Mobile IP

-

Die wesentliche Funktionsweise am Beispiel von Wireless LAN

Seminararbeit

Hochschule Bremen
Fachbereich Elektrotechnik und Informatik

Studiengang: Technische Informatik

Einführung in das wissenschaftliche Arbeiten
Dipl. Ing. Alke Myrzik

Wintersemester 2004/2005

Vorgelegt von:	René Büst	Stefan van Lier
Matr.-Nr.	152400	153433

Bremen, 13.01.2005

Inhaltsverzeichnis

1 Einleitung

Mobile IP wurde 1996 von der Internet Engineering Task Force (IETF) entwickelt und veröffentlicht. Es ist ein Protokoll und arbeitet auf der Netzwerkschicht des TCP/IP Modells. Mobile Geräte, wie z.B. Laptops oder PDAs können damit den Standort wechseln, ohne dass deren Anwendungen neu gestartet werden müssen. Außerdem kann eine Kommunikation ohne Unterbrechung zu anderen Systemen erfolgen, wie z.B. zu Servern oder anderen mobilen Systemen. Mobile IP ermöglicht dem Anwender ohne Änderung seiner IP-Adresse von einem Subnetz in ein Anderes zu wechseln. Es nutzt das Internet Protokoll als Basis und erweitert dieses um die Funktion der Mobilität.

1.1 Warum Mobile IP

Die Planung und der Einsatz von Mobile IP sind streng mit der Größe des zu implementierenden Netzwerkes sowie der Subnetzbildung verbunden.

In kleineren Netzwerken, in denen keine detaillierten Strukturen (z.B. Aufteilungen nach Abteilungen) notwendig sind, kann auf die Bildung von Subnetzen (speziell für Wireless LAN) verzichtet werden. In größeren Netzwerken ist dieses allerdings unumgänglich. Bei einer Verzichtung auf die Unterteilung würden sämtliche Broadcast- und Multicastpakete an alle Funkzellen weitergeleitet werden und somit das Wireless LAN (WLAN) unnötigen Belastungen aussetzen und dessen Performance beeinträchtigen.
Das Problem des Broadcast- bzw. Multicast-flooding gilt nicht nur für ein Wireless LAN Netz, sondern auch für Ethernet.

Das Internet Protokoll IPv4 wurde für eine statische Netzwerktopologie entwickelt. Alle Stationen haben in einem Netzwerk eine feste IP-Adresse, dies macht einen Wechsel in ein anderes Subnetz ohne einen Verbindungsverlust der Stationen unmöglich. Für diese Problematik wurde Mobil IP entwickelt, welches im Folgenden allgemein und mit Beispielen genauer erläutert wird.

1.2 Technischer Hintergrund

1.2.1 Mobile-Node

Der Mobile-Node ist das jeweilige Endgerät, wie z.B. ein Notebook, PDA oder ein Mobiltelefon, welches sich in einem Netzwerk von einem Subnetz in ein Anderes bewegt. Dabei kann dieser seine laufende Kommunikation aufrechterhalten und er behält seine eindeutige IP-Adresse.

1.2.2 Home-Agent

Der Home-Agent ist der Router im Heimatnetzwerk des Mobile-Node. Er ist der Bezugspunkt des Mobile-Node, wenn sich dieser durch die Subnetze bewegt. Der Home-Agent kommuniziert mit dem Foreign-Agent oder sendet die Daten direkt an den Mobile-Node, je nach IP-Version.

1.2.3 Foreign-Agent

Der Foreign-Agent ist der Router im Subnetz in dem sich der Mobile-Node aufhält. Dieser kommuniziert mit dem Home-Agent und ist dafür verantwortlich, dass der Mobile-Node von seinem Home-Agent die Daten bekommt. Home-Agent und Foreign-Agent zusammen sind dafür zuständig, dass der Mobile-Node seine IP-Adresse während des Wechsels in ein anderes Subnetz nicht verändern muss und durch das Netzwerk wandern kann.

1.2.4 Care-of-Address

Die Care-of-Address ist die IP-Adresse, die der Mobile-Node von dem jeweiligen Foreign Agent, in dessen Subnetz er sich befindet, zugeteilt bekommt. Über diese Adresse ist er im fremden Subnetz erreichbar. Die Care-of-Address wird dem Mobile-Node über DHCP (Dynamic Host Configuration Protocol) zugewiesen und ändert sich in dem Moment, wenn der Mobile-Node in ein anderes Subnetz wechselt.

1.2.5 Roaming

Roaming bezeichnet die Möglichkeit, dass eine mobile Station zwischen zwei oder mehreren Funkzellen (Access Points) oder Subnetzen wechseln kann. Dabei entscheidet der Mobile-Node an Hand der Signalstärke der so genannten Beacon Frames, die jeder Access Point regelmäßig sendet, an welchen Access Point er sich anmelden wird.

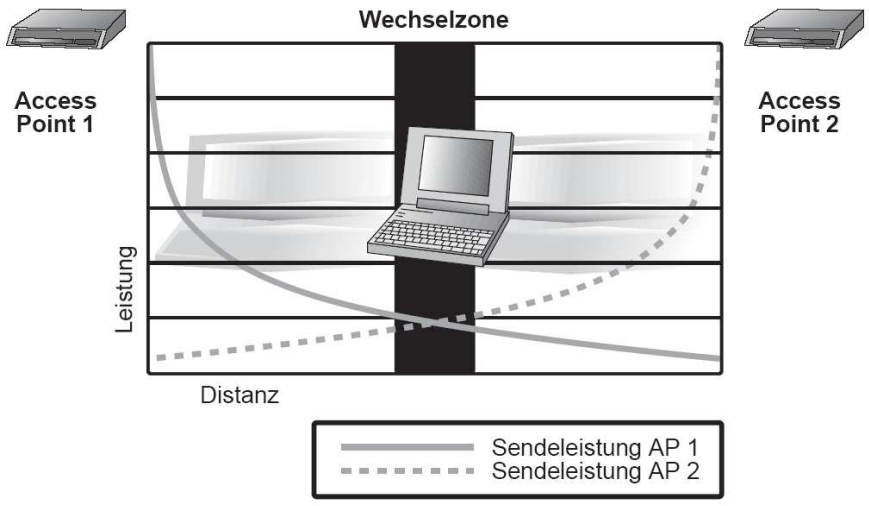


Abb.1 Roaming eines Access Points (Jörg Rech (2004), **Wireless LANs**, Heise Verlag)

2 Die Funktionsweise von Mobile IP

2.1 IPv4

Wechselt ein Mobile-Node in ein für ihn fremdes Subnetz, registriert er sich automatisch bei dessen Foreign-Agent und bekommt die Care-of-Address mitgeteilt. Unter dieser ist er dann für den Foreign-Agent erreichbar. Anschließend übermittelt der Mobile-Node dem Home-Agent seinen Aufenthaltsort und die Adresse des Foreign-Agent, sowie seine Care-of-Address. Daten die jetzt an die bekannte statische IP-Adresse des Mobile-Node gesendet werden, erreichen nun zuerst den Home-Agent. Dieser kapselt die Daten in weitere IP-Datagramme (IP Pakete), in deren IP-Header die Zieladresse des Foreign-Agent eingetragen wird. Zusätzlich wird ein weiterer IP-Header erzeugt, der die Care-of-Address des Mobile-Node beinhaltet. Der Home-Agent sendet die gekapselten Daten an den zuständigen Foreign-Agent in dem Netz, in dem sich der Mobile-Node gerade befindet. Dieses Verfahren wird als Tunneling oder auch IPIP-Encapsulation bezeichnet. Der Foreign-Agent (ent-)kapselt das Datagramm, liest dabei den zusätzlichen Header aus und sendet die Daten an die hinterlegte Care-of-Address und somit an den Mobile-Node.
In welchem Subnetz sich ein Mobile-Node gerade befindet, kann er mit den Funktionen der Agent Discovery bestimmen. Dazu überwacht er die Agent Advertisements, die der Home-Agent bzw. die Foreign-Agents in regelmäßigen Abständen als Broadcasts oder Multicasts aussenden. Advertisements werden von den Agents dazu benutzt um den Nodes Dienste anzubieten. Ein Mobile-Node kann daher schnell einen Subnetzwechsel bestimmen, indem er über einen bestimmten Zeitraum kein Advertisement vom selben Agent erhalten hat. Mit einer Agent Solicitation kann der Mobile-Node anschließend einen Agent oder mehrere auffordern, wieder ein Advertisement zu senden, um seine Position zu bestimmen.

2.2 IPv6

Im Gegensatz zu IPv4 wird bei IPv6 kein Foreign-Agent benötigt. Wechselt ein Mobile-Node in ein Subnetz teilt er seinem Home-Agent seine Position, sowie die Care-of-Address mit. Werden nun Daten an den Mobile-Node gesendet, werden diese zuerst an den Home-Agent übermittelt. Dieser kapselt die Daten in neue Datagramme und tunnelt sie mit der Care-of-Address als Zieladresse an den Mobile-Node. Nachdem der Mobile-Node die Daten erhalten hat, (ent-)kapselt dieser die Datagramme und sieht nun jedoch die ursprüngliche Absenderadresse des anderen Client/Server. Der Mobile-Node sendet eine direkte Nachricht an den Client/Server mit dem Inhalt seiner Care-of-Address als Absender. Der Client/Server speichert die Care-of-Address des Mobile-Nodes in seinen Binding-Cache ab und die Kommunikation kann nun direkt zwischen den Beiden erfolgen, ohne den Home-Agent zu benutzen. Der Client/Server verwendet dazu die Care-of-Address des Mobile-Node als Zieladresse.

3 Probleme von Mobile IP

3.1 Sicherheit

Während der Implementierung eines „Mobile IP Netzes“, z.B. eines WLAN, welches in der Regel sehr oft fremde Nodes aufnimmt, sollte auf ein VLAN, bzw. auf ein separates WLAN-Netz nicht verzichtet werden. Der Grund dafür ist, dass die Mobile-Nodes eine IP-Adresse aus dem „normalen“ Ethernet beziehen, wenn sie in ein WLAN wechseln, das seine IP-Adresse per DHCP vergibt. Diese Gast Nodes wären somit in der Lage über die IP-Ebene des Ethernets Verbindungen zu dessen Clients aufzubauen. In einem Funknetz, wie Wireless LAN, sind die Nodes (Clients) gegenüber Angriffen (mithören) viel sensibler als in einem Ethernet-LAN, was seine Daten über ein Kabel verschickt. Daher sollten die Daten über ein Wireless LAN zusätzlich verschlüsselt übertragen werden, z.B. über ein VPN. Ein weiteres Problem, das in Betracht gezogen werden sollte ist das so genannte Ingress Filtering. Ein Mobiler Node kann seine Verbindungen zu anderen Stationen aufbauen, ohne den Foreign-Agent oder den Home-Agent vorher zu kontaktieren. Probleme entstehen, wenn der Mobile-Node wieder eine Verbindung zu den Stationen in seinem Heimnetz aufbauen möchte. Viele Router (Firewalls) am Eingang des Netzes sind so konfiguriert, dass sie IP-Datagramme mit der Quelladresse aus dem eigenen Netz nicht mehr in das Subnetz hineinlassen. Eine Verbindung des Mobile-Nodes mit Clients oder Servern aus seinem eigenen Netz wäre somit nicht mehr möglich. Ingress Filtering wird aus sicherheitstechnischen Gründen verwendet, um unter anderem Address-Spoofing und Port-Scanning zu verhindern.

3.2 Technik

Nicht nur die Sicherheit kann ein Problem darstellen, sondern auch die eingesetzte Hardware. Wenn der Home-Agent ausfallen sollte, ist die Kommunikation mit dem Mobile-Node nicht mehr möglich. Für den Mobile Node wäre das Netzwerk nicht mehr erreichbar. Ähnliches kann passieren, wenn sich der Client in einem fremden Netz befindet und der dortige Foreign-Agent ausfällt. Der Client hat dann keine Möglichkeit aus dem fremden Subnetz Daten in sein Heimatnetz zu senden. Befindet sich der Client hingegen im Heimatnetz, so ist es egal, ob ein Foreign-Agent ausfällt, da er diesen zu dem Zeitpunkt nicht benötigt. Ein weiteres Problem besteht im nicht optimalen Routing, das durch die Dreieckskommunikation zwischen Home-Agent, Foreign-Agent und Mobile-Node entsteht. Dieses führt zu höheren Laufzeiten, die wiederum die Flusskontrollmechanismen in der Transportschicht negativ beeinflussen.

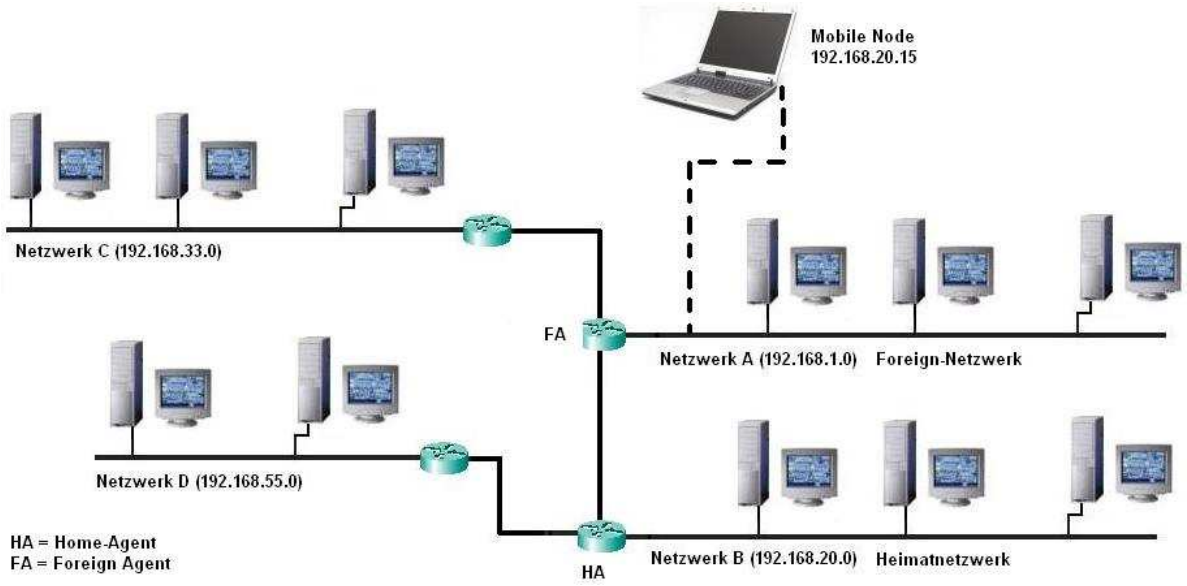
4 Anwendungsbeispiel und Einsatzbereiche

4.1 Einsatzbereiche

Mobile IP ist für große Unternehmen, in denen das Netzwerk in verschiedene Subnetze unterteilt ist besonders gut geeignet. Die Subnetzbildung hat den Vorteil, dass das Netzwerk nicht durch Broadcast und Multicast Anfragen an Performance verliert. Damit ein Client die Möglichkeit hat, in jedem Subnetz erreichbar zu sein, ohne ständig seine IP-Adresse zu ändern, ist der Einsatz von Mobile IP empfehlenswert. Grundsätzlich wird Mobile IP verwendet, wenn verschiedene Subnetze in Verbindung mit Wireless Lan eingesetzt werden. Dieses ist oftmals erforderlich, damit der Client seine statische IP-Adresse behält und somit trotzdem in seinem Heimatnetz bleibt. In kleineren Netzwerken sollte hingegen vor der Implementierung von Mobile IP genau berechnet werden, ob es wirtschaftlich ist.

4.2 Großes Unternehmen

Das Netzwerk eines großen Unternehmens wurde so aufgeteilt, dass die Büros, Labore, Konferenzräume und die einzelnen Abteilungen über ihre eigenen Subnetze verfügen. Zudem wurde in dem Netzwerk ein WLAN eingerichtet, das mit der Technik von Mobile-IP betrieben wird. Somit befindet sich in jedem Subnetz ein Home-Agent und ein Foreign-Agent. Durch den Einsatz von Mobile IP hat jeder Mitarbeiter mit seinem mobilen Client (Mobile-Node) die Möglichkeit, von jedem Punkt des Unternehmens aus und bei jedem Wechsel in ein anderes Subnetz, auf sein Heimatnetz zuzugreifen. Die Änderung der IP-Adresse des Clients ist nicht mehr nötig. Ohne den Einsatz von Mobile IP könnte der Mitarbeiter mit seinem Client, nach dem Wechsel in ein anderes Subnetz, keine Verbindung in sein Heimatnetz aufbauen, da die Kommunikation abbrechen würde.



4.3 Kleines Unternehmen

In einem kleinen Unternehmen mit rund 25 WLAN-Clients, die alle in einem Netzwerk arbeiten, wäre die Unterteilung in verschiedene Subnetze nicht sehr sinnvoll. Der technische, wie auch administrative Aufwand würde keinen entscheidenden Performancevorteil bringen. Daher sollte ein Subnetz genutzt und auf den Einsatz von Mobile IP verzichtet werden. Die Einführung von Subnetting und Mobile IP in diesem Unternehmen wäre nur dann sinnvoll, wenn eine starke Expansion in naher Zukunft abzusehen wäre. Eine Einführung würde hohe Anschaffungskosten bezüglich der Hardwareanschaffung, wie auch der Schulung der Mitarbeiter zur Folge haben. Diese stehen oftmals nicht im Verhältnis zu dem gewünschten Geschwindigkeitsvorteil.

5 Reflexionen & Lösungen

5.1 Zusammenfassung

Die derzeitige Problematik von IPv4 ist, dass die Struktur für statische Netzwerke entwickelt wurde. Daher besteht keine Möglichkeit, mit einem mobilen Client in ein anderes Subnetzwerk zu wechseln, ohne dass die Verbindung unterbrochen wird oder dass die IP-Adresse geändert werden kann. Um dieses Problem zu lösen, wurde Mobile-IP entwickelt. Mit dieser Technologie ist es möglich in ein fremdes Subnetz zu wechseln, ohne die Verbindung zum Heimatnetz zu verlieren. Bei IPv4 kommuniziert der Mobile-Node zuerst mit dem Foreign-Agent, der ihm dann eine Care-of-Address zuteilt. Der Mobile-Node sendet dem Home-Agent anschließend seine derzeitige Position und seine Care-of-Address. Werden nun Daten an den Mobile-Node gesendet, erreichen diese zuerst den Home-Agent. Dieser kapselt die Daten in ein Datagramm, das als Header-Information die IP-Adresse des Foreign-Agent beinhaltet. Zudem enthält dieses Datagramm einen weiteren IP-Header mit der Care-of-Adress des mobilen Clients. Der Home-Agent sendet die Daten anschließend an den Foreign-Agent, der diese dann an den Mobile-Node übergibt.
Bei der IP-Version IPv6 wird im Gegensatz zur IP-Version IPv4 kein Foreign-Agent benötigt. Der Mobile-Node sendet seine aktuelle Position und seine Care-of-Address an den Home-Agent. Wenn Daten an den Mobile-Node gesendet werden, erhält diese zuerst der Home-Agent. Dieser kapselt die Datagramme und schickt diese direkt an den Mobile-Node. Der Mobile-Node (ent-)kapselt die Datagramme und schickt anschließend eine direkte Nachricht an den Client oder dem Server, von dem die Daten ursprünglich stammen. Damit teilt er diesem seine Care-of-Address mit. Nach diesem Vorgang können beide direkt mit einander kommunizieren.

5.2 Problemlösungen

Eine Lösung für das Ingrees-Filtering Problem ist, den Router so zu konfigurieren, dass die IP-Adresse des entsprechenden Mobile-Nodes das Heimnetz erreichen darf. Dieses wäre aber bei einer großen Anzahl von mobilen Clients zu aufwändig, wodurch das so genannte Reverse Tunneling zum Einsatz kommen sollte. Bei diesem Verfahren kapseln die mobilen Clients die Datagramme, in denen sie ihre topologisch korrekte Care-of-Adress eintragen. Diese Datagramme schicken sie anschließend zu ihrem Home-Agent, der diese wiederum zu der in den Datagrammen eingetragenen Zieladresse routet.

5.3 Ausblick / Zukunft

Die Entwicklung von Mobile IP in den nächsten Jahren ist noch ungewiss. Nach der Einführung im Jahr 1996 konnte Mobile IP auf Grund der geringen Möglichkeiten noch nicht effektiv eingesetzt werden. Durch den Wandel unserer Gesellschaft in eine mobile Gesellschaft hat Mobile IP aber bereits an Bedeutung gewonnen und wird es auch immer mehr. Dies ist verbunden mit dem Einzug von Wireless LAN, sowie Voice over IP (VoIP) in den Mainstream. Für den Einsatz im Unternehmensumfeld in Verbindung mit tragbaren VoIP-Telefonen ist Mobile IP nicht mehr wegzudenken, da durch das Arbeiten in verschiedenen Räumen ein Wechsel des Subnetzes erforderlich ist. Mobile IP ist aber nicht nur eine Technik für das Netzwerk innerhalb eines Unternehmens, sondern sollte im Hinblick auf die weltweite kabellose Vernetzung an jedem Ort verwendet werden! Seit der Einführung von UMTS (3G), der Integration der WLAN-Technik in gewöhnliche Mobiltelefone, der immer stärkeren Verbreitung von Hotspots, sowie der fast vollständigen weltweiten Vernetzung hat sich der Arbeitsplatz eines Arbeitnehmers verändert. Es ist nicht nur der Platz an einem Schreibtisch im Büro, sondern zum Beispiel auch der zu Hause, bzw. im kleinen Café um die Ecke oder im Stadtpark. Von dieser Technik werden aber auch Außendienstmitarbeiter enorm profitieren, die somit von jedem Ort der Welt auf ihr Firmennetzwerk zugreifen können, als ob sie innerhalb diesem wären.

5.4 Fazit

Mobile IP sollte nur in Netzwerken (wie z.B. in der Hochschule Bremen) eingesetzt werden, in denen ca. 30 oder mehr mobile Clients vorhanden sind. Damit kann ein Verlust von Performance durch Broadcast und Multicast Anfragen verringert werden. Das WLAN Netz sollte zunächst in verschiedene Subnetze unterteilt werden, in denen dann Mobile IP implementiert wird.

Für kleinere Netzwerke (Class C Netz, bis zu 253 Clients, max. 30 mobile Clients) ist die Unterteilung in Subnetze, sowie die Nutzung von Mobile IP nicht empfehlenswert. Der Aufwand der Subnetzbildung und der zusätzlichen Hardwareinstallation, sowie die Administration, bringen nicht den gewünschten Performancevorteil und verursachen zudem unnötige Kosten.

6 Quellenangaben

6.1 Bücher

- Neeli Prasad, Anand Prasad (2001), **WLAN Systems and Wireless IP for next Generation Communications**, Editor Verlag, SUB Bremen, Neustadtswall

- Herbert Wiese (2002), **Das neue Internetprotokoll IPv6**, Hanser Verlag

- Jörg Rech (2004), **Wireless LANs**, Heise Verlag

- Ernst Schawohl (2002), **Cisco Systems - Cisco Networking Academy Program, Lehrbuch 1. und 2. Semester**, Cisco Press,

- Ernst Schawohl (2002), **Cisco Systems - Cisco Networking Academy Program, Lehrbuch 3. und 4. Semester**, Cisco Press,

- Jörg Fritsch, Steffen Gundel (2003), **Firewalls illustriert - Netzwerksicherheit durch Paketfilter**, Addison-Wesley

6.2 Internetseiten

[01] E. Perkins, Charles: Mobile Networking Through Mobile IP
URL: http://www.computer.org/internet/v2n1/perkins.htm
07.01.2005

[02] GigaPort SURFnet (2002): Hoe werkt Mobile IP
URL: http://www.gigaport.nl/netwerk/access/ta/mip/mobileip.html
07.01.2005

[03] Montenegro, Roberts, Basavaraj (2002): IP Routing for Wireless/Mobile Hosts
URL: http://www.ietf.org/html.charters/mobileip-charter.html
07.01.2005

[04] Jain, Raj: Wireless Networking and Mobile IP References
URL: http://www.cse.ohio-state.edu/~jain/refs/wir_refs.htm
07.01.2005

[05] Chen, Yi-an (1995): A Survey Paper on Mobile IP
URL: http://www.cse.ohio-state.edu/~jain/cis788-95/ftp/mobile_ip.pdf 07.01.2005

[06] Cisco Systems: Mobile IP
URL: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mbxul_wp.pdf
07.01.2005

[07] IETF: Mobile IP, IPv4, IPv6
URL: http://www.ietf.cnri.reston.va.us/ids.by.wg/mobileip.html
07.01.2005

[08] MobileIN.com: Mobile IP
URL: http://www.mobilein.com/mobile_IP.htm
07.01.2005

[09] IETF: Mobile IP-RFC 2002
URL: http://www.ietf.org/rfc/rfc2002.txt
07.01.2005

Die Zahlen in [ ] bezeichnen den Ordnernamen auf der beigelegten CD-ROM.