktur-Netzwerke werden vor allem in größeren Netzwerken eingesetzt, um als Schnittstelle zwischen stationärem Netzwerk und tragbaren Geräten zu fungieren. Sie sind etwas schwieriger zu konfigurieren als Ad-hoc-Netzwerke, erlauben aber eine differenzierte Skalierung des Netzes.

In nachfolgender Grafik sind in einem LAN drei Access-Points installiert, die alle zum gleichen Funknetzwerk gehören. Die in deren Reichweite befindlichen Clients A und B haben Zugriff auf alle Netzwerkressourcen. Über die Roaming-Funktion kann sich ein Client wie A auch von einer Funkzelle in die andere bewegen ① und behält die logische Verbindung zum Netzwerk bei. Die Funkverbindung besteht aber nun zum neuen Access-Point ②.



Infrastruktur-Netzwerk

WDS – Wireless Distribution System

Werden mehrere WLAN-Access-Points zu einem Funknetzwerk zusammengefasst, spricht man von WDS. Damit erreicht man eine größere Abdeckung als mit nur einem Zugangspunkt. Für die Access-Points müssen nur entsprechende Stromanschlüsse vorhanden sein.

Werden die Access-Points nur direkt verbunden und dürfen sich an diesen keine weiteren Clients anmelden, spricht man vom **Bridging-Modus**. Ist auch die Anmeldung von Clients möglich, bezeichnet man das als **Repeating-Modus**. Alle WDS-Access-Points sollten auf dem gleichen Kanal arbeiten sowie dieselbe SSID und denselben WLAN-Schlüssel verwenden. Zudem müssen jedem Access-Point die WLAN-MAC-Adressen des anderen Access-Points bekannt sein. Sollen mehrere Access-Points zu einem WDS zusammengeschaltet werden, sollte darauf geachtet werden, dass sie nach Möglichkeit vom gleichen Hersteller stammen. Ansonsten kann es passieren, dass nur der unsichere WEP-Modus möglich ist. Gleichzeitig sollte auf den benötigten Funkstandard geachtet werden (z. B. 802.11b/g oder 802.11n).

OSI-Einordnung und Standards

Schicht 2: Sicherungsschicht (Data Link Layer)	802.11 Protokollfamilie
Schicht 1: Bitübertragungsschicht (Physical Layer)	

Die Protokolle, die vom IEEE (Institute of Electrical and Electronic Engineers) für die Standards der drahtlosen Netzwerke definiert wurden, sind in 802.11 zusammengefasst. Sie definieren die Vorgehensweisen auf den Schichten Eins und Zwei des OSI-Modells sowie Geschwindigkeiten und Zugriffsverfahren. Neben dieser Aufstellung gibt es viele proprietäre Lösungen von Herstellern entsprechender Netzwerkkomponenten. Beim durchgehenden Einsatz von Hardware eines Herstellers sind höhere Übertragungsraten möglich. Beispiel: die Firma AVM aus Berlin, die in ihrem Bereich Marktführer ist (<http://www.avm.de/>), bekannt als Hersteller der „FRITZ!Box“.

802.11	Definiert eine Übertragung von bis zu 2 Mbit/s auf dem 2,4-Ghz-Band
802.11 a	Definiert eine Übertragung von bis zu 54 Mbit/s auf dem 5-Ghz-Band
802.11ac	Erweiterung von 802.11n. Mit 2 Antennen sind derzeit max. 867 MBit/s; mit 3 Antennen 1300 MBit/s brutto im 5-GHz-Band erreichbar.
802.11ad	In Zukunft im 60-GHz-Band mit vier 2000 MHz breiten Funkkanälen auf kurze Distanzen bei Übertragungsraten von bis zu 6930 Mbit/s
802.11ah	„Wi-Fi HaLow“, veröffentlicht Anfang 2016; im Frequenzband um 900 MHz; kurze Übertragungen im „Internet der Dinge“ (IoT; Internet of Things).
802.11 b	Definiert eine Übertragung von bis zu 11 Mbit/s auf dem 2,4-Ghz-Band
802.11 g	Definiert eine Übertragung von bis zu 54 Mbit/s auf dem 2,4-Ghz-Band
802.11 h	Definiert eine Übertragung von bis zu 54 Mbit/s auf dem 5-Ghz-Band
802.11 n	Definiert eine Übertragungsrate von 600 Mbit/s auf dem 2,4- und dem 5-Ghz-Band
802.11 p	Definiert eine Übertragung von bis zu 27 Mbit/s auf dem 5-Ghz-Band (Einsatz im Verkehr)

Laufend aktualisierte Angaben zur Normenfamilie 802.11 finden Sie unter https://de.wikipedia.org/wiki/IEEE_802.11.

17.2 Sicherheit

Zugang zum WLAN

Um den Zugang zu einem WLAN zu erlangen, ist es nötig, eine Anmeldung der beteiligten Komponenten untereinander durchzuführen: Sender und Empfänger müssen voneinander wissen, ehe sie Daten senden können.

Dabei kann zusätzlich eine Zugriffskontrolle durchgeführt werden, diese ist jedoch keine Voraussetzung. Allerdings sollte sie nach Möglichkeit erfolgen, um das Netzwerk vor unautorisierten Zugriffen zu schützen. Die Standards, die hierbei Verwendung finden, sind vor allem:

- ✓ Open System Authentication (802.11)
- ✓ Shared Key Authentication (802.11)
- ✓ 802.1X-Authentifizierung mit Unterverfahren

Open System Authentication

Die Open System Authentication basiert auf dem Prinzip der gegenseitigen Bekanntmachung der beteiligten Komponenten und enthält keinerlei Form von Zugriffskontrolle. Es handelt sich lediglich um eine Reihe von Nachrichten, mit denen sich die Geräte gegenseitig über verwendete Frequenzen, Geschwindigkeiten und ihre generelle Erreichbarkeit in Kenntnis setzen, ohne dass ein Gerät etwa in der Lage wäre, dem anderen den Zugriff zu verwehren. Open System Authentication ist das Standardverfahren von WLAN-Geräten gemäß 802.11-Spezifikation.

Shared Key Authentication

Die Shared Key Authentication wird als Verfahren mit integrierter Zugriffssicherheit gemäß 802.11 eingesetzt. Es basiert auf einem gemeinsamen Schlüssel, der vor dem Zugriff auf das WLAN zwischen den beteiligten Komponenten ausgetauscht wurde. Über das Funknetz darf der Schlüssel jedoch nie versendet werden, da ihn ein potenzieller Angreifer sonst abfangen könnte. Alle Geräte, die innerhalb eines Netzes miteinander kommunizieren wollen, müssen über denselben Schlüssel verfügen. Sie benötigen außerdem eine Implementierung des Wired-Equivalent-Privacy-Algorithmus (WEP-Algorithmus), des von Shared Key Authentication verwendeten Verschlüsselungsmechanismus.

Eine Shared Key Authentication läuft folgendermaßen ab:

Sender	Empfänger
Sendet eine Bekanntmachung, wobei im Paket ein Wert enthalten ist, der mit dem Schlüssel verschlüsselt wurde.	
	Sendet eine Empfangsbestätigung mit einem 128-Bit-Challenge-Block, der unter Verwendung von WEP generiert wurde.
Kopiert den Challenge-Block in ein neues Paket und verschlüsselt ihn mit WEP unter Verwendung des Shared Key.	
	Entschlüsselt den empfangenen Challenge-Block mit seinem Shared Key und vergleicht ihn mit der Ursprungsnachricht. Wenn beide identisch sind, ist die Authentifizierung erfolgreich abgeschlossen.

802.1X-Authentifizierung

Die Authentifizierung von Hosts mittels 802.1X ist nicht für ein bestimmtes Übertragungsmedium definiert, sondern stellt ein Standardverfahren für die Zugangskontrolle zu Netzwerken dar. Sie ist unter dem Namen RADIUS (Remote Authentication Dial-In User Service) vor allem bei Einwahlservfern ein Standardverfahren, das sich in unterschiedlichen Implementierungen bewährt hat. Im WLAN-Bereich können unterschiedliche Authentifizierungsprotokolle mit RADIUS eingesetzt werden. Das verbreitetste ist eine Unterversion des Extensible Authentication Protocols (EAP), die speziell auf der Transportschicht aufsetzt.

EAP-TLS

Extensible Authentication Protocol-Transport Level Security (EAP-TLS) ist ein herstellerübergreifendes Verfahren für die gegenseitige sichere Authentifizierung bei Netzwerkzugriffen, das auf der Private Key Infrastructure (PKI) basiert und die Verwendung digitaler Zertifikate voraussetzt.

PEAP-MS-CHAP v2

Ein weiteres Verfahren ist das proprietäre PEAP-MS-CHAP v2 (Protected EAP-Microsoft Challenge-Handshake Authentication Protocol), das auf einer Übertragung der schwach verschlüsselten CHAP-v2-Authentifizierung innerhalb eines stark verschlüsselten Kanals basiert. Es kommt in Windows-Server-2003- und Windows-XP-Umgebungen zum Einsatz, in denen keine PKI implementiert ist.

Verschlüsselung

Um den Datenverkehr in ein WLAN zu sichern, sollte unbedingt die Kommunikation verschlüsselt werden. Das Standardverfahren für die Verschlüsselung war laut 802.11 eine RC4-Verschlüsselung mit Wired Equivalent Privacy (WEP), die auf Shared Key Authentication aufbaut. Diese erwies sich jedoch aufgrund zahlreicher Designfehler und Schwächen im verwendeten RC4-Algorithmus als Katastrophe.

Nachdem die gravierenden Probleme von WEP bekannt wurden, wurde fieberhaft an besseren Sicherheitsprotokollen gearbeitet. Dabei wurde allerdings auch klar, dass diese neuen Standards nicht kurzfristig verfügbar sein könnten.

Zusätzlich war abzusehen, dass man in einem neuen Standard nicht einfach einen neuen Verschlüsselungsalgorithmus vorschreiben kann, da in der bereits verkauften und im Einsatz befindlichen Hardware der verwendete RC4-Algorithmus hardwaremäßig implementiert war.

Als Interimslösung wurde deswegen Ende 2002 der Standard WPA verabschiedet, der die wichtigsten Änderungen des endgültigen Sicherheitsstandards 802.11i vorwegnehmen sollte, und zwar in einer Form, in der er auch auf bereits verkaufter WEP-kompatibler Hardware lief.

WPA

Wireless Protected Access führt einen auf RC4-basierten neuen Algorithmus zur Verschlüsselung ein, der TKIP genannt wird. Des Weiteren wurde die Authentifizierung der Datenpakete statt mit einem für diese Zwecke unbrauchbaren CRC32 nun mit dem Michael-Algorithmus durchgeführt.

Als eine der wichtigsten Verbesserungen in WPA ist aber die Tatsache anzusehen, dass das festgelegte Passwort in WPA nicht mehr der Verschlüsselungsschlüssel selbst ist, sondern dass die Schlüssel mit kryptografisch gesicherten Methoden hergeleitet und regelmäßig erneuert werden. Die Schlüssel werden automatisch in einem Zeitraum erneuert, in dem es mit üblichen Methoden nicht mehr möglich erscheint, diese Schlüssel zu knacken. Sollte WPA zusammen mit einem Preshared Key (PSK) betrieben werden, besteht natürlich die Gefahr, dass man durch einen schlecht gewählten oder zu einfach erratbaren PSK den Sicherheitsgewinn von WPA wieder zunichtemacht.

Zusätzlich sieht WPA auch die Unterstützung von RADIUS-Servern (Remote Authentication Dial-In User Service) zur Authentifizierung der Funkteilnehmer vor.

802.11i / WPA2

Im Juni 2004 wurde der endgültige WLAN-Sicherheitsstandard mit der Bezeichnung IEEE 802.11i verabschiedet, der nun von einigen Herstellern als WPA2 zitiert wird. Die wesentlichen Kernpunkte, die im WPA schon vorweggenommen wurden (wie z. B. regelmäßige automatische Erneuerung der verwendeten Verschlüsselungsschlüssel), blieben erhalten.

Anstatt des betagten RC4-Verschlüsselungsalgorithmus bzw. seiner Ableitung TKIP und dem Michael-Algorithmus zur Authentifizierung wird hier nun der moderne Standardalgorithmus AES (Advanced Encryption Standard) verbindlich vorgeschrieben.

Ein Funknetz, das mit 802.11i-Verschlüsselung betrieben wird, kann als wesentlich sicherer angesehen werden als ein WEP- oder sogar ein WPA-Netzwerk. Allerdings sollten Sie dabei beachten, dass bei Absicherung Ihres Netzes mit Preshared Keys Ihre Sicherheit davon abhängt, wie leicht oder schwer die verwendeten Preshared Keys (also die Passwörter) zu erraten sind.

18 Firewall und DMZ

In diesem Kapitel erfahren Sie

- ✓ was eine Firewall ist und wofür man sie einsetzt
- ✓ welche Typen von Firewalls sich unterscheiden lassen
- ✓ wie Sie mit Firewalls eine DMZ aufbauen können
- ✓ was sich hinter NAT verbirgt

Voraussetzungen

- ✓ Netzwerkprotokolle
- ✓ Internet-Protokoll
- ✓ Ports
- ✓ ISO/OSI-Schichtenmodell

18.1 Wie Firewalls arbeiten

Aufgaben einer Firewall

Der englische Begriff Firewall steht für eine Wand bzw. Mauer aus nicht brennbarem Material, die in Gebäuden platziert wird, um die flächendeckende Ausbreitung von Bränden zu verhindern. Als Analogie in der Informationsverarbeitung soll eine Firewall, die sich an der Grenze zwischen dem eigenen Netzwerk und dem Internet (oder auch auf den einzelnen Rechnern) befindet, die Ausbreitung von Gefahren (=Bränden) aus dem Internet in das eigene Netz verhindern. Einfacher formuliert: eine Firewall schützt vor unerwünschten Netzwerzkriegen.

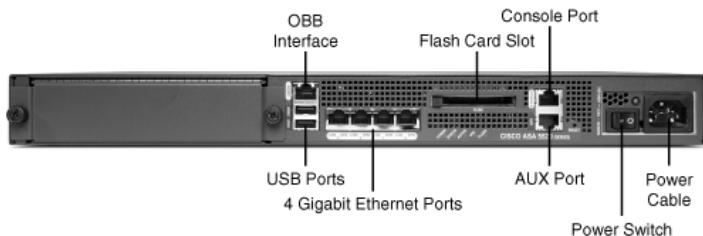
Eine Firewall ist ein System oder eine Gruppe von Systemen, deren Aufgabe darin besteht, die Kommunikation zu und von einem Netzwerk anhand von vorhandenen Regeln (Policies) zu erlauben oder zu verbieten. Eine Firewall verwendet Regeln bzw. Regelsätze, um den Datenverkehr einzuschränken. Wurde eine Firewall ohne eine klare Definition ihres Nutzens eingerichtet oder ohne Regeln auf dem neuesten Stand, dürfte sie relativ nutzlos sein.

Obwohl Firewalls gewisse Schutzmaßnahmen gegen Angriffe von außen zur Verfügung stellen können, sind sie nur im Team mit flankierenden Maßnahmen wirklich wirkungsvoll. Neben Firewalls sind für Firmen weitere Schutzmaßnahmen wie beispielsweise aktualisierte VirensScanner, Netzwerkbereiche mit Zugangskontrolle und Verschlüsselung nötig. Die Schutzmaßnahmen erfordern eine konstante Aktualisierung und Wartung.

Es spricht übrigens nichts dagegen, neben einer leistungsstarken Firewall an der Grenze des eigenen Netzwerks auch verfügbare lokale Firewalls (personal firewall) zusätzlich zu betreiben. Aktuelle Windows-Betriebssysteme bieten z. B. die „Windows-Firewall mit erweiterter Sicherheit“ (Microsoft Firewall with Advanced Security). Das Verständnis, dass Bedrohungen nur von außerhalb eines Netzwerks zu erwarten sind, hat sich in den letzten Jahren verändert.

Hard- oder Software

Firewalls können entweder als Hard- oder Softwarelösungen verfügbar sein. Die Grenzen hierfür sind fließend. Die Bandbreite erstreckt sich von der Open Source Linux Firewall über die Microsoft Firewall with Advanced Security bis zu Hardware Appliances wie z. B. der Cisco ASA Firewall.



Cisco ASA Firewall

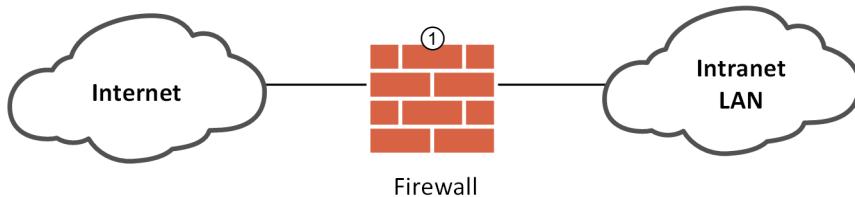
In Appliances (engl. appliance Vorrichtung, auch: Gerät) kommen speziell angepasste Betriebssysteme zum Einsatz, die für die Verwendung als Firewall „gehärtet“ wurden. Das bedeutet, dass das Firewallbetriebssystem nur über die optimierte Funktionalität der Dienste verfügt und so gegen Sicherheitslücken effizienter geschützt ist. Eine Firewall ist nur so stabil wie das Betriebssystem, auf dem sie aufsetzt. Gelingt es einem Angreifer von außen, Systemrechte auf einem Firewallsystem aufgrund eines Fehlers im Betriebssystem zu erlangen, so ist die Firewall nutzlos.

Bei einer Entscheidung für die eine oder andere Lösung sollten Sie berücksichtigen, dass zwar Software möglicherweise einfacher zu warten oder zu aktualisieren ist als eine Hardware-Firewall. Dagegen haben Hardwarelösungen den Vorteil, vom Betriebssystem eines normalen Rechners abgekoppelt zu sein. Die meisten Profis ziehen – nicht nur bei diesem Thema – bei freier Wahl eine spezialisierte Hardwarelösung vor.

Firewall-Konzepte

Je nach Schutzbedarf und Topologie eines Netzwerkes können eine oder mehrere Firewalls platziert werden. Wichtig in allen Fällen ist jedoch, dass sämtliche Kommunikationswege in das geschützte Netzwerk hinein und aus dem geschützten Netzwerk heraus über die Firewall laufen. Das beste Firewall-Konzept wird untergraben, wenn sich hinter der Firewall im internen Netz z. B. ein Einwahlserver oder ein WLAN-Access-Point befindet, der Zugriffe von außen erlaubt.

Die einfachste Lösung besteht aus einer Firewall ①, die am Übergabepunkt vom Intranet zum Internet den Datenverkehr überwacht.



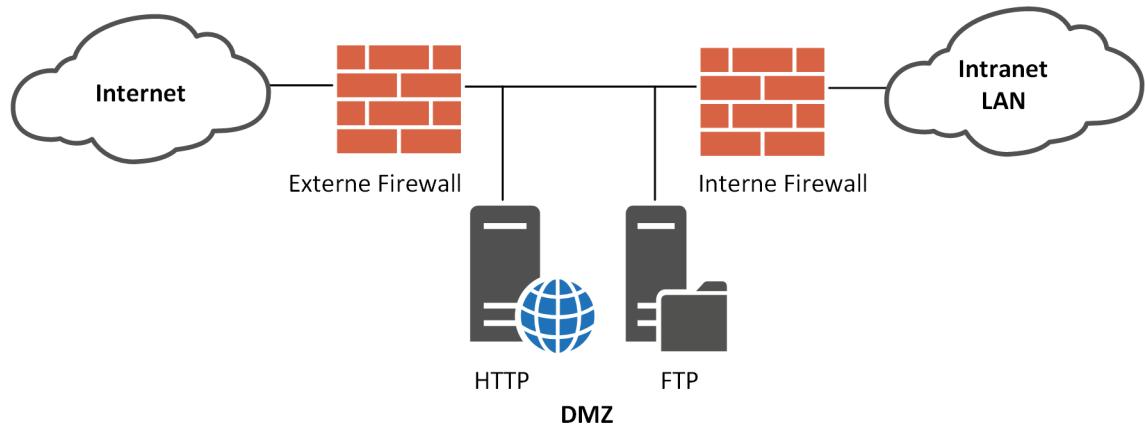
Einfaches Firewallkonzept

Obwohl diese Lösung relativ einfach zu realisieren ist, ist die damit erzielte Sicherheit im Vergleich zu den anderen möglichen Lösungen eher bescheiden. Sollte diese Firewall selbst einem Angriff zum Opfer fallen, so steht das Intranet dem Angreifer offen.

Darüber hinaus ist es mit diesem Konzept problematisch, im Intranet einen Server zu betreiben, der vom Internet aus erreichbar sein soll. Konfigurieren Sie die Firewall so, dass Zugriffe von außen auf diesen benötigten Server (z. B. auf einen WWW-Server) erlaubt sein sollen, so könnte dies auch ein Angriffsfläche für externe Angreifer werden. Gelingt es einem Angreifer in diesem Szenario, Kontrolle über den WWW-Server zu erlangen, so kann dieser als Relaystation für weitere Zugriffe auf sämtliche andere Rechner im Netzwerk benutzt werden.

Als Antwort auf die Problematik, dass das Intranet geschützt werden sollte, bestimmte Rechner aber weiterhin von außen erreichbar sein sollen, werden die von außen zugreifbaren Server in einen vorgelagerten Bereich des Intranets verlagert. Die Rechner mit diesen speziellen Serveraufgaben (Bastion-Host, da sie besonders gesichert werden sollten) befinden sich also im Niemandsland zwischen dem Intranet und dem Internet.

Als Fachausdrücke für dieses Niemandsland haben sich die Begriffe „Perimeternetzwerk“ oder „Demilitarisierte Zone“ (DMZ) durchgesetzt.

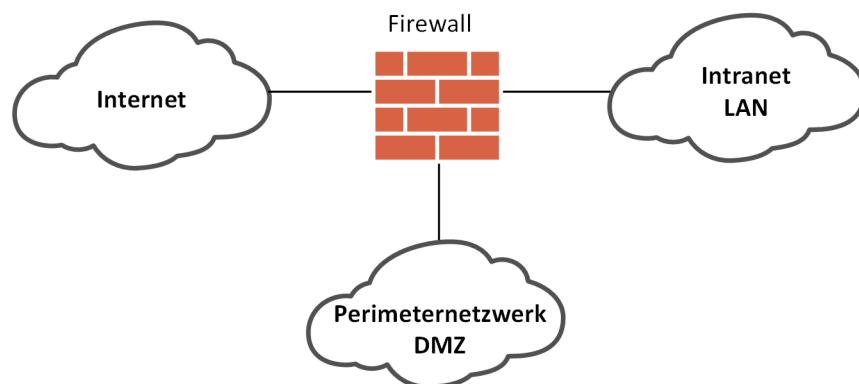


Zweistufige Firewall mit DMZ

Im Normalfall wird die externe Firewall über Zugriffsregeln (erweiterte Access-Listen) so konfiguriert, dass sie eingehenden Datenverkehr nur erlaubt, wenn das Ziel einer der in der DMZ installierten Serverdienste ist (in diesem Beispiel HTTP und FTP). Alle anderen Verbindungsversuche werden verworfen. Die interne Firewall sollte keinen Zugriff vom Internet in das Intranet erlauben, um die Systeme im Intranet zu schützen. Umgekehrt kann die interne Firewall so konfiguriert werden, dass es Computern aus dem Intranet nur gestattet ist, den firmeneigenen WWW- oder FTP-Server zu nutzen. Eine darüber hinausgehende Nutzung des Internets kann dann an der externen Firewall unterbunden werden, die außer den Servern in der DMZ keine Verbindungen erlaubt. In diesem Szenario, das von vielen als Ideallösung beschrieben wird, unterscheidet sich die Konfiguration beider Firewalls grundlegend, da die externe Firewall die Kommunikation von außen zu den Servern in der DMZ steuert, die interne Firewall idealerweise aber nur die Kommunikation mancher Server in der DMZ mit netzwerkinternen Hosts zulässt und entsprechend steuert.

Würde in so einem Fall die externe Firewall oder einer der Server in der DMZ von einem Hacker übernommen, so blieben seine Zugriffsmöglichkeiten durch das Blockieren durch die interne Firewall nur auf die DMZ beschränkt.

Eine günstige Version eines Perimeternetzwerkes kann dadurch realisiert werden, dass an einem Firewallrechner bzw. einer Firewall-Appliance mehrere Interfaces vorhanden sind. So kann das Perimeternetz ohne weiteren Hardwareaufwand, aber mit der Möglichkeit zur speziellen Konfiguration eingebunden werden.



Firewall mit frei konfigurierbaren Interfaces

18.2 Paketfilter-Firewall

Access Control Lists

Die Methoden, mit denen Firewalls zwischen erwünschtem/erlaubtem und unerwünschtem/verbotenem Datenverkehr unterscheiden, können auf unterschiedlicher Ebene im OSI-Modell ansetzen. Der einfachste Firewalltyp ist bei einer derartigen Unterscheidung die sogenannte **Paketfilter-Firewall**. Sie ist prinzipiell auf jedem Router und Multilayerswitch möglich.

In einer Paketfilter-Firewall wird anhand vorgegebener Regeln verifiziert, welche Art von Datenverkehr überprüft werden soll. Die verwendete Liste wird Access Control List (ACL) genannt und enthält üblicherweise eine tabellarische Aufstellung von Zulassen/Verbieten-Regeln zu Quelladressen, Zieladressen, Protokollen und Portnummern. Eine Paketfirewall ist auf Layer 3 und 4 des OSI-Referenzmodells angesiedelt.

```
access-list 100 deny      ip 10.0.0.0 0.255.255.255 any
access-list 100 deny      ip 172.16.0.0 0.15.255.255 any
access-list 100 deny      ip 192.168.0.0 0.0.255.255 any
access-list 100 deny      ip 169.254.0.0 0.0.255.255 any
access-list 100 deny      ip 192.0.2.0 0.0.0.255 any
access-list 100 permit    tcp any host mailgate eq smtp
access-list 100 permit    udp any host pdc01 eq domain
access-list 100 permit    tcp host admin1 host nas eq ftp
access-list 100 permit    tcp host admin1 host nas eq ftp-data
access-list 100 permit    tcp any gt 1024 host websrv eq www
```

Beispiel der ACL auf einem Cisco Router

Der erste Teil beschreibt nur Regeln auf Layer 3, der zweite Teil zusätzliche Regeln auf Layer 4. Der allgemeine Aufbau einer ACL stellt sich wie folgt dar:

- ✓ Die Klassifizierung als ACL und die Nummer bzw. der Name der ACL (`access-list 100`)
- ✓ Die Aktion (Verbieten/Erlauben), die auf diesen Regeleintrag angewendet werden soll (`deny` oder `permit`)
- ✓ Das Protokoll, das diese Policy nutzen soll (Layer 3: `ip`, `icmp`, `ipv6`, `icmpv6`; Layer 4: `udp`, `tcp`)
- ✓ Das Source-Netz mit Wildcard (`10.0.0.0 / 0.255.255.255`) oder ein einzelner Host (`host admin1`) oder jeder (`any`) und ggf. der Source-Port (im Bsp. `gt 1024`, greater than 1024, größer als 1024)
- ✓ Das Destination-Netz mit Wildcard oder ein einzelner Host (`host mailgate`) oder jeder (`any`) und ggf. der Destination-Port (im Bsp. `eq snmp`, equal snmp, gleich snmp)

Die oben genannten Regeln werden nacheinander abgearbeitet. Sobald eine Übereinstimmung (Match) mit einem Paket erfolgt, wird das Regelwerk verlassen und nachfolgende Regeln kommen nicht mehr zur Anwendung. Damit es immer einen Match gibt, heißt die letzte Regel, die automatisch von System gesetzt wird, `access-list <Nummer oder Name> deny ip any` bzw. bei einer erweiterten ACL `access-list <Nummer oder Name> deny ip any any`.

Beim Setzen einer ACL gibt es die „goldene Regel“ *Deny-All*, die besagt: Alles ist verboten (deny), erlauben (permit) muss man ausdrücklich selbst.

Da das Filtern von Paketen auf Grundlage dieser **statischen** Listen keinen kompletten Schutz vor komplexen Angriffen bieten kann, ist ein alleiniger Schutz durch Paketfilter nicht zu empfehlen, aber zur Basisfilterung sinnvoll.

18.3 Stateful Inspection Firewall

Pakete im Kontext betrachten

Im Gegensatz zu den statischen Paketfiltern ist das Stateful Inspection Firewalling eine **dynamische Filtermethode**. Eine Firewall, die für die Entscheidung über die Weiterleitung eines bestimmten Datenpakets nicht nur die Merkmale dieses Pakets, sondern auch den individuellen Kontext in Betracht zieht, in dem es durchgeführt werden soll, ist eine **Stateful Inspection Firewall**.

Um die nötigen Informationen als Entscheidungsgrundlage zur Verfügung zu haben, legt die Firewall auf der Basis der Regelabelle zusätzlich eine State-Tabelle (engl. State = Zustand) an, in der bei den ein- und ausgehenden Verbindungen alle Zustände vermerkt sind.

Der Firewall ist somit bekannt, welche Pakete zu einem Zeitpunkt legitim sind und prinzipiell passieren können und welche zu keiner gültigen Verbindung gehören. Ein Angriff, der beispielsweise Pakete mit ACK-Flags an Rechner im geschützten Netz sendet und vorgaukelt, der Angreifer würde nur auf eine Anfrage des geschützten Rechners antworten, kann somit die Firewall nicht mehr überlisten, da hier in der State-Tabelle keine ausgehende Anfrage eines geschützten Rechners vermerkt ist, zu der das empfangene Paket mit ACK-Flag passen würde – das Paket wird verworfen.

Mit anderen Worten: Die Ports einer SPI (Stateful Packet Inspection) Firewall sind grundsätzlich geschlossen. Benötigt eine Anfrage aus dem internen Netzwerk den Port, wird genau dieser Port nur für den Zeitraum geöffnet, in dem er benutzt wird.

Um eventuelle Verbindungsinformationen aus den Paketen auslesen zu können, muss eine SPI Firewall den Inhalt der Pakete genauer als nur bis zu den IP- und Portnummern überprüfen. Untersuchte Daten sind bei TCP-Datenströmen z. B. die angesprochenen Flags und die Sequenznummern der Pakete. Eine spezielle Form der SPI ist die Deep Packet Inspection, bei der auch die Nutzdaten des Pakets analysiert werden.

IP-Fragmentation

Manche Angriffsmethode zielt darauf ab, den Inhalt von Paketen vor der Inspektion durch eine Firewall zu verborgen. Bei diesen sogenannten Fragmentation-Attacken werden die versendeten Pakete bewusst in Fragmente aufgeteilt.

Fragmentierung kommt in IP-Netzwerken üblicherweise dann zum Einsatz, wenn die Paketlänge auf dem Weg vom Sender zum Empfänger die maximale Segmentgröße in einem Netzwerk übersteigt. Die aufgeteilten, kleineren Fragmente können aber problemlos übertragen werden und werden empfängerseitig wieder zusammengesetzt.

Durch geschicktes absichtliches Fragmentieren von Datenpaketen ist es mitunter möglich, eine Firewall über den Inhalt der Pakete zu täuschen.

Analog dazu entgeht dem menschlichen Beobachter der Inhalt eines Wortes leichter, wenn dieses in Buchstabengruppen „fragmentiert“ wurde:

CY BE RKR I MI NA L ITÄ T.

Haben Sie nur wenig Zeit, dieses Wort zu entziffern, entgeht Ihnen möglicherweise die Bedeutung.

Ein weiterer Effekt, der durch IP-Fragmentierung genutzt wird, lässt sich als Text so umschreiben:

Ein fragmentiertes Paket wird verschickt. Die erste Hälfte enthält "LASTWAGEN", die zweite Hälfte "ERHAFT".

Eine nicht korrekt reassemblierende Firewall würde ggf. den Inhalt des Paketes als "LASTWAGENERHAFT" beurteilen und als nicht bedrohlich. "Ø" ist jedoch ein Löscheichen und löscht das zuvor gedruckte Zeichen. In diesem Textbeispiel werden also beim Zusammensetzen beider Informationshälften die letzten fünf Zeichen von LASTWAGEN gelöscht und die Zeichen ERHAFT angefügt. Das Ergebnis ist LASTERHAFT.

Auf IP-Ebene wird ein ähnlicher Effekt durch Manipulation der Datenzeiger erreicht. So werden die zuvor gesendeten „Tarn“-Daten mit den Daten der zweiten Fragmenthälfte wieder überschrieben, sodass sie auf dem Zielrechner das vom Angreifer gewünschte Datenpaket ergeben.

18.4 Proxy Level/Application Level Firewall

Höhere Schichten im OSI-Modell

Werden neben der Paketinformation in den Datenströmen auch die Informationen von höheren Schichten ausgewertet, so ist es technisch möglich, einen Datenstrom bis zur Anwendungsebene auf Schicht 7 wieder zusammenzufügen. Die Firewall wertet nun den enthaltenen Datenverkehr nicht mehr nur auf Netzwerk- oder Transportebene aus, sondern überprüft die Informationen bis zur Applikationsschicht. Dadurch kann auch der Dateninhalt vollständig überprüft werden.

Logisch gesehen bedeutet das: Wird mit Datenpaketen eine E-Mail versandt, so baut die Firewall die Pakete zusammen, bis die E-Mail komplett auf dem Firewall-System vorliegt. Anschließend kann entschieden werden, ob die Weiterleitung dieser E-Mail in Abhängigkeit von Absender, Empfänger, Betreff, Inhalt oder angehängten Dateien erlaubt oder gesondert behandelt wird.

Dieses Konzept stellt eine sogenannte **Application Level Firewall** oder **Proxy Firewall** dar. Je nach Protokoll ermöglicht diese Vorgehensweise durch entsprechende Regeln z. B. das Sperren von E-Mail von bestimmten Absendern oder mit definierten Inhalten sowie das Blockieren von Websites mit bestimmten Inhalten (z. B. Active Scripting). So könnten auch Werbebanner und Popup-Fenster gefiltert, der restliche Inhalt einer Website aber zugelassen werden.

Wenn Application Level Firewalls quasi als Stellvertreter für Clients den eigentlichen Server im Internet kontaktieren, werden sie als Proxy-Firewalls bezeichnet (engl. Proxy: Stellvertreter, Bevollmächtigter).

Der Nachteil dieser Methode ist der große Ressourcenaufwand, der nötig ist, um in der Firewall diese Protokolle nachzubilden und entsprechende Filterregeln anzuwenden. Des Weiteren ist für jede Anwendung bzw. jedes Protokoll eine entsprechend kompatible Proxy-Firewall nötig. Firewalls auf Paketebene arbeiten dagegen anwendungsunabhängig.

Zugriff auf eine Webseite im Internet

Möchte beispielsweise ein Clientrechner eine Webseite eines bestimmten Servers abrufen, so wird die Verbindung zunächst mit der Firewall aufgebaut. Diese prüft die Zulässigkeit der Verbindung und baut dann ihrerseits die Verbindung zum gewünschten Server auf. Nun wird die HTML-Seite übertragen und ihr Inhalt analysiert. Soll die Firewall z. B. Werbebanner filtern, so werden aus der empfangenen HTML-Seite alle Anweisungen entfernt, die einen Popup-Aufruf oder eine Bannereinblendung enthalten. Diese so modifizierte Seite wird dann an den Client weitergeleitet. Da der Client seinerseits die HTML-Seite auswertet und anschließend die zu deren Darstellung nötigen Grafiken nachlädt, lädt die Firewall schon vorsorglich die entsprechenden Grafiken vom Internet-Webserver und reicht diese an den Client weiter. Als Ergebnis sieht der Client eine werbefreie Webseite. Auch die Bandbreite wird geschont, da Bannergrafiken gar nicht erst heruntergeladen werden müssen.

Flexible Einsatzmöglichkeiten

Je nach Aufbau und Ausrichtung der Regelsets können so Webseiten, FTP-Dienste oder beliebige andere Internetprotokolle und -anwendungen gefiltert und überwacht werden, bevor deren Nutzung für interne Clients zugelassen wird.

Proxies bieten die umfassendsten Möglichkeiten zur Filterung von Datenverkehr, sind aber aufwendig, da die Proxyfunktionen für jede Anwendung angepasst sind. Um die Performance der Application Level Firewall zu gewährleisten, werden u. a. einige Proxyanwendungen der Applikationen zusammengefasst. Man nennt dies generic Proxy.

18.5 NAT

Interne IP-Adressen verbergen

Damit jeder Rechner Zugang zum Internet hat, benötigt er eine offiziell gültige IP-Adresse. Durch die chronische Knappheit an öffentlich verfügbaren IP-Adressen beim IPv4-Protokoll wäre es nicht machbar, für jeden Rechner in einem Netzwerk auf Dauer eine öffentliche IP-Adresse zu reservieren. Darüber hinaus wäre ein Anschluss von Netzwerkrechnern mit öffentlichen IP-Adressen problematisch, weil theoretisch eben diese IP-Adressen von außen ebenfalls zu erreichen wären, sofern man keinen konfigurierten Paketfilter betreibt.

Das Konzept hinter der **Network Address Translation (NAT)** ist nun, dass nur die Firewall oder ein Router, der den LAN-Anschluss an das Internet realisiert, eine gültige öffentliche IP-Adresse besitzt. Alle im LAN befindlichen Rechner erhalten private IP-Adressen (nach RFC 1918, z. B. aus dem Bereich 192.168.x.x/16), die intern frei vergeben werden können.

Auf diese Weise werden vom Pool an öffentlichen Adressen nur sehr wenige benötigt, und zusätzlich werden die Rechner im LAN vor dem Internet verborgen. Ein Außenstehender sieht nur die öffentliche IP-Adresse des Routers und glaubt, dieser wäre sein Kommunikationspartner. Ein Client im LAN, der eine Verbindung zum Internet aufbauen möchte, kommuniziert wie üblich über den Router als Gateway.

Verwaltung der Verbindungen mit NAT

Bei ausgehenden Verbindungen vermerkt die Firewall oder der Router in einer Tabelle, welcher interne Client zu welchem Rechner im Internet eine Verbindung aufbauen möchte. Anschließend passt sie den Header der ausgehenden IP-Pakete so an, dass die externe IP-Adresse des Routers im Absender-Feld steht. Diese Pakete werden dann versandt.

Treffen an der Firewall oder dem Router Pakete aus dem Internet ein, so wird verglichen, ob diese eine Antwort auf eine Anfrage aus dem internen Netz sind. Wenn ja, kann sie eine Zuordnung zur entsprechenden LAN-IP vornehmen, den Header der Datenpakete entsprechend anpassen und diese dann ins LAN weiterleiten. Kann sie keine Übereinstimmung finden, so werden von außen kommende Datenpakete verworfen.

Sicherheit von NAT

NAT ist eine sichere und effiziente Methode, die interne Netzstruktur gegenüber dem Internet zu verbergen. Zu beachten ist jedoch, dass das Betreiben von Servern, die öffentlich verfügbar sein sollen, hinter einer NAT-Firewall nicht ohne Weiteres funktioniert. Dies hängt von der Wahl des NAT-Verfahrens ab.

Da eintreffende Pakete ohne Anforderung von innen verworfen werden müssen, weil die Firewall sie keinem internen Rechner zuordnen kann, muss die Zuordnung manuell vorgenommen werden. Diese Zuordnung geschieht meist anhand einer Tabelle, in der für eingehende Pakete mit bestimmten TCP- und UDP-Portnummern die internen Ziel-Adressen definiert werden. Hierbei spielt keine Rolle, ob ein eingehendes TCP auf Port 25 auf den Intranet-SMTP-Server ebenfalls auf Port 25 oder auf irgendeinen anderen Port umgeleitet wird. Die Verwendung von Nicht-Standard-Portnummern bringt allerdings kein erhöhtes Maß an Sicherheit.

18.6 Personal Firewall

Firewall auf dem Desktop-PC

Auf dem Softwaremarkt haben sich zunehmend sogenannte Personal Firewalls etabliert. Eine Personal Firewall ist ein Softwarepaket, das den im Betriebssystem vorhandenen TCP/IP-Stack durch einen funktionserweiterten Stack der Firewall ersetzt und somit dem Anwender die Kontrolle über die Nutzung der Internet-Funktionalität durch die laufenden Programme ermöglicht. Microsoft-Betriebssysteme ab Windows XP SP2 haben bereits eine Firewallfunktionalität im Betriebssystem integriert.

Eine Personal Firewall erledigt also innerhalb eines PCs dieselbe Funktion wie ein Firewall-Router in einem Netzwerk mit mehreren Computern.

Der Vorteil vor allem für Privatanwender ist, dass diese ihren PC bei der Nutzung des Internets relativ kostengünstig vor Zugriffen von außen schützen können. Darüber hinaus beinhalten viele Personal Firewalls Funktionen, die auch den Verbindungsweg vom Computer in das Internet kontrollieren und so unkontrollierbares „Nach-Hause-Telefonieren“ von installierter Software unterbinden können.

Personal Firewall in der Firma

In Firmennetzwerken sind Personal Firewalls maximal als zusätzliche Instanz zu anderen Lösungen anzutreffen, da sie eingeschränkte Konfigurationsmöglichkeiten bzw. kein zentrales Managementtool aufweisen und eine Remoteüberwachung selten vorhanden ist.

Wird der Schutz eines Firmennetzwerkes nur der „Haupt-Firewall“ am Einwahlpunkt ins Internet überlassen, so könnte die geschickte Platzierung eines Trojaners oder ein unbefugt angeschlossenes Modem am PC eines Mitarbeiters jeglichen Schutz unwirksam werden lassen. Ist jedoch jeder PC einzeln wiederum durch eine „kleine“ Firewall geschützt, so erschwert das die Arbeit eines Angreifers ungemein.

In allen aktuellen Betriebssystemen sind bereits Firewall-Lösungen integriert, die kommerzielle Produkte zunehmend verdrängen. In Microsoft-Betriebssystemen sind ab Windows Vista in Zusammenarbeit mit Server 2008 die Firewalleteinstellungen über Gruppenrichtlinien zentral konfigurierbar. Die Wartung ist mit Angeboten wie den Microsoft Security Essentials inzwischen so pflegeleicht geworden, dass diese uneingeschränkt empfehlenswert sind.

18.7 Sicherheitskonzept Firewall

Auswahl des Sicherheitskonzeptes

Für den Schutz Ihres Netzwerkes sollten Sie ein mehrstufiges Sicherheitskonzept anwenden. Dies sollte sowohl Aspekte der Sicherheit in Ihrem Intranet als auch Zugriffsregularien zwischen Intranet und Internet beinhalten. Einzelne Bereiche Ihres Intranets können Sie separat mit einer Stateful Packet Inspection Firewall absichern. Als Verbindung zwischen Internet und Intranet sollten mindestens eine Stateful Inspection Firewall und Proxies für die wichtigsten Dienste implementiert werden. Diese Firewall sollte auch die DMZ beinhalten. Auf dem Router, der als Verbindung zum Provider dient, sollten Sie zusätzlich Paketfilter aufsetzen.

8					
802.11	167	Bereichsoptionen	128	Default Gateway	
802.11i	169	Bereitstellung verteilter Dienst	8	Delay	
		Bewegtbildübertragung	50	Delegierte Zonen	
		Bindung des TCP/IP-Stacks	80	Demilitarisierte Zone	
		BIND-Version	108	DeNIC	
		Biometrische Verfahren	151	Destination Port	
		B-ISDN	132	Dezidierte Routen	
		Bitübertragungsschicht	22	DHCP	
		B-Knoten	113	DHCP Message Type	
		Bootimage	117, 118	DHCP-Ack	
		BootP	116	DHCP-Client-Zustände	
		BootP Forwarding	118	DHCP-Decline	
		BootP Request/Reply	117	DHCP-Discover	
		BootP Server	117, 118	DHCP-Failover	
		BootP-Datenbank	118	DHCP-Inform	
		BootP-Protokoll	117	DHCP-Nachrichten	
		BootP-Relay-Agent	118	DHCP-NACK	
		Bootstrap-Protokoll	116	DHCP-Offer	
		Border Gateway Protocol	84	DHCP-Optionen	
		BRI	138	DHCP-Request	
		Bridging-Modus	166	DHCP-Server	
		Broadcast and Unknown Server	136	Dienste	
		Broadcast-Adresse	43, 80	Diensteinträge	
		Broadcast-Domänen	9, 43	Dienstgüte	
		Broadcast-Emulatoren	15	Dienstpublikationslisten	
		BUS	136	Diensttyp	
A					
AAL	133	C			
Abfragevorgang	95	cache.dns	101	Discrete Multitone Modulation	
Access Control List	173	CAP	140	DISPLAYDNS	
ACK	61	Carrier Sense, Multiple Access	6	Distance-Vector-Protokolle	
Acknowledgment	61	Chain of trust	110	DMT	
ACL	173	Checksum	50	DMZ	
Active-Directory-integrierte Zonen	91, 104	CIDR	40	DNS	
Address Resolution Protocol	31, 35	CIFS	32	DNS Standard Query Request	
Ad-hoc-Netzwerke	165	Client	125	DNS Standard Query Response	
Adressauflösung	90	Client für Microsoft-Netzwerke	112	DNS-ALG	
Adressbindung	81	Client Identifier	127	DNS-Cache	
Adressierung	23	Code	50	DNS-Registrierung, dynamische	
Adresskonflikte	35, 129	Collision Detection	6	DNSSEC	
Adress-Pool	119, 129	Congestion Window Reduced	63	DNS-Server	
Adressübersetzung	71, 73	Counting-to-Infinity	86	DoD-Modell	
ADSL	139, 141, 142	CRC23		Domain Name Service	
ADSL over ISDN	142	CSMA/CD	6	Domain Name System	
AES	169	CWR-Flag	63	Domänen	
AH	32, 47, 159	D			
Aktualisierungsintervall	94	Darstellungsschicht	24	DSL	
ALG	75	Data Link Layer	23	DSLAM	
ANSI	24	Datagramme	7, 60	Dual-Stack	
Anwendung	20	Datagram-Service	112	Durchsatz	
Anwendungsschicht	20, 24	Datenbank	93	DWMT	
APIPA	116, 129, 130, 131	Datenbankdatei, WINS	115	Dynamic Host Configuration	
APIPA deaktivieren	131	Datenbanken, dynamische	10	Protocol	
Appliance	171	Datenbanken, statische	10	Dynamische Datenbanken	
Application Layer	24	Datenintegrität	7	Dynamische Einträge	
Application Layer Gateway	75	Datensicherungsschicht	23	Dynamisches DNS	
Application Level Firewall	175	Datensicherungsschicht, Unterschichten	26	Dynamisches Routing	
ARP	30, 31, 35	Datentransport	7	E	
ARP-Request	123	Datenübertragungsverfahren	6	EAP-TLS	
ASCII	24, 32	D-DNS	12, 106, 125	EBCDIC	
ASN.1	24	Schulversion		Echo Reply	
Asymmetric DSL	139	Index			
Asynchronous Transfer Mode	14, 132				
ATM	14, 132				
ATM-Adressen	95, 136				
ATM-LANE	15				
ATM-LAN-Emulation	15				
Ausfallsicherheit	8, 107				
Ausfallsicherheit durch NAT	74				
Authentication Header	32, 159				
Authentifizierung	151				
Authentifizierungsmethode	151				
Authentifizierungsprotokoll	151				
Automatic Private IP Addressing	116, 129				
B					
Basic Rate Interface	138				
Bastion-Host	171				
BDSL	139				
Benutzerauthentifizierung	8, 150				
Bereich	127				
E					
EAP-TLS	168				
EBCDIC	24				
Echo Reply	49				

Echo Request	31, 49	H-Knoten	113	Kerberos	32, 160
ECN-Echo	63	Hold Down Timer	86	Kernnetz	138
EGP	47	Hop Count	85	Key-Distribution-Center	160
Einmal-Passwort-Generatoren	151	Hostadresse	38, 95	Knotentyp	113
Eintragstypen	95	Hostanteil	41	Kooperative Redundanz	128
Encapsulating Security Payload	32, 159	Hostbereich	44		
Encapsulation	45	Hosteintrag	97		
Entkapselung	28	Hostname	90		
ESP	32, 47, 159	Hosts-Datei	11, 92, 113		
Ethernet	9				
Expire	94				
Explicit Congestion Notification	63	I			
Exposed server	74	ICMP	30, 31, 47, 49	L	
		Identifikation	47	L2F	158
		Identifikationsnummer	47	L2TP	48, 158
		IEEE	167	LAN	134, 136
FCS	23	IEEE 802.11i	169	LAN Emulation	136
Fehlerkorrektur	62	IGMP	47	LANE	15, 136
Fehlerüberwachung	23	IKE	159	LAN-Emulation-Address-	
Fenstergröße	66	in-addr.arpa	103	Resolution-Protokoll	136
Fernwartung	148	INET-Information	97	Längeninformation	66
Firewall, Deny All	173	Infrastruktur-Netzwerke	165	Längsparität	48
Firewall, Personal	170, 177	Integrated Services Digital Network	14	Lastenausgleich durch NAT	74
Firewalls	170, 171	Interior Gateway Routing Protocol	84	Lastenverteilung	8, 107
Flags	47	International Network Information		Layer 2 Forwarding	158
FLUSHDNS	92	Center	39	Layer 2 Tunneling Protocol	158
Flusskontrolle	63	Internet Access Router	74	LDAP	104
Flussteuerung	23	Internet Key Exchange	159	LE-ARP	136
Forward Lookup	92, 93	Internet Network Information Center	91	Lease	120
FQDN	91	Internet Security Association and Key		Lease verlängern	124
Fragmentabstand	47	Management Protocol	159	Lease-Dauer	120, 121
Fragmentierungsfehler	50	Internet-Control-Message-		LEC	136
Frame Relay	14, 144, 146	Protokoll	31, 49	LECS	136
Frame-Relay-Netzwerk	146	Internet-Protokoll	30, 50	Length	46
Frames	23	InterNIC	12, 39, 91	LES	136
Frequenzband	138	IP	30, 47, 129	Lightweight-Directory-Access-	
FTP	33	IP Address Pool	127	Protokoll	104
Füllbits	48	IP-Adressen, dynamische	119	Linkstate-Protokolle	87
Fully Qualified Domain Name	91	IP-Adressen, permanente	119	LMHosts	113
Funkkommunikation	16	IP-Adressen, reservierte	119	LMHosts-Datei	11, 113
Funkübertragung	16	IP-Adressen, statische	119	Logisches UND	78
		IP-Broadcastverkehr	114	Logisches Undieren	40
G		IPCONFIG	92	Lokale Netze	108
Gateway	80	IPnP	50	Loopback	80
Generic Routing Encapsulation	32, 158	IP-Paket	45		
Geroutete Protokolle	7	IPSec	151, 158	M	
Gesamtlänge	47	IPv4	15	MAC-Adresse	35
Get Nearest Server	11	IPv4-Header	46	MAC-Broadcast	31, 35
GETHOSTBYNAME()	113	IPv6	15, 50	Mailbox	95
GGP	47	IPv6-Übergangsmechanismen	54	Master/Slave-Konfiguration	12
GNS-Request	11	ISAKMP	159	Maximum Hop Count	86
GRE	32, 47, 158	ISDN	14, 132, 138, 141	M-DSL	139
		ISO/OSI-Modell	19	Metrik	80
H		ISP	141	Michael-Algorithmus	169
H.323	148	Iterative Abfrage	95	Microsoft-enhanced-Knoten	113
Hardware-Router	78	Iterative Namensauflösung	96	M-Knoten	113
HDSL	138, 141	J		Mobile Geräte	16, 121
Header	21, 45, 65, 134	Jumbogramm	52	Modular	22
Headerlänge	46			Modulationsarten	140
Header-Prüfsumme	48			MPLS	135
Herstellererweiterungen	125			Multicast-Bereiche	81
Herstellerspezifisch	117	K		Multi-Master-Modell	12
Hierarchisches Konzept	90	Kapselung	28	Multiplexing	31
		KDC	160	N	
				Namensauflösende Broadcast-	
				Anfragen	10
				Namensauflösende Dienste	10

Namensauflösung	90
Namensauflösung, WINS	114
Namensgebungsregel	10
Namenspublizierende Broadcasts	10
Namensserver	91
Namensserver, NetBIOS	113
Namensserver-Einträge	95
Name-Service	112
NAP	154
NAPT	71
NAPT-Router	71
NAT	70, 176
NAT-Editor	75
NAT-Gateway	75
NAT-Router	72, 73, 74
NAT-Tabelle	71
NBF	112
NBT	112
NDP	35
Neighbor Discovery Protocol	35
NetBEUI	112
NetBIOS	11, 13
NetBIOS Enhanced User Interface	112
NetBIOS Frame	112
NetBIOS over TCP/IP	112
NetBIOS-Broadcast	81, 115
NetBIOS-Namen	113, 114
NetBIOS-Namenscache	113
NetBIOS-Namensserverdienst	114
NetBIOS-Ressourcen	113, 115
NetBT	112, 114, 115
Network Access Policy	154
Network Address Port Translation	71
Network Address Translation	70, 176
Network Layer	23
Network Policy Server	154
Netzadresse	38
Netzwerkadresse	41
Netzwerkklassen	42
Netzwerkkonfigurationsdienste	116
Netzwerkklast	85
Netzwerkmaske	80
Netzwerkmodelle	18
Netzwerkprotokolle	8
Netzwerkschicht	23
NFS	32
Nichtkooperative Redundanz	129
Nicht-routingfähige Protokolle	9
NIS	32
Node type	113
NPS	154
NS Records	95
O	
Open Shortest Path First	84
Open System Authentication	167
Optionen	48
Optionsnummer	125
Organisationseinheit	91
OSI-Modell	19, 20
OSI-Referenz-Modell, Funktionsprinzip	21
P	
Paketfilter	61, 173
Paketswitching	30
Pakettransport	7, 23
PAM	140
Payload	134
PDU	21
PEAP-MS-CHAP v2	168
Perimeternetzwerk	172
Physical Layer	22
Ping	49
P-Knoten	113
Pointer	95
Point-to-Point-Protocol	157
Point-to-Point-Tunnelling-Protocol	157
Ports	33
Ports, private	33
Ports, registrierte	33
Ports, Well known	33
POTS	138, 141
PPP	141, 157
PPPoA	141
PPPoE	141
PPTP	157
Präsentationsschicht	20, 24
Precedence	46
Presentation Layer	24
Primäre Server	128
Primäre Zonen	104
Priorität	46, 108, 135
Private Netze	42
Protokolle	47
Protokolle, Aufgaben	30
Protokoll-Stapel	30
Protokollversion	46
Proxy	175
Prüfsumme	66, 67
Pullpartner	115
Pushpartner	115
PVC	134
Q	
Q-DSL	139
QoS	135
Quelladresse	48
Quellport	65
R	
RARP	30, 31, 35
RAS	148
RAS-Anbindungen	148
RAS-Authentifizierung	151
RAS-Protokoll	148
Ratenadaption	140
RAW	48
Rebinding Time	120, 124, 127
Rechnernamen	10
Redirector	24
Redundante Routen	82
Redundanz von DHCP-Servern	128
Refresh	94
Relay-Agent	127, 129
Reliability	46
Remote Access Service	148
Remote-Host	41
Renewal Time	120, 124, 127
Repeating-Modus	166
Replikat	12
Replikation	94
Replikation, WINS-Datenbank	115
Reservierungsoptionen	128
Retry	94
Reverse ARP	31
Revisionsnummer	94
RFC 1340	34
RFC 1918	70
Roaming	166
Root	12, 91
Round Robin	107
Route Poisoning	86
Routenaggregation	45
Router	9, 39
Routing	23, 78
Routing Information Protocol	84
Routingfähige Protokolle	9
Routing-Protokolle	7
Routing-Schleifen	86
Rufnummernübermittlung	150
S	
SA	159
SAP	11, 21, 33, 47
Schichtengruppen	25
Schleifen	86
Schnittstelle	21
Schnittstellenliste	80
SDSL	139, 141
Second-Level-Domain	91
Security Association	159
Security Extensions, DNS	13
Security Parameters Index	159
Segmentieren	9
Sekundäre Zonen	104
Sekundärer DNS-Server	94
Sequence Number	50
Sequenznummer	61
Seriennummer	94
Server Identifier	123, 127
Serveroptionen	128
Service	95
Service Access Point	33, 47
Service-Advertisement-Protokoll	11
Serviceklassen	135
Services (Datei)	33
Session Layer	24
Session-Service	112
SHA	154
Shared Key Authentication	168
SHV	154
Sicherheit	150
Sicherheitsbedarf	15
Sicherungsschicht	23
Sitzungsschicht	20, 24

Sky-DSL	139	Time To Live	47, 95	Verzeichnisdienstpartitionen	105
SLC	140	TKIP	169	Verzögerung	46
Sliding Window Size	63	Top-Level-Domain	91	Virtual Private Network	156
Smartcards	151	Trailer	23	Virtuelle Verbindungen	149, 151
SMTP	33	Transaktions-ID	117	VPI	133
SOA	94	Transmission Control Protocol	31	VPN	149, 156
Socket	71	Transport Control Protocol	60		
Source of Authority	94	Transport Layer	23	W	
Source Port	65	Transport Relay Translation	55	Wählverbindungen	149, 150
SPI	159, 174	Transportmodus	160	WAN-Dienste	13
Split-Horizon	86	Transportprotokolle	60	WAN-Protokolle	13
Splitter	142	Transportschicht	19, 23	WDS	166
SRV	12	Trivial File Transfer Protocol	116	Wegermittlung	7
Standbyserver	128	TRT	55	Weiterleitung	95
Standleitungen	149, 150	TTL	47, 95	Well known Ports	33
Stateful Packet Inspection	174	Tunnelung	55	Wiederholungsintervall	94
Statische Adressdatenbank	12			Windows Internet Name	
Statische Datenbanken	10			Service	13, 114
Statische Einträge, WINS	115	Übermittlungsprotokolle	8, 9	WINS	13, 32, 113
Stub Border Router	74	Überschrift	74	WINS-Clients	114, 115
Stubzonen	104, 105	Übersetzung	55	WINS-Datenbank	115
Subdomain	90	Übertragungsprotokolle	8, 9	WINS-Namensdienst	114
Subnetting	43	Übertragungssicherheit	151	WINS-Proxy	115
Subnetzadresse	38, 43	UDP	31, 47, 60, 66	WINS-Server	114
Subnetzmaske	40	UDP-Header	45	WINS-Server, primärer/sekundärer	115
Supernetting	45	UDP-Header-Längeninformation	67	Wireless LAN	164
SVC	134	UDSL	139	WLAN	164
Switch	40, 134	ULP-Nummer	47	WLAN, Sicherheit	167
Symbole	5	Upper-Layer-Protokoll	47	WPA	169
SYN	61	U-R2	142	WPA2	169
Synchronisation	24, 61	URGENT-Flags	66		
Synchronisationsanforderung	61	URL-Schreibweise	54	X	
Synchronisationsbestätigung	61	User Datagram Protocol	31, 60, 66	X.500-Datenbanken	104
System Health Agent	154			xDSL	138
System Health Validator	154				
		V		Z	
		VC	133, 134	Zeiger	47
T		VDSL	141	Zieladresse	48
TCP	31, 47, 60	Verbindung	134	Zielnetzwerk	9
TCPBEUI	112	Verbindungslos	31	Zielport	65
TCP-Header	65	Verbindungsorientiert	31	Zonendatei	93
TCP-Modell	27	Verbindungssicherheit	150	Zonendelegierungen	105
TCP-Segmente	66	Verfallsdatum	94	Zoneninformation	94
T-DSL	139	Vermittlungsschicht	23	Zugriffsverfahren	135
Telefonnetz	138	Verschlüsselungstechniken	151	Zuverlässigkeit	46
TFTP	116	Versionsnummer	94		
Three-Way-Handshake	61	Verzeichnisdienst	114		
Throughput	46				

Impressum

Matchcode: NWPD

Autor: Andreas Dittfurth

Produziert im HERDT-Digitaldruck

9. Ausgabe, 1. Aktualisierung, Januar 2020

HERDT-Verlag für Bildungsmedien GmbH

Am Kümmerling 21-25

55294 Bodenheim

Internet: www.herdt.com

E-Mail: info@herdt.com

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten. Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.