

Streaming (flux) multimedia o instanță a aplicației va putea recepționa în timp real secvențe multimedia transmise prin rețea de la o altă instanță a aplicației. Aplicația nu va trimite un fișier integral, ci va transfera streamuri de date fără confirmare. Prin streaming, utilizatorii pot începe să vadă sau să asculte un document înainte ca acesta să fie transmis în întregime.

MIME-se adaugă linii de antet pentru a declara tipul conținutului; facilitare: includerea unor obiecte multiple într-un singur mesaj; reprezentarea textelor și cu alte seturi de caractere decât ASCII, includerea imaginilor sau fragmentelor video în mesaj

Fiecare protocol are definite 2 interfețe: 1. protocol care oferă servicii altor obiecte de pe același calculator 2. a 2-a interfață definește forma și semnificația mesajelor schimbat cu protocoale echivalente de pe alte calculatoare.

TCP 3way handshake în TCP este o metodă folosită de TCP pentru a seta o conexiune TCP/IP peste un IP din rețea. Acest mecanism este construit astfel încât 2 calculatoare care vor să comunice, să poată negocia parametrii conexiunii prin socket, înainte de a transmite date.

Un Web Service este o stivă de protocoale folosită pentru a defini, a localiza, implementa și a face ca serviciile web să interacționeze între ele.

SOAP-protocol bazat pe XML care asigură schimbul de informații între aplicații peste un canal HTTP. Protocol de comunicație; Format propriu de reprezentare a datelor; Independent de platformă, limbaj.

WSDL-web services description language-protocol bazat pe XML care asigură descrierea și localizarea serviciului web.

REST-simplifică modelul SOAP; orientat pe filozofia web clasică; fără niveluri de abstractizare suplimentare

LAN: -dist. dintre calc. nu depășește câțiva km; -conectarea se realizează prin diferite suporturi (cablu coaxial, fibră optică etc) -debitul se măsoară în MB/sec sau GB/sec -mecanismele de securitate sunt reduse

MAN: o interconectare a mai multor rețele LAN distribuite pe o zonă a unei localități sau chiar la nivelul întregii localități -viteză mare de transmisie -rețea privată sau publică -include diverse tehnici de conectare și comunicație -sunt prevăzute mecanisme de securitate -asigură leg. către rețele de tip WAN

WAN -acoperă o țară, continent sau chiar mai multe continente -leg. dintre două stații poate utiliza ca suport de comunicație rețeaua telefonică, undele radio sau sateliți -debitul obținut depinde de suportul utilizat -mecanismele de securitate sunt complexe

Switch-redirecționează mesajele pe baza de adresă fizică (adresă unică alocată dispozitivelor pentru plăcile de rețea și care permite identificarea unică a calc. din cadrul unei rețele).

Endpoint-După ce s-a creat un socket trebuie să realizăm o conexiune la server. Pentru a ne conecta la un computer din rețea trebuie să știm adresa de IP și portul la care ne conectăm. .NET oferă clasa `EndPoint` din cadrul namespace-ului `System.Net` ce reprezintă un terminal din rețea printr-o adresă de IP și un număr de port. Primul parametru al constructorului trebuie să fie o instanță a clasei `IPAddress` iar al doilea de tip `int` întreg reprezentând portul de comunicație: `EndPoint (IPAddress address, int port);`

Modelul de referință ISO/OSI

Nivelul fizic: pp. gestiunea și exploatarea suporturilor fizice de comunicație – interfețe mecanice și electrice, proceduri de recepție și emisie a informației binare, adaptarea semnalelor la suport, etc.

Exemplificarea conceptelor: --Serviciu: schimbul de info între 2 sisteme conectate printr-o leg. fizică; -

Interfață: specifică modul de transmitere a unui bit; -Protocol: utilizarea schemei de codificare pt. reprezentarea unui bit, nivel de tensiune, durata unui bit.

Nivelul legătură de date: generează cadrele ce vor fi transmise prin niv. fizic, asigură detectia și corectia erorilor de transmisie. Exemplificarea conceptelor.-- Serviciu: construirea cadrelor; emiterea cadrelor de date; alte servicii optionale: arbitrarea accesului la canalul de comunicație, controlul fluxului, asigurarea fiabilității transmisiei. - Interfață: emiterea unei unități de date la o mașină conectată la același mediu fizic; - Protocol: adresarea nivelului, implementarea controlului pt. accesul la mediu fizic.

Nivelul rețea: controlează operațiile din subrețea (directionează info în traversarea rețelei sau rețelilor; are capacitatea să stabilească și să întrerupă comunicații);

Nivelul transport: accepta datele de la nivelul superior, le fragmentează în unități de date care vor fi transmise nivelului rețea, controlează transferul de date punct-la-punct în traversarea rețelei.

Nivelul sesiune: realizează funcțiile care sunt necesare ca suport al dialogului dintre procese, cum ar fi inițializarea, sincronizarea și terminarea dialogului.

Nivelul prezentare: definește semantic și sintaxa datelor care se vor schimba.

Nivelul aplicație: oferă utilizatorului serviciile, definește mecanisme și protocoale specific tipurilor de aplicații: posta electronică, transferul de fișiere, serviciu web, etc.

Arhitectura Internet

Modelul arhitectural Internet a fost dezvoltat pornind în primul rând de la experiența practică dobândită de către cercetătorii ARPA în proiectarea și dezvoltarea aplicațiilor de rețea. Modelul Internet se mai numește și modelul TCP/IP după protocoalele principale care stau la baza acestuia. Modelul TCP/IP este alcătuit din patru niveluri: La nivelul cel mai de jos sunt protocoalele de acces la rețea, reprezentate de obicei printr-o combinație de specificații hardware și software (ex: placă de rețea și drivere pentru placa de rețea). Exemple de protocoale la nivelul acces la rețea ar fi protocol Ethernet sau protocolul Fiber Distributed Data Interface (FDDI). Nivelul Internet se ocupă cu expedierea pachetelor de date și transmiterea lor până la destinație și este reprezentat în primul rând prin protocolul IP. Acest protocol asigură interconectarea multitudinii de echipamente din rețea într-un model logic unic. Nivelul transport cuprinde două protocoale principale, Transmission Control Protocol (TCP) și User Datagram Protocol (UDP). Aceste protocoale asigură canale logice alternative pentru programele de aplicație. TCP asigură un canal fiabil orientat pe conexiune prin care sunt transmise fluxuri de date. UDP asigură un canal nefiabil prin care sunt transmise datagrame. Deasupra nivelului transport se găsește nivelul aplicație unde sunt o serie de protocoale care se ocupă printre altele cu reprezentarea și codificarea datelor sau cu controlul dialogului între aplicații. Amintim aici File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Domain Name System (DNS) sau Simple Mail Transfer Protocol (SMTP). **Modelul TCP/IP** asigură mecanismul de încapsulare și decapsulare a datelor precum și pe cel de multiplexare și demultiplexare a mesajelor. La nivelul transport mesajele sunt încapsulate în datagrame sau segmente, la nivelul rețea sunt generate pachete iar la nivelul acces la rețea sunt construite cadre care sunt transmise bit cu bit prin rețea. La recepție mesajul este livrat la nivelul aplicație după ce fiecare protocol de nivel inferior folosit a operat despachetarea mesajului primit.

Serverul Web reprezintă sistemul pe care rulează un software ce are ca scop principal distribuția informației stocate, sub forma unor documente. Exemplu de servere Web: httpd NCSA (National Computer Security Association), Apache, Zeus, IIS (Internet Information Server), PWS (Personal Web Server). Serverele vor fi suport pentru: eliberarea documentelor de pe server către client, când documentul este solicitat, appleturi scrise în Java, scripturi pe partea de server, maparea imaginilor clicabile

Nivelul transport realizează nivelul superior al serviciilor care se ocupă cu transferul informațiilor. El realizează comunicația punct-la-punct, sigură și eficientă, între procesele care se execută pe mașini situate la distanță.

Principalele funcții ale nivelului transport sunt:

- stabilirea și eliberarea conexiunii transport;
- transferul unităților de date normale și speciale;
- traducerea adresă transport - adresă rețea;
- numerotarea TPDU (Transport Protocol Data Unit), secvențierea unităților de date ale protocolului;
- reglarea fluxului;
- detectarea erorilor și supravegherea calității serviciului;

- reluarea în caz de eroare;
- realizarea multiplexării pe conexiunile de transport;
- segmentarea, gruparea, concatenarea.

UDP este utilizat ca un multiplexor/demultiplexor pentru emiterea și recepționarea datagramelor.

- UDP oferă un serviciu de transmisie a datagramelor: *fără conexiune, nefiabil, nu deține nici un mecanism pentru controlul fluxului sau recuperarea erorilor*
- UDP nu garantează corectitudinea transmisiei: datagramele pot ajunge la destinație în mod *neordonat, duplicate* sau *nu ajung*; Fiecare datagrama UDP este emisă într-o singură datagramă IP.
- UDP se utilizează în transmisiile *broadcast* și *multicast*.

Structura unui datagram UDP conține: *Portul sursă* – identifică numărul de port al procesului emitor (16 biți) și reprezintă portul ce va fi adresat în răspuns - *Portul destinație* - numărul de port al procesului de pe hostul destinație (16 biți) - *Lungimea* - dimensiunea datagramului (în octeți) - *Suma de control* este opțională și se utilizează pentru verificarea integrității datelor recepționate (16 biți) - *Datele UDP* urmează antetului. Aplicațiile care utilizează UDP: **TFTP** (Trivial File Transfer Protocol); **DNS** (Domain Name System); **RPC** (Remote Procedure Call) utilizat de NFS (Network File System); **SNMP** (Simple Network Management Protocol); **LDAP** (Lightweight Directory Access Protocol).

TCP asigură un serviciu orientat pe conexiune pentru transmiterea fiabilă a datelor, cu detectarea erorilor și controlul fluxului. Este utilizat de majoritatea protocoalelor nivelului aplicație, cum ar fi: HTTP, SSH, Telnet, FTP etc. **Protocolul TCP** realizează: *conexiunea logică* - fiecare conexiune este identificată unic printr-o pereche de socketuri utilizate de procesele de emisie și recepție; *transferul fluxului de date*; *fiabilitatea transmisiei*; *controlul fluxului de date*; *multiplexarea* – prin utilizarea porturilor.

TCP - grupează octeții în segmente TCP. Segmentele TCP sunt încapsulate în datagrama IP pentru a fi transmise, prin rețea, la destinație. Pentru garantarea fiabilității, TCP asociază un număr de secvență fiecărui octet transmis și așteaptă o confirmare (acknowledgment - ACK) pozitivă de la receptorul TCP.

Interfața socket este una dintre interfețele de programare a aplicațiilor din rețea.

Când se utilizează socket-urile se are în vedere următoarele: Un socket este un tip special de *descriptor de fișier*. O *adresă de socket* conține tripletul: <protocol, adresa _locală, proces _local>

Tipurile de interfețe socket:

- *tipul stream*: serviciu orientat pe conexiune - oferă un canal de comunicație bidirecțional, secvențial și sigur; mesajele transmise ajung sigur la destinație;
- *tipul datagram*: serviciu fără conexiune - asigură tot un canal bidirecțional, nu se garantează recepționarea mesajelor transmise;
- *tipul raw*: serviciu de acces direct la protocoalele de nivel inferior
- Apeluri socket de bază:
 - socket(): crearea unui socket
 - bind(): se asociază unui socket o adresă
 - listen(): socketul este gata să asculte cererile de conectare
 - accept(): serverul poate accepta cererile care sosesc

Nivelul rețea este responsabil cu transferul transparent al datelor între entitățile nivelurilor transport ale celor două stații care comunică. Serviciile nivelului rețea au fost proiectate în așa fel încât:

- să fie independente de tehnologia subrețelei;

- nivelul transport trebuie să fie independent de numărul, tipul și topologia subrețelelor existente;
- adresele de rețea accesibile prin nivelul transport trebuie să folosească o schemă de numerotare uniformă (atât în rețele LAN, cât și cele WAN).

Principalele funcții ale nivelului rețea:

- **Interconectarea rețelelor;**
- **Dirijarea pachetelor** de la mașina sursă către mașina destinație;
- **Controlul congestiei** – într-o subrețea apare fenomenul de congestie când numărul pachetelor emise depășește capacitatea de transport. La un trafic intens performanțele se deteriorează și este posibil ca, la un moment dat, pachetele să nu mai ajungă la destinație.

Nivelul Legătura de date Rolul nivelului legătura de date. Principalele funcții realizate: sincronizarea emitorului și receptorului; controlul fluxului de date; detectarea și recuperarea erorilor între două puncte ale legăturii; menținerea unor condiții pe legătură, astfel încât să se diferențieze cadrele de date de cele de control și să se identifice stațiile care comunică.

2. Tipuri de protocoale Protocoalele nivelului legătura de date pot fi:

- *asincrone* (nu necesită sincronizare între emitor și receptor): un bloc de informație, compus dintr-un singur caracter, este încadrat de cifre binare pentru delimitare;
- *sincrone* – folosește o configurație de cifre binare pentru delimitarea blocului de informație (orientate pe caracter, bloc sau bit) .

Protocoale ale nivelului legătura de date în Internet

Pentru transmisia și recepționarea datelor în mod serial, prin linia telefonică, se pot utiliza protocoalele de comunicație ale nivelului legătura de date:

SLIP (Serial Line IP)

PPP (Point-to-Point Protocol).

SLIP a fost primul protocol utilizat, fiind conceput pt conectarea la stațiile de lucru Sun la Internet prin intermediul unui canal comutat. SLIP este în momentul de față un *standard de facto*, utilizat pt interconectarea stațiilor izolate prin TCP/IP și o linie telefonică. Cu toate că nu este standard Internet, el este documentat prin RFC.

Protocolul definește un mecanism simplu pt realizarea cadrelor, utilizând o secvență de caractere ce încadrează pachetele IP pe o linie serială.

PPP include trei componente:

- Metoda pentru **încapsularea datagramelor** pe o linie serială;
- **Protocolul de control al legăturii, LCP (Link Control Protocol)**, care furnizează informații de control referitoare la legătura serie LCP. Sunt realizate următoarele faze:
 - stabilirea conexiunii și negocierea parametrilor de configurare, prin schimbarea unor pachete de control;
 - verificarea calității legăturilor, opțional;
 - autentificarea (opțional) reprezintă procesul prin care se verifică dacă un calculator are drepturile necesare să comunice cu un altul;
 - configurarea protocolului nivelului rețea negociat (în această fază este utilizat NCP);
 - închiderea conexiunii.

Fibra optică are capacitatea să transmită semnalele binare sub forma unor impulsuri luminoase.

Fibra multimod: razele generate de sursă pot urma prin fibră trasee de lungimi diferite; numărul de moduri de propagare depinde de indicii de refracție n_1 și n_2 , lungimea de undă a sursei și diametrul nucleului (diametrul nucleului și al învelișului sunt de ordinul 50 μm și respectiv 100 μm (fibră 50/100)).

Fibra monomod: razele generate de sursă se propagă de-a lungul axului fibrei; diametrul nucleului unei fibre optice cu salt de indice scade foarte mult, tipic 10 µm.

Legătura optică este constituită din:

- *sursa de lumină*, dioda electroluminiscentă (LED: Light Emitting Diode) sau dioda laser;
- *fibra optică*;
- *detectorul de lumină*, care poate fi o fotodiodă de tip PIN (Positive Intrinsic Negative) sau fototranzistor.

Funcții ale subnivelului MAC:

- Transmisia unui cadru:
 - ☐ acceptă date de la LLC;
 - ☐ realizarea cadrului;
 - ☐ prezintă o serie de biți nivelului fizic pentru a fi transmiși prin suport;
- Recepția cadrelor:
 - ☐ primește o serie de biți ce provin din nivelul fizic;
 - ☐ verificarea cadrelor recepționate;
 - ☐ prezintă nivelului LLC cadrele primite, cu adresa de grup sau cu adresa stației;
 - ☐ elimină cadrele foarte scurte sau nu dețin adresa stației;
 - ☐ extragerea câmpului de date utile din cadrele recepționate.
- Așteaptă înainte de a transmite, dacă suportul este ocupat;
- Așteaptă expirarea timpului inter-cadre înainte de a transmite;
- Oprirea transmisiei, dacă o coliziune este detectată;
- Tentativa de retransmisie după o coliziune, are loc după un interval de timp calculat printr-un algoritm de reluare (backoff);
- Transmiterea caracterelor de avertizare, pentru confirmarea unei coliziuni;

Securitatea datelor;sec electronica

- *Securitatea electronică* este definită ca fiind: politici, recomandări și acțiuni necesare minimizării riscului asociat efectuării tranzacțiilor electronice, risc ce se referă la breșe în sistem, intruziuni sau furt sau orice mijloc, tehnică sau proces utilizat pentru a proteja informațiile unui sistem
- Măsurile de securitate nu garantează eliminarea completă a oricărui risc, dar poate să-l reducă la un nivel acceptabil.
- *Securitatea IT* – se concentrează, în general, pe crearea unei platforme de calcul unde persoane/programe să nu poată desfășura acțiuni pentru care nu au drepturi alocate.
- Asigurarea securității în sistemele informatice este o problemă esențială.
- Uniunea Europeană a dezvoltat reguli pentru comunicații electronice sigure - de exemplu, directiva asupra semnăturii electronice sau legislația cu privire la protecția datelor din comunicațiile electronice.

Criptarea este procesul de transformare a unui mesaj dintr-o formă în care poate fi citit - *text clar*, într-o formă codificată.

- Criptarea, în general, se utilizează pentru:
 - protejarea datelor tranzitate prin rețele împotriva interceptărilor și manipulărilor neautorizate;
 - protejarea datelor stocate pe calculatoare împotriva vizualizărilor și manipulărilor neautorizate;
 - să împiedice și să detecteze modificarea accidentală sau intenționată a datelor;
 - să verifice autenticitatea tranzacțiilor sau documentelor.
- Noțiunea de *cheie* se referă la o informație, de regulă în formă binară, de o anumită lungime, care este folosită împreună cu un algoritm criptografic, pentru criptare și/sau decriptare.

- La criptare, cheia afectează modul în care datele sunt modificate.
- La decriptare, doar cu cheia corectă se pot recupera datele Originale

După modul de utilizare a cheilor, sistemele criptografice sunt:

sisteme criptografice cu chei secrete (simetrice) - cheia secretă (privată) este folosită atât pentru criptare cât și pentru decriptarea mesajelor transmise între părți;

sisteme criptografice cu chei publice (asimetrice) - se utilizează o pereche de chei - *cheia privată* și *cheia publică*; Cheia folosită pentru criptare (de exemplu, cheia publică) este diferită de cheia folosită pentru decriptare (cheia privată).

Firewall este numele generic al unei componente de rețea care controlează traficul între rețeaua de calculatoare a unei organizații și cele externe, prin utilizarea unor politici de securitate.

Principalele funcții ale unui firewall sunt:

- blochează accesul la site-uri particulare din Internet;
- limitează traficul la unele servicii publice ale organizației (se au în vedere adrese IP și porturi);
- interzice anumitor utilizatori accesul la unele servere și servicii;
- monitorizează comunicațiile între rețeaua internă și o rețea externă;
- monitorizează și înregistrează toate comunicațiile între o rețeaua internă și rețelele externe;
- criptează pachete transmise prin rețele VPN.

Firewall-urile pot fi clasificate după:

- nivelul modelului de referință OSI (Open Systems Interconnect) la care operează:

ruter pentru filtrarea pachetelor: acționează la nivel rețea;

inspectarea în funcție de stare ("stateful inspection"): nivel transport;

firewall la nivel de aplicație: nivel aplicație. • modul de implementare.

Tipurile de **firewall la nivel aplicație**:

poartă la nivel de aplicație (application level gateway) sau agent *proxy*

poartă la nivel de circuit (circuit level gateway)- realizează o conexiune controlată (circuit virtual) între un host intern și altul extern

LLC (Logical Link Control). LLC - standard care derivă din HDLC și este utilizat în rețelele locale.

Standardul LLC (IEEE 802.2) definește : protocolul subnivelului LLC, comun standardelor IEEE 802.3, 802.4, 802.5 etc.; interfața cu nivelul rețea; interfața cu subnivelul MAC (Medium Access Control).

Standardul IEEE 802.2 prezintă nivelului rețea următoarele tipuri de servicii :

- serviciu fără conexiune, fără achitare (LLC1);
- serviciu orientat pe conexiune, cu achitare (LLC2);
- serviciu fără conexiune, cu achitare (LLC3).

LLC1 permite transferul de date punct la punct, punct-multipunct sau prin difuzie. LLC1

oferă emisia și recepția cadrelor fără :

- nici o secvențialitate;
- nici o formă de achitare din partea destinatarului (fără a se garanta recepția și fără a înregistra o situație de eșec);
- nici un control al erorilor.

Hardware

-calc:server/client

-echipamente periferice

-placile cu interfața de rețea

-alte echipamente:transceiver, repetor, hub, bridge, comutator(switch), router

Server: calc care are capacitatea sa raspunda oricand cererilor pe care le primeste din partea clientilor. Calc rapid, care detine o mare capacitate de stocare, iar accesul se face printr-o interfata de retea de mare viteza. Pot exista mai multe servere.

Tipuri de servere:

- file servers:stocarea datelor si fisierelor. Fisierul se pastreaza pe calc gazda si aplicatia se executa pe calc client

- alte: tiparire,fax,mail,web,aplicatii, BD, baze de comunicatie etc

Placa de interfata cu retea: realizeaza unele servicii din serviciile de comunicare pentru un calc conectat la o retea. Comunica printr-o conexiune seriala cu retea si printr-o conexiune paralela cu sist de calcul; fiind dotata cu LED-uri care ofera o serie de inform despre starea conexiunii la retea si a placii.

Software

- SO in retea (NOS) coordoneaza activitatile calc dintr-o retea:per-to-peer sau client/server;

Peer-to-peer:

- sunt generate de dimensiuni mici si pretenti prea mari de securitate;

- se bazeaza pe partajarea resurselor g=hard si soft

- este usor de instalat si administrat

- nu necesita servere dedicate

- exemple:AppleShare,Windows for Workgroups

Client/Server:

- so permit concentrarea functiilor si aplicatiilor in unul sau mai multe servere de fis dedicate;

- serv de fisier de in centrul sistemului, oferind accesul la resurse in concordanta cu politica de securitate;

- exemple:Novell Netware si Windows 2000 Server