2.2a OSI-Referenzmodell: Schicht 2a – Mediumzugriff

PROVISORISCH, UPDATE AM 13.7.2002

- Aufgaben und Funktionen
- ALOHA, Slotted-ALOHA, CSMA, CSMA/CD
- Ethernet 10/100 Mbit/s, 1 Gbit/s, 10 Gbit/s

Medienzugriffsprotokolle

Zur Abwicklung eines geordneten Zugriffs auf ein gemeinsames Übertragungsmedium sind Medienzugriffsprotokolle notwendig. Man spricht von einem MAC-Protokoll (Medium Access Control). Gemeinsame Medien findet man zum Beispiel in lokalen Netzen (LAN, Local Area Network), in Mobilfunknetzen (gemeinsame Funkschnittstelle) und in Satellitennetzen. Ausgehend von Ethernet und Token Ring als den bekanntesten Vertretern der ersten LAN-Generation hat sich eine Vielzahl von Medienzugriffsprotokollen entwickelt. Demnach finden in nahezu allen Protokollen Modifikationen oder Kombinationen folgende Basismechanismen Verwendung:

- zufälligen Zugriff
- Tokenverfahren
- Reservierungsverfahren
- Schedulingverfahren
- Creditverfahren

Beim **zufälligen Zugriff** mit den Protokollen ALOHA und Slotted-ALOHA senden die Stationen ihre Pakete unkoordiniert weg. Bei diesem unkontrollierten Medienzugriff können mehrere Stationen gleichzeitig senden. Die Übertragungssignale deren Pakete werden sich dann überlagern und die Pakete werden dadurch zerstört. Es finden Kollisionen statt. Deshalb müssen das MAC-Protokoll oder Instanzen auf höheren Protokollebenen Mechanismen zur Erkennung und Behebung möglicher Datenverluste beinhalten. Beim MAC-Protokoll Ethernet oder CSMA/CD (Carrier Sense Multiple Access with Collision Detection) prüft eine Station vor dem Sendebeginn, ob das Medium aktuell frei ist. Durch Signallaufzeiten auf dem Medium können bei dem Verfahren trotzdem Kollisionen auftreten.

Token-Verfahren vergeben das Senderecht in zyklischer Reihenfolge an alle Stationen. Dabei kann das Token explizit als Bitmuster von einer Station zur nächsten weitergereicht oder ein vordefinierter Netzzustand als virtuelles Token interpretiert werden. Aus verschiedenen Servicekonzepten (Single-, Multiple- oder Exhaustive Service) und abweichenden Zeitpunkten der Weiterleitung des Token (Single Frame-, Single Token- oder Multiple Token-Verfahren) resultiert für das Token-Verfahren eine Vielzahl von Protokollvarianten.

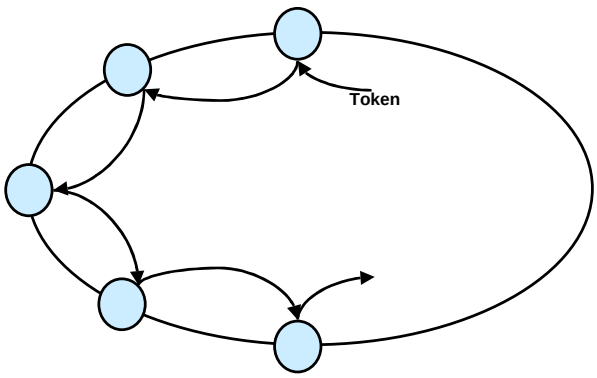


Bild: Token Passing – Explizites Token

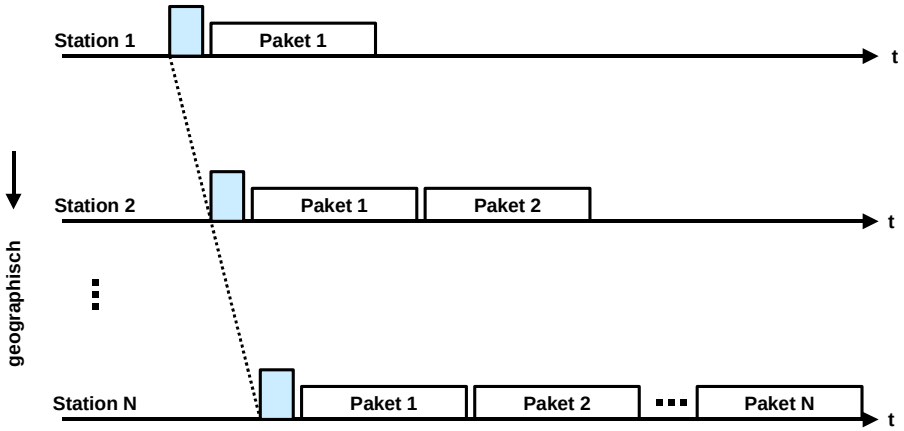


Bild: Token Passing – Implizites Token

Reservierungs-, Scheduling- und Creditverfahren haben gemein, dass sie jeder Station pro Protokollzyklus eine gewisse Sendekapazität garantieren. Bei den Creditverfahren stellt der Credit eine obere Schranke für die nutzbare Kapazität pro Zyklus dar. Dieser wird entweder global, wenn alle sendebereiten Stationen ihren Credit verbraucht haben, oder lokal durch ein ständig zirkulierendes Kontrollsignal erneuert. Bei den Reservierungs- und Schedulingverfahren wird sendebereiten Stationen auf Antrag eine feste Kapazität zugewiesen. Beide Verfahren unterscheiden sich in der zeitlichen Folge der Zuteilungs- und Sendephasen. Bei Reservierungsverfahren zerfällt ein Zyklus in eine Reservierungsphase, nach deren Abschluss jede aktive Station die ihr zugewiesene Übertragungskapazität kennt, und die sich anschließende Sendephase. Dagegen sind die Zuteilungs- und Sendephase bei den Schedulingverfahren zeitlich verschachtelt, und die Kapazitätszuteilung erfolgt parallel zum Sendevorgang auf der Basis der aktuell beantragten und der bisher genutzten Sendekapazität.

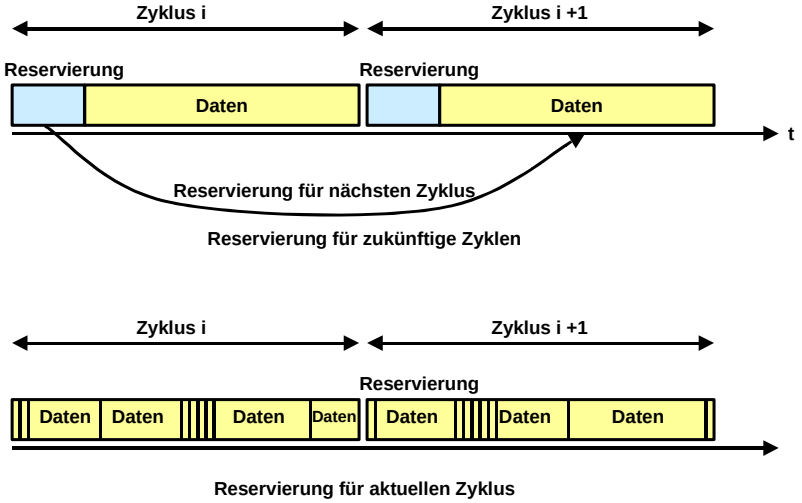


Bild: Reservierungsverfahren

Der mit ansteigender Datenrate und anwachsender Netzausdehnung größer werdende Nachteil einer zentralen Zuteilung der Kanalkapazität soll mit dem Konzept der **verteilten Warteschlange** aufgehoben werden. Dabei hat jede Station Kenntnis über die aktuell von den anderen Stationen beantragte Kapazität und kann den eigenen Sendeantrag, den sie über eine Reservierungsmeldung im Netz bekannt gibt, virtuell in eine globale Warteschlange eintragen. Da diese nach dem FIFO-Prinzip abgearbeitet wird, weiß jede Station, wann sie die beantragte Kanalkapazität belegen darf.

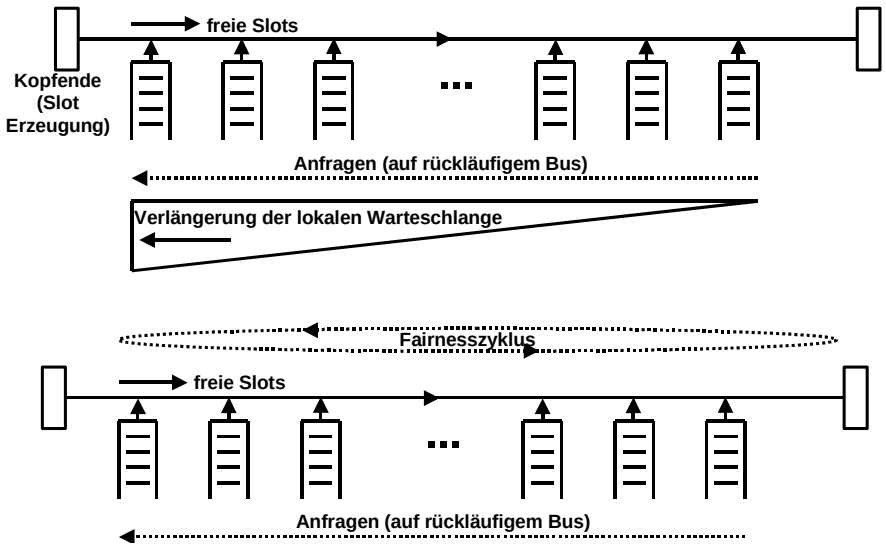


Bild: Verteilte Warteschlange

Auf einem **getakteten Ring** kreisen Slots fester Länge auf dem Medium. Jeder Slot führt Kontrolldaten mit sich, aus denen u.a. seine Ziel- und Absenderadresse, sein Typ und sein Zustand (frei / belegt) ersichtlich sind. Eine sendebereite Station erhält die Zugriffsberechtigung, wenn sie einen freien Slot empfängt und das MAC-Protokoll dessen Belegung gestattet. In Abhängigkeit davon, wie viele Slots jede Station gleichzeitig nutzen darf und ob der Sender oder der Empfänger einen Slot nach erfolgreicher Übertragung wieder freigibt, entsteht eine Vielzahl von Protokollvarianten.

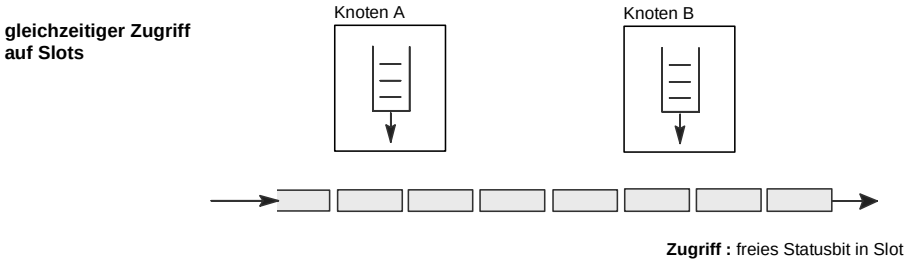


Bild: Zugriff bei getaktetem Ring

Wie beim getakteten Ring kann beim **Buffer Insertion-Ring** eine sendebereite Station das als frei erkannte Medium direkt nutzen. Dabei ist die Übertragungskapazität nicht notwendigerweise in feste Slots aufgeteilt. Pakete von variabler Länge, die nur durch ein protokollspezifisches Maximum begrenzt sind, können gesendet werden. Während des Sendevorganges werden ankommende Daten von ringaufwärts gelegenen Stationen in einem in Datenpfad installierten Schieberegister (Insertion Buffer) zwischengepuffert und erst am Ende des Sendevorganges weitergeleitet. Startet eine Station ihre Übertragung immer erst dann, wenn ihr Insertion Buffer genug Pufferkapazität zur Aufnahme eines Pakets maximaler Länge hat, können auf dem Ring keine Daten verlorengehen.

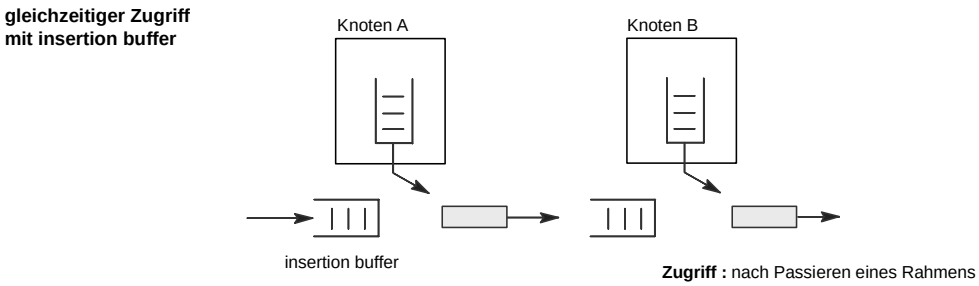


Bild: Zugriff mit Insertion Buffer

Je nach Einsatzumgebung und unterliegender Topologie zeigen die aufgeführten Zugriffsmechanismen unterschiedliche Leistungsmerkmale. Um entscheiden zu können, welche Modifikationen und Kombinationen ihren Einsatz auch in lokalen hochbitratigen Netzen ermöglichen, muss erst nach den Anforderungen an solche Systeme gefragt werden.

Quotenbasierte Protokolle

Der Medienzugriff auf einem getakteten Lokalen Netz wird von einigen Protokollen nach der Analyse des Verkehrsflusses des letzten Protokollzyklus durch die Reservierung von Übertragungskapazitäten für benachteiligte Stationen bzw. durch die kurzzeitige Blockierung dominanter Stationen geregelt. Alternativ gibt es weitere Verfahren, die für eine Medienzugriffskontrolle in lokalen hochbitratigen Netzen zur Regelung der asynchronen Datenübertragung zur Standardisierung vorgeschlagen worden sind. Zusätzlich wird ein weiteres Zugriffsprotokoll erwähnt, das ein gleichmäßiges Sendeverhalten der Stationen bewirken soll. Die Algorithmen unterscheiden sich im wesentlichen in ihren Mechanismen zur Festsetzung der Quoten und der Erkennung eines neuen Protokollzyklus.

Allgemeine Systemeigenschaften

Während das erstgenannte Protokoll universell auf getakteten Ring- und Bustopologien einsetzbar ist, bedürfen die meisten quotenbasierten Protokolle logisch immer eines getakteten Rings mit aktiv angeschlossenen Stationen. Die Verfahren arbeiten unabhängig von der Datenrate des Mediums, und alle Protokolle sind auf beiden Systemen einsetzbar, und die Daten können slot-orientiert oder in Paketen variabler Länge übertragen werden.

Alle Verfahren dienen der asynchronen Medienzugriffskontrolle mit dem Ziel einer fairen Kapazitätszuteilung und garantierter fester Obergrenzen für die Verzögerungszeiten. Dabei unterstützen sie das Prinzip des Slot Reuse durch die Freigabe und die Möglichkeit der direkten Wiederbenutzung eines Datenslots an der Zielstation.

Bei den Quotenverfahren verfügt jede Station zyklisch über eine bestimmte Quote, welche die Kanalkapazität bzw. die Anzahl der Slots bestimmt, die eine Station pro Zyklus maximal belegen darf. Die Kennzeichnung der auf dem Medium kreisenden Slots unterscheidet dabei nur zwischen frei und belegt, und freie Slots stehen aktiven Stationen für die Datenübertragung direkt zur Verfügung. Mit Ablauf ihrer Quote wird eine Station inaktiv, und sie darf solange keine Slots belegen, bis ein spezieller Initialisierungsmechanismus die Quote erneuert und ein neuer Zyklus beginnt. Eine Station wird auch dann inaktiv, wenn keine sendebereiten Daten mehr in der Sendequeue vorliegen, kann aber, sobald wieder Daten zur Übertragung bereitstehen, ohne Protokollaktion in den aktiven Zustand zurückkehren.

Beim Verfahren der Continuous Quota ist die Quote auf eine andere Art zu interpretieren. Hier wird nicht die absolut zur Verfügung stehende Kanalkapazität vorgegeben sondern die Senderate der Station gesteuert. Hat eine Station einen Slot belegt, bleibt sie solange inaktiv, bis sie der Quote gemäß viele Slots hat passieren lassen. Danach ist sie wieder aktiv und darf den nächsten freien Slot belegen. Die Grundfunktionen der Medienzugriffskontrolle in einer Station sind dennoch für alle quotenbasierten Verfahren nahezu identisch.

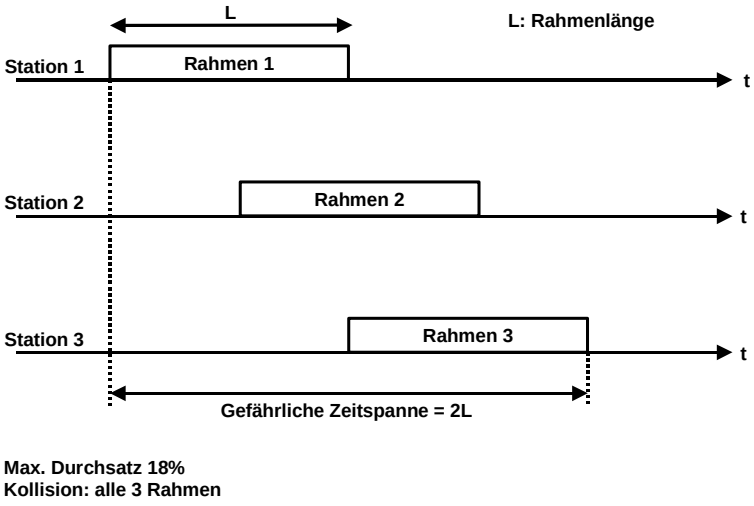


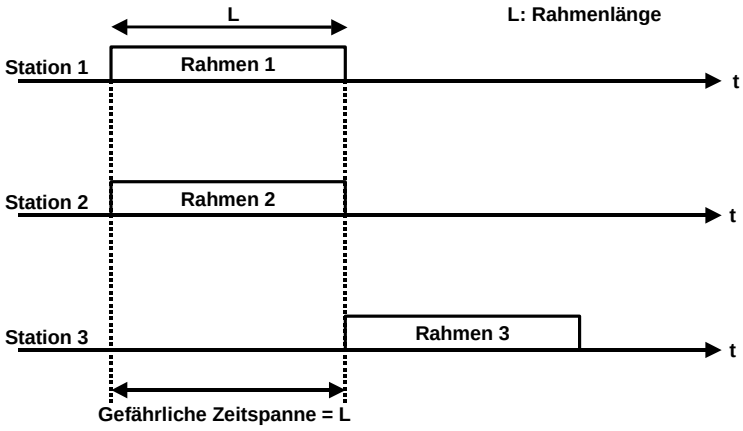
Bild: ALOHA

Reines ALOHA

Das grundlegende Konzept eines ALOHA-Systems ist einfach: Benutzer jederzeit übertragen zu lassen, wenn sie Daten senden müssen. Es treten selbstverständlich Kollisionen auf, und die kollidierenden Rahmen werden zerstört. Aber durch die Bestätigungsmöglichkeit der Broadcast-Technik kann ein Absender immer herausfinden, ob sein Rahmen zerstört wurde, indem er einfach die Meldungen des Kanals abhört. Bei einem LAN folgt diese Bestätigung unmittelbar. Bei Satelliten ergibt sich eine Verzögerung von 270 ms, bis der Absender weiß, ob die Übertragung erfolgreich war. Falls der Rahmen zerstört wurde, wartet der Absender eine zufällig gewählte Zeitspanne und sendet ihn dann nochmals.

Die Wartezeit muß zufällig sein, sonst kollidieren die gleichen Rahmen immer wieder, bis in alle Ewigkeit. Systeme, in denen Benutzer einen gemeinsamen Kanal so benutzen, daß es zu Problemen kommen kann, sind allgemein als Konkurrenzsysteme (Contention Systems) bekannt. Jedesmal, wenn zwei Rahmen zur gleichen Zeit versuchen, den Kanal zu besetzen, entsteht eine Kollision, und beide werden verstümmelt. Falls auch nur das erste Bit eines neuen Rahmens das letzte Bit eines

fast beendeten Rahmens überschneidet, werden beide Rahmen völlig zerstört, und beide müssen später erneut übertragen werden.



text text text text text text text text text text text text text text text text text text text text

Max. Durchsatz 36%
Kollision: Rahmen 1 und 2

Anwendung: Mobilfunk (GSM, GPRS, UMTS)

Bild: Slotted-ALOHA

text text text text text text text text text text text text text text text text text text text text

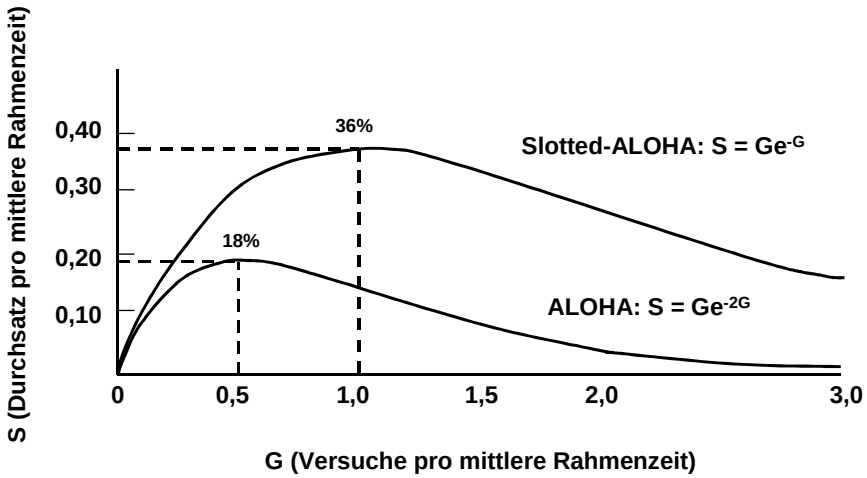
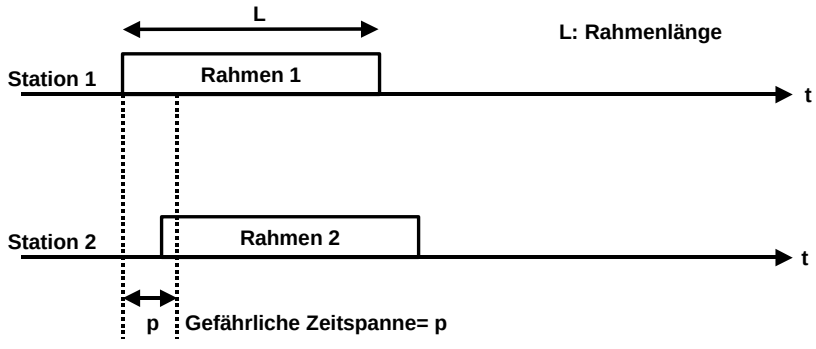


Bild: Durchsatz bei ALOHA und S-ALOHA



Kollision: Rahmen 1 und 2
p = Signallaufzeit (propagation delay)

CSMA: Carrier Sense Multiple Access

Bild: Zufällig mit Rahmen-Kollision: CSMA

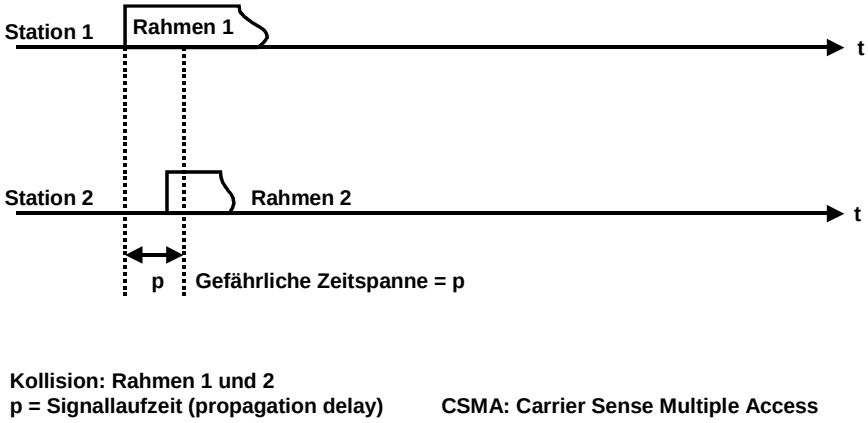
CSMA

Als erstes Trägererkennungsprotokoll befassen wir uns mit dem 1-Persistent CSMA. Wenn eine Station Daten zu übertragen hat, hört sie erst den Kanal ab, ob bereits jemand übermittelt. Ist der Kanal besetzt, wartet sie, bis er frei wird. Wenn die Station einen freien Kanal entdeckt, wird ein Rahmen übertragen. Falls eine Kollision auftritt, wartet die Station eine zufällige Zeitspanne und beginnt von vorn. Dieses Protokoll heißt 1-Persistent, weil die Station mit einer Wahrscheinlichkeit von 1 sendet, wenn der Kanal frei ist.

Die Ausbreitungsverzögerung hat einen großen Einfluß auf die Leistungsfähigkeit des Protokolls. Es gibt eine winzige Möglichkeit, daß kurz nachdem eine Station zu senden begonnen hat, eine andere Station auch senden will und den Kanal über-

prüft. Wenn das Signal der ersten Station die zweite noch nicht erreicht hat, findet die zweite einen freien Kanal vor und beginnt auch zu senden, was zu einer Kollision führt. Je größer die Ausbreitungsverzögerung ist, desto wichtiger wird dieser Effekt und desto geringer wird die Leistungsfähigkeit des Protokolls.Eine zweite Variante ist Non-persistent CSMA. Bei diesem Trägererkennungsprotokoll wird bewußt der Versuch unternommen, etwas weniger gierig zu sein als im vorherigen. Vor dem Senden überprüft eine Station den Kanal. Falls niemand sendet, fängt die Station selbst an. Ist allerdings der Kanal bereits belegt, überprüft ihn die Station nicht andauernd mit dem Hintergedanken, ihn sofort an sich zu reißen, sobald das Ende der vorherigen Übertragung erkannt wird. Statt dessen wird eine zufällige Zeitspanne gewartet und dann der Vorgang wiederholt. Dieser Algorithmus führt zu einer besseren Kanalauslastung und längeren Wartezeiten als beim 1-Persistent CSMA.

Eine weitere Variante ist P-Persistent CSMA. Es gehört zu getakteten Kanälen und arbeitet folgendermaßen: Wenn eine Station senden will, überprüft sie den Kanal. Ist er frei, sendet die Station mit einer Wahrscheinlichkeit p. Mit einer Wahrscheinlichkeit von q = 1 – p wartet sie bis zum nächsten Zeitschlitz. Ist dieser Slot auch frei, wird entweder gesendet oder gewartet, wiederum mir den Wahrscheinlichkeiten p und q. Dieser Vorgang wird wiederholt, bis entweder der Rahmen übertragen worden ist oder eine andere Station zu senden begonnen hat. Im letzteren Fall wird reagiert, als ob eine Kollision stattgefunden hat (d.h. eine zufällige Zeitspanne warten und dann alles von vorn beginnen). Wenn die Station den Kanal von vornherein belegt vorfindet, wartet sie auf den nächsten Slot und beginnt die obige Prozedur.



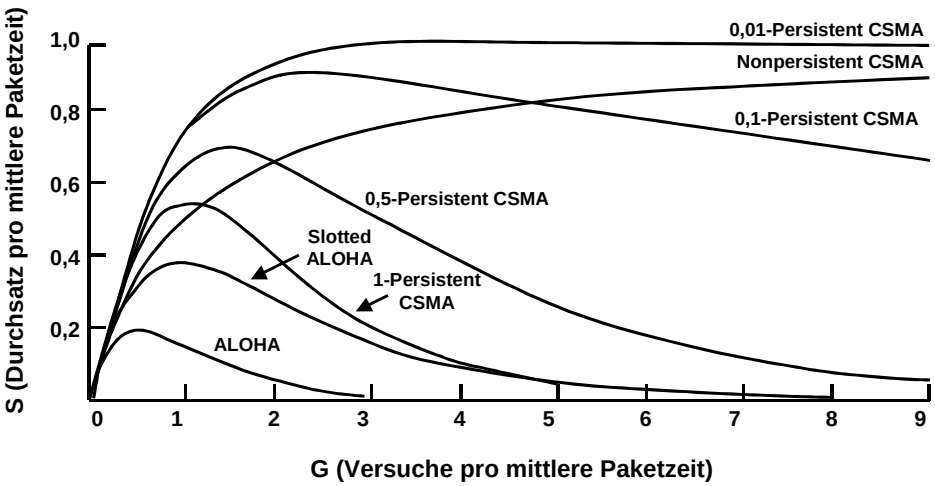
CSMA mit Kollisionserkennung

Die CSMA-Protokolle sind zweifellos gegenüber ALOHA eine Verbesserung, da sie sicherstellen, daß keine Station sendet, wenn sie den Kanal als belegt erkennt. Eine weitere Verbesserung ist der Abbruch einer Übertragung, wenn eine Kollision erkannt wird. Mit anderen Worten, wenn zwei Stationen den Kanal als frei erkennen und beide gleichzeitig zu senden beginnen, werden beide fast sofort eine Kollision erkennen.

Bild: Zufällig mit Kollisionserkennung: CSMA/CD

Anstatt die Übertragung der Rahmen zu beenden, die ohnehin irreparabel verstümmelt wären, sollten sie die Übertragung abbrechen, sobald eine Kollision erkannt wird. Die sofortige Beendigung der Übertragung bei beschädigten Rahmen spart Zeit und Bandbreite. Dieses Protokoll heißt CSMA/CD (Carrier Sense Multiple Access with Collision Detection) und wird meist bei LANs in der MAC-Teilschicht verwendet.

CSMA/CD benutzt genau wie viele andere LAN-Protokolle das folgende Konzept. Zum Zeitpunkt t_0 hat eine Station die Übertragung ihres Rahmens beendet. Jede andere Station, die einen Rahmen zu senden hat, kann das jetzt versuchen. Wenn sich zwei oder mehr Stationen gleichzeitig zum Senden entschließen, kommt es zu einer Kollision. Kollisionen können erkannt werden, indem die Leistung oder Impulsbreite des empfangenen Signals mit dem übertragenen Signal verglichen wird. Jede Station erkennt die Kollision, unterbricht ihre Übertragung, wartet eine zufällige Zeitspanne und versucht es dann erneut, unter der Annahme, daß inzwischen keine andere Station zu übertragen begonnen hat. Deshalb besteht das CSMA/CD-Modell aus abwechselnden Konkurrenz- und Übertragungsperioden, wobei Leerlauf entsteht, sobald keine Station sendet.



Das Bild zeigt den Durchsatz gegenüber dem Verkehrsangebot für alle drei Protokolle sowie das reine und getaktetes ALOHA.

Bild: Zufallsgesteuerte Protokolle: Durchsatz

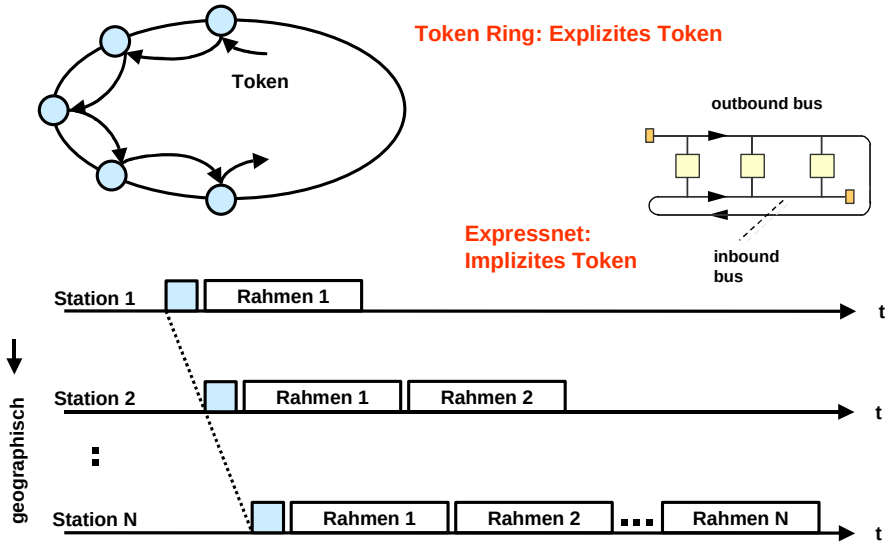
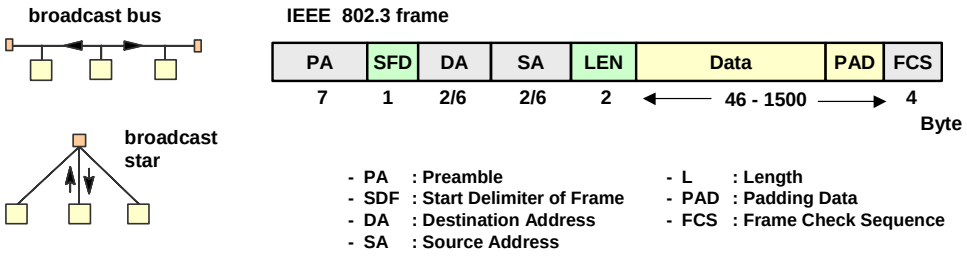


Bild: Token passing
text text text text text text text text text text text text text text



text text text text text text text text text text

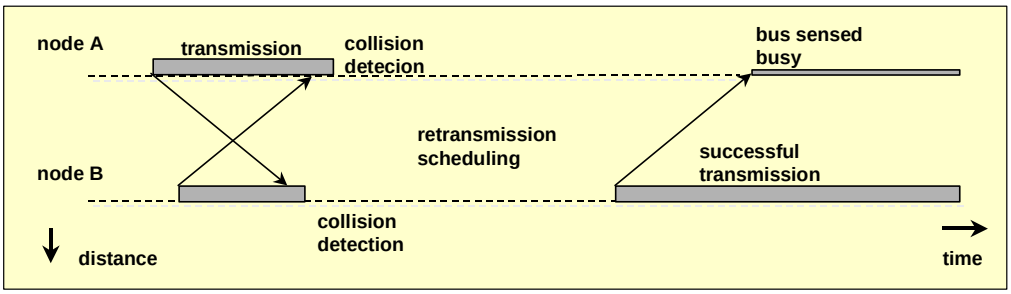


Bild: IEEE 802.3 Standard CSMA/CD

Mediumzugriffsverfahren - CSMA/CD

Der Zugriff auf das Medium erfolgt durch das CSMA/CD-Verfahren (Carrier Sense Multiple Access with Collision Detection). Das Prinzip setzt viele beteiligte Sender voraus (Multiple Access), die vor dem Senden in den Kanal hineinhören (Carrier Sense) und auch während der Datenübertragung den Kanal überprüfen (Collision Detection).
Entdeckt eine Station eine Kollision bzw. einen Fehler, so sendet sie ein sogenanntes Jamming-Signal (JAM), das sich in seiner Bitkombination deutlich von allen anderen unterscheidet und den Fehler dadurch noch verstärkt. Wenn die gleichzeitig sendenden Stationen abgebrochen haben, müssen alle einen Moment warten, damit sich der Kanal beruhigt (interframe gap). Dann wählt jede sendewillige Station mit Hilfe des Backoff-Algorithmus eine zufällige Zeitspanne, nach der sie ihren Sendevorgang wiederholt. Die Station mit der kürzesten Verzögerung beginnt die Übertragung erneut. Die restlichen Stationen hören diese Station und warten ihren Sendeversuch ab. Sollten zufällig zwei Stationen gleichzeitig begonnen haben, so tritt erneut eine Kollision auf und das beschriebene Verfahren beginnt von Neuem.
Um die Kollisionserkennung sicherzustellen, muß die minimale MAC-Frame-Dauer mindestens doppelt so groß sein wie die Signalausbreitungszeit zwischen zwei Stationen mit der maximalen Entfernung. Hierbei entsteht ein Zielkonflikt zwischen möglichst großer Buslänge, hoher Datenrate und der Möglichkeit, auch kurze Frames zu senden.
Bei einer Bitrate von 10 MBit/s ist die Bitdauer 0,1µs. Dies entspricht einer Kabellänge von 20 Metern.
Der IEEE 802.3-Standard sieht eine minimale Framelänge von 512 Bits vor, daraus resultiert die im Standard festgeschriebene maximale Signallaufzeit (Slot-Time) von 51,2µs. Die Signallaufzeit - auch Kollisionsfenster genannt - gibt die Zeit an, die maximal vergehen darf, bis ein Datenframe von einer Station an einem Ende des LANs zu einer Station am anderen Ende des LANs und wieder zurückgewandert ist. Nur so können entstandene Kollisionen von den einzelnen Stationen entdeckt werden. Das Kollisionssignal muß ankommen, bevor das letzte Frame-Bit gesendet wird.
Es ergibt sich also ein Kollisionsfenster von 51,2µs. Dieses wird benötigt, um den sogenannten Konfliktparameter K auf einem Wert kleiner 1 zu halten. Steigt K auf einen Wert größer 1, könnte ein Sender seine gesamte Nachricht über den Kanal übergeben, ohne daß ein Konflikt erkennbar würde.
Der Parameter K berechnet sich aus den Formeln:

$$K = \frac{\text{max. Signallaufzeit}}{\text{Nachrichtenübertragungszeit}}$$

$$K = \frac{\text{Kanallänge / Signalgeschwindigkeit}}{\text{Nachrichtenlänge / Kanalübertragungsrate}}$$

Die Grenzen für CSMA/CD liegen also u.a. in der Distanz, in der Bitrate und in der minimalen Framelänge.
Die Funktionen von CSMA/CD lassen sich in fünf Gruppen aufteilen:

- Sendedaten-Verpackung (transmit data encapsulation)
- Sendedaten-Verwaltung (transmit link Management)
- Sendedaten-Codierung (transmit data encoding)
- Empfangsdaten-Decodierer (receive data Decoding)
- Empfangsdaten-Verwaltung

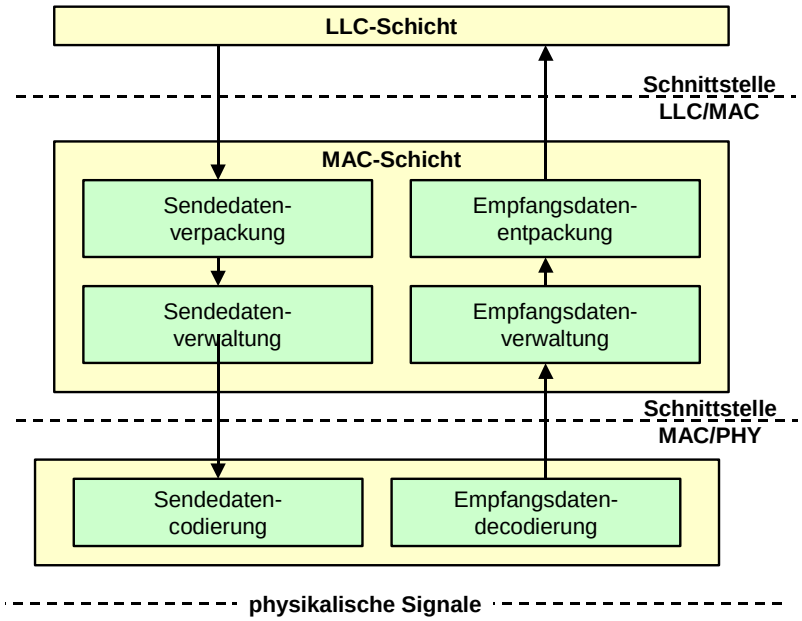
Die Funktion der Sendedatenverpackung besteht darin, einen Frame zu erzeugen, in den sie die von der LLC-Schicht erhaltenen Informationen aufnimmt.
Die Sendedatenverwaltung stellt fest, ob das Medium frei ist, und veranlaßt die Übertragung. Im Anschluß an eine Übertragung muß ein Inter Frame Gap (inter frame delay = 9,6µs) eingelegt werden, um den Frame zu schützen und um ein garantiert störungsfreies Medium für die nächste Übertragung zur Verfügung zu haben. Desweiteren veranlaßt sie bei auftretenden Kollisionen die Aussendung eines Störsignals (JAM).

Die Sendedatencodierung übernimmt den Bitstrom und codiert ihn nach dem Manchester-II-Verfahren. Der Empfangsdatendecodierer decodiert den empfangenen Bitstrom und übergibt ihn an die Empfangsdatenverwaltung. Bei der Empfangsdatenverwaltung wird die Prüfung auf Korrektheit und Vollständigkeit des empfangenen Frames durchgeführt.
Die notwendigen Informationen des CSMA/CD-Zugriffsverfahrens der MAC-Frames finden sich in dem MAC-Frame. Wie anfangs erwähnt wurde, existiert neben dem IEEE 802.3-Standard auch die Vorgängerversion Ethernet (V.2). Im Ethernet wird ein anderer MAC-Frame spezifiziert. Wie im folgenden Bild zu sehen ist, ist bei Ethernet keine Längenangabe vorgesehen, desweiteren ist keine Unterstützung bzw. eine Schnittstelle zur LLC-Schicht festgelegt. Dafür bietet Ethernet ein Typ-Feld, das Umsetzungungsmechanismen (SNAP) in die LLC-Struktur erforderlich macht.

PA	Präambel	Hierbei handelt es sich um eine Folge von 0 und 1 über 7 Byte. Sie dient zur Bitsynchronisation.
SFD	Start Frame Delimiter	Das SFD-Feld kennzeichnet den FrameBeginn und hat das Format 10101011.
DA	Destination Address	Zieladresse
SA	Source Address	Quelladresse
LEN	Length	Dieses 2 Byte große Feld enthält die Länge des Frames.
LLC		In LLC stehen die Daten, die innerhalb der LLC-Schicht erzeugt und an die MAC-Schicht übergeben wurden.
PAD	Padding	PAD ist ein Füllfeld. Wenn die Framelänge kleiner als für einen CSMA/CD-Betrieb notwendig ist, wird der Frame mit einer entsprechenden Anzahl Bytes bis zum Erreichen der Framemindestgröße (512 Bytes) aufgefüllt.
FCS	Frame Check Sequence	Das 4 Byte große Frame-Prüffeld beinhaltet eine Frame-Prüfsequenz, die mittels zyklischem Kodierungsverfahren gebildet werden. Abgesichert werden Adressen, Länge, LLC-Daten und die Füllzeichen. Ein Frame wird als fehlerhaft erkannt, wenn die Framelänge nicht mit der im Length-Feld angegebenen Länge übereinstimmt, die Framelänge nicht ein Vielfaches von 8 Bit ist oder die FCS-Prüfung negativ verläuft.

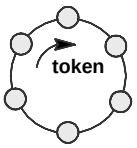
Nach einer erkannten Kollision muß die sendende Station den Sende-Prozeß unterbrechen und eine Pause einlegen. Die Pausendauer wird nach dem Backoff-Algorithmus, der für alle Stationen gültig ist, ermittelt. Die Pausendauer ist immer ein Vielfaches eines Slots. Weil das Kollisionsfenster 51,2µs groß ist, muß ein Slot eine Länge von 512 Bits haben. Um den Algorithmus an einem Beispiel zu erklären, nehmen wir i als Parameter an. Der Parameter i ist die Anzahl der Kollisionen bezüglich eines Frames. Der nächste Übertragungsversuch ist über die nächsten 2*i Slots gleichverteilt.

1. Kollision: i = 1; 2*i = 2: Der Übertragungsversuch findet im nächsten oder übernächsten Slot statt.
2. Kollision: i = 2; 2*i = 4: Der Übertragungsversuch findet innerhalb der nächsten vier Slots statt.
Der Parameter i darf maximal den Wert 10 annehmen, d.h. daß i nach der 10. Kollision nicht mehr erhöht wird (Backofflimit). Insgesamt sind nur 16 Kollisionen (attempt limit) innerhalb der Übertragung eines Frames erlaubt. Bei mehr als 16 Kollisionen wird ein Excessive Collision Error ausgegeben.

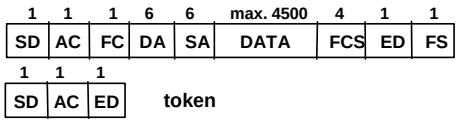


text text text text text text text text text text text text text text text text text text text text text text

Bild: IEEE 802.3 (CSMA/CD) - Funktionen

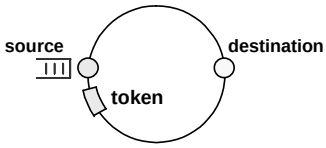


token ring

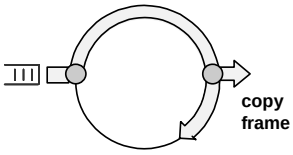


- SD : Start Delimiter
- AC : Access Control
- FC : Frame Control
- DA : Destination Address
- S A : Source Address
- FCS : Frame Check Sequence
- ED : End Delimiter
- FS : Frame Status

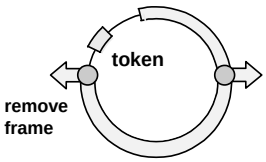
Bild: IEEE 802.5 Standard: Token Ringtext text text text text text text text text text



① source :
wait for token



② destination :
copy frame



③ source :
- remove frame
- issue token if header has returned

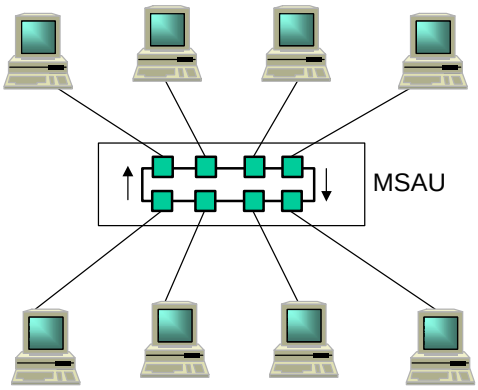
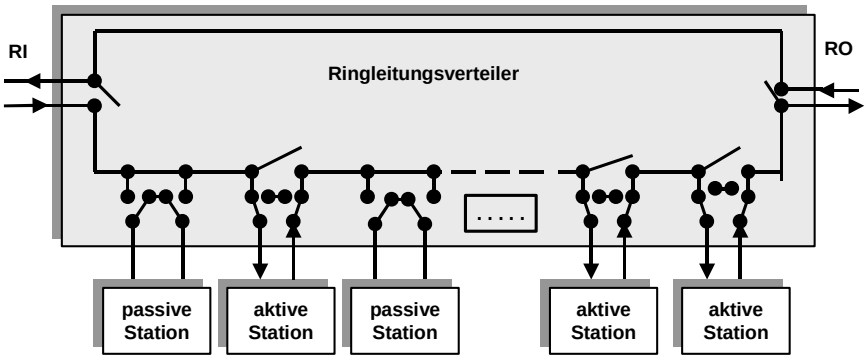


Bild: Multi-Station Access Unit (MSAU)

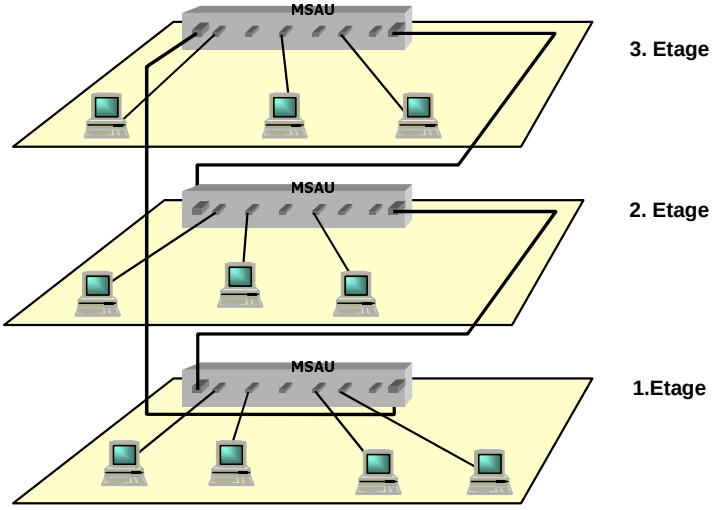
text text text text text text text text text text text text text text text text text text text text text text



text text text text text text text text text text text text text text text text text text text text

RI : Ring In
RO : Ring Out

Bild: IEEE 802.5 - Anschlusstechnik

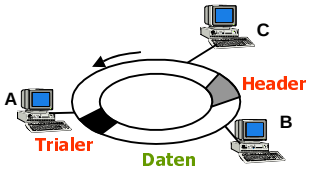


text text text text text text text text text text text text text text text text text text text text

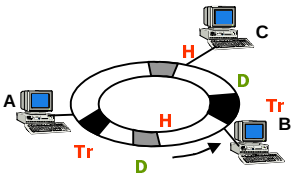
MSAU : Multi-station Access Unit

Bild: IEEE 802.5 - Gebäude-Ring

Single Token-Verfahren
nur eine Nachricht auf dem Ring



text text text text text text text text text text text text text text text text text text text text



Early Token-Release
mehrere Nachrichten auf dem Ring

Bild: IEEE 802.5 - Tokenverfahren

text text text text text text text text text text

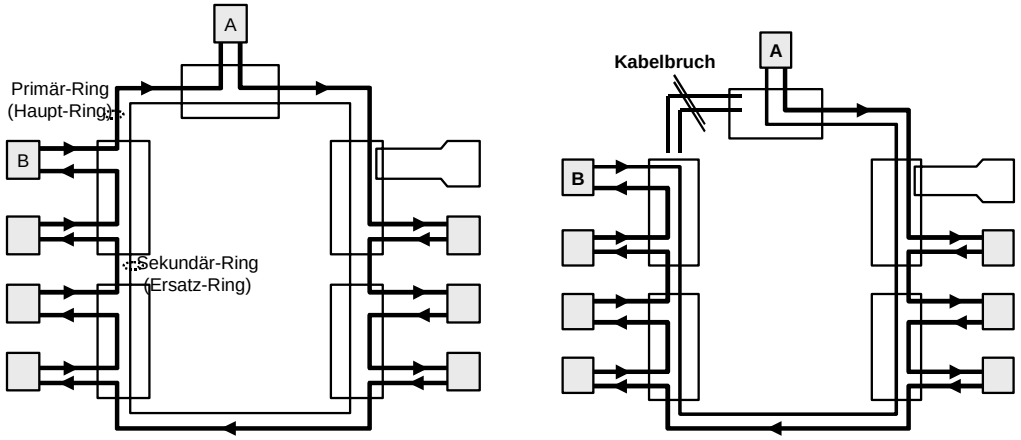


Bild: IEEE 802.5 Netztopologie

text text text text text text text text text text text text text text text text

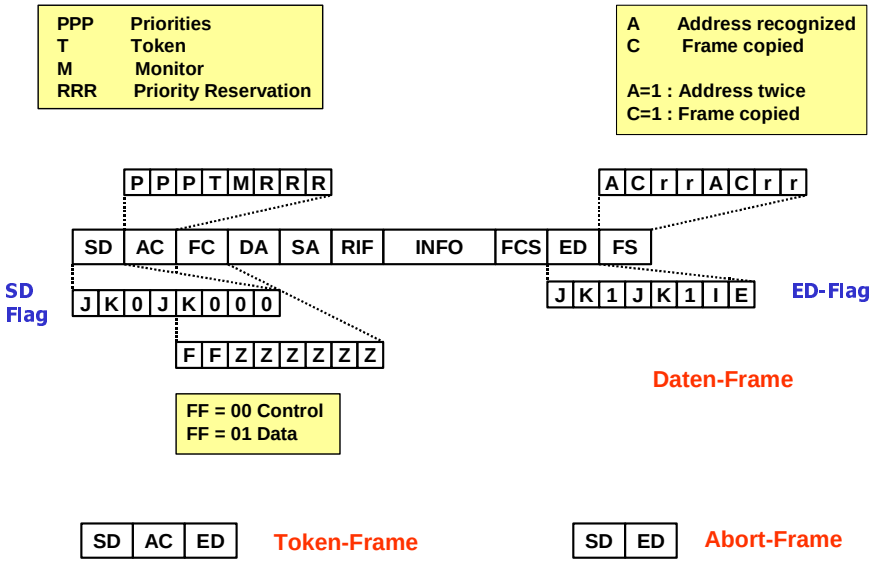


Bild: IEEE 802.5 - MAC-Frame

Mediumzugriff

Die Betriebsweise des MAC-Protokolls ist grundsätzlich unkompliziert. Wenn kein Datenverkehr vorliegt, kreist ständig ein 3-Byte-Token und wartet, daß es von einer Station dadurch übernommen wird, daß diese ein bestimmtes 0-Bit im zweiten Byte auf 1 setzt. Dieser Vorgang ändert die ersten beiden Byte in eine Rahmenstartfolge ab. Dann gibt die Station den Rest eines normalen Datenrahmens aus.

Unter normalen Bedingungen umkreist das erste Bit des Rahmens den Ring und kehrt zum Absender zurück, bevor der ganze Rahmen übertragen worden ist. Höchstens ein sehr langer Ring kann eventuell einen kleinen Rahmen als ganzen enthalten. Deshalb muß die übertragende Station den Ring leeren, während sie weitersendet. Das heißt, daß die Bits, die ihre Rundreise um den Ring beendet haben, zurückkommen und vom Absender entfernt werden.

Eine Station darf das Token höchstens für die Dauer der Token-Haltezeit behalten, die normalerweise bei 10 ms liegt, wenn nicht ein anderer Wert eingestellt wurde. Falls nach der Übertragung des ersten Rahmens noch genug Zeit bleibt, können weitere Rahmen gesendet werden. Nachdem alle anstehenden Rahmen übertragen wurden oder die Übertragung eines weiteren Rahmens die Token-Haltezeit überschreiten würde, baut die Station den 3-Byte großen Token-Rahmen wieder auf und gibt ihn auf den Ring aus.

Beim Token Ring wird zwischen zwei Stationstypen unterschieden: normale Stationen und die Monitorstation. Die Station, die sich als erste aktiv an den Ring koppelt, wird zur Monitorstation. Sie hat die besondere Aufgabe der Tokenverwaltung, d.h. sie generiert das Token, das auf dem Ring kreist.

Empfängt eine zum Senden bereite Station dieses Token, dann wandelt sie es in ein Daten-Frame um und versendet ihre Daten mit diesem Frame. Diese Daten werden dann von jeder Station empfangen, überprüft und falls die Daten nicht für sie bestimmt sind, regeneriert und auf dem Ring weitergeleitet. Sind die Daten an der Zielstation angelangt, werden sie von dieser Station kopiert, als kopiert gekennzeichnet und wieder auf den Ring weitergeleitet. Die Quellstation muß ihre eigenen Daten wieder entfernen sowie ein neues Token generieren und absenden. Mit diesem Verfahren hat die Quellstation eine einfache Kontrolle über die korrekte Rahmenübertragung.

Man unterscheidet folgende MAC-Frames:
- Token-Frame,
- Abort-Frame,
- Daten-Frame.

Ein Abort-Frame wird generiert, wenn eine Station ein fehlerhaftes Token oder einen sonstigen nicht behebbaren Fehler erkennt.

Der eigentliche Daten-Frame beinhaltet, wie auch der Token-Frame, den Starting Delimiter (SD), das Zugriffskontrollfeld (AC) und den Ending Delimiter (ED). Weiterhin werden zusätzliche Felder benötigt, um den Daten-Frame korrekt zum Empfänger zu leiten.

SD Starting Delimiter	Das erste Feld beinhaltet die Startsequenz des Frames mit der statische Bitkombination JK0JK000. Dadurch kann eine Präambel zur Bitsynchronisation entfallen.
AC Access Control	Das Zugriffskontrollfeld beinhaltet die Bitkombination PPPTMRRR (PPP – Zugriffspriorität, T – Token, M – Monitor, RRR – Prioritäten-Reservierung)
	Das Token wird durch das gesetzte Tokenbit (T=1) gekennzeichnet, das bedeutet, daß als nächstes nur noch das 1 Byte große Ending Delimiter-Feld (ED) folgen kann. Ist das T-Bit nicht gesetzt, so handelt es sich um ein Daten-Frame. Mit Hilfe der P-Bits können Zugriffsprioritäten vergeben werden. Das M-Bit kann nur von der aktiven Monitorstation gesetzt werden. Die R-Bits dienen der Reservierung von Zugriffsprioritäten.
FC Frame Control	Das Frame-Kontrollfeld hat die Bitkombination FFZZZZZZ - FF=00 MAC-Frame mit Steuerinformationen - FF=01 LLC-Frame mit Daten - Z-Bits: Kontroll-Bits für Token-Ring Protokoll und dessen Management
DA Destination Address	Entspricht dem Aufbau einer MAC-Adresse
SA Source Address	Der Aufbau der Quelladresse entspricht im wesentlichen dem Aufbau der Zieladresse, nur mit dem Unterschied, daß das 0.Bit nicht zur Unterscheidung zwischen Individual- und Gruppenadresse herangezogen wird. Wird das 0.Bit auf 1 gesetzt, bedeutet das, daß sich Routing-Informationen (RIF-Feld) im Frame befinden.
RIF Routing Information Field	Das Routing-Informationsfeld kann optional vorhanden sein und beinhaltet Informationen für das Source Routing. Diese Information ist dann wichtig, wenn mehrere LANs über Bridges vernetzt sind und sich eine Zielstation in einem anderen LAN befindet.
Info Information	Das Info-Feld beinhaltet entweder Daten oder Steuerinformationen der MAC-Schicht
FCS Frame Check Sequence	Prüfsumme. Bezieht sich alle Felder bis auf das FS-Feld und das ED-Feld alle Framefelder ab.
ED Ending Delimiter	Das ED-Feld beinhaltet die Bit-Kombination JK1JK1 I E I-Bit (Intermediate-Bit): I=1 , Frame gehört zu einer Gruppe von aufeinanderfolgenden Frames I=0 , das letzte Frame oder einzelnes Frame E-Bit (Error-Bit) wird gesetzt bei Erkennung eines Fehlers im Frame.
FS Frame Status	Das Frame-Statusfeld hat die Bitkombination ACrrACrr A-Bit (Address-Recognized-Bit), C-Bit (Frame-Copied-Bit) Die einzelnen Bits werden doppelt aufgeführt, weil das FCS-Prüffeld das FS-Feld nicht absichert. A=1 wenn eine Adresse in einem Netz doppelt vorkommt C=1 wenn eine Station die an sie adressierten Daten empfangen (kopiert) hat r-Bits für zukünftige Erweiterungen reserviert

Token Ring-Management

Die Überwachung des Token-Zugriffsverfahrens wird von einer Station im Token Ring übernommen, die als sogenannter aktiver Monitor eingesetzt wird. Die restlichen Stationen im Ring werden als Standby-Monitore (d.h. Reservemonitore) bezeichnet. Die Standby-Monitore kontrollieren die Funktionsfähigkeit des aktiven Monitors mit Hilfe spezieller Timer.

Der aktive Monitor muß:	- eine minimale Pufferkapazität im Ring sicherstellen, - ein fehlerhaftes Token oder Frame erkennen, - Mehrfachumkreisungen eines Frames verhindern, - sicherstellen, daß nur ein aktiver Monitor im Ring vorhanden ist.

Minimale Pufferkapazität
Bei Übertragungsrate von 4 Mbit/s ist ein Bit ca. 50 m lang. Weil das Token 24 Bit lang ist, müßte der Ring 1200 m lang sein. Da diese Länge in der Praxis nicht immer realisierbar ist, muß der aktive Monitor dafür sorgen, daß die Speicherfähigkeit des Ringes so groß ist wie das Token selbst, weil das Token ja die grundlegende Basis für das Token-Protokoll ist. Der Monitor stellt dazu ausreichend Pufferplatz bereit.

Es gilt: Länge des Bits = Signalausbreitungsgeschwindigkeit im Medium / Bitrate

Standardmäßig wird jeder Station eine maximal mögliche Übertragungszeit von 10 ms eingeräumt. Durch die vorgegebene Übertragungszeit ergibt sich die im Token Ring maximale Framegröße von 4000 Byte (4 Mbit/s) bzw. 18000 Byte (16 Mbit/s). Wird nun diese zur Übertragung bereitgestellte Zeit von einer Station überschritten, so wird der Token- bzw. Daten-Frame von der Monitorstation als Verlust angesehen. Treten des weiteren unvorhergesehene Fehlersituationen und damit Störungen des Token oder eines Frames auf (z.B. durch Signalverletzungen im Medium), dann wird ein neues Frei-Token generiert.

Mehrfachumkreisungen eines Frames, die dann zustande kommen, wenn eine Quellstation ihren Frame nicht vom Ring nimmt, werden vom aktiven Monitor entfernt. Hierzu setzt der Monitor das M-Bit im AC-Feld jedes Frames und erkennt somit, daß ein Frame schon zum zweiten Mal den Ring umkreist. Erhält der Monitor nun ein solches Frame, bei dem das M-Bit gesetzt wurde, dann wurde dieser Frame nicht gelöscht. Der Monitor nimmt den Frame vom Ring und generiert ein neues Frei-Token.

AMP-Frame Active Monitor Present Frame ZZZZZZ=000101	Mit Hilfe des Active-Monitor-Present-Frame, das in bestimmten Zeitintervallen vom aktiven Monitor ausgesendet wird, können die Standby-Monitore erkennen, daß immer noch ein aktiver Monitor vorhanden ist. Bleiben diese Frames aus, gehen die Stationen davon aus, daß der aktive Monitor nicht mehr funktionsfähig ist. Ist dies der Fall, dann wird der Claim-Prozeß gestartet.
Claim-Token-Frame ZZZZZZ=000011	Sollte eine Station im Ring, die nicht gerade aktiver Monitor ist, anhand Unfähigkeit eines ihrer Timer oder aufgrund fehlender AMP-Frames bemerken, daß der aktive Monitor nicht mehr korrekt funktioniert, beginnt sie, ein Claim-Token-Frame auszusenden. Nach seiner Aussendung wird das Claim-Token von Station zu Station weitergeleitet. Die einzelnen Stationen setzen als Quell-MAC-Adresse (SA-Feld) ihre eigene MAC-Adresse ein, sofern sie numerisch größer als die im Claim-Token eingetragene Adresse ist. Mit dieser Vorgehensweise wird die Station mit der numerisch größten MAC-Adresse zum neuen aktiven Monitor im Ring.
Purge-Frame ZZZZZZ=000100	Zur Initialisierung des Rings wird vom aktiven Monitor ein Purge-Frame versendet. Dies veranlaßt die Stationen, ihre Sendevorgänge abzubrechen und ihre Timer neu zu initialisieren.
SMP-Frame Standby Monitor Present Frame ZZZZZZ=000110	Ein SMP-Frame (Standby Monitor Present Frame) wird von einem Standby-Monitor in bestimmten Zeitabständen ausgesendet. Dies dient dazu, die MAC-Adresse der Station ausfindig zu machen, die sich vor der Station befindet, welche den SMP-Frame aussendet. Mit der Aussendung von SMP-Frames kennt somit jede Station im Ring ihre Vorgängerstation. Das Wissen darüber, welche Station die Vorgängerstation ist, ist für den nachfolgend beschriebenen Beacon-Prozeß besonders wichtig.
	Das SMP-Frame wird als Broadcast ausgesendet, d.h. jede Station schaut sich das SMP-Frame an. Da üblicherweise die A- (Address Recognized) und C-Bits (Frame Copied) im Frame Status Feld (FS-Feld) von den Stationen gesetzt werden, weiß die Station, die ein solches Broadcast-Frame mit nicht gesetztem A- und C-Bit empfangen hat, daß die eingetragene Quell-MAC-Adresse die Adresse ihrer Vorgängerstation sein muß. Diese Adresse wird abgespeichert und das SMP-Frame neu ausgesendet, und so weiter.
Beacon-Frame	Der Beacon-Prozeß wird nach Erkennung bzw. Lokalisierung von Netzfehlern gestartet. Fehler

ZZZZZZ=000010	treten entweder in einer Station oder im Übertragungsmedium zwischen zwei Stationen A und B auf. Der Beacon-Prozeß wird dann gestartet, wenn Station B innerhalb einer bestimmten Zeitspanne keinerlei Token bzw. Frames erhalten hat. Ist dies der Fall, nimmt Station B an, daß ein Versagen in der Vorgängerstation A oder im Übertragungsmedium dazwischen aufgetreten ist. Station B sendet daraufhin ein Beacon-Frame. In diesem Frame stehen die MAC-Adresse der Station B und die MAC-Adresse ihrer Vorgängerstation A. Die angeschlossenen Stationen, die den Beacon-Frame erhalten, senden diesen unverändert weiter und stoppen das Token Ring-Protokoll. Der Datentransport wird somit eingestellt und es wird innerhalb kürzester Zeit bekannt, daß zwischen Stationen A und B ein Fehler aufgetreten ist. Als mögliche Fehlerbehebungsmaßnahme wird die fehlerhafte Station vom Ring getrennt oder der Sekundär-Ring mit dem Primär-Ring verbunden, um so den einwandfreien Ablauf des Token Ring-Protokolls bis zur Behebung des Fehlers zu gewährleisten.

Prioritäten im Token Ring

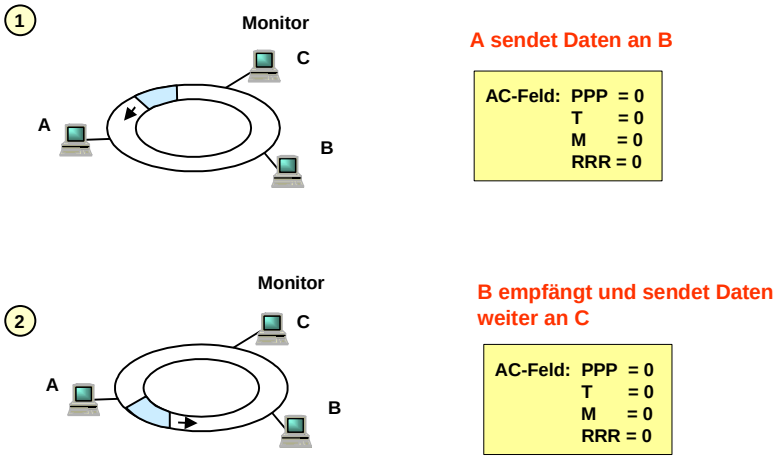
Im Token-Ring besteht die Möglichkeit, daß einzelne Stationen für Daten, die sie versenden wollen, Prioritätsstufen angeben. Diese Prioritätsstufen liegen im Bereich von 0 bis 7, wobei die 7 die höchste Priorität darstellt. Damit läßt sich die Zugriffsmöglichkeit jeder Station auf den Ring festlegen. Das bedeutet, daß eine Station nur dann auf den Ring zugreifen kann, wenn die Priorität des empfangenen Token kleiner oder gleich der Stationspriorität ist. Die Priorität eines Token wird mit Hilfe der drei P-Bits im AC-Feld des Token festgelegt.

Das 802.5-Protokoll enthält ausführliche Beschreibungen für die Behandlung von Rahmen mehrerer Prioritäten. Der 3-Byte große Token-Rahmen enthält ein Feld im mittleren Byte, das die Priorität des Tokens angibt. Will eine Station einen Rahmen der Priorität n übermitteln, muß sie warten, bis sie ein Token mit einer Priorität kleiner oder gleich n erlangt. Weiterhin kann eine Station versuchen, sich das nächste Token zu reservieren, indem sie in die Reservierungsbits eines passierenden Datenrahmens die Priorität des zu sendenden Rahmens einträgt. Wenn dort bereits eine höhere Priorität vorgemerkt ist, kann die Station keine Reservierung durchführen. Nach Beendigung des aktuellen Tokens wird das nächste Token mit der reservierten Priorität erstellt.

Durch diesen Vorgang wird die Reservierungspriorität immer höher geschraubt. Das Protokoll enthält mehrere komplexe Regeln, um dieses Problem zu eliminieren. Der Grundgedanke ist, daß eine Station, welche die Reservierungspriorität erhöht, dafür verantwortlich ist, die Priorität nach Erledigung auch wieder herabzusetzen.

Dieses Prioritätenschema unterscheidet sich grundsätzlich vom Token-Bus, bei dem jede Station immer einen gerechten Anteil der Bandbreite erhält, unabhängig davon, was bei anderen Stationen im Moment geschieht. Im Token-Ring kann eine Station verhungern, wenn sie nur Rahmen mit niedriger Priorität abzusenden hat und warten muß, bis ein Token mit niedriger Priorität auftaucht.

Das Beispiel verdeutlicht das Prioritätenschema. Dabei sind drei Stationen (A, B und C) am Ring angeschlossen. Die Station C ist der aktive Monitor. Es wird deutlich, daß die Station, bevor sie Daten mit einer bestimmten Priortät senden kann, diese durch einen Eintrag in die R-Bits des AC-Feldes anzeigen muss.



text text text text text text text text text text text text text text text text text text text text

Bild: IEEE 802.5: Prioritätszugriff (1)

text text text text text text text text text text text text text text text text text

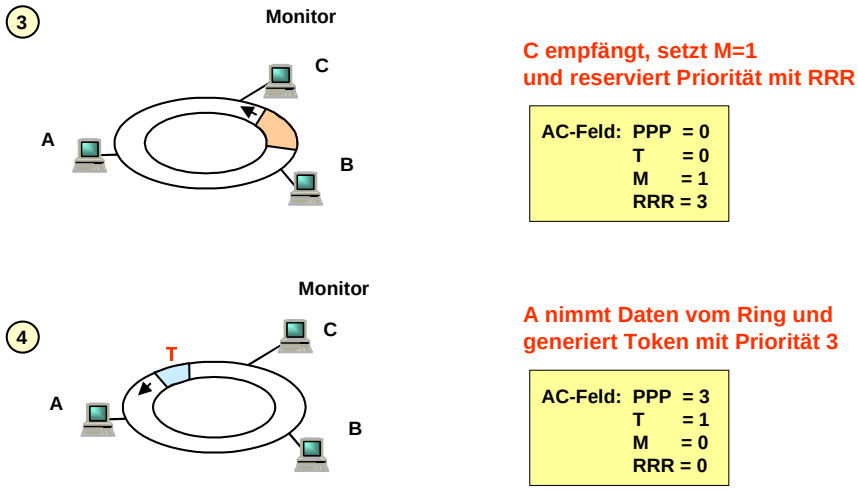


Bild: IEEE 802.5: Prioritätszugriff (2)

text text text text text text text text text text text text text text text text

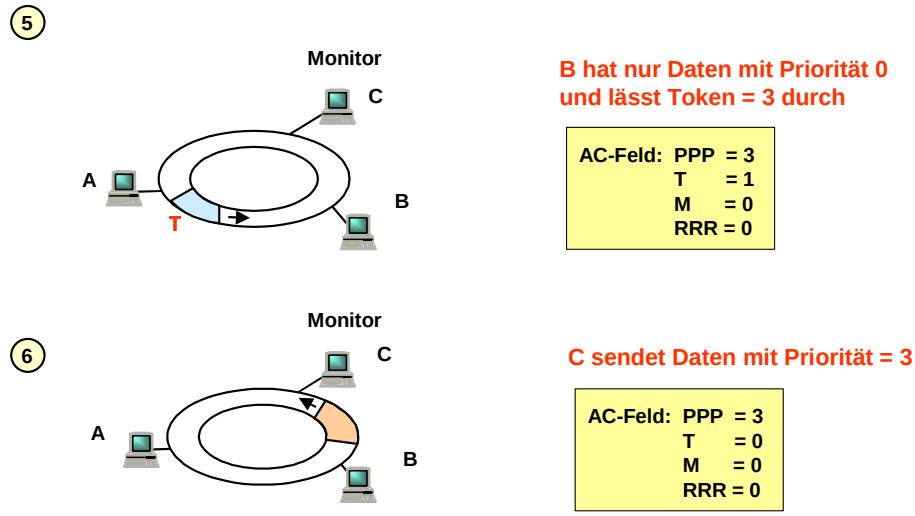


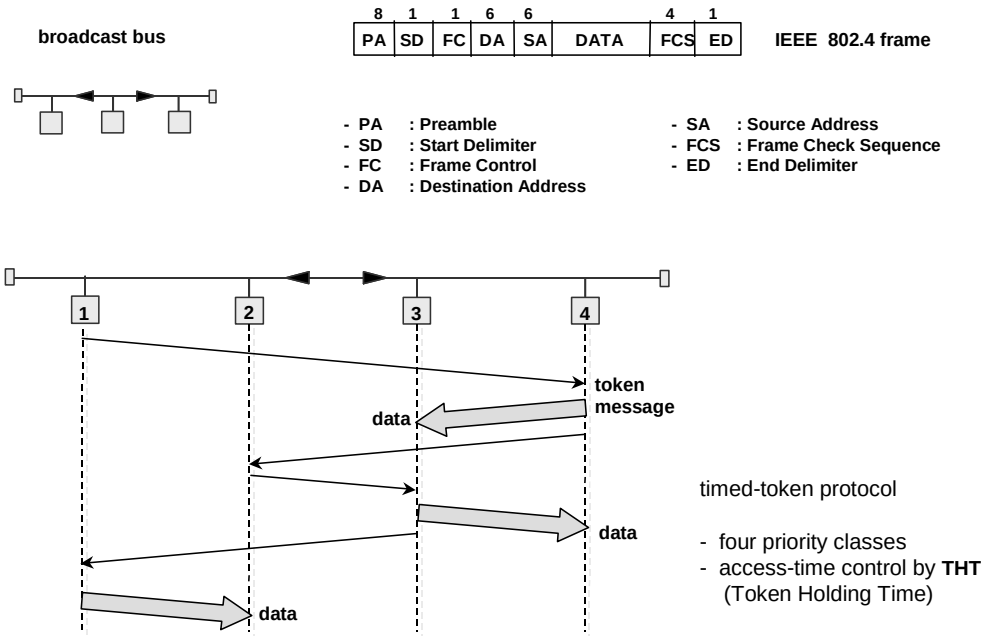
Bild: IEEE 802.5: Prioritätszugriff (3)

Weiterentwicklungen

Der ursprüngliche Token Ring wurde durch drei Konzepte weiterentwickelt:

- **Switched Token Ring.** Sein Ansatz entspricht dem des Switched Ethernet: von jedem Port des Switch zu genau einem Teilnehmer besteht eine dedizierte Verbindung mit 16 Mbit/s. An den Ports eines Switch können Teilnehmer mit 4 Mbit/s und auch mit 16 Mbit/s angeschlossen werden, was zu einer erhöhten Flexibilität führt. Damit ist das Prinzip des shared niedium, wie es beim konventionellen Token Ring besteht, ergänzt durch dedicated media zwischen dem Switch und den einzelnen Teilnehmern. Mit Token Ring Switches können auch Backbones aufgebaut werden. Backbones sind Netze höherer Leistung, die einzelne Netze (Teilnetze) zu einem gesamten Netz zusammenfügen.
- **Full-Duplex Token Ring** (auch als **DTR:** Dedicated Token Ring bezeichnet). Dieser Vorschlag ist in IEEE 802.5r standardisiert. Er ist analog zum Full Duplex Ethernet und sieht auf jeder dedizierten Verbindung zwischen Switch-Port und Teilnehmer eine Vollduplex-Obertragung vor. Damit steigt die effektive Datenrate auf 32 Mbit/s.
- **HSTR** (High-Speed Token Ring), standardisiert in IEEE 802.5t. Er ist analog zum Fast Ethernet, indem einfach die Datenrate von 16 Mbit/s auf 100 Mbit/s erhöht wird. Auf der physischen Schicht des HSTR werden die Vorgaben der physischen Schicht von Fast Eihernet übernommen. Da Fast Ethernet durch starken Wettbewerb preisgünstig ist, kann HSTR davon profitieren.

Weitere Konzepte für den Token Ring sind in Entwicklung. Dazu gehören eine Gbit/s-Variante (IEEE 802.5v), ein Konzept zur Realisierung von VLAN und das Konzept der Link Aggregation. Link Aggregation bedeutet die Verbindung zweier Switches durch parallele Links zur Erhöhung der Bandbreite.



text text text text text text text text text text text text text

Bild: IEEE 802.4 Standard: Token Bus

Token-Bus-Protokoll auf der MAC-Teilschicht

Bei der Initialisierung des Rings werden die Stationen in der Reihenfolge ihrer Stationsadressen eingefügt, von der höchsten zur niedrigsten. Die Übergabe des Tokens erfolgt ebenfalls von oben nach unten. Jedes Mal, wenn eine Station das Token erhält, darf sie für eine bestimmte Zeitspanne Rahmen übertragen. Dann muss sie das Token weitergeben. Erhält eine Station das Token, hat aber nichts zu senden, gibt sie es sofort weiter.

Der Token-Bus definiert die vier Prioritätsklassen 0, 2, 4 und 6. Für Datenverkehr; 0 ist die niedrigste und 6 die höchste Klasse. Am einfachsten kann man sich vorstellen, dass jede Station intern in vier Unterstationen entsprechend den vier Prioritätsklassen aufgeteilt wird. Wenn die MAC-Teilschicht Daten schickt, werden sie auf ihre Priorität geprüft und zu einer der vier Unterstationen weitergeleitet. Dadurch enthält jede Unterstation ihre eigene Warteschlange von zu übertragenden Rahmen.

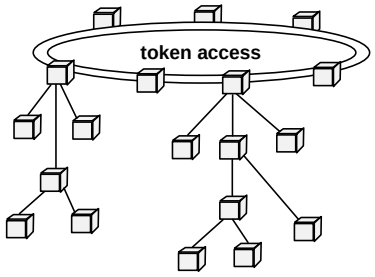
Wenn eine Station über das Kabel das Token erhält, wird es intern an die Unterstation der Priorität 6 weitergeleitet, die nun Rahmen übertragen kann, wenn welche vorhanden sind. Wenn sie fertig ist (oder der Timer abläuft), wird das Token intern an die Unterstation der Priorität 4 weitergegeben. Dieser Vorgang wird wiederholt, bis entweder die Unterstation der Priorität 0 alle eigenen Rahmen Übertragen hat oder der Timer abgelaufen ist. In jedem Fall wird das Token an die nächste Station im Ring weitergegeben. Durch genaues Setzen der Timer kann ein Mindestanteil der gesamten Token-Zeit für Datenverkehr der Priorität 6 garantiert werden. Die niedrigeren Prioritäten müssen sich mit dem zufriedengeben, was übrigbleibt. Wenn die Unterstationen mit den höheren Prioritäten ihren Anteil der verfügbaren Zeit nicht brauchen, wird er nicht verschwendet, sondern kann durch die Stationen der niedrigeren Priorität verwendet werden. Dieses Prioritätsschema, das dem Datenverkehr der Priorität 6 einen festen Anteil der Netzkapazität garantiert, kann für die Übertragung von Sprache und Datenverkehr in Echtzeit benutzt werden.

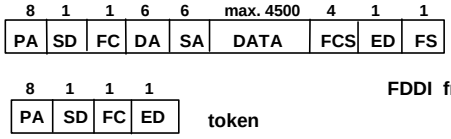
Das Rahmenformat vom Token-Bus ist im Bild dargestellt. Die Präambel wird wie bei 802.3 benutzt, um den Takt des Empfängers zu synchronisieren, allerdings kann sie 1 Byte kurz sein. Die Felder Startbegrenzer und Endbegrenzer werden benutzt, um die Rahmengrenzen zu kennzeichnen. Beide Felder beinhalten analoge Codierungen, die anderen Symbolen als 0 oder l entsprechen. Folglich können sie nicht zufällig in normalen Daten vorkommen, so dass kein Längenfeld nötig ist.

Das Feld Rahmensteuerung unterscheidet Datenrahmen von Steuerrahmen. Im Fall eines Datenrahmens enthält es auch noch die Rahmenpriorität. Es kann auch einen Indikator enthalten, der vom Empfänger eine Bestätigung über den korrekten oder fehlerhaften Empfang eines Rahmens fordert. Ohne diesen Indikator durfte der Empfänger nichts mehr senden, da er ja nicht über das Token verfügt.

Bei Steuerrahmen wird durch das Feld Rahmensteuerungdie Art des Rahmens festgelegt. Darunter fallen die Token-Weitergabe und verschiedene Wartungsrahmen, die z.B. die Eingliederung neuer Stationen bewerkstelligen oder einer Station ermöglichen, den Ring zu verlassen.

Die Felder Zieladresse und Quelladresse wie bei 802.3 können auch hier für das ganze Netz entweder nur 2-Byte- oder nur 6-Byte-Adressen sein, eine Mischung innerhalb des Netzes ist nicht zulässig. Die
Möglichkeiten der Einzel- und Gruppenadressierung sowie der Zuordnung von lokalen und globalen Adressen ist mit 802.3 identisch.





- PA : Preamble
- SD : Start Delimiter
- FC : Frame Control
- DA : Destination Address
- SA : Source Address
- FCS : Frame Check Sequence
- ED : End Delimiter
- FS : Frame Status

- ANSI standard
- 100 Mbit/s data rate (125 Mbit/s bit rate on medium)
- 4B/5B coding
- ring with ring / tree wiring
- up to 500 nodes, up to 100 km total ring length
- second ring for redundancy
- timed-token protocol
- synchronous and asynchronous traffic classes
- eight priority classs for asynchronous traffic

timed-token protocol

- access-time control by TTRT (Target Token Rotation Time)

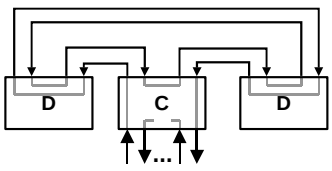
FDDI spezifiziert eine Netztopologie, die in einen Ringbereich (Trunk) und einen Baumbereich (Tree) zerfällt.
Der Ringbereich besteht aus einem gegenläufigen Glasfaser-Doppelring (Primär- und Sekundärring), an dem die FDDI-Stationen angeschlossen sind. Zwischen den Stationen existiert jeweils eine Punkt-zu-Punkt-Verbindung. Falls das Netz fehlerfrei arbeitet, wird nur der Primärring für die Datenübertragung genutzt, der Sekundärring dient als Back-up-Medium im Störungsfall (z.B. Glasfase-Unterbrechung).

Bild: Fiber Distributed Data Interface (FDDI)

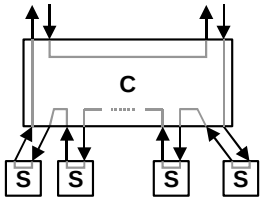
FDDI-Stationstypen

In FDDI werden vier Stationstypen definiert:

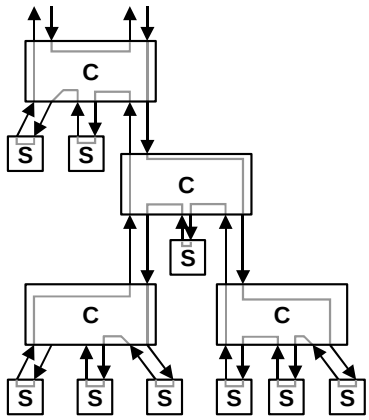
- DAS: Doppelanschluß-Station (Dual Attached Station)
- SAS: Einzelanschluß-Station (Single Attached Station)
- DAC: Doppelanschluß-Konzentrator (Dual Attached Concentrator)
- SAC: Einzelanschluß-Konzentrator (Single Attached Concentrator)



Doppelring



Stern



Baum

text text text text text text text text text text text text text text text text text text

Bild: FDDI: Netztopologien

Wie beim Token Ring darf eine Station nur dann senden, wenn sie sich im Besitz des Token befindet. Es gibt aber einige Besonderheiten, wie:

- Die Sendezeit in jeder Station ist variabel und ist durch den Parameter THT (Token Holding Time) bestimmt.
- Der maximale THT-Wert ist begrenzt.
- Innerhalb der THT-Zeit kann eine Station mehrere MAC-Frames senden.
- Die maximale Framelänge ist auf 4500 Bytes festgelegt.

Hat eine Station Daten zum Senden, so wartet sie auf das Token. Kommt das Token an die sendewillige Station an, erhält sie mit dem Eintreffen des Token die Sendeberechtigung. Sie nimmt das Token vom Ring und sendet ihre Frames. Unmittelbar nach dem Aussenden des letzten Frames reicht die sendeberechtigte Station das Token an ihre Nachbar-Station weiter. Das direkte Absenden des Token nach den Frames ist ein wesentliches Merkmal des FDDI-Zugriffsverfahrens und wird als Early Token Release bezeichnet. Damit besteht die Möglichkeit, mehrere Frames von verschiedenen Stationen auf dem Ring gleichzeitig zu übertragen, wodurch der Ring bei starkem Frame-Verkehr voll belegt (ausgelastet) sein kann.
Die Zielstation (MAC-Zieladresse) erkennt ihre eigene MAC-Adresse, kopiert ihre Frames und leitet sie weiter. Die Quellstation (MAC-Quelladresse) erkennt schließlich ihre eigene MAC-Adresse im Frame wieder und ist damit verpflichtet den MAC-Frame vom Ring zu nehmen. Stationen, die nicht sendeberechtigt sind, prüfen die vorbeilaufenden Frames auf Fehler, die im FS-Feld eingetragen werden können und leiten sie auf den Ring weiter

text text text text text text text text text text
text text text text text text

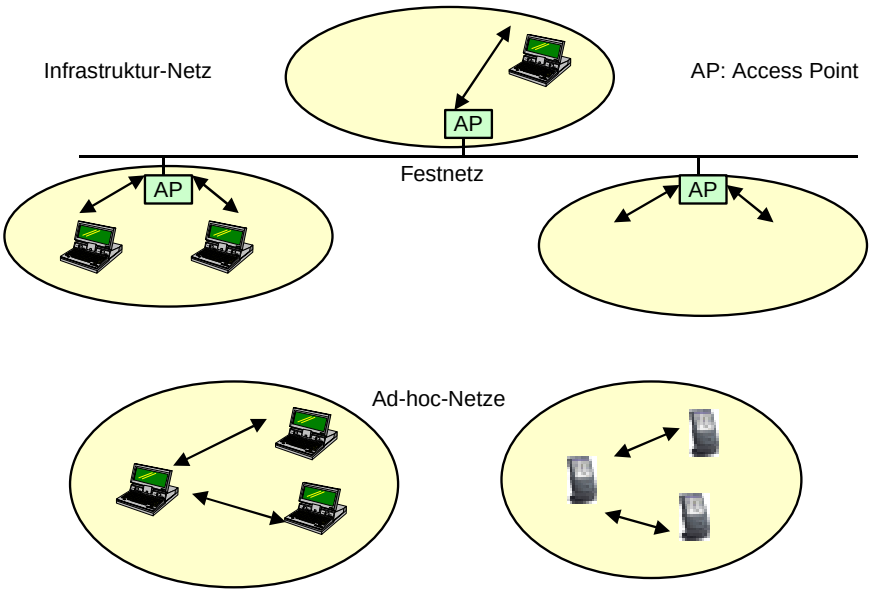


Bild: IEEE 802.11 Wireless LAN Architektur

- Station (STA)
  - Rechner mit Zugriffsfunktion auf drahtloses Medium und Funkkontakt zum Access Point
- Basic Service Set (BSS)
  - Gruppe von Stationen, welche dieselbe Funkfrequenz nutzen
- Access Point (AP)
  - Station, die in Funk-LAN und das verbindende Festnetz (Distribution System) integriert ist
- Portal
  - Übergang in anderes Festnetz

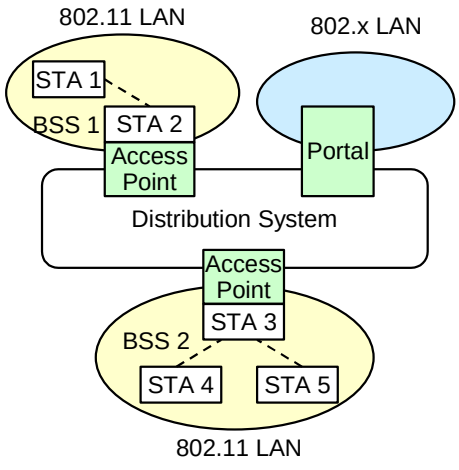
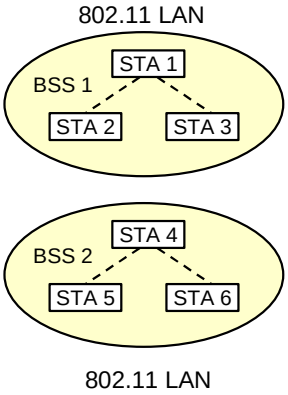


Bild: IEEE 802.11-Infrastrukturnetze

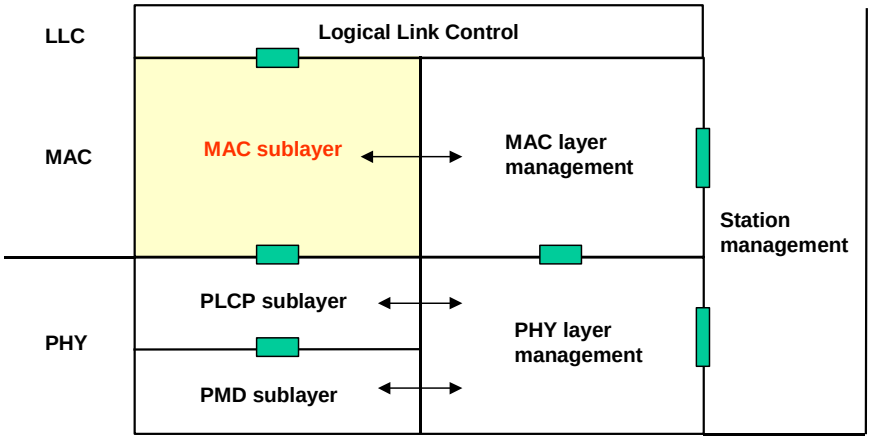
text text text text text text text text text text
text text text text text text

- direkte Kommunikation mit begrenzter Reichweite
- Station (STA)
  – Rechner mit Zugriffsfunktion auf das drahtlose Medium
- Basic Service Set (BSS)
  – Gruppe von Stationen, welche die selbe Funkfrequenz nutzen



text text text text text text text text text text text text text text text text text text text text text text

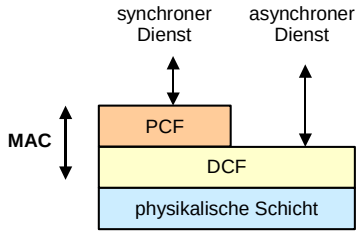
Bild: IEEE 802.11 Ad-hoc-Netze



text text text text text text text text text text text text text text text text text text

PLCP: Physical layer – common part
PMD : Physical layer – medium dependent

Bild: IEEE 802.11 Protokollstruktur



text text text text text text text text text text text text text text text text

- Distributed Coordination Function (DCF)
  – asynchroner Datenverkehr mit einer auf die Stationen verteilten Zugriffsfunktion
  – CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
  – MAC-Schicht-Quittierung für alle nicht-Broadcast-Rahmen mit eventueller Übertragungswiederholung
- Point Coordination Function (PCF)
  – synchroner Datenverkehr unter der Kontrolle des Access Point
  – Stationen senden nur nach Polling durch PCF
  – Aufbau einer Polling-Liste
  – optionaler Modus

Bild: 802.11-Zugriffsverfahren

- CSMA/CA (CA = Collision Avoidance)
  - Medium wird abgehört.
  - Wenn das Medium frei wird, wird nicht sofort, sondern nach einer Verzögerungszeit gesendet (Random Backoff).
- Probleme in drahtlosen LANs
  1. Hidden Node Problem
  2. Empfänger kann sich ausserhalb des Funkbereichs befinden
- Lösungen
  1. Ready To Send (RTS) / Clear To Send (CTS)
  2. Quittierung

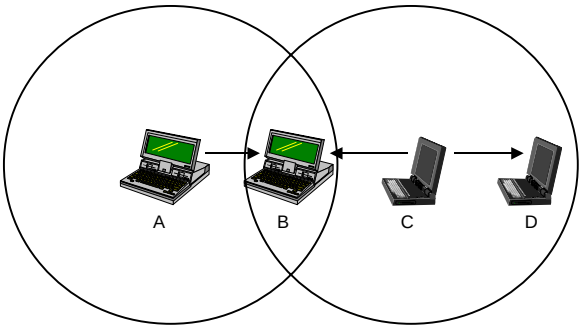
Bild: IEEE 802.11 Wireless LANs

text text text text text text text text text text text text text text text text text text text text text text text text text text

- Backoff-Zeit = Int [CW * R] * Slotzeit
  - CW (contention window, z.B. CW_{min}= 31) wird bei jedem erfolglosem Versuch verdoppelt bis Cw_{max} (z.B. = 255) erreicht ist
  - R: Zufallszahl zwischen 0 und 1
  - Slotzeit
    = Verzögerung zum Anschalten des Senders
    + Signallaufzeit
    + Verzögerung um belegtes Medium zu erkennen
- Dekrementieren des Backoff-Timers bei freiem Medium

Bild: Berechnung der Backoff-Zeit

text text text text text text text text text text text text text text text text text text text text text text text text text text



- A sendet an B und C sendet an D
- Problem: Empfang bei B wird durch C gestört (C erkennt nicht, dass A gesendet hat !)

Bild: Hidden Node Problem

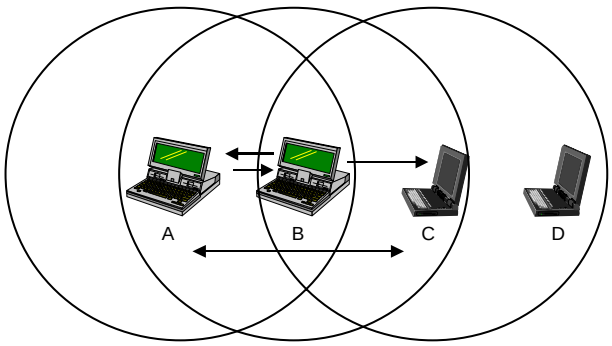


Bild: Ready / Clear To Send

1. Ready To Send (RTS) durch A
2. Clear To Send (CTS) durch B, C erkennt folgende Übertragung
3. A sendet Daten
4. B quittiert

text text text text text text text text text text text text text text text text text text

text text text text text text text text text text text text text text

- sendebereite Station hört Medium ab
- Senden bei freiem Medium der Dauer eines Inter-Frame Space (IFS)
- Verzögerung um IFS + eine zufällige Backoff-Zeit bei belegtem Medium ⇒ Kollisionsvermeidung
- Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen.
- Prioritätsklassen durch unterschiedlich lange IFS
  1. short IFS (SIFS): CTS, ACK, poll response
  2. PCF IFS: poll
  3. DCF IFS (DIFS): RTS, Daten

Bild: IEEE 802.11: CSMA/CA-Verfahren

text text text text text text text text text text text text text text

DIFS : DCF interframe space
PIFS : PCF interframe space
SIFS : Small interframe space

DCF : Distributed coordination function
PCF : Point coordination function

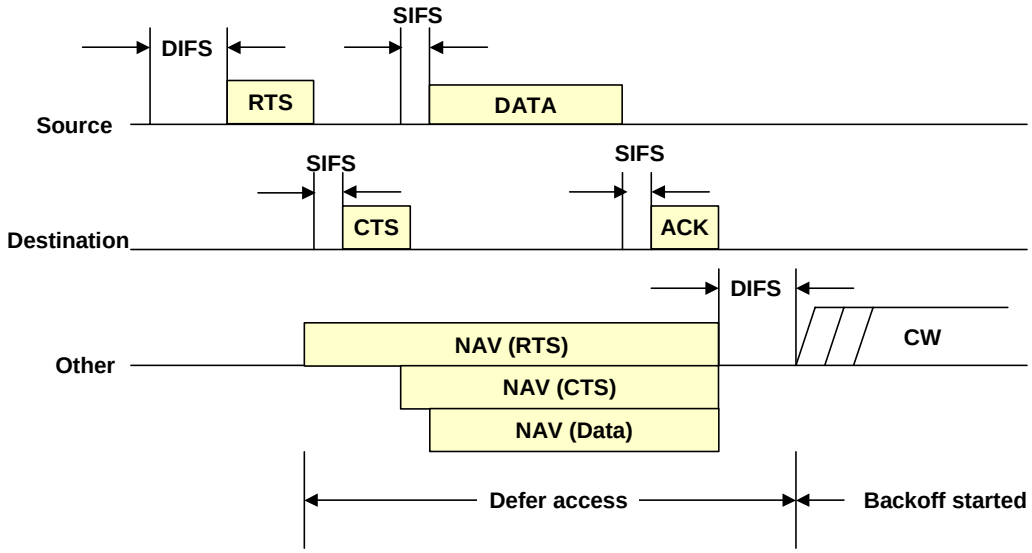
Bild: CSMA/CA access mechanism

text text text text text text text text text text text text text text text text text text

CW : Collision window
NAV : Network allocation vector
SIFS : Short interframe space
DIFS : DCF interframe space

Bild: IEEE 802.11: Medium Access Control

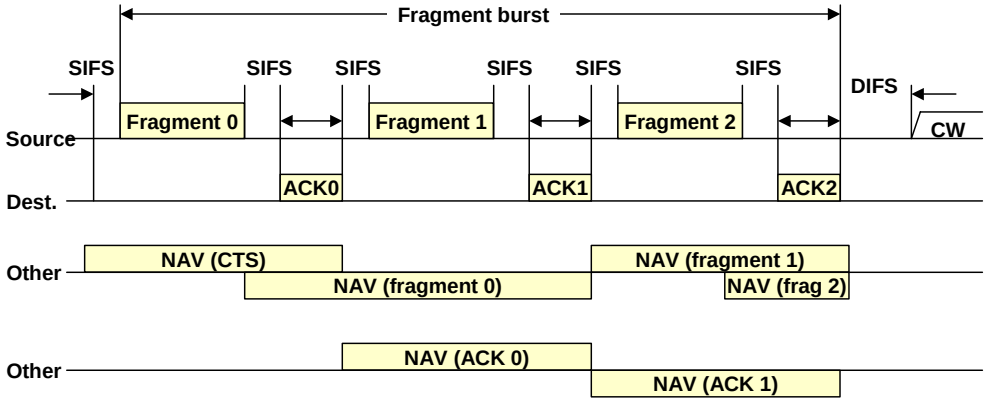
text text text text text text
text text text text



RTS : Request to transmit **CW : Collision window** **SIFS : Short interframe space**
CTS : Confirmation to transmit **NAV : Network allocation vector** **DIFS : DCF interframe space**

Bild: IEEE 802.11: Medium Access Control

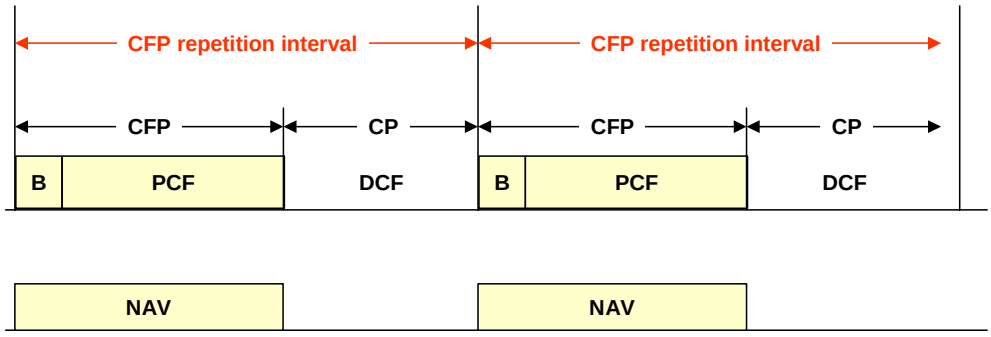
text text text text text text text
text text text text text



RTS : Request to transmit **CW : Collision window** **SIFS : Short interframe space**
CTS : Confirmation to transmit **NAV : Network allocation vector** **DIFS : DCF interframe space**

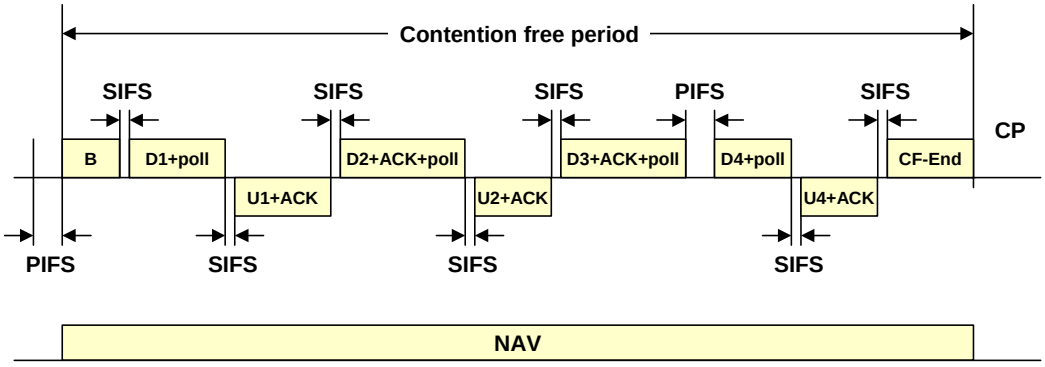
Bild: IEEE 802.11: Medium Access Control

text text text text text text text
text text text text text



B : Beacon
CFP : Collision free period DCF : Distributed coordination function
CP : Collision period PCF : Point coordination function
NAV : Network allocation vector

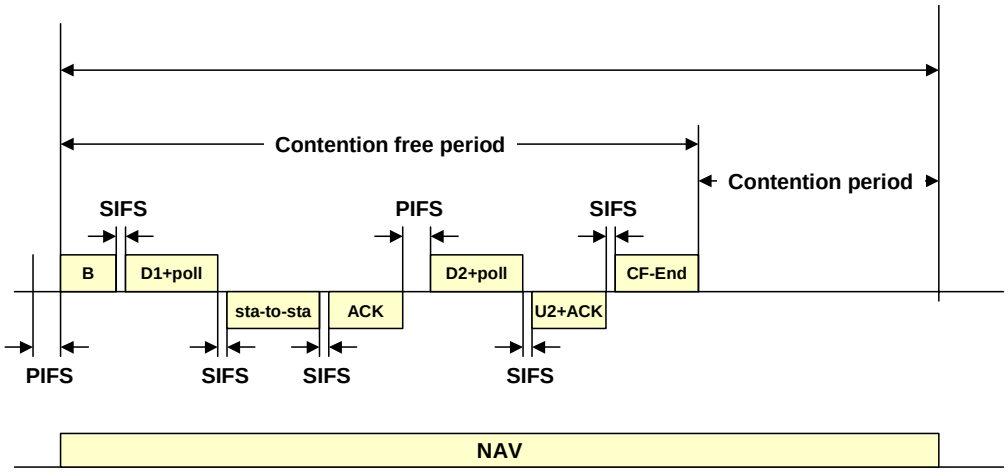
Bild: IEEE 802.11: Medium Access Control



text text text text text text
text text text text

B : Beacon
PIFS : PCP interframe space
SIFS : Small interframe space
NAV : Network allocation vector

Bild: IEEE 802.11: Medium Access Control



text text text text text text
text text text text

B : Beacon
PIFS : PCP interframe space
SIFS : Small interframe space
NAV : Network allocation vector

Bild: IEEE 802.11: Medium Access Control

IEEE 802.11 Wireless Local Area Networks

Wireless computing is a rapidly emerging technology providing users with network connectivity without being tethered off of a wired network. Wireless local area networks (WLANs), like their wired counterparts, are being developed to provide high bandwidth to users in a limited geographical area. WLANs are being studied as an alternative to the high installation and maintenance costs incurred by traditional additions, deletions, and changes experienced in wired LAN infrastructures. Physical and environmental necessity is another driving factor in favor of WLANs. Typically, new building architectures are planned with network connectivity factored into the building requirements. However, users inhabiting existing buildings may find it infeasible to retrofit existing structures for wired network access. Examples of structures that are very difficult to wire include concrete buildings, trading floors, manufacturing facilities, warehouses, and historical buildings. Lastly, the operational environment may not accommodate a wired network, or the network may be temporary and operational for a very short time, making the installation of a wired network impractical. Examples where this is true include ad hoc networking needs such as conference registration centers, campus classrooms, emergency relief centers, and tactical military environments.

Ideally, users of wireless networks will want the same services and capabilities that they have commonly come to expect with wired networks. However, to meet these objectives, the wireless community faces certain challenges and constraints that are not imposed on their wired counterparts.

- Frequency Allocation: Operation of a wireless network requires that all users operate on a common frequency band. Frequency bands for particular uses must typically be approved and licensed in each country, which is a time-consuming process due to the high demand for available radio spectrum.
- Interference and Reliability: Interference in wireless communications can be caused by simultaneous transmissions (i.e., collisions) by two or more sources sharing the same frequency band. Collisions are typically the result of multiple stations waiting for the channel to become idle and then beginning transmission at the same time. Collisions are also caused by the "hidden terminal" problem, where a station, believing the channel is idle, begins transmission without successfully detecting the presence of a transmission already in progress. Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations at the receiver. The reliability of the communications channel is typically measured by the average bit error rate (BER). For packetized voice, packet loss rates on the order of 10^{-2} are generally acceptable; for uncoded data, a BER of 10^{-5} is regarded as acceptable. Automatic repeat request (ARQ) and forward error correction (FEC) are used to increase reliability.
- Security: In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. A wireless network is more difficult to secure, since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance.
- Power Consumption: Typically, devices connected to a wired network are powered by the local 110 V commercial power provided in a building. Wireless devices, however, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy-efficient, resulting in "sleep" modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs.
- Human Safety: Research is ongoing to determine whether radio frequency (RF) transmissions from radio and cellular phones are linked to human illness. Networks should be designed to minimize the power transmitted by network devices. For infrared (IR) WLAN systems, optical transmitters must be designed to prevent vision impairment.
- Mobility: Unlike wired terminals, which are static when operating on the network, one of the primary advantages of wireless terminals is freedom of mobility. Therefore, system designs must accommodate handoff between transmission boundaries and route traffic to mobile users.

- Throughput: The capacity of WLANs should ideally approach that of their wired counterparts. However, due to physical limitations and limited available bandwidth, WLANs are currently targeted to operate at data rates between 1-20 Mbit/s. To support multiple transmissions simultaneously, spread spectrum techniques are frequently employed.

Of particular interest in the specification is the support for two fundamentally different MAC schemes to transport asynchronous and timebounded services. The first scheme, distributed coordination function (DCF), is similar to traditional legacy packet networks supporting best effort delivery of the data. The DCF is designed for asynchronous data transport, where all users with data to transmit have an equally fair chance of accessing the network. The point coordination function (PCF) is the second MAC scheme. The PCF is based on polling that is controlled by an access point (AP). The PCF is primarily designed for the transmission of delay-sensitive traffic.

DESCRIPTION OF THE IEEE 802.1 1 STANDARD

ARCHITECTURE

The *basic service set* (BSS) is the fundamental building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that are under the direct control of a single coordination function (i.e., a DCF or PCF) which is defined below. The geographical area covered by the BSS is known as the *basic service area* (BSA), which is analogous to a cell in a cellular communications network. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS. However, transmission medium degradations due to multipath fading, or interference from nearby BSSs reusing the same physical-layer characteristics (e.g., frequency and spreading code, or hopping pattern), can cause some stations to appear "hidden" from other stations.

An ad hoc network is a deliberate grouping of stations into a single BSS for the purposes of internetworked communications without the aid of an infrastructure network. Figure 1 is an illustration of an *independent BSS* (IBSS), which is the formal name of an ad hoc network in the IEEE 802.11 standard. Any station can establish a direct communications session with any other station in the BSS, without the requirement of channeling all traffic through a centralized access point (AP).

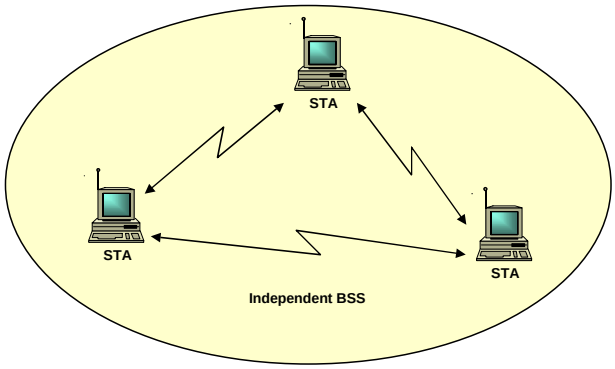


Figure 1: Ad hoc network

In contrast to the ad hoc network, infrastructure networks are established to provide wireless users with specific services and range extension. Infrastructure networks in the context of IEEE 802.11 are established using APs. The AP is analogous to the base station in a cellular communications network. The AP supports range extension by providing the integration points necessary for network connectivity between multiple BSSs, thus forming an *extended service set* (ESS). The ESS has the appearance of one large BSS to the *logical link control* (LLC) sublayer of each station (STA). The ESS consists of multiple BSSs that are integrated together using a common *distribution system* (DS). The DS can be thought of as a backbone network that is responsible for MAC-level transport of MAC service data units (MSDUs). The DS, as specified by IEEE 802.11, is implementation - independent. Therefore, the DS could be a wired IEEE 802.3 Ethernet LAN, IEEE 802.4 token bus LAN, IEEE 802.5 token ring LAN, fiber distributed data interface (FDDI) metropolitan area network (MAN), or another IEEE 802.11 wireless medium. Note that while the DS could physically be the same transmission medium as the BSS, they are logically different, because the DS is solely used as a transport backbone to transfer packets between different BSSs in the ESS.

An ESS can also provide gateway access for wireless users into a wired network such as the Internet. This is accomplished via a device known as *a portal.* The portal is a logical entity that specifies the integration point on the DS where the IEEE 802.11 network integrates with a non-IEEE 802.11 network. If the network is an IEEE 802.X, the portal incorporates functions which are analogous to a bridge; that is, it provides range extension and the translation between different frame formats. Figure 2 illustrates a simple ESS developed with two BSSs, a DS, and a portal access to a wired LAN.

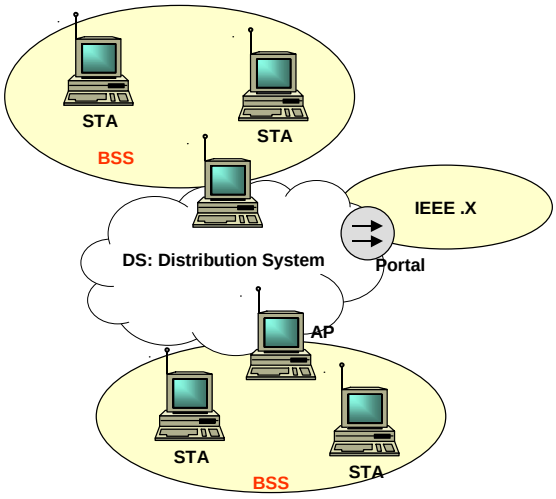


Figure 2: Infrastructure network

MEDIUM ACCESS CONTROL SUBLAYER

The MAC sublayer is responsible for the channel allocation procedures, protocol data unit (PDU) addressing, frame formatfing, error checking, and fragmentation and reassembly. The transmission medium can operate in the contention mode exclusively, requiring all stations to contend for access to the channel for each packet transmitted. The medium can also alterrate between the contention mode, known as the *contention period* (CP), and a *contention-free period* (CFP). During the CFP, medium usage is controlled (or mediated) by the AP, thereby eliminating the need for stations to contend for channel access. IEEE 802.11 supports three different types of frames: management, control, and data. The management frames are used for station association and disassociation with the AP, timing and synchronization, and authentication and deauthentication. Control frames are used for handshaking during the CP, for positive acknowledgments during the CP, and to end the CFP. Data frames are used for the transmission of data during the CP and CFP, and can be combined with polling and acknowledgments during the CFP. The standard IEEE 802.11 frame format is illustrated in Fig. 3. Note that the frame body (MSDU) is a variable-length field consisting of the data payload and 7 octets for encryption/decryption if the optional Wired Equivalent Privacy (WEP) protocol is implemented. The IEEE standard 48-bit MAC addressing is used to identify a station. The 2 duration octets indicate the time (in microseconds) the channel will be allocated for successful transmission of a MAC protocol data unit (MPDU). The type bits identify the frame as either control, management, or data. The subtype bits further identify the type of frame (e.g., Clear to Send control frame). A 32-bit cyclic redundancy check (CRC) is used for error detection.

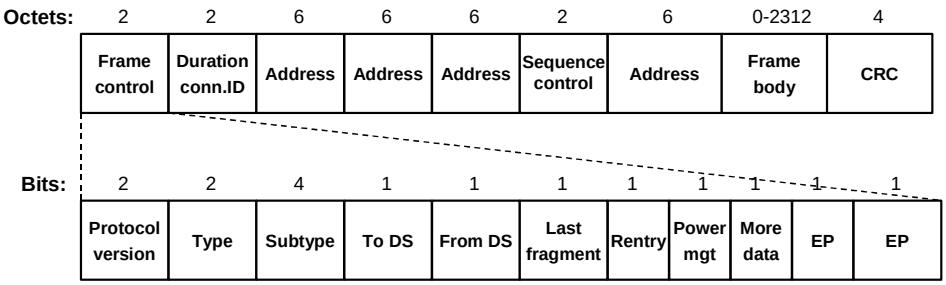


Figure 3: IEEE 802.11 frame format

DISTRIBUTED COORDINATION FUNCTION

The DCF is the fundamental access method used to support asynchronous data transfer on a best effort basis. As identified in the specification, all stations must support the DCF. The DCF operates solely in the ad hoc network,

and either operates solely or coexists with the PCF in an infrastructure network. The MAC architecture is depicted in Fig. 4, where it is shown that the DCF sits directly on top of the physical layer and supports contention services. Contention services imply that each station with an MSDU queued for transmission must contend for access to the channel and, once the MSDU is transmitted, must recontend for access to the channel for all subsequent frames. Contention services promote fair access to the channel for all stations.

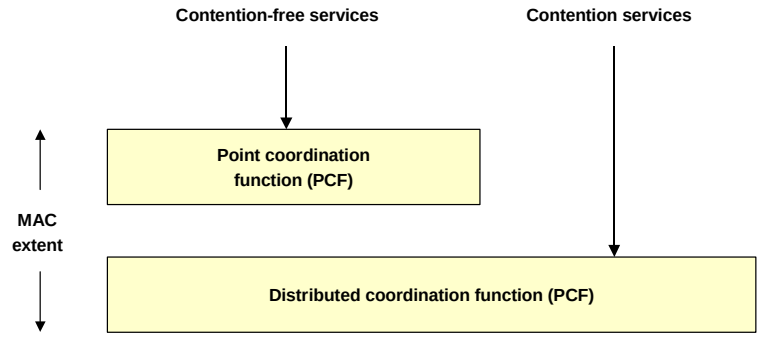


Figure 4: Medium Access Control

The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). CSMA/CD (collision detection) is not used because a station is unable to listen to the channel for collisions while transmitting. In IEEE 802.11, carrier sensing is performed at both the air interface, referred to as *physical carrier sensing*, and at the MAC sublayer, referred to as *virtual carrier sensing.* Physical carrier sensing detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets, and also detects activity in the channel via relative signal strength from other sources.

A source station performs virtual carrier sensing by sending MPDU duration information in the header of request to send (RTS), clear to send (CTS), and data frames. An MPDU is a complete data unit that is passed from the MAC sublayer to the physical layer. The MPDU contains header information, payload, and a 32-bit CRC. The duration field indicates the amount of time (in microseconds) after the end of the present frame the channel will be utilized to complete the successful transmission of the data or management frame. Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV), which indicates the amount of time that must elapse until the current transmission session is complete and the channel can be sampled again for idle status. The channel is marked busy if either the physical or virtual carrier sensing mechanisms indicate the channel is busy.

Priority access to the wireless medium is controlled through the use of interframe space (IFS) time intervals between the transmission of frames. The IFS intervals are mandatory periods of idle time on the transmission medium. Three IFS intervals are specified in the standard: short IFS (SIFS), point coordination function IFS (PIFS), and DCF-IFS (DIFS). The SIFS interval is the smallest IFS, followed by PIFS and DIFS, respectively. Stations only required to wait a SIFS have priority access over those stations required to wait a PIFS or DIFS before transmitting; therefore, SIFS has the highest-priority access to the communications medium. For the basic access method, when a station senses the channel is idle, the station waits for a DIFS period and samples the channel again. If the channel is still idle, the station transmits an MPDU. The receiving station calculates the checksum and determines whether the packet was received correctly. Upon receipt of a correct packet, the receiving station waits a SIFS interval and transmits a positive acknowledgment frame (ACK) back to the source station, indicating that the transmission was successful. Figure 5 is a timing diagram illustrating the successful transmission of a data frame. When the data frame is transmitted, the duration field of the frame is used to let all stations in the BSS know how long the medium will be busy. All stations hearing the data frame adjust their NAV based on the duration field value, which includes the SIFS interval and the ACK following the data frame.

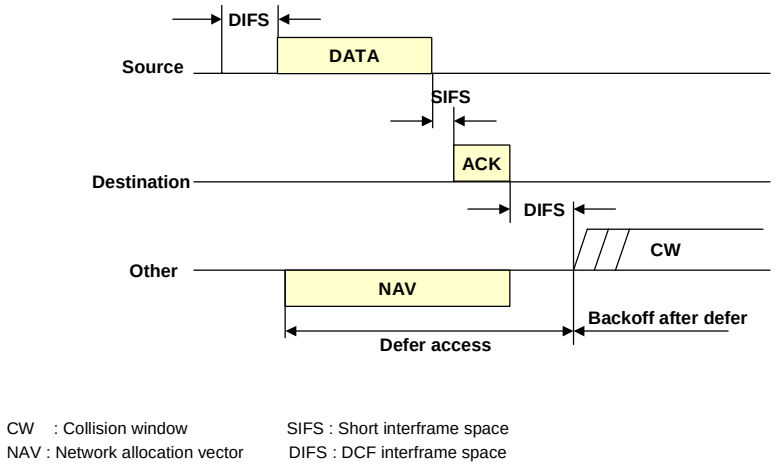


Figure 5: Transmission of an MPDU without RTS/CTS

Since a source station in a BSS cannot hear its own transmissions, when a collision occurs, the source continues transmitting the complete MPDU. If the MPDU is large (e.g., 2300 octets), a lot of channel bandwidth is wasted due to a corrupt MPDU. RTS and CTS control frames can be used by a station to reserve channel bandwidth prior to the transmission of an MPDU and to minimize the amount of bandwidth wasted when collisions occur. RTS and CTS control frames are relatively small (RTS is 20 octets and CTS is 14 octets) when compared to the maximum data frame size (2346 octets). The RTS control frame is first transmitted by the source station (after successfully contending for the channel) with a data or management frame queued for transmission to a specified destination station. All stations in the BSS, hearing the RTS packet, read the duration field (Fig. 3) and set their NAVs accordingly. The destination station responds to the RTS packet with a CTS packet after an SIFS idle period has elapsed. Stations hearing the CTS packet look at the duration field and again update their NAV. Upon successful reception of the CTS, the source station is virtually assured that the medium is stable and reserved for successful transmission of the MPDU. Note that stations are capable of updating their NAVs based on the RTS from the source station and CTS from the destination station, which helps to combat the "hidden terminal" problem. Figure 6 illustrates the transmission of an MPDU using the RTS/CTS mechanism. Stations can choose to never use RTS/CTS, use RTS/CTS whenever the MSDU exceeds the value of RTS_Threshold (manageable parameter), or always use RTS/CTS. If a collision occurs with an RTS or CTS MPDU, far less bandwidth is wasted when compared to a large data MPDU. However, for a lightly loaded medium, additional delay is imposed by the overhead of the RTS/CTS frames.

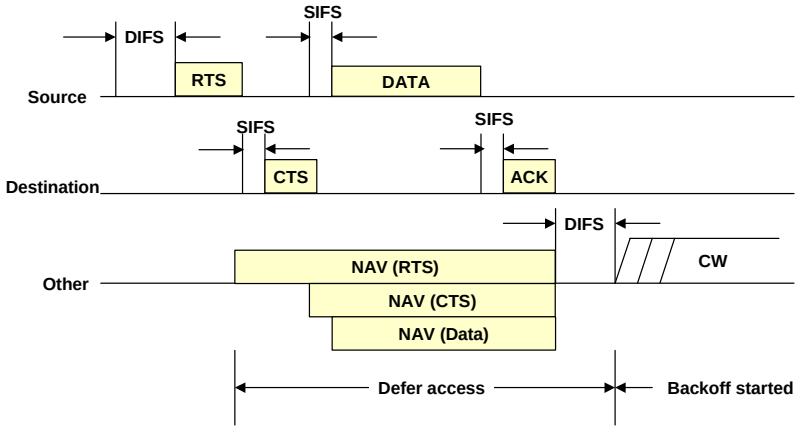


Figure 6: Transmission of an MPDU using RTS/CTS

Large MSDUs handed down from the LLC to the MAC may require fragmentation to increase transmission reliability. To determine whether to perform fragmentation, MPDUs are compared to the manageable parameter Fragmentation Threshold. If the MPDU size exceeds the value of Fragmentation Threshold, the MSDU is broken into multiple fragments. The resulting MPDUs are of size Fragmentation Threshold, with exception of the last

MPDU, which is of variable size not to exceed Fragmentation Threshold. When an MSDU is fragmented, all fragments are transmitted sequentially (Fig. 7). The channel is not released until the complete MSDU has been transmitted successfully, or the source station fails to receive an acknowledgment for a transmitted fragment. The destination station positively acknowledges each successfully received fragment by sending a DCF ACK back to the source station. The source station maintains control of the channel throughout the transmission of the MSDU by waiting only an SIFS period after receiving an ACK and transmitting the next fragment. When an ACK is not received for a previously transmitted frame, the source station halts transmission and recontends for the channel. Upon gaining access to the channel, the source starts transmitting with the last unacknowledged fragment.

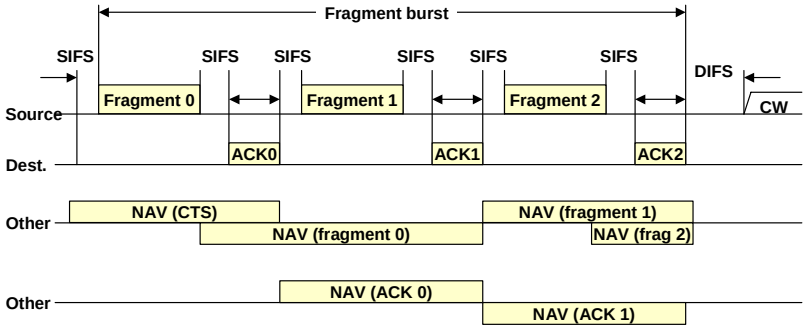


Figure 7: Transmission of a fragmented MPDU

If RTS and CTS are used, only the first fragment is sent using the handshaking mechanism. The duration value of RTS and CTS only accounts for the transmission of the first fragment through the receipt of its ACK. Stations in the BSS thereafter maintain their NAV by extracting the duration information from all subsequent fragments.

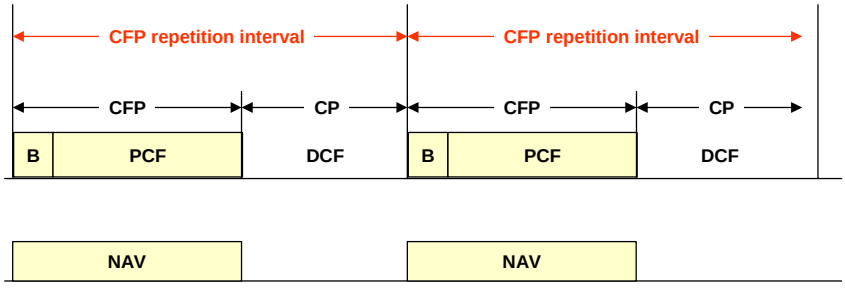
The collision avoidance portion of CSMA CA is performed through a random backoff procedure. If a station with a frame to transmit initially senses the channel to be busy; then the station waits until the channel becomes idle for a DIFS period, and then computes a random backoff time. For IEEE 802.11, time is slotted in time periods that correspond to a Slot Time. Unlike slotted Aloha, where the slot time is equal to the transmission time of one packet, the Slot Time used in IEEE 802.11 is much smaller than an MPDU and is used to define the IFS intervals and determine the backoff time for stations in the CP. The Slot Time is different for each physical layer implementation. The random backoff time is an integer value that corresponds to a number of time slots. Initially, the station computes a backoff time in the range 0-7. After the medium becomes idle after a DIFS period, stations decrement their backoff timer until the medium becomes busy again or the timer reaches zero. If the timer has not reached zero and the medium becomes busy, the station freezes its timer. When the timer is finally decremented to zero, the station transmits its frame. If two or more stations decrement to zero at the same time, a collision will occur, and each station will have to generate a new backoff time in the range 0-15. For each retransmission attempt, the backoff time grows as $\lfloor 2^{2+i} * random() \rfloor *$ Slot_Time where i is the number of consecutive times a station attempts to send an MPDU, *random*() *is* a uniform random variate in (0,1), and $\lfloor x \rfloor$ represents the largest integer less than or equal to x. The idle period after a DIFS period is referred to as the *contention window (CW).* The advantage of this channel access method is that it promotes fairness among stations, but its weakness is that it probably could not support DTBS. Fairness is maintained because each station must recontend for the channel after every transmission of an MSDU. All stations have equal probability of gaining access to the channel after each DIFS interval. Time-bounded services typically support applications such as packetized voice or video that must be maintained with a specified minimum delay. With DCF, there is no mechanism to guarantee minimum delay to stations supporting time-bounded services.

POINT COORDINATION FUNCTION (PCF)

The PCF is an optional capability, which is connection-oriented, and provides contention-free (CF) frame transfer. The PCF relies on the point coordinator (PC) to perform polling, enabling polled stations to transmit without con-

tending for the channel. The function of the PC is performed by the AP within each BSS. Stations within the BSS that are capable of operating in the CF period (CFP) are known as *CF-aware* stations. The method by which polling tables are maintained and the polling sequence is determined, is left to the implementer.

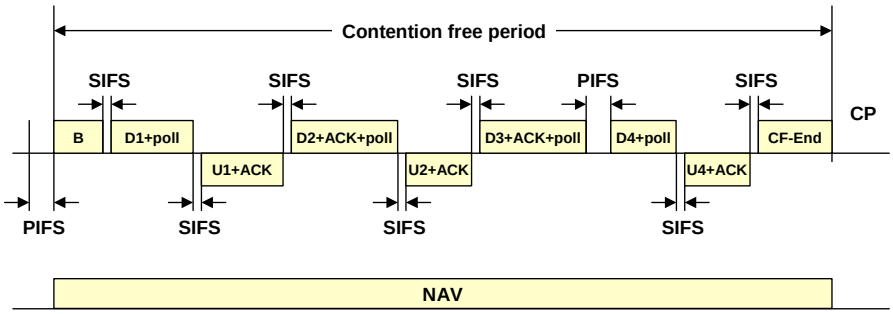
The PCF is required to coexist with the DCF and logically sits on top of the DCF (Fig. 4). The CFP repetition interval (CFP Rate) is used to determine the frequency with which the PCF occurs. Within a repetition interval, a portion of the time is allotted to contention-free traffic, and the remainder is provided for contention-based traffic. The CFP repetition interval is initiated by a beacon frame, where the beacon frame is transmitted by the AP. One of its primary functions is synchronization and timing. The duration of the CFP repetition interval is a manageable parameter that is always an integral number of beacon frames. Once the CFP_Rate is established, the duration of the CFP is determined. The maximum size of the CFP is determined by the manageable parameter CFP Max Duration. The minimum value of CFP Max Duration is the time required to transmit two maximum-size MPDUs, including overhead, the initial beacon frame, and a CF-End frame. The maximum value of CFP_Max_Duration is the CFP repetition interval minus the time required to successfully transmit a maximum size MPDU during the CP (which includes the time for RTS/CTS handshaking and the ACK). Therefore, time must be allotted for at least one MPDU to be transmitted during the CP. It is up to the AP to determine how long to operate the CFP during any given repetition interval. If traffic is very light, the AP may shorten the CFP and provide the remainder of the repetition interval for the DCF. The CFP may also be shortened if DCF traffic from the previous repetition interval carries over into the current interval. The maximum amount of delay that can be incurred is the time it takes to transmit an RTS/CTS handshake, maximum MPDU, and ACK. Figure 8 is a sketch of the CFP repetition interval, illustrating the coexistence of the PCF and DCF.



B : Bacon
CFP : Collision free period
CP : Collision period
DCF : Distributed coordination function
PCF : Point coordination function

Figure 8: Coexistence of the PCF and DCF

At the nominal beginning of each CFP repetition interval, all stations in the BSS update their NAV to the maximum length of the CFP (i.e., CFP Max Duration). During the CFP, the only time stations are permitted to transmit is in response to a poll from the PC or for transmission of an ACK a SIFS interval after receipt of an MPDU. At the nominal start of the CFP, the PC senses the medium. If the medium remains idle for a PIFS interval, the PC transmits a beacon frame to initiate the CFP. The PC starts CF transmission a SIFS interval after the beacon frame is transmitted by sending a CF-Poll (no data), Data, or Data+CF-Poll frame. The PC can immediately terminate the CFP by transmitting a CF-End frame, which is common if the network is lightly loaded and the PC has no traffic buffered. If a CF-aware station receives a CF-Poll (no data) frame from the PC, the STA can respond to the PC after a SIFS idle period, with a CF-ACK (no data) or a Data + CF-ACK frame. If the PC receives a Data + CFAck frame from a station, the PC can send a Data + CFACK + CF-Poll frame to a different station, where the CF-ACK portion of the frame is used to acknowledge receipt of the previous data frame. The ability to combine polling and acknowledgment frames with data frames, transmitted between stations and the PC, was designed to improve efficiency. If the PC transmits a CF-Poll (no data) frame and the destination station does not have a data frame to transmit, the station sends a Null Function (no data) frame back to the PC. Figure 9 illustrates the transmission of frames between the PC and a station, and vice versa. If the PC fails to receive an ACK for a transmitted data frame, the PC waits a PIFS interval and continues transmitting to the next station in the polling list.



PIFS : PCP interframe space
SIFS : Small interframe space

Figure 9: PC-to-station transmission

After receiving the poll from the PC, as described above, the station may choose to transmit a frame to another station in the BSS. When the destination station receives the frame, a DCF ACK is returned to the source station, and the PC waits a PIFS interval following the ACK frame before transmitting any additional frames. Figure 10 illustrates station-to-station frame transmission during the CFP. The PC may also choose to transmit a frame to a non-CFaware station. Upon successful receipt of the frame, the station would wait a SIFS interval and reply to the PC with a standard ACK frame. Fragmentation and reassembly are also accommodated with the Fragmentation Threshold value used to determine whether MSDUs are fragmented prior to transmission. It is the responsibility of the destination station to reassemble the fragments to form the original MSDU.

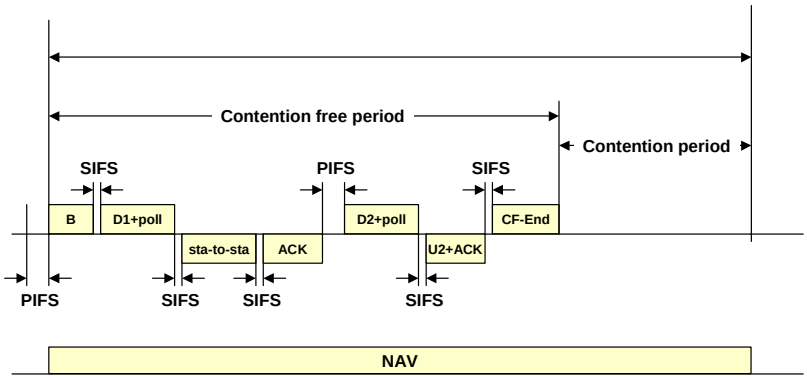


Figure 10: Station-to-station transmission