TCP / IP & Co. . . .

... wo bitte geht's hier zum Internet?

Hubert Pitner

Diese Zusammenstellung will einige Fragen zum Thema “Netzwerktechnik” beantworten, die das “Cisco Netzwerk Seminar" offen gelassen hat, die aber zum Verständnis der Zusammenhänge, wie Daten über das "Internet" transportiert werden, unbedingt erforderlich sind.

1.1 Es geht auch einfacher

das vereinfachte vierschichtige OSI (*Open System Interconnection*) Modell für TCP/IP Netzwerke:

Applikationsschicht (*Application*)	E-Mail, FTP, Telnet, HTTP
Transportschicht (*Transport*)	TCP (*Transmission Control Protocol*) UDP (*User Datagram Protocol*)
Netzwerkschicht (*Network*)	IP (*Internet Protocol*) als Teil von TCP/IP
Physikalische Schicht (*Physical*)	Ethernet, Token Ring, FDDI (*Fiber Distributed Data Interface*)

1.2.1 Noch mehr Netzwerkprotokolle

Ein Netzwerkprotokoll definiert genau, wie Sender und Empfänger einer bestimmten Schicht des OSI-Modells miteinander Daten austauschen.

Oft verwendete Anwendungsprogramme als Teil der TCP/IP Protokollgruppe sind:

- FTP (*File Transfer Protocol*),
- SMTP (*Simple Mail Transfer Protocol*),
- DNS (*Domain Name Service*),
- Telnet
- HTTP (*Hypertext Transfer Protocol*),
- SNMP (*Simple Network Management Protocol*) u.a.m.

1.2.2 Es geht auch anders

Neben der TCP/IP-Protokollgruppe sind, vor allen in lokalen Netzwerken (auf Englisch: *Local Area Network* = “LAN”), auch andere Protokolle weit verbreitet:

- IPX/SPX (*Internet Packet Exchange / Sequenced Packet Exchange*), wird von Novell Netware verwendet.
- NetBIOS und NetBEUI (*Network BIOS Extended User Interface*), sind Protokolle, welche insbesondere von Microsoft Betriebssystemen verwendet werden.

2. Alles ist offen, TCP/IP im Internet

TCP/IP ist ein “offenes Protokoll”; das bedeutet, dass alle technischen Spezifikationen in öffentlich zugänglichen Dokumenten beschrieben sind. Jedermann kann somit TCP/IP auf jeder geeigneten Hardwareplattform implementieren.

2.1 Bitte kommentier' mich - die RFC's

Alle Details von TCP/IP sind in den RFC Dokumenten beschrieben (“RFC” heißt "*Request for Comment*", was soviel wie "Bitte kommentier mich" bedeutet). Alle RFC's stehen im Internet zur freien Einsichtnahme zur Verfügung. Derzeit existieren rund 2300 solcher RFC. z.B. die RFC 768 "*UDP - User Datagram Protocol*" oder RFC 793 "*TCP - Transmission Control Protocol*", um nur zwei zu nennen.

2.2 Hausnummern im Internet - die IP - Adressen

Für den Betrieb eines TCP/IP-Netzwerkes benötigt jeder angeschlossene Computer eine eigene IP-Adresse. Jede IP-Adresse besteht dabei aus einer Netzwerk- und einer Hostadresse; die Netzwerkadresse gibt an, in welchem Netzwerk (z.B. in welchem LAN) sich ein Computer befindet, die Host-Adresse identifiziert den Computer innerhalb dieses Netzwerkes. Eine IP-Adresse ist immer ein 4 Byte großer Wert. Als Konvention wird jedes Byte als dezimaler Wert angeschrieben, die einzelnen Bytes werden dabei durch Punkte getrennt, auf Englisch bezeichnet man das als “*Dotted Decimal Notation*”. Eine gültige IP-Adresse wäre z.B. die "`140.90.23.100`".

2.2.1 Ganz Große und ganz Kleine - die Adressklassen

Die Bits einer IP-Adresse werden zusammen als `<Netzwerk Adresse, Host Adresse>` interpretiert. Je nach vorgesehenem Einsatzbereich werden Netzwerke den Klassen A, B oder C zugeordnet.

2.2.2 Spezielle IP Adressen

- enthält der Netzwerkteil ausschließlich Nullen, so ist das lokale Netzwerk gemeint. Die Adresse `0.0.0.200` bezeichnet so z.B. den Host 200 in einem lokalen Klasse-C-Netzwerk.
- die Klasse-A-Adresse `127.xxx.xxx.xxx` wird für das “Loopback” verwendet, das ist die Kommunikation mit demselben Host, und dient zu Testzwecken; meist wird die `127.0.0.1` als Loopback-Adresse verwendet.
- sind im Adressteil sämtliche Bits auf “Eins” gesetzt, so wird damit ein Rundruf (*Broadcast*) signalisiert. Die Adresse `128.18.255.255` spricht z.B. alle Hosts in einem Klasse-C-Netz an.

2.2.3 Wer will mich ? Die Vergabe von IP Adressen

Will man sein Netzwerk permanent an das Internet anbinden, z.B. wenn man seinen eigenen Server betreiben möchte, so benötigt man dafür eine eigene “stati-

Klasse A: von 1.xxx.xxx.xxx bis 126.xxx.xxx.xxx

0	. . . . .	. . . . .	. . . . .
7-Bit Netzwerkadresse, erlaubt: 1..126; reserviert: 0 und 127	3-Byte Host Adresse (16.77.214 Hosts pro Netzwerk)		

Klasse B: von 128.xxx.xxx.xxx bis 191.xxx.xxx.xxx

1 0	. . . . .	. . . . .	. . . . .
14-Bit Netzwerkadresse (16.384 Netzwerke) Erstes Byte von 128 bis 191		2-Byte Host Adresse (65.534 Hosts pro Netzwerk, alle Nullen und Einsen sind reserviert)	

Klasse C: von 192.xxx.xxx.xxx bis 223.xxx.xxx.xxx

1 1 0	. . . . .	. . . . .	. . . . .
21-Bit Netzwerkadresse (2.097.152 Netzwerke) Erstes Byte von 192 bis 223			1-Byte Host Adresse (254 Hosts pro Netzwerk, 0 und 255 sind reserviert)

sche" IP-Adresse; diese wird vom "InterNIC", dem "*Internet Network Information Center*", verwaltet - dort kann man auch seinen eigenen speziellen Domänennamen beantragen (wie z.B. "**meine_firma.at**") .. das alles wird jedoch üblicher Weise von unserem Provider für uns erledigt.

Will man nur temporär auf das Internet zugreifen, z.B. um im Internet zu "surfen", so erhält man für die jeweilige Sitzung eine dynamische IP-Adresse zugewiesen ... doch davon später bei PPP.

2.2.4 My home is my castle private Netzwerke

... damit sind Netzwerke gemeint, die nicht direkt mit dem Internet verbunden werden sollen; folgende IP-Adressen sind dafür reserviert (IP-Adressen aus diesem Bereich können beliebig, ohne das InterNIC einzuschalten, verwendet werden):

10.0.0.0 bis 10.255.255.255
172.16.0.0 bis 172.16.255.255
192.168.0.0 bis 192.168.255.255

2.2.5 Netzwerkmasken

Die Netzwerkmaske ist eine IP-Adresse, in der alle Bits, von denen die Netzwerkadresse festgelegt wird, den Wert "1" haben, die übrigen Bits sind "0". Die Netzwerkmaske für ein Klasse-C-Netz lautet z.B. **255.255.255.0**; für ein Klasse-B-Netz **255.255.0.0** und für ein Klasse-A-Netz **255.0.0.0**.

2.2.6 Netzwerkadressen

Die Netzwerkadresse ergibt sich aus einer logischen "UND" Verknüpfung der IP-Adresse mit der Netzwerkmaske. Beispiel: ein Computer hat die IP-Adresse **206.197.168.200**, die Netzwerkmaske ist **255.255.255.0** somit ist die Netzwerkadresse **206.197.168.0**.

2.2.7 Subnetze

An eine Klasse-B-Adresse können maximal 65.534 Hosts angeschlossen werden. Oft ist es sinnvoll, dieses Netz in Subnetze zu unterteilen. Beispiel: für jede Filiale eines großen Unternehmens wird ein eigenes Subnetz angelegt. Dazu können einige Bits aus der Host-IP-Adresse innerhalb der IP-Adresse abgetrennt und zur Netzwerkadresse hinzugefügt werden; das bezeichnet man als "Definieren einer Subnetzmaske". Im Prinzip wird damit die Netzmaske um einige Bits erweitert. So ist die Netzmaske eines normalen Klasse B Netzes **255.255.0.0**. Möchte man dieses Netz in 128 Subnetze mit jeweils 512 Hosts unterteilen solautet die neue Netzmaske **255.255.254.0**.

2.3 Quer über fünf Kontinente TCP/IP Routing

Als Routing bezeichnet man das Weiterleiten von Informationen von einem Netzwerk zum anderen. Dazu geeignete Geräte bezeichnet man als Router. Ein

Router benötigt zumindest 2 physikalische Netzwerkschnittstellen und zwei logische Netzwerkadressen - jede der beiden Netzwerkkarten hat somit ihre eigene, dem jeweiligen Netz zugeordnete IP-Adresse. Router können entsprechend ausgerüstete PCs oder spezielle Router (Cisco, 3Com ...) sein.

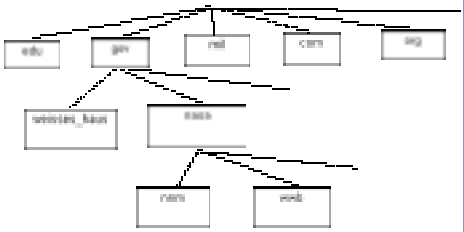
Für Router wird oft auch der Begriff "*Gateway*" verwendet. Beispielsweise besteht das Internet aus einer sehr großen Anzahl solcher Gateways, die auf die unterschiedlichsten Arten miteinander verbunden sind. Die Art und Weise wie ein Gateway ein anderes Gateway oder einen anderen Rechner erreicht, wird in so genannten Routing-Tabellen beschrieben; diese Routing-Tabellen legt jeder Router in seinem Speicher für sich an und aktualisiert sie zyklisch. Treffen bei einem Router Datenpakete ein, deren IP ihm nicht bekannt ist, so werden diese einfach an den Ausgang weitergereicht. Die Pakete werden so lange von einem Router zum nächsten gereicht, bis sie ihr Ziel erreicht haben, oder als unzustellbar wieder zurückkommen, wodurch jedoch eine Fehlermeldung erzeugt wird.

Die einzelnen Router tauschen ihre Routingtabellen untereinander aus; damit weiß jeder Router welche Netzwerke sich in seiner Umgebung befinden. Der Austausch dieser Information erfolgt mit dem RIP, dem "*Routing Information Protocol*". TCP/IP bezeichnet jeden Durchgang durch einen Router als einen "*Hop*" (=Sprung). RIP begrenzt die maximal mögliche Anzahl von Hops auf 15; erreicht ein Paket sein Ziel nicht nach längstens 15 Hops, so gilt das Paket als unzustellbar und wird retourniert. Mit dem DOS Befehl "**TRACERT**" kann man den Weg verfolgen, den die Pakete durch das Internet bis zum Zielrechner genommen haben.

Innerhalb eines lokalen Netzwerkes wird kein Router benötigt, allerdings nur sofern keine Subnetzmaske verwendet wird.

2.4 Domänennamen

Zu Beginn der Netzwerktechnik waren die Namen und IP-Adressen aller Hosts des Internet in der Datei "**HOSTS.TXT**" zentral beim NIC gespeichert, wobei die Router in der Startphase diese Datei jedesmal neu laden mussten. Mit zunehmender Zahl an Hosts stellte sich dieses Verfahren als nicht zielführend heraus. Es wurde daraufhin das heute verwendete Verfahren der Domänennamen entwickelt, welches als DNS "*Domain Name System*" bekannt ist.



Hierarchie der Domänennamen

DNS ist ein hierarchisches System, vergleichbar mit einer Postanschrift die aus Namen, Straße, Stadt und Land besteht. DNS teilt das Internet in verschiedene Domänen ein, z.B. **gov** (Goverment .. Verwaltung), **edu** (Education), **ac** (Academic), **com** (Comercial), **mil** (Military) .. und die Domänen für verschiedene Länder z.B. **at** (Austria), **de** (Deutschland) u.a.m. Jede Domäne wird wieder in Subdomänen unterteilt. Innerhalb einer Subdomäne erhält wieder jeder Host einen eigenen symbolischen Namen. Die einzelnen Elemente eines Domänennamens werden durch Punkte getrennt. Ein eindeutiger Domänenname wird als FQDN (*Fully Qualified Domain Name*) bezeichnet. Bei den Domänennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

z.B. hat eine kommerzielle Firma die Adresse "**metrolink.com**"; die Verkaufsabteilung erreicht man nun unter **sales@metrolink.com** (der "@" bedeutet "at" d.h. "bei"). Achtung: beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden !

2.4.1 Name Server

TCP/IP ermittelt die IP-Adresse zu einem Host-Namen, indem Nameserver befragt werden. In jedem Netzwerk muss die IP-Adresse eines Nameservers bekannt sein.

3. TCP/IP Dienste - Client / Server Architektur

Üblicher Weise werden Internet-Dienste in zwei Teilen implementiert: ein "Server" liefert Informationen, welche von beliebig vielen "Clients" abgerufen werden können.

3.1 TCP / IP und Sockets

TCP/IP ist eine standardisierte Methode, mit der Clients und Server miteinander kommunizieren können. Als Schnittstelle

wurden bereits 1982 im Berkeley-UNIX die "*Sockets*" (engl. "Steckdosen") definiert.

3.1.1 Definition von Sockets

Ein Socket repräsentiert den bidirektionalen Endpunkt einer Verbindung; über einen Socket können Daten gesendet und empfangen werden.

3.1.2 Ein Socket hat drei Attribute

- die IP-Adresse des Systems, sie identifiziert den Netzwerkknoten.
- die Port-Nummer des Prozesses (= des Programmes), der Daten durch den Socket austauscht,
- den Typ des Sockets (z.B. Stream oder Datagramm). Der Typ legt das Protokoll für den Datenaustausch fest (verbindungsorientiertes oder verbindungsloses Protokoll).

3.1.3 Verbindungsorientiertes Protokoll

Ein verbindungsorientiertes Protokoll ist mit einem Telefongespräch vergleichbar. Zuerst wird eine Punkt-Zu-Punkt-Verbindung aufgebaut, über die dann Daten übertragen werden. Das Protokoll für einen zuverlässigen bidirektionalen Datenaustausch ist TCP.

Für die Übertragung der Pakete ist das IP (=*Internet Protocol*) zuständig. IP garantiert jedoch nicht, dass die Pakete a) beim Empfänger abgeliefert werden bzw. b) dass die Pakete in der richtigen Reihenfolge beim Empfänger ankommen. Für Fehlerprüfung und Sicherstellung der richtigen Reihenfolge ist TCP zuständig.

3.1.4 Verbindungsloses Protokoll

Ein verbindungsloser Datenaustausch ist mit einem Rundruf vergleichbar; es wird dabei keine Punkt-Zu-Punkt-Verbindung aufgebaut. Ein Protokoll für verbindungslosen Datentransfer ist UDP (=*User Datagram Protocol*). UDP garantiert nicht, dass Datagramme ihren Empfänger erreichen; mit UDP werden daher meist nur kleine Datenmengen übertragen. Beispiel: SNMP (=*Simple Network Management Protocol)*.

Im Sockets Modell wird ein Socket der UDP verwendet als "Datagram Socket" bezeichnet.

3.1.5 Sockets und das Client / Server Modell

Es werden immer zwei Sockets benötigt, um einen Kommunikationspfad aufzubauen. Die Serveranwendung überwacht einen bestimmten Port auf ihrem System; der Server wird identifiziert durch die IP-Adresse des Systems auf dem er läuft und die Portnummer an der er auf eine Verbindung wartet. Der Client startet die Verbindung von einem beliebigen verfügbaren Port aus und versucht eine Verbindung zum Server herzustellen. Nach dem Verbindungsaufbau erfolgt der Datenaustausch zwischen Client und Server entsprechend ihren Protokollen. Die Sequenz der Ereignisse beim Socket basierten Datenaustausch hängt davon ab ob die Übertragung verbindungsorientiert (TCP) oder verbindungslos (UDP) ist.

Beim verbindungsorientierten Datenaustausch horcht der Server an einem bestimmten Port und wartet darauf, dass ein Client eine Verbindung anfordert; der Datenaustausch beginnt erst, nachdem die Verbindung aufgebaut ist. Beim verbindungslosen Datenaustausch wartet der Server darauf, dass an einem bestimmten Port ein Datagramm eintrifft; der Client sendet sofort ein Datagramm an den Server.

3.2 Client / Server Kommunikation via TCP / IP

Client/ Server Anwendungen führen die folgenden Schritte durch, um in einem TCP Netzwerk Daten auszutauschen:

- die Anwendung legt einen Socket an.
- sie verknüpft die IP Adresse mit diesem Socket.
- falls sie Anwendung ein Server an einem "Stream Socket" ist, wartet sie auf eine Verbindung.
- ist die Anwendung ein Client an einem Stream Socket, so baut sie eine Verbindung auf.
- die Anwendung tauscht Daten mit der Gegenseite aus.
- nach Abschluss des Datenaustauschs wird der Socket geschlossen.

Bei verbindungslosen Sockets (Datenübertragung via UDP) entfallen die Schritte 3) und 4)

Sowohl Server- als auch Clientanwendungen legen zuerst einen Socket an. Anschließend verknüpfen "binden" sie den Socket mit der IP Adresse des lokalen Computers und einer Portnummer. Die IP-Adresse identifiziert den Computer, die Portnummer identifiziert die Anwendung, die den Socket benutzt.

Normaler Weise warten Server an genau definierten Port-Nummern darauf, dass ein Client mit ihnen in Verbindung treten möchte. Bei einer Client-Anwendung wird ein Socket wie beim Server mit einer IP- und einer Port-Nummer verknüpft; der Client kann jedoch auch die Port-Nummer "0" angeben, vom Server wird dann automatisch ein freier Socket gewählt.

Beim Client/Server Modell muss zuerst der Server laufen, bevor ein Client seinen Dienst anfordern kann. Nachdem die Serveranwendung einen Socket angelegt und mit einem Port verknüpft hat, richtet sie eine Warteschlange mit Verbindungen ein. Die Warteschlange legt fest, wie viele Clients gleichzeitig mit dem Server eine Verbindung aufnehmen können. Nach dem Einrichten der Warteschlange wartet der Server darauf, dass ein Client eine Verbindung aufbaut.

Die Client-Anwendung legt einen Socket an und verknüpft ihn mit einer Netzwerk-Adresse; dann baut sie eine Verbindung zum Server auf, wozu die IP-Adresse oder der Name des Servers und die Port-Nummer bekannt sein müssen.

3.3 die wichtigsten Internet Dienste und ihre Port Nummern

- FTP (*File Transfer Prot.*) Port 20: Daten, Port 21: Steuerinformationen.
- HTTP (*Hypertext Transfer Prot.*): Port 80.
- SMTP (*Simple Mail Transfer Prot.*): für E-Mails, Port 25.
- NNTP (*Network News Transfer Prot.*): Newsgroup Beiträge, Port 119.
- Telnet: zum Anmelden auf entfernten Systemen, Port 23
- SNMP (*Simple Network Management Prot.*): Verwaltung von Netzwerkgeräten, Port 161 und 162.
- TFTP (*Trivial File Transfer Prot.*) laden von Boot Dateien.
- NFS (*Network File System*): gemeinsame Nutzung von Dateien, Port 111.
- WAIS (*Wide Area Information Service*) sucht Daten auf verteilten Systemen, Port 210.

3.4 der Super Server "inetd"

Das CS (=Client/Server) Modell setzt voraus, dass ein Server betriebsbereit ist, bevor ein Client seinen Dienst anfordert. Auf einem Server alle Dienste gleichzeitig laufen zu lassen ist jedoch aufgrund der verfügbaren Systemresourcen nicht sinnvoll. UNIX löst das Problem durch Starten des Superservers "Inetd", welcher ständig alle Ports überwacht und bei Bedarf den entsprechenden Dienst startet.

3.5 Stand alone Server

Werden Dienste sehr oft angefordert, so ist "inetd" oft zu langsam. Als Abhilfe laufen solche *Stand Alone Server* permanent und überwachen kontinuierlich einen Port. Unter UNIX heißen solche Programme "Dämonen" unter DOS werden sie als TSR (*terminate and stay resident*) bezeichnet, unter Windows NT als Services.

Der Artikel wird in einer der nächsten Ausgaben mit Informationen zu PPP, dem "*Point to Point Protocol*" und dem "virtuellen privaten Netzwerk" mittels *Tunneling Protocol* fortgesetzt.