IP Routing

Vortrag: *Felix von Leitner* <fefe@ccc.de>
WWW:

Bericht: *ISCS* <iscs@ailis.com>

Der Vortrag von Felix, genannt Fefe, zum Thema "IP-Routing" fand von 13 Uhr bis 15 Uhr im Workshopraum 1 statt. Der völlig überfüllte Saal musste zu Anfang von allen Tischen befreit werden, um Platz für die großen Menschenmassen zu schaffen, die sich nunmehr mit Stehplätzen zufrieden geben mussten.

Die Grundlage, um Routing zu verstehen, ist das Verständnis des IP-Protokolls, das zuvor von Pirx in seinen Vortrag "IP für Anfänger" trefflich vermittelt wurde. Routing beginnt bei jedem zu Hause im eigenen Ethernetz. Mit dem ARP-Protokoll werden IP-Pakete innerhalb des eigenen Netzes zugestellt.

Ein Beispiel: Rechner 1 möchte ein Paket an Rechner 2 (mit der IP 1.2.3.4) senden. Rechner 1 und 2 haben jeweils eine Netzkarte mit einer fest vom Hersteller eingebauten weltweit eindeutigen Ethernet-Adresse (MAC-Adresse). Die IP-Adresse (die nicht fest in die Karte eingebaut ist, sondern selber in die Software eingetragen werden muß) ist noch nicht mit der MAC-Adresse der Karte verknüpft.

Hierzu dient das ARP-Protokoll. Rechner 1 (der Sender) sendet einfach eine Nachricht an alle Rechner innerhalb des eigenen Netzes (eine Broadcast-Nachricht): "Wer hat eigentlich die IP 1.2.3.4?" Alle Rechner empfangen diese Nachricht, doch die meisten ignorieren sie. Nur der Rechner 2 mit der IP 1.2.3.4 (denn der kennt am Besten seine eigene IP) antwortet dem Rechner 1 (diesmal auf direktem Wege, die MAC des Rechners Nummer 1 entnimmt Rechner 2 der Absender-Adresse der Broadcastnachricht) und antwortet "Ich habe die IP 1.2.3.4". Für zukünftige Anfragen merkt sich Rechner 1 nun in seinen ARP-Cache die MAC-Adresse des Rechners mit der IP 1.2.3.4.

Hier ergeben sich Angriffsmöglichkeiten, wenn ein Hacker-Rechner solche ARP-Pakete fälscht und sich so für jemand anderen ausgibt. Folgende Pakete, die eigentlich für einen anderen Rechner bestimmt waren, werden nun brav an den Hacker zugestellt.

Das eigentliche IP-Routing behandelt nun die Frage: "Woher weiß ein IP-Paket, wo es im Internet auf dem Weg zu seinen Ziel hingehen muß?" Dies ist kein Problem in meinem eigenen Privatnetz. Hier hängen alle Rechner an einem einzigen Kabel, und man muss nur via ARP-Request fragen, wer das Paket haben will. Soll ein Paket nach draußen zugestellt werden (zum Beispiel durch einen Router, der mit einer Standleitung zum Internet verbunden ist), so muss der Rechner wissen, dass jedes Paket, was nicht innerhalb des eigenen Netzes zugestellt werden kann, durch diesen Router weitergeleitet werden muss. Dazu trägt man einfach in der Konfiguration des Clients die IP-Adresse des Standard-Gateways des Routers mit Verbindung zum Internet ein. Der Client verlässt sich einfach darauf, dass dieser Router schon wissen wird, wohin er das Paket weiter zustellen soll.

Woher weiß der Client aber, welche Zieladresse eines Pakets innerhalb des eigenen Netzes liegt oder nicht? Die Netmask gibt an, wie groß das eigene Netz ist. Eine Netmask von 255.255.255.0 sagt aus, dass das eigene Netz daran zu erkennen ist, dass alle Rechner innerhalb des Netzes drei identische erste Stellen in ihrer IP besitzen, z.B. ein Netz von 5.6.7.0 bis 5.6.7.255.

Bei einem bitweisen Vergleich zwischen der eigenen Adresse und der Zieladresse mit Hilfe der Subnetmask kann auf diese Weise herausgefunden werden, ob das Ziel innerhalb des eigenen Netzes liegt. Jedes Bit innerhalb der Subnetmask, das auf Eins gesetzt ist, kennzeichnet, dass hier innerhalb der IP die Netzadresse steht. Sind sie bei Absender- und Zieladresse gleich, so liegt das Ziel im eignen Netz. Andernfalls wandert das Paket zum Standard-Gateway.

Die Netze wurden in verschiedene Klassen unterteilt: Klasse A: 0-127.x.x.x (Netmask: 255.0.0.0) Klasse B: 128-191.x.x.x (Netmask: 255.255.0.0) Klasse C: 192-223.x.x.x (Netmask: 255.255.255.0)

Klasse D und E sind Sondernetze (Multicast-Netze und reservierte Adressen für zukünftige Anwendungen). Was aber nun, wenn ein Router mehrere Ausgänge hat? Er benötigt eine Routing-Tabelle. In ihr

ist festgehalten, welches Netz (gekennzeichnet durch die IP-Adresse des Netzes und die Netmask) durch welches Netzinterface zu erreichen ist und an welches Gateway es weitergeleitet werden muss.

Wie werden diese Routing-Tabellen aufgebaut? Dies kann entweder manuell geschehen, indem der Administrator des Routers diese Tabellen selbst einträgt (statisches Routing), oder durch dynamisches Routing, bei dem ein Protokoll diese Aufgabe übernimmt.

Routen können auf diese Weise symmetrisch oder asymmetrisch festgelegt werden. Der Weg, den ein Paket in eine Richtung nimmt, ist entweder mit dem Rückweg identisch bzw. beim asymmetrischen Routing von diesem verschieden. Asymmetrische Konfigurationen können zum Beispiel dazu missbraucht werden, Pakete über einen Spionage-Rechner umzuleiten, damit dieser sich alle Pakete ansehen kann.

Beim dynamischen Routing werden die Routingtabellen automatisch gesetzt. Auf diese Weise reagiert das Netz selbständig auf Ausfälle aller Art, indem es sich von selbst Umleitungen in die Routingtabellen einträgt, und der ohnehin geplagte Netzadministrator nicht mehr durch die Keller kriechen muss, um jeden Rechner bei einer Änderung im Netz umzukonfigurieren.

Das Bekannteste seiner Art ist RIP, das Routing Information Protocol. Es arbeitet nach dem Prinzip, dass ein Router in regelmässigen Abständen seinem Nachbar-Router seine Routingtabelle übermittelt. Gut für kleine Netze - schlecht für große. Schnell wird viel Traffic verursacht, da ständig Routingtabellen übermittelt werden müssen. Alternativen sind OSPF (Open Shortest Path First), welches nur an bekannte Router Routingtabellen überträgt - nicht an alle. Auf diese Weise bilden sich innerhalb des Rechners regelrechte Karten von dem Netz in seiner Umgebung, woraus er die beste Route für ein Paket errechnet. Der Informationsaustausch geschieht über das Hello-Protokoll.

OSPF bietet aber noch weitere Möglichkeiten. So können mehrere Leitungen, die alle zu einem Ziel führen, zu einer großen Leitung zusammengefasst werden. Sie bilden sogenannte Autonome Systeme (Systeme, die für sich ein eigenes Netz bilden, mit mehreren Verbindungen zu anderen Netzen). Weitere Protokolle, die sich am "großen Routen" beteiligen, sind das EGP (Extended Gateway Protocol) und das BGP (Border Gateway Protocol), die allerdings für richtig große Netze gedacht sind - und dementsprechend selten genutzt werden.