1 Arhitectura de retea

Notiuni:

Organizare pe stiva de nivele. Arhitectura de retea insumeaza multimea de nivele si de protocoale. Stiva de protocoale este lista de protocoale (de pe toate nivelele) utilizate de un anumit sistem.

Serviciu: furnizeaza functionalitatea unui nivel.

Protocol: reguli si conventii prin care se realizeaza comunicarea.

Serviciu!=Protocol.

Tipuri de servicii:

-Orientat-conexiune: comunicarea necesita stabilirea unei conexiuni

-Fara conexiune

Modele de referinta pentru arhitecturi de retea: ISO/OSI, TCP/IP

2 Modelul OSI

Ofera metode generale pentru realizarea comunicatiei/ sistemelor de calcul pentru ca acestea sa poata schimba informatii indiferent de particularitatile constructive ale sistemelor (producator, sistem de operare etc.)

Modelul OSI dispune de 7 niveluri: aplicatie, prezentare, sesiune, transport, retea, legatura de date, fizic.

1. Nivelul fizic

Defineste specificatii electrice, mecanice, procedurale si functionale pentru activarea, mentinerea si dezactivarea legaturilor fizice intre sisteme. Rol: transmiterea unui sir de biti pe un canal de comunicatii. Medii de transmisie: cu/fara fir. Transmiterea datelor: analogic/digital. Conversia datelor din analogic in digital si invers: codec si respectiv modem. Aspecte: largimea de banda, latenta, atenuarea, zgomotul, distorsiunea.

Concluzii: datele pot fi alterate, distruse, pierdute etc.

2. Nivelul legatura de date

Se ocupa cu adresarea fizica, topologia retelei, accesul la retea. Ofera mecanisme de detectie si corectare a erorilor, de reglementare a fluxului de date etc. Furnizeaza un transport sigur, fiabil al datelor de-a lungul unei legaturi fizice. Datele se incapsuleaza in frame-uri. Ofera servicii nivelului de retea (neconfirmate fara conexiune, confirmate fara conexiune, confirmate orientate-conexiune).

Este divizat in doua subniveluri: LLC (logical link control) si MAC (medium access control).

MAC: in caz de coliziune, se retransmit datele pana la succes. Protocoale: ALOHA (pure si slotted), CSMA, MACA, MACAW.

3. Nivelul retea

Rol: determinarea caii optime pentru realizarea transferului de informatii intr-o retea constituita din mai multe segmente, prin fragmentarea si reasamblarea informatiei. Preia pachetele si le transfera catre destinatie. Ofera servicii nivelului de transport. Se compune din pachete (datagrame). Protocoale: IP, X.25.

4. Nivelul transport

Ofera siguranta si cost eficient in transportul datelor de la masina sursa la masina destinatie, independent de reteaua fizica sau de retelele in prezent in uz. Rol: transportul fiabil al informatiei intre doua end points ale unei comunicatii. Furnizeaza controlul erorilor si controlul fluxului de date, asigurand ordinea corecta a pachetelor de date. Primitive: LISTEN, CONNECT, SEND, RECEIVE, DISCONNECT.

5. Nivelul sesiune

Rol: furnizeaza controlul comunicatiei intre aplicatii. Stabileste, mentine, gestioneaza si inchide conexiuni (sesiuni) intre aplicatii.

6. Nivelul prezentare

Se ocupa de prezentarea datelor, codificandu-le intr-un format standard.

7. Nivelul aplicatie

Realizeaza interfata cu utilizatorul si interfata cu aplicatiile. Gestioneaza servicii ale retelei: terminal virtual abstract, transfer de fisiere, posta electronica etc.

3 Modelul TCP

Niveluri: aplicatie, transport, retea (internet), acces la retea. Ofera posibilitatea de a interconecta mai multe tipuri de retele. Are ca axa nivelurile retea si transport.

1. Nivelul acces la retea

Se ocupa cu toate problemele legate de transmiterea efectiva a unui pachet IP pe o legatura fizica, incluzand si aspectele legate de tehnologii si de medii de transmisie, adica nivelurile OSI Legatura de date si Fizic.

2. Nivelul retea

Permite gazdelor sa emita pachete in orice retea; pachetele circula independent pana la destinatie. In stiva TCP/IP, protocolul IP asigura rutarea pachetelor de la o adresa sursa la o adresa destinatie, folosind si unele protocoale aditionale, precum ICMP sau IGMP. Determinarea drumului optim intre cele doua retele se face la acest nivel. Comunicarea la nivelul IP este nesigura, sarcina de corectie a erorilor fiind plasata la nivelurile superioare (de exemplu

prin protocolul TCP). in IPv4 (nu si IPv6), integritatea pachetelor este asigurata de sume de control.

3. Nivelul transport

Este identic cu cel din modelul OSI, ocupandu-se cu probleme legate de siguranta, control al fluxului si corectie de erori. El este proiectat astfel incat sa permita comunicarea intre entitatile pereche: sursa, respectiv, destinatie. In acest sens au fost definite doua protocoale end-to-end: TCP si UDP.

4. Nivelul aplicatie

Nivelul aplicatie se refera la protocoalele de nivel inalt folosite de majoritatea aplicatiilor, precum terminalul virtual (TELNET), transfer de fisiere (FTP) si posta electronica (SMTP). Alte protocoale de nivel aplicatie sunt DNS (sistem de nume de domeniu), NNTP sau HTTP.

4 OSI vs TCP

Asemanari:

-Ambele se bazeaza pe o stiva de protocoale
-Functionalitatile straturilor este oarecum asemanatoare
-Ambele au nivelul aplicatie ca nivel superior
-Se bazeaza (direct sau indirect) pe nivelul transport

Deosebiri:

-ISO/OSI este indicat ca model teoretic; TCP/IP este eficient in implementare -OSI face explicita distinctia intre serviciu, interfata si protocol; TCP/IP nu -ISO/OSI pune la dispozitie protocoale care asigura o comunicare fiabila (detectarea si tratare de erori la fiecare nivel); TCP/IP face verificarea comunicarii la nivelul transport -OSI suporta ambele tipuri de comunicatii la nivel retea (fara conexiune si orientate conexiune); TCP/IP suporta la nivelul retea comunicatii fara conexiune si la nivelul transport ambele moduri

5 Nivelul retea

Rol: ofera servicii neorientate-conexiune pentru a transporta datagrame de la sursala destinatie; sursa si destinatia pot fi in retele diferite. Fiecare datagrama este independenta de celelalte.

6 Protocolul IP

Este un protocol prin care datele sunt trimise de la un calculator la altul prin intermediu Internetului. Mesajul este împărțit în blocuri de mici dimensiuni denumite pachete. Fiecare pachet cuprinde adresa expeditorului și pe cea a destinatarului. Fiecare pachet este trimis, prima dată la un calculator-pasarelă,

care înțelege o mică parte din internet. Calculatorul pasarelă citește destinația pachetelor și trimite pachetele către o altă pasarelă, și așa mai departe, până ce pachetul ajunge la pasarela vecină cu computerul destinatar. Adresa IP este utilizată la nivelul programelor de prelucrare în rețea. În schimb, la nivelul utilizatorilor cu acces la Internet, identificarea calculatoarelor se face printr-un nume de gazdă gestionat de sistemul DNS.

Cum functioneaza?

Nivelul transport preia șiruri de date și le divide în datagrame. Teoretic, datagramele pot avea fiecare până la 64 KO, dar în practică ele nu depășesc 1500 de octeți (pentru a intra într-un cadru Ethernet). Fiecare datagramă este transmisă prin Internet, fiind eventual fragmentată în unități mai mici pe parcurs. Când toate aceste fragmente ajung la mașina destinație ele sunt reasamblate de nivelul rețea în datagrama originală. Datagrama este transparentă nivelului transport, care o inserează în șirul de intrare al procesului receptor. Cea mai mică adresă este 0.0.0.0, iar cea mai mare 255.255.255.255. Adresa IP 0.0.0.0 este folosită de gazde atunci când sunt pornite. Adresele IP cu 0 ca număr de rețea se referă la rețeaua curentă. Aceste adrese permit ca mașinile să acceseze propria rețea fără a cunoaște numărul de rețea (dar trebuie cunoscută clasa rețelei pentru a ști câte zerouri trebuie introduse). Adresele care constau numai din 1-uri permit difuzarea în rețeaua curentă, în mod uzual o rețea locală. Toate adresele de forma 127.xx.yy.zz sunt rezervate pentru testări în buclă locală. Pachetele trimise către această adresă nu sunt trimise prin cablu, ele sunt prelucrate local și tratate ca pachete sosite.

Al doilea element, care este necesar pentru ca TCP/IP să funcționeze, este masca de subrețea. Masca de subrețea este utilizată de protocolul TCP/IP pentru a stabili dacă o gazdă se află pe subrețeaua locală sau într-o rețea la distanță. Masca de rețea este un număr pe 32 biți care separă biții de rețea de biții de stație dintr-o adresă IP. Bitii NetID sunt 1, bitii HostID sunt 0.

7 UDP

Protocol de transport neorientat conexiune, nesigur, minimal. Nu recurge la negocieri sau la confirmari ale primirii datelor. Utilizeaza IP. Pentru a oferi servicii de comunicare intre procese foloseste porturi. UDP transmite pachete: antet (8 bytes) + continut. Utilizari: DNS, RPC, media streaming.

8 TCP

Protocol de transport orientat conexiune, fara pierdere de informatii. Controleaza fluxul de date (stream-oriented). Utilizeaza conexiuni, nu porturi ca abstractiuni fundamentale. Conexiunile se identifica prin perechi reprezentate de adresa IP:PORT. Conexiunile TCP sunt full-duplex. O conexiune TCP este un flux de octeti si nu un flux de mesaje.

Care e ideea?

Fiecare segment trimis contine un numar de secventa (Sequence Number) indicand pozitia octetilor transmisi in cadrul fluxului de date. Receptorul verifica numarul de secventa pentru fiecare segment si răspunde cu un numar de confirmare (acknowledgement number) specificand numarul de secventa al urmatorului octet care se astepta a fi receptionat de fiecare data când primește un pachet de date. Expeditorul păstrează o copie a fiecarui pachet trimis, și așteaptă confirmarea înainte de a trimite pachetul următor. Expeditorul păstrează, de asemenea, și un timer, atunci când pachetul a fost trimis, și va relua retransmiterea pachetului în cazul în care timer-ul expira iar confirmarea recepției întârzie sa apară. Contorul de timp este necesar în cazul în care un pachet se pierde sau este deteriorat.

(Fun fact) În timp ce IP-ul se ocupa doar de livrarea efectiva a datelor, TCP-ul are grija ca un mesaj sa fie împărțit în unități individuale de date, numite segmente, și sa tina evidenta segmentelor transmise, pentru dirijarea eficientă prin intermediul rețelei. De exemplu, când un fișier HTML este trimis de la un server web, stratul software TCP de pe acel server împarte secvența de octeți al acelui fișier, în segmente și le transmite în mod individual către stratul software IP (Nivelul Internet). Nivelul Internet încapsulează fiecare segment TCP într-un pachet IP prin adăugarea unui antet, care include (printre alte date) adresa IP destinație. Chiar dacă fiecare pachet are aceeași adresă de destinație, acestea pot fi rutate pe căi diferite prin intermediul rețelei. În cazul în care programul client pe computerul destinație le primește, stratul TCP (Nivelul Transport) reasamblează segmentele individuale asigurându-se totodată de ordonarea corecta și fără erori a acestora, înainte de a fi livrate către nivelul aplicație.

9 UDP vs TCP

TCP este folosit pe scară largă de multe de aplicații de Internet cele mai populare, inclusiv a World Wide Web (WWW), E-mail, File Transfer Protocol (FTP), Secure Shell, de tip peer-to-peer file sharing, precum și unele aplicații media de streaming. TCP este optimizat, mai degrabă, pentru livrarea exacta decât livrarea la timp a datelor, și prin urmare, TCP înregistrează uneori, întârzieri relativ mari de timp (de ordinul secundelor), în timpul de așteptare pentru unele mesaje ce sosesc în alta ordine sau pentru retransmisia de mesaje pierdute. Acesta nu este deosebit de potrivit pentru aplicații în timp real, cum ar fi Voice over IP. Pentru acest gen de aplicații, sunt recomandate protocoale cum ar fi Real-Time Transport Protocol (RTP), ce rulează peste UDP.

Concluzii: UDP ofera servicii minimale de transport (efort minim de transmisie). TCP ofera servicii orientate-conexiune, fullduplex, sigure – pentru transportul fluxurilor de octeti (mecanism complex de transmisie).

10 Socket-uri

Facilitate generala, independenta de arhitectura hardware, de protocol si de tipul de transmisiune a datelor, pentru comunicare intre procese aflate pe masini diferite, in retea. Ofera suport pentru familii multiple de protocoale. Abstractiune a unui end-point la nivelul transport.

11 DNS

DNS este un sistem distribuit de păstrare și interogare a unor date arbitrare într-o structură ierarhică. Cea mai cunoscută aplicație a DNS este gestionarea domeniilor în Internet.

Caracteristici:

-folosește o structură ierarhizată;

-deleagă autoritatea pentru nume;

-baza de date cu numele și adresele IP este distribuită.

Fiecare implementare TCP/IP conține o rutină software (name resolver) specializată în interogarea serverului de nume (DNS) în vederea obținerii translatării nume/adresă IP sau invers.

Există 2 tipuri de rezoluție de nume:

-rezoluție recursivă (name resolverul cere serverului de nume să facă translatarea);

-rezoluție iterativă (name resolverul cere serverului de nume să îi furnizeze adresa IP a unui server care poate face translatarea).

12 Protocolul DNS

REDIRECTORUL: La un calculator conectat la o rețea se pot executa atât aplicații care necesită numai resursele sistemului respectiv (programe de calcul tabelar, programe de procesare de texte etc.), cât și aplicații care accesează resursele rețelei (browsere de navigare în internet etc.). Nivelul aplicație este cel care permite accesul aplicațiilor la mediul de rețea. Într-o rețea LAN, redirectorul este protocolul care lucrează la nivelul sistemului de operare al calculatorului și permite să se facă distincție între cererile adresate unității centrale a calculatorului respectiv și cele adresate unui server. Redirectorul permite administratorului de rețea să atribuie nume logice resurselor aflate pe diverse unități, iar utilizatorul, pentru a accesa o anumită resursă, va utiliza numai acești identificatori, fără nici o referință la rețeaua respectivă. Astfel, redirectoarele extind componentele software locale. Astfel, este posibilă utilizarea în comun a resurselor logice și fizice ale rețelei, precum și integrarea aplicațiilor locale cu cele de rețea. Fiecare “site” de pe Internet are alocată o adresă IP. Folosirea de către utilizatorii obișnuiți a acestor adrese este dificilă și poate genera erori. Astfel, este necesar un protocol care să facă corespondența dintre numele diverselor componente de rețea și adresele lor IP. Această problemă este rezolvată de către protocolul DNS.

DOMENIUL: este un grup de calculatoare care sunt asociate prin localizarea lor geografică sau prin tipul de activitate al organizației pe care o deservesc. Numele de domeniu este un șir de caractere și/sau numere, de obicei un nume sau prescurtarea unui nume.

IERARHIA DE DOMENIU: DNS implementează un spațiu ierarhizat de nume pentru obiectele din Internet. Spre deosebire de numele de fișiere (calea către acestea), care sunt prelucrate de la dreapta la stânga, fiind separate de slash-uri, numele DNS sunt prelucrate de la stânga la dreapta, separatorul fiind caracterul [.] . Asemănător ierarhiei de fișiere, ierarhia DNS poate fi văzută ca un arbore.

SERVERE DE NUME: Primul pas în organizarea acestor servere este partiționarea ierarhiei în zone. Fiecare zonă poate fi gândită ca fiind corespondentă la o anumită autoritate administrativă, responsabilă pentru acea porțiune a ierarhiei.

13 Nivelul aplicatie

Nivelul aplicaţie stabileşte disponibilitatea unui calculator cu care se doreşte iniţierea unei conexiuni, stabileşte procedurile ce vor fi urmate în cazul unor erori şi verifică integritatea datelor. Nivelul aplicaţie conţine o varietate de protocoale frecvent utilizate: SMTP, POP, TFTP, FTP, HTTP.

14 SMTP

Simple mail transfer protocol este un protocol simplu din suită de protocoale de Internet, care este folosit la transmiterea mesajelor în format electronic în rețea de calculatoare. Protocolul SMTP specifică modul în care mesajele de poștă electronică sunt transferate între procese SMTP aflate pe sisteme diferite. Procesul SMTP care are de transmis un mesaj este numit client SMTP iar procesul SMTP care primește mesajul este serverul SMTP. Protocolul nu se referă la modul în care mesajul ce trebuie transmis este trecut de la utilizator către clientul SMTP, sau cum mesajul recepționat de serverul SMTP este livrat utilizatorului destinatar și nici cum este memorat mesajul sau de câte ori clientul SMTP încearcă să transmită mesajul. Comunicarea intre client și server se realizeaza prin texte ASCII. 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 trimirea acestui raspuns. Dupa primirea mesajului cu codul 220 , clientul trimite comanda HELO prin care isi va indica identitatea. Pentru a trimite un mesaj se foloseste comanda MAIL prin care se specifica adresa clientului. Dacă aceasta comanda este corecta serverul va raspunde cu mesajul [250 OK]. Clientul trimite apoi o serie de comenzi RCPT prin care specifică destinatarii mesajului. Serverul va raspunde cu [550 No such user here], sau [250 OK], in functie de corectitudinea comenzii primite. După ce se specifică destinatarii, și serverul acceptă comenzile, se trimite comanda DATA, prin care serverul e anunțat că expeditorul va incepe sa scrie conținutul

mesajului. Serverul poate răspunde cu mesajul [503 Command out of sequence] sau [554 No valid recipients] dacă nu a primit comenzile MAIL sau RCPT sau aceste comenzi nu au fost acceptate. Dacă serverul va raspunde cu mesajul [354 Start mail input], clientul va putea introduce textul mesajului.

15 POP

Utilizat la transferul de mesaje de pe un server de posta la un MUA – portul 110

16 TFTP

Folosit la transferul de fisiere - sigur si eficient. Utilizeaza UDP si portul 69. Mai multe scheme in curs. Succes.

17 FTP

Uilizat pentru accesul la fișiere aflate pe servere din rețele de calculatoare particulare sau din Internet. FTP utilizeaza doua conexiuni TCP pentru transferul fisierelor: conexiune de control si conexiune de date. Comenzile si raspunsurile sunt linii de text. Pentru interactivitate se foloseste protocolul TELNET.

18 TELNET

Telnet este un protocol de rețea care se folosește în Internet precum și în rețele de calculatoare tip LAN la comunicația textuală, bidirecțională și interactivă, bazată pe realizarea unei conexiuni virtuale cu stația de lucru destinatară. Datele ce urmează a fi transmise celeilalte stații de lucru sunt întâi întrețesute cu informațiile de control ale telnet-ului și apoi transmise împreună cu acestea, folosind nivelul de protocol legătură de date pe 8 biți al protocolului TCP.

19 HTTP

Este metoda cea mai des utilizată pentru accesarea informațiilor în Internet care sunt păstrate pe servere World Wide Web (WWW). HTTP oferă o tehnică de comunicare prin care paginile web se pot transmite de la un computer aflat la distanță spre propriul computer. Dacă se apelează un link sau o adresă de web cum ar fi http://www.example.com, atunci se cere calculatorului host să afișeze o pagină web (index.html sau altele). În prima fază numele (adresa) www.example.com este convertit de protocolul DNS într-o adresă IP. Urmează transferul prin protocolul TCP pe portul standard 80 al serverului HTTP, ca răspuns la cererea HTTP-GET. Informații suplimentare ca de ex. indicații pentru browser, limba dorită ș.a. se pot adăuga în header-ul (antetul) pachetului

HTTP. În urma cererii HTTP-GET urmează din partea serverului răspunsul cu datele cerute, ca de ex.: pagini în (X)HTML, cu fișiere atașate ca imagini, fișiere de stil (CSS), scripturi (Javascript), dar pot fi și pagini generate dinamic (SSI, JSP, PHP și ASP.NET). Dacă dintr-un anumit motiv informațiile nu pot fi transmise, atunci serverul trimite înapoi un mesaj de eroare.

Deseori utilizatorul dorește să transmită informații speciale la website. Aici HTTP pune la dispozitie două posibilități:

-Transferul datelor în combinație cu o cerere pentru o resursă (HTTP-metoda "GET")

-Transferul datelor în combinație cu o cerere specială (HTTP-metoda "POST")

20 Paradigma P2P

Peer-to-peer este o arhitectură de rețea pentru aplicațiile distribuite care împarte sarcinile la mai mulți parteneri. Rețeaua Peer-to-peer permite calculatoarelor să se conecteze în mod direct unul la celălalt, pentru schimb de fișiere (partajare de fișiere) în comun. P2P este arhitectura de retea in care nodurile sunt relativ egale (in sensul ca fiecare nod este, in principiu, capabil sa realizeze functii specifice retelei). Atlfel spus, partenerii sunt participanți egal privilegiați, echipotenți în aplicație. Se spune că o rețea peer-to-peer este formată din mai multe noduri (peers). O rețea Peer-to-peer (P2P) este un tip de rețea în care fiecare computer are drepturi si responsabilități egale. Perechile partajează o parte din resursele lor în mod direct către alte calculatoare aflate în rețea, fără a fi nevoie de un coordonator central cum ar fi un server sau o gazdă stabilă. Perechile sunt atât furnizori cât și consumatori de resurse, în contrast cu tradiționalul sistem client-server unde serverul este furnizor iar clientul este consumator.

Sistemele P2P pure sunt rare (de ex. Gnutella); majoritatea sunt hibride, avand supernoduri sau servere cu diferite roluri (de ex. cautare de date, control, etc.).

Rezulta ca arhitectura P2P are puncte tari, precum: utilizarea eficienta a resurselor, scalabilitate, siguranta, administrare usoara, anonimitate, dinamism. Totusi, exista si unele dezavantaje, cum ar fi: localizare impredictibila a resurselor, resurse volatile, inexistenta unui control centralizat, posibile probleme de securitate, performante scazute in sistemele cu mai multe calculatoare etc.

Tipuri de aplicatii P2P: comunicare+colaborare, calcul distribuit, stocare (baze de date), distribuire de continut digital.

Exista si o clasificare a retelelor P2P (in functie de centralizare):

1. Arhitecturi pur descentralizate: toate nodurile realizeaza exact aceleasi activitati, jucand simultan roluri de servere si clienti, fara a beneficia de o coordonare centrala. Nodurile se numesc SERVENTS

2. Arhitecturi partial centralizate: unele noduri au un rol mai important (de ex. stocand indecsi locali pentru fisierele partajate)

3. Arhitecturi descentralizate hibride: exista un server central facilitand interactiunea intre noduri, mentinand cataloage de meta-date ale fisierelor. Rețelele descentralizate se pot clasifica la rândul lor, în funcție de structura

lor, în rețele nestructurate și rețele structurate. De asemenea există rețelele P2P semantice, rețele anonime și rețele private.

Rezulta o alta clasificare:

1. Nestructurate: plasarea continutului este complet independenta de topologia retelei suprapuse. Într-un sistem peer-to-peer nestructurat, căutările și rezultatele acestora, sunt dirijate într-o conexiune deschisă. Rețelele nestructurate se organizează după cum evoluează evenimentele din cadrul acesteia. La nivelul nodurilor (peers), dacă un utilizator trimite o interogare, nodul acestuia va deveni un nod sursă ce va trimite interogarea tuturor vecinilor săi. Într-un sistem super-peer-to-peer, rețeaua este împărțită în grupuri, fiecare dintre ele conține un nod special, denumit super-nod (super-peer). Toate nodurile de grup sunt conectate la acest super-nod, iar acesta este conectat la alte super-noduri din alte grupuri. Grupul format din super-nod și celelalte noduri membre ale grupului se numește cluster. Dacă legătura din super-nodurile din grupuri diferite se întrerupe, atunci tot clusterul este deconectat unul față de celălalt. Gnutella, Freenet, KaZaA sunt exemple de rețele nestructurate.

2. Slab structurate (loosely structured): desi localizarea continutului nu e complet specificata, aceasta este afectata de dirijare

3. Structurate: topologia este controlata, iar fisierele (sau pointerii la ele) sunt plasate in locatii precise. În cazul sistemelor peer-to-peer structurate, plasarea resurselor și a nodurilor sunt strâns legate de structura rețelei. Topologia rețelei P2P structurată este controlată strict și datele sunt plasate în locații cunoscute, ceea ce eficientizează căutările. Asemenea sisteme structurate P2P utilizeaza distributed has tables pentru localizarea nodurilor și resurselor din aplicația folosită. Această funcție garantează localizarea fișierului sau a nodului.

21 Paradigma RPC

O aplicatie RPC va consta dintr-un client si un server, serverul fiind localizat pe masina pe care se executa procedura. La realizarea unui apel la distanta, parametrii procedurii sunt transferati prin retea catre aplicatia care executa procedura; dupa terminarea executiei procedurii rezultatele sunt transferate prin retea aplicatiei client.

RPC permite programatorului să construiască un program obişnuit pe care poate să-l transforme într-un program distribuit prin mutarea procedurilor pe calculatorul aflat la distanţă (remote). Se minimizează astfel modificările ce trebuie efectuate şi se reduce şansa apariţiei erorilor la adăugarea procedurilor stub la program. Aceste proceduri stub implementează comunicarea şi permit ca procedura apelantă şi cea apelată să rămână nemodificate.

Clientul si serverul vor comunica prin mesaje, printr-o reprezentare independenta de retea si de sistemul de operare: External Data Representation (XDR) - asigura conversia simetrica a datelor client si server.

RPC furnizeaza un punct central pentru aplicatiile server sa obtina porturi TCP/UDP pe masina respectiva pe care ruleaza. Aplicatiile nu trebuie

[legate] pe anumite porturi specificate pentru ca serviciul de port mapping al RPC-ului furnizeaza porturi libere mai mari de 1024 serverelor RPC. Serviciul de lookup folosit pentru asa ceva include PORTMAPPER-UL (PMAP) si RPCBIND *care sunt descrise in RFC 1833. Portmapper are un port fix pe care sta deschis (111) fie TCP, fie UDP. Acest serviciu de lookup trebuie deschis inaintea serverului/clientului si trebuie sa ramana functional pe toata durata executiei aplicatiei RPC.

O problema este introdusa de acest mecanism. Serverele RPC nu utilizeaza porturi rezervate (asa cum sunt cele specificate pentru servicii in fisierul /etc/services); atunci cand pornesc, utilizeaza portul disponibil dat de serviciul portmapper. Atunci cand un program client doreste sa apeleze un anumit serviciu RPC, el nu stie pe ce port ruleaza acesta pentru a face apelul. Trebuie sa existe o metoda de aflare a acestui port. Deamonul portmapper rezolva aceasta problema. Atunci cand un client face un apel RPC, mai intai apeleaza serviciul de portmapper pentru aflarea portului serverului. Un apel RPC este analog cu un apel de functie. Ca la un apel de functie, atunci cand un apel RPC este facut, argumentele de apelare sunt trimise procedurii apelante si procesul apelant asteapta intoarcerea raspunsului de la procedura de la distanta. https://profs.info.uaic.ro/~busaco/publications/articles/rpc.pdf are mai multe detalii despre asta.

22 Rutarea

Este partea software-ului nivelului retea care alege calea pe care un pachet receptionat trebuie trimis pentru a ajunge la destinatie. Deci se refera la procesul de alegere a căii pe care un pachet este transmis de la sursă la destinație sau destinații, chiar și între două rețele diferite. Rutarea este bazată pe o tabelă care are în principal următoarele câmpuri: adresa rețelei (net address), masca de rețea (netmask), adresa următorului rute (next hop) și/sau adresa interfeței de ieșire.

Daca se folosesc datagrame, decizia de rutare trebuie luata pentru fiecare pachet. Daca se utilizeaza circuite virtuale, decizia de rutare se ia la stabilirea unui nou circuit.

Comutare: Un host are de trimis un pachet la un alt host. Host-ul sursa trimite pachetul la un router, folosind MAC-ul acestuia, un pachet continand adresa de retea a gazdei destinatie. Routerul examineaza adresa de retea a destinatarului, iar daca nu cunoaste unde sa trimita pachetul, il va distruge. Altfel, va modifica adresa continuta de pachet in MAC-ul urmatorului hop (Intermediate System) si va trimite pachetul spre acesta. Daca urmatorul hop nu este destinatia finala, atunci procesul se repeta pentru un alt router, s.a.m.d.

Cu alte cuvinte: Algoritmul de rutare extrage adresa IP destinație din pachetul IP, apoi verifică dacă acea adresă corespunde cu vreuna din adresele interfețelor sale. Dacă nu, parcurge secvențial tabela de rutare comparând rezultatul operației ȘI logic efectuată între adresa IP destinație și masca rețelei extrasă din înregistrarea tabelei de rutare. Dacă rezultatul operației ȘI logic

corespunde cu adresa rețelei din înregistarea tabelei de rutare, pachetul IP este transmis la IP-ul specificat (next-hop). Dacă niciuna din rețelele din tabela de rutare nu corespunde cu adresa destinație, pachetul este ignorat.

23 Algoritmii de rutare

Algoritmii de rutare – clasificare:

1.Statici (neadaptivi)

– Dirijare pe calea cea mai scurta: algoritmul lui Dijkstra - este folosit de protocolul OSPF

– Inundare (eng. flooding): un pachet primit este copiat si transmis prin toate legaturile de comunicare (exceptand cea pe unde a venit) - aplicatii militare, baze de date distribuite, etc.

– Deflecting routing (sau hot-potato routing): la fiecare pas un pachet este examinat in raport cu adresa destinatie; daca legatura ceruta este libera pachetul este trimis, altfel este deviat (deflected) catre o alta linie de comunicare aleasa random

2.Dinamici (adaptivi)

– Cu vectori distanta: fiecare router mentine un tabel (vector) cu distanta si linia de comunicare catre destinatie; tabelele sunt actualizate cu informatiile de la vecini / Algoritmul Bellman-Ford - algoritm folosit de protocoalele RIP, BGP, IGRP

Problema: conform algoritmului cu vectori distanta, la fiecare actualizare a rutelor, tabelele de rutare trebuie trimise fiecarui vecin; unele pachete cu informatii legate de dirijare trec pe ruta de pe care deja au venit (reverse route). Pentru asta, se utilizeaza tehnica split horizon. Cand router-ul trimite actualizari de rute folosind o anumita interfata de retea, ele nu vor fi expediate retelelor ale caror rute au fost invatate din actualizari primite via acea interfata.

– Folosind starea legaturilor

– Dirijare ierarhica: ruterele stiu detalii asociate unei regiuni , dar nu stiu detalii despre structura interna a altor regiuni, pentru ca in retele de mari dimensiuni nu este fezabil ca un router sa aiba cate o intrare despre fiecare alt router.

– Prin difuziune (broadcast): utilizare: actualizarea stocurilor (de la bursa de valori), streaming multimedia, serviciu de distribuire a rapoartelor despre vreme, etc

– Cu trimitere multipla (multicast): router-ul va face periodic o interogare asupra host-urilor care apartin unui grup; apoi informatia este propagata catre routere

24 RIP

Routing Information Protocol este un protocol de rutare de tip distanță-vector ce implică utilizarea ca metrică de rutare a numărului de pași de rutat (hop count). Prin aceasta, RIP previne apariția buclelor de rutare, utilizând o valoare limită maximă ca număr de pași de rutare pe calea de la sursă la destinație. În general, limita este fixată la 15 (o valoare fixată la 16 reprezintă o distanță de rutare infinită, inoperabilă, prin urmare de evitat în selecția procesului de rutare). Se aplica algoritmul Bellman-Ford (pentru host-uri si routere).

25 OSFP

Open Shortest Path First este un protocol IP dinamic destinat rutării în interiorul unei rețele mari (guvernate de un singur gestionar) - sistem autonom (AS). Principial, OSPF este bazat pe caracteristicile conexiunilor dintre interfețe.

26 BGP

Border Gateway Protocol este protocolul de rutare folosit în nucleul Internetului. El menține o tabelă cu rețele IP (sau "prefixe") care arată calea folosită pentru a ajunge la rețeaua respectivă prin diferitele sisteme autonome (AS). BGP este considerat din acest motiv un protocol de rutare vector-cale (spre deosebire de protocoalele vector-distanță, care nu păstrează toată calea). BGP nu folosește aceleași metrici ca protocoalele de rutare folosite în interiorul AS-urilor, ci ia decizii bazându-se pe cale și pe politicile de rutare ale sistemului autonom din care face parte.

Alte protocoale: IGRP, EIGRP, SMRP, RVSP. Rutare interna: RIP, IGRP, EIGRP, OSPF, IS-IS. Rutare externa: BGP, EGP.

27 Retele wireless

Wi-Fi este o tehnologie radio folosită deseori la implementarea rețelelor locale de calculatoare de tip rețea locală fără fir (Wireless Local Area Network, WLAN). Un WLAN este un sistem de comunicații implementat ca extensie la, sau ca alternativă pentru o rețea locală (LAN) cablată, într-o clădire sau campus, combinând conectivitatea la viteză mare cu mobilitatea utilizatorilor, într-o configurație mult simplificată. Avantaje: mobilitatea, flexibilitatea, simplitatea în instalare, costurile de întreținere reduse și scalabilitatea.

Componente: dispozitive, NIC (Network Interface Card - asigura interfata dintre dispozitive si infrastructura retelei wireless), base stations, access controllers (componenta hardware care se afla intre punctul de access si partea de retea protejata), soft de conectare.

Categorii: WPAN (Personal-Area), WLAN (Local Area), WMAN (Metropolitan Area), WWAN (Wide Area).

Standarde de conectivitate pentru WPAN: IrDa (Infrared Data Association): comunicatie point-to-point bidirectionala via porturi cu infrarosu; Bluetooth.

WLAN - componente: dispozitive utilizator, radio NIC, access point, routere, repeater.

Standarde de conectivitate pentru WLAN: MIMO si alte coduri complicate.

WMAN (asigura conectivitatea intre cladiri si utilizatori in cadrul unui oras folosind cateva configuratii) - componente: bridges (asigura conectivitatea a doua retele care utilizeaza protocoale similare sau diferite la nivelul legaturii de date), antene (pentru retelele WMAN se folosesc in special antene directionale, pentru maximizarea intensitatii undelor radio intr-o directie).

Standarde de conectivitate pentru WMAN: Wi-Fi, WiMAX.

WWAN - componente: radio NIC, base stations (cell towers, sateliti), antene.

28 WAP

Wireless Application Protocol. Standard permitind accesarea informatiilor si serviciilor oferite de Internet via un dispozitiv mobil. Mai multe cifre cu care se bat campii in curs.

29 MIP - Mobile IP

Protocol care permite unui dispozitiv mobil deplasarea dintr-o retea in alta si mentinerea adresei IP.

Nodul mobil are doua adrese: Home Address (adresa IP a nodului mobil) si CoA (Care-of Address - desemneaza marginea retelei ce poate fi accesata prin rutari obisnuite).

Mecanismul general:

Un nod care doreste sa comunice cu nodul mobil va utiliza permanent home adress a acestuia

- Daca nodul mobil se gaseste in HomeNetwork, atunci daca cineva ii trimite un pachet se foloseste IP forwarding
- Daca nodul mobil se afla intr-o retea straina se foloseste CoA
- Nodul mobil isi inregistreaza locatia reala la home agent
- Pachetele sunt trimise printr-un tunel de la home agent la CoA (capatul tunelului)

Observatie: Daca nodul nu primeste mesaje de tip agent advertisment, atunci incearca sa obtina o adresa prin tehnici precum DHCP pentru a-si cunoaste locatia curenta

Tuneluri: legaturi logice la distanta de 1 hop, aflate la marginile Foreign Network la care sunt atasate nodurile mobile.

Rutarea: cand nodul mobil doreste sa trimita pachete, el nu le va trimite la home agent, ci le va trimite direct la nodul cu care doreste sa comunice, folosind

home adress ca valoare a campului source adress a pachetului IP (folosind foreign agent) – triangle routing.

30 Securitatea in retelistica

Forme de protectie:

1.Controlul accesului - modele: MAC (Mandatory Access Control), DAC (Discretionary Access Control), Role Based Access Control (RoBAC), Rule Based Access Control (RuBAC).

2.Confidentialitatea: imposibilitatea unei terte entitati sa aiba acces la datele vehiculate intre doi receptori. Solutii: Conexiuni private intre cele 2 puncte terminale ale canalului de comunicatie; datele circula printr-un tunel oferit de o retea privata virtuala (VPN – Virtual Private Network) + Criptarea datelor via diverse tehnici (biblioteci specializate si/sau oferite de mediile de dezvoltare).

3.Privacy: vizeaza drepturile ce trebuie respectate privind caracterul datelor vehiculate

4. Integritatea: implica detectarea incercarilor de modificare neautorizata a datelor transmise. Solutii: algoritmi de tip digest, semnaturi digitale.

5. Disponibilitatea: o anumita resursa poate fi accesata la momentul oportun.

6. Nerepudierea: expeditorul mesajului nu poate afirma ca nu l-a trimis. Solutie: certificate digitale.

Vulnerabilitate = slabiciune a unui sistem hardware/software care permite utilizatorilor neautorizati sa aiba acces asupra lui.

Tipuri de atac: accesul la nivel de utilizator, accesul de la distanta la diverse aplicatii, inocularea de programe pe calculatorul utilizatorului.

Moduri de atac: spargerea sau penetrarea (cracking), e-mail bombing, e-mail spamming, e-mail spoofing, social engineering, denial of service, teardrop, buffer overflow, IP sniffing, virusi, trojan horses, back doors/traps, worms, password guessing, reverse code-engineering.

Politici de securitate: gestionarea accesului (nume de cont, modul de schimbare a parolei, politica de acces din exterior etc.), accesul la resurse (drepturi de acces la fisiere, directoare, criptarea fisierelor importante etc.), administrarea copiilor de siguranta (tipuri de salvari, medii de stocare, durata pastrarii, ...).

Monitorizarea securitatii retelei (NSM – Network Security Monitoring) = colectarea, analiza si aprecierea indicatorilor si avertismentelor privind detectarea si raspunsul la incidente de securitate.

Protocoale pe niveluri: Nivelul retea - IPSec, Nivelul transport - TLS (Transport Layer Security), Nivelul aplicatie - SSH, PGP, S/MIME.