NIVELUL LEGĂTURII DE DATE

Nivelul Legăturii de date este nivelul care face trecerea datelor din calculator în mediul prin care este trimisă informaţia (cablu, fibra optică sau unde radio). Acest nivel controlează fluxul de date în mediul de transport şi oferă adresarea fizică (adresele MAC). Aici se implementează tehnologiile care asigură diferite topologii logice ale reţelelor (Ethernet, IEEE 802.3, IEEE 802.11 etc). Pe scurt, se poate afirma că nivelul Legătură de date este responsabil cu adresarea fizică şi cu accesul la mediu (canal de comunicare). Nivelul Legăturii de date este stratul cu numărul 2 corespunzător modelului OSI –figura 1.



Fig. 1 Nivelul Legăturii de date în structura modelului ISO-OSI

În cadrul nivelului Legăturii de date are loc un nou proces de încapsulare prin adaugarea:

● unui antet, în care principala informaţie este adresa fizică (MAC address);

● unei cozi (trailer) ce conţine informaţii pentru corectarea de erori.

În urma acestui proces PDU poartă numele de cadru (frame).

Nivelul legătură de date este deci responsabil cu transmiterea corectă a datelor printr-o legătură fizică existentă, între două puncte conectate direct prin această legătură fizică. Nivelul fizic nu poate realiza acest lucru, deoarece la nivelul fizic nu putem vorbi despre nici un fel de date, ci numai despre biţi şi, mai exact, despre reprezentarea fizică a acestora (niveluri de tensiune, intensitate a luminii etc.).

Nivelul legătură de date este împărţit în două subniveluri, cu roluri diferite:

● Subnivelul de control al legăturii logice, LLC (Logical Link Control);

Acest subnivel are scopul de a asigura comunicarea între nivelul Legăturii de date şi nivelul superior, nivelul Reţea. Acest subnivel este independent de tehnologie, adică el oferă nivelurilor superioare funcţii ce sunt aceleaşi pentru orice variaţii ale nivelului fizic şi ale subnivelului MAC. El se ocupă de formarea cadrelor, controlul erorilor, servicii de confirmare dacă este cazul, interfaţa cu nivelul superior etc. indiferent cum este partajat mediul de transmisie. El crează o interfaţă uniformă între nivelele superioare şi subnivelul MAC.

● Subnivelul de control al accesului la mediu, MAC (Media Acces Control)

Al doilea subnivel are două roluri majore:

◦ stabilirea şi respectarea regulilor de acces la mediu comun de transmisie a mai multor utilizatori;

◦ adaptarea la mediul fizic, astfel încât, să ascundă diferenţele legate de diferite medii de transmitere, forme de semnal, coduri de linie etc.

Acest subnivel asigură accesul ordonat şi controlat la mediu. Aceasta înseamnă, spre exemplu, că două staţii nu pot transmite în acelaşi timp, iar erorile cauzate de încercările de a transmite simultan sunt detectate. Acest subnivel este dependent de tehnologia LAN care este implementată. De exemplu, în cazul Ethernet-ului, este necesar un mecanism de detecţie a coliziunilor, dar în cazul Token Ring acest lucru nu mai este necesar.

Formatul cadrelor diferă de la un protocol la altul, dar o formă generală este cea din figura 2.



Fig. 2 Formatul general al unui cadru

Semnificaţia câmpurilor din figura 2 este următoarea:

● Câmpurile Start şi Stop au structură fixă şi reprezintă delimitatori de cadru;

● Câmpul Adresă conţine adresele de nivel fizic (sau MAC) ale sursei şi ale destinaţiei;

● Câmpul Control are rolul de a permite controlul transmisiei în funcţie de timpul de recepţie, inclusiv prelucrare şi retransmisie în caz de erori;

● Câmpul Verificare este destinat monitorizării erorilor de transmisie;

Cea mai simplă metodă de control a erorilor este bitul de paritate. O altă metodă mai elaborată este suma de control. Ea se efectuează la emisie, se înscrie în câmpul de control şi se verifică la recepţie. Dacă valorile sunt diferite, rezultă că în timpul transmisiei au apărut erori şi se iau decizii în consecinţă. Verificarea erorilor se poate face pentru tot blocul de date (tot cadrul ) sau numai pentru antet. La nivelurile 1 şi 2 ale modelului ISO-OSI s-au impus de-a lungul timpului standardele stabilite de IEEE (Institutul Inginerilor Electicieni şi Electronişti). Conform acestora, cele două niveluri au fost împărţite în două părţi, una dependentă de tehnologie, care de obicei este materializată prin implementare hardware şi una independentă de tehnologie, ce este reprezentată de nivelul LLC. Comparând modelul OSI cu standardele IEEE, figura 3, ar putea părea, la prima vedere, că acestea din urmă nu respectă modelul OSI din două puncte de vedere.

● standardul IEEE creează propriul nivel în model, nivelul LLC;

● standardele IEEE pentru MAC traversează două niveluri din modelul OSI.

Pentru a explica această neconcordanţă, trebuie întâi să facem observaţia că modelul OSI constituie baza teoretică general acceptată în ceea ce priveşte reţelele de calculatoare. Standardele IEEE au apărut mai târziu pentru a rezolva unele probleme de natură pur practică apărute în timp. Prin urmare, din considerente de natură exclusiv practică, a apărut acest model al standardelor IEEE, model ce separă partea ce depinde de implementarea fizică efectivă a reţelei şi a tehnologiilor folosite de interfaţa cu nivelurile superioare, ce sunt niveluri unde prelucrările se realizează prin software.



Fig.3 Formatul general al unui cadru

**1 Funcţiile nivelului Legăturii de date**

Nivelul Legăturii de date este situat deasupra nivelului fizic şi asigură servicii pentru nivelul Reţea. Rolul său de bază este transmiterea corectă a blocurilor de date între două noduri vecine din reţea. Nivelul legătură de date oferă transportul sigur al informaţiei printr-o legătură fizică directă. Pentru a realiza acest lucru, nivelul legătură de date se ocupă cu adresarea fizică, topologia reţelei, accesul la reţea, detecţia şi anunţarea erorilor şi controlul fluxului fizic (flow control).

 Problemele principale rezolvate de nivelul legatura de date se refera la:

● Oferirea unor funcţii de comunicare generice către nivelurile superioare, ascunzând tehnologia pe care se bazează reţeaua.

Acestea sunt asigurate la subnivelul LLC şi au scopul de a uniformiza transmisia din punctul de vedere al nivelului Reţea şi de a face prezenţa diferitelor tehnologii de reţea transparentă pentru acesta;

● Oferirea unei modalităţi de indetificare fizică a nodurilor care comunică (identificarea sursei si destinatiei datelor). Acest lucru se realizează printr-o schemă de adresare fizică bazată pe adrese MAC.

Adresele MAC sunt unice pentru fiecare calculator şi nu pot fi modificate. Este important de reţinut că adresele MAC sunt asignate unic pe fiecare placă de reţea şi nu pe fiecare calculator. Astfel, dacă unui calculator i se schimbă placa de reţea, adresa acestuia de MAC se va modifica. Adresele MAC nu pot fi modificate şi vor rămâne aceleaşi dacă calculatorul este mutat dintr-o reţea în alta;

● Gruparea şirurilor de biţi transmise de nivelul fizic în cadre. Aceasta este prima forma de interpretare a biţilor, care fără această grupare în cadre sunt lipsiţi de semnificaţie;

● Asigurarea accesului ordonat şi controlat la mediu prin subnivelul MAC;

● Detecţia erorilor de transmisie.

Acest lucru se realizează prin intermediul adaugării la cadre a unei informaţii de control, constituită dintr-o sumă ciclica CRC ce permite identificarea erorilor apărute în transmisia realizată de nivelul fizic.

**2. Protocoale de acces la mediu**

Nivelul Legaturii de date este responsabil cu asigurarea accesului sigur la mediu. Responsabilitatea sa este de a gestiona şi de a organiza accesul la mediul de transmisie astfel încât transmiterea efectivă să se realizeze corect. Acest lucru presupune, spre exemplu, în cazul în care conexiunea este de tipul share-media (în care mediul de transmisie este accesibil tuturor simultan şi este împărţit între staţii), să se realizeze detecţia şi corecţia cazurilor în care doua staţii încearcă să transmită simultan (aşa-numitele coliziuni). Subnivelul MAC conţine protocoalele care determină într-o reţea locală care staţie are dreptul să transmită la un moment dat. Aceste protocoale organizează comunicarea şi gestionează modul şi momentul în care fiecare staţie are acces la mediul de transmisie.

Exista doua mari categorii de acces la mediu de transmisie:

● Determinist (asigurarea unui interval exclusiv de emisie, pe rând, pentru fiecare staţie), care presupune faptul că fiecare staţie ştie exact când va transmite. Se presupune că există o secvenţă garantată şi regulată (reproductibilă) de oportunitaţi de transmisie pentru fiecare staţie. În această metodă, fiecare staţie are dreptul să transmită pe rând. De obicei implementarea pentru accesul la mediu determinist este realizată prin pasarea unui jeton (token). O staţie care doreşte să transmită date captează jetonul şi astfel nici o altă staţie nu mai poate transmite. După ce a terminat transmisia, staţia care deţinea jetonul îl eliberează pentru a putea fi folosit de o altă staţie. În funcţie de topologia reţelei, există protocoale cu jeton pe magistrală (IEEE 802.4 - Token bus) sau pe inel (IEEE 802.5 - Token ring).

Asigurarea unui interval exclusiv de emisie permite garantarea, pentru fiecare staţie, a unui debit minim cu care poate emite şi a unui interval maxim de aşteptare din momentul în care are ceva de transmis şi până la intrarea în emisie;

● Nedeterminist (acceptarea posibilităţii coliziunilor şi retransmisia pachetelor distruse în coliziuni) care utilizeaza o abordare de tipul primul venit, primul servit. Această alocare dinamică permite accesul abonaţilor la mediu după anumite reguli care pot asigura utilizarea eficientă a acestuia. Alocarea dinamică are la bază câteva ipoteze:

◦ Există N staţii (terminale) independente care generează cadre de transmis. Rata generării cadrelor este constantă iar probabilitatea de a genera un cadru într-un interval de timp este proporţională cu acest interval. Odată ce a fost generat un cadru, staţia nu mai generează altul până nu s-a transmis acesta.

◦ Canalul unic este accesibil tuturor staţiilor pentru a transmite sau recepţiona din linie.

◦ Când două sau mai multe cadre se suparpun chiar şi parţial în canal, apare o coliziune şi transmisia trebuie să înceteze deoarece semnalele electrice interferează.

◦ Timpul apariţiei cadrelor este o varibilă continuă. Nu există un ceas care să împartă timpul în momente discrete. Într-o altă variantă se poate lua în considerare şi ipoteza unui timp discret.

◦ Detecţia purtătoarei este metoda curentă prin care se poate afla dacă un canal este ocupat sau liber.

Prima procedură bine elaborată de control a accesului la mediu a fost ALOHA. La început se baza pe ipoteza timpului continuu (ALOHA pur) iar ulterior a apărut şi varianta cu timp cuantificat (slotted ALOHA). Ideea de bază la ALOHA pur este că utilizatorii sunt lăsaţi să transmită în voie cadrele după necesităţi. Când apar coliziuni pachetele vor fi distruse şi cadrele retransmise, deoarece transmiţătorul este anunţat despre acest lucru. Într-ul LAN retransmisia este imediată datorită distanţei de propagare mici. Pe o linie cu întârzieri mare (270 ms) reacţia este mult mai lentă şi eficienţa transmisiei scade foarte mult.

În scopul reducerii riscului coliziunilor, înainte de a transmite, o staţei ascultă mediul de transmisie pentru a vedea dacă este libel şi apoi transmite. Şi în acest caz există mai multe reguli.

◦ CSMA (Carrier Sense Multiple Access) persistent. Când o staţie are date de transmis, asultă mediul şi dacă este liber transmite imediat. Din cauza timpului de propagare prin canal, o altă staţie (mai apropiată sau mai depărtată) ascultând canalul îl găseşte liber şi începe şi ea să transmită. În scurt timp apare coliziunea şi ambele staţii încetează emisie revenind în ascultare. La prima sesizare de canal liber începe din nou să emită.

◦ CSMA nepersistent diferă de primul caz prin aceea că staţiile nu sunt aşa de lacome să emită imediat ce găsesc din nou liber pe canal, ci aşteaptă un timp aleator. În acest mod sacde probabilitatea unei noi coliziuni.

◦ CSMA cu detecţia coliziunii (CSMA/CD). Când două staţii găsesc canalul liber şi încep emisia simultan, vor detecta imediat şi coliziunea şi opresc imediat transmisia cadrelor care oricum se pierd. Astfel se câştigă oarece timp în care canalul este ocupat. Protocolul CSMA/CD este larg folosit în LAN-urile Ethernet.

◦ CSMA cu evitarea coliziunii CSMA/CA) este folosit în LAN-urile wireless (standardul 802.11). Evitarea coliziunii se face în acest caz prin trimiterea unui cadru scurt care să oprească toate transmisiile care ar putea exista la un moment dat.

*a) Protocolul CSMA/CD*

Protocolul CSMA/CD este cel pe baza căruia funcţionează Ethernetul. După cum se ştie, Ethernetul se bazează pe un mediu de tip share-media, deci numai o singura staţie poate transmite la un moment dat.

Când o staţie doreşte să transmită, ea urmează umătorul procedeu:

◦ Ascultă mediul până când nu mai transmite nimeni (exista mijloace hardware de detecţie a faptului că o altă staţie foloseşte mediul pentru a transmite);

◦ Când este sesizat faptul că nimeni altcineva nu mai transmite, se aşteaptă un timp aleator şi apoi se începe transmisia. Este posibil însă ca la acelaşi moment o altă staţie să fi început să transmită în acelaşi timp, caz în care apare o coliziune;

◦ La detectarea unei coliziuni, este transmis un semnal de bruiaj (semnalul de jam) o perioada foarte scurtă de timp, pentru a avertiza toate staţiile din reţea asupra producerii unei coliziuni.

◦ După ce această coliziune a fost remarcată de toate staţiile din reţea (din domeniul de coliziune mai exact), este apelat un algoritm de backoff şi transmisia încetează. Toate staţiile se opresc din transmis pentru o perioadă aleatoare de timp, după care reîncearcă să transmită. Procedurile anterioare ridică mai multe probleme de timp (temporizare), toate depinzind de Perioada Critică ( Slot Time).

Slot Time are următoarele semnificaţii:

◦ este o limită superioară a timpului necesar pentru a detecta o coliziune, deci a pierderii de banda de transmisie;

◦ este o limită superioară a timpului de ocupare efectivă a mediului (acquisition time of the o medium), adică perioada după care transmisia nu mai sufera coliziuni;

◦ este o limită superioară a lungimii fragmentului de cadru transmis la apariţia unei coliziuni;

◦ este o cuantă de planificare pentru retransmisie.

Pentru a acoperi aceste functii, Slot Time este definită ca fiind mai mare decât suma dintre timpul de propagare a semnalului dus-întors pe mediul fizic (de doua ori timpul necesar ca un semnal sa parcurgă drumul de la un capat la celalalt al mediului fizic) şi timpul de bruiaj (la nivelul MAC ). Acest timp depinde de particularitatile mediului fizic.

*b) Protocolul CSMA/CA*

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) este un protocol de acces la mediu care ascultă mediul pentru a evita coliziunile, spre deosebire de CSMA/CD, care îşi reglează transmisia de date odată ce coliziunile s-au produs. Staţiile care fac parte dintr-o reţea fără fir emit într-o bandă de frecvenţe alocată, limitată ca dimensiune. Din cauza limitării intervalului alocat, mediul partajat de staţii este deschis coliziunilor. Tehnica de acces la mediu folosită în prezent de reţelele locale este CSMA/CA, un protocol de acces care are câteva asemănări cu CSMA/CD pe Ethernet. CSMA/CA este proiectat astfel încât să reducă probabilitatea de coliziune la accesarea multiplă a mediului, în punctele în care e cel mai probabil să apară coliziuni, adică imediat ce mediul de transmisie devine liber în urma unei transmisii, când mai multe staţii care îşi aşteptau rândul ar putea începe să transmită. Protocolul foloseşte ascultarea mediului, ca şi CSMA/CD. În plus, pentru a acapara mediul se trimit rezervări, în forma unor mesaje de cerere de ocupare a mediului. Distribuirea informaţiilor de rezervare a mediului se face prin interschimbarea de către staţiile care vor să converseze a unor cadre de tip RTS (Request to Send) şi CTS (Clear to Send). Aceste două tipuri de cadre conţin un câmp de durată, care specifică perioada de timp pentru care se doreşte ocuparea mediului pentru transmisia datelor, a cadrului ACK de la terminarea conversaţiei, şi a tuturor intervalelor de timp dintre cadrele trimise. routerele.

*c) Domeniul de coliziune şi de broadcast*

Domeniul de coliziune este acea zona dintr-o retea care va fi afectată de apariţia unei coliziuni în interiorul ei. Dispozitivele din categoria hub-urilor şi repetoarelor propagă coliziunea. Creşterea numărului de coliziuni este cauzată de intensificarea transmisiilor mai ales datorită unui număr crescând de staţii din acelaşi domeniu de coliziune şi duce la degradarea abruptă a performanţelor reţelei. Reteaua locala poate fi împarţită în domenii de coliziune separate prin intermediul switch-urilor. Domeniul de broadcast este constituit din staţiile care vor auzi un mesaj de tip broadcast trimis de unul dintre ele. Creşterea numărului broadcast-urilor duce la scăderea performanţelor reţelei. Singurele dispozitive care pot separa domeniile de broadcast sunt routerele.

**3. Standardul ETHERNET**

Pentru orice comunicare în reţea trebuie să existe un mecanism de adresare, care să permită recunoaşterea unică a calculatoarelor conectate. Primul standard Ethernet a fost publicat în 1980 de un consorţiu format din firmele DEC, Intel şi Xerox, consorţiu numit DIX. Ethernet-ul funcţiona atunci pe un suport de cablu coaxial gros, numit thicknet, şi atingea viteze de până la 10Mbps. În 1985, IEEE (Institute of Electrical and Electronics Engineers) au publicat o serie de standarde pentru LAN, serie care începea cu 802.x. Standardul pentru Ethernet este 802.3 şi a adus ceva modificări faţă de standardul iniţial propus de DIX, însă modificările sunt atât de mici, încât în linii mari cele două standarde sunt aproape identice. Datorită creşterii spectaculoase a performanţelor în domeniul calculatoarelor personale, a fost foarte clar simţită nevoia creşterii performanţelor în lumea reţelelor, care trebuiau să poată oferi viteze de acces din ce în ce mai mari. Astfel, în 1995 IEEE a anunţat un standard pentru Ethernet la 100Mbps – Fast Ethernet (IEEE 802.3u), iar în 1999 alt standard pentru Gigabit Ethernet (1 Gbps) – Gigabit Ethernet (IEEE 802.3z).

Formatul de bază a cadrului (frame-ului) rămâne acelaşi. Atunci când apare o dezvoltare nouă în această familie de tehnologii (aşa cum a fost cazul FastEthernet-ului şi GigabitEthernet-ului) IEEE scoate un nou supliment la standardul 802.3. Ethernet-ul foloseşte semnalizarea în banda de bază (baseband), de aici provine şi termenul de "Base" din denumirile tehnologiilor:10BaseT, 100BaseTX, etc.

● Standardul Ethernet 802.3.

Ethernet-ul este situat pe două niveluri ale stivei OSI şi anume partea de jos a nivelului legătură de date (subnivelul MAC) şi nivelul fizic. Pentru codificarea semnalului la nivel fizic în Ethernet sunt utilizate: codificarea Manchester (Manchester encoding) şi codificarea Manchester diferenţială (diferential Manchester encoding).

◦ Codul Manchester la care intervalul de un bit este împărţit în două interval egale. În prima jumătate a bitului 1 se transmite un nivel ridicat de tensiune, iar în a doua jumătate un nivel scăzut de tensiune. Bitul 0 este şi el împărţit în două jumătăţi, în prima jumătate se transmite nivelul scăzut de tensiune iar în a doua jumătate nivelul ridicat;

◦ Codul Manchester diferenţial la care bitul 0 are tranziţie la începutul intevalului iar bitul 1 nu are tranziţie la începutul intervalului. În ambele cazuri la jumătatea intervalului de bit are loc o tranziţie între cele două nivele semnificative ale semnalului electric.

Necesitatea folosirii unor coduri de linie speciale apare din nevoia de a Evita succesiunile lungi de 1 sau 0 consecutivi. Structura cadrului Ethernet este aproape identică, indiferent de varianta de Ethernet folosită, fiind prezentată în figura 4.



Fig. 4 Formatul general al cadrului Ethernet

Semnificaţia câmpurilor din figura 4 este următoarea:

◦ Preambul - 7 octeţi pentru sincronizarea ceasului receptorului. Fiecare octet conţine şablonul de biţi 10101010. Acest preambul permite ceasului receptorului să se sincronizeze cu cel al emiţătorului. Ceasurile trebuie să rămînă sincronizate pe durata cadrului, folosind codificarea Manchester pentru a detecta graniţele biţilor;

◦ Început cadru - 1 octet delimitator de cadru iniţial;

◦ Adresa destinaţie - 6 octeţi. Bitul cel mai semnificativ al adresei destinaţie este 0 pentru adresele obişnuite şi 1 pentru adresele de grup. Adresele de grup permit mai multor staţii să asculte de la o singură adresă. Cînd un cadru este trimis la o adresă de grup, toate staţiile din grup îl recepţionează. Trimiterea către un grup de staţii este numită multicast (trimitere multiplă). Adresa avînd toţi biţii 1 este rezervată pentru broadcast (difuzare). Un cadru conţinînd numai biţi de 1 în cîmpul destinaţie este distribuit tuturor staţiilor din reţea;

◦ Adresa sursă - 6 octeţi;

◦ Lungime/Tip (Type field) - 2 octeţi. Câmpul Lungime/Tip poate fi interpretat în două feluri: dacă valoarea acestuia este mai mică de 1536 (0x600 în hexazecimal) atunci el reprezintă lungimea. Dacă este mai mare de 1536, el reprezintă protocolul de nivel superior folosit;

◦ Date – până la 1500 octeţi. Pentru a facilita distingerea cadrelor valide de reziduri, Ethernet cere ca toate cadrele valide să aibă cel puţin 64 de octeţi, incluzînd adresa destinaţiei şi suma de control. Dacă porţiunea de date dintr-un cadru este mai mica de 46 de octeţi, se foloseste cîmpul de completare pentru a se ajunge la lungimea minima necesară. Câmpul de date nu are voie să depăşească valoarea de MTU – Maximum Transmission Unit - care pentru Ethernet este 1500 octeţi, ceea ce înseamnă că un cadru Ethernet nu are voie să fie mai mic de 64 şi mai mare de 1518 octeţi;

◦ Pad – până la 46 octeţi. Câmpul de date trebuie să fie mai mare de 46 de octeţi. Dacă cumva datele sunt de lungime mai mică, atunci i se adaugă o "umplutură" numită padding pentru a ajunge la dimensiunea de 46 octeţi

◦ Sumă contol (FCS) - 4 octeţi. Aceasta este un cod de dispersie pe 32 de biţi (32-bit hash-code) a datelor. Algoritmul sumei de control este un control cu redundanţă ciclică (CRC). El realizează doar detectarea erorilor şi nu are legătură cu corectarea lor.

● Fast Ethernet (Ethernet-ul rapid) IEEE 802.3u Din punct de vedere tehnic schimbările nu sunt multe schimbări la Fast Ethernet. În loc de codificarea Mancester se utilizează codificarea 8В/6Т şi 4В/5В.

● GigaBit Ethernet (Ethernetul Gigabit) IEEE 802.3z Ethernetul Gigabit suportă două moduri diferite de operare: modul duplex integral şi modul semi-duplex. Schema codificării semnalului la nivel fizic - 8В/10В.

**4. Standardul pentru reţele fără fir (WLAN)**

Reţelele locale fără fir (WLAN) oferă utilizatorilor aceleaşi facilităţi ca şi reţelele locale bazate pe infrastructura de cablu, dar fără limitarea impusă de fire. În plus, conform standardului, este posibilă şi conectarea fără fir la distanţă mare între reţele (până la 40Km). Standardizarea impusă reţelelor fără fir de IEEE şi Wi-Fi Alliance a permis interoperabilitatea echipamentelor, ceea ce a dus în final la scăderea costurilor şi la un proces de dezvoltare mai rapid. În momentul de faţă costurile de instalare a reţelei fără fir sunt considerabil mai mici, ceea ce face ca instalarea unui LAN fără fir să fie o soluţie viabilă, nu numai în cazul utilizatorilor mobili, ci şi ca un substitut al LAN-urilor clasice. IEEE 802.11 este o familie de protocoale care defineşte nivelul fizic şi subnivelul MAC al nivelului legatură de date. Standardul stabileşte ca medii de transmisie benzi de unde din domeniul infraroşu şi radio (incluzând microundele). În domeniul radio sunt specificate trei tipuri de transmisie folosind unde radio din benzile nelicenţiate de frecvenţe ISM de 2.4GHz şi 5GHz:

● 802.11b este primul standard lansat în domeniul reţelelor LAN fără fir, şi cea mai populară tehnologie astăzi; lucrează în banda de 2.4GHz şi atinge viteze de 11Mbps; problemele de care s-a lovit acest standard au fost încărcarea benzii ISM de 2.4GHz (în care lucrează multe alte sisteme, cum sunt Bluetooth şi cuptoarele cu microunde) şi viteza de transfer relativ mică;

● 802.11a lucrează în banda de 5GHz şi atinge viteze de 54Mbps; din cauza benzii diferite de transmisie este incompatibil cu 802.11b, dar lucrează într-o bandă de frecvenţe mult mai puţin aglomerată şi oferă viteze de transmisie comparabile cu cele oferite de reţelele de cupru;

● 802.11g este în fapt un amendament la 802.11b, care specifică o viteză de transfer de 54 Mbps (egală cu viteza 802.11a); este perfect compatibilă cu tehnologia 802.11b şi oferind viteze ri de transfer.

Echipamentele necesare implementării unei reţele fără fir 802.11 sunt:

● adaptoare de reţea, care înlocuiesc plăcile de reţea tradiţionale pentru calculatoare fixe sau mobile;

● acces point (AP), care este punctul central al unei reţele fără fir, dar care poate funcţiona şi ca un repetor sau poate asigura conectivitatea între o reţea fără fir şi una clasică;