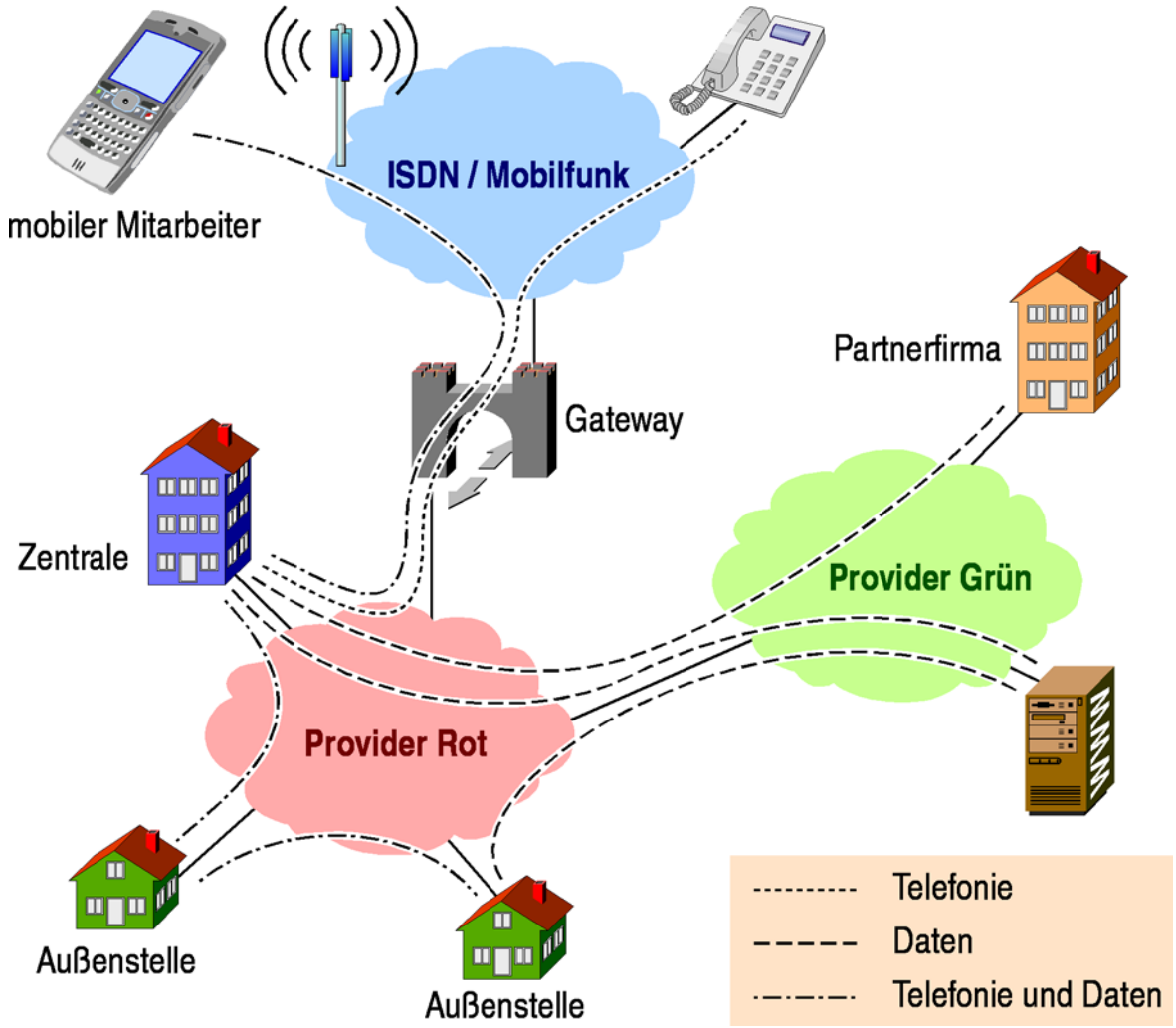
Kapitel 1

Netzwerke – eine Einführung (Auszug)

Zusammenfassung

Dieses Kapitel bietet eine Einführung in die Grundbegriffe der Netzwerktechnik. Der Zweck von Netzwerken wird ebenso klar wie ihr grundsätzlicher Aufbau. Als wesentliche Funktion von Netzwerkkomponenten wird der Begriff Multiplexen besonders genau unter die Lupe genommen. Eine ausführliche Diskussion des Schichtenmodells (OSI-Modell) rundet das Kapitel ab.

1.1 Ein typisches Szenario: Firmennetz



- **Datenströme zwischen den Standorten und innerhalb der Standorte**
- **Kommunikation mit Partnern und mobilen Mitarbeiten**
- **Vielfalt: Sprache, Daten und ggf. Video**

Ein typisches Szenario: Firmennetz

Zentrale und Außenstellen

Als Beispiel für die Welt der Netzwerktechnik soll eine Firma mit mehreren Standorten dienen. Es gibt eine Firmenzentrale, mehrere Außenstellen sowie mobile Mitarbeiter.

Datenströme

Zwischen den Standorten fließen Datenströme. Mitarbeiter greifen von den Außenstellen auf zentrale Server und Datenbanken zu. Ein gleichberechtigter Zugang zu der Zentrale ist auch für mobile Mitarbeiter erforderlich, die mit Smart Phones oder Laptops unterwegs sind. Innerhalb der Standorte müssen Datenströme fließen können, damit Informationen von den Arbeitsplätzen zu den Servern, Druckern und der weiteren Endgeräten fließen können.

Externe Ziele

Neben den firmeninternen Datenströmen sind auch solche zu externen Zielen notwendig. Mit Partnerfirmen wird eine gemeinsame Zuliefererplattform für elektronischen Handel betrieben, und für Recherchen wird der Zugriff auf Web Server benötigt. E-Mail-Verkehr mit Kunden und Partnern ist für die Geschäftsbeziehungen unverzichtbar.

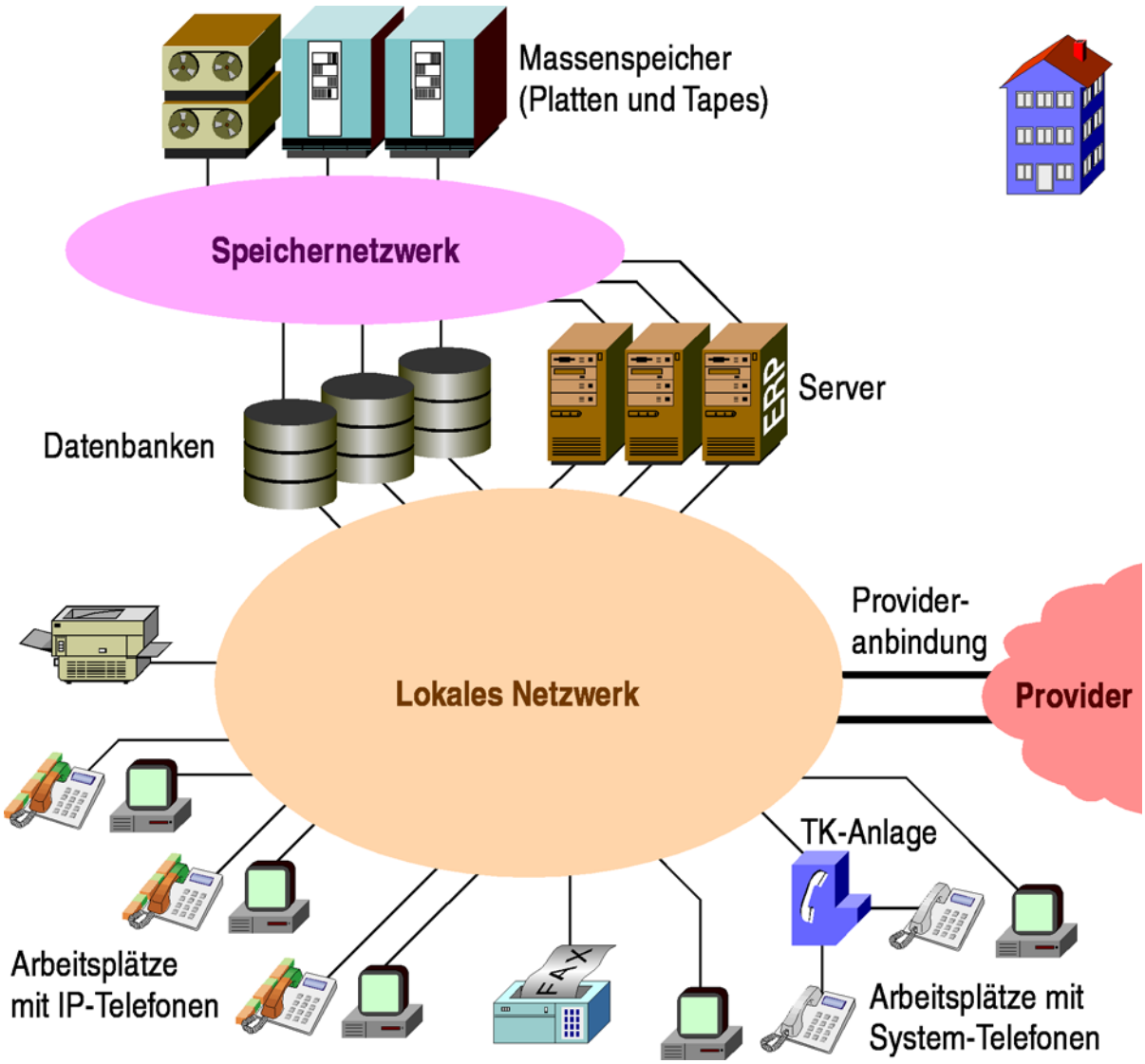
Telefonie und Video

Telefonie sorgt für weitere Vernetzungsanforderungen sowohl innerhalb der Standorte, zwischen den Standorten und zu externen Zielen. Gegebenenfalls wird dies durch Videokommunikation ergänzt – sei es für Videokonferenzen, zu Bildungs- oder auch zu Überwachungszwecken.

Provider

Die Infrastruktur für die Kommunikation über längere Distanzen wird von Providern (Netzwerkanbieter) bereitgestellt. Sie stellen als Mindestdienstleistung den Transport von Datenströmen aller Art (Telefonie und Video eingeschlossen) zur Verfügung. Zwischen verschiedenen Providern bestehen Kopplungen – je nach Technik mit oder ohne Gateway als Umsetzer.

1.1.1 Die Zentrale



- **Arbeitsplätze mit Telefonen, PCs und Peripheriegeräten (Drucker, Fax)**
- **Server und Datenbanken**
- **Massenspeicher**
- **Redundante Provideranbindung**

Die Zentrale

Datenbanken, Server etc.

In der Firmenzentrale finden sich üblicherweise Datenbanken, Server und Massenspeicher. Die Datenbanken enthalten beispielsweise den Datenbestand, der von Enterprise Resource Planning Systems (ERP-Systemen) wie SAP oder Oracle benötigt wird.

Arbeitsplätze und LAN

Weiterhin existieren Arbeitsplätze, die mit PCs, Telefonen und Peripheriegeräten wie Druckern, Kopierern, Scannern oder Faxgeräten ausgestattet sind. Innerhalb der Firmenzentrale wird eine Infrastruktur benötigt, über die Datenströme zwischen den PCs, den Servern und Datenbanken und den Peripheriegeräten fließen können. Eine solche Infrastruktur nennt man LAN (Local Area Network).

Telefonie

Die Telefonie kann in das LAN integriert sein; in diesem Fall verhalten die Telefone sich aus Sicht der Infrastruktur ähnlich wie die PCs. Man spricht auch von Voice over IP (VoIP). Möglich ist aber auch eine separate Realisierung der Telefonie mittels herkömmlicher Telefonanlagen (TK-Anlagen, Private Branch Exchange, PBX).

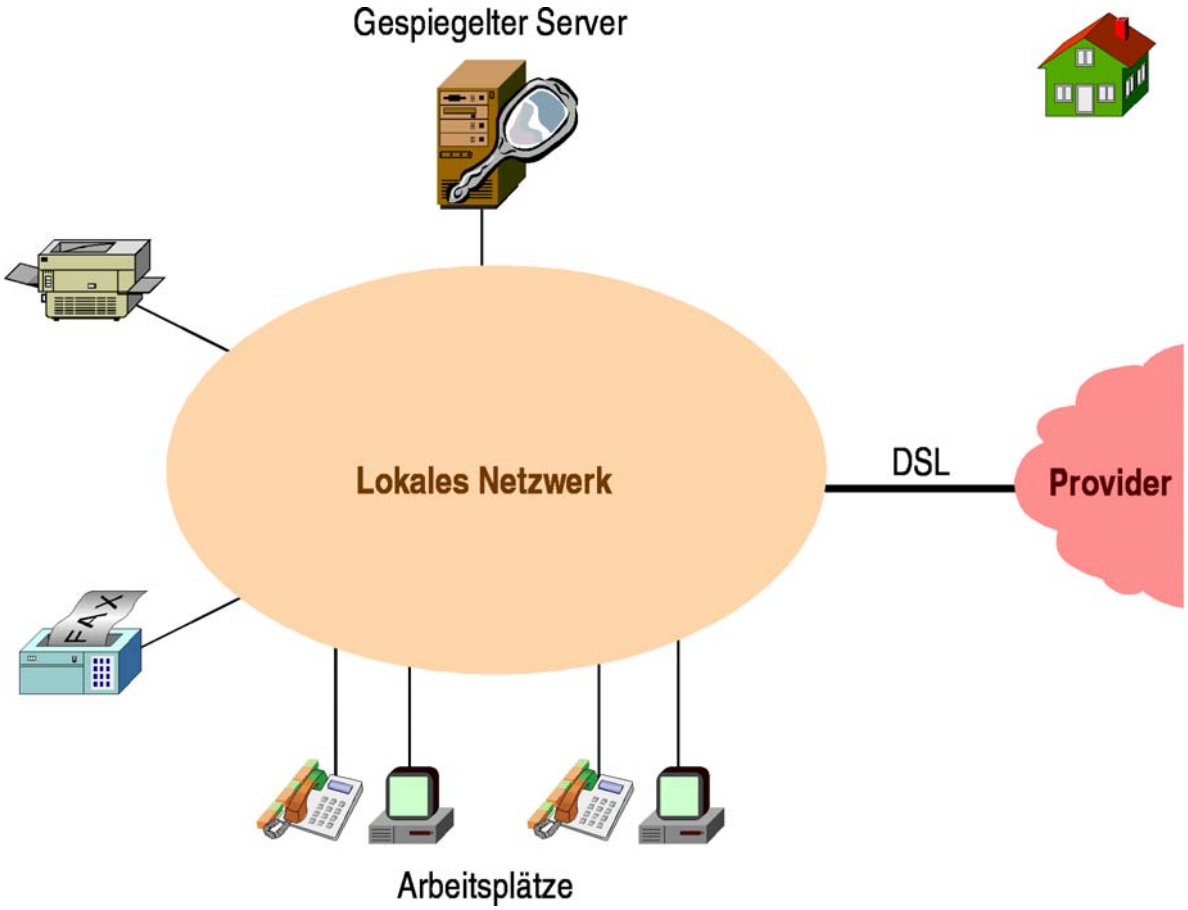
SAN

Massenspeicher – beispielsweise die Archivierung von geschäftlicher Korrespondenz – stellt besondere Anforderungen an die Infrastruktur. In vielen Fällen schafft man dazu ein ausschließlich diesem Zweck gewidmetes Netzwerk – ein Storage Area Network (SAN).

Provideranbindung

Die Anbindung der Firmenzentrale an den oder die Provider ist in doppelter Hinsicht ein Dreh- und Angelpunkt der Firma. Erstens muss sie hochverfügbar und hochperformant sein, damit die Kommunikation mit Außenstellen, Kunden und Partnern stets gewährleistet ist. Zweitens muss sie besonders gesichert sein, damit keine unbefugten Zugriffe von außen erfolgen. Die Anbindung erfolgt oft mittels Festverbindungen.

1.1.2 Die Außenstellen



- **Ebenfalls Arbeitsplätze mit Telefonen, PCs und Peripherie**
- **Einige Server ggf. gespiegelt**
- **Oftmals große Anzahl von Außenstellen**
- **Daher starker Kostendruck bei der Provideranbindung**
- **DSL als preisgünstige Variante**

Die Außenstellen

Ähnlichkeiten und Unterschiede

Die Infrastruktur der Außenstellen unterscheidet sich nicht fundamental von der Zentrale. Allerdings gibt es Unterschiede im Detail.

Kein Speichernetz

Massenspeicher werden in den Außenstellen normalerweise nicht vorhanden sein, so dass auf eigene Speichernetzwerke verzichtet werden kann.

Gespiegelte Server

Eigenständige Server finden sich in der Regel nicht in den Außenstellen, aber in manchen Fällen erweist es sich aus Performance-Gründen als günstig, dort gespiegelte Versionen einiger Server in der Zentrale vorzuhalten. In diesem Fall findet die Kommunikation zwischen Arbeitsplatz-PC und Server lokal statt, und der lokale Server gleicht sich automatisch mit seinem Pendant in der Zentrale ab.

Arbeitsplätze und LAN

Für die Vernetzung der Arbeitsplätze wird, wie auch in der Zentrale, ein LAN benötigt. Ob die Telefone dort direkt an das LAN angeschlossen sind, oder ob eine Telefonanlage (TK-Anlage) benötigt wird, hängt von der Strategie des Unternehmens ab.

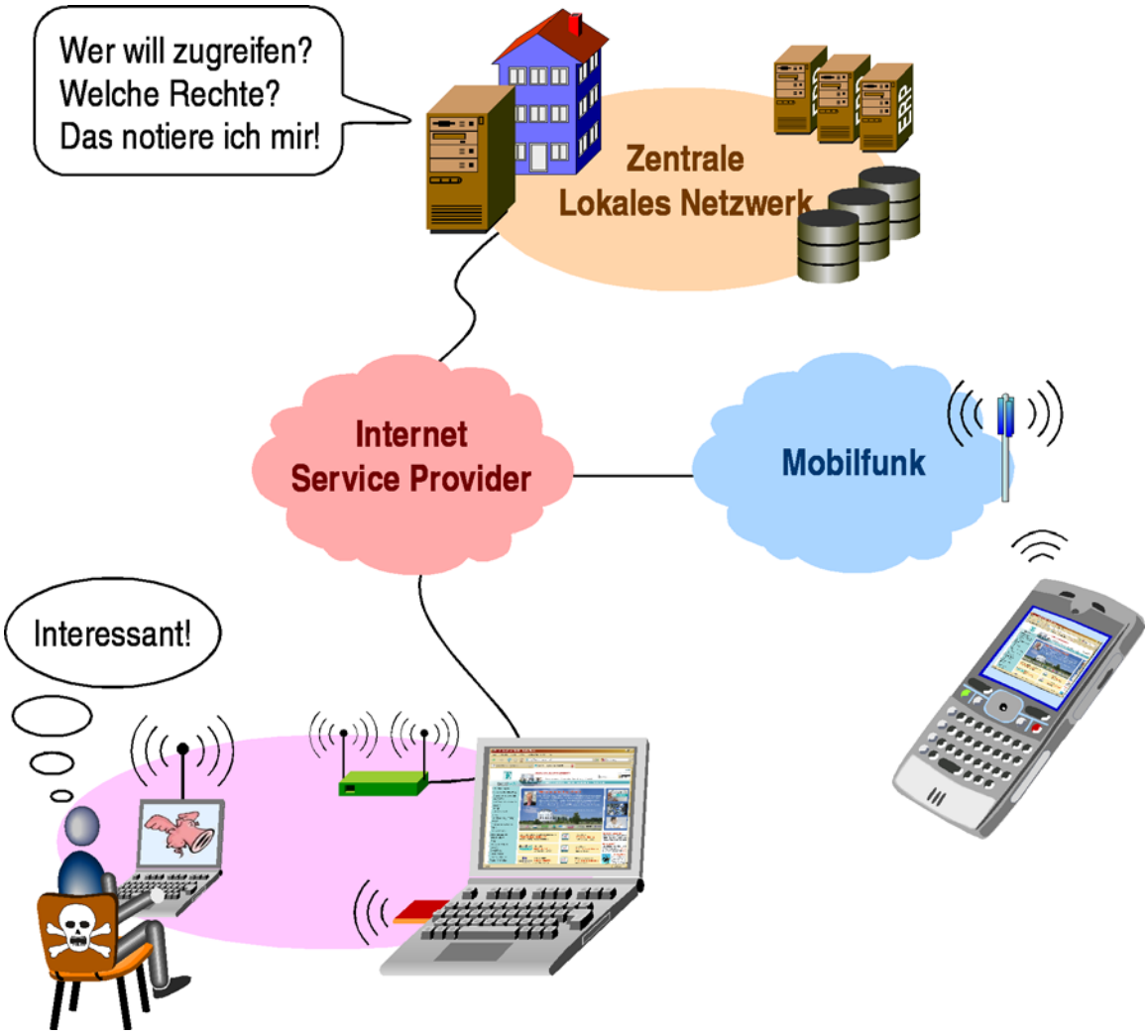
Anbindung mit DSL

Die Provideranbindung wird bei den Außenstellen normalerweise weniger aufwändig ausgelegt als bei der Zentrale. Je mehr Außenstellen anzubinden sind, desto wichtiger ist die Minimierung der Kosten für die einzelne Anbindung, und ein Ausfall einer solchen wird toleriert, wenn er nicht zu häufig vorkommt. Am beliebtesten ist der Einsatz von DSL.

Externe Kommunikation

Die Art und Weise, wie Kommunikation (sei es Daten- oder Sprachkommunikation) mit Zielen außerhalb der Firma erfolgen soll, hängt von der Politik der Firma ab. Sowohl eine zentrale als auch eine dezentrale Lösung ist möglich.

1.1.3 Mobile Mitarbeiter



- **Laptop, Smart Phone oder PDA über Telefonnetz, Mobilfunk oder WLAN**
- **Zentrales Thema: Security**
- **In der Zentrale:**
  - **Authentisierung (Wer?)**
  - **Autorisierung (Welche Rechte?)**
  - **Accounting (Buchführung)**

Mobile Mitarbeiter

Kein fester Arbeitsplatz

Außendienstmitarbeiter, die einen großen Teil ihrer Arbeitszeit nicht an einem festen Arbeitsplatz verbringen, benötigen einen zuverlässigen und gleichzeitig sicheren Zugang zu den Servern in der Zentrale.

Laptops, Smart Phones, PDAs

Als Endgeräte kommen Laptops, Smart Phones oder PDAs (Personal Digital Assistants) in Frage. Die Anbindung an den Provider kann fallsweise per Telefonnetz, Wireless LAN (WLAN) oder auch via Mobilfunk erfolgen. Dabei ist Flexibilität erwünscht – je nach Aufenthaltsort soll jeweils die preisgünstigste und gleichzeitig performanteste Anbindung genutzt werden können.

Im Brennpunkt: Sicherheit

Besonderes Augenmerk ist dabei auf Sicherheit zu richten. Wird das Endgerät gestohlen, muss gewährleistet sein, dass der Dieb nicht in den Besitz wertvoller oder vertraulicher Daten gerät, und dass er keinen Zugriff auf das Firmennetz erreichen kann.

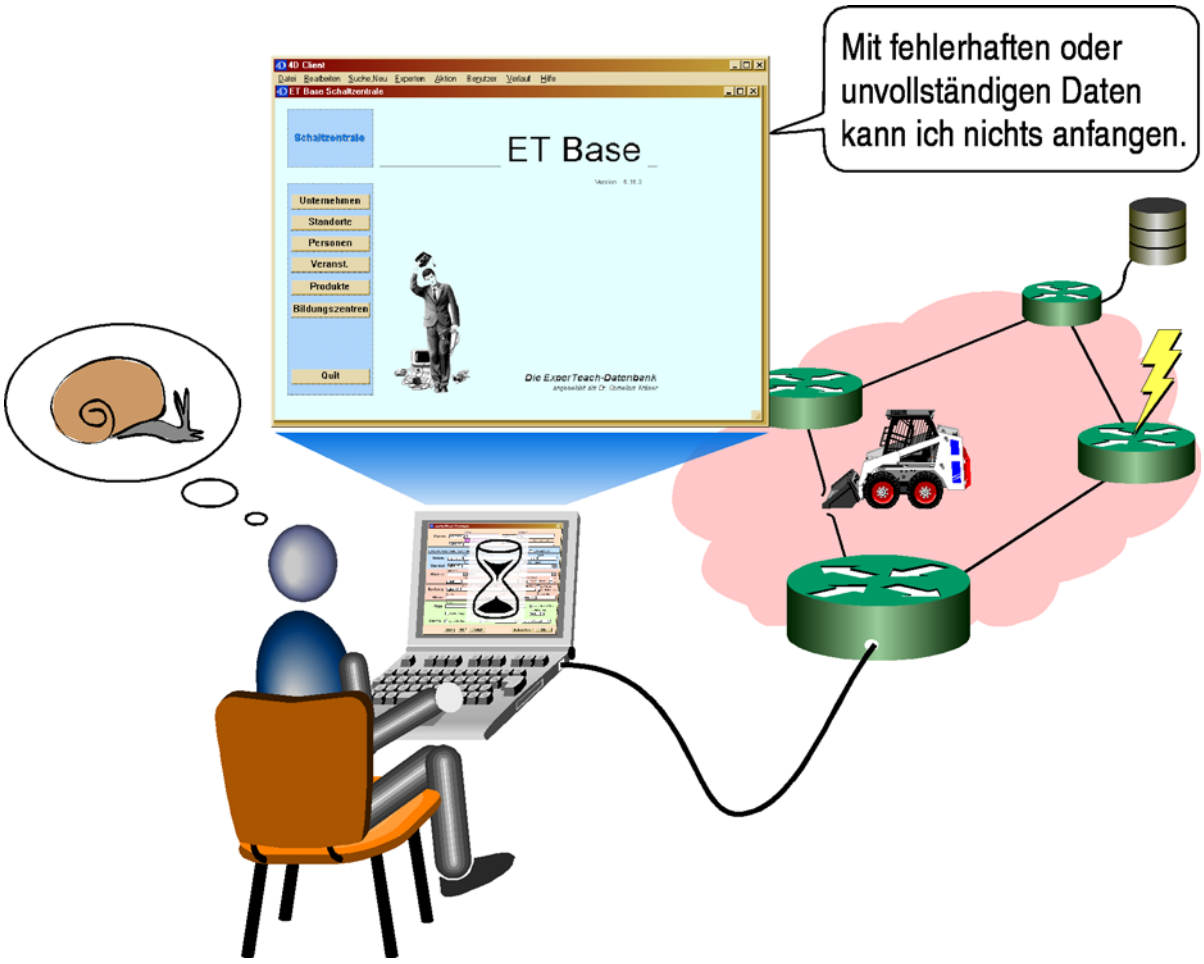
Drahtlos?

Werden drahtlose Technologien benutzt, muss dafür gesorgt werden, dass ein Lauscher keine Chance hat, vertrauliche Daten mitzulesen.

Prüfung in der Zentrale

Nimmt das Endgerät des mobilen Mitarbeiters Kontakt zur Zentrale auf, ist dort dafür zu sorgen, dass die Identität geprüft (Authentisierung, auch Authentifizierung genannt) wird, und dass die zur Person passenden Rechte erteilt werden (Autorisierung). Eine Buchhaltung (Accounting), wer wann, von wo aus, mit wem und wie lange kommuniziert hat, ist aus vielerlei Gründen wünschenswert. Entsprechende Vorkehrungen müssen zu diesem Zweck in der Zentrale getroffen werden.

1.2 Applikationen und Anforderungen



- **Warum Geräte und Standorte vernetzen?**
- **Das eigentliche Ziel: Anwendungen sollen kommunizieren können.**
- **Verschiedene Anwendungen stellen auch verschiedene Anforderungen an das Netz.**
- **Zufriedenheit des Nutzers entscheidet.**

Applikationen und Anforderungen

Standorte? Geräte?

Warum macht man sich die Mühe, Standorte untereinander und Geräte innerhalb von Standorten miteinander zu vernetzen? Die Frage scheint überflüssig zu sein: Natürlich, damit die Geräte miteinander kommunizieren können. Dennoch ist folgende Frage legitim: Was hat man eigentlich davon, wenn Geräte miteinander kommunizieren? In den meisten Fällen geht es gar nicht so sehr um das Gerät an sich, sondern um eine Anwendung, die darauf läuft.

Anwendungen!

Anwendungen können beispielsweise sein:

- Browser,
- Office Software,
- ERP-Systeme,
- Telefonie,
- Videokonferenz,
- Zugriff auf File Server,
- Datenbanken,
- Spiele oder
- E-Mail.

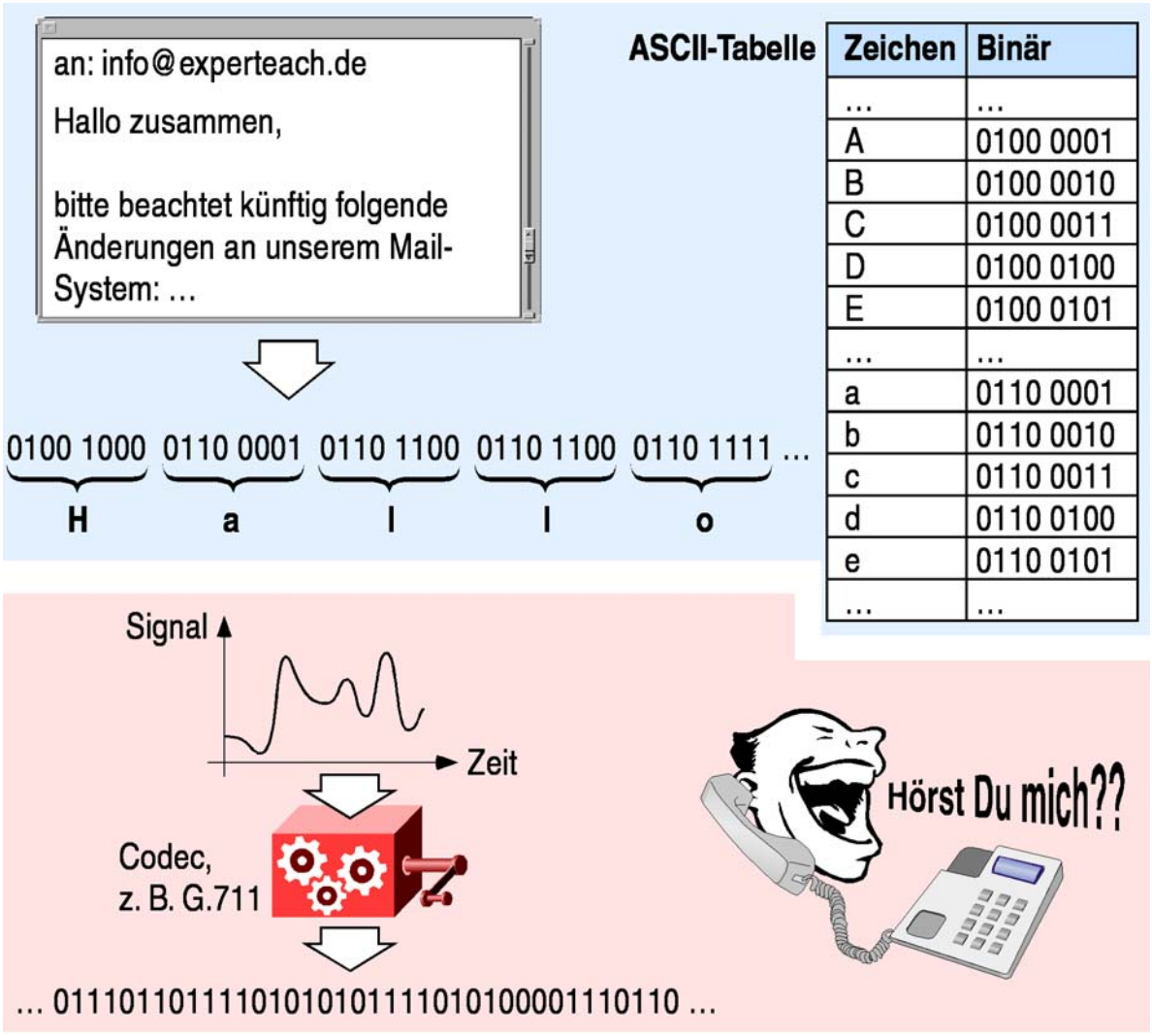
Anforderungen

Verschiedene Anwendungen stellen auch verschiedene Anforderungen an die Vernetzung. Zum Teil lassen sich die Anforderungen direkt aus dem Charakter einer Anwendung ableiten, zum Teil auch aus den Wünschen des menschlichen Benutzers dahinter.

Die Anwendung und der Nutzer

Im Charakter einer Datenbankanfrage ist verankert, dass Fehler in der Übertragung nicht toleriert werden können. Daten, die von der Datenbank angezeigt werden, dürfen auf dem Weg durch das Netz nicht verfälscht worden sein. Für das Funktionieren der Anwendung ist dabei innerhalb gewisser Grenzen weniger wichtig, wie schnell die Antwort geliefert wird. Für einen ungeduldigen Nutzer kann das aber ein wesentliches Kriterium sein.

Die Prämisse moderner Netzwerke: Alles digital



Zeichen	Binär
…	…
A	0100 0001
B	0100 0010
C	0100 0011
D	0100 0100
E	0100 0101
…	…
a	0110 0001
b	0110 0010
c	0110 0011
d	0110 0100
e	0110 0101
…	…

- **Moderne Netzwerke transportieren Sprache und Daten nur in digitaler Form.**
- **Anwendungen mit analogen Ausgangsdaten müssen diese digitalisieren.**
- **Das Netz transportiert nur Bits (Einsen und Nullen).**

Die Prämisse moderner Netzwerke: Alles digital

Analog: Jeder Wert erlaubt

Manche Anwendungen liefern ihre Rohdaten in digitaler Form, andere in analoger. Analog nennt man Daten, die innerhalb eines bestimmten Wertebereichs jeden Zwischenwert annehmen können. Ein Beispiel ist Musik – jede Tonhöhe und Lautstärke ist innerhalb gewisser Grenzen möglich.

Digital: nur diskrete Werte

Digitale Daten haben einen diskreten Wertevorrat. Ein Beispiel für eine Anwendung mit digitalen Rohdaten ist eine E-Mail. Es existiert ein genau definierter Zeichensatz, der für das Schreiben von Texten zur Verfügung steht. Zwischenwerte sind nicht möglich.

Warum nur digital?

Heutzutage hat man sich in der Netzwerktechnik endgültig festgelegt. Nur digitale Daten werden transportiert, und vor dem Transport werden sie in ein Binärsignal verwandelt. Ein Binärsignal ist eine Folge von Bits – also von Einsen und Nullen. Der Grund für diese Beschränkung auf binäre Signale ist einfach: man kann sie besonders einfach übertragen. Sie lassen sich leicht verstärken, und Störungen lassen sich leicht ausfiltern. Der Vergleich im Klang zwischen einer staubigen Schallplatte und einer staubigen CD illustriert das anschaulich. Dreht man die Lautstärke hoch, wird das Rauschen bei der Schallplatte mit verstärkt; die CD rauscht nicht.

Digitalisieren

Analoge Anwendungen, die ein digitales Netzwerk nutzen möchten, müssen ihre Rohdaten zunächst digitalisieren. Das kann entweder im Endgerät geschehen (Beispiel ISDN-Telefon), durch ein zwischengeschaltetes Gerät (Beispiel: ISDN-Telefonanlage mit analogen Telefonanschlüssen oder Terminal Adapter, TA) oder auch am Netzeingang (zunehmend unüblich, Beispiel ISDN-Vermittlungsstelle mit analogem Teilnehmeranschluss).

Typische Anwendungen

Massendaten	Laufzeit (Delay)	Laufzeit-schwankungen (Jitter)	Bitrate	Kontrolle von Fehlern (Error / Loss)
E-Mail	–	–	••	••• / •••
File Transfer	–	–	••	••• / •••
Backups	–	–	••	••• / •••
Daten, interaktiv				
WWW	–	–	•	••• / •••
Citrix	••	•	••	••• / •••
Datenbank	••	•	••	••• / •••
SAP	••	•	••	••• / •••
Streaming				
Web-Radio	•	••	•••	• / ••
IP TV	•	••	•••	•• / •••
Video on Demand	•	••	•••	•• / •••
Echtzeit				
Telefonie	•••	•••	•••	• / ••
Videokonferenz	•••	•••	•••	• / ••

Legende:

– : muss nicht kontrolliert werden
•• : muss kontrolliert werden
• : sollte kontrolliert werden
••• : muss strikt kontrolliert werden

- **Delay und Jitter: Anforderungen bezüglich der Zeit**
- **Bitrate: Anforderungen bezüglich des Durchsatzes (Bandbreite)**
- **Error: Verfälschte Daten**
- **Loss: Verlorene Daten**

Typische Anwendungen

Die üblichen Parameter

Untersucht man die Anforderungen, die von Anwendungen an das Netzwerk gestellt werden, so stößt man immer wieder auf einige wenige Parameter, auf die eine Anwendung empfindlich reagiert:

- Laufzeit (Delay): Wie lange sind Daten im Netzwerk unterwegs?
- Laufzeitschwankungen (Jitter): Bleibt die Laufzeit konstant, oder ändert sie sich?
- Bitrate (oft fälschlicherweise Bandbreite genannt): Wie ist der Datendurchsatz?
- Bitfehler (Bit Error): Sind die Daten unverändert?
- Verluste (Loss): Ist alles angekommen?

Beispiel SAP

Eine ERP-Anwendung wie SAP hat eine interaktive Natur. Lange Verzögerungen sind für den Benutzer unangenehm. Die Laufzeit der Daten ist daher nicht egal. Da eine bestimmte Transaktion jeweils auch ein bestimmtes Datenvolumen bewegt, muss auch die Bitrate kontrolliert werden, um Verzögerungen zu vermeiden. Essentiell wichtig ist, dass alle Daten fehlerfrei ankommen. Der Nutzer möchte sich auf seine Transaktionen verlassen können.

Telefonie

Bei Telefonie gibt der Dialogcharakter der Anwendung vor, dass die Laufzeit und der Jitter sehr gering sein müssen. Für die Telefonierenden ist es nicht akzeptabel, wenn von Wort zu Wort spürbare oder gar unterschiedliche Verzögerungen durch das Netzwerk verursacht würden. Wird auf Sprachpausenerkennung verzichtet, erzeugt Telefonie einen kontinuierlichen Datenstrom konstanter Bitrate. Die Bitrate muss im Netz daher streng kontrolliert werden (also sicher zur Verfügung stehen). Einzelne Bitfehler würde das menschliche Ohr gar nicht wahrnehmen – ihre Häufigkeit muss nur innerhalb gewisser Grenzen bleiben. Das Fehlen von Daten kann jedoch Folgen von hörbaren Störungen bis hin zu Verbindungsabbrüchen haben.