WissenHeute Jg. 57 5/2004

Fernzugriff auf Computer-Netze mit DSL-Anschluss.

Mehr als 20 Prozent der deutschen Unternehmen aller Größen setzen bereits DSL (Digital Subscriber Line) für ihren Internetzugang ein. Darüber hinaus nutzen immer mehr Unternehmen einen DSL-Anschluss mehrfach, um verteilte Standorte günstig miteinander zu vernetzen oder um ihren Außendienstmitarbeitern eine einfache Einwahl über das Internet ins eigene Unternehmensnetz zu bieten. Gerade für kleinere Unternehmen bildet DSL die Basis für neue Anwendungsfelder, wie z. B. Virtual Private Networks (VPN) oder Einwahllösungen, die bislang nur über teure Standleitungen zum Internet mit fester IP-(Internet Protocol-)Adresse möglich waren und über ISDN oder herkömmlichen Modem-Verbindungen nicht realisiert werden konnten. Der Einsatz flexibler Einwahllösungen – insbesondere unter Einbeziehung mobiler Zugangswege, wie z. B. GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunications System) oder WLAN (Wireless Local Area Network) – wird für viele Branchen immer wichtiger.

Der Autor

Dipl.-Ing. Stefanus Römer ist seit 1994 bei der Deutschen Telekom im Produktmanagement tätig. Seit April 2001 arbeitet er als Produktmanager bei T-Mobile, wo er insbesondere für das Produkt Mobile IP VPN sowie für mobile Intranet-Access-Lösungen zuständig ist.

Ausgangslage

Um vorhandene DSL-Anschlüsse auch für VPN- bzw. für Einwahl-Lösungen nutzen zu können, müssen zwei Voraussetzungen erfüllt werden:

- Die DSL-Verbindung zwischen Unternehmensnetz und Internet muss ständig aktiv sein und
- die jeweilige Gegenstelle muss jederzeit die gerade aktuelle Internetadresse des DSL-Anschlusses kennen, um über das Internet eine Verbindung zum Unternehmensnetz aufbauen zu können.

Die erste Voraussetzung erfordert einen DSL-Anschluss mit einem Pauschaltarif (Flat Rate) oder zumindest mit einem Volumentarif. Zudem muss gewährleistet sein, dass nach jeder Unterbrechung die Verbindung zum Internet automatisch wieder aufgebaut wird. Da sich in den meisten Fällen (abhängig vom Provider) die IP-Adresse jedoch bei jeder Ein-

Das Thema im Überblick

Um DSL-Anschlüsse für VPN- und Einwahllösungen verwenden zu können, muss die Verbindung zwischen Unternehmensnetz (LAN) und dem Internet ständig aktiv und die aktuelle Internetadresse der jeweiligen Gegenstelle bekannt sein. Nach einer Unterbrechung muss die Verbindung zum Internet automatisch wieder hergestellt werden. Die Internetadresse kann sich bei jeder Einwahl über einen Internet Service Provider jedoch ändern. Daher wird ein dynamischer Auskunftsdienst benötigt, der der Gegenstelle jeweils die aktuelle IP-Adresse bekannt gibt. Dieser kann als Dynamic DNS oder als Dynamic VPN realisiert werden. Mit Dynamic DNS lässt sich auf einfache Weise eine Einwahlmöglichkeit z. B. für File-Transfer oder Wartungsarbeiten am eigenen Netz realisieren. Dynamic VPN eignet sich eher für Verbindungen zwischen verschiedenen Unternehmensstandorten.

wahl über DSL ändert (dynamische IP-Adressvergabe) und daher nicht von vornherein feststeht, stellt sich die Frage, wie dennoch sichergestellt werden kann, dass der jeweiligen Gegenstelle bzw. dem Einwahl-Client jederzeit die aktuelle IP-Adresse bekannt ist. Um dies zu gewährleisten, wird ein zusätzlicher „dynamischer" Auskunftsdienst benötigt, der den Einwahl-Clients auf Anfrage jeweils die aktuelle IP-Adresse bekannt gibt. Dieser Dienst kann grundsätzlich auf zwei Arten realisiert werden: Entweder als

- zentraler Auskunftsdienst im Internet – die übliche Bezeichnung ist „Dynamic DNS (Dynamic Domain Name System)" – oder als
- ISDN-basierte Zusatzfunktion im DSL-Router des Unternehmensnetzes, welche von den meisten Herstellern „Dynamic VPN" genannt wird.

In beiden Fällen muss zumindest der jeweilige Auskunftsdienst über eine feste Adresse bekannt sein. Im Fall des zentralen Auskunftsdienstes im Internet (Dynamic DNS) ist dies die feste IP-Adresse eines DNS-Server und beim ISDN-basierten Auskunftsdienst (Dynamic VPN) eine feste ISDN-Rufnummer, über die der DSL-Router im Unternehmensnetz angewählt werden kann. Da Dynamic VPN nur für VPN-Verbindungen zwischen verschiedenen DSL-Anschlüssen zur Anwendung kommt und zudem herstellerabhängig ist, wird im Folgenden lediglich die Funktionsweise von Dynamic DNS sowie die Gesamtlösung für den mobilen Fernzugriff über DSL auf das Unternehmensnetz beschrieben (Bild 1).

Grundlagen DSL – das DSL-Angebot der T-Com

Die digitale Übertragungstechnik DSL[1] ist eine Zugangstechnik für den Teilnehmeranschluss, die sich durch zwei grundlegende Eigenschaften auszeichnet:

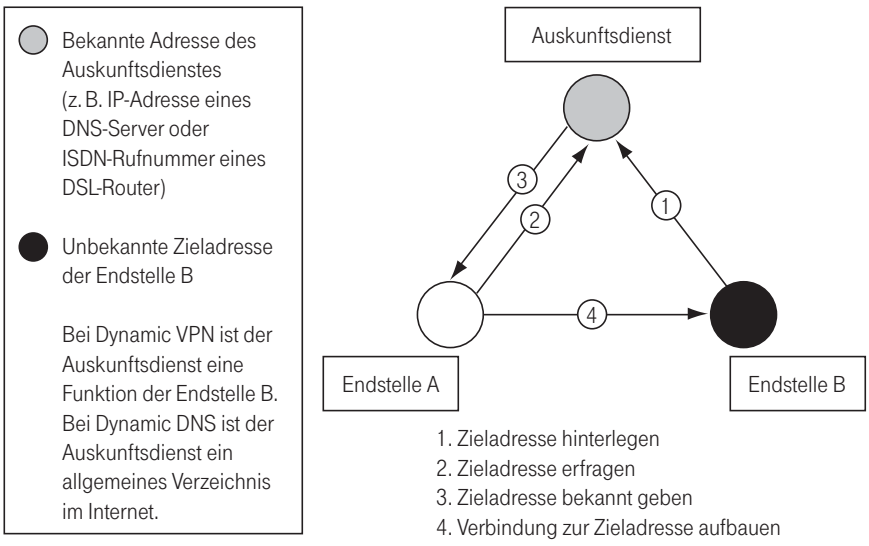
- DSL nutzt die vorhandenen Kupferdoppeladern des Telefonnetzes und kann somit ohne kapitalintensive und langwierige Infrastrukturmaßnahmen in vielen Ortsnetzbereichen bereitgestellt werden.
- DSL bietet wesentlich höhere Übertragungsraten als mit Analogmodem oder ISDN und ermöglicht somit eine Vielzahl neuartiger Internet-Dienste (z. B. Video on Demand).

Die vorhandenen Kupferdoppeladern lassen sich theoretisch bis zu einer Grenzfrequenz von 1,1 MHz nutzen. Der analoge Telefonverkehr belegt jedoch nur einen Frequenzbereich bis etwa 4 kHz. Für eine ausreichende Sprachverständigung genügt bereits ein Frequenzband von 300 Hz bis 3 400 Hz. Durch die Belegung des bisher ungenutzten Frequenzbereichs oberhalb von 4 kHz mit Hilfe der DSL-Technik lassen sich entfernungsabhängig Übertragungsgeschwindigkeiten von theoretisch bis zu 8 Mbit/s erzielen. Mit Hilfe einer Frequenzweiche, dem so genannten Splitter, werden Schmalbandverkehr (z. B. Telefon, Fax, Modem) unterhalb von 4 kHz und Breitbandverkehr (DSL) oberhalb von 4 kHz getrennt. Daher kann über eine Kupferdoppelader telefoniert werden, während zur gleichen Zeit Daten übertragen werden.

Es gibt eine Vielzahl verschiedener DSL-Verfahren (Bild 2). Die wichtigsten Varianten sind

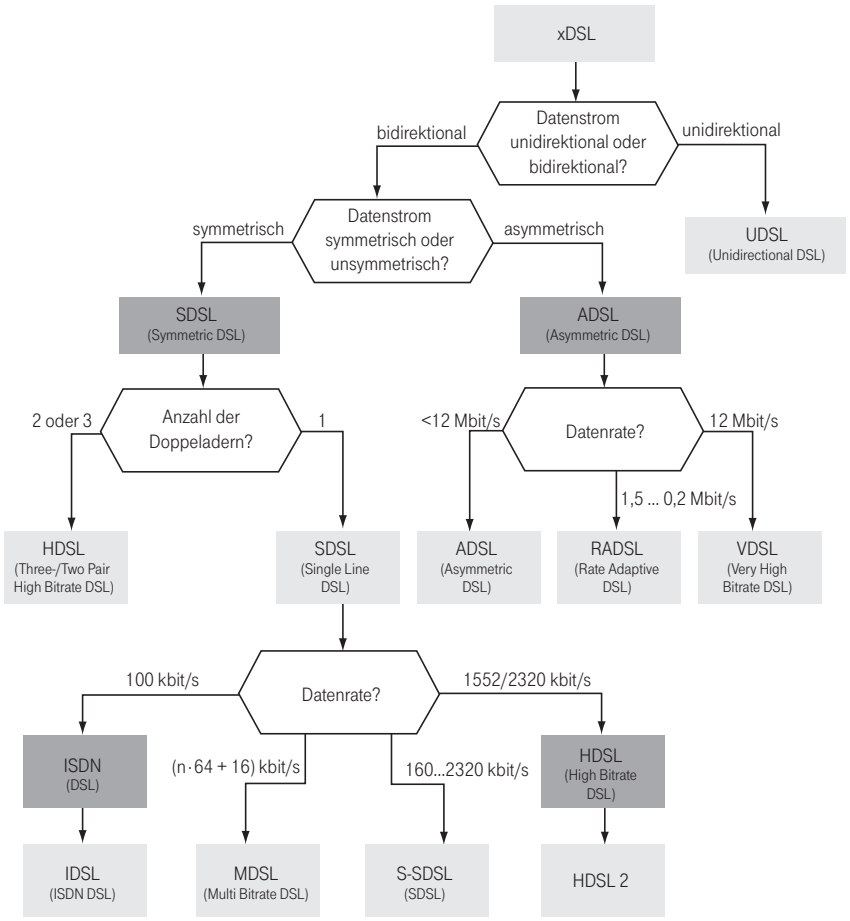
[1] Siehe hierzu „DSL – die Technik", Nachrichten – Neuerungen, Unterrichtsblätter Nr. 2/2003, S. 111 ff. [2].

Bild 1 Schematische Funktionsweise eines Auskunftsdienstes



DNS Domain Name System/Server
DSL Digital Subscriber Line
IP Internet Protocol
VPN Virtual Private Network

Bild 2 **DSL-Varianten**



DSL Digital Subscriber Line

ADSL (Asymmetric DSL), SDSL (Symmetric DSL), HDSL (High Bitrate DSL), SHDSL (Symmetric High Bitrate DSL) sowie VDSL (Very High Bitrate DSL) und wurden mit Ausnahme von SDSL von der International Telecommunication Union (ITU) standardisiert. Die Tabelle zeigt die wichtigsten Varianten und deren Kennzahlen im Überblick.

Die maximal erzielbare Datenrate hängt entscheidend von der Entfernung des DSL-Modems zu der jeweiligen DSL-Vermittlungsstelle (DSL-Access Multiplexer = DSLAM) ab. Für den Parallelbetrieb von Sprach- und Datenübertragung kommt entweder – wie bei ADSL – die oben erwähnte Splittertechnik zum Einsatz, oder die Integration der Sprachdaten wird mit Hilfe von Voice over ATM (VoATM) oder Voice over IP (VoIP) vorgenommen.

Die am häufigsten vorkommenden Varianten sind ADSL und SDSL. In Deutschland ist überwiegend die ADSL-Variante verbreitet, weil diese die größte Entfernung zur DSL-Vermittlungsstelle erlaubt und auf Grund der asymmetrischen Übertragungsbandbreiten für die normale Internet-Nutzung im Massenmarkt am besten geeignet ist. Die SDSL-Technik hingegen ist eher im Bereich der Unternehmensnetze (z. B. für VPN-Lösungen) die bessere Wahl, weil hier das Nutzungsverhalten keine starke Asymmetrie aufweist. Für die Einrichtung von ADSL sind folgende Voraussetzungen zu erfüllen:

- Telefonanschluss (T-ISDN oder T-Net)
- Zugang zu einem ISP (Internet Service Provider), der die DSL-Technik unterstützt (z. B. T-Online)
- DSL-Modem oder DSL-Router sowie ein
- PC mit Ethernet-Karte

Der Zugang zu DSL wird in der Regel gegen ein festes monatliches Grundentgelt überlassen. Das nutzungsabhängige Entgelt ist an den jeweiligen Internet Service Provider zu entrichten. Die meisten ISP bieten hier eine Vielzahl unterschiedlicher Tarife, angefangen von Zeit- oder Volumentarifen mit oder ohne Budgets bis hin zu Pauschalangeboten (Flat-Rate-Angebote) für eine unbegrenzte Nutzung. Gerade die Flat-Rate-Angebote sind für Internet-basierte Einwahllösungen in Kombination mit Dynamic DNS für viele Kunden interessant.

Die Interneteinwahl über DSL wird wie bei jeder anderen Zugangsart (z. B. über ISDN) mit Hilfe des Point to Point Protocol (PPP, RFC[2] 1661) vorgenommen. Da die Schnittstelle zwischen DSL-Modem und PC auf Grund der höheren Datenraten jedoch über Ethernet ausgeführt ist, kommt hier als spezielle Variante das Protokoll PPP over Ethernet (PPPoE, RFC 2516) zur Anwendung.

Fast alle ISP bieten den DSL-Zugang nur mit einer dynamischen IP-Adresszuteilung an. Bei diesem Verfahren ändert sich die IP-Adresse bei jeder Einwahl. Der Grund hierfür liegt in der allgemeinen Knappheit an offiziellen IP-Adressen. Auf Grund der dynamischen IP-Adresszuteilung können die vorhandenen IP-Adressen effektiver genutzt werden, weil sie nur für aktive Verbindungen belegt werden und nicht fest einem Nutzer bzw. Anschluss zugeordnet sind.

Grundlagen DNS

Der Domain Name Service[3] (DNS, RFC 1034, 1035) ist der zentrale Auskunftsdienst im Internet, bei dem jede beliebige IP-Adresse unter einem festen Namen, dem so genannten Domain Name oder Host Name – oft wird auch vom FQDN (Fully Qualified Domain Name) gesprochen –, in einem verteilten Verzeichnis hinterlegt und abgefragt werden

[2] **RFC:** Abk. Request for Comments. Sammlung von Empfehlungen, Artikeln und Standards (RFC-Standards), in denen netzrelevante Konventionen und allgemeine Informationen zum Internet festgehalten sind. Als RFC sind auch die Anregungen und Verbesserungsvorschläge bezeichnet, die die Teilnehmer des Internets beim so genannten RFC-Editor einreichen.

[3] Siehe hierzu den Beitrag „Einführung in die Technik der Computernetze – Teil 3“, Unterrichtsblätter Nr. 12/2003 sowie Internet-Glossar, Unterrichtsblätter Nr. 2/2001, S. 81.

Tabelle Datenraten und Entfernungen bei xDSL

Name	Max. Datenrate (Downlink)	Max. Entfernung zur DSL-Vermittlungsstelle
ADSL	1,5 Mbit/s – 8 Mbit/s	Bis 5,5 km
SDSL	2 Mbit/s	Bis 3 km
HDSL	1,5 Mbit/s – 2 Mbit/s	Bis 4 km
SHDSL	4,6 Mbit/s	Bis 4 km
VDSL	13 Mbit/s – 55,2 Mbit/s	0,3 km – 1,4 km

kann. Der DNS wird in der Regel bei jedem Seitenaufruf in einem Web-Browser vom Anwender unbemerkt in Anspruch genommen, um die vom Benutzer angegebene URL (Uniform Resource Locator) in eine IP-Adresse zu übersetzen. Nur mit Hilfe der IP-Adresse der gewünschten Seite kann erst eine IP-Verbindung zu dem entsprechenden Server aufgebaut werden. Da sich Menschen jedoch besser Namen als numerische IP-Adressen merken können, ist DNS unverzichtbar.

Das DNS-System ist hierarchisch organisiert. Innerhalb dieser Hierarchie wird die Zuständigkeit für die Auflösung einzelner Domain Names jeweils an die zuständige DNS-Serverinstanz delegiert. Hierdurch wird vermieden, dass jeder einzelne Domain Name und jede einzelne IP-Adresse in einem einzigen DNS-Server bekannt sein muss. Auf Grund der Größe des Internets und der damit verbundenen Vielzahl der IP-Adressen ist ein zentralisiertes Verfahren aus administratorischen Gründen nicht praktikabel. Domain Namen werden nach einem festgelegten Schema entsprechend RFC 1035 vergeben. Anhand dieses Schemas lässt sich jeweils eindeutig erkennen, welcher DNS-Server innerhalb der Server-Hierarchie für die Auflösung der IP-Adresse zuständig ist. Jeder Domain Name endet mit einer so genannten Top Level Domain (TLD) wie z. B. „.de“, „.net“ oder „.com“ und kann zusätzlich beliebig viele Subdomains enthalten:

<Domain Name> := <Subdomain n>. ... <Subdomain 1>.<Top-Level-Domain>.

Insgesamt sind maximal 255 Zeichen erlaubt, wobei jede Subdomain bzw. TLD maximal 63 Zeichen umfassen darf. Zulässig sind die Buchstaben ‚a‘ bis ‚z‘ sowie die Ziffern ‚0‘ bis ‚9‘. Zwischen Groß- und Kleinbuchstaben wird nicht unterschieden. Eine aktuelle Erweiterung erlaubt zudem seit kurzem auch Umlaute wie z. B. ä, ö, ü.

Das DNS-System ist als Baumstruktur organisiert (Bild 3). Den Ursprung dieses Baums, die so genannte Root-Level Domain, und gleichzeitig die höchste Ebene, bilden die so genannten Root-Server, die die Top-Level Domains verwalten. Die Top-Level Domains kennzeichnet nach der Root-Level Domain die erste Ebene innerhalb der Domain-Hierarchie. Danach folgen Second-Level Domains sowie beliebig viele Subdomains. Die DNS-Server jeder Ebene enthalten neben den IP-Adressen für die entsprechende Hierarchiestufe selbst zusätzlich Verweise auf nachgeordnete DNS-Server der nächsten Ebene, die für die jeweilige Subdomain zuständig sind bzw. an die die Adressauflösung für die jeweilige Subdomain delegiert wurde.

Nach diesem Prinzip wird erreicht, dass das gesamte DNS-System dezentral verwaltet und betrieben werden kann, ohne für jeden einzelnen Domain-Namen und jede einzelne IP-Adresse weltweite Absprachen treffen zu müssen. Stattdessen wird einmalig das Organisationsprinzip festgelegt und die Zuständigkeiten delegiert. Domain-Namen, die weder vom jeweiligen DNS-Server selbst noch innerhalb der jeweiligen Subdomain-Struktur aufgelöst werden können, werden an die jeweils nächst höhere Hierarchiestufe zurückdelegiert.

Der Domain-Name „roemer.homedns.org“ und die dazugehörige IP-Adresse ist zu finden unter der Top-Level-Domain „.org“ im DNS-Server der zweiten Ebene, der für die Subdomain „homedns.org“ zuständig ist.

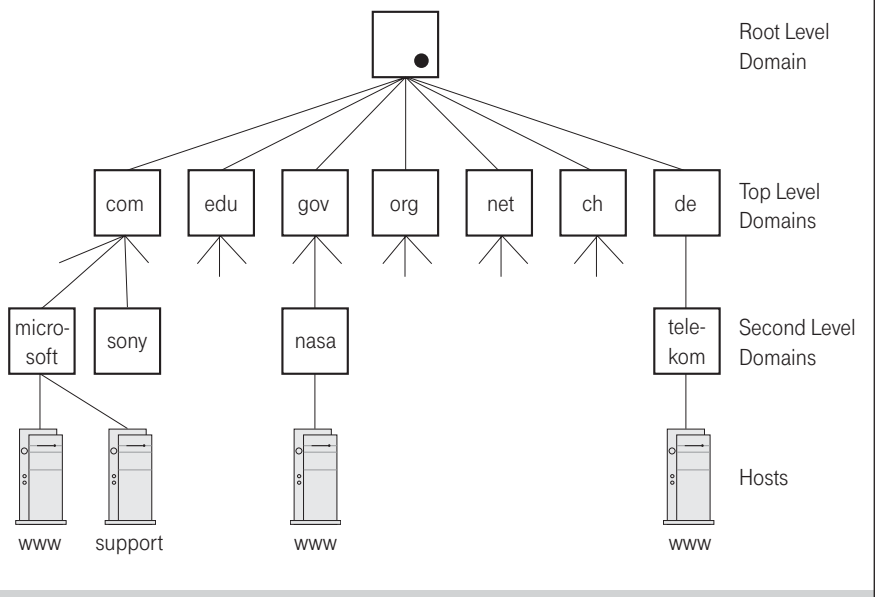
Verwendete Abkürzungen

ADSL	Asymmetric Digital Subscriber Line
DNS	Domain Name System/Server
DSL	Digital Subscriber Line
DSLAM	DSL-Access Multiplexer
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
HDSL	High Bitrate Digital Subscriber Line
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point-Tunneling Protocol
RFC	Request for Comments
SDSL	Symmetric Digital Subscriber Line
SHDSL	Symmetric High Bitrate Digital Subscriber Line
SSL	Secure Socket Layer
T-DSL	DSL-Anschluss der T-Com
T-ISDN	ISDN-Anschluss der T-Com
T-Net	Analoger Anschluss der T-Com
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TTL	Time To Live
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VDSL	Very High Bitrate Digital Subscriber Line
VoATM	Voice over Asynchronous Transfer Mode
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

Falls beispielsweise in einem Browser dieser Domain-Name als URL angegeben wird, so wird eine rekursive[4] Namensauflösung in folgenden Teilschritten vorgenommen:

[4] **rekursiv:** zurückgehend (bis zu bekannten Werten).

Bild 3 **DNS-Hierarchie**



WWW World Wide Web

- Anfrage des Browser an den vordefinierten DNS-Server des jeweiligen Internet Service Provider (ISP).
- Anfrage des DNS-Server des ISP an den DNS-Server der TLD „.de“. Der „.de“-Domain Server liefert die IP-Adresse des DNS-Server der TLD „.org“, weil sich diese IP-Adresse mit hoher Wahrscheinlichkeit in seinem lokalen Cache[5] befindet. Anderenfalls würde der „.de“-DNS-Server an die Root Level Domain verweisen.
- Anfrage des DNS-Server des ISP am TLD-DNS-Server „.org“. Dieser DNS-Server antwortet mit der IP-Adresse des DNS-Server der Subdomain „homedns.org“.
- Anfrage des DNS-Server des ISP am DNS-Server der Subdomain „homedns. org” und Auflösung der zugeordneten IP-Adresse.
- Der DNS-Server des ISP liefert dem Browser die gewünschte IP-Adresse zu „roemer.homedns.org“.

Sofern ein DNS-Server bereits kurze Zeit zuvor die gleiche Anfrage erhalten hat, so liegt die entsprechende IP-Adresse in manchen Fällen bereits in seinem lokalen Cache vor und kann direkt ausgegeben werden, ohne weitere DNS-Server einzuschließen. In der Regel werden Host-Namen und zugehörige IP-Adresse mehrere Tage im lokalen Cache eines DNS-Server vorgehalten. Die Zeitdauer, wie lange diese Informationen im Cache gespeichert werden, wird als Time To Live (TTL) bezeichnet. Dieses Verfahren erspart wiederholte Anfragen und verkürzt somit die Zeit für die IP-Adressauflösung. Nachteilig ist, dass Änderungen der jeweiligen IP-Adresse wie beispielsweise bei Dynamic-DNS-Verfahren sich gegebenenfalls nur sehr langsam im DNS-System verbreiten. Sollte sich innerhalb der TTL die zugehörige IP-Adresse ändern, so führen weitere DNS-Anfragen zu einem falschen Ergebnis.

Funktionsweise Dynamic DNS

Dynamic DNS ist innerhalb des DNS-Systems ein Verfahren zur namensbasierten IP-Adressauflösung einer dynamisch sich ändernden IP-Adresse. Dieses Verfahren wird häufig dazu genutzt, um die jeweils aktuelle IP-Adresse eines DSL-Anschlusses zu hinterlegen und bekannt zu geben. Beispielsweise lässt sich damit ein Fernzugriff für Wartungsarbeiten am eigenen Netz (Remote Control) oder eine Einwahllösung für Außendienstmitarbeiter realisieren. Auch ein einfacher Datenaustausch per File Transfer Protocol (FTP) im privaten Bereich oder eine Web-Kamera kann damit problemlos eingerichtet werden.

Ein Dynamic-DNS-Server ist ein normaler DNS-Server, der über eine zusätzliche externe „Updater-Schnittstelle“ jederzeit die Möglichkeit zur Aktualisierung des IP-Adresseintrags bietet. Diese Aktualisierungen bzw. Updates werden innerhalb des DNS-Systems im Rahmen einer Namensauflösung über normale DNS-Anfragen verbreitet. Wichtig ist jedoch hierbei, dass das TTL-Feld innerhalb der DNS-Antwort auf einen sehr niedrigen Wert (meistens einen Wert von maximal einigen Minuten – Dyndns.org setzt den Wert auf 60 Sekunden) eingestellt wird. Der TTL-Wert gibt an, wie lange ein IP-Adresseintrag im lokalen Cache eines DNS-Server vorgehalten wird, bis der für den zugehörigen Domain Name jeweils zuständige DNS-Server erneut kontaktiert werden muss. Um innerhalb des DNS-Systems eine möglichst geringe Reaktionszeit auf einen Update für eine IP-Adresse zu erhalten, muss der TTL-Wert möglichst klein sein.

Das Bild 4 veranschaulicht die grundlegende Funktionsweise sowie den Gebrauch von Dynamic DNS für die mobile Einwahl mit Hilfe eines VPN Client über GPRS oder UMTS auf einen DSL-Anschluss mit dynamischer IP-Adresse.

Um für mobile Einwahl-Clients erreichbar zu sein, muss der DSL-Anschluss permanent mit dem Internet verbunden bleiben. Dies bedeutet, dass der DSL-Router oder ein Updater- Programm auf einem internen Rechner hinter dem DSL-Anschluss die Verbindung ständig überwachen und sich bei Unterbrechung automatisch wieder mit dem ISP verbinden muss (1). Bei jeder neuen Einwahl erhält der DSL-Anschluss eine neue IP-Adresse. Diese Adresse wird über eine Updater-Schnittstelle (z. B. über HTTPS[6]) vom DSL-Router oder dem Updater-Programm auf dem

[5] **Cache:** engl. für Lager, Versteck, Zwischenspeicher. Oberbegriff für Zwischenträger von Daten zweier kommunizierender Funktionseinheiten. Durch seine Speicherfunktion kann ein Cache beispielsweise unterschiedliche Übertragungsraten zwischen Sender und Empfänger kompensieren. Beispiel: Cache zur Geschwindigkeitskompensation zwischen Computer und Drucker.

[6] **HTTPS:** HTTP Secure. Bezeichnung für die Kombination des auf der Anwendungsschicht platzierten Protokolls HTTP (Hypertext Transfer Protocol) mit dem darunter liegenden Sicherheitsprotokoll SSL (Secure Socket Layer). Diese Kombination gilt als eigenständiges Kommunikationsprotokoll und dient der verschlüsselten Datenübertragung, beispielsweise zum Austausch von Kreditkartendaten.

Dynamic-DNS-Server unter dem entsprechenden Domain Name (z. B. „roemer. homedns. org“) sowie unter Verwendung eines Passworts automatisch aktualisiert (2). Danach kann die neue IP-Adresse über eine entsprechende DNS-Namensauflösung von jedem beliebigen Internet-Rechner abgefragt werden (3).

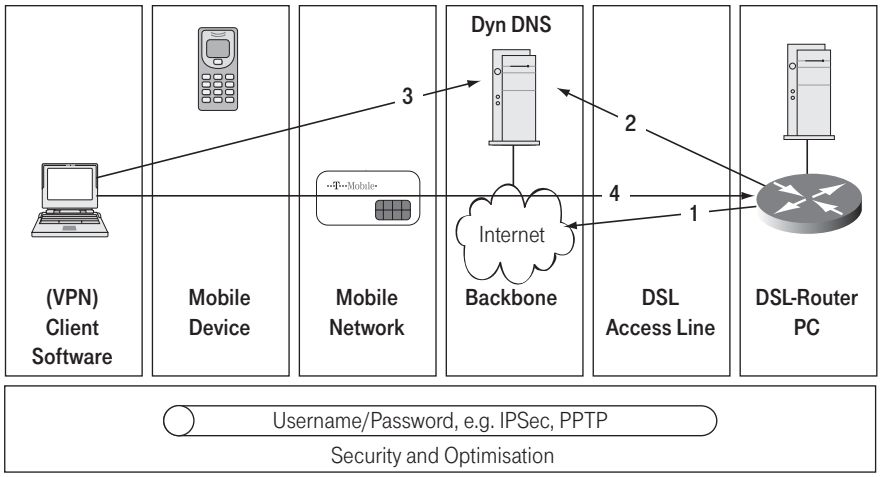
Wählt man sich nun beispielsweise über GPRS ins Internet ein[7] und gibt in der Eingabeaufforderung seines Rechners das Kommando „ping –w 3000 roemer.homedns.org“ ein, so wird zunächst über den DNS-Server seines ISP (hier: der DNS des Mobilfunk-Provider) die aktuelle IP-Adresse in Erfahrung gebracht, bevor der „Ping“ vom Rechner am jeweiligen DSL-Anschluss beantwortet wird. Die Angabe „–w 3000“ ist eine Angabe in Millisekunden und bestimmt die maximale Wartedauer des Ping-Kommandos bis zum entsprechenden Reply. In GPRS-Netzen kann das Roundtrip-Delay zeitweilig bei über zwei Sekunden liegen. Die Wartedauer für das Ping-Kommando sollte daher entsprechend gewählt werden, um einen Time-Out zu vermeiden.

In der Regel wird bei Einwahllösungen über das Internet eine VPN-Software eingesetzt, die eine gesicherte Datenverbindung zwischen den beiden Verbindungsendpunkten mit Hilfe von Authentisierung, Verschlüsselung und Tunneling bereitstellt. Die VPN-Verbindung wird hierbei stets vom VPN Client beispielsweise zu einem VPN Gateway hinter dem DSL-Anschluss aufgebaut (4). Da die IP-Adresse des DSL-Anschlusses jedoch nicht von vornherein bekannt ist, muss im VPN Client der Domain Name hinterlegt sein, der mit Hilfe von Dynamic DNS automatisch aktualisiert und vor Verbindungsaufbau vom VPN Client über eine DNS-Abfrage in Erfahrung gebracht wird.

Im Internet gibt es bereits ein breites Angebot an Dynamic DNS. Für den privaten Gebrauch sind fast alle Angebote kostenlos. Die bekanntesten Anbieter sind:

- www.dyndns.org
- www.hn.org
- www.ods.org
- dyns.cx
- gnudip2.sourceforge.net

Bild 4 Funktionsweise von Dynamic DNS



1 Der DSL-Router verbindet sich mit dem Internet und erhält eine neue IP-Adresse
2 Der DSL-Router oder ein Updater-Programm aktualisiert automatisch den DNS-Eintrag im Dynamic-DNS-Server mit der neuen IP-Adresse
3 Der VPN-Client nutzt den zugeordneten DNS-Namen, um die entsprechende Ziel-IP-Adresse von einem DNS-Server im Internet zu erfragen
4 Der VPN-Client baut einen VPN-Tunnel (z. B. mit IPSec) zur Ziel-IP-Adresse auf

DNS	Domain Name System/Server	IPSec	Internet Protocol Security
DSL	Digital Subscriber Line	PPTP	Point-to-Point Tunneling Protocol
IP	Internet Protocol	VPN	Virtual Private Network

Zurzeit ist die Updater-Schnittstelle noch nicht standardisiert. Die Hersteller von Updater-Programmen bzw. DSL-Routern unterstützen in der Regel jedoch die Updater-Schnittstellen von mehreren Dynamic-DNS-Anbietern.

Beispiel DynDNS.org

Der bekannteste Anbieter von Dynamic DNS ist „dyndns.org“. Das Anlegen eines Dynamic-DNS-Account ist denkbar einfach und benötigt wenige Minuten. Der Nutzer muss hierzu lediglich auf die Startseite www.dyndns.org gehen, dort unter „Account“ den Unterpunkt „Creat Account“ auswählen, danach die Nutzungsbedingungen akzeptieren, Username und Password wählen, seine E-Mail-Adresse angeben sowie einen DNS-Name unterhalb von vorgegebenen Subdomains eingeben (z. B. roemer. homedns.org).

Anschließend erhält er per E-Mail eine Bestätigung, die er innerhalb von 48 Stunden auf einer speziellen Internetseite ebenfalls quittieren muss.

Als nächstes muss ein Updater-Programm auf dem eigenen PC installiert werden. Die Aufgabe dieses Programms ist es, die Internet-Verbindung zu überwachen und bei jeder Unterbrechung automatisch eine Neueinwahl sowie eine Aktualisierung der neuen IP-Adresse im Dynamic-DNS-Server vorzunehmen. Dyndns.org bietet auf seiner Internet-Site eine vielfältige Auswahl verschiedener Updater-Programme (z. B. DeeEnEs oder Direct Update) sowie verschiedene Empfehlungen. Die Updater-Programme lassen sich in der Regel problemlos als Systemdienst installieren, der bei jedem Hochfahren des Windows-Betriebssystems jeweils automatisch im Hintergrund gestartet wird. Bevor der Updater jedoch genutzt werden kann, muss der jeweilige Dynamic-DNS-Provider, in diesem Fall dyndns.org, sowie Username und Passwort des jeweiligen Account im Updater-Programm hinterlegt werden.

[7] Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access“, Unterrichtsblätter Nr. 3/2001, S. 168 ff.

Verwendet man für die DSL-Einwahl einen DSL-Router, so kann je nach Fabrikat auf die Installation eines Updater-Programms verzichtet werden. Viele Hersteller unterstützen bereits verschiedene Dynamic-DNS-Lösungen durch eine eigene Updater-Funktion im DSL-Router.

Die vollständige Spezifikation der Updater-Schnittstelle zwischen Updater und Dynamic-DNS-Server ist unter http://www.dyndns.org/developers/specs/index.html zu finden. Als Protokoll kommt HTTP/1.0 (Hypertext Transfer Protocol) oder HTTP/1.1 zur Anwendung. Alternativ kann die Übertragung mit Hilfe von SSL (Secure Socket Layer, HTTPS) gesichert werden.

Eine Aktualisierung kann für den Domain-Name „roemer.homedns.org“ und der neuen IP-Adresse „80.133.124.66“ beispielsweise mit folgendem Befehl veranlasst werden:

```
http://roemer:<password>@members.
dyndns.org/nic/update?system=dyndns&
hostname=roemer.homedns.org&myip=
80.133.124.66&wildcard=OFF&mx=mail.
exchanger.ext&backmx=NO&offline=NO
```

Erläuterung
Die Parameter **„roemer:<password>“** entsprechen der Username-Passwort-Kombination, die sich der Nutzer beim Anlegen des Account ausgesucht hat.

Der Domain-Name „members.dyndns.org“ entspricht der Zieladresse des Update-Server (oder allgemein des Host). Auf diesem Host wird unter dem Pfad „/nic/“ der Server-seitige Update-Prozess unter dem Namen „update“ gestartet. Diesem Programm werden die Parameter hinter dem „?“ übergeben. Er liefert einen Ergebnis-Code, der als Antwort per http zurückgegeben wird.

Die einzelnen Parameter werden durch das Trennzeichen „&“ voneinander getrennt: Der Parameter „system“ gibt hier an, dass es sich um einen Dynamic-DNS-Service handelt. Der Parameter „hostname“ definiert den Dynamic-DNS-Name, für den die IP-Adresse mit dem Parameterwert von „myip“ aktualisiert werden soll. Mit dem Parameter „wildcard“ wird angegeben, ob die gewählte Subdomain, in diesem Beispiel „roemer“, auch unter einem beliebigen vorangestellten Namen wie z. B. www.roemer.homedns.org erreichbar sein soll. In unserem Beispiel ist diese Option nicht aktiviert. Der Parameter „mx“ steht für „Mail Exchanger“ und ist nur von Interesse, wenn man einen eigenen Mail-Server betreibt, der E-Mails für diese Subdomain abwickeln soll. Die Werte der übrigen Parameter werden von Dyndns.org vorgegeben.

Der oben angegebene Befehl ist in der Kommandozeile des Browser anzugeben. Das Passwort ist in diesem Beispiel bewusst nicht angegeben.

Ein Updater-Programm muss mit diesen Parametern genauso wie ein Browser eine entsprechende http-GET-Message (s. RFC 2616) erzeugen, um die geforderten Parameter an den Updater-Server zu übergeben. Die entsprechende GET-Message sieht für das obige Beispiel wie folgt aus:

```
GET /nic/update?system=dyndns&host-
name=roemer.homedns.org&myip=
80.133.124.66&wildcard=OFF&mx=mail.
exchanger.ext&backmx=NO&offline=NO
HTTP/1.0 Host: members.dyndns.org
Authorization: Basic roemer:<password>
```

Diese GET-Message wird im Nutzdatenfeld über TCP (Transmission Control Protocol) an den Port 80 des Update-Server geschickt. Falls der Update erfolgreich war, antwortet der Server in diesem Beispiel mit:

```
good 80.133.124.66
```

Fehler-Codes sind der Spezifikation von dyndns.org zu entnehmen.

Anwendungsbeispiel – File Access über GPRS

Ein einfaches Anwendungsbeispiel von Dynamic DNS ist der Datenaustausch per FTP. Hierzu wird neben einem Dynamic-DNS-Account lediglich ein zusätzlicher FTP-Server benötigt. Einen geeigneten FTP-Server findet man z. B. kostenlos unter www.cerberus.com. Die Installation ist selbsterklärend.

Nach der Installation müssen zunächst FTP-User mit entsprechenden Profilen angelegt werden. Ein FTP-User hat einen User-Name (z. B. „roemer“), ein Passwort sowie ein Root-Verzeichnis mit Lese- und/oder Schreibrechte. Als Root-Verzeichnis kann jedes beliebige Unterverzeichnis im lokalen Netz bzw. auf dem lokalen Rechner definiert werden. Der jeweilige FTP-User kann sich anschließend lediglich innerhalb dieses Root-Verzeichnisses bewegen und entsprechend seines Rechteprofils Dateien hochladen, herunterladen oder gar löschen. Die meisten FTP-Server, so auch Cerberus, legen bei der Installation automatisch den User „Anonymous“ an. Dieser User zeichnet sich u. a. dadurch aus, dass er kein Passwort benötigt und sich frei im gesamten Dateisystem bewegen darf. Aus Sicherheitsgründen sollte dieser User auf jeden Fall gelöscht werden.

Verbindet man nun den ersten PC über den DSL-Anschluss mit dem Internet und gibt danach auf einem zweiten PC, der ebenfalls mit dem Internet verbunden sein muss (z. B. über GPRS), die URL „ftp:\\roemer@roemer.homedns.org“[8] im Browser ein, so erscheint als nächstes ein Pop-Up-Fenster, in dem man nach dem FTP-Password für den User „roemer“ gefragt wird. Nach Angabe dieses Passworts erscheint im Browser automatisch das entsprechende Root-Verzeichnis und man kann – wie vom Windows Explorer gewohnt – zwischen Verzeichnissen wechseln sowie Dateien hin- und herschieben.

Schlussbetrachtung

In Bezug auf Sicherheit sollten vertrauliche bzw. unternehmenskritische Daten nicht ohne zusätzlichen Schutz über das Internet übertragen werden. Zudem sollte der Zugriff auf unternehmenskritische Netze zusätzlich

[8] Die URL „ftp:\\roemer@roemer.homedns.org“ setzt sich in diesem Beispiel aus dem FTP-Usernamen „roemer“, dem Trennzeichen „@“ sowie dem Dynamic-DNS-Namen „roemer.homedns.org“ zusammen.

mit Hilfe einer Firewall abgesichert werden. Das beschriebene Beispiel soll lediglich zeigen, wie einfach Dynamic DNS ohne spezielle Kenntnisse, die über diesen Artikel hinausgehen, genutzt werden kann. Weitergehende Sicherheitsaspekte werden bewusst ausgeklammert, weil sie nicht in unmittelbaren Bezug zu Dynamic DNS stehen und daher über das Thema dieses Beitrags hinausgehen.

(Ge)

Literaturhinweise

[1] LANLine, Nr 10, Oktober 2003, S. 83 ff.

[2] LANline, Nr.10, Oktober 2002, S. 56 ff.

[3] c't, Nr. 10, 2003, S. 210 ff.