2.4 Elemente des Internets

„Das" Internet gibt es nicht, sondern eine Vielzahl verbundener Teilnetze, die zusammen ein weltumspannendes Netz bilden. Grundlage bilden aber gemeinsame Absprachen, was den Verkehr betrifft. Wir haben das TCP/IP Protokoll bereits kennen gelernt. Aber lokale Netze können mit anderen Protokollen, wie Ethernet, angeschlossen werden.

Viele Anforderungen sind zu erfüllen, um die vielen kleinen Netze mit Sicherheit und Zuverlässigkeit zum Gesamtnetz zu verbinden. Die einzelnen Anforderungen und Elemente werden in diesem Kapitel näher betrachtet.

2.4.1 Client, Server und Host

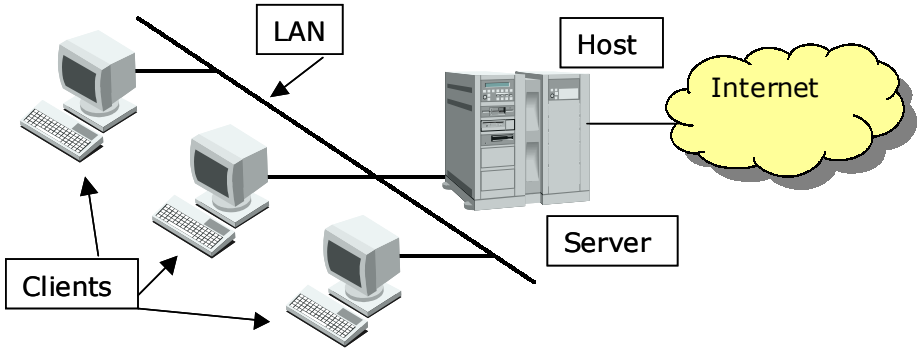

Abbildung 2-11: Client-Server Prinzip

Wir kennen bereits aus unserer Büroumgebung das Client-Server-Prinzip. Daten werden nicht auf den Büro-PC dezentral gespeichert, sondern zentral auf einem Server. Dies vermindert den Aufwand für Administration, Backup und Teamworking. Grundsätzlich muss ein Datenübertragungsnetzwerk eingesetzt werden. Viele Firmen nutzen hier das Ethernet als LAN-Lösung in verschiedenster Konfiguration. Dieses kann aber mit TCP/IP überlagert werden und somit sind die angeschlossenen lokalen Rechner im Internet adressierbar.

Host

Ein Client hat im Netzwerk eine feste Hardware-Adresse, die dem Typ des Netzwerkes entspricht. Diese nennt man auch **MAC-Adresse (Media Access Control)** und sind für die Adressierung der einzelnen Rechner auf dem LAN eingeführt. Die Länge ist meist 48 bit.

Als Host bezeichnen wir einen Server, der permanent mit dem Internet oder Intranet verbunden ist, z. B. mit Inhalten wie Homepages, Dateisystemen, etc.

2.4.2 Bridges

Abbildung 2-12: Bridge

Die lokalen Netze sind nur von sehr geringen Ausmessungen. Die einzelnen Netze werden als Segmente bezeichnet und können über Bridges (Brücken) zusammengeschaltet werden. Es erfolgt keine Vermittlung der Daten, sondern nur Daten mit Adressen aus dem anderen Teilnetz werden durchgeschaltet. Verkehr, der nur innerhalb eines Teilnetzes adressiert ist, bleibt in diesem Segment ohne Weiterleitung und belastet die Bridge nicht. Die Übertragung erfolgt auf Grund der Auswertung der MAC[26]-Adresse der zu übertragenen Pakete.

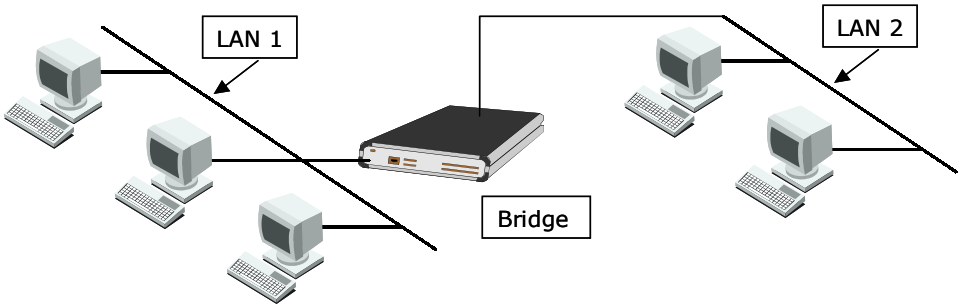

Abbildung 2-13: Kopplung zweier Netzsegmente mit einer Bridge

Notizen

2.4.3 Switches

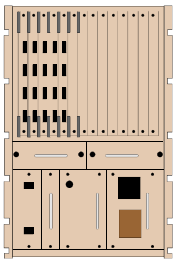

Abbildung 2-14: Switch

Switches (*engl.:* Schalter) haben mehr Möglichkeiten als Bridges, obwohl sie auch Teilnetze (**Segmente**) miteinander verbinden. Sie ermöglichen exklusive und den Bedarf entsprechende Verbindungen zwischen angeschlossenen Segmenten oder Netzelementen. Hier werden meist Netzelemente mit hohem Bandbreitebedarf an einen Eingang (Port) angeschlossen, die den Verkehr direkt vermitteln können, ohne das restliche Netz zu belasten. Die Regeln werden innerhalb des Switches in Adresstabellen mit entsprechenden Portverknüpfungen

[26] MAC - Media Access Control

angegeben. Ist die Zieladresse nicht bekannt, kann eine Weiterleitung z. B. in alle angeschlossenen LAN-Segmente erfolgen. Es erfolg im Switch kein IP-Routing. Anwendungsfälle sind z. B. Serververbindungen oder Workstations von Arbeitsgruppen, die ein hohes Datenaufkommen haben. Diese Datenverbindungen werden direkt im Switch geschaltet und belasten nicht den Rest des Netzes.

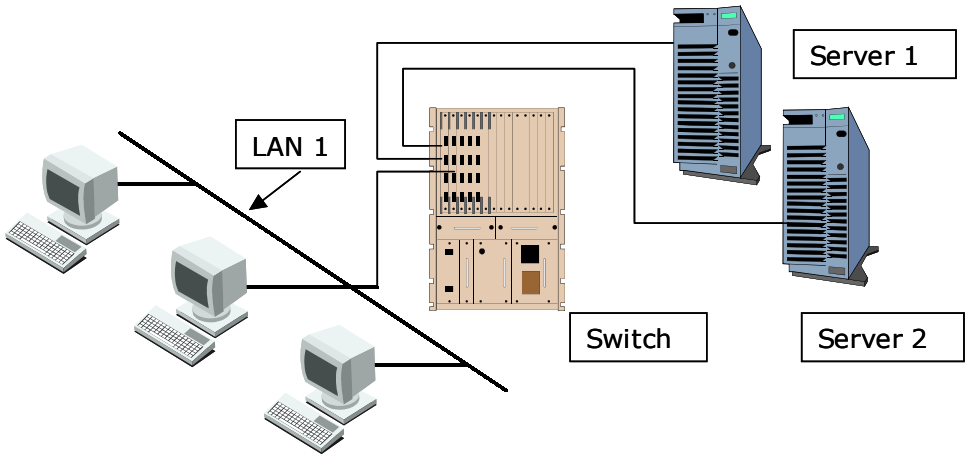

Abbildung 2-15: Betrieb von Servern an einem Switch

2.4.4 Router

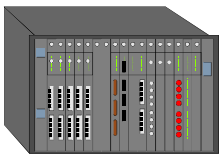

Abbildung 2-16: Router

Während Bridges für die Kopplung zweier Netzsegmente sorgen, können Router auch mehrere Segmente miteinander verbinden und den Verkehr zielgerichtet weiterleiten. Aus diesem Grund müssen Routingregeln vorhanden sein. Idealerweise kann sich ein Router selbst

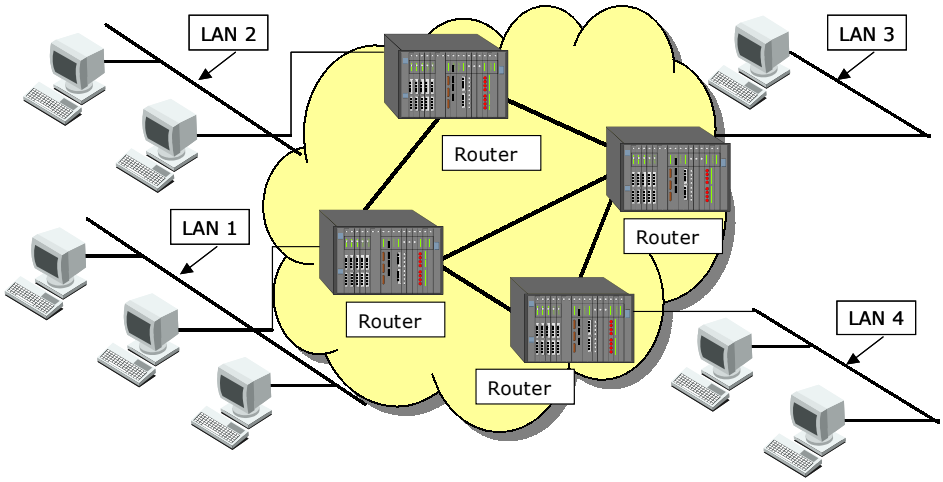

Abbildung 2-17: Router verbinden Teilnetze und leiten Verkehrsströme

orientieren, welche Netze in der Nachbarschaft angeschlossen sind und wie deren Adressraum aussieht. Treffen Pakete mit entsprechender Zieladresse ein, kann somit der Verkehr zielgerichtet weitergeleitet werden.

Router werten die IP-Adresse der Datenpakete aus, im Gegensatz zur Bridge, die nur die physikalischen MAC-Adressen der Netzwerkkarten auswertet. Router bilden das Vermittlungsnetzwerk des lokalen Netzwerks und des Internets und werden auch Netzknoten genannt.

2.4.5 Firewalls

Mit Firewall bezeichnet man Schutzmassnahmen, um ein LAN oder Teile davon innerhalb eines Unternehmens gegen Zugriff abzuschotten. Dies kann auch für den Verkehr ausserhalb gelten, z. B. für Zugriffe ins und vom Internet. Ziele sind Unterbindung unerlaubter Eingriffe, Schutz vor Virenattacken und Zugriffschutz auf sensible Daten. Die Datensicherheit wird durch vielfältige Möglichkeiten erhöht, z. B.

- Beschränkung der extern nutzbaren Dienste (z. B. Unterbindung von Internetzugriffen)
- Beschränkung von Zugriffsrechten (Lese-/Schreibrechte)
- Authentisierungsmechanismen
- Datenverschlüsslung

Packet Filter

Es können alle Aktionen im Firewall protokolliert werden, um nachträglich Eingriffe fest zu stellen. Es gibt mehrere Arten von Firewalls, die sich im Konzept unterscheiden. Meist werden in Routern sogenannte in **Packet Filter** eingesetzt. Diese analysieren die Adressen von Sender und Empfänger im IP-Datagramm. Mittels einer Tabelle wird entschieden, ob eine Verbindung dieser beiden Instanzen zulässig ist, oder nicht. Dies ist aber nur sinnvoll, wenn die IP-Adressen der betreffenden Instanzen fest vorgegeben sind und nicht dynamisch vergeben werden (siehe auch DHCP).

Notizen

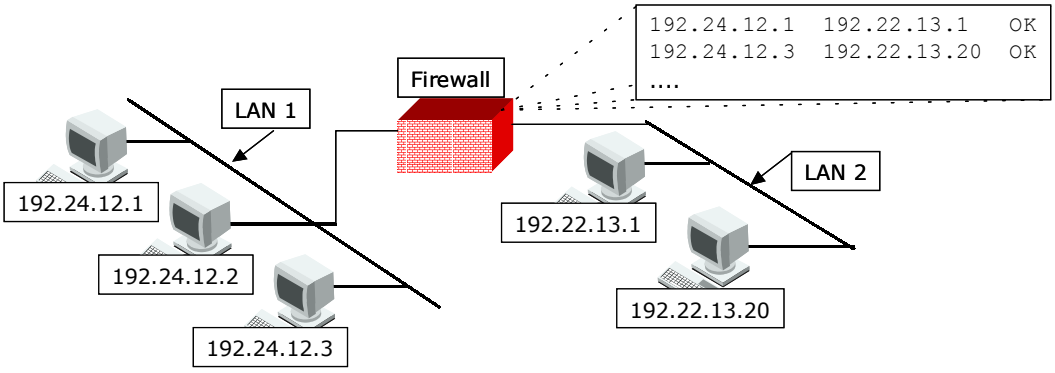

Abbildung 2-18: Firewall mit Adress-"Screening"-Tabelle

2.4.6 Gateway

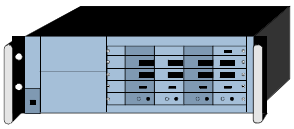

Abbildung 2-19: Gateway

Mit Gateway bezeichnen wird Geräte, die nicht nur Routingfunktionen besitzen, sondern zusätzlich noch Protokollumsetzungen durchführen. Dies ist notwendig, wenn Netze mit unterschiedlichen Übertragungs-Protokollen arbeiten, z. B. ein TCP/IP-Netz an ein X.25-Netz gekoppelt wird. Zum Beispiel könnte ein Gateway den Mailverkehr zwischen unterschiedlichen Systemen und Netzwerken ermöglichen, wie von Lotus Notes und einem Internet-Mailserver. Meist benutzen wir den generischen Ausdruck **IWU (Interworking Unit)**, wenn wir eine Kopplung von verschiedenen Netzen über Bridges, Router oder Gateways beschreiben.

Proxy Gateway

Eine spezielle Form von Gateway, bzw. Routern, stellt das **Proxy Gateway** dar. Haben wir bisher mit der IP-Adresse immer auf den jeweiligen Hostrechner direkt Kontakt aufgenommen, stellt ein Proxy einen Stellvertreter der nachfolgenden Rechner dar. Eine Verbindung zu den nach dem Proxy geschalteten Hosts geht immer über den Proxy, der als einziger von aussen direkt über eine IP-Adresse erreichbar ist. Der Proxy fordert nun von den nachgeschalteten Servern die Daten an und stellt diese im Proxy zur Verfügung. Somit kann kein Verkehr direkt auf die nachfolgenden Rechner gelangen und die Sicherheit ist deutlich erhöht. Weitere Merkmale von Proxies sind auch:

- Jeder Dienst kann einzeln konfiguriert werden (HTTP, FTP, etc.)
- Authentisierung (Login) erforderlich

- Zwischenspeicherung der Daten in lokalem Speicher
- Ggf. Kombination mit Gateway zur Protokollumsetzung für erhöhte Sicherheit

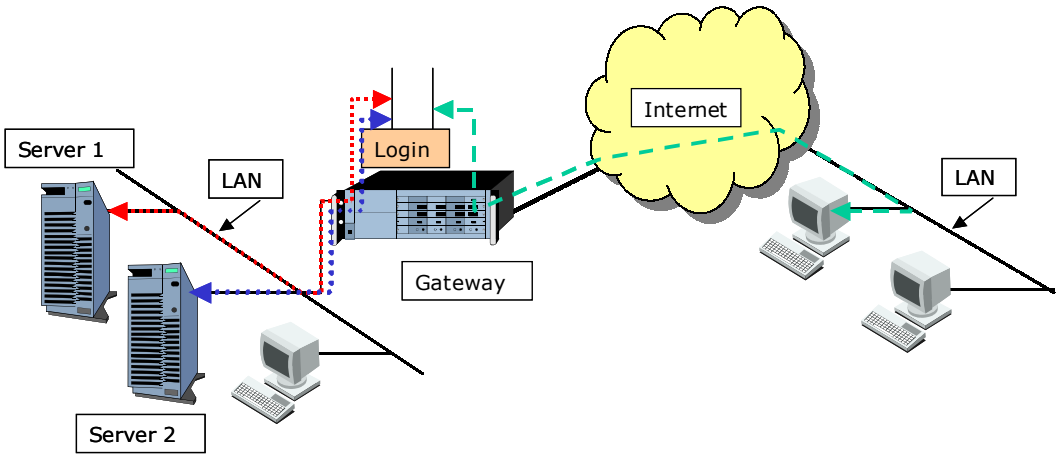

Abbildung 2-20: Prinzip eines Gateways

2.4.7 Dynamische Host Konfiguration

IP-Adressen sind ein sehr kostbares Gut. Wir haben erfahren, dass es nur einen sehr beschränkten Adressraum gibt. Für Nutzer von Klasse-C-Netzen haben wir 256 Hostadressen zur Verfügung. Um nicht durch nicht benötigte Server den Adressraum zu blockieren, werden Internet-Adressen oftmals nur verliehen (IP-Lease). Der Host ist nur während der Gültigkeit über IP erreichbar. Wird die IP-Adresse zurückgegeben kann kein IP-Verkehr mehr empfangen oder versendet werden. Die Vergabe von IP-Adresse geschieht meist über das **Dynamic Host Configuration Protocol – DHCP.** Dieses vergibt aus einem Pool von verfügbaren Adressen zeitlich gültige Zuweisungen. Sind feste Adressen (z. B. beim Einsatz von Firewalls) notwendig, werden diese nicht fremd vergeben, sondern immer nur den zugeordneten Hosts.

GPRS

Beim Einsatz von GPRS in Mobilfunknetzen werden nur bei einem **GPRS Attach** IP-Adressen vergeben. Nur dann ist das Mobilgerät „online". Auch für die Einwahl per PC über ein Telefonnetz wird während der Sitzung eine temporäre IP-Adresse vom Serviceprovider verliehen.

Notizen

2.4.8 Domain Name Service - DNS

Die IP-Adressen entsprechen dem Sinn nach den Telefonnummern im Telekommunikationsnetz. Die einzelnen Netze erhalten eine Netz-Adresse, die zentral vergeben wird und lokale Netze kennzeichnet. Z. B. kann eine Firma die Klasse-C-Adresse 192.12.5.x erhalten. Damit kann innerhalb des Routerverbundes diese Teilnetz erreicht werden, mit den zugeordneten lokalen Hosts. Innerhalb der Subnetze wird weitervermittelt. Somit erhalten wir ein logisches Gesamtnetz.

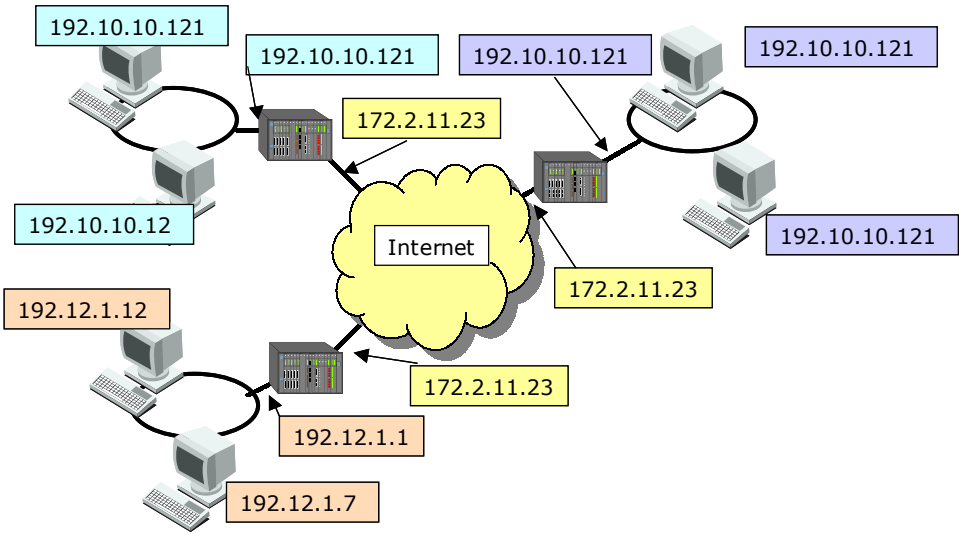

Abbildung 2-21: Adressierungen der Subnetze

Da wir aber diese Nummern teilweise nur geliehen haben und bei einem Umzug in ein anderes Netz die IP-Adresse nicht mehr gültig wäre, muss ein Verfahren gefunden werden, dass mehr Benutzerfreundlichkeit enthält.

Statt der numerischen IP-Adresse verwenden wir sprechende Namen, z. B. wird www.p-manent.de in 192.44.151.1 umgesetzt. Diese Umsetzung muss in Tabellen enthalten eines Servers enthalten sein: dem Name-Server oder DNS[27]-Server. Gültige Namen enthalten eine TOP-Level Domain, gefolgt von Sub-Domain und Servern.

Top Level Domains

Die **TOP-Level Domains (TLD)** sind fest vergeben und kennzeichnen meist das Land, das die Domain vergeben hat, nicht wo der Host lokalisiert ist. Ausser den USA, die ohne Landeskennungen verschienene Klassifizierungen haben, verwendet die Länder zweistellige TOP-Level Domains. Eine kurze Übersicht gibt folgende Tabelle:

[27] DNS - Domain Name System

TLD-Endung	Beschreibung
.COM	Kommerzielle Organisationen und Firmen
.ORG	Organisationen, allgemein
.EDU	Erziehungs- und Bildungseinrichtungen
.GOV	Amerikanische Regierung
.MIL	Amerikanisches Militär
.DE	Deutschland
.AT	Österreich
.UK	Grossbritannien
.SE	Schweden
.EU	Europäische Gemeinschaft

Notizen

Die Sub-Domain ist frei wählbar und kann gegen eine Registrierungsgebühr reserviert werden.

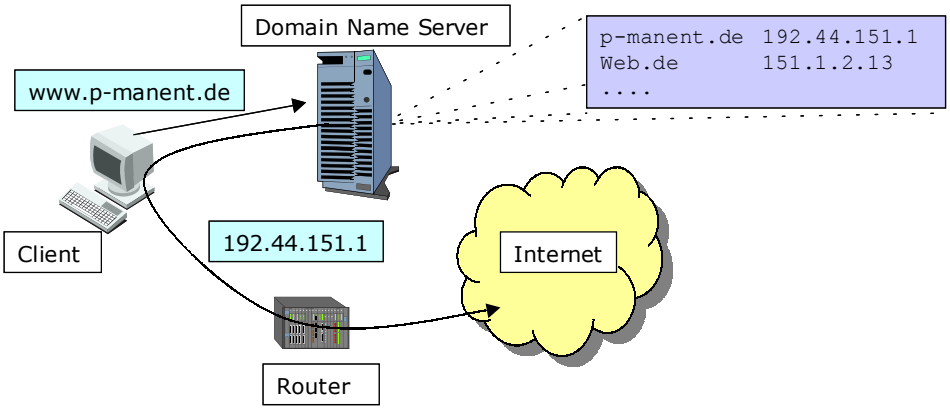

Abbildung 2-22: Namensauflösung mit DNS-Server

Der DNS-Server muss die Namensauflösung durchführen. Wird die Internetpräsenz www.p-manent.de angegeben, so kann damit kein Router arbeiten. Zuerst muss der Name aufgelöst und in die richtige IP-Adresse umgewandelt werden.

Zieht eine Internetpräsenz, z. B. www.p-manent.de, bei einem Providerwechsel um, dann wird eine neue IP-Adresse vergeben.

Da meist nur der Name verwendet wird, kann der DNS (solange er die Informationen über die neue Adresse schon hat!) die neue korrekte Adresse dem Router mitteilen.

Das DNS ist ein verteiltes System. Nicht jeder DNS-Server hat alle Informationen über Netzadressen weltweit. Kann der Name lokal nicht aufgelöst werden, wird ein übergeordneter DNS-Server angefragt, der weitere Informationen hat. Auch sorgen Protokolle für die ständige Aktualisierung der Daten.

Notizen

2.4.9 Network Access Server

Viele Rechner sind nicht ständig mit dem Internet verbunden. Dies gilt beispielsweise für den Heim-PC, der nur per Anwahl über das öffentliche Telefonnetz zeitweise verbunden wird. Diese zeitweise Verbindung mit dem Internet wird meist über Internet Service Provider (ISP) angeboten. Da die Kunden eine Rechnung für die genutzten Leistungen erhalten und auch persönliche Bereiche einrichten können, ist eine Authentisierung notwendig. Dies kann über den **Remote Authentication Dial-In User Service (RADIUS)** geschehen.

RADIUS-Server

Ein entsprechender Server steht in Verbindung mit dem Wählzugangs-Server. Erfolgt ein externer Rufaufbau, werden über das verschlüsselte RADIUS-Protokoll vom RADIUS-Server die Freigaben erteilt. Dies erfolgt nach erfolgreicher Authentisierung durch den Kunden, z. B. Abfrage von Kennung und Passwort. Der RADIUS-Server ist mit einer Kundendatenbank verbunden, wo er Zugangsdaten und Profile des Kunden erhält. Dies ist im Mobilfunk ähnlich mit dem HLR gelöst. Der RADIUS-Server hat aber keine Routing- oder Vermittlungsfunktionen.

2.4.10 Directory Services

Directory Services (Verzeichnisdienste) bieten die Möglichkeit, Kundendaten abzulegen. Dies kann als eine Art Karteikartensystem angesehen werden. Da viele Systeme unterschiedliche Formate je nach Betriebssystem vorsehen, wurde z. B. mit **X.500** ein übergreifender Standard geschaffen. Um die Daten aus den Benutzerdatenbanken abzufragen ist ein spezielles Protokoll, das **Lightweight Directory Access Protocol (LDAP)** vorgesehen.

Ein entsprechender Verzeichnisserver, der über dieses Protokoll z. B. an einen RADIUS-Server angeschlossen ist, nennt man oft LDAP-Server oder Directory-Server.

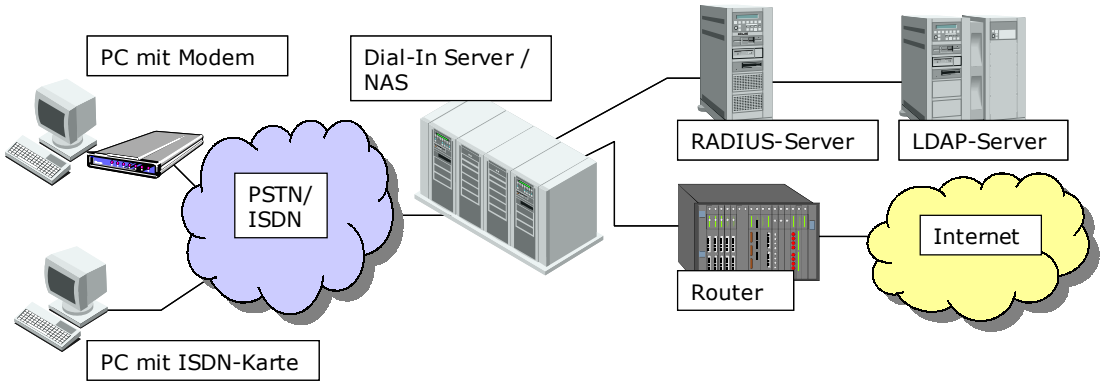

Abbildung 2-23: RADUIS- und LDAP-Server

Notizen

2.4.11 Fragen

Mehrere Antworten können richtig sein.

1. Die einfache Kopplung von zwei Netzwerksegmenten wird vorgenommen durch

a) eine Bridge
b) einen Router
c) einen Switch
d) eine Gateway

2. Welche Netzelemente sorgen für das Routing des IP-Datagrammes?

a) Bridges
b) Router
c) Hosts
d) Clients

3. Die Aufgabe einer Firewall ist es

a) Verbindungen zu blocken
b) Unterschiedliche Netze zu verbinden und Daten zu konvertieren
c) Gebührendaten zu erzeugen
d) IP-Adresse zu vergeben

4. Zu dynamischen Vergabe von IP-Adressen verwenden wir z. B.

a) DHCP
b) HTTP
c) FTP
d) LAN

5. Die höchste Hierarchiestufe im DNS heisst

a) TLD
b) Subnetz
c) Segment
d) .COM

6. Mit welchem Konzept kann der Zugriff für Wählverbindungen gesichert werden?

a) LDAP
b) RADIUS
c) TLD
d) WWW