

Grundlagen

Das TCP/IP-Protokoll ist das wohl verbreitetste Netzwerkprotokoll und wird von allen modernen Betriebssystemen unterstützt. Merkmale von TCP/IP sind:

- offener Protokollstandard, frei verfügbar und unabhängig von einer bestimmten Hardware oder Betriebssystem;
- von der physikalischen Netzwerk-Hardware unabhängig, so daß über TCP/IP unterschiedlichen physikalische Netzwerke (z.B. Ethernet, Token Ring, Wählleitungen, Funk . . .) kommunizieren können;
- zwischen verschiedenen logischen Netzwerken können Pakete geroutet werden;
- einheitliches Adressierungsschema, jedes TCP/IP-Gerät ist im gesamten Netzwerk eindeutig adressierbar;
- weitere Dienst-Protokolle können auf TCP/IP aufsetzen

Die IP-Adresse hat bei der aktuellen IP-Version (IPv4) eine Länge von 32-Bit und setzt sich aus dem Netz- und dem Hostanteil zusammen. Zuerst wurden die IP-Adressen in Klassen aufgeteilt, wobei es immer einen festen Netz- und Hostanteil gab (8 zu 24 (Class-A), 16 zu 16 (Class-B), 24 zu 8 (Class-C)). Nur feineren Granulierung (ein Class-C-Netz war zu klein, ein Class-B aber zu groß), der Verknappung gerade an Class-B-Netzen und Minimierung der Routing-Einträge wurde TCP/IP um das Sub- und Supernetting erweitert (klassenfreie IP-Adressen). Hierbei werden größere Netze in mehrere kleine unterteilt oder mehrere (zusammenhängende) kleine zu einem größeren zusammengeführt. Die Definition, wie eine IP-Adresse in Netz- und Hostanteil aufzuteilen ist, wird über die Netzmaske eingestellt.

natürliche Netzklassen

Class-A

Adressen: 0.0.0.0 - 127.255.255.255

Netzmaske: 255.0.0.0

Class-B

Adressen: 128.0.0.0 - 191.255.255.255

Netzmaske: 255.255.0.0

Class-C

Adressen: 192.0.0.0 - 223.255.255.255

Netzmaske: 255.255.255.0

private Netze

Normalerweise muß eine IP-Adresse weltweit eindeutig sein. Netzwerkadressen werden deshalb zentral vergeben (bzw. die Vergabe von bestimmten Netzbereichen an andere Stellen delegiert). In jedem der drei Netzklassen ist ein Bereich definiert, die jeder frei verwenden kann, die sogenannten privaten Netze. Die privaten Netze dürfen nicht im Internet geroutet werden.

Folgende Netze sind für den privaten Bereich bestimmt:

- Class-A-Netz 10.0.0.0
- Class-B-Netze 172.16.0.0 bis 172.31.0.0
- Class-C-Netze 192.168.0.0 bis 192.168.255.0

Reservierte IP-Adressen

Einige IP-Adressen haben bestimmte Aufgaben:

- 127.0.0.0 ist das Localnet, ein Netz was nur im lokalen Rechner existiert
- 127.0.0.1 ist der Localhost, die IP-Adresse des Rechners im Localnet
- 0.0.0.0 ist die Netzadresse für alle Rechner, die irgendwo existieren
- die erste Adresse in einem Netz ist die Netzadresse
- die letzte Adresse in einem Netz ist die Broadcast-Adresse

Netzmasken

Die Netzmaske, zur Festlegung des Netz- und Hostanteils einer IP-Adresse, ist bei IPv4 ebenfalls 32-Bit lang. Jedes Bit der Netzmaske, das den Wert 1 hat, legt bei der IP-Adresse fest, daß das entsprechende Bit zum Netzanteil gehört, ist das Netzmaskenbit 0, dann gehört das IP-Adressen Bit zum Hostanteil. Zur Vereinfachung der Schreibweise wird die Netzmaske häufig nicht in der Dezimalschreibweise, sondern einfach durch die Anzahl der Netzbits angegeben. Z.B. bezeichnen 192.168.1.0/255.255.255.0 und 192.168.1.0/24 jeweils ein natürliches Class-C-Netz. Folgende Tabelle gibt die Aufteilung eines Class-C-Netzes und die dadurch entstehenden Änderungen der Netzanzahl und verfügbaren Adressen je Netz wieder:

Netze	Adressen	Netzmaske
1	256	255.255.255.0 (24)
2	128	255.255.255.128 (25)
4	64	255.255.255.192 (26)
8	32	255.255.255.224 (27)
16	16	255.255.255.240 (28)
32	8	255.255.255.248 (29)
64	4	255.255.255.252 (30)
128	2	255.255.255.254 (31)

TCP, UDP und ICMP

Zwar wird häufig von TCP/IP gesprochen, jedoch gibt es neben dem TCP-Protokoll noch das UDP- und ICMP-Protokoll, die auf IP aufsetzen. Die Merkmale dieser drei Protokolle TCP, UDP und ICMP sind:

- TCP (Transmission Control Protocol) ist ein verbindungsorientiertes Protokoll; das bedeutet, vor jedem neuen Kommunikationswunsch wird eine Verbindung über ein Drei-Wege-Verfahren hergestellt und somit sichergestellt, daß der Zielhost erreichbar und bereit ist, die Kommunikation durchzuführen. Der Empfang eines Datenpaketes wird vom Zielhost bestätigt, auch die Korrektheit eines Datenpaketes kann über Checksummen überprüft werden.
- UDP (User Datagram Protocol) ist dahingegen ein verbindungsloses Protokoll; der Sender schickt eine Nachricht an den Zielhost ohne vorher zu prüfen, ob der Zielhost erreichbar ist. Es sieht also keine Techniken vor, mit denen geprüft werden kann, ob das Paket wirklich sein Ziel erreicht hat. Hierdurch ist das Protokoll natürlich schlanker und schneller als TCP, aber unsicherer.
- ICMP (Internet Control Message Protocol) versendet Nachrichten, die Kontroll-, Fehlermeldungs- und Informationsfunktionen beinhalten. Die bekannteste Anwendung ist wohl der Ping-Befehl, der ICMP-Echo-Meldungen sendet, um zu überprüfen, ob ein System aktiv und das IP-Protokoll funktionsfähig ist und das System (routingtechnisch) erreichbar ist.

Ports und Sockets

Über die IP-Adresse kann nur ein bestimmter Rechner (oder Netz) angesprochen werden. Einen bestimmten Dienst auf einem Rechner wird über die

Portnummer angesprochen. Für wichtige Standarddienst sind bestimmte Portnummern reserviert, aber es steht jedem frei, einen entsprechenden Dienst auch auf einem anderen Port bereitzustellen (mit der Gefahr, das andere Rechner den entsprechenden Dienst nicht auf diesem Port erwarten und somit keine Kommunikation stattfinden kann).

Würde nur eine Verbindung Client-IP -> Server-IP:Server-Port stattfinden, bestände das Problem, daß der Server bei mehreren gleichzeitig geöffneten Verbindungen von einem Client auf den gleichen Dienst die Verbindungen nicht auseinanderhalten könnte. Um diesem Problem zu umgehen, öffnet der Client auch einen derzeit unbenutzten Port und teilt dem Server mit, daß er die Verbindung auf diesem Port etablieren möchte. Eine Verbindung zwischen Client und Server ist immer durch Client-IP:Client-Port -> Server-IP:Server-Port definiert, dem sogenannten Socket. Hierdurch kann der Server die einzelnen Pakete den jeweiligen Verbindungen zuordnen, da die Portnummern im TCP- und UDP-Paket enthalten sind.

Namensauflösung

Protokoll- und Portnummern sowie IP-Adressen sind in ihrer numerischen Form für den Menschen nicht so einprägsam (welcher Dienst steckt hinter Portnummer 119 oder welcher Host hat die IP-Adresse 192.168.1.1?). Zur Vereinfachung gibt es für Protokoll- und Portnummern einen (beschreibenden) Namen, IP-Adressen können als Hostnamen/Domainname angegeben werden. Zur Umsetzung von Namen in Nummern gibt es zwei Möglichkeiten: eine Textdatei, die die entsprechende Umsetzung durchführt oder einen eigenen Dienst (z.B. DNS für die Auflösung von Hostnamen/Domainnamen in IP-Adressen und andersherum).

Folgende Textdateien sind auf einem Linux-System für die Umsetzung von Namen in Adressen vorgesehen:

/etc/protocols Protokollnamen <-> Nummern

/etc/services Portnummern/Protokoll <-> Nummern

/etc/hosts Hostnamen <-> IP-Adressen

/etc/network Netzwerknamen <-> IP-Netzadressen