Netzwerkkomponenten

Hub, Bridge, Switch, Router, Firewalls, IDS/IPS und Load-Balancer

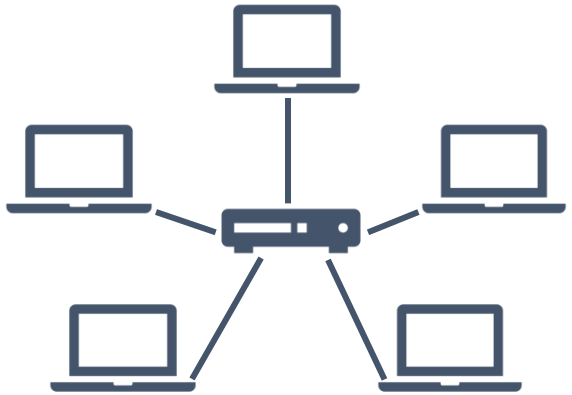
Tom Gries

Dokumenten URL: http://docs.tx7.de/TT-NK2

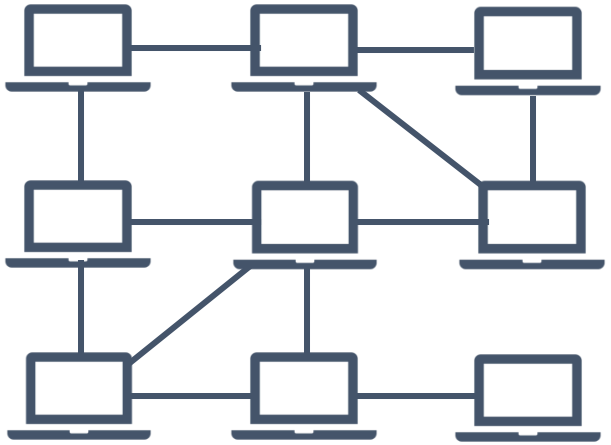
Autor: Tom Gries <TT-NK2@tx7.de>
@tomo@chaos.social

Version: 7.2.0 vom 02.02.2024

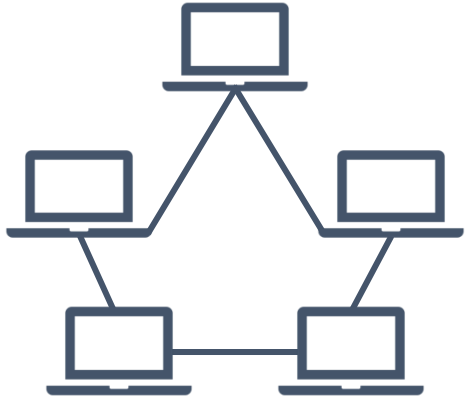
Netzwerk Topologien



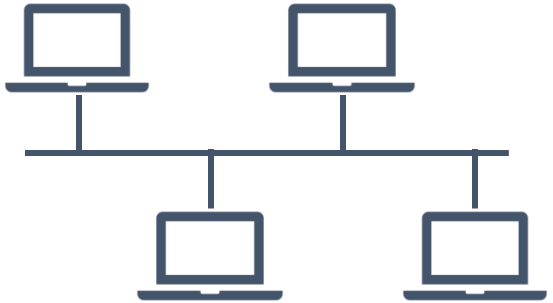
Stern-Topologie



Meshed-Topologie



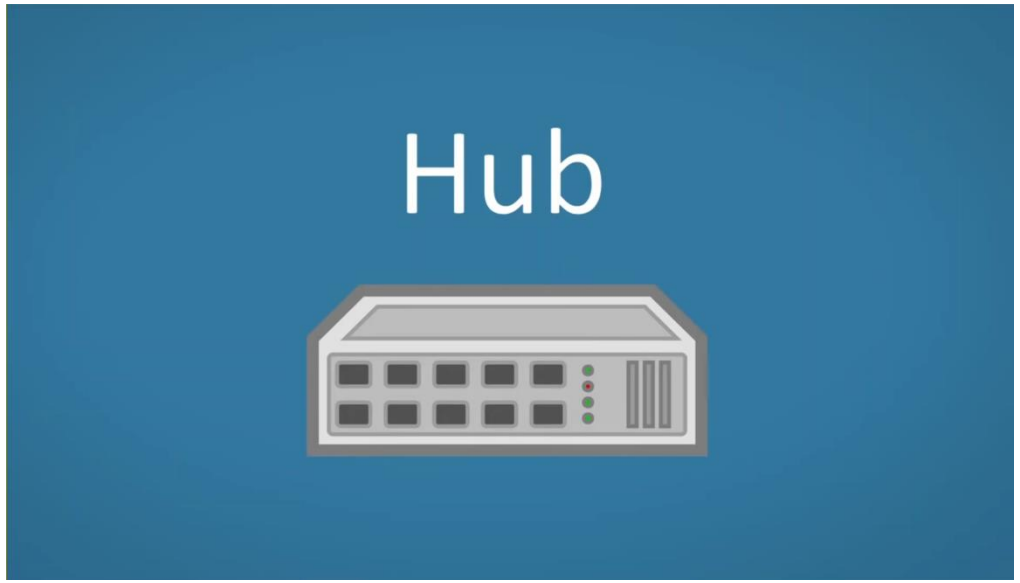
Ring-Topologie



Bus-Topologie

Hub

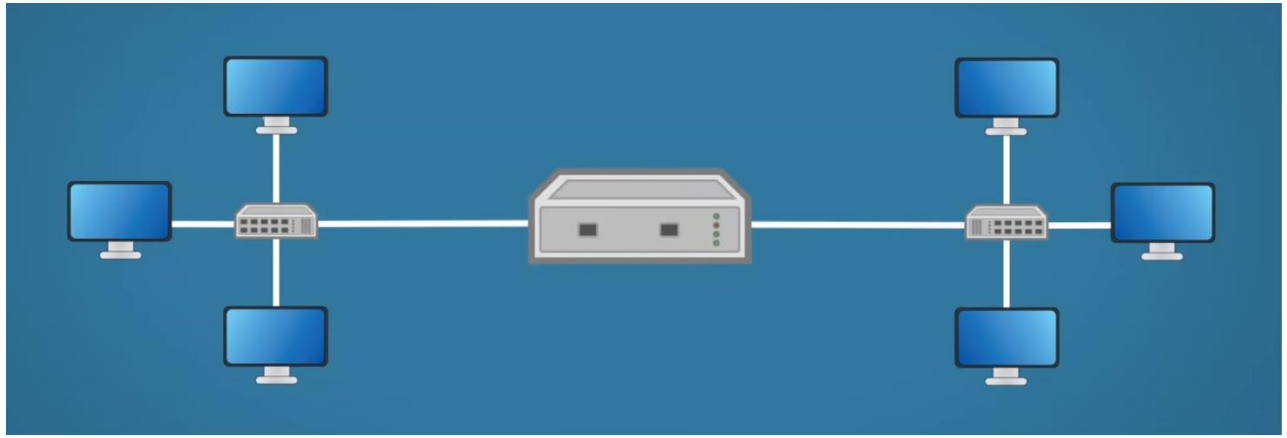
Von A nach B



Bild/Animation: https://www.certbros.com

- Verschwendet Bandbreite
- Arbeitet Half-Duplex
- Ist ein Layer 1 Device (ein Repeater)
- Hat **eine** Kollisions-Domain
- Ist sicherheitsproblematisch: Jeder Teilnehmer kann alles sehen/hören.
- Ist alte Technologie - wurde durch Switched Hubs (Switche) ersetzt.

Bridge



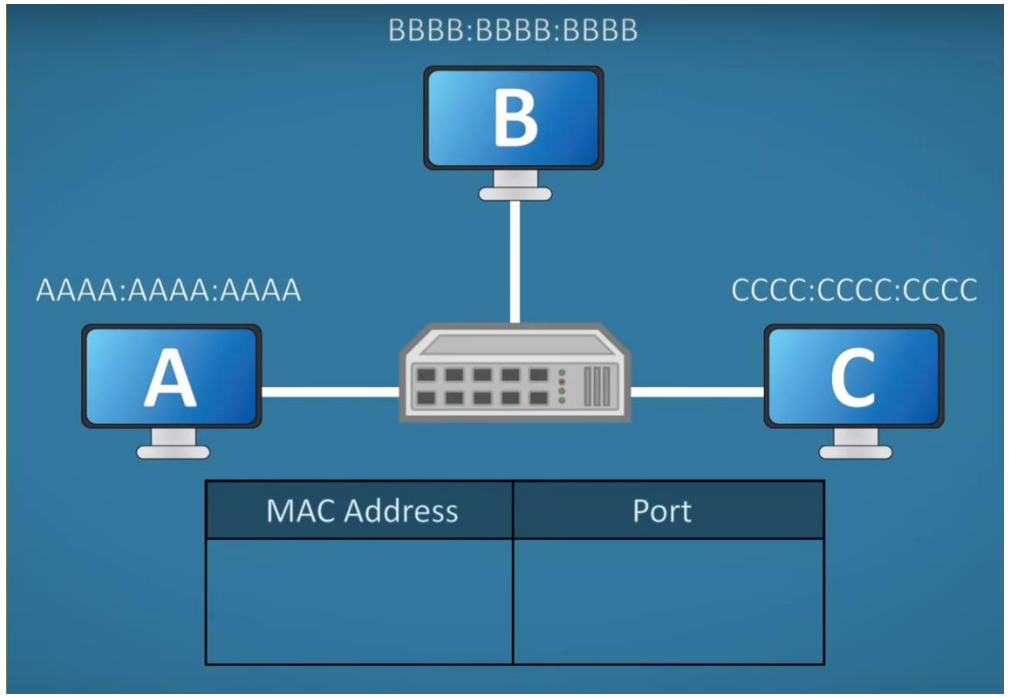
Bild/Animation: https://www.certbros.com

- Ist ein Layer 2 Device ("lernt" die MAC-Adressen)
- Hat üblicherweise nur zwei Ports
- Verbindet bzw. segmentiert (Hub-) Netzwerke*
- Hat **zwei** Kollisions-Domain
- Ist alte Technologie - wurde durch Switched Hubs (Switche) ersetzt.
- Hat einen Sicherheitsgewinn: Die Teilnehmer des anderen Netzes können den Datenverkehr nicht abhören.

Normalerweise will man ein großes Netzwerk segmentieren, um die Kollisions- und Broadcastdomains zu verkleinern.

Switched Hub

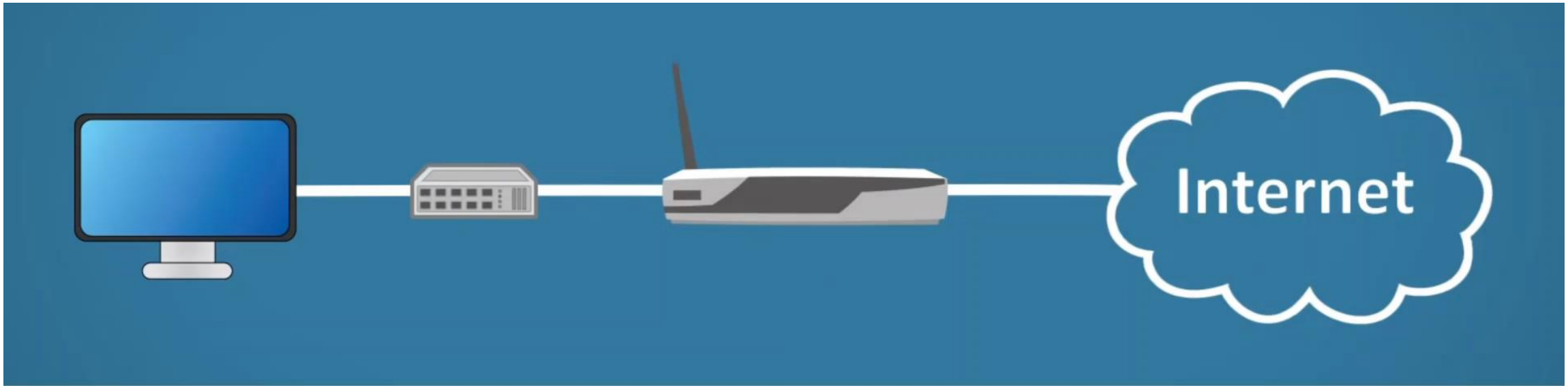
Von A nach C



Bild/Animation: https://www.certbros.com

- Ist ein Layer 2 Device ("lernt" die MAC-Adressen)
- Arbeitet Full-Duplex
- Hat mehrere Kollisions-Domainen
- Spart Bandbreite
- Hat einen erheblichen Sicherheits-gewinn: Nur der tatsächliche Empfänger kann den Datenverkehr sehen.

Router



Bild/Animation: https://www.certbros.com

- Ist ein Layer 3 Device (entscheidet anhand der IP-Adressen)
- Routed Traffic zwischen Netzwerken
- Hat mehrere Ports (mindestens zwei)

Firewall

Eine Firewall hat die Aufgabe, den Netzwerkverkehr (Traffic) zwischen zwei oder mehreren Netzen kontrolliert zu filtern und die gegebene Securitypolicy durchzusetzen. In den meisten Fällen soll eine Firewall das lokale Netzwerk (LAN) gegen Angriffe aus dem Internet schützen. Man unterscheidet im Wesentlichen

1. Packet Filter (Filterung auf Sender, Empfänger und Port)
2. Application Layer Gateways (Proxy für Anwendungen)
3. Stateful Inspection (merkt sich den Zustand, also Sender und Empfänger)

Darüber hinaus werden auf Arbeitsplatzrechnern **Personal Firewalls** eingesetzt. Personal Firewalls trennen keine Netzbereiche, sondern schützen nur den einzelnen Rechner.

IDS und IPS

Intrusion-Detection- und Intrusion-Prevention-Systeme sind Werkzeuge, die den Datenverkehr zu/von IT-Systemen oder Netzen aktiv überwachen. Das Ziel ist es, Ereignisse herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Die Verfahren basieren auf Mustererkennung, um ein Abweichen von einem Normalzustand zu signalisieren. Mit heuristischen Methoden sollen auch bisher unbekannte Angriffe erkannt werden.

Während IDS Angriffe nur erkennen, sollen IPS diese auch abwehren bzw. verhindern. Dazu wird der Datenstrom unterbrochen oder über Module Firewallregeln aktiviert oder modifiziert.

Load Balancer

Load Balancing ist eine Lastverteilung und soll große Mengen von Anfragen an parallel arbeitende Systeme verteilen. Eine mögliche Variante ist das Vorschalten eines Systems (Load Balancer), der die Anfragen aufteilt.

Beim DNS ist das Round Robin Verfahren bereits implementiert. Einem Namen werden mehrere IP-Adressen zugeordnet. Bei Abfragen werden diese der Reihe nach (Round Robin) als Antwort geliefert.

Anmerkungen oder Fragen?