

Linux für Einsteiger

Teil 4

Der Netzzugang

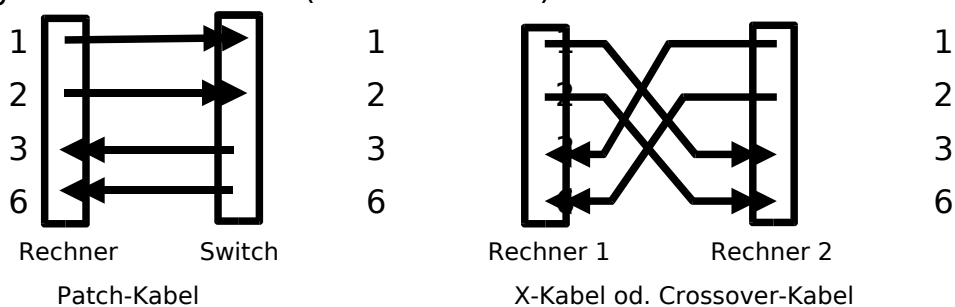
Die Netzwerkschnittstellen

Auch ohne Netzwerkkarte oder irgendwelche Anschlüsse gibt es immer eine „interne“ Netzwerkschnittstelle, genannt „localhost“. Ein Rechner ohne Verbindung zu anderen Rechnern kann damit Netzwerkdienste einrichten und testen.

Die am weitesten verbreitete Schnittstelle ist der Ethernet-Anschluss. Ihn gibt es in verschiedenen Geschwindigkeitsstufen, d.h. es gibt eine Obergrenze der Rohdatenrate von 10 Mbit/sek, 100 Mbit/sek, 1000 Mbit/sek. Der topologische Netzaufbau ist busartig und wird heutzutage durch eine sternförmige Verkabelung realisiert. Ring- oder Schleifenbildung sind nicht zulässig.

Ein Rechner kann mehrere Netzwerkschnittstellen besitzen, diese werden mit einer laufenden Nummer unterschieden (eth0,eth1,...)

Wenn einmal nur 2 Rechner direkt verbunden werden sollen (ohne Sternpunkt), dann ist darauf zu achten, dass ein spezielles Kabel mit gekreuzten Anschlüssen verwendet wird. Bei normalen Verbindungskabeln zum Sternpunkt (Hub, Switch) werden Sende- und Empfangsleitungen 1:1 verbunden (siehe Schema)



Es ist auch möglich, zwei Rechner mit „Firewire“(IEEE1394)-Schnittstelle direkt zu verbinden, bei Linux gibt es entsprechende Module, die das Ethernet-Protokoll physikalisch über Firewire leiten. Firewire ist eine schnelle (bis zu 400 Mbit/sek), bidirektionale, serielle Verbindung, die keine verschiedenen (gekreuzten) Kabel braucht.

Immer stärker verbreitet sind drahtlose Verbindungstechniken, insbesondere WLAN (wireless LAN). Die Unterstützung durch Linux ist im selben Maße stark verbessert worden. Viele gängigen PC-Cards für WLAN laufen ohne Probleme. Jeder sollte sich beim Einsatz dieser Technik über die Sicherheitsproblematik im klaren sein, selbst die gängigen Verschlüsselungstechniken, die bei WLAN vorgesehen sind, schützen

nicht 100%tig vor Hackern. Sicherheitsrelevante Daten müssen zusätzlich geschützt werden, z.B. durch weitere Verschlüsselung (Stichwort VPN – virtual private network), Zugangsbeschränkungen auf bestimmte Rechner (IP- und MAC-Adressen).

Der Aufbau der Internetadressen

Ich vereinfache die Darstellung auf das für das Verständnis der Vorgänge notwendige Maß. Zur Zeit ist das noch weit verbreitete Protokoll IPv4, die Adressierung erfolgt durch eine 32-bit-Dualzahl, sie wird zur besseren menschlichen Lesbarkeit unterteilt in 4 Bytes mit Punkten dazwischen: 0.0.0.0 bis 255.255.255.255

Bestimmte Adressen, bzw. Adressgruppen haben eine bestimmte Bedeutung:

- 0.0.0.0 steht für das ganze Internet
- x.y.z.0 bezeichnet ein Netzwerk (mit Rechnernr. 1..254)
- x.y.z.255 ist die Broadcast-Adresse des Netzwerkes (alle Rechner im Netzwerk x.y.z.0 werden angesprochen)
- 127.0.0.1 ist die localhost Adresse (intern)
- 255.255.255.255 steht für einen allgemeinen Broadcast

Für den Aufbau privater Netze sind bestimmte Adressbereiche reserviert worden, die nicht ins Internet weitergeleitet (gerouted) werden:

- 10.0.0.0 bis 10.255.255.255 hier kann ein großes, privates Netz mit bis zu 16777214 Rechnern erstellt werden
- 172.16.0.0 bis 172.31.255.255 hier sind 16 verschiedene Netze mit jeweils bis zu 65534 Rechnern möglich
- 192.168.0.0 bis 192.168.255.255 hier sind 256 verschiedene Netze mit jeweils bis zu 254 Rechnern möglich

Rechner, die in einem privaten Netzwerk liegen und auf das Internet zugreifen wollen, müssen sich eines sogenannten „Gateways“ bedienen. Das ist ein Rechner (od. Router), der neben der Verbindung ins private Netz auch eine Verbindung zum Internet hält. Er hat für die Internetverbindung eine weltweit gültige, einmalige Adresse zugeteilt bekommen (statisch=fest oder dynamisch=vom Provider nach Bedarf aus seinem Adresspool zugeordnet). Dieser Rechner versieht nun alle Anfragen aus dem privaten Netzbereich mit der gültigen Internetadresse (Masquarading bzw. NAT (Network Adress Translation)).

Wie können verschiedene Dienste über eine IP-Adresse abgewickelt werden?

Neben der IP-Adresse gibt es noch Portnummern (1..65536), die unterscheidbare Datenströme zu einer IP-Adresse ermöglichen. Ein Rechner kann mehrere Verbindungen gleichzeitig aufbauen und bedienen. Bestimmte Portnummern sind festen Diensten zugeordnet, eine Tabelle hi-

erzu findet sich unter „/etc/services“. Die Portnummer muss nicht immer angegeben werden, da bestimmte Internetprotokolle (HTTP, FTP,..) implizit immer die richtigen Ports ansprechen, ansonsten ist die richtige Schreibweise : w.x.y.z:NNNN

In der Un*x Geschichte hat sich eingebürgert, die Portnummern bis 1023 als privilegierte Ports zu bezeichnen, sie sind Serverdiensten vorbehalten, die root-Rechte erfordern.

Was ist die Netzwerkmaske (netmask)?

Sie gibt an, welche Rechner in einem gemeinsamen Netz zusammengeschaltet sind und sich damit unmittelbar erreichen können. Rechner in anderen Netzwerken können nur über einen „Gateway“-Rechner erreicht werden. Beispiel: netmask 255.255.255.0 bezeichnet ein Netz mit max 254 Rechnern, wie 192.168.100.x

Firewalls

Sie sind eine Möglichkeit, den Datenverkehr über Netzwerkschnittstellen zu überwachen und einzuschränken. Wir behandeln an dieser Stelle die sogenannten Paketfilter-Firewalls, d.h. Filterkriterium sind IP-Adressen und Portnummern. Wir können für jede Netzwerkschnittstelle getrennt nach Eingang und Ausgabe IP-Adressen und Portnummern blockieren oder freigeben. Neben der grundsätzlichen Haltung, nur unbedingt nötige Serverdienste auf dem eigenen Rechner laufen zu lassen, können wir bei den verbliebenen Diensten den potentiell gefährlichen Zugriff aus dem Internet verhindern. Bei Vorhandensein eines lokalen Netzwerks, welches auch Kontakt zum Internet hat, ist besonders exakt auf die erstellten Regeln zu achten (insbesondere beim SMB-Protokoll bzw. W*-Rechnern im Netz). Wir werden beispielhaft Regeln mit Hilfe des graphischen Programms „Guarddog“ erstellen, es erleichtert uns die Handhabung und entbindet uns davon, das eigentlich benutzte „iptables“ bzw. „ipchains“ mit seiner komplizierten Syntax benutzen zu müssen. Interessierte können sich das von „Guarddog“ erstellte Script mal ansehen (zu finden unter /etc/rc.firewall).

Paketfilter können zwar schon sehr viele Angriffe aus dem Internet stoppen, jedoch ist keine Inhaltskontrolle möglich. Es wird z.B. nicht geprüft, ob das zulässige Paket zu einem Webserver (auf dem eigenen Rechner) gefährlichen Code enthält, eine Kontrolle auf der Anwendungsebene ist anderen Programmen vorbehalten.

Wir gehen ins Internet

Welche Verbindungsmöglichkeiten gibt es?

1. Analoges Modem

- serieller Anschluss – praktisch alle Modems mit AT-Befehlssatz werden unterstützt

- USB-Anschluss – nur teilweise von Linux unterstützt
- Netzwerkanschluss (Ethernet) – neueste Entwicklung für eine problemlose Einwahl ins Internet, basiert auf dem PPPoE Protokoll, wird von Linux problemlos unterstützt.

2. ISDN-Modem (Karte)

- Die Unterstützung durch Linux ist sehr unterschiedlich, da es keine der CAPI unter W****s vergleichbare Funktionalität gibt. Unterstützt werden viele passive ISDN-Karten durch ISDN4LINUX. Vereinzelt veröffentlichen Hersteller eigene Linux-Lösungen.

3. DSL-Modem

- Anschluss über Ethernet-Netzwerkanschluss. Die IP Pakete werden in Ethernet-Frames verpackt, auch die Steuerung erfolgt über spezielle Frames (Verbindungsaufbau, -abbau). Das Protokoll heißt PPPoE (Point to Point over Ethernet) und wird von Linux voll unterstützt.

4. Router (mit und ohne DSL-Modem)

- Er enthält die Funktionalität, selbstständig Verbindungen auf- und abzubauen, der eingebaute Minirechner kann noch weitere Aufgaben übernehmen (Firewall, Server (Festplatte, Drucker)).

Für alle diese Möglichkeiten enthält Linux entsprechende Einstellungs- und Verbindungsprogramme (-dialoge).