C7 Protokolle der Anwendungsschicht

DNS (Domain Name System)

Für viele Anwendungen z.B. WWW wäre es unpraktisch müssten die Server über ihre IP-Adressen angesprochen werden. Stattdessen wird eine Kette von durch Punkten getrennten Namen benutzt. Der erste Name bezeichnet dabei den Host und die folgenden von unten nach oben die Domänen. Beispiel:
www.uni-koblenz.de

www ist der Host-Name des WWW Servers des RZ an der Universität Koblenz.
Uni-koblenz ist eine Subdomäne des Top-Level-Domains de.
Die Top-Level-Domains werden von der ICANN (Internet Corporation for Assigned Names and Numbers) vergeben. Diese beauftragt auch eine Institution, hier das DE-NIC, mit der Verwaltung der direkten Subdomains.
Die Top-Level-Domains sind entweder durch 2 Buchstaben bezeichnete Länder, wie

de	Deutschland
at	Österreich
nl	Niederlande
fr	Frankreich

oder noch aus dem Internet Vorgänger ARPA stammende Domains:

com	Kommerzielle Organisationen (ibm.com, sun.com)
edu	Bildungseinrichtungen (berkeley.edu)
gov	Amerikanische Regierungsstellen (nsf.gov)
mil	US Militär (army.mil)
net	Netzwerk Organisationen (nsf.net)
org	Nicht kommerzielle Organisationen
int	Internationale Organisationen (nato.int)

Für jede Domäne muss es einen DNS-Server geben. Dieser kennt die zumindest die IP-Adressen der DNS-Server aller direkten Subdomains und aller Hosts in dieser Domäne. Ferner kennt er die IP- Adresse des Domains- Servers in der übergeordneten Domäne. Um nicht für jede Auflösung verschiedene DNS Server bemühen zu müssen arbeiten diese mit einer Caching Strategie.
Beispiel: In der Domain uni-koblenz.de wird die IP- Adresse von www.sun.com gesucht.

1. Der Rechner leitet die Anfrage an den Nameserver von uni-koblenz.de
2. Der lokale Nameserver hat die Adresse nicht im Cache. Er leitet sie an den Nameserver der de- Zone.
3. Der Nameserver der de- Zone wird die Adresse des Nameservers der com- Zone in seiner Datenbank haben. Er antwortet mit einem Verweis auf den Nameserver der com- Zone.
4. Der Nameserver der com- Zone antwortet mit einem Verweis auf den Nameserver von sun.com
5. Der Nameserver von sun.com liefert die IP- Adresse von www.sun.com

Telnet

Telnet setzt auf TCP auf und erlaubt das Einloggen und die interaktive Arbeiten auf einem entfernten über TCP/IP erreichbaren Zielsystem. Initiator ist der Telnet-Client, der die Verbindung zu einem Telnet-Server aufnimmt. Der Telnet-Server wird unter dem TCP-Port 25 erreicht. Telnet fußt auf dem Konzept eines Network Virtual Terminal (NVT), des Funktionsumfang und Arbeitsweise von einem früher verbreiteten Terminal DEC VT52 abgeleitet ist. Das Telnet Protokoll arbeitet halbduplex. Der Client gibt Kommandos auf die

der Server mit einer Änderung des Bildschirminhalts reagiert. Das ASCII Zeichen FFh dient zur Umschaltung zwischen den Daten und den Kommandos (IAC). Das darauf folgende Zeichen bestimmt das Kommando. Zu Beginn der Sitzung werden die Parameter ausgehandelt.
Beispiel:

Server	Client	Ablauf
<IAC,DO,24>	<IAC,WILL,24>	Server möchte Bildschirmtyp und Client gibt Zustimmung
<IAC,SB,1,IAC,SE>	<IAC,SB,24,0, “IBM3278“,IAC,SE	Server fragt mit Untermodus 1 nach dem Terminaltyp. Client antwortet mit "IBM3278"
<IAC,DO,0>	<IAC,WILL,0>	Binär Modus

Wichtigste Kommandos:

Name	ASCII Code	Beschreibung
EOF	236	Dateiende
EOR	239	Zeilenende
AO	245	Unterbreche Ausgabe
EC	247	Lösche Zeichen
EL	248	Lösche Zeile
SB	250	Start Parameterverhandlung
DO	253	Wunsch Optionen
WILL	251	Akzeptierung Optionen

Die Dateneingabe wird jeweils durch CRLF beendet. Ähnlich wird auch bei den Protokollen FTP und SMTP vorgegangen.

FTP

Das File Transfer Protokoll (FTP) dient zur Übertragung von Dateien zwischen einem FTP-Server und einem FTP-Client. Das FTP Modell definiert eine symmetrische Client/Server Kommunikation. FTP benutzt für die Kommandos (Port 21) und die Daten (Port 20) getrennte TCP-Verbindungen. Die FTP-Kommandos werden durch einen dreistelligen Statuscode quittiert. Die FTP-Server arbeiten mit einem Inactivity Time-Out Limit, das nach 15 Minuten ohne Kommando die FTP Verbindung beendet.

FTP stellt folgende Dienste zur Verfügung:

- Übertragen von Dateien zwischen Client und Servern
- Erzeugen von Dateien und Verzeichnissen
- Löschen von Dateien und Verzeichnissen
- Wechseln des aktuellen Verzeichnis
- Anhängen von Daten an existierende Dateien

Die Übertragung kann als ASCII Text oder im Binäermodus erfolgen.
Die Übertragung der Kommandos erfolgt durch Kommandozeilen. Die meisten Clients haben jedoch graphisches Benutzer Frontend, das die Kommandos und Daten erzeugt. FTP setzt i.A. voraus, das der Anwender auf dem Zielrechner einen Benutzer Account besitzt. Eine Ausnahme bildet der **Anonymnous FTP.** Der Benutzer meldet sich unter seiner e-mail Adresse an. Er kann das Dateien von einem FTP-Archiv runterladen (download) und evtl. auch Dateien zum FTP-Archiv übertragen (upload). Der Server regelt dabei in welche Verzeichnisse und in welchem Umfang Dateien zum Server übertragen werden dürfen.

Beispiel einer FTP Sitzung:

Client	Server	Datenübertragung
FTP	220 Service ready	
USER Mueller	331 User name ok	
PASS xxxx	230 User logged in	
ASCII		
GET f1.txt myf1.txt	150 File Status ok	Transfer der Datei
	226 File Transfer ok	
BYE		

Die Datenverbindungen werden nach der Übertragung jeweils beendet. Die Kommandoverbindung bleibt permanent bis zum BYE. Der Anwender muss die Struktur der Daten kennen um den geeigneten Modus (ASCII,BINARY) auszuwählen.

SMTP

Das Simple Mail Transport Protocol SMTP dient zum Austausch von e-mail mittels TCP Verbindungen. SMTP regelt die Kommunikation zwischen den Mail Transport Agent (MTA) den SMTP-Servern. Eingehende Mail legt der SMTP-Server lokal in einem Message Store (MS) ab. Das Abholen und Weiterverarbeiten ist Sache eines User Agents (UA), z.B. Outlook. Dieser kann sich auch auf einem anderen Rechner befinden. Die Kommunikation zwischen dem Mail-Server und dem User Agent erfolgt über die Protokolle POP (Post Office Protocol) , IMAP (Internet Message Access Protocol) oder es wird ein Web-Interface zum Zugriff auf den Mail Speicher bereitgestellt. Erhält ein MTA Mail von einem anderen MTA, die aber nicht an eine von ihm bediente e-mail Adresse gerichtet ist, sondern an einen anderen MTA weiter zu leiten ist, spricht man von einem Mail-Relay. Von den meisten Mailservern wird aber heute ein Relay abgelehnt, da hierdurch oft SPAM-Mail verbreitet wird.
Das SMTP Protokoll ist angelehnt an das TELNET Protokoll.

Client SMTP mailhost.uni-koblenz.de	Server SMTP mailer.msn.com
TCP SEGMENT Port 25	->
	220 QMAIL ESMTP Service ready
EHLO mailhost.uni-koblenz.de	
	250 mailer.msn.com 250 PIPELINEING 250 8BITMIME
MAIL from: <ros@uni-koblenz.de>	
	250 ok
RCPT to: <xyz@msn.com>	
	250 ok
DATA	
	354 Start Mail Input; end with "."
Date 11.Juni 03 From: ros@uni-koblenz.de <CRLF> To: xyz@msn.com <CRLF> Subject: Wie gehts <CRLF> Wie geht es Dir <CRLF> <CRLF>.<CRLF>	
	250 ok 958562713 qp 137
QUIT	
	221 mailer.msn.com closing connection

Die wichtigsten SMTP Kommandos:

HELO	Vorstellen des Clients beim Server
EHLO	Vorstellen bei V2
MAIL	Angabe des Absenders
RCPT	Angabe des Empfängers
DATA	Text der Nachricht folgt als ASCII
QUIT	Beenden des Dialogs

Zur Bestätigung der Kommandos benutzt SMTP wie FTP dreiziffrige Returncodes. Die Mailadresse muss den Hostnamen des Mailservers in der Domäne nicht enthalten, es genügt die Angabe der Domäne, z.B. ros@uni-koblenz.de. Der Sender stellt mit Hilfe eines DNS-Look Up fest, ob die Domäne einen Mail-Exchange(MX) Eintrag enthält. Dieser Eintrag liefert Name und IP-Adresse des Mailservers der Domäne. Auf diese Weise ist auch eine Domänen-basierte Zustellung möglich.

Um mehr als nur reine ASCII Text zu übermitteln, wurden die Multipurpose Internet Mail Extension (MIME) definiert. Sie definieren ein System von Typen und Subtypen.
Neben dem jeweiligen Typ identifiziert MIME die Teile der mail über eine Content-ID und separiert sie im Falle eines Multipart-Typs durch eine Boundery-Signatur. Für jeden Typ kann hierbei sowohl der verwendete Zeichensatz (7 Bit, 8 Bit, Binär, Base64 usw.) spezifiziert werden, so dass der Empfänger die Mail korrekt interpretieren kann. Diese MIME-Information wird im Mail-Header hinterlegt.

E-mails sind heute der meistbenutzte Weg zur Verbreitung von Viren und Würmern. Es ist daher wichtig das der User-Agent, d.h. das eigentliche Mail-Programm des Benutzers wie Netscape oder Outlook nicht beim Öffnen einer Mail bereits Attachments ausführt. Gefährlich sind alle Attachments, die ausführbaren Programmcode enthalten, dies sind u.a. EXE-Dateien (Programme), DLLs (Bibliotheken) aber auch Word-Dateien mit ausführbaren Makros. Die besondere Gefahr der Würmer besteht darin, dass sie selbst wieder neue Mails erzeugen. Die Adressen entnehmen sie dem eigenen Outlook Adressbuch, als Absender geben sie den befallenen Rechner an. Der Empfänger erhält so eine Mail von einem vertrauenswürdigen Absender, die aber von dem Wurm erzeugt ist und wieder Schadprogramme enthält.

Ein weiteres Problem stellen die unerwünschten Massen E-Mails (SPAM) da. Hier wird ausgenutzt, dass das Versenden einer e-mail für den Absender kostenlos bzw. sehr billig ist. Findet der Versender einen Mail-Server der als Relay arbeitet, kann er beliebig Mail verschicken. Da man die Absenderangaben fälschen kann, ist die Quelle der SPAM-Mails nicht zu ermitteln. Die einzige Möglichkeit ist, die eingehende Mail zu filtern nach entsprechenden verdächtigen Schlüsselworten und sie in einem speziellen SPAM-Folder abzulegen. Ferner kann man Mails von Mailservern, die oft SPAM verschicken, generell ausfiltern.

NNTP

Das Network News Transfer Protocol NNTP dient zur Übertragung der Usenet-News. Eine Usenet Nachricht ist wie eine e-mail Nachricht aufgebaut. Adressat ist aber nicht ein spezieller Benutzer sondern eine Newsgroup. Die Usenet Newsgroups sind hierachisch aufgebaut und enthalten alle möglichen Gebiete. In einer Domäne z.B. uni-koblenz.de können aber auch eigene Newsgruppen eingerichtet werden, z.B. infko.general, infko.inf etc.

IRC

Der Internet Relay Chat (IRC) erlaubt den Austausch schriftlicher Nachrichten in Echtzeit. Zwei oder mehr Personen können sich bei einem IRC- Server anmelden und eine Gruppe

bilden. Die IRC-Clients auf den Benutzerrechnern senden Nachrichten an den IRC-Server, der sie dann an alle Mitglieder der Gruppe verteilt.

NTP, SNTP

Das (Simple) Network Time Protocol ((S)NTP) ist ein Protokoll zur Synchronisation mehrere Uhren. NTP verwendet eine Hierarchie von Zeitgebern. Die primären Zeitgeber sind direkt mit Atomuhren synchronisiert, sekundäre Zeitgeber sind mit primären Zeitgebern synchronisiert. NTP erreicht eine Genauigkeit im Millisekundenbereich.