Data Link Layer-Local Area Network (LAN)

Ein Local Area Network (LAN) ist ein Netzwerk für die bit-serielle Übertragung von Informationen zwischen mehreren Geräten, die

unabhängig voneinander arbeiten
miteinander verbunden sind, und
rechtlich vom Nutzer kontrolliert werden

Eigenschaften von LANs:
-hohe Geschwindigkeit
-kostengünstige Verbindungsmöglichkeit
-begrenzte Reichweite (normalerweise auf Gebäude oder Campus)

Kernproblem von LANs: da mehrere Sender das gleiche Medium nutzen, benötigt man eine Regelung, wer wann senden darf -> Medium Access Control (MAC).

2. Medium Access Control (MAC)

da in einem LAN mehrere Geräte gleichzeitig senden können, kann es zu Kollisionen komen, die vermieden oder gehandhabt werden müssen. Dafür gibt es verschiedene Methoden.

2.1 Static Channel Allocation (statische Kanalzuweisung):

FDM (Frequency Division Multiplexing):
TDM (Time Division Multiplexing):

!Nachteil: ineffizient bei wechselndem (bursty) Verkehr
Lösung: dynamische Kanalzuweisung

2.2 Dynamic Channel Allocation (dynamische Kanalzuweisung)

2.2.1 Kollisionsfreie Verfahren (coordinated access-contention free):

1. Polling Verfahren:
   Eine zentrale Kontrollstation fragt alle Stationen der Reihe nach ab (Polling)
   Problem: wenn keine Daten gesendet werden müssen, ist Zeit verschwendet
   Schwachpunkt: wenn die zentrale Station ausfällt, funktioniert das System nicht mehr
2. Token Passing:
   Ein Token (eine Berechtigung zum Senden) wandert durch das Netzwerk
   Wer das Token besitzt, darf senden
   Waiting time for token + deterministic scheme (fair)
   Vorteil: Kollisionen werden vermieden
   Nachteil: Bei Token-Verlust muss ein neuer generiert werden, was Zeit kostet

2.2.2. Verfahren mit Kollisionen (random access-with contention)

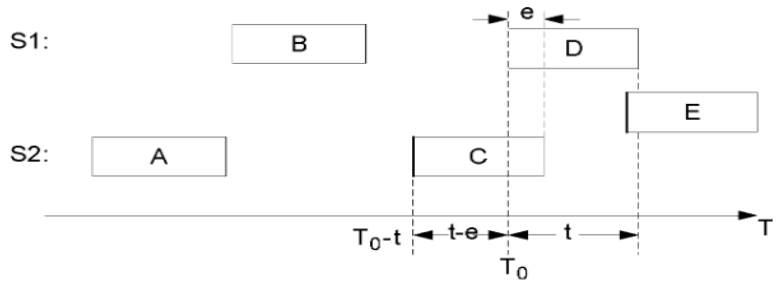
Diese Verfahren setzen auf Mechanismen, die Kollisionen erkennen oder minimieren

1. **ALOHA (Pure & Slotted):**
   a. ***Pure ALOHA:***
      Stationen senden einf. Daten, ohne vorher zu prüfen, ob das Medium frei ist
      Nach einer Kollision versucht das Gerät nach einer zufälligen Wartezeit erneut Daten zu senden
      Problem: hohe Kollisionsrate, da mehr Stationen gleichzeitig senden können + das gesamte Zeitintervall für Kollisionen anfällig ist
   b. ***Slotted ALOHA***
      Verbesserung: Slotted ALOHA-Nachrichten dürfen nur zu bestimmten Zeiten (Slots) gesendet werden, bzw. nur zu Beginn eines Zeitslots
      Kollisionsrate niedriger als Pure ALOHA, da Kollisionen nur am Beginn eines Slots auftreten können.

Nach einer Kollision übertragen Geräte wieder nach einer zufälligen Anzahl der Timeslots

!in identischen Bedingungen (bei selber Last) kann die Verzögerung in beiden Protokollen nicht gleichgroß sein

Effizienz: Pure ALOHA: 18,4% maximale Kanalnutzung;
Slotted ALOHA: 36,8% maximale Kanalnutzung

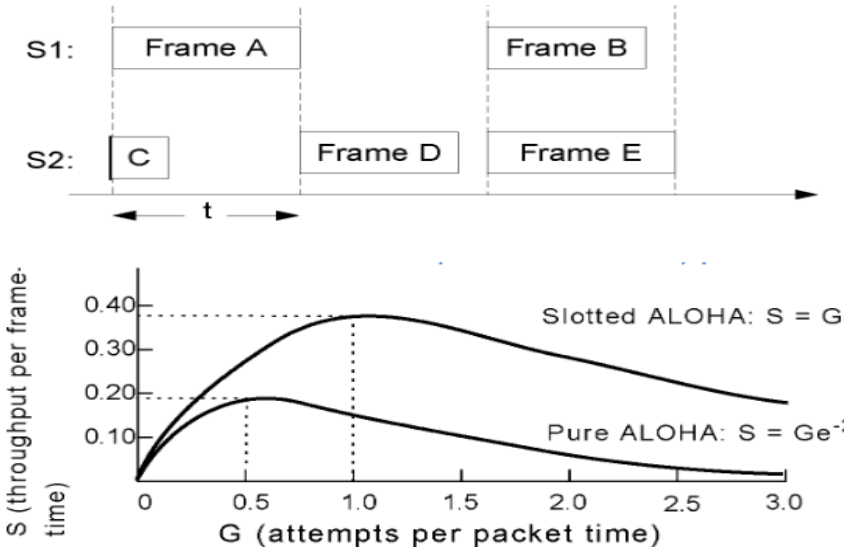


- Jede Übertragung dauert t Sekunden.
- Eine Kollision kann auftreten, wenn ein anderer Frame frühestens bei T_0 - t und spätestens bei T_0 + t startet.
- Dadurch ergibt sich ein Gesamtkollisionsfenster von 2t.
  Mathematisch:

$$\text{Kollisionszeitraum} = 2t - \varepsilon$$

$$\lim_{\varepsilon \to 0}(2t - \varepsilon) = 2t$$

Das bedeutet: Sobald das Netz stark ausgelastet ist, nähert sich der Kollisionszeitraum exakt 2t an.



!Es kann ein Zeitvorteil bei der Pure ALOHA entstehen:
Geringer Datenverkehr:

- Pure ALOHA kann einen Vorteil haben, weil es keine festen Zeitslots gibt, d.h. keine unnötigen Wartezeiten.
- Falls nur wenige Stationen aktiv sind, dann sind Kollisionen selten und die Stationen müssen nicht auf das nächste Zeitslot warten, um zu senden.

2. ***CSMA (Carrier Sense Multiple Access):*** ??????????????????????
   Stationen prüfen, ob das Medium belegt ist, bevor sie senden
   Varianten:
   1-Persistent CSMA: wenn das Medium frei ist, wird sofort gesendet (hohe Kollisionsgefahr)
   non-Persistent CSMA: warten für eine zufällige Zeit, wenn das Medium belegt ist (reduziert Kollisionen, aber erhöht Verzögerung)
   p-Persistent CSMA: Nur für Zeitslots: Gerät sendet mit Wahrscheinlichkeit p, wartet sonst (wird in Slotted ALOHA verwendet)
3. ***CSMA/CD (with Collision Detection)***
   verwendet in Ethernet (IEEE 802.3)
   Stationen überprüfen das Medium vor dem Senden
   Falls eine Kollision erkannt wird, wird die Übertragung abgebrochen
   verwendet den Binary Exponential Backoff-Algorithmus: nach jeder Kollision wird eine zufällige Wartezeit gesetzt, die exponentiell wächst

   !ist CSMA/CD gut bei Flugzeugen?
   CSMA/Cd ist für Flugzeugen weniger geeignet, weil es Kollisionen erkennen und verwalten muss, was zu Verzögerung und potenziellen Leistungsproblemen führen kann.
   Stattdessen sind zeitlich geregelte Zugriffsverfahren wie TDMA besser geeignet, um die Anforderungen an Echtzeitkommunikation in solchen kritischen Umgebungen besser zu erfüllen.

!Data Link Layer im OSI-Modell besteht aus zwei Unterschichten: MAC und LLC
!LLC (IEEE 802.2): Steuerung der Kommunikation zwischen Layer 2 und Layer 3
!MAC (802.x): Steuerung des Zugriffs auf das Medium (Kabel, WLAN, etc)

3. Logical Link Control (LLC)

LLC ist eine Teilschicht der Data Link Layer und in IEEE 802.2 definiert
Es bietet eine einheitliche Schnittstelle zur Netzwerkschicht für verschiedene LAN-Technologien

3.1 Funktionen der LLC-Schicht

unterstützt verschiedene Netzwerkschichten, indem es einheitliche Kommunikation über verschiedene LANs ermöglicht
bietet Fehlerkontrolle, Flusskontrolle und Multiplexing für verschiedene Protokolle
definiert, wie Datenpakete an die richtige MAC-Adresse übergeben werden

3.2 LLC-Diensttypen

LLC unterstützt drei Arten der Kommunikation:
a- unacknowledged connectionless mode (UC): kein Verbindungsaufbau oder Bestätigung
b- acknowledged connectionless mode (AC): jedes gesendete Paket wird durch eine Bestätigung (ACK) quittiert
c- connection-oriented mode (CO): Verbindungsaufbau vor Datenübertragung. Jedes Paket wird bestätigt, Reihenfolge wird eingehalten

4. Link Layer Addressing (MAC-Adressen)

4.1 MAC-Adressen (LAN oder Ethernet-Adressen)

MAC-Adressen sind physische Adressen auf der Data Link Layer, die ein Gerät innerhalb eines LANs identifizieren

Eigenschaften:

- 48-Bit-Adresse (6 Bytes), oft hexadezimal dargestellt
  - 24 Bits OUI (Organizationally Unique Identifier)-Herstellerkennung (von IEEE vergeben)
  - 24 Bits Geräterkennung-eindeutige Nummer des Geräts (device identifier)
- weltweit eindeutig durch IEEE-Zuweisung, somit wird es verhindert, dass MAC-Adressen doppelt vergeben werden

MAC-Adressarten:

- Unicast-Adresse: Daten gehen an genau ein Gerät-> 00:1A:2B:3C:4D:5E
- Multicast-Adresse: Daten gehen an eine Gruppe von Geräten-> 01:1A:2B:3C:4D:5E
- Broadcast-Adresse: Daten gehen an alle Gerät-> FF:FF:FF:FF:FF:FF

Eigenschaft	MAC-Adresse (Layer 2)	IP-Adresse (Layer 3)
Typ	Physische Adresse	Logische Adresse
Reichweite	Lokales Netzwerk (LAN)	Weltweite Kommunikation (Internet)
Änderung	Bleibt gleich	Ändert sich je nach Netzwerk
Verwendung	Switches nutzen sie zur Weiterleitung	Router nutzen sie für Routing

!IEEE 802.2 (LLC) ist oberhalb von allen diesen MAC-Schichten. Das bedeutet: egal, ob das Netzwerk Ethernet (802.3) oder WLAN (802.11) nutzt (verschiedene IEEE 802.x-Standards verwenden unterschiedliche MAC-Protokolle), LLC (802.2) bleibt gleich.

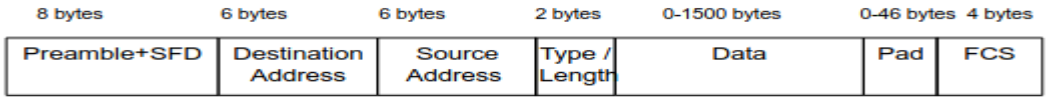
Netzwerktyp	MAC-Standard
Ethernet (kabelgebunden)	IEEE 802.3 (CSMA/CD)
Token Ring	IEEE 802.5
WLAN (Wi-Fi)	IEEE 802.11 (CSMA/CA)
Bluetooth	IEEE 802.15

5. IEEE 802.3: CSMA/CD (Ethernet)

definiert als offizieller Standard für Ethernet

Grundprinzip:

- 1-persistent CSMA/CD
- unterstützt verschiedene Übertragungsarten: 10Mbps, 100Mbps, 1Gbps, 10Gbps



Feld	Größe	Beschreibung
Preamble	7 Bytes	Synchronisationsbits (`10101010`).
Start Frame Delimiter (SFD)	1 Byte	Zeigt den Start des Frames (`10101011`).
Destination MAC-Adresse	6 Bytes	MAC-Adresse des Empfängers.
Source MAC-Adresse	6 Bytes	MAC-Adresse des Senders.
Type / Length	2 Bytes	Gibt an, welches Protokoll (z. B. IP, ARP) transportiert wird.
Daten (Payload)	46–1500 Bytes	Die eigentlichen Daten.
Pad (optional)	0–46 Bytes	Falls das Datenfeld zu kurz ist, wird Padding eingefügt, um die Mindestlänge (64 Bytes) zu erreichen.
Frame Check Sequence (FCS)	4 Bytes	Fehlererkennung mit **CRC-32**.

!Mindestlänge eines Frames:
Ethernet hat eine Mindestlänge von 64 Bytes (512-Bit) =6+6+2+46+4
Warum gibt es eine Mindestlänge:
-während der Übertragung kann es Kollisionen geben
-wenn ein Frame zu kurz ist (invalid frame), könnte der Sender den Konflikt nicht erkennen
-Kollisionserkennung muss während der gesamten Übertragung möglich sein
-Padding ist erforderlich, um die Kollisionserkennung zu gewährleisten
-wenn ein Frame zu kurz ist, könnte es passieren, dass eine Station den Frame komplett sendet und erst danach die Kollision bemerkt-das wäre zu spät
-Mindestlänge von 64 Bytes stellt sicher, dass das Signal genügend Zeit hat, um das gesamte Netzwerk zu durchlaufen, bevor der Frame vollständig gesendet wird
-wenn eine Kollision auftritt, kann sie noch erkannt und behandelt werden, in der Sender die Übertragung stoppt

!Kollisionserkennung:
1-Carrier Sense (CS): die Station, die senden möchte, hört das Medium ab, ob das Medium frei ist. Falls das Medium frei ist, beginnt sie mit dem Senden
2-falls zwei oder mehr Stationen gleichzeitig senden, kollidieren ihre Signale
3-Collision Detection (CD): jede sendende Station hört das Medium ab während der Übertragung und vergleicht ihr gesendetes Signal mit dem tatsächlichen Signal auf dem Medium. Falls das empfangene Signal anders ist als das gesendete, liegt eine Kollision vor
4-Jamming Signal: wenn eine Kollision erkannt wird, sendet die betroffene Station ein Jamming SIgnal zur Signalisierung der Kollision. Dadurch wird sichergestellt, dass alle anderen Stationen ebenfalls die Kollision bemerken
5-Alle betroffenen Stationen beenden sofort ihre Übertragung. Jede Station wartet eine zufällige Zeit (berechnet mit dem Binary Exponential Backoff Algorithmus), bevor sie es erneut versucht
!Binary Exponential Backoff Algorithmus:
die Wartezeit nach einer Kollision wird zufällig aus einem Intervall gewählt
das Intervall wird mit jeder neuen Kollision exponentiell verdoppelt

Anzahl der Kollisionen (n)	Mögliche Wartezeiten (r · Δt, in Slots)
1. Kollision	0 oder 1
2. Kollision	0, 1, 2 oder 3
3. Kollision	0, 1, 2, 3, 4, 5, 6 oder 7
n. Kollision	0 bis $2^k - 1$ (mit $k = \min(n, 10)$)
Nach 16 Kollisionen	Fehler wird an Layer 3 (IP) gemeldet

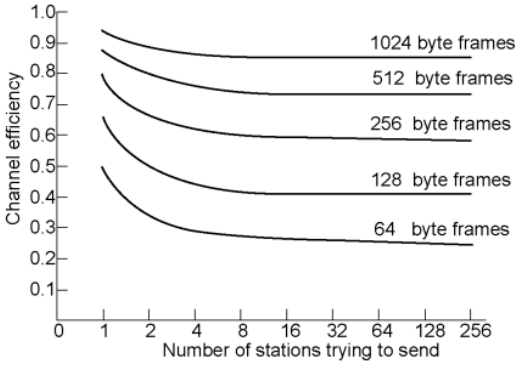
Formel für Backoff-Zeit:

$$\text{backoff} = r \cdot \Delta t, \quad 0 \leq r < 2^k$$

- Δt = 512 Bit-Zeiten (51,2 µs bei 10 Mbps)
- k wächst mit ieder Kollision. maximal bis 10

- n = number of unsuccessful attempts to send (1 ≤ n ≤ 16)

!Kanal-Effizienz in Abhängigkeit der Netzwerklast:
x-Achse: Anzahl der Stationen, die gleichzeitig versuchen zu senden (Netzwerklast)
y-Achse: Wie viel der verfügbaren Bandbreite tatsächlich für erfolgreiche Datenübertragung genutzt wird (Kanal-Effizienz)



anfangs (wenige sendende Stationen)-Kanal-Effizienz ist hoch, weil nur wenige Stationen senden -> kaum Kollisionen
steigende Anzahl an Stationen: -mehr Stationen = mehr Kollisionen -> mehr Zeit für Backoff -> weniger effektive Übertragungszeit
-kleine Frames haben extrem niedrige Effizienz, weil mehr Kollisionen auftreten, der Overhead-Anteil relativ größer ist und Backoff-Zeiten überwiegen
-große Frames haben höhere Effizient, da bei erfolgreicher Übertragung mehr Daten pro erfolgreichem Frame gesendet werden können

Früher nutzte Ethernet Hubs, die Daten an alle Geräte im Netzwerk sendeten.
Problem: Hohe Kollisionen, ineffiziente Nutzung der Bandbreite, langsame Ethernet-Netzwerke.
Heute sind Switches der Standard in Ethernet (IEEE 802.3).

- Jeder Port ist eine eigene Kollisionsdomäne → Keine Kollisionen mehr
- Switches leiten Ethernet-Frames gezielt weiter (MAC-Adress-Tabelle)
- Full-Duplex unterstützt → CSMA/CD nicht mehr nötig
- Moderne Ethernet-Netzwerke nutzen nur noch Switches für höhere Effizienz und Sicherheit

Fazit: Hubs sind veraltet – Ethernet-Netzwerke nutzen heute ausschließlich Switches.

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">channel is checked (regarding decision to send, not with regard to collision)</th><th colspan="3">behavior in case of desire to send and if one of the following states has been determined</th><th rowspan="2">Time slot</th></tr>
<tr><th>before</th><th>during</th><th>after</th><th>busy</th><th>idle</th><th>collision</th></tr>
<tr><td rowspan="5">ALOHA</td><td>pure</td><td></td><td></td><td>X</td><td colspan="2" rowspan="2">sender does not know these conditions</td><td rowspan="2">re-transmit after random time interval</td><td></td></tr>
<tr><td>slotted</td><td></td><td></td><td>X</td><td>X</td></tr>
<tr><td rowspan="3">CSMA</td><td>nonpersist</td><td>X</td><td></td><td>(X)</td><td>re-check channel only after random time interval</td><td rowspan="2">sends immediately</td><td rowspan="3">wait random time interval then re-check channel and send (if possible) (depending on algorithm “idle/ busy”)</td><td></td></tr>
<tr><td>1 persist.</td><td>X</td><td></td><td>(X)</td><td>continuous wait until channel is idle</td><td></td></tr>
<tr><td>p persist.</td><td>X</td><td></td><td>(X)</td><td>initially: continuous wait until chnl/slot idle</td><td>sends with probability p, waits with probability 1-p (for next slot, then re-checks status)</td><td>X</td></tr>
<tr><td colspan="2">CSMA/CD</td><td>X</td><td>X</td><td></td><td colspan="2">depending on procedure, (see above) 1-persistent is e.g. Ethernet</td><td>Terminates sending immediately, waits random time</td><td></td></tr>
</table>

5.1. IEEE 802.3u: Fast Ethernet
Einführung 1995 als 100 Mbit/s-Standard.
Prinzip: Beibehaltung des CSMA/CD-Protokolls, aber Bit-Dauer von 100 ns auf 10 ns reduziert.
Einschränkung:
- Kollisionsdomäne (maximale Netzwerkausdehnung) auf nur 412 m reduziert.
- Hohe Kollisionsrate → Geringere Effizienz bei vielen Stationen.

5.2.. IEEE 802.3z: Gigabit Ethernet
1998 standardisiert, um Ethernet auf 1 Gbit/s zu beschleunigen.
Zwei Betriebsmodi:
- Full-Duplex (Point-to-Point, Switched Ethernet) → Keine CSMA/CD nötig.
- Half-Duplex (Shared Broadcast Mode) → CSMA/CD bleibt erhalten.

Einführung von Carrier Extension (Frame-Mindestgröße auf 512 Byte erhöht) und Frame Bursting (mehrere Frames in einer Übertragung senden) für höhere Effizienz.

5.3. IEEE 802.3ae: 10 Gigabit Ethernet
2002 standardisiert, basiert auf optischen Fasern (später auch Kupfer).
Kein CSMA/CD mehr notwendig, da nur Full-Duplex unterstützt wird.

5.4. 40 Gbit/s und 100 Gbit/s Ethernet
IEEE 802.3ba (2010) und spätere Standards.
Hauptziel: Beibehaltung des Ethernet-Frame-Formats mit minimaler Verzögerung.
Einführung verschiedener optischer und elektrischer Schnittstellen für unterschiedliche Reichweiten.

5.5. Drahtlose Netzwerke – IEEE 802.11

Probleme mit CSMA/CD in WLANs:

- Signalstärke nimmt mit der Entfernung ab.
- Kollisionen werden nicht immer erkannt (Hidden Terminal Problem).

MACA (Multiple Access with Collision Avoidance):

- Verwendet RTS (Request to Send) und CTS (Clear to Send), um Kollisionen zu vermeiden.

IEEE 802.11 (Wi-Fi):

- CSMA/CA statt CSMA/CD → Kollisionen vermeiden, nicht erkennen.
- Dynamische Zeitfenster (IFS, Inter-Frame Spaces) bestimmen, wer zuerst senden darf.

Fazit

- Ethernet hat sich von 10 Mbps (CSMA/CD) zu 100 Gbps (Switched Ethernet, Full-Duplex) entwickelt.
- CSMA/CD ist in modernen Netzwerken nicht mehr relevant (da Fast Ethernet und Gigabit Ethernet Switched LANs nutzen).
- WLAN verwendet CSMA/CA, um Kollisionen zu vermeiden, da CSMA/CD hier nicht funktioniert.
- Höhere Geschwindigkeiten und neue Technologien (z. B. Frame Bursting, Carrier Extension) verbessern die Effizienz von Gigabit-Ethernet.

Hidden und Exposed Terminal Problem in WLANs:

WLANs verwenden CSMA/CA (Collision Avoidance) anstelle von CSMA/CD, weil Kollisionen nicht direkt erkannt werden können. Zwei Hauptprobleme dabei sind das Hidden Terminal Problem und das Exposed Terminal Problem.

!Warum passiert das nur in WLANs und nicht in Ethernet?

-In Ethernet (Kabelnetzwerken) können alle Geräte das gleiche Medium abhören.
-In WLANs ist die Reichweite begrenzt, und Signale werden durch Wände, Störungen oder Entfernungen geschwächt, sodass nicht alle Geräte sich gegenseitig wahrnehmen können.
-CSMA/CD (Collision Detection) funktioniert nicht in WLANs, weil ein sendendes Gerät sein eigenes Signal nicht hören kann → Deshalb wird CSMA/CA (Collision Avoidance) verwendet.

1. Hidden Terminal Problem (verstecktes Terminal):

Ein Hidden Terminal ist ein Gerät, das mit einem Access Point (AP) oder einem anderen Gerät kommunizieren will, aber nicht alle anderen sendenden Geräte "sehen" kann.
Dadurch kann es ungewollt eine Kollision verursachen, weil es nicht merkt, dass jemand anderes gerade sendet.

Problem::

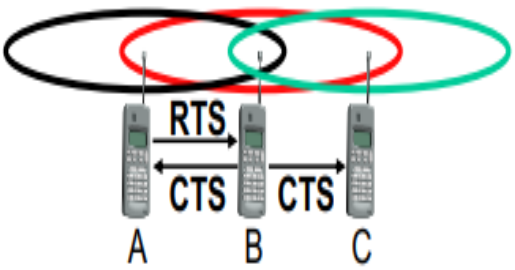
- A und C wollen gleichzeitig Daten an B senden.
- Da A und C sich gegenseitig nicht hören können (Hidden Terminal), könnten sie eine Kollision am Empfänger B verursachen.

Warum passiert das?

- In kabelgebundenen Netzen kann jede Station das Medium überwachen (CSMA/CD).
- In WLANs ist die Reichweite begrenzt, sodass manche Geräte sich gegenseitig nicht erkennen.

Lösung durch MACA (RTS/CTS):

1. A sendet zuerst eine RTS-Nachricht (Request to Send) an B.
2. B sendet eine CTS-Nachricht (Clear to Send) zurück an A.
3. C empfängt die CTS-Nachricht von B und weiß jetzt, dass B gerade mit A kommuniziert.
4. C wartet, bis die Übertragung von A abgeschlossen ist, um eine Kollision zu vermeiden.



2. **Exposed Terminal Problem (offenes Terminal):**

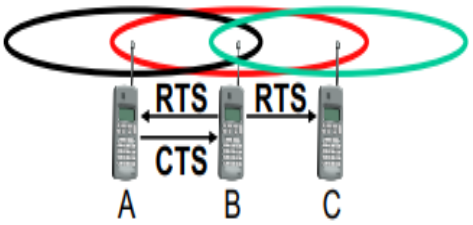
Ein Exposed Terminal ist ein Gerät, das nicht sendet, weil es fälschlicherweise glaubt, dass es eine andere Übertragung stören würde.
Das Medium wird unnötig blockiert, obwohl eine parallele Übertragung möglich wäre.

Problem:

- B will Daten an A senden, während C Daten an ein anderes Gerät senden möchte.
- C hört B‘s RTS-Signal und würde normalerweise denken, dass das Medium belegt ist, obwohl es A gar nicht erreichen will (Exposed Terminal).
- In einem normalen CSMA/CA-Netzwerk würde C unnötig warten, obwohl es eigentlich problemlos senden könnte.

Lösung durch MACA (RTS/CTS):

1. B sendet eine RTS-Nachricht an A.
2. A sendet eine CTS-Nachricht zurück an B.
3. C hört B's RTS, aber nicht A's CTS.
4. Da C keine CTS empfängt, weiß es, dass es nicht in dieselbe Übertragung eingreifen würde.
5. C kann jetzt trotzdem Daten senden, weil er erkennt, dass seine Übertragung unabhängig ist.



Data Link Layer - Internetworking

Die Verbindung unterschiedlicher Netzwerke (Internetworking) wird durch unterschiedliche Netzwerkgeräte wie Repeater, Bridges, Switches, Router und Gateways durchgeführt.

Gründe für die Internetworking:

bessere Skalierbarkeit und Sicherheit
Ressourcenteilung
höhere Verfügbarkeit

Netzwerke können auf verschiedenen Schichten verbunden werden:

Schicht	Gerät	Funktion
Layer 1 (Physikalische Schicht)	Repeater / Hub	Verstärkt Signale, verbindet Kabelsegmente.
Layer 2 (Data Link Layer)	Bridge / Switch	Verbindet LANs, arbeitet mit MAC-Adressen.
Layer 3 (Netzwerkschicht)	Router	Verbindet verschiedene Netzwerke, arbeitet mit IP-Adressen.
Layer 4-7 (Transport & Anwendungsschicht)	Gateway	Konvertiert Protokolle zwischen Netzwerken.

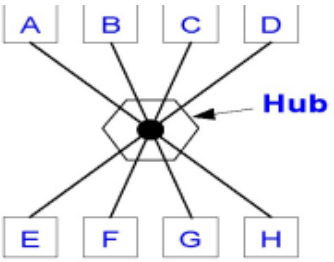
Geräte für Internetworking:

1. Repeater & Hubs (Layer 1 – Physikalische Schicht):

Repeater:

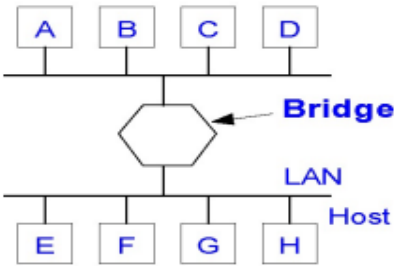
- Verstärkt und regeneriert schwache oder verrauschte Signale in Netzwerken.
- Wird verwendet, um die Reichweite eines Kabelsegments zu verlängern.
- Arbeitet auf Bit-Ebene, ohne zu prüfen, welche Daten übertragen werden.
  Problem: Kann keine Kollisionen verhindern und erhöht nur die Signalreichweite.

Hub:



- Ein Multiport-Repeater, der Daten an alle angeschlossenen Geräte sendet.
- Keine Intelligenz – verteilt das Signal einfach an alle Ports.
- Alle Geräte im Hub teilen sich eine einzige Kollisionsdomäne
  Problem: Hohe Kollisionsrate → Ineffizient bei steigender Netzwerklast.
  Wurde durch Switches ersetzt.

2. Bridges & Switches (Layer 2 – Data Link Schicht)



Bridge:

- Verbindet zwei oder mehr LAN-Segmente und filtert Daten anhand von MAC-Adressen.
- Arbeitet auf Frame-Ebene (Layer 2) und lernt MAC-Adressen automatisch.
- Kann Kollisionen zwischen Segmenten reduzieren.
  Problem: Schleifen können auftreten, wenn mehrere Bridges miteinander verbunden sind.
  Lösung: Spanning Tree Protocol (STP) zur Vermeidung Loops.
  Heute durch Switches ersetzt

Arten von Bridges

a-Transparent Bridge: Funktioniert ohne Konfiguration, erstellt MAC-Adress-Tabellen automatisch.

Funktionsweise:

-Die Bridge „hört" den Datenverkehr mit und merkt sich, welche MAC-Adresse zu welchem Port gehört.

-Wenn die Bridge das Zielgerät kennt, sendet sie den Frame nur an den richtigen Port.

-Wenn die Bridge die MAC-Adresse nicht kennt, sendet sie den Frame an alle Ports außer dem Ursprungsport (Flooding).

-Nach der Antwort lernt die Bridge die MAC-Adresse und speichert sie für zukünftige Kommunikation.

Problem:

Schleifen können auftreten, wenn mehrere Bridges miteinander verbunden sind.
Lösung: Spanning Tree Protocol (STP) zur Vermeidung von Loops.

b-Source Routing Bridge: Sender gibt expliziten Pfad zum Empfänger an (zB: in TokenRing)

Funktionsweise:

-Wenn ein Sender eine Nachricht an ein Zielgerät senden will, sucht es nach verfügbaren Routen und fügt den gewählten Pfad in den Frame-Header ein.

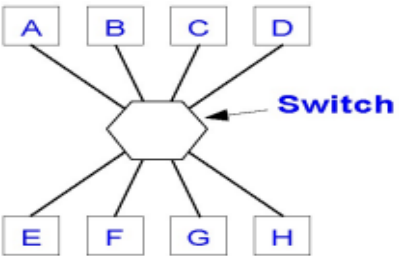
-Die Bridge leitet den Frame genau nach dieser Route weiter, ohne eigene Routing-Entscheidungen zu treffen.

Vorteile: kein unnötiges Flooding, klare Pfadkontrolle

Nachteile: hohe Verwaltungsaufwand, ineffizient in dynamischen Netzwerken

Switch:

- Ersetzt Hubs und Bridges in modernen Netzwerken.
- Jeder Port ist eine eigene Kollisionsdomäne → Keine Kollisionen mehr.
- Speichert MAC-Adressen in einer CAM-Tabelle (Content Addressable Memory).
- Leitet Frames gezielt an das Zielgerät weiter.
  Vorteile:
  -Vollduplex-Betrieb möglich → Kein CSMA/CD erforderlich.
  -Schnellere Datenübertragung als Hubs oder Bridges.



!Ein Switch verbindet Geräte innerhalb eines Netzwerks (LAN) und arbeitet mit MAC-Adressen.
!Ein Router verbindet unterschiedliche Netzwerke (LAN zu WAN oder LAN zu LAN) und arbeitet mit IP-Adressen.
!Ohne einen Router kann ein lokales Netzwerk nicht mit dem Internet kommunizieren.

!Ein Switch kann keine Verbindung zum Internet herstellen, weil er nur innerhalb eines Netzwerks (LAN) arbeitet und keine IP-Adresszuordnung oder Routing-Funktionen besitzt.
!Ein Router besitzt eine **WAN-Schnittstelle**, die mit dem Internet verbunden ist, und eine **LAN-Schnittstelle**, die mit dem lokalen Netzwerk verbunden ist.

3. Router (Layer 3 – Netzwerkschicht)

Router:

- Verbindet verschiedene Netzwerke anhand von IP-Adressen.
- Entscheidet den besten Pfad für Datenpakete (Routing).
- Verwendet Routing-Tabellen und Routing-Protokolle (z. B. OSPF, RIP, BGP).
- Arbeitet zwischen LANs und WANs.
  Routing-Funktionen:
  -Statisches Routing: Administrator definiert feste Routen.
  -Dynamisches Routing: Router lernen automatisch den besten Weg.
  Problem:
  -Routing ist langsamer als Switching, da IP-Pakete analysiert werden müssen.
  -Router haben mehr Verarbeitungsaufwand als Switches.

4. Gateways (Layer 4-5 – Transport- & Application Layer)

- Übersetzt Protokolle zwischen unterschiedlichen Netzwerken.
- Kann Daten von einem Format in ein anderes konvertieren.
  Einsatzgebiete:
  -Verbindung von heterogenen Netzwerken mit unterschiedlichen Protokollen.
  -Kommunikation zwischen alten und neuen Systemen.
  Problem:
  -Sehr hoher Rechenaufwand → Latenz kann ein Problem sein.

Gerät	Welche Schicht?	Was verbindet es?	Hauptfunktion
Bridge	Schicht 2 (Data Link)	Zwei oder mehrere **Netzwerksegmente**	Segmentierung, Kollisionsvermeidung
Switch	Schicht 2 (manchmal Schicht 3)	Mehrere Geräte im **gleichen LAN**	Schnelle, gezielte Weiterleitung von Frames
Router	Schicht 3 (Network)	Verschiedene Netzwerke (z. B. LAN und WAN)	Leitet Pakete über Netzwerke anhand von IP-Adressen