Nivelurile OSI (Open Systems Interconnection)

Nivelul fizic se ocupã de transmiterea biþilor printr-un canal de comunicaþie. Proiectarea trebuie sã garanteze cã atunci când unul din capete trimite un bit 1, acesta e receptat în cealaltã parte ca un bit 1, nu ca un bit 0. Problemele tipice se referã la câþi volþi trebuie utilizaþi pentru a reprezenta un 1 ºi câþi pentru un 0, dacã transmisia poate avea loc simultan în ambele sensuri, cum este stabilitã conexiunea iniþialã ºi cum este întreruptã când au terminat de comunicat ambele pãrþi, câþi pini are conectorul de reþea ºi la ce foloseºte fiecare pin. Aceste aspecte de proiectare au o legãturã strânsã cu interfeþele mecanice, electrice, funcþionale ºi procedurale, ca ºi cu mediul de transmisie situat sub nivelul fizic.

Nivelul legaturii de date trateaza erorile de transmisie produse la nivelul fizic, realizand o comunicare corecta intre doua noduri adiacente. Mecanismul utilizat in acest scop este impartirea sirului de biti in cadre, carora le sunt adaugate informatii de control (coduri de verificare, numere de secventa etc). Cadrele sunt transmise individual putand fi verificate si confirmate de catre receptor. Alte functii ale nivelului se refera la: controlul fluxului datelor (astfel incat transmitatorul sa nu furnizeze date mai rapid decat le poate accepta receptorul) si gestiunea legaturii (stabilirea legaturii, controlul schimbului de date si desfiintarea legaturii).

Nivelul retea asigura dirijarea unitatilor de date intre nodurile sursa si destinatar, trecand eventual prin noduri intermediare. Decizia este luata astfel incat sa nu existe in acelasi timp legaturi suprain-carcate si legaturi neutilizate, evitandu-se deci congestionarea retelei. O alta functie importanta a nivelului retea este cea de interconectare a retelelor cu arhitecturi diferite.

Nivelul transport realizeaza o comunicare sigura intre doua calculatoare gazda, detectand si corectand erorile pe care nivelul retea nu le trateaza. El este important nu numai prin pozitia pe care o ocupa, la mijlocul ierarhiei de nivele, dar si prin functia sa, de a furniza nivelelor superioare o interfata independenta de tipul retelei utilizate. Functiile sunt realizate de entitati situate in sistemele gazda, fara concursul altor entitati similare intermediare, motiv pentru care se numesc functii "capat la capat" (capetele fiind cele doua entitati de transport corespondente).

Nivelul sesiune ofera toate serviciile pentru gestiunea jetoanelor, lasand la latitudinea utilizatorilor semnificatiile asociate acestora. Ele au la baza utilizarea unui mesaj special, numit jeton (token), care poate fi trecut de la un utilizator la altul si a carui posesie ofera detinatorului anumite privilegii: de a transmite date, de a stabili puncte de sincronizare, de a stabili inceputul unei activitati etc.

Nivelul prezentare realizeaza transformari ale reprezentarii datelor, astfel incat sa se pastreze semnificatia lor, rezolvandu-se totodata diferentele de sintaxa. Functiile principale se refera la codificarea standard a datelor transmise intre calculatoare cu conventii de reprezentare diferite, la comprimarea textelor, precum si la criptarea/decriptarea acestora in vederea protectiei si securitatii lor.

Nivelul aplicatie, cel mai inalt nivel al arhitecturii, are rolul de fereastra de comunicare prin care se fac toate schimburile de date intre utilizatori. Fiind nivelul care furnizeaza servicii direct aplicatiilor, el cuprinde toate functiile pe care acestea le pot solicita: - identificarea utilizatorilor cooperanti, autentificarea lor si determinarea disponibilitatii acestora, - stabilirea calitatii servici-ului, - sincronizarea aplicatiilor cooperante si selectarea modului de dialog, - stabilirea responsabilitatilor pentru tratarea erorilor, - identificarea constrangerilor asupra sintaxei datelor, - transferul informatiei.

NAT

a) Ce este NAT?
b) Cum functioneaza NAT?
c) apreciati daca este un protocol eficient
d) descrieti functionarea la trimiterea si apoi receptionarea unui pachet
Rezolvare: a)NAT(Network Adress Translation) este un protocol care face translatarea din adrese locale in adrese globale.
c) Nat e efficient deoarece acest mod permite un trafic/traseu mai optim într-o rețea interna și permite accesul la mai multe porturi.
d)NAT foloseste adresa IP si numar port transmitator alaturi de tabela de translatare.
La transmisie: -inlocuieste adresa ip locala cu una globala
-memoreaza corespondenta si nr port
-inlocuieste in tabela de translatare numar port cu index
-recalculeaza sumele de control pentru ip si tcp
La primire: -obtine numar port din pachet(index din tabela de translatare)
-extrage adresa ip si numar port
-inlocuieste adresa ip si numar port
-recalculeaza sumele de control pentru ip si tcp

IPV4

2.a)Enumerati deficientele protocolului IPV4
b)precizati cum rezolva IPV6 deficientele IPV4
c)descrieti modul in care decurge fragmentarea in IPV4 si IPV6
d)descrieti relatia intre protocoalele IPV4 si ICMP,prezicand la ce se foloseste ICMP
-----Rezolvare-----
2.a)Adrese insuficiente pentru a face fata cresterii numarului de dispozitive cu acces la INternet,antet complicat,
nu suporta pachete de dimensiuni mari,are suport redus pentru IPsec si multicast.
b)IPV6 rezolva problemele versiunii IPV4 deorecere are:Spatriu de adrese mult mai mare.suport simplificat pentru
multicast,suport pentru IPsec,antet eficient,Jumbograme adica pachete de pana la 4GB.
c)La IPV4,când un pachet este prea mare pentru urmatoarea legatura peste care va trece, poate fi fragmentat de expeditor
(gazda sau ruter).
Pentru IPv6, fragmentarea poate avea loc numai la nodul sursa, iar reasamblarea este facuta doar la nodul destinatie.
Este folosit antetul extensiei de fragmentare.
d)Protocolul ICMP(internet control message protocol) este utilizat in identificarea erorilor aparute in retele.
ICMP foloseste IPV4 pentru transmisie ,iar IPV4 foloseste ICMP pentru raportarea de erori.

DNS

3.1a)Modul de organizare DNS
b)Prezentati redundanta serverelor DNS si replicarea informatiilor DNS
c)Cum se poate face securizarea DNS
REZOLVARE: a)DNS face traducerea dintre nume simbolice si adrese ip.
Pentru a stabili corespndenta dintre un nume si o adresa ip,programul de aplicatie apeleaza o procedura de biblioteca numita
resolver,transferandu-i numele ca parametru.
Resolverul trimite un pachet UDP la serverul DNS local,care cauta numele si returneaza adresa IP catre rezolver,care o returneaza apelantului.
b)Redundanta serverelor DNS:
Roluri:
Primar:Pe el se fac toate modificarile inregistrarilor. Colecteaza informatii despre una sau mai multe zone aflate in sistemul de fisiere. Raspunde intrebarilor resolverelor
Secundar:Preia modificarile de la alte servere. Asigura redundanta.Master files(sursa aplicarii):Fisiere text care contin inregistrari de resurse.
c)Serviciului poate fi cu usurinta gresit configurat astfel încât sa el devine fara voie un serviciu DNS de tip openresolver. Solutia este un fi?ier de configurare a serviciului DNS (folosind BIND), ce poate fi utilizat de oricine doreste sa securizeze serviciul de DNS oferit utilizatorilor sai.
a) Organizare DNS
b)RR la DNS
a) Sistemul de nume DNS are o organizare ierarhică, sub formă de arbore. Acesta are o rădăcină unică (root) care are subdomenii. Fiecare nod al arborelui reprezintă un nume de domeniu sau subdomeniu.
b)Una dintre componentele DNS este reprezentata de Înregistrări de resurse (RR - resource records)- Baza de date DNS conţine înregistrări de resurse. Aceste înregistrări provin din mapările între nume şi obiecte din reţea.

Dirijarea pachetelor

Descrieti rolul dirijarii si precizati cand si cum efectiv revine in practica. Dirijarea pachetelor de la masina sursa catre destinatie este functia principal a nivelului retea. Dirijarea este foarte importanta in special atunci cand destinatia si sursa nu sunt in aceeasi retea. Algoritmii de dirijare raspund de alegere liniei de iesire pe care un pachet receptionat trebuie trimis mai departe. Daca subreteaua foloseste datagrame,-decizia de dirijare trebuie luata din nou pentru fiecare pachet receptionat,deorece e posibil ca cea mai buna ruta sa se fi modificat in timp. Daca subreteaua foloseste circuite virtuale,decizia se ia doar la stabilirea unui nou circuit virtual.Dupa aceea,pachetele vor urma doar calea stabilita anterior.

Start-stop

b) protocolul start-stop - functionare
c) probleme ce pot aparea la nivelul protocolului si rezolvare
d) avantaje si dezavantaje ale protocolului start-stop
b)+c)Protocolul start-stop.
Presupunem ca avem un protocol in care expeditorul trimite destinatarului pachete de date.Cum destinatarul nu are cum sa isi dea seama daca primul pachet trimis a fostr primit sau nu,acesta continua sa trimita pachete.Protocolul start-stop rezolva problema inundarii destinatarului,deorece acest protocol functioneaza astfel:trimitem un mesaj,cand il primeste trimite un mesaj de confirmare asa ca putem sa trimitem urmatorul pachet.
d)Avantajulprotocolului start-stop este faptul ca e usor de implementat,nu necesita un hardware performat sau conditii speciale.
Dezavantajul este utilizarea lărgimii de bandă care este cu mult sub optim.

TCP

a) Carui nivel apartine TCP, precizati functiile si caracteristicile acestuia.
b) diferenta intre serviciile cu confirmare si cele orientate pe conexiune
c) cum se face conexiunea la TCP
d) controlul fluxului la TCP
e) verificarea segmentelor la TCP
1.a)TCP apartine nivelului transport,nivel ce are ca functie transportarea datelor de la masina sursa la masina destinatie intr-o maniera sigura si eficace d.p.d.v al costurilor. De asemenea,ofera interfata uniforma cu utilizatorii. TCP (Transmission Control Protocol) este cel mai folosit protocol de transport. Adigura livrarea sigura a datelor pe o retea nesigura. Este orientat pe conexiune.Stabileste o conexiune permanent intre client si server.
Realizeaza controlul congestiei,adaptand viteza de transmisie. Are un overhea mare,in comparative cu UDP-ul. Este full-duplex,are confirmare. Protocolul utilizat de TCP este protocolul cu fereastra glisanta. In TCP conexiunile se stabilesc folosindu-se "Three Way Handshake".
b)Diferenta dintre serviciile cu confirmare si cele orientate pe conexiuneAICI subiectul e ciudat,nu e bine scris dar am inteles de la cineva ca s-a dat diferenta intre datagrame si CV Serviciile cu confirmare sunt cele cu datagrame,iar cele orientate pe conexiune ,cu circuite virtuale. Stabilirea circuitului virtual nu e necesara la datagrame,pe cand la circuitele virtuale este obligatorie. Adresare este diferita:la datagrame,fiecare pachet contine adresa complete pentru sursa si destinatie si la circuitele virtuale,fiecare pachet contine un numar mic de circuite virtuale. La datagrame,ruterele nu pastreaza informatii despre conexiuni,pe cand fiecare circuit virtual necesita spatiu pentru tabela ruterului per conexiune. La datagrame,fiecare pachet e dirijat independent,pe cand la CV,calea e stabilita la initierea CV si toate pachetele o urmeaza. Daca ruterul se strica,la datagrame nu are niciun effect decat pachete pierdute in timpul defectari.La CV,toate circuitele care trec prin ruterul defect sunt terminate.
c)Conexiunea TCP se face prin "Three Way Handshake". Serverul asculta ,clientul incearca se se conecteze si trimite primul pachet(SYN). Serverul primeste SYN-ul si raspunde cu SYN-ACK.ACK-ul ajunge la client,clientul trimite ACK(confirmarea de primire) si conexiunea e realizata.
d)Fluxul de date e transmis pe o cinexiune TCP limitat de minimul dintre dimensiunea ferestrei receptorului si capacitatea retelei. Algoritmul de control al congestiei:
-Foloseste un prag(threshold) -La un time-out,pragul e setat la jumatate din fereastra de congestive -Se aplica procedeul de crestere a ferestrei de congestive pana atinge pragul.
-Peste prag se aplica o crestere liniara. SAU(aici nu sunt sigura ca am gasit mai multe,prima e din cursuri,a doua din carte)
Fiecare maşină care suportă TCP dispune de o entitate de transport TCP, fie ca proces utilizator, fie ca parte a nucleului care gestionează fluxurile TCP şi interfeţele către nivelul IP. O entitate TCP acceptă fluxuri de date utilizator de la procesele locale, le împarte în fragmente care nu depăşesc 64K octeţi (de regulă în fragmente de aproximativ 1500 de octeţi) şi expediază fiecare fragment ca o datagramă IP separată. Atunci când datagramele IP conţinând informaţie TCP sosesc la o maşină, ele sunt furnizate entităţii TCP, care reconstruieşte fluxul original de octeţi.
e) Există două limite care restricţionează dimensiunea unui segment. în primul rând, fiecare segment, inclusiv antetul TCP, trebuie să încapă în cei 65.535 de octeţi de informaţie
utilă IP. în al doilea rând, fiecare reţea are o unitate maximă de transfer sau MTU (Maximum
Transfer Unit), deci fiecare segment trebuie să încapă în acest MTU. în realitate, MTU este în
general de câteva mii de octeţi, definind astfel o limită superioară a dimensiunii unui segment. Dacă un segment parcurge o secvenţă de reţele fără a fi fragmentat şi ajunge apoi la o reţea ai cărui MTU este mai mică decât dimensiunea segmentului, ruterul de la frontiera acelei reţele fragmentează segmentul în două sau mai multe segmente mai mici.
a)TCP
b)ce este un socket
c) IP, port
a)TCP(Transmission control protocol) este cel mai folosit protocol de transport.
Ofera livrare sigura a datelor pe o retea nesigura(datagrame).
Stablieste o conexiune intre client si server.
Realizeaza controlul congestiei,adaptand viteza de transmisie.
Este full duplex,are confirmare.
Protocolul de baza utilizat de TCP este protocolul cu fereastra glisanta.
In TCP conexiuni;e sunt stabilite utilizand "Three Way Handshake".
b)Socketul este punctual in care procesul de aplicatie se leaga la retea.

Servicii transport neorientate vs servicii de confirmare

Serviciile de transport neorientate:
Serverul:deschide un socket(socket)->asculta la o adresa->primeste/trimite mesaje->inchide trimitere/primirea/inchide socketul
Clientul:Creaza un socket,trimite/primeste,se opreste din trimitere/primire,inchide socketul
Servicii de transport de confirmare:
Serverul:Creaza socket,asculta la o adresa,Stab nr maxim de cereri pe care le poate avea(listen),
accepta,repetat,cate o cerere-accept,repetat-primeste date recv
Clientul:creaza socket,se conecteaza la server,trimite date,elibereaza resursele conexiunii,informeaza serverul despre inchiderea conexiunii.

Detectia si corectura erorilor + checksum (sume de control)

a) detectia si corectarea erorilor
b) la ce folosesc sumele de control si confirmarile.
a) Corectarea erorilor este mai complexă decât detectarea lor.
Detectia erorilor utilizează sindromul, o combinatie liniară a simbolurilor cuvântului de cod,pe cand corectarea erorilor necesită aflarea zerourilor unor polinoame cu coeficienti functii rationale de componentele sindromului
b) Suma de control(Checksum) este folosita pentru detectarea eorilor de transmisie.
Un pachet este trimis de la transmitator avand o anumita suma de control.-Daca la receptie,suma de control a pachetului este alta decat cea initiala inseamna ca pachetul a fost modificat,daca suma este aceeasi inseamna ca datele din pachet sunt corecte. Confirmarile reprezinta o solutie pentru a preveni inundarea receptorului de catre transmitator. Presupunem ca avem un canal fara erori,canal pe care se trimit pachete cce contin anumite date. Transmitatorul trimite pachet dupa pachet,nesttind daca receptorul ii poate face fata . Viteza cu care se trimit pachetele trebuie sa fie mai mica sau cel putin egala cu viteza cu care se primesc. Astfel,folosim confirmarile.Transmitatorul trimite un pachet,receptorul il primeste si trimite un cadru de confirmare.Transmitatorul primeste cadrul de confirmare si doar atunci poate trimite urmatorul pachet.
b)confirmari
c)diferenta intre detectarea erorilor si corectarea erorilor
b)Confirmarile reprezinta o solutie pentru a preveni inundarea receptorului de catre transmitator. Presupunem ca avem un canal fara erori,canal pe care se trimit pachete cce contin anumite date. Transmitatorul trimite pachet dupa pachet,nesttind daca receptorul ii poate face fata . Viteza cu care se trimit pachetele trebuie sa fie mai mica sau cel putin egala cu viteza cu care se primesc. Astfel,folosim confirmarile.Transmitatorul trimite un pachet,receptorul il primeste si trimite un cadru de confirmare.Transmitatorul primeste cadrul de confirmare si doar atunci poate trimite urmatorul pachet.
c) Corectarea erorilor este mai complexă decât detectarea lor. Detectia erorilor utilizează sindromul, o combinatie liniară a simbolurilor cuvântului de cod,pe cand corectarea erorilor necesită aflarea zerourilor unor polinoame cu coeficienti functii rationale de componentele sindromului.

SMTP

a) Ce este SMTP?
b) Cum functioneaza modelul client server - cereri & raspunsuri
c) Comparatie cu metodele oferite de POP3
a)SMTP(simple mail transfer protocol) este protocolul standard de aplicatie pentru livrarea mesajelor de posta electronica de la sursa la destinatie.O alta functie a smtp-ului este verificarea adreselor de email.
b) Inițial clientul stabilește conexiunea către server și așteaptă ca serverul să-i răspundă cu mesajul "220 Service Ready" . Dacă serverul e supraîncărcat, poate să întarzie cu trimiterea acestui raspuns. Dupa primirea mesajului cu codul 220 , clientul trimite comanda HELO prin care isi va indica identitatea. Odată ce comunicarea a fost stabilită, clientul poate trimite unul sau mai multe mesaje, poate incheia conexiunea sau poate folosi unele servicii precum verificarea adreselor de e-mail. Serverul trebuie să raspundă după fiecare comandă indicand astfel dacă aceasta a fost acceptată, dacă se mai asteaptă comenzi sau dacă există erori în scrierea acestor comenzi. Comenzi:-MAIL,RCPT,DATA,QUIT. Raspunsuri:Numar(cod) din 3 cifre urmat de text.
c) Există mai multe metode diferite de autentificare disponibile:
Metoda de text simplu. Cel mai simplu este să utilizați parola text simplu atunci când utilizatorul trimite la server SMTP , numele și parola, înainte de a trimite mesajul. Principalul dezavantaj al metodei text simplu este că acesta nu este suficient de sigura.
Cineva, luand pachete de pe fir,ar putea descoperi parola. Totuși, această problemă poate fi evitată prin utilizarea unei conexiuni criptate.
-POP înainte de SMTP-.
Această metodă de autentificare necesită utilizatorului să verifice contul lui / ei de e-mail POP3 (de obicei, de asemenea, folosind parola de text simplu), înainte de a li se permite să trimita un e-mail.
La primaetapa, serverul de mail înregistrează adresa IP de intrare a cererii POP3 și apoi, în a doua etapă, permite temporar trimiterea de emailuri de la această adresă IP. Cu toate acestea, e-mail nedorit încă ar putea fi trimis în cazul în care adresa IP, care este autorizata de către serverul
POP-înainte-SMTP este împărțită între mai mulți utilizatori și computere.

Fereastra glisanta

Cand soseste un cadru cu date,in locul emiterii imediate a unui cadru de confirmare,receptorul sta si asteapta urmatorul pachet.Confirmarea e transportata pe gratis de catre urmatorul cadru.
Tehnica intarzierii confirmarii,astfel incat sa fie agatata de urmatorul cadru de date,se numeste piggybacking.
Avantaj,la acest tip de protocol,este faptul ca lungimea de banda este folosita mai eficient. separat. Dezavantajul este ca nu stim cat timp trebuie sa astepte nivelul legatura,pachetul pe care sa ataseze confirmarea.
Solutia dezavantajului este asteptarea pentru un numar fixat de milisecunde. Daca un pachet soseste mai repede,confirmarea este adaugata in el.
Daca pana la sfarsitul perioadei de timp nu a aparut un nou pachet,se trimite un cadru de confirmare

HTTP

b) sa descriem o sesiune ce face clientul, serverul (cum functioneaza comunicatia HTTP)
c)la ce foloseste antetul autentificare din HTTP
b)Clientul e browserul. Browserul determina URL-ul cerut si cere DNS-ului adresa ip pentru URL-ul respectiv. DNS-ul raspunde. Browserul deschide o conexiune TCP la port 80 pe ip-ul dat si trimite o comanda GET. Serverul trimite fisierul si conexiunea TCP e inchisa. Browserul afiseaza continutul paginii si afiseaza toata imaginile din fisier.Pentru fiecare imagine e deschisa o noua conexiune.
c)Antetul autentificare din HTTP este o modalitate de a securiza HTTP-ul. Serverul verifica credentialele de autorizare si satisfice cererea sau refuza.
b) care este formatul general al unui URL si daca este valid url-ul http://cs.-pub.ro/~pc2013
d) cum se poate securiza HTTP
b)Format general:
protocol://nume_adresa_ip[:port]/cale/…../[;url_parametrii][?query_string][anchor]
URL-ul http://cs.pub.ro/~pc2013 cred ca este valid deorece respecta formatul general.Acest URL ne trimite pe serverul ce gazduieste platform cs.pub.ro,intr-o pagina ~pc2013,pagina ce poate contine la randul ei mai multe pagini sau directoare.
d) Solutia este un fisier de configurare a serviciului DNS (folosind BIND), ce poate fi utilizat de oricine doreste sa securizeze serviciul de DNS oferit utilizatorilor sai
a)Rolul si caracteristici HTTP
b)descrieti structura cererilor si raspunsurilor HTTP
c)descrieti headere-le pentru autorizare si autentificare
a)HTPP(HyperText Transfer Protocol) este un protocol pentru transferul mesajelor specializate prin retea. Este un protocol stateless,adica trateaza cererile individual. Foloseste paradigma request-response. Clientul comunica direct sau prin proxyuri.
b)Structura de mesaje(cere/raspuns):
1.Linia de comanda/raspuns. 2.Linia de antet. 3.Corp mesaj
c)Header-le pentru autorizare si autentificare Autorizare de baza:Prin antet de autorizare,nume si parola criptat trimise(base64)
Secvente de actiuni:-Cere sursa restrictionata
-Serverul raspunde cu 401
-Navigatorul retrimite cererea cu antet sumplimentar de autorizare
-Serverul verifica credentialele de autorizare si satisface cererea sau refuza cu cod 403
-Navigatorul foloseste credentiale si in viitoarele cereri la URL dependente.

HTML

a) de ce sunt utile paginile dinamice HTML
b) cum functioneaza comunicatia intre browser si serverul web in contextul cgi
c) cum functioneaza comunicarea intre server web si programul cgi
d) dati exemplu de alternativa moderna la cgi
e) ce este mvc
a)Paginile de Web dinamice sunt utile pentru ca:
-permit interactiunea intre pagini -serverul furnizeaza pagina si adauga in aceasta continut generat in mod dinamic -iti permite personificarea paginii(de exemplu,cand te loghezi undeva,sau pee mag cand faci cumparaturi si ai COSUL TAU,tine minte de ce ai adaugat in cos) -sunt flexibile -poti manevra usor continutul acestora.
b)Browserul va cere URL-ul de la server. Serverul receptioneaza cerea,seziseaza ca URL-ul specifica un script si apoi executa scriptul. Scriptul efectueaza operatiile cerute pe baza datelor furnizate de browser. Scriptul transforma rezultatul intr-un format inteles si de serverul web. Serverul web preia rezultatul si il trimite browserului care-l formateaza si afiseaza.
c)Cream un process pentru executia programului CGI(SPAWN)
Paseaza corpul cererii prin intrearea standard imput. Dirijeaza iesirea standard output catre modulul din server care primeste raspunsul. Parseaza raspunsul si adauga antetele implicite(stare,tip,continut,etc)
d)Alternativele modern ale lui CGI sunt:
-NSAPI(NetScape API) -MSAPI(Microsoft Internet Server API)
e)MVC este o arhitectura,iniţiată în Smalltalk, pentru a asocia introducerea datelor, prelucrarea lor şi prezentarea rezultatelor cu modelul de interfaţa grafică utilizator.

OSPF (Open Shortest Path First)

OSPF suportă trei tipuri de conexiuni şi reţele: -Linii punct-la-punct între exact două rutere. - Reţele multiacces cu difuzare (de exemplu, cele mai multe LAN-uri). - Reţele multiacces fără difuzare (de exemplu, cele mai multe WAN-uri cu comutare de pachete). Multe din AS-urile din Internet sunt foarte mari şi nu sunt simplu de administrat. OSPF le permite să fie divizate în zone numerotate, unde o zonă este o reţea sau o mulţime de reţele învecinate. Orice AS are o zonă de coloană vertebrală, numită zona 0. Toate zonele sunt conectate la coloana vertebrală, eventual prin tunele, astfel încât este posibil să se ajungă din orice zonă din AS în orice altă zonă din AS prin intermediul coloanei vertebrale. Un tunel este reprezentat în graf ca un arc şi are un cost.

Dirijarea

.Despre dirijari (clasificari)
Fara tabela de dirijare: -inundare -hot potato
Cu tabele de dirijare-criterii:
#Adaptare la conditii de traffic: -Statica -Dinamica
#Locul unde se fac calculele: -Descentralizata -Centralizata -Distribuita
#Criterii de dirijare: -Calea cea mai scurta -Intarzierea medie globala -Folosirea eficienta a resurselor -Echitabilitatea
#Informatii schimbate intre noduri: -Starea legaturii -Vectorul distantelor
#Tipul retelei: -Uniforma -Ierarhica
a) ce este dirijarea si la ce foloseste in practica
b) cum functioneaza algoritmul de dirijare ad-hoc
c) ce structuri de date pastreaza ruterele din cadrul unei retele ad-hoc
d) ce actiuni executa un ruter dintr-o retea ad-hoc la primirea unui mesaj sau a unei confirmari
a)Dirijarea pachetelor de la masina sursa catre destinatie este functia principal a nivelului retea. Dirijarea este foarte importanta in special atunci cand destinatia si sursa nu sunt in aceeasi retea. Algoritmii de dirijare raspund de alegere liniei de iesire pe care un pachet receptionat trebuie trimis mai departe. Daca subreteaua foloseste datagrame,decizia de dirijare trebuie luata din nou pentru fiecare pachet receptionat,deorece e posibil ca cea mai buna ruta sa se fi modificat in timp. Daca subreteaua foloseste circuite virtuale,decizia se ia doar la stabilirea unui nou circuit virtual.Dupa aceea,pachetele vor urma doar calea stabilita anterior.
b)AODV(ad hoc on demand distance vector) determina ruta la cerere. Reteaua ad hoc este un graf. Muchiile sunt conexiunile,nodurile putand comunica direct. Fiecare nod e ruter si gazda. Fiecare nod contine:
-tabela de dirijare(contine destinatie,pas urmator,distanta,numar secventa destinatie) -tabela History(contine identitatile cererilor precedente)
-tabela reverse-route(calea spre sursa unui pachet cerer)
Un nod construieste un pachet de tip ROUTE REQUEST. Când în final pachetul ROUTE REQUEST ajunge la nodul destinaţie, acesta construieşte la rândul lui un nou pachet cu numele ROUTE REPLY si il trimite pe legatura inversa.
c)MATRICI
d) La un mesaj de tip ROUTE REQUEST executa urmatoarele actiuni:
Actiunile depend de tipul mesajului. La un mesaj de tip ROUTE REQUEST executa urmatoarele actiuni:-Verifica duplicat in tabela de History locala
-Transmite Route Reply daca a gasit o noua ruta,atfel:
-Incrementeaza HopCount si redifuseaza Route Request
-Memoreaza informatia in tabela reverse-route.
La un mesaj de tip ROUTE REPLY executa urmatoarele actiuni:
-Actualizeaza tabela de dirijare locala
-Transmite pe legatura inversa
-Trece prin anumite noduri
a) Descrieti rolul dirijarii si precizati cand si cum efectiv revine in practica.
Dirijarea pachetelor de la masina sursa catre destinatie este functia principal a nivelului retea. Dirijarea este foarte importanta in special atunci cand destinatia si sursa nu sunt in aceeasi retea. Algoritmii de dirijare raspund de alegere liniei de iesire pe care un pachet receptionat trebuie trimis mai departe. Daca subreteaua foloseste datagrame,decizia de dirijare trebuie luata din nou pentru fiecare pachet receptionat,deorece e posibil ca cea mai buna ruta sa se fi modificat in timp. Daca subreteaua foloseste circuite virtuale,decizia se ia doar la stabilirea unui nou circuit virtual.Dupa aceea,pachetele vor urma doar calea stabilita anterior.

POP3 (Post Office Protocol Version 3)

POP3 începe când utilizatorul porneşte programul cititor de poştă (mail reader). Acesta sună la ISP (în caz că nu există deja o conexiune) şi stabileşte o conexiune TCP cu agentul de transfer de mesaje, prin portul 110. Odată ce conexiunea a fost stabilită, protocolul POP3 trece succesiv prin următoarele trei stări: 1. Autorizare se referă la admiterea utilizatorului în sistem (login). 2. Tranzacţionare tratează colectarea e-mail-urilor şi marcarea lor pentru ştergere din cutia poştală. 3. Actializare se ocupă cu ştergerea efectivă a mesajelor.

IMAP

MAP prevede mecanisme extinse pentru citirea mesajelor sau chiar a părţilor de mesaje, o facilitate folositoare când se utilizează un modem încet pentru citirea părţii textuale a unui mesaj cu mai multe părţi audio şi video de mari dimensiuni. IMAP asigură mecanisme pentru crearea, distrugerea şi manipularea mai multor cutii poştale pe server. Stilul general al protocolului IMAP este similar cu cel al POP3-ului, cu excepţia faptului că există zeci de comenzi. Serverul IMAP ascultă pe portul 143

POP3 si IMAP

POP3 foloseste potul 110,iar IMAP 143.
La POP3 mailul este stocat in calculatorul userului,iar la IMAP pe server.
La POP3 mailul ecitit offline,pe cand la IMAP e citit online.
Timpul necesar conectarii in cazul POP3 e mic,iar la IMAP este mare.
La POP3 folosirea resurselor serverului este minima,pe cand la IMAP e intense.
POP3 nu are mai multe cutii postale,dar IMAPUL are.
Copiile de siguranta la cutiile postale le face userul in cazul POP3,iar la IMAP ISP-UL.
POP3 nu e bun pt utilizatorii mobile,pe cand IMAP este perfect.
La POP3 utilizatorul are un control mica supra mesajelor preluate,pe cand la IMAP controlul este mare.
POP3 este simplu de implementat ,iar IMAPul nu.