

Netze

Quelle: H. R. Hansen: Wirtschaftsinformatik - Seiten 714 bis 743

1. Netzwerkentwicklung:

1. Die in den 70er Jahren dominierende die hierarchische Struktur, bei der bestimmte Knotentypen im Netz anderen untergeordnet waren, resultierte aus den damals typischen Terminalnetzen, bei denen ein Host viele „dumme“ Datenstationen zu bedienen hatte.
2. Infolge des Minirechnerbooms wurden die Datenstationen aller Hierarchiestufen und Größenklassen gleichberechtigt um miteinander kommunizieren zu können (peer to peer).
3. In den 80er Jahren gab es eine Unmenge an verschiedenen Netzen. Aus diesem Grund wurden multiprotokollfähige Steuereinheiten entwickelt, die mit Datenstationen verschiedener Hersteller kommunizieren konnten.
4. Auf die OSI Normierungsbestrebungen der ISO (International Organisation for Standardisation; Vereinigung von über 50 nationalen Normausschüssen) und auf die Herausbildung des herstellerübergreifenden Marktstandards TCP/IP haben alle Hersteller mit Gateway Produkten reagiert und damit ihre Welten für die Kommunikation nach außen geöffnet.
5. Die Client Server Architektur wird zwar überall als das Zukunftskonzept der Datenverarbeitung gepriesen, über die reale Ausgestaltung und die Aufgabenverteilung in solchen verteilten Datenverarbeitungssystemen gibt es aber unterschiedliche Meinungen. Die Stellung des Großrechners ist noch nicht ganz klar.

2. Herstellerspezifische und offene Netze

Ein herstellerspezifisches Netz (proprietary computer network) ist ein Rechnernetz, dessen Kommunikationsarchitektur nicht dem ISO-OSI Referenzmodell (Das ISO-OSI Referenzmodell für die Kommunikation offener Systeme - Open Systems Interconnection - beschreibt ein allgemeines abstraktes Modell für die Kommunikation zwischen Datenstationen, d.h. es werden nur die wichtigsten Eigenschaften des Außenverhaltens funktional festgelegt - 7 Schichten) entspricht. Der Informationsaustausch zwischen den verbundenen Datenstationen erfolgt nach herstellereigenen Standards, die zu den Protokollen anderer Hersteller bzw. zu den ISO-Normen nicht oder nur schwach kompatibel sind.

- ◆ SNA (Systems Network Architecture) von IBM
- ◆ TRANSDATA von Siemens
- ◆ DNA (Digital Network Architecture) von DEC
- ◆ DCA (Distributed Communications Architecture) von Unisys
- ◆ DSE (Distributed Systems Environment) von Bull
- ◆ DSN (Distributed Systems Network) von Hewlett Packard

2.1 SNA von IBM

Anhand dieses Beispiels wollen wir uns die Datenverarbeitung im Großrechnerumfeld anschauen.

SNA wurde von IBM 1974 angekündigt, um eine einheitliche Kommunikationsbasis für IBM-Rechner zu schaffen. Seither erlebte diese Netzwerkarchitektur einige bedeutende Entwicklungsstufen. Dadurch wurde es zu einer sehr mächtigen, aber im Vergleich zu anderen Netzwerkarchitekturen auch sehr komplexen Kommunikationsarchitektur. IBM setzte mit SNA einen de-facto Standard, für den viele kleinere Hersteller in der Kommunikationsbranche kompatible Produkte entwickelt haben. Auch die anderen großen Computerhersteller haben in ihren Netzwerkarchitekturen SNA Übergänge implementiert. In SNA ist, wie in OSI, ein funktionales Schichtenmodell und zugehörige Protokolle definiert, darüber hinaus sind jedoch noch zusätzliche Komponenten der physischen und logischen Struktur des Systems spezifiziert.

Funktional besteht SNA genauso wie das ISO OSI Referenzmodell aus einer siebenschichtigen Architektur. Jedoch entsprechen diese nicht ganz dem ISO OSI Referenzmodell. Jede Schicht nimmt (wie bei OSI) Dienste der darunterliegenden Schicht in Anspruch, erbringt Dienste für die nächst höhere Schicht und kommuniziert mittels Protokollen mit den korrespondierenden Schichten in anderen SNA Produkten.

Ein SNA Netzwerk besteht aus einer Vielzahl von Hardware- und Softwarekomponenten, den sogenannten Nodes. SNA definiert einen Knoten als Set von Hardware- und dazugehörigen Softwarekomponenten, das die Funktionen der sieben Schichten des SNA Architekturmodells implementiert. Je nach Aufgabe werden vier verschiedene Knotentypen unterschieden:

- Subarea Nodes (T5 Knoten od. Host Nodes): Sie sind die hierarchisch am höchsten stehenden Knoten. Sie sind normalerweise als Großrechner (Mainframe) implementiert und stellen jene Funktionen zur Verfügung, die zur Steuerung eines Netzwerkes notwendig sind.
- Communicatoin Controller Nodes (T4 Knoten): Werden als Vorrechner direkt an den T5 Knoten angeschlossen und enthalten Funktionen, die den Datenfluß innerhalb eines Subarea Networks steuern.
- Peripheral Nodes (T2.0 und T2.1): Dies sind alles periphere Geräte. Ein T2.1 Knoten unterscheiden sich von einem T2.0 Knoten durch die Fähigkeit, mit einem anderen T2.1 Knoten kommunizieren zu können, ohne einen T5 Knoten dazwischenschalten zu müssen dh er besitzt Peer-orientierte Funktionen. Zwei direkt miteinander in einem Subarea Network verbundene T2.1 Knoten werden als LEN Nodes (Low Entry Networking Nodes) bezeichnet.

3. Lokale Netze

lokales Netz: LAN = local area network ermöglicht die Kommunikation zwischen mehreren unabhängigen Datenstationen mit hoher Übertragungsgeschwindigkeit (mehrere Mio. Bits/sec) und niedriger Fehlerrate in einem begrenzten Gebiet (in vielen Ländern wegen Postmonopol begrenzt auf ein Grundstück; maximale Entfernung zw. Knotenrechnern ca. 10 km)

3.1 Zugangsverfahren

Man kann sich ein lokales Netz wie ein großes Förderband vorstellen, auf dem Datenpakete transportiert werden. Dabei sind aber folgende Probleme zu lösen: Wer darf wann ein Datenpaket auf das Förderband legen und wer entfernt es wieder? Das Entfernen der Pakete erfolgt bei einem Förderband von selbst - es fällt hinunter. Bei einem lokalen Busnetz muß an jedem Ende ein „Dämpfer“ eingebaut sein, der die Signale schluckt. Bei einem Ringnetz muß der Sender sein Datenpaket sobald es wieder bei ihm angelangt ist, wieder löschen. Lesen von Nachrichten im lokalen Netz heißt also nicht, daß die Nachricht heruntergenommen wird, sondern daß eine Kopie des Inhaltes angelegt wird.

Dabei gibt es prinzipiell zwei Möglichkeiten:

Eine strenge Vorschrift, die exakt festlegt, wann welche Station senden darf, oder jede Station ist sendeberechtigt, bis durch die Sendekonkurrenz der kommunizierenden Station ein Fehler auftritt, der dann korrigiert wird.

3.2 Strenge Zugangsregelung - Tokenverfahren

Wenn sichergestellt wird, daß zu einem Zeitpunkt nur eine Station senden darf, kann es nie zu Überschneidungen kommen. Für die strenge Zugangsregelung hat sich das Tokenkonzept durchgesetzt:

In einem Netz kursiert ein eindeutiges Zeichen in Form eines speziellen Bitmusters, das Token. Jede Station, die senden will, muß auf das Token warten. Wenn es bei ihr eintrifft, kann sie es vom Netz entfernen und darf das eigene Paket senden. Spätestens nach einer vorgegebenen Zeitspanne ist die Sendung zu beenden, und als Endmarke wird das Token an die Nachricht angefügt. Dadurch wird auch gleichzeitig die Sendeberechtigung an den nächsten Teilnehmer weitergegeben. Natürlich gibt es auch Regelungen, um zu vermeiden, daß Daten, die wie das Token aussehen als Token interpretiert werden können. Es kann also nie dazu kommen, daß zwei Stationen gleichzeitig senden. Der einzige Fehler kann nur dann auftreten, wenn das Token verlorenght. In diesem Fall erzeugt eine beliebige Station ein Ersatztoken, welches von allen Stationen bestätigt wird oder eine Station meldet, daß sie das Token hat.

Zusammenfassung 1: Tokenverfahren

3.3 Wettkampfverfahren - CSMA/CD

Das Konzept dieses Systems, bei dem natürlich auch nach strengen Regeln vorgegangen wird, wurde in der Universität in Haiti entwickelt. Die einzelnen Institute sind auf viele Inseln verteilt und können nicht durch Kabel verbunden werden. Durch diese Lage war man gezwungen, ein Rundfunkverfahren zu entwickeln: Einer sendet, die anderen hören zu. Da aber jede Station gleichzeitig Sender und Empfänger ist, kann es natürlich vorkommen, daß mehrere Stationen zugleich senden und daher keiner etwas versteht.

Das Verfahren wurde also mit folgender Vorschrift verbessert: Bevor eine Station sendet, muß sie sich überzeugen, daß kein anderer Teilnehmer sendet. Wenn der Kanal frei ist, kann man mit der Übertragung beginnen, wenn jemand sendet muß man warten, bis der Kanal wieder frei wird. Dieses System arbeitet schon viel besser. Es kann aber ein Fehler auftreten, wenn zwei Stationen zur gleichen Zeit senden wollen.

Folglich gibt es noch einen dritten Entwicklungsschritt: Nicht nur vor, sondern auch während der Sendung ist der Übertragungskanal abzuhören. Damit kann jede Kollision erkannt werden und die Sender brechen die Übertragung ab.

Das eben beschriebene Verfahren ist bei Busnetzen gebräuchlich und heißt CSMA/CD (carrier sense multiple access with collision detection):

viele beliebige Sender: multiple access

vor dem Senden hineinhören: carrier sensing

und auch während der Übertragung den Kanal prüfen: collision detection.

Zusammenfassung 2: CSMA/CD

Der Vergleich der Zugangsprotokolle läßt keine schlüssige Bewertung zu, welches Verfahren besser ist. Es hängt von den Bedingungen im lokalen Netz ab. Im Hochlastbereich ist das Tokennetz schneller als das CSMA/CD. Dafür hat CSMA/CD bei einer geringeren Zahl von Stationen und nicht so intensivem Nachrichtenverkehr, daß man nicht auf das Token warten muß, sondern gleich senden kann.

3.4 Kopplung von lokalen Netzen

Für viele Betriebe ist es günstiger, mehrere lokale Netze zu installieren, da jede Abteilung andere Software benötigt. Auch wäre ein großes Netz viel langsamer, weil alle Daten an alle geschickt würden. So werden aber nur die notwendigen Informationen außerhalb des lokalen Netzes gebracht. Dies wird durch spezielle Kopplungseinheiten realisiert (Repeater, Bridges, Router, Gateways, ...). Lokale Netze können so natürlich auch über lange Strecken mit Standleitungen verbunden werden. Wenn nun eine Station eine Nachricht an eine Station in einem anderen lokalen Netz senden will, so sendet sie diese an den Router, der die Weiterleitung übernimmt. Falls das Zielnetz nicht direkt von Router erreichbar ist, wird die Nachricht an den nächstgelegenen Router weitergeleitet. Einem Router muß also die gesamte Topologie des Netzes bekannt sein.

3.5 LAN-Standards: Ethernet, Tokenring, FDDI

Noch vor einem Jahrzehnt gab es eine Vielzahl an LAN-Systemen. Die IEEE (Institute of Electrical and Electronics Engineers; große herstellerneutrale Vereinigung, die Anwenderinteressen vertritt) hat mit dem Standard IEEE 802 diese Vielzahl auf einige Grundsysteme reduziert.

- ◆ IEEE 802.3: CSMA/CD - ein Bussystem mit CSMA/CD - Zugangsverfahren
- ◆ IEEE 802.5: Tokenring - ein Ringsystem mit Token - Zugangsverfahren
- ◆ IEEE 802.4: Tokenbussystem
- ◆ IEEE 802.6: Metropolitan Area Network
- ◆ IEEE 802.8: FDDI - ein Hochgeschwindigkeitsnetz mit Glasfaserkabeln

Die ISO hat die IEEE - 802 - Normen als ISO 8802 - Normen übernommen.

Tokenbus:

Bei einem Tokenbussystem ist ein logischer Ring auf einem physikalischen Bus implementiert. Das heißt, die Stationen sind physikalisch durch einen Bus miteinander verbunden, als Zugangsregelung wird das Tokenverfahren verwendet.

Ethernet:

Das Ethernet ist der am weitesten verbreitete LAN - Standard. Ein Ethernet ist relativ Kostengünstig und bietet eine hohe Betriebssicherheit. Es verwendet einen passiven Basisbandbus, der eine Übertragungsgeschwindigkeit von 10 Mbit/s ermöglicht. Das Zugangsprotokoll ist CSMA/CD. Die maximale Netzwerklänge beträgt 2500 m, bis zu 1024 Stationen können angeschlossen werden.

Tokenring:

Das Tokenring ist ein von IBM favorisierter LAN - Standard, der in der ISO 8802-5 Norm definiert ist. Die Netzwerktopologie ist ein Ring, die Zugangsregelung erfolgt mittels Tokenverfahrens. Für das Medium bestehen zwei Varianten: Verdrillte Kupferkabel erlauben Übertragungsraten von 1 bis 4 Mbit/s, bei Basisbandübertragungen über Koaxialkabel sind Übertragungsraten von 4 bis 40 Mbit/s möglich.

FDDI:

Der FDDI - Standard (FDDI: fiber distributed data interface; Deutsch: Datenschnittstelle für verteilte Glasfasernetze) spezifiziert einen Glasfaserring mit einer maximalen Länge von 100 km für Hochgeschwindigkeitsnetze. Mit einer Übertragungsgeschwindigkeit von 100 Mbit/s wird er vorwiegend als „Backbone“ für unternehmensweite Netze eingesetzt. FDDI unterstützt sowohl synchrone als auch asynchrone Datenübertragung und bietet Schnittstellen zu Ethernet und Tokenring - Netzen an. Bis zu 500 Stationen können an einen FDDI - Ring angeschlossen werden, wobei die maximale Entfernung von je zwei Datenstationen 2 km beträgt. FDDI ist als Doppelring mit einer Gesamtlänge von 200 km definiert, wobei in den beiden Ringen gegenläufig zueinander übertragen wird. Der Sekundärring dient im normalen Betrieb als Backup - Ring, auf den bei Bedarf und in Notfällen automatisch umgeschaltet wird. Die Doppelring - Struktur ermöglicht ein hohes Maß an Fehlertoleranz und Ausfallsicherheit. Bei Störungen wird das Netz automatisch neu konfiguriert. Bezüglich des Netzanschlusses werden zwei Arten von Datenstationen unterschieden: Typ A Stationen sind direkt mit dem Primär und dem Sekundärring verbunden und erhalten folglich die Komponenten der physikalischen Schicht in doppelter Ausführung. Typ B Stationen sind nicht direkt sondern über Konzentratoren einfach an den FDDI Ring angeschlossen. Es können auch an Konzentratoren weitere Konzentratoren angeschlossen werden.

4. PC - Host Verbund

In vielen Firmen ist es heute so, daß die Mitarbeiter den Komfort eines PCs ausnützen wollen, aber trotzdem auf die Daten des Großrechners zugreifen sollen. Dabei prallen nun zwei verschiedene Welten aufeinander. Der physikalische Anschluß eines Microrechners an das Rechnernetz wird meist über eine Adapterkarte realisiert. Die Abwicklung des Programmes erfolgt programmgesteuert. Die dazu erforderliche Software für den Mikrorechner wird beim Kauf der Adapterkarte mitgeliefert.

Im einfachsten Fall arbeitet der Microrechner als Stapelstation. In diesem Fall werden Daten von Großrechner zum Microrechner übertragen und natürlich auch umgekehrt. Soll der

Microrechner auch die Hardware (Prozessor, Drucker, Platten, ...), Programme und Datenbestände des Zentralrechners im Dialogbetrieb nutzen können, so ist eine Terminalemulation erforderlich. Dabei wird durch die Software das Kommunikationsverhalten eines „dummen“ Terminals nachgebildet. Probleme gibt es oft damit, daß der Großrechner eine andere Tastatur verwendet, als der Microrechner.

5. Client-Server-Systeme

Eine Client-Server-Anwendung kann quasi als „geteilte Anwendung“ betrachtet werden, die in der Verarbeitung teilweise von Client und teilweise von Server vorgenommen wird. Für die funktionale Trennung der Programmlogik zwischen Client und Server innerhalb einer Anwendung gibt es meist mehrere Möglichkeiten. Grundidee der Client-Server-Architektur ist eine möglichst optimale Ausnutzung der Ressourcen der beteiligten Systeme. In diesem Modell werden die Vorzüge von Arbeitsplatzrechnern mit mehrbenutzerfähigen Verarbeitungsrechnern integriert.

Meist werden im Client-Teil der Anwendung die Benutzeroberfläche, die Eingabeprüfung, die Verarbeitung und die Kommunikatoinskomponente (Kommunikation mit Server) realisiert. Ein Server besteht aus einer Kommunikationskomponente und einer Komponente zur Datenspeicherung und Datenmanipulation.

Client-Server-Computing bedeutet also eine bestimmte Rollenaufteilung einer Anwendung in die dienstansfordernde (Client) und dienstbringende Teil (Server). Das Serversystem stellt eine od. mehrere Funktionen zur Verfügung (Drucken, Datenbanken, ...), die von Client aufgerufen werden können.

Entwicklungen, die das Client-Server-Modell unterstützen:

- * Steigende Leistungsfähigkeit von Arbeitsplatzrechnern
- * Verfügbarkeit von immer leistungsfähigeren und kostengünstigeren Netzverbindungen
- * zunehmendes Angebot von Kommunikationsstandards und Standardsystemplattformen
- * veränderte Unternehmensstrukturen
- * verstärkter Wunsch nach Integration bestehender PC-Insellösungen