2.2 Netzwerktopologie

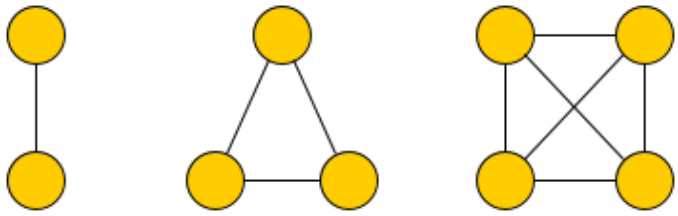
Nachdem wir uns bisher damit beschäftigt haben, wie eine Kommunikation ablaufen kann, müssen wir uns nun anschauen, wie wir diese Nachrichten von einem Rechner zum nächsten bekommen. Dabei stellt sich vor allem die Frage, welcher Rechner mit welchem anderen Rechner verbunden sein sollte.

Über die Zeit haben sich vier Mögliche sogenannte Netzwerktopologien herauskristallisiert:

2.2.1 Direkte Verbindung (point-to-point)

Die auf den ersten Blick einfachste Verbindung zwischen Rechnern liegt darin, zwischen zwei Rechnern je eine Verbindung anzulegen.

Die direkte Verbindung zwischen allen Rechnern klingt erst mal einfach, wird allerdings mit der Menge der Rechner immer aufwändiger und teurer. Das Hinzufügen eines Rechners in das Netz kostet mehr, umso mehr Rechner bereits im Netz sind.



Vorteile:

- Sehr ausfallsicher
- Fehlersuche einfach
- Hohe Sicherheit, da ein kompromittierter PC nur die Kommunikation zu sich selber scannen kann

Nachteile:

- Nur schwer skalierbar
- Bei n Rechnern in der Topologie braucht man n neue Kabel um einen weiteren Rechner anzuschließen

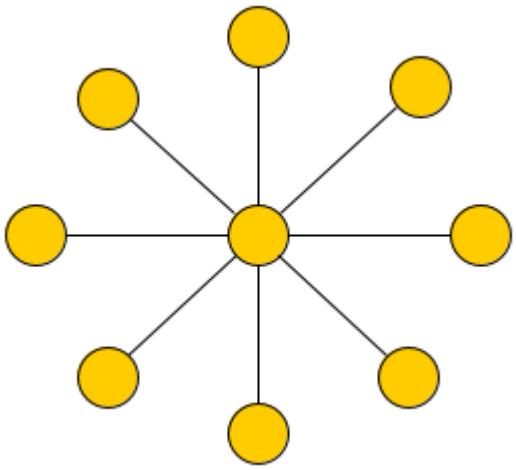
Hauptanwendung:

- System mit wenigen Rechnern, das hohe Ausfallsicherheit braucht

2.2.2 Der Stern

Besonders für größere Netzwerke brauchte man schnell eine Alternative, die kostengünstiger skalierbar ist.

Im Stern werden alle Rechner über einen zentralen Knotenpunkt „in der Mitte“ miteinander verbunden. Dabei muss der Knotenpunkt in der Mitte leistungsfähig genug sein, um alle Übertragungen verarbeiten zu können.



Vorteile:

- Leicht und kostengünstig skalierbar (Bis der zentrale Knoten ersetzt werden muss)
- Fehlersuche einfach
- Kostengünstig in der Einrichtung (nur n-1 Leitungen bei n Knoten)

Nachteile:

- Störanfällig, wenn der zentrale Knoten ausfällt ist keine Kommunikation mehr möglich
- Anfällig für Angriffe, da wenn der zentrale Server gehackt wird, alle Kommunikation abgegriffen werden kann.

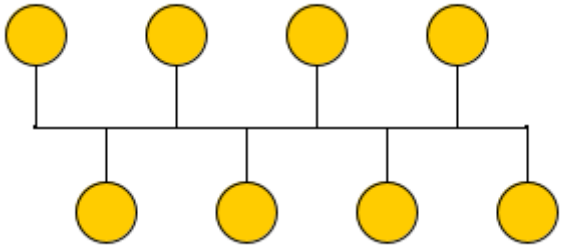
Hauptanwendung:

- Intranet mit ggf. Backupserver zur Sicherung des zentralen Knoten. Der zentrale Knoten bildet oft die Schnittstelle nach außen und schirmt das interne Netz nach außen ab.

2.2.3 Der Bus

Bei der suche nach einem System, das skalierbar und ausfallsicher ist, hat man die Bus Topologie entwickelt.

Beim Bus werden alle Endgeräte mit einer zentralen Leitung verbunden. Es gibt keinen Zentralen Knoten, der die interne Kommunikation routet. Soll ein internes Bus Netzwerk mit dem Internet verbunden werden, wird oft ein Server in das System eingebunden, der die Verbindung nach außen zur Verfügung stellt.



Vorteile:

- Leicht und kostengünstig skalierbar
- Kostengünstig in der Einrichtung (nur n-1 Leitungen bei n Knoten)

Nachteile:

- Störanfällig, wenn die Leitung irgendwo gekappt ist, fällt alles aus
- Anfällig für Angriffe, da ein kompromittierter PC alles mitlesen kann
- Übertragungskapazität ist durch die Leitung beschränkt. Wenn einer viel Übertragungskapazität braucht, ist das Netzwerk für alle anderen langsamer
- Senden und Empfangen nach „Trial and Error“. Jeder Teilnehmer versucht zu übertragen und falls die Leitung belegt ist, versucht er es einfach etwas später nochmal. Das führt oft zu vielen Abbrüchen und wiederholten Anfragen.
- Nicht beliebig skalierbar, da mehr Rechner weniger Übertragung für jeden bedeutet

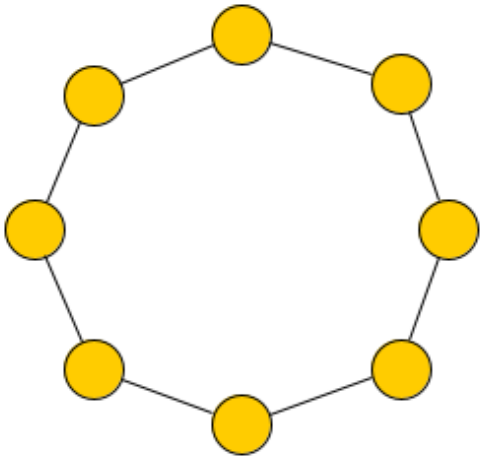
Hauptanwendung:

- Wireless Systeme die auf einer Bandbreite von Frequenzen senden

2.2.4 Der Token-Ring

Manche Netzwerke müssen hohen Anforderungen an ihre Übertragungskapazität gerecht werden, dürfen aber auch nicht so teuer sein, wie eine Direktverbindung. Für diesen Anwendungsfall wurde der Token-Ring entwickelt.

Beim Token-Ring werden immer benachbarte Rechner über eine Leitung verbunden. Eine Monitorstation erstellt ein Token, das herumgegeben wird. Nur ein Rechner, der das Token hat darf übertragen. Die Leitungen werden so gelegt, dass bei Ausfall eines Rechners dieser in der Topologoie übersprungen wird. Das Token gibt ein Rechner dann weiter, wenn er mit seiner Übertragung fertig ist oder er gerade keine Übertragung braucht.



Vorteile:

- Leicht und kostengünstig skalierbar
- Kostengünstig in der Einrichtung
- Bei niedriger und hoher Last im System bietet der Token eine konstante Übertragungsrate
- Keine Kollisionen in der Übertragung.

Nachteile:

- Im Durchschnitt langsamer als ein Bus System, da die Übertragung des Token einen zusätzlichen Zeitfaktor darstellt
- Anfällig für Angriffe, da ein kompromittierter PC alles mitlesen kann
- Nicht beliebig skalierbar, da sonst die Übertragungszeit des Token alles ausbremst

Hauptanwendung:

- Hauptsächlich Brandmeldeanlagen - bei Rechnern eigentlich keine mehr. Wurde früher in Forschungsnetzwerken verwendet, ist inzwischen allerdings durch Ethernet komplett ersetzt worden.
- Niemand konnte bisher stichhaltig erklären, warum dieses in der Theorie ideale System schlechter ist als das zufällige „Aloha“ Verfahren der anderen Systeme. Die Einsparung von Kollisionen beim Senden sollte eigentlich die Performance boosten. In der Praxis passiert dies einfach nicht.