Reţele de calculatoare

Partea a 4-a

Sebastian Fuicu

- **Transmisii fiabile pe nivelul Legătură de Date**
- **Reţele locale (Standardul IEEE 802)**
- **Reţele LAN Ethernet (802.3)**
- **Reţele WLAN (802.11)**

Transmisii fiabile pe nivelul Legătură de Date

- Pentru a asigura o transmisie de date sigură se folosesc:
  - coduri detectoare si corectoare de erori.
  - mecanisme de tipul “automatic repeat request” (ARQ).

- Un protocol de nivel legătură de date care realizează livrarea sigură a datelor, trebuie să fie capabil să recupereze cadrele pierdute sau afectate de eroare.

Transmisii fiabile pe nivelul Legătură de Date

Automatic repeat request (ARQ)

- Presupune folosirea combinată a două mecanisme:
  - Confirmările (acknowledgements - ACK)
  - Temporizările (timeouts)
- Confirmarea este reprezentată de un mic cadru de control pe care un protocol îl trimite înapoi sursei pentru a semnaliza recepţia corectă a cadrului.
- Există si varianta de piggybacking la transmiterea confirmării, adică ataşarea confirmării la un pachet de date.
- Dacă nu se primeşte confirmarea după un anumit interval de timp (timeout), se retransmite cadrul original.

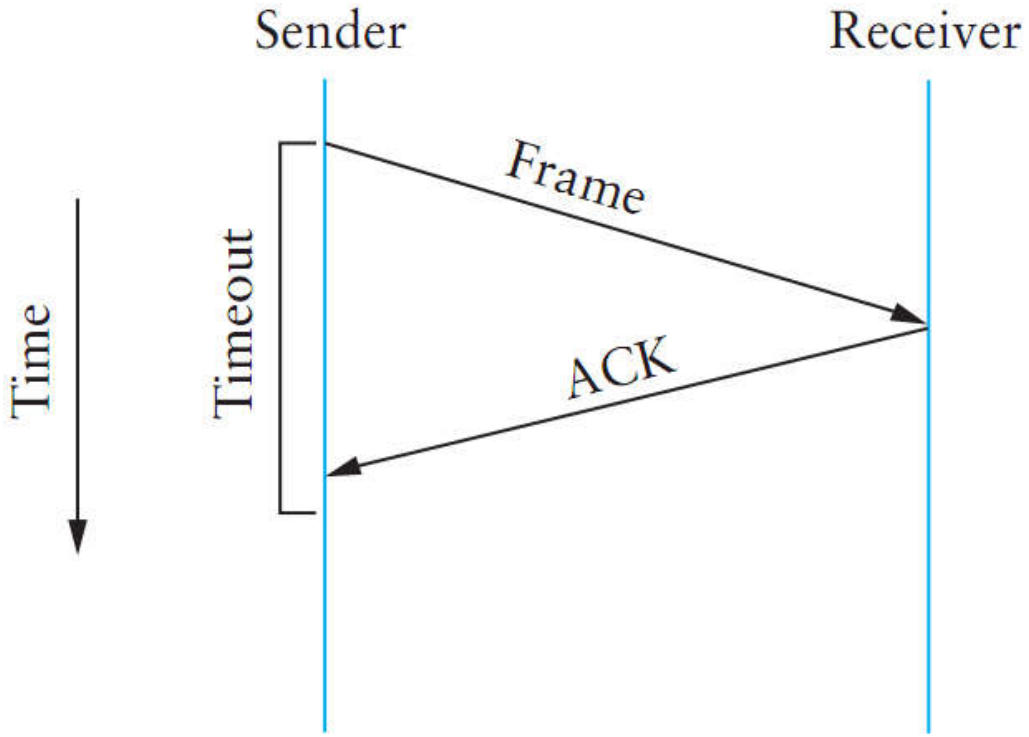
Transmisii fiabile pe nivelul Legătură de Date

Stop-and-Wait

- Cea mai simplă schemă ARQ este algoritmul stop-and-wait.
- După transmiterea unui cadru, emiţătorul se opreşte şi aşteaptă primirea confirmării.
- După primirea confirmării este trimis următorul cadru.
- Este posibil ca atât cadrul cât şi confirmarea să fie afectate de erori sau să se piardă. În această situaţie, după scurgerea unui interval de timp, dat de un timer, cadrul de date este retransmis.
- Mai jos sunt redate situaţiile în care se poate afla protocolul stop and wait.

Transmisii fiabile pe nivelul Legătură de Date

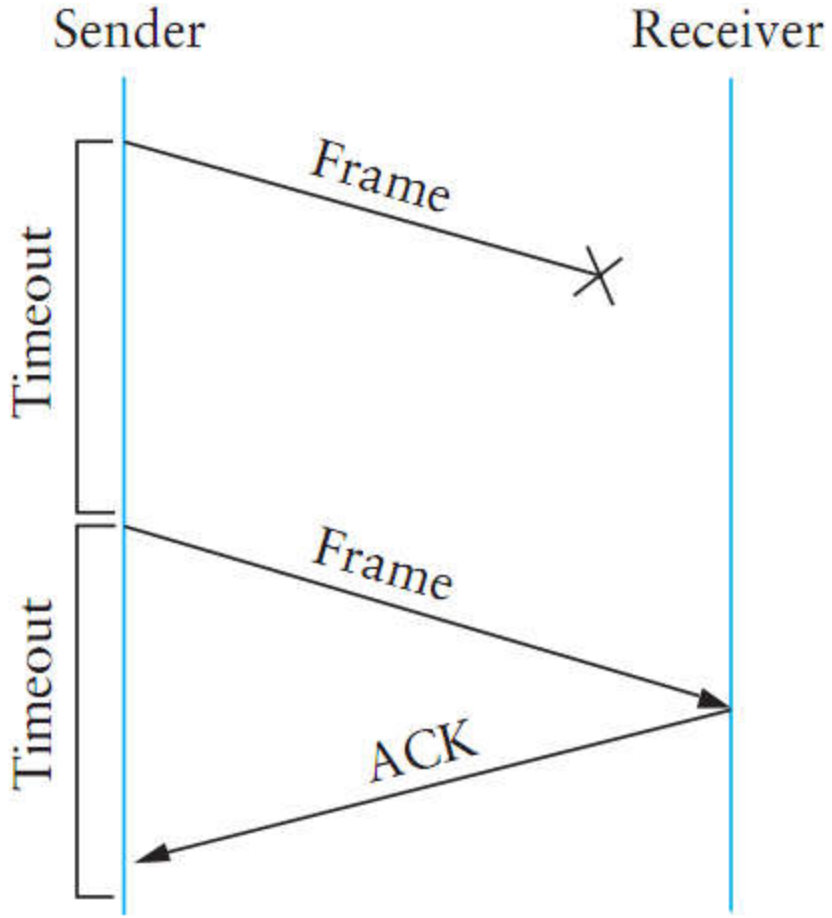
Stop-and-Wait



a) Confirmarea este primită înainte de expirarea timpului

Transmisii fiabile pe nivelul Legătură de Date

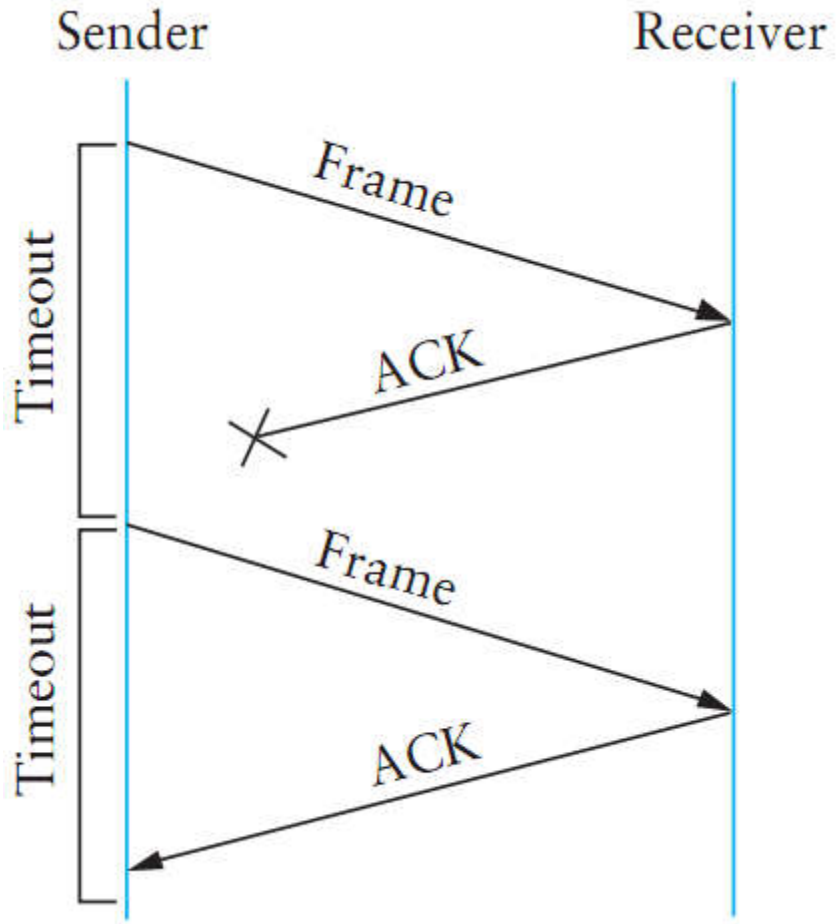
Stop-and-Wait



b) Cadrul de date original se pierde

Transmisii fiabile pe nivelul Legătură de Date

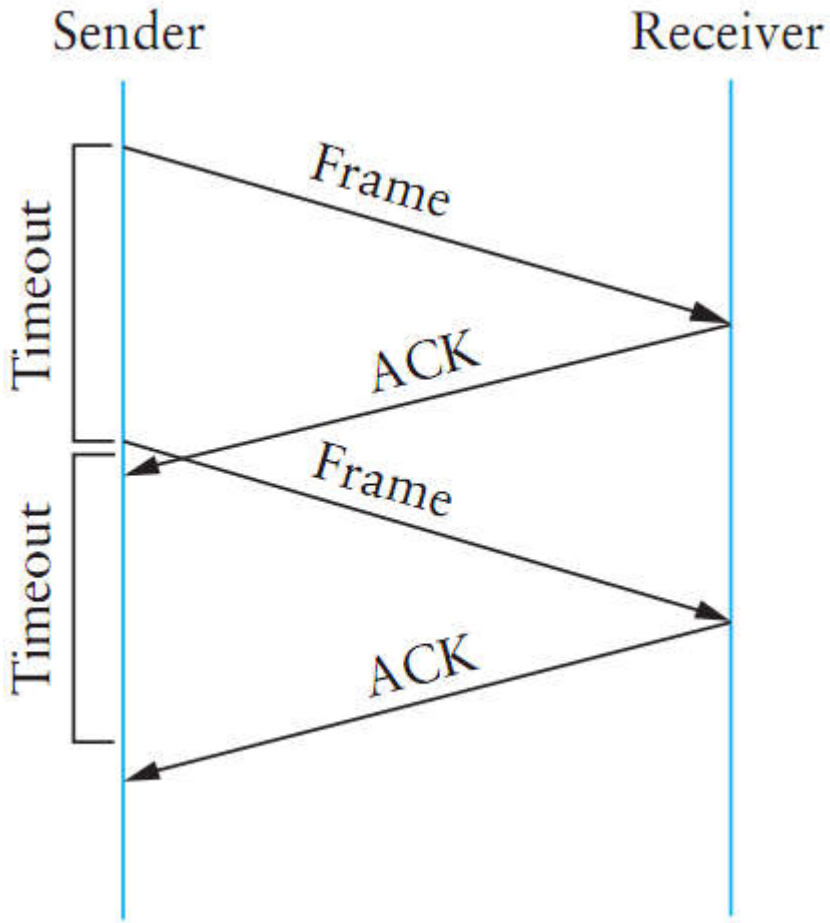
Stop-and-Wait



c) Cadrul de confirmare se pierde

Transmisii fiabile pe nivelul Legătură de Date

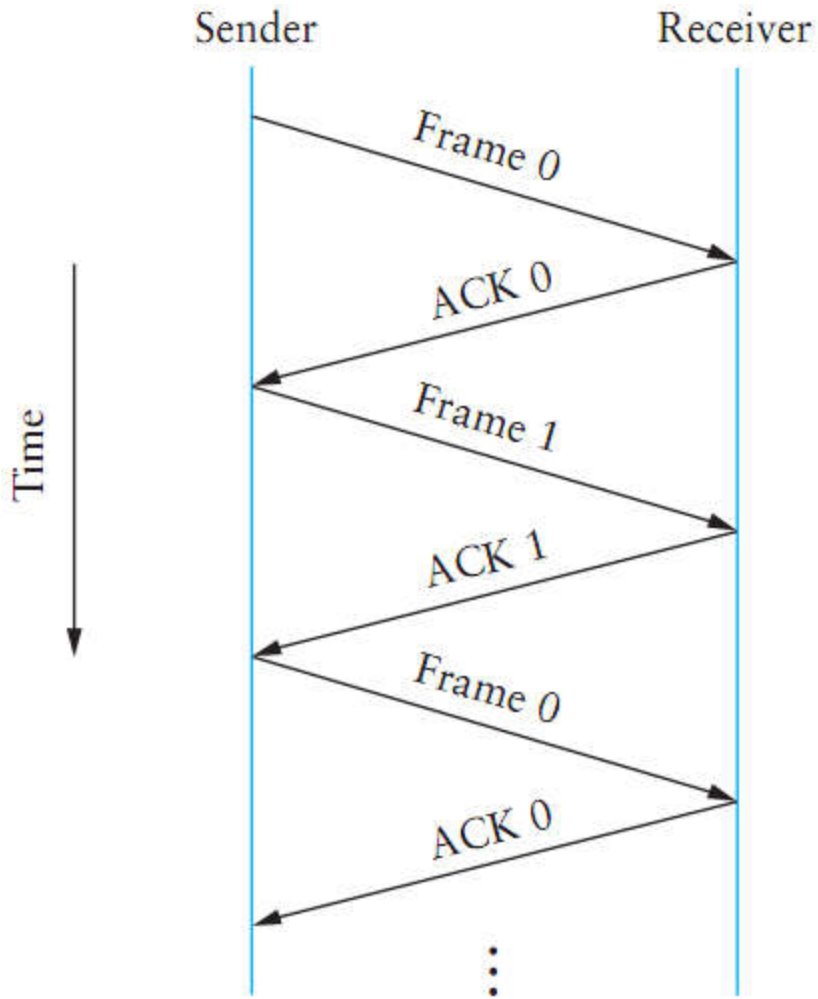
Stop-and-Wait



d) Timpul expiră prea repede

Transmisii fiabile pe nivelul Legătură de Date

Stop-and-Wait



- Pentru procolul stop and wait sunt suficiente doar doua numere de secvenţă, în cazul acesta ele fiind 0 şi 1.

Transmisii fiabile pe nivelul Legătură de Date

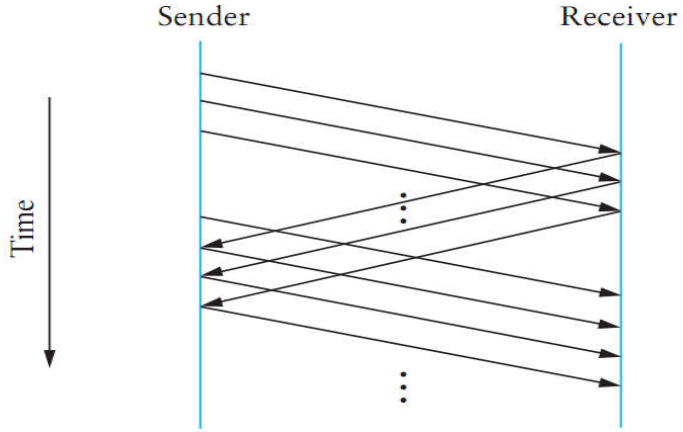
Stop-and-Wait

- Problema majoră a protocolului stop and wait este aceea că la un moment dat un singur frame se poate afla în reţea. După transmiterea unui frame, protocolul trebuie să se oprească şi să aşteapte primirea confirmării.
- În această manieră, capacitatea de transfer a liniei de comunicaţii nu este folosită la maxim.

Transmisii fiabile pe nivelul Legătură de Date

Protocoale cu fereastră glisantă (Sliding Window Protocols)

- Problema protocolului stop and wait enunţată mai devreme este soluţionată de către familia de protocoalele numită cu “fereastră glisantă”. Acestea permit transmiterea în reţea a frame-urilor de date unul după altul, fără a fi necesară oprirea după fiecare frame în parte şi aşteptarea confirmării.
- Diagrama de timp pentru un protocol de tip “fereastră glisantă”.



- Fiecărui cadru i se atribuie un număr de secvenţă distinct (SequnceNumber).

Transmisii fiabile pe nivelul Legătură de Date

Protocoale cu fereastră glisantă (Sliding Window Protocols)

- Emiţătorul foloseşte următoarele 3 variabile:

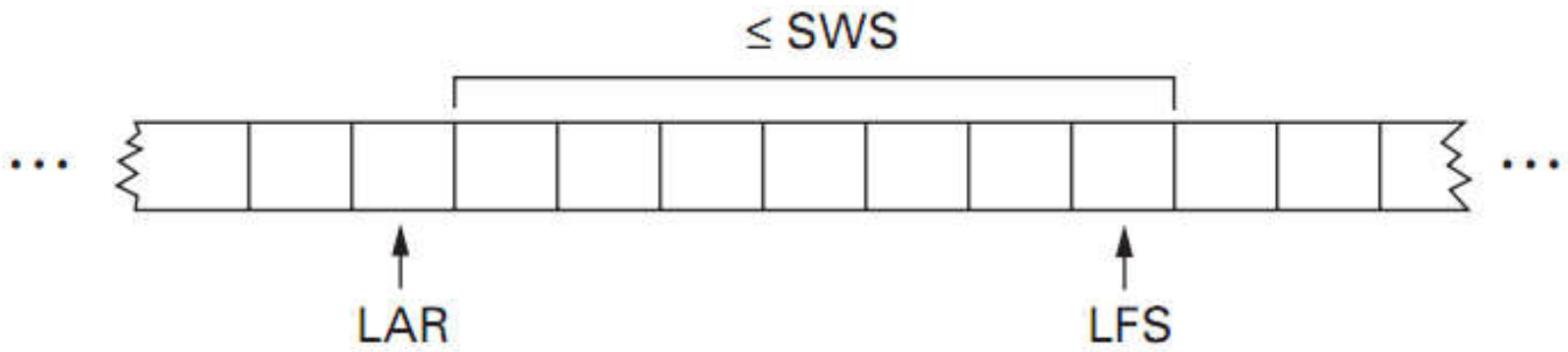
  SWS (Sending Window Size)

  LAR (Last Acknowledgement Received)

  LFS (Last Frame Sent)

- Emiţătorul păstrează următoarea inegalitate:

  LFS – LAR <= SWS



Transmisii fiabile pe nivelul Legătură de Date

Protocoale cu fereastră glisantă (Sliding Window Protocols)

- Receptorul foloseşte următoarele 3 variabile:

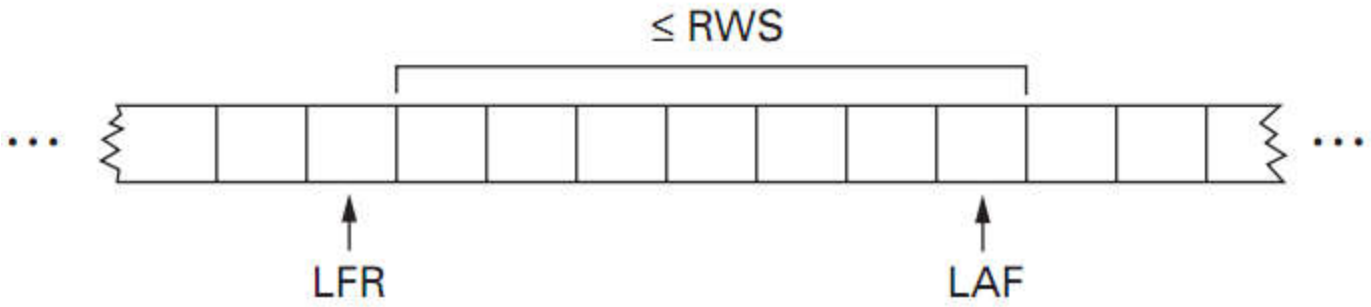
  RWS (Receiving Window Size)

  LAF (Largest Acceptable Frame)

  LFR (Last Frame Received)

- Emiţătorul păstrează următoarea inegalitate:

  LAF– LFR <= RWS



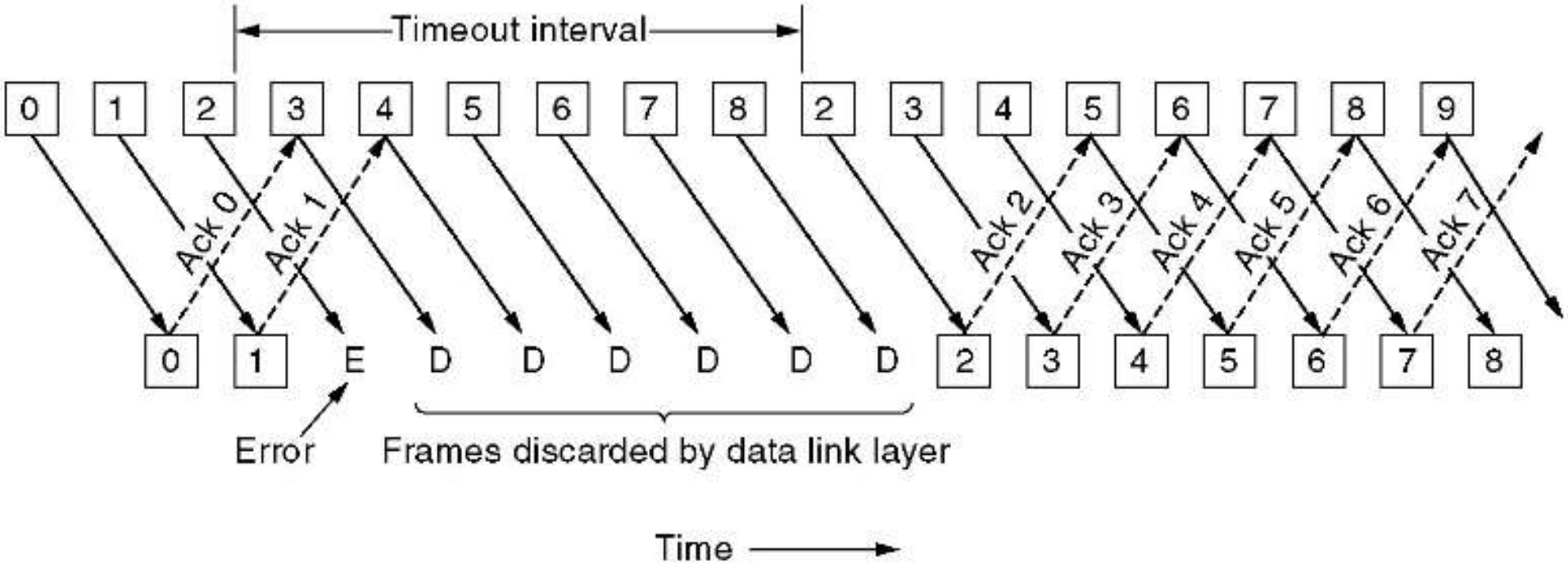
Transmisii fiabile pe nivelul Legătură de Date

Protocoale cu fereastră glisantă
- Protocol “Go Back N” (RWS = 1)

- Protocolul Go Back N, este un caz particular de protocol cu fereastră glisantă, unde dimensiunea ferestrei receptorului are valoarea 1.
- Se observă ca dacă un cadru de date se pierde sau este afectat de eroare, toate cadrele de date care urmează după el sunt ignorate, netrimiţându-se confirmări pentru ele.
- Fiecare cadru de date trimis are asociat un timer. Dacă până la timeout, nu este recepţionată confirmarea, atunci cadrul de date este retrimis.
- În cazul tutoror tipurilor de protocoale cu fereastră glisantă este necesar ca frame-urile de date care au fost trimise să fie salvate local într-un buffer, până la primirea confirmării din partea receptorului. În cazul în care confirmarea nu soseşte, în momentul generării timeout-ului, frame-urile vor fi luate din acest buffer şi retransmise.

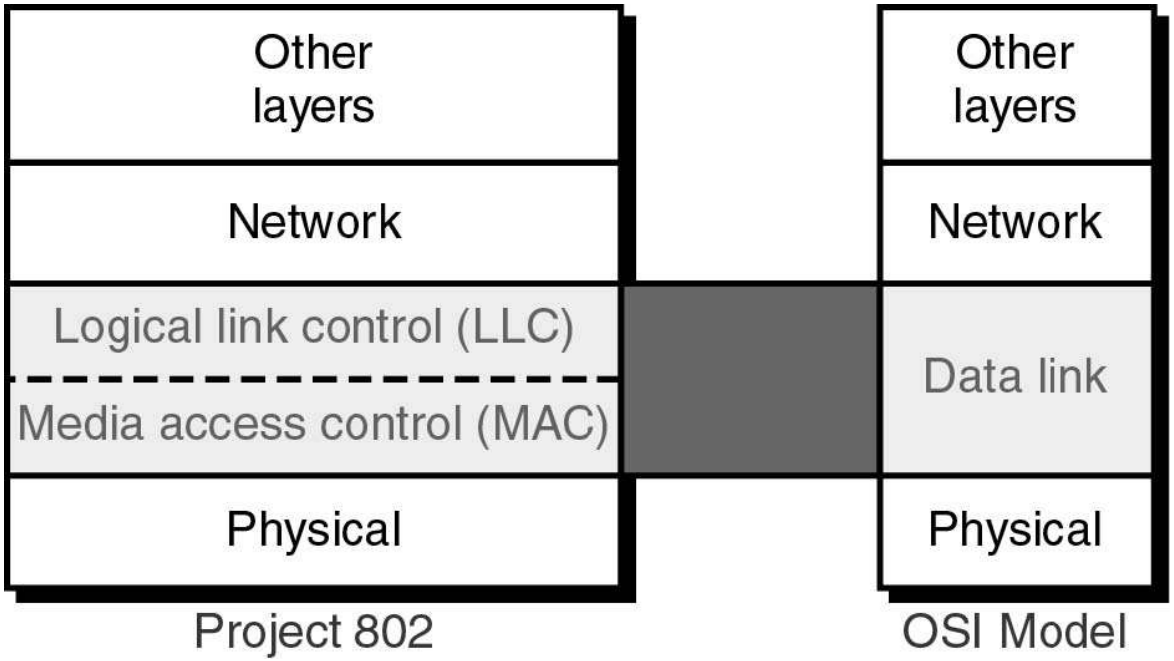
Transmisii fiabile pe nivelul Legătură de Date

Protocoale cu fereastră glisantă
- Protocol de tip "Go Back N" (RWS = 1)



Reţele locale (Standardul IEEE 802)

- Odată cu diversificarea reţelelor locale (Ethernet, Arcnet, Token-ring, etc.) s-a simţit nevoia unei standardizări.
- A fost demarat proiectul IEEE 802.
- A fost propus un model pentru reţelele locale.



Reţele locale (Standardul IEEE 802)

- Acest model specifică existenţa unui nivel Fizic:

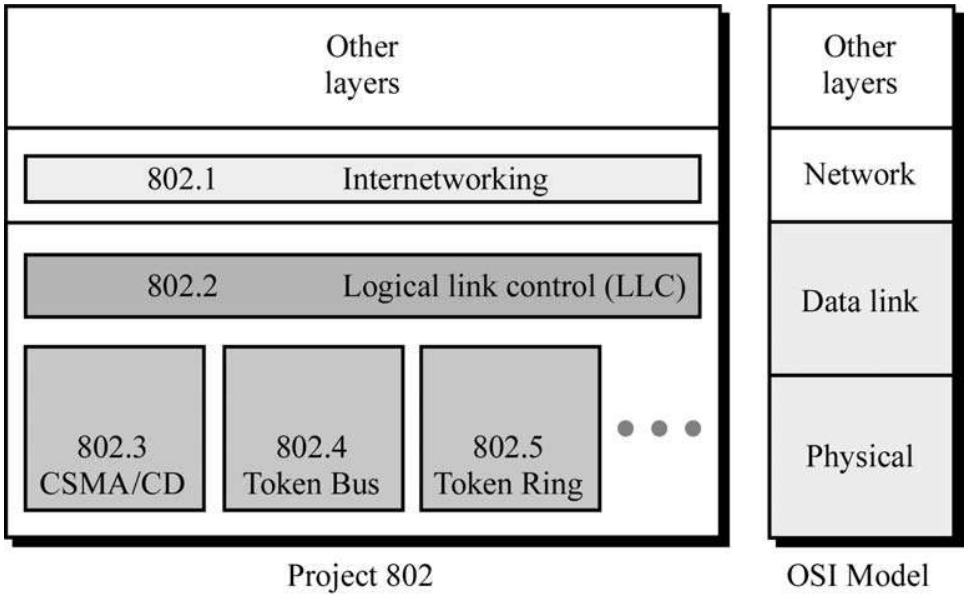
  - acesta acoperă toate aspectele legate de comunicaţia pe un mediu fizic.

- Acelaşi model specifică două subniveluri ce implementează funcţii asociate nivelului Legătură de Date:

  - Subnivelul de control al accesului la mediu (MAC – Medium Access Control): asigură accesul la mediul de transmisie.

  - Subnivelul pentru controlul legăturii logice (LLC – Logical Link Control): asigură interfaţa cu protocoalele de pe nivelele superioare.

Reţele locale (Standardul IEEE 802)



IEEE 802 Standards	
802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

Reţele locale (Standardul IEEE 802)

Subnivelul LLC (IEEE 802.2)

- Specifică tipurile de servicii oferite şi protocolul care le implementează.
- Are ca scop oferirea unei interfeţe unificate, indiferent de ceea ce se găseşte dedesuptul său.
- Există 3 tipuri de servicii:

  1) serviciu nebazat pe conexiune şi fără confirmare (*Unacknowledged Connectionless Service*)

  2) serviciu orientat pe conexiune şi cu confirmare(*Connection Oriented Service)*

  3) serviciu neorientat pe conexiune, dar cu confirmare (*Semireliable Service*)

Reţele locale (Standardul IEEE 802)

Subnivelul MAC

- Este specific fiecărui tip de reţea LAN.
- Are ca principală funcţie, aceea a partajării mediului fizic (*medium sharing*).
- Asigură modul de operare cu difuzare (*broadcast*) specific reţelelor locale. Prin acest mod de operare, o staţie are acces la toate cadrele care circulă în reţea, indiferent care este emiţătorul.
- Modul de operare cu difuzare implică două probleme:

  - *la transmsie* trebuie să determine dacă mediul este liber şi apoi să detecteze eventualele conflicte.

  - *la recepţie* fiecare staţie trebuie să stabilească daca mesajul îi este adresat ei.

Reţele LAN Ethernet (802.3)

- Cea mai de succes tehnologie pentru reţele locale din ultimii 20 de ani.
- Versiuni apărute de-a lungul timpului:
  - Ethernet v1.0
  - Ethernet v2.0
  - IEEE 802.3
- Primele două versiuni au fost generate de un consorţiu format din firmele (Digital, Intel şi Xerox).
- Standardul IEEE 802.3 are la bază versiunea Ethernet v2.0
- Standardul IEEE 802.3 acoperă nivelul Fizic şi subnivelul de acces la mediu (MAC).
- Pentru subnivel MAC, metoda de acces la mediu se numeşte CSMA/CD (*Carrier Sense Multiple Access / Colission Detection*).

Reţele LAN Ethernet (802.3)

CSMA/CD

- Operează în 3 faze:

  1. sesizarea purtătoarei (*carrier sense*): fiecare staţie trebuie să “asculte” dacă mediul este sau nu liber.

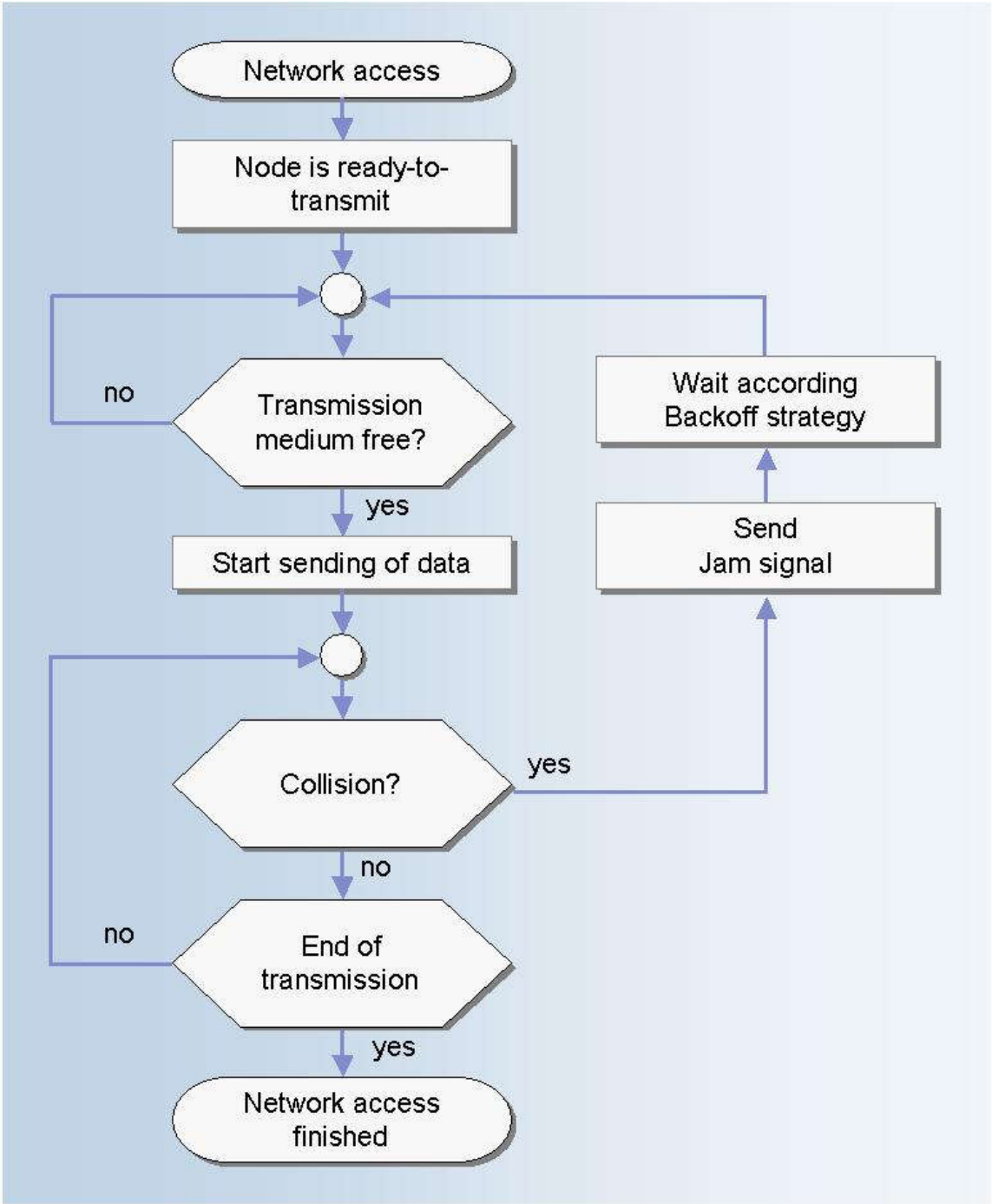
  2. accesul multiplu: posibilitatea ca oricare staţie care a detectat mediul liber să poată transmite. Acesta poate duce la coliziuni.

  3. detectarea coliziunii (*collision detection).* În timp ce transmite, fiecare staţie “ascultă” în continuare mediul pentru detectarea eventualelor coliziuni.

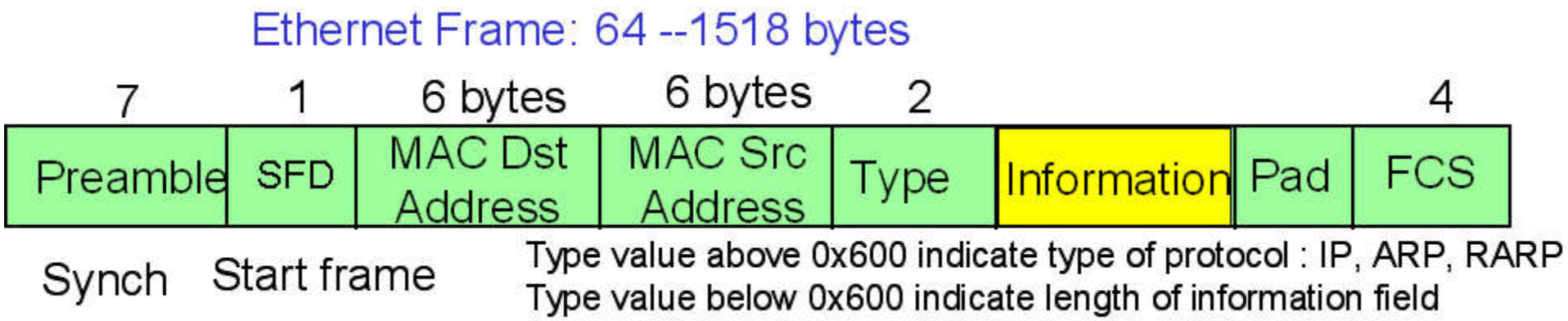
- La detectarea coliziunii este emis un semnal special (*jamming)*, având lungimea echivalentă a 32 de biţi. Acest semnal permite tuturor staţiilor să ia cunoştiinţă despre coliziune.
- Durata de aşteptare până la reluarea paşilor pentru transmisie este variabilă, fiind dată de un algoritm de revenire (*back-off algorithm*).
- Prin dispozitivele de interconectare se pot crea domenii de coliziune diferite.

Reţele LAN Ethernet (802.3)

CSMA/CD



Reţele LAN Ethernet (802.3)



- Lungimea unui cadru Ethernet este cuprinsă între 64 şi 1518 octeţi
  - valoarea minimă este stabilită din considerente de detectare a coliziunii, iar cea maximă din considerente de timp legate de ocuparea mediului.
- ***Preamble*** este folosite pentru sincronizarea ceasului staţiei receptoare cu ceasul staţie transmiţătoare.
- Ultimul octet din ***Preamble*** se numeşte ***SFD(Start Frame Delimiter)*** şi este folosit pentru a marca începutul cadrului.
- ***FCS (Frame Control Sequence)*** reprezintă valoarea sumei de control pentru câmpurile anterioare.

Reţele LAN Ethernet (802.3)

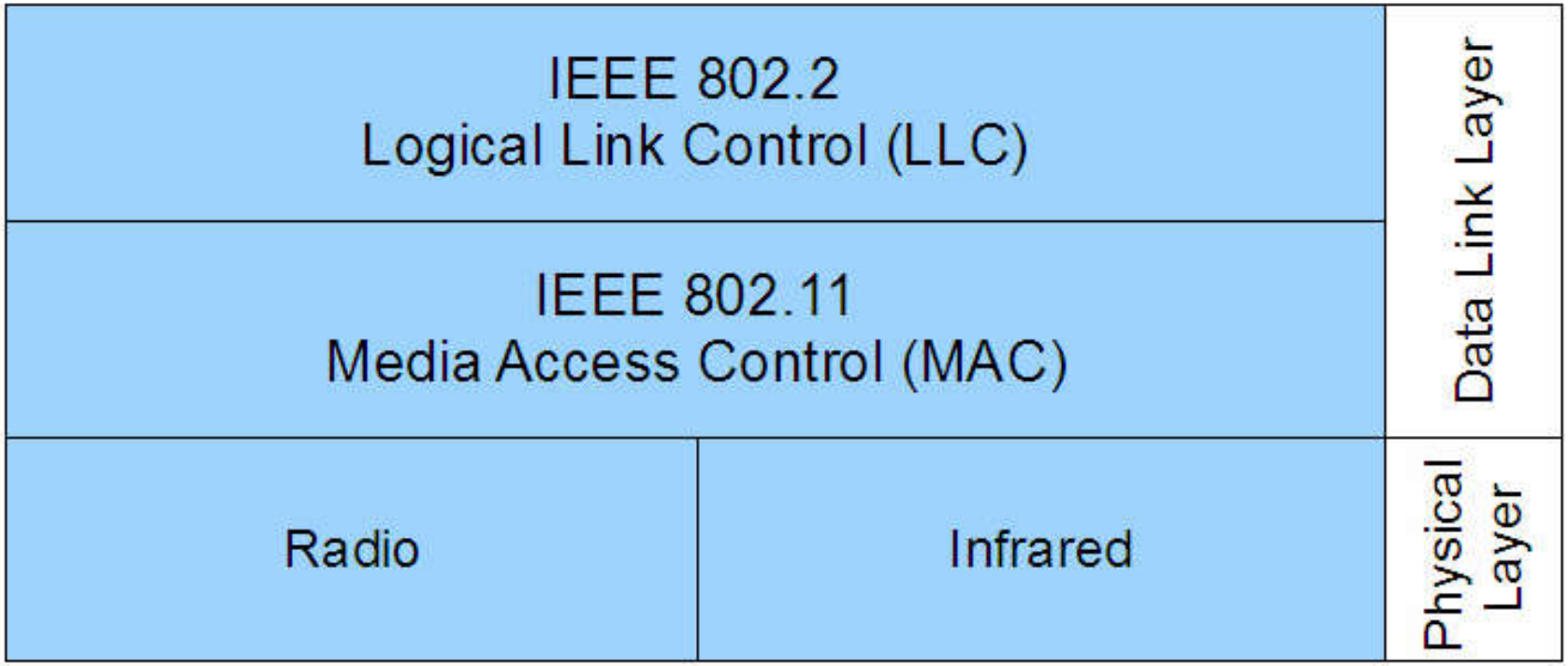
Versiuni ale standardului 802.3

- 10Base5, 10Base2, 10Base36 – toate sunt bazate pe cablu coaxial
- 10BaseT, 100BaseT, 10GBaseT, 100GBaseT – pentru cablu cu perechi de fire răsucite (cablu torsadat)
- 10BaseFP, 100BaseFX, 10GBaseR – pentru fibră optică

Reţele WLAN (802.11)

- Principala particularitate a reţelelor wireless este aceea că mediul fizic folosit în acest caz sunt undele radio.
- Acestea au proprietăţi total diferite de ale celorlalte medii fizice folosite în comunicaţiile de date:
  - este un mediu care nu are o delimitare clară în spaţiu.
  - nu este protejat faţă de interferenţele cu alte semnale.
  - are o topologie care se poate modifica uşor.
  - nu putem avea certitudinea că orice staţie este „auzită” de către a orice altă staţie.
  - modul de propagare a semnalelor poate varia în timp şi poate prezenta asimetrii.

Reţele WLAN (802.11)



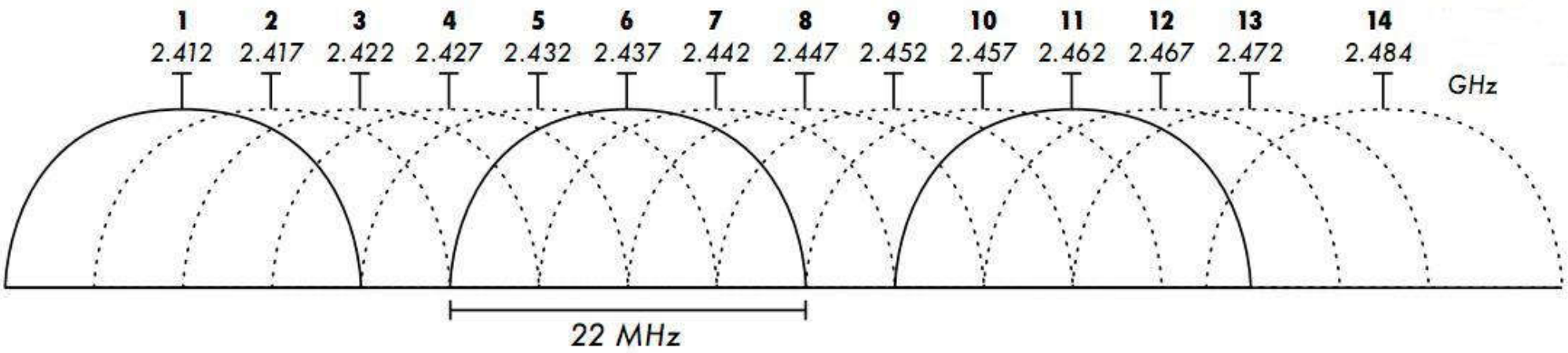
Reţele WLAN (802.11)

Wireless Transmission 802.11 Protocols					
Standards	**Year Established**	**Band Frequency**	**Maximum Data Transfer**	**Channel Bandwidth**	**Antenna Configuration**
802.11a	1999	5 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11b	1999	2.4 GHz	11 Mbps	20 MHz	1 x1 SISO
802.11g	2003	2.4 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11n	2009	2.4 & 5 GHz	600 Mbps	20 & 40 MHz	Up to 4x4 MIMO
802.11ac	2013	5 GHz	1.3 Gbps	20, 60, 80, 160 MHz	Up to 3x3 SU-MIMO
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	20, 60, 80, 80+80, 160 MHz	Up to 4x4 SU-MIMO & MU-MIMO

Reţele WLAN (802.11)

802.11b

- Foloseşte ca metodă de acces la mediu DSSS (Direct Sequence Spread Spectrum) în banda de 2,4 GHz.
- Lăţimea de bandă avută la dispoziţie este de 97MHz, împărţită în 14 canale, cu doar 3 canale nesuprapuse.
- Lăţimea fiecărui canal este de 22MHz, cu o distanţă între purtătoare de doar 5MHz.
- Rata maximă de transfer este de 11Mbps, dar ca valoare efectivă se obţine maxim 5Mbps.



Reţele WLAN (802.11)

802.11g

- Este o extensie a standardului 802.11b.
- Operează tot în banda de 2,4GHz, dar ca metodă de acces la mediul fizic este folosită tehnologia OFDM (*Orthogonal Frequency Division Multiplexing*).
- Lăţimea de bandă oferită este la fel ca şi în cazul lui 802.11b, adică de 97MHz, impărţită în 14 canale, cu 3 canale nesuprapuse.
- Rata maximă de transfer este de 54Mbps, dar ca valoare efectivă maximă se obţine 22Mbps.
- Datorită compatibilităţii dintre cele două standarde, un dispozitiv 802.11g va putea comunica cu un dispozitiv 802.11b, dar la rate de transfer de maxim 11Mbps.

Reţele WLAN (802.11)

802.11a

- Operează în banda de 5GHz şi de aceea compatibilitatea cu standardele 802.11b şi 802.11g nu este posibilă.
- Metoda de acces la mediul fizic este tot OFDM, dar datorită lăţimii de banda mai mari (300 MHz) s-au putut obţine mai multe canale, existând 8 canale nesuprapuse, faţă de 3 în cazul benzii de 2,4GHz.
- Rata maximă de transfer este tot de 54Mbps, iar ca rată de transfer efectivă se obţine un maxim de 27Mbps, mai mare decât în cazul lui 802.11g.

Reţele WLAN (802.11)

Topologii posibile pentru o reţea 802.11

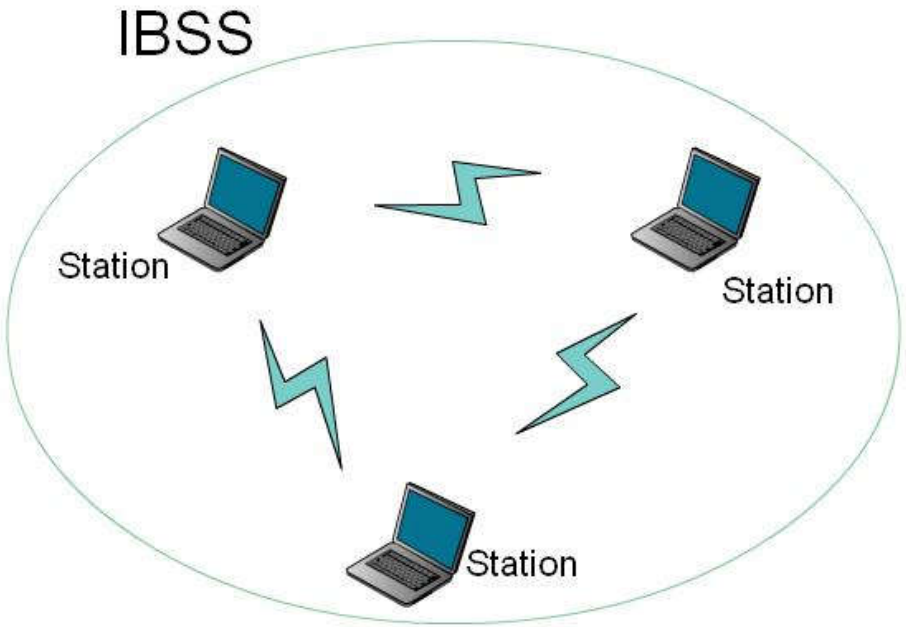
- O reţea locală de tipul 802.11 se bazează pe o arhitectură de tip celular.
- O celulă poarte denumirea de BSS (*Basic Service Set*) şi este controlată de către un AP (*Access Point*).
- AP-ul are un rol de releu pentru staţiile (STA în terminologie 802.11) din interiorul unui BSS, după cum se va vedea în continuare.

- Există trei tipuri de topologii pentru o reţea de tip WLAN:
    - Independent basic service set (IBSS)
    - Basic service set (BSS)
    - Extended service set (ESS)

Reţele WLAN (802.11)

Independend basic sevice set

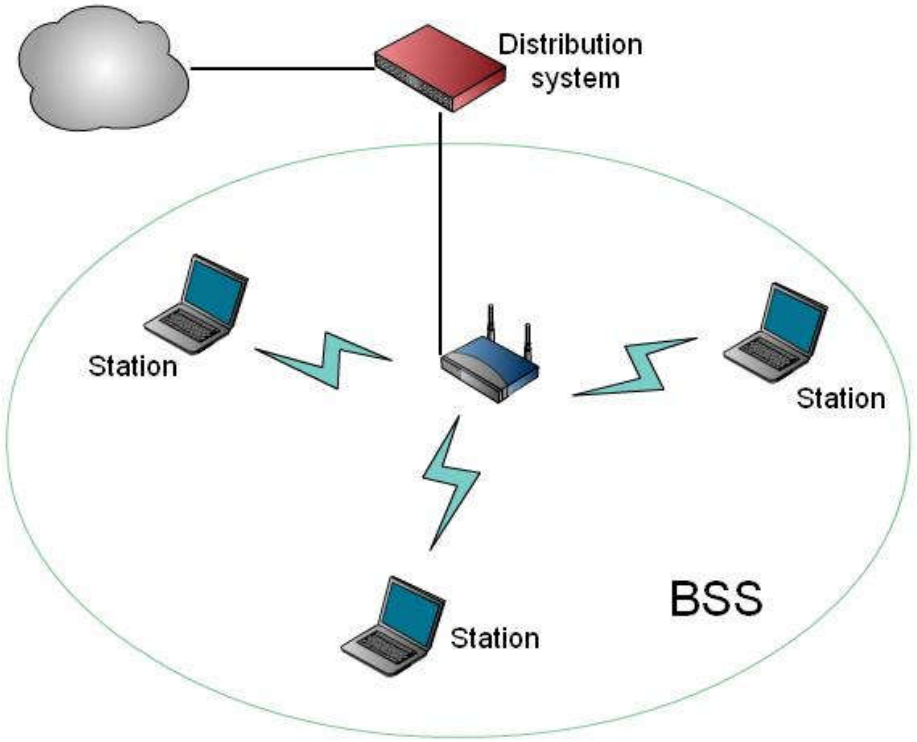
- În acest tip de topologie reţeaua WLAN este alcătuită dintr-un grup de staţii care comunică direct unele cu altele şi de aceea mai este numită şi reţea ad-hoc.



Reţele WLAN (802.11)

Basic service set

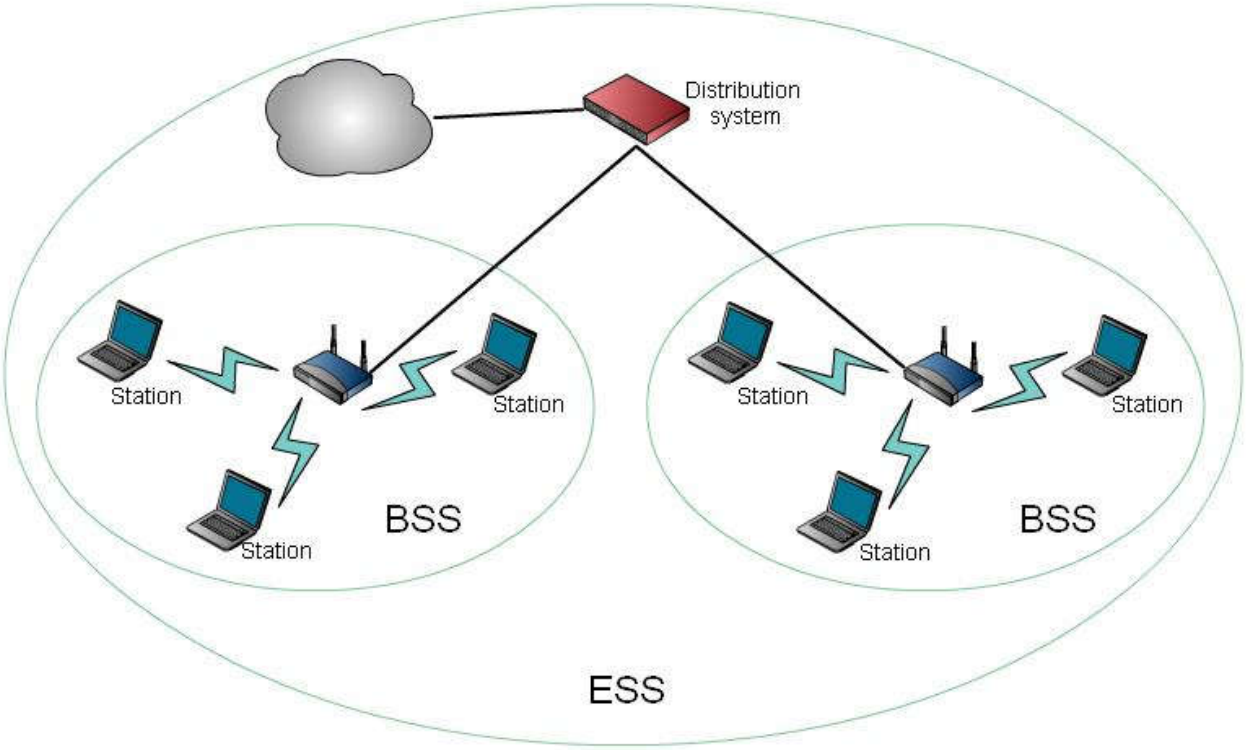
- Staţiile nu vor comunica direct între ele, ci doar cu un dispozitiv specializat, numit Acceess Point (AP).
- Se creează o topologie de tip celular, o celulă fiind alcătuită dintr-un AP şi staţiile conectate la el.



Reţele WLAN (802.11)

Extended sevice set

- Mai multe AP-uri pot fi conectate între ele prin intermediul unei infrastructuri (ex: Ethernet)



Reţele WLAN (802.11)

Subnivelul MAC

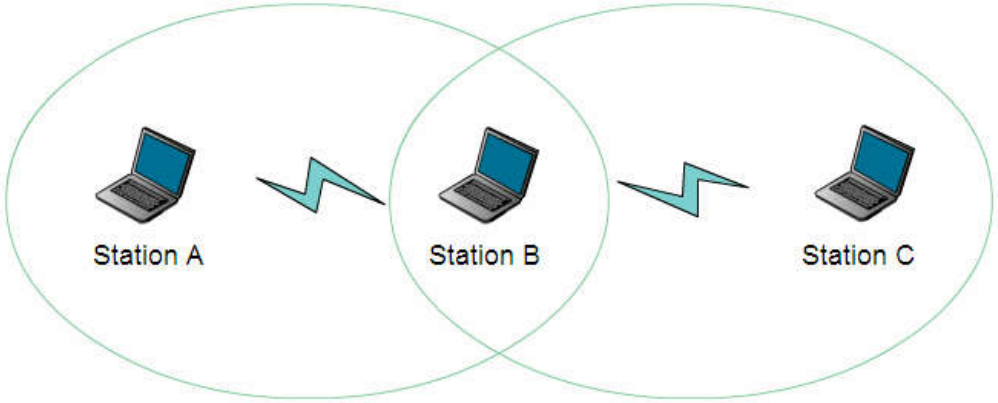
- În cazul WLAN subnivelul MAC trebuie să îndeplinească următoarele operaţii:
  - fragmentarea pachetelor
  - transmisia pachetelor
  - retransmisia pachetelor
  - confirmarea pachetelor

- Metoda de acces la mediu este CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), ceea ce înseamnă că se incearcă pe cât posibil evitarea coliziuniilor.

Reţele WLAN (802.11)

Subnivelul MAC

- Metoda *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) folosită în reţelele Ethernet nu ar fi practică în acest caz din două motive:
  - necesită implementarea unui mecanism full duplex de comunicaţie între staţii, ceea ce ar conduce la costuri ridicate de producţie
  - nu există certitudinea că staţiile se „aud" toate între ele, adică este posibil ca cel care transmite, să creadă că mediul este liber, dar de fapt în zona receptorului mediul să fie ocupat (*the hidden node problem*). În figura de mai jos se observă că staţia A nu "aude" conversaţia dintre B şi C şi nici staţia C nu „aude" conversaţia dintre A şi B.



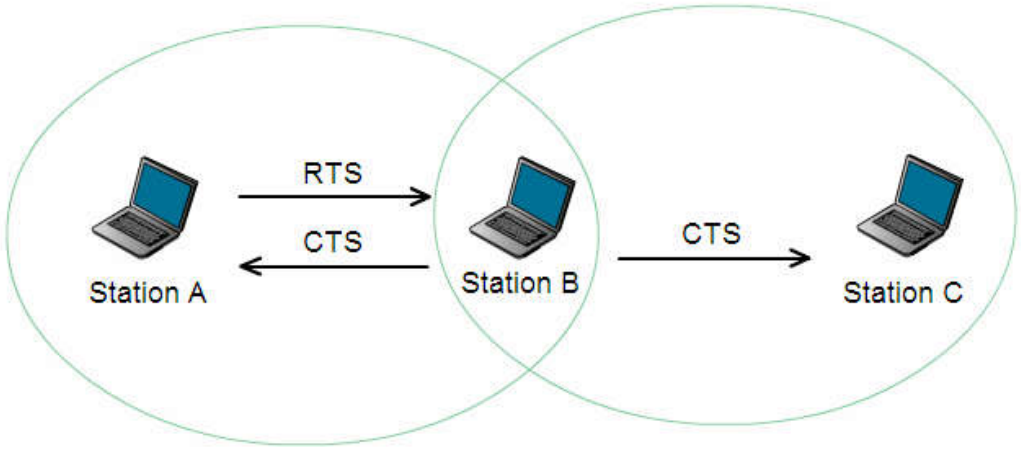
Reţele WLAN (802.11)

Subnivelul MAC

- Există două modalităţi de a detecta dacă mediul fizic este liber:

  - detectarea prezenţei altor transmisii prin ascultarea propriu-zisă a mediului (*Physical Carrier Sense*).

  - ascultare virtuală a mediului (*Virtual Carrier Sense*). Această metodă presupune folosirea unor pachete de control numite RTS (Request to Send) şi CTS (Clear to Send).



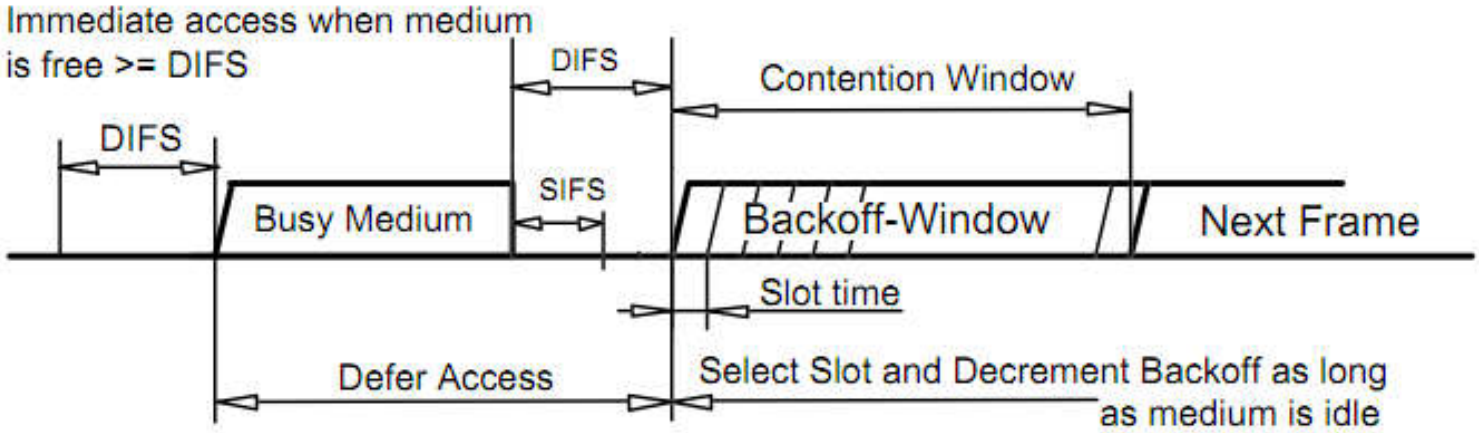
Reţele WLAN (802.11)

Subnivelul MAC - *Physical Carrier Sense*:

- Staţia care transmite ascultă mediul. Daca acesta este ocupat amână transmisia, iar dacă este liber pentru o perioada de timp egala cu DIFS (Distributed Inter Frame Space) poate trece la transmiterea pachetele. Deoarece există o probabilitate destul de mare ca două staţii care sesizează că mediul este liber să încerce să transmită simultan, există un mecanism de evitare a unor astfel de situaţii, prin care staţiile mai aşteptă un interval de timp aleator, şi doar după scurgerea acestui interval de timp, dacă mediul este în continuare liber, staţia poate trece la transmiterea datelor.
- Staţia care recepţionează pachetele verifică suma de control care le însoţeşte, iar apoi le confirmă printr-un pachet de tip ACK. Dacă sursa primeşte pachetele de confirmare înseamnă că nu a avut loc nici o coliziune. Dacă nu se primeşte confirmarea înseamnă că a avut loc o coliziune şi pachetul care nu a fost confirmat este retransmis.

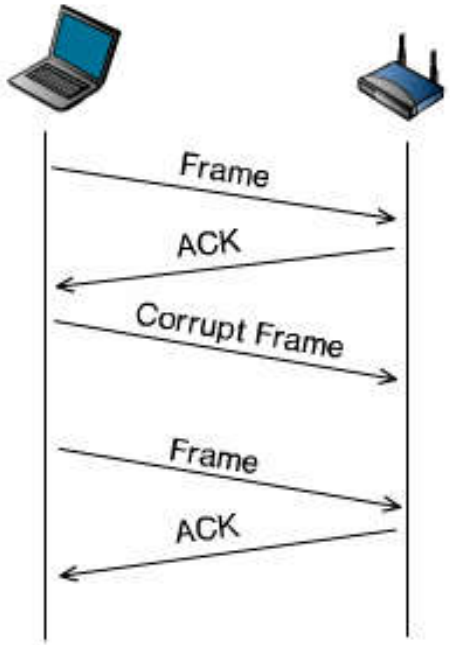
Reţele WLAN (802.11)

Subnivelul MAC -
Physical Carrier Sense



BackoffTime=Random() x *SlotTime*

- În 802.11 sunt practicate confirmările pozitive (*positive acknowledge*).



Reţele WLAN (802.11)

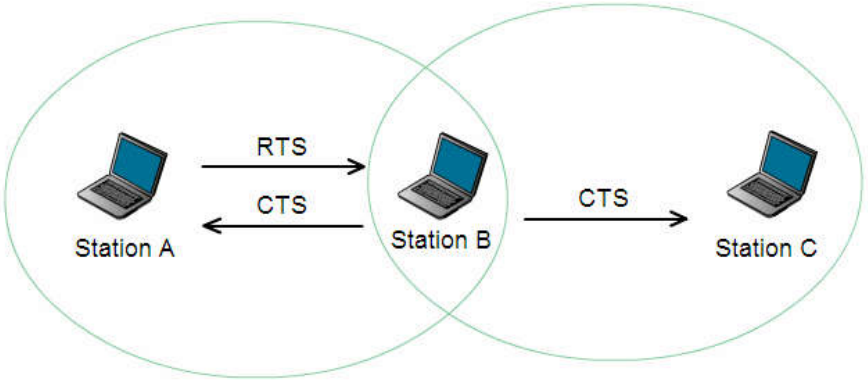
Subnivelul MAC - Virtual Carrier Sense

- Pentru a reduce probabilitatea unor coliziuni, situaţie care apar frecvent pentru cazul descris de către „the hidden node problem”, standardul a prevăzut şi metoda Virtual Carrier Sense.
- O staţie care vrea să transmită date, mai întâi trimite un scurt pachet de control numit RTS (Request to Send), care include adresa sursei, adresa destinaţiei şi durata transmisiei care urmează să aibe loc, această durată incluzând şi recepţia pachetului de confirmare, în scopul de a rezerva mediul pentru toate etapele unei transmisii. Dacă mediul este liber, atunci staţia destinaţie răspunde cu un pachet numit CTS (Clear to Send), care conţine aceleaşi informaţii legate de durata transmisiei.
- Când staţiile învecinate recepţionează fie un pachet RTS fie un pachet CTS îşi setează un indicator numit *NAV (Network Allocation Vector)* în conformitate cu informaţia de timp conţinută în aceste pachete. Acesta este de fapt un timer care este decrementat şi doar când ajunge la zero staţia poate încerca să transmită din nou, dacă mediul este liber. Daca una dintre staţii nu recepţionează pachetul RTS, nefiind în aria de acoperire a acelei staţii, atunci ea va recepţiona pachetul CTS, care vine ca răspuns la RTS. Prin acest mecanism este rezolvată şi „problema nodului ascuns”.

Reţele WLAN (802.11)

Subnivelul MAC - Virtual Carrier Sense

- Chiar dacă staţia C nu „aude” pachetul de tip RTS, ea va recepţiona pachetul CTS trimis de staţia B. Pe baza informaţiei din acest pachet îşi va seta indicatorul NAV.



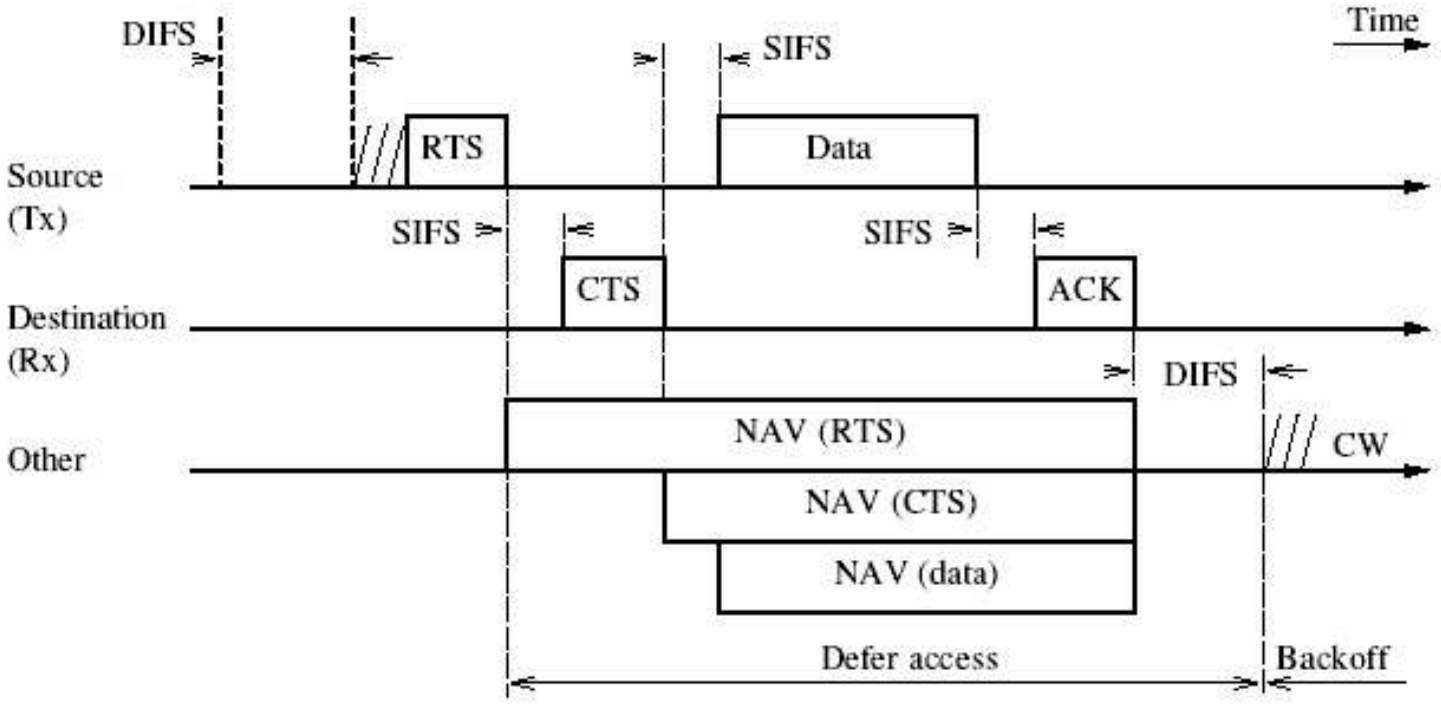
- O staţie care vrea să transmită va aştepta un interval de timp egal cu valoarea dată de NAV, iar apoi apelează la algoritmul de tip *backoff* pentru a calcula momentul transmisiei. Mecanismul oferit de timer-ul NAV nu implică neapărat folosirea pachetelor RTS/CTS. Există situaţii când pachetele de date conţin informaţii de timp care duc la actualizarea timer-ului NAV.

- Dacă este activat mecanismul RTS/CTS, capacitatea de transfer a reţelei este diminuată. De aceea, acest mecanism este eficient, doar în cazul în care există o densitate relativ mare de staţii şi există riscul apariţiei fenomenului *the hidden node problem*.

Reţele WLAN (802.11)

Subnivelul MAC - *Virtual Carrier Sense*

- *Pentru cazul ilustrat în figura de mai jos, presupunem că înainte de transmisia datelor, au fost parcurşi toţi paşii prezentaţi în diagrama de pe slide-ul următor, pentru a determina dacă sunt îndeplinite toate condiţiile care să permită transmisia unui frame.*
  - *DIFS (Distributed InterFrame Space)* este intervalul minim pe durata căruia mediul de transmisie trebuie să fie liber.
  - *SIFS (Short Inter Frame Space)* Este ales în aşa fel încât să îi permită staţiei transmiţătoare să treacă din modul de transmisie în modul de recepţie.
  - *NAV (Network Allocation Vector)*



Reţele WLAN (802.11)

Subnivelul MAC

- În diagrama de mai jos sunt sintetizate condiţiile care trebuie îndeplinite pentru ca o staţie sau un access point să poată trece la transmisia unui frame.