

1. Noțiuni generale privind rețelele de calculatoare [9; 10].

Esența rețelor de calculatoare:

Informațiile, Acces la informații, Transferul de informații, Procesarea informațiilor, Servicii informaționale, Cooperarea resurselor.

Rolul rețelor de calculatoare în societatea informațională:

- 1) Economia informațională
- 2) Comerțul electronic
- 3) VoIP
- 4) TV-IP
- 5) IoT
- 6) Rețelele sociale
- 7) Realitatea augmentată

Componente funcționale RC:

Medii de transmisie și noduri fără fir: cupru, fibră optică, wireless.

Notificare unele componente RC:

- a) noduri terminale: calculator, laptop, imprimantă, telefon IP, tabletă wireless
- b) noduri intermediare: router wireless, switch multilayer, switch-ul LAN, router, instrument firewall
- c) medii de transmisie: mediu wireless, mediul WAN, mediul LAN

2. Evoluția sistemelor de calcul de la sisteme locale la rețele de calculatoare [9].

Calculatoare electronice Etape de cooperare a resurselor:

- 1) Calculatoare autonome (stand alone)
- 2) Complexe de calcul (clustere)
- 3) Sisteme de teleprelucrare a datelor
- 4) Rețele de calculatoare.

Dinamica dezvoltării rețelor de calculatoare

- 1) Folosire autonomă a calculatoarelor
- 2) Complexe de calcul multicalculator(clustere)
- 3) Sisteme de teleprelucrare a datelor
- 4) Rețele de calculatoare – 1968. ♣ NPL (1968) ♣ ARPA (1969) ♣ CYBERNET (1969) ♣ SITA (1969) ♣ TYMNET (1969) ♣ ALOHA (1971) ♣ Ethernet (1973) ♣ Internet (1974) ♣ Abilene (10 Gbps, 1998) ♣ 100 Gigabit Ethernet (2010) ♣ 400 Gbps router (Alcatel-Lucent, 2012)

3. Caracteristici de bază ale rețelor de calculatoare [6/108-112].

- - Viteza de comunicare
- - Securitate
- - Scalabilitate
- - Fiabilitate

O **rețea de calculatoare** leagă între ele o mulțime mai mică sau mai mare de [calculatoare](#), astfel încât un calculator poate accesa [datele](#), [programele](#) și facilitățile sau resursele unui alt calculator conectat la aceeași rețea.

Există rețele de calculatoare centralizate și descentralizate. Printre [rețelele descentralizate](#) se numără ca exemplu rețelele [ARPAnet](#), [Metanet](#) și [Freenet](#).

Rețelele de calculatoare pot fi clasificate și după tehnologia care este folosită pentru a conecta dispozitive individuale din rețea, cum ar fi fibră optică, Ethernet, Wireless LAN, HomePNA sau Power line.

Rețelele de calculatoare mai pot fi clasificate în funcție de relațiile funcționale care există dintre elementele unei rețele, ca de exemplu: *Active Networking Architecture*, *Client-Server Architecture* și *Peer-to-peer (workgroup) Architecture*.

Rețelele de calculatoare se împart după extinderea lor în următoarele tipuri: [LAN](#), [MAN](#), [WAN](#) și, ceva mai nou, PAN.

4. Clasificarea rețelelor de calculatoare [1/13-24].

- 1) **Rețelele cu difuzare** au un singur canal de comunicații care este partajat de toate mașinile din re-țea
- 2) **Rețele locale** se disting de alte tipuri de rețele prin trei caracteristici: mărime, tehnologie de transmisie și topologie.
- 3) **Rețea metropolitană** sau **MAN** deservește un oraș, rețeaua de televiziune prin cablu disponibilă în mai multe orașe).
- 4) **Rețea larg răspândită geografic** sau WAN, acoperă o arie geografică în-tinsă - deseori o țară sau un continent întreg.
- 5) **Rețele fără fir** Comunicațiile digitale fără fir
- 6) **Rețelele casnice (Home networks)** Fiecare dispozitiv din casă va fi capabil să comuni-ce cu orice alt dispozitiv și toate vor fi accesibile prin Internet.
- 7) **Inter-rețelele** colecție de rețele interconectate este numită **inter-rețea** sau **internet**

5. Esența, componente și funcțiile de bază ale rutelor și comutatoarelor [2].

Componentele principale ale unui **Ruter** din prima generație sunt:

- **Procesorul** (asigură, prin implementarea softurilor pe parcursul comutării pachetelor, interfața cu utilizatorul fără a utiliza hardware specializat; construiește tabelele de rutare și le menține); **memoria** (este gestionată de către sistemul de operare) - memoria cu acces aleatoriu (**RAM**), memoria cu acces aleatoriu non-volatilă (**NVRAM**), memoria **FLASH**, memoria read-only (**ROM**) și **interfețele** (elementele discrete ce asigură recepționarea și transmiterea pachetelor pentru diversele medii de transmisie suportate de ruter).
- **Funcția** îndeplinită de rutere se numește **rutare**. Ruterul este un dispozitiv care conectează două sau mai multe [rețele de calculatoare](#) bazate pe „comutarea de pachete” (*packet switching*).

Componentele și funcțiile de baza a **comutatoarelor**:

- Componentele de baza ale unui switch sunt: un **procesor de uz general**, **memorie** pentru cadre și o **magistrală** sau **switch** prin care circula cadrele în procesul de switching strins cuplata cu unul sau mai multe **procesoare specializate** care realizează comutarea pachetelor.
- Switch-ul analizează frame-urile primite și decide dacă frame-ul trebuie trimis și dacă da pe ce port.

6. Accesarea unui echipament și navigarea în IOS [2].

Există câteva modalități pentru a accesa mediul CLI. Cele mai obișnuite metode sunt: Consola , Telnet sau SSH, Port AUX.

Comenzile enable și disable sunt utilizate pentru a modifica CLI-ul între modul EXEC al utilizatorului și modul EXEC privilegiat. Pentru a accesa modul EXEC privilegiat, folosiți comanda enable . Modul EXEC privilegiat este denumit uneori modul enable.

7. Noțiunea Hostname, comanda show și limitarea accesului la echipamente în IOS [2].

Atunci când se configurează un echipament de rețea, unul din primii pași este reprezentat de configurarea unui nume de echipament unic sau a unui hostname. **Hostname**-urile apar în prompt-urile CLI, pot fi utilizate în procese de autentificare diferite între echipamente. **Hostname**-urile sunt configurate pe echipamente de rețea active. Dacă numele echipamentului nu este explicit configurat, Cisco IOS folosește un nume de echipament implicit alocat din fabrică (Switch).

Comandă **show** poate fi utilizată pentru a examina aproape totul despre un router Cisco și configurația acestuia.

Fiecare echipament, fiecare router de domiciliu ar trebui să aibă parole configurate pentru a limita accesul. IOS-ul folosește moduri ierarhice pentru a ajuta la securitatea echipamentului. Ca parte a acestei îmbunătățiri de securitate, IOS-ul poate accepta câteva parole pentru a permite diferite privilegii de acces la echipament.

Tipurile de parole introduse sunt:

- **Parola Enable** - Limitează accesul la modul EXEC privilegiat
- **Enable secret** - Criptat, limitează accesul la modul EXEC privilegiat
- **Parola Consolei** - Limitează accesul al echipamente folosind conexiunea la consolă
- **Parola VTY** - Limitează accesul echipamentului prin Telnet

8. Adresarea echipamentelor și verificarea conectivității în IOS [2].

Pentru ca un echipament final să comunice prin rețea, trebuie configurat cu informațiile corecte ale adresei IP. Echipamentul final trebuie configurat cu o adresă IP și o mască de subrețea. Această informație se află în setările calculatorului.

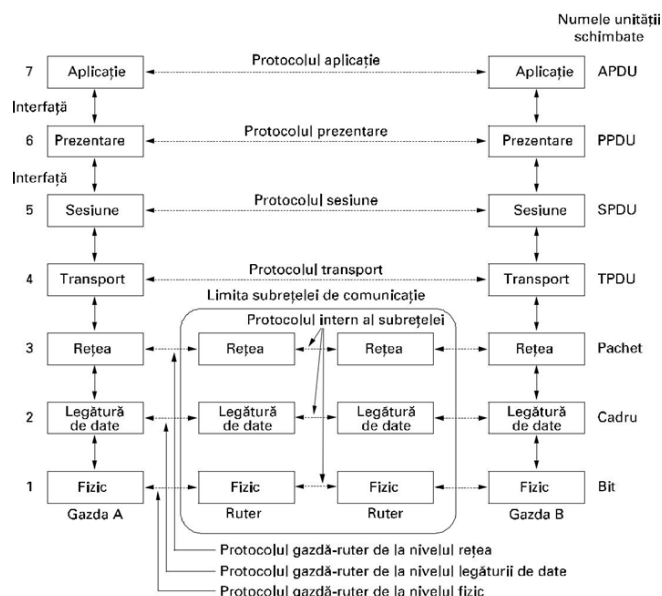
Pentru a activa conectivitatea IP la S1, folosind adresa IP 192.168.10.2:

- **interface vlan 1** Folosită pentru a naviga în modul de configurare al interfeței în modul de configurare global
- **ip address 192.168.10.2 255.255.255.0** - Configurează adresa IP și masca de subrețea pentru switch (este doar una din combinațiile posibile pentru o adresă IP și o mască de subrețea)
- **no shutdown** - Se activează din punct de vedere administrativ interfața într-o stare activă

Informația adresei IP poate fi introdusă în calculator manual sau folosind DHCP. DHCP permite echipamentelor finale să configureze automat informația despre IP.

Comanda **ping** poate fi utilizată pe un calculator, dar și pe un echipament cu Cisco IOS. În aceeași manieră în care se folosesc comenzile și utilitățile pentru a verifica configurarea hostului, se folosesc comenzile pentru a verifica interfețele echipamentelor intermediare: **show ip interface brief**

9. Descrierea generală a modelului de referință OSI ISO [1/34-37; 6/18-22].



Modelul **ISO OSI** se ocupă de conectarea sistemelor deschise - adică de sisteme deschise comunicării cu alte sisteme. În continuare vom folosi mai ales termenul prescurtat de model OSI.

Modelul OSI cuprinde șapte niveluri.

- 1) **Nivelul fizic** se ocupă de transmiterea biților printr-un canal de comunicație.
- 2) **Nivelul legăturii de date** transformă un mijloc oarecare de transmisie într-o linie care să fie disponibilă nivelului rețea fără erori de transmisie nedetectate.
- 3) **Nivelul rețea** se ocupă de controlul funcționării subrețelei.
- 4) **Nivelul transport** acceptă date de la nivelul sesiune, le descompune, dacă este cazul, în unități mai mici, transferă aceste unități nivelului rețea și se asigură că toate fragmentele sosesc corect la celălalt capăt.
- 5) **Nivelul sesiune** permite utilizatorilor de pe mașini diferite să stabilească între ei sesiuni.
- 6) **Nivelul prezentare** se ocupă de sintaxa și semantica informațiilor transmise.
- 7) **Nivelul aplicație** conține o varietate de protocoale frecvent utilizate. Un exemplu de protocol utilizat pe scară largă este **HTTP (HyperText Transfer Protocol)**, care stă la baza **WWW (World Wide Web)**

10. Funcțiile straturilor modelului de referință OSI ISO [1/34-37; 6/22-25].

Nivelul Aplicație Rol: realizează interfața cu utilizatorul și interfața cu aplicațiile, specifică interfața de lucru cu utilizatorul și gestionează comunicația între aplicații. Acest strat nu reprezintă o aplicație de sine stătătoare, ci doar interfața între aplicații și componentele sistemului de calcul.ex(HTTP; FTP; SNMP; SSH; NFS...)

Unitatea de date: mesajul

Nivelul Prezentare Rol: transformă datele în formate înțelese de fiecare aplicație și de calculatoarele respective, compresia datelor și criptarea.

Unitatea de date: -

Nivelul Sesiune Rol: furnizează controlul comunicației între aplicații. Stabilește, menține, gestionează și închide conexiuni (sesiuni) între aplicații.

Unitatea de date: -

Nivelul Transport Rol: transferul fiabil al informației între două sisteme terminale (*end points*) ale unei comunicații. Furnizează controlul erorilor și controlul fluxului de date între două puncte terminale, asigurând ordinea corectă a pachetelor de date. Oferă un serviciu de transport de date care izolează nivelurile superioare de orice specificități legate de modul în care este executat transportul datelor.

Unitatea de date: segmentul, datagrama

Nivelul Rețea Rol: determinarea căii optime pentru realizarea transferului de informații într-o rețea constituită din mai multe segmente, prin fragmentarea și reasamblarea informației

Unitatea de date: pachetul

Nivelul Legătură de Date *Nivelul legătură de date se ocupă cu adresarea fizică, topologia rețelei, accesul la rețea, detecția și anunțarea erorilor și controlul fluxului fizic (flow control).*

Rol: furnizează un transport sigur, fiabil, al datelor de-a lungul unei legături fizice, realizând:

- Controlul erorilor de comunicație
- Controlul fluxului de date
- Controlul legăturii
- Sincronizarea la nivel de cadru

Unitatea de date: cadru

Nivelul Fizic definește specificații electrice, mecanice, procedurale și functionale pentru activarea, menținerea și dezactivarea legăturilor fizice între sisteme.

Rol: transmiterea unui șir de biți pe un canal de comunicații. Se precizează modulații, codări, sincronizări la nivel de bit. Un standard de nivel fizic definește 4 tipuri de caracteristici:

- Mecanice (forma și dimensiunile conectorilor, numărul de pini)
- Electrice (modulația, debite binare, codări, lungimi maxime ale canalelor de comunicație)
- Funcționale (funcția fiecărui pin)
- Procedurale (succesiunea procedurilor pentru activarea unui serviciu)

Unitatea de date: bitul

11. Esența, arhitectura și evoluția Internet [1/44-53; 6/15-18].

Internetul este o rețea ce interconectează rețele răspândite în lumea întreagă, încadrându-se în categoria rețelilor WAN (*Wide Area Network*). Calculatoarele din *Internet* sunt conectate prin intermediul unor linii de comunicație (cablu, radio, fibra optică, e.t.c) prin care se transmit datele.

Rețeaua *Internet* poate fi privită ca un graf, care are drept muchii liniile de comunicație, iar ca noduri un echipament *hardware*. Într-un nod nu se afla neapărat un calculator gazda, ci se poate amplasa un echipament

periferic (display, imprimanta) sau un controler de comunicare (numit si nod de comutare sau *router*) avand sarcina de a dirija datele in cadrul rețelei.

12. Modelul arhitectural TCP/IP și compararea lui cu cel OSI [1/37-41; 6/25-26].

Nivelul internet permite gazdelor să emită pachete în orice rețea și a face ca pachete-le să circule independent până la destinație

Nivelul transport permite conversații între entitățile pereche din gazdele sursă și, respectiv, destinație.

Nivelul aplicație conține toate protocoalele de nivel mai înalt. Primele protocoale de acest gen includeau terminalul virtual (TELNET), transferul de fișiere (FTP) și poșta electronică (SMTP).

Nivelul gazdă-rețea - gazda trebuie să se lege la rețea, pentru a putea trimite pachete IP, folosind un anumit protocol. Acest protocol nu este definit și variază de la gazdă la gazdă și de la rețea la rețea.

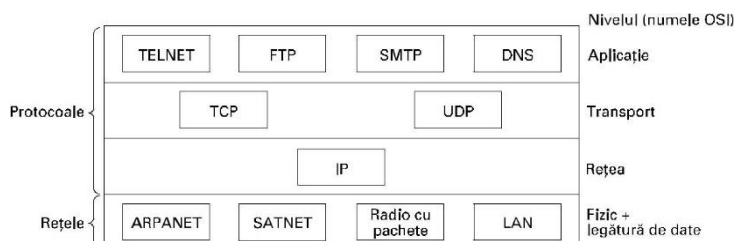


FIG. Protocoale și rețele din modelul TCP/IP inițial.

TCP/IP și compararea lui cu cel OSI

Asemănări:

1. Ambele [au niveluri](#)
2. Ambele au nivelul aplicației, deși fiecare conține servicii diferite
3. Ambele au nivelurile rețelei [și transportului comparabile](#)
4. Ambele folosesc tehnologia de tip packet switching (nu cea circuit switching)
5. Administratorii de rețea trebuie să le cunoască pe amândouă

Deosebiri:

1. TCP/IP combină în nivelul său Aplicație (4) nivelele Aplicație (7), Prezintăre (6) și Sesiune (5) din modelul OSI.
2. TCP/IP combină nivelul Legătură de date (2) și nivelul Fizic (1) din modelul OSI într-un singur nivel numit Acces Rețea (1).
3. TCP/IP pare a fi mai simplu deoarece are mai puține niveluri.
4. Protocoalele TCP/IP reprezintă standardele pe baza cărora s-a dezvoltat Internetul.
5. Rețelele tipice nu sunt construite [pe baza protocoalelor OSI](#), deși modelul OSI este considerat ca ghid.
6. TCP / IP folosește protocolul UDP care nu garantează întotdeauna livrarea de pachete precum face nivelul transport din modelul OSI.

13. Adrese fizice ale entităților de rețea [6/62-65].

Adresa fizică(MAC) lucrează pentru a identifica un echipament din rețea. Similar cu numele unei persoane, adresa MAC a unui host nu se poate modifica; este alocată în mod fizic la placa de rețea a hostului și este cunoscută ca adresă fizică. Adresa fizică rămâne aceeași indiferent de locul în care este plasat hostul.

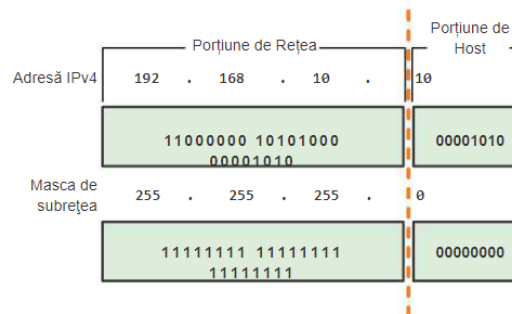
Utilizarea adresei MAC este una dintre cele mai importante aspecte ale tehnologiei LAN Ethernet. Adresele MAC utilizează numerotarea în hexazecimal. În Ethernet, adresele MAC diferite sunt utilizate pentru comunicații multicast, broadcast și unicast de Layer 2.

14. Adrese și scheme de adrese IP [6/43-48].

Adresa IP este similară cu adresa unei persoane. Adresa este în funcție de locul în care se află în momentul acesta hostul. Folosind această adresă, este posibil ca un frame să determine locația în care va fi trimis un frame. Adresa

IP sau a rețelei este cunoscută ca o adresă logică din cauză că este alocată logic. Este alocată fiecărui host de către un administrator de rețea în funcție de rețeaua locală la care este conectat hostul. O adresa IPv4 este o secvență de 32 biti de 1 și 0. Pentru ca o adresă IPv4 să fie ușor de utilizat, ea este scrisă ca patru numere zecimale separate prin punct.

Fiecare computer din rețea trebuie să aibă o adresă IP. Adresa IP nu este codificată în mod unic în interfața rețelei computerului. Administratorul de rețea atribuie adresa IP fie în mod static, fie dinamic. Aceasta înseamnă că trebuie să existe o gestionare atentă a adreselor IP pentru a evita conflictele cauzate de adresele duplicate.



15. Tipuri de adrese IPv4 [6/49-51].

Class	Theoretical Address Range	Used for
A	0.0.0.0 to 127.255.255.255	Very large networks
B	128.0.0.0 to 191.255.255.255	Medium networks
C	192.0.0.0 to 223.255.255.255	Small networks
D	224.0.0.0 to 239.255.255.255	Multicast
E	240.0.0.0 to 247.255.255.255	Experimental

16. Adrese IPv6 [6/53-61]. Exemplu : 2001:0DB8:AC10:FE01::

IPv6 are adrese mai lungi decât IPv4. Ele au o lungime de 16 octeți, ceea ce rezolvă problema: să furnizeze o sursă efectiv nelimitată de adrese Internet.

A doua mare îmbunătățire a lui IPv6 este simplificarea antetului. El conține numai 7 câmpuri (față de 13 în IPv4). Această schimbare permite rutelor să prelucreză pachetele mai rapid, îmbunătățind astfel productivitatea și întârzierea.

A treia mare îmbunătățire a fost suportul mai bun pentru opțiuni. Această caracteristică accelerează timpul de prelucrare a pachetelor.

Un al patrulea domeniu în care IPv6 reprezintă un mare progres este în securitate.

17. Mesaje, discretizarea mesajelor continui, cantitatea informației în mesaje [9].

Mesaje - Informațiile se transmit între stațiile unei rețele prin mesaje (comunicate). Mesajul este o totalitate de informații cu înțeles finit prezentate într-o anumită formă. Mesajele pot fi continue și discrete. Ca exemplu de **mesaj discret** poate servi cursul valutar al leului R. Moldova. Cursul în cauză poate primi un număr finit de valori.

Un exemplu de **mesaj continuu** – temperatura într-un anumit punct al mediului înconjurător; ea poate primi o infinitate de valori. Operarea cu mesaje discrete este, de obicei, mai facilă și este considerabil mai facilă la folosirea sistemelor de calcul numeric.

Discretizarea mesajelor continui - Orice mesaj continuu cu un spectru de frecvențe limitat poate fi transformat, cu orice exactitate necesară dinainte stabilită, într-un mesaj discret. Acest proces se numește discretizare și are la bază teoremele Fourier și Nyquist.

Cantitatea informației în mesaje - Cantitatea de informații conținută în mesaj este: $I_i = -\log_2 P_i$.

18. Transformarea mesajelor în semnale [9].

Semnal - În calculatoarele numerice informația este reprezentată în formă numerică. Numerele sunt reprezentate în sistemul binar, utilizând "0" și "1". **Reprezentarea** - nivel de tensiune înaltă (fie +3 v) pentru cifra "1" și nivel de tensiune joasă (fie 0 v) pentru cifra "0". Sau, stare magnetizată a unei porțiuni de material feromagnetic pentru reprezentarea cifrei "1" și stare nemagnetizată - pentru cifra "0".

Procesul **transformării mesajului** în semnal uzual include trei operații:

- 1) transformarea propriu-zică (primară);
- 2) codificarea;
- 3) modularea.

Uneori două sau chiar toate trei aceste operații se realizează simultan. Transformarea propriu-zică constă în conversia datelor sau mărimilor fizice, care reprezintă mesajul, în semnal primar (electric, optic, etc.).

Modulare se numește schimbarea parametrului purtătorului semnalului conform funcției, ce reprezintă mesajul care se transmite. În calitate de purtător poate servi curentul electric continuu, curentul electric alternativ, un șir periodic de impulsuri scurte, inclusiv de natură optică, unde electromagnetice, met. mixte.

Moduri de modulație în impulsuri: ♣ de amplitudine (MIA); ♣ de durată (MID); ♣ de frecvență (MIF); ♣ de fază (MIF).

19. Medii de transmisie ghidată [1/82-90, 2].

Mediile **ghidate** cuprind: **cablu de cupru, cablu torsadat, cablu coaxial și fibre optice** iar cele **neghidate**, unde radio și laserul, propagându-se prin eter (wireless).

Cablul torsadat - Acest tip de cablu constă într-un număr de perechi de fire (normal patru), răsucite două câte două.

Cablul coaxial - Este format dintr-o pereche de fire de cupru, un fir central (firul cald) și un conductor exterior, împletit în jurul firului cald (manta).

Fibra optică - Data fiind frecvența foarte mare a purtătoarei informației, are o viteză de transmisie foarte ridicată, atingându-se curenți de ordinul 1Gbit/s.

20. Trunchiuri și multiplexare [1/123-129].

Metodele de multiplexare se pot împărți în două categorii principale: **FDM** (multiplexare cu divizare în frecvență) și **TDM** (multiplexare cu divizare în timp). La FDM, spectrul de frecvență este împărțit în mai multe canale logice, fiecare utilizator având drepturi exclusive asupra unei anumite benzi de frecvență. La TDM, utilizatorii își așteaptă rândul (în mod re-petă, circular), fiecare utilizator obținând întreaga bandă de frecvență pentru o scurtă perioadă.

Multiplexarea prin divizarea în frecvență

Filtrele limitează lărgimea de bandă folosită la 3100 de Hz pe canal de bandă vocală. Atunci când sunt multiplexate împreună mai multe canale, fiecărui canal îi sunt alocate 4000 de Hz, astfel încât canalele să fie bine separate. Mai întâi, canalele de voce sunt deplasate în frecvență, fiecare cu o valoare diferită. Apoi ele pot fi combinate, deoarece nu există două canale care să ocupe aceeași zonă a spectrului.

Multiplexarea prin divizarea lungimii de undă

Pentru canalele de fibră optică se utilizează o alternativă a multiplexării prin divizarea în frecvență - **WDM**. Principiul de bază pentru WDM pe fibre - se întâlnesc patru fibre la nivelul unui combinator optic, fiecare cu energia și lungimea de undă proprie. Cele patru raze sunt combinate într-o singură fibră comună pentru a fi transmise către o destinație depărtată. La destinație, raza este despărțită în atâtea fibre câte au fost inițial. Fiecare fibră de la destinație conține un mic filtru special construit, care filtrează toate lungimile de undă mai puțin una. Semnalele rezultate pot fi rutate către destinație sau recombinate în diferite feluri pentru transmisii multiplexate ulterioare.

Multiplexarea prin divizarea în timp

Semnalele analogice sunt digitizate în oficiul final de un echipament numit **codec**, operație care are ca rezultat o serie de numere de 8 biți. Codec-ul realizează 8000 de eșantioane pe secundă. Această tehnică se numește **PCM** (modularea în cod de impulsuri). PCM constituie nucleul sistemelor telefonice moderne.

21. Comutarea în rețele [1/132-136].

Comutarea de circuite

Atunci când formezi – tu sau calculatorul tău – un număr de telefon, echipamentele de comutare din sistemul telefonic caută o cale fizică între telefonul tău și telefonul apelat.

Comutarea de mesaje

Atunci când se utilizează acest tip de comutare, nu se stabilește de la început o cale între apelant și apelat. În schimb, atunci când apelantul are de transmis un bloc de date, acesta este memorat în primul oficiu de comutare (ruter) și este retransmis mai târziu, pas cu pas. Fiecare bloc este recepționat în întregime, verificat pentru a detecta eventualele erori și apoi retransmis.

Comutarea de pachete

Rețelele cu comutare de pachete fixează o limită superioară precisă pentru dimensiunea blocului, permițând pachetelor să fie păstrate în memoria principală a ruterului, în loc să fie salvate pe disc. Asigurându-se faptul că nici un utilizator nu va putea monopoliza o linie de transmisie mult timp (milisecunde), rețelele cu comutare de pachete au devenit adecvate pentru traficul interactiv.

22. Tehnologii și mijloace de acces la rețea [2, 6/68-74].

Ethernet - este tehnologia LAN cel mai frecvent instalată prin cablu (rețea locală). Ethernet LAN utilizează de obicei cablu coaxial sau clase speciale de fire pereche torsadată.

LAN-urile wireless - permit utilizatorilor de dispozitive mobile să se conecteze printr-o conexiune wireless (radio).

Rețelele cu fibră optică - cum ar fi fibrele la domiciliu (FTTH), utilizează fibră optică dintr-un punct central direct la clădiri individuale, cum ar fi locuințe, clădiri de apartamente și întreprinderi.

ADSL (Asymmetric Digital Subscriber Line) - este o tehnologie pentru transmiterea informațiilor digitale la o lățime de bandă ridicată pe liniile telefonice existente către case și firme.

23. Servicii oferite stratului Rețea de către stratul Legătură de date [1/166-169].

Funcția nivelului legătură de date este să ofere servicii nivelului rețea. Principalul serviciu este transferul datelor de la nivelul rețea al mașinii sursă la nivelul rețea al mașinii destinație. La nivelul rețea al mașinii sursă există o entitate, să-i spunem proces, care trimite biți către nivelul legătură de date, pentru a fi transmiși la destinație. Funcția nivelului legătură de date este să transmită biții spre mașina destinație, pentru ca acolo să fie livrați nivelului rețea.

Nivelul legătură de date poate fi proiectat să ofere diferite servicii:

- 1) Serviciu neconfirmat fără conexiune.
- 2) Serviciu confirmat fără conexiune.
- 3) Serviciu confirmat orientat-conexiune.

24. Aspecte generale privind controlul erorilor și al fluxului la nivel Legătură de date [1/172-173].

Controlul erorilor.

Modul uzual de a asigura o transmitere sigură este de a furniza emițătorului o reacție inversă (feedback) despre ceea ce se întâmplă la celălalt capăt al liniei. De obicei protocolul îi cere receptorului să trimită înapoi cadre de control speciale, purtând confirmări pozitive sau negative despre cadrele sosite.

Atunci când emițătorul trimite un cadru, pornește de obicei și un contor de timp. Contorul de timp este setat să expire după un interval suficient de lung pentru ca acel cadru să poată ajunge la destinație, să fie prelucrat acolo și confirmarea să se propage înapoi către emițător.

Este necesar să atribuim numere de secvență cadrelor de ieșire, așa încât receptorul să poată face distincție între cadrele retransmise și cele originale.

Controlul fluxului.

Există două abordări des utilizate. În cazul celei dintâi, **controlul fluxului bazat pe reacție**, receptorul acordă emițătorului permisiunea de a mai transmite date, sau cel puțin comunică emițătorului informații despre starea sa. În cea de-a doua, **controlul fluxului bazat pe rată**, protocolul dispune de un mecanism integrat care limitează rata la care emițătorul poate transmite, fără a folosi informații de la receptor.

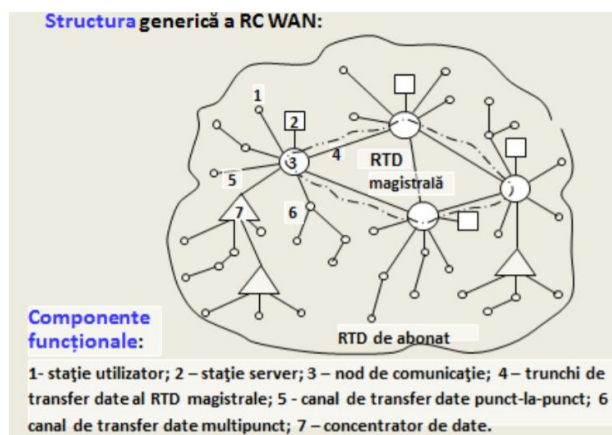
25. Caracteristica generală a protocoalelor stratului Legătură [6/34-35].

Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 Wi-Fi, FDDI, PPP

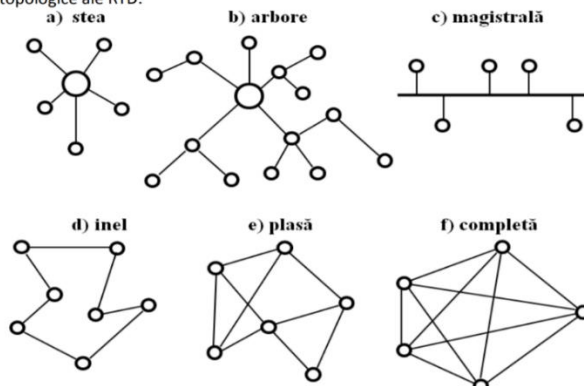
26. Protocolul PPP [6/35-40].

Protocolul punct-la-punct (PPP) este un protocol TCP/IP utilizat pentru a conecta un sistem de calculatoare la altul. Calculatoarele utilizează PPP pentru a comunica prin rețeaua telefonică sau prin Internet. O conexiune PPP se realizează atunci când două sisteme sunt conectate fizic printr-o linie telefonică. Puteți folosi PPP pentru a conecta un sistem la altul.

27. Rețeaua de transfer de date (RTD) – subrețea a rețelei de calculatoare. Structuri topologice (forme) ale RTD: clasificare, esență, caracteristici [9].



Structuri topologice ale RTD:



Caracteristica structurilor topologice ale RTD

Topologia	Utilizare		Simplitatea	Lungimea canalelor, (costul)	Fiabilitatea
	domeniul	gradul			
Stea	LAN	scăzut	maximă	mică-mare	minimă
Stea	RTD acces	scăzut	maximă	mică-mare	minimă
Arbore	LAN	maxim	întaltă	minimă	joasă
Arbore	MAN	scăzut	întaltă	minimă	joasă
Arbore	RTD acces	maxim	întaltă	minimă	joasă
Magistrală	LAN	deja rar	maximă	mic	joasă
Inel	LAN	deja rar	minimă	mic	medie
Plasă	RTD magistr.	maxim	complexă	mare	întaltă
Completă	RTD magistr.	minim	complexă	maximă	maximă

28. Rețele de transfer date cu comutare. Analiza comparativă a metodelor de comutare folosite în rețele [9].

Rețelele de comunicații comutate constau din noduri de comunicație (NC), interconectate prin canale de transfer date. Nodurile de comunicație sunt destinate comutării canalelor sau a traficului de date între canalele rețelei. Utilizarea lor permite reducerea numărului de canale și, respectiv, a costului rețelei.

Rețelele de comunicații comutate pot fi:

- ♣ cu comutare de canale;
nodurile de comutație, la cerere, stabilesc conexiunile temporare solicitate între canalele de comunicație incidente.
- ♣ cu comutare de mesaje (depășite);
nodurile de comunicație, assemblează fiecare mesaj recepționat, îl înscrie temporar în memorie, determină canalul de ieșire și retransmite mesajul următorului nod din rețea în conformitate cu destinația lui.
- ♣ cu comutare de pachete;
e este o dezvoltare firească a comutării de mesaje. Ea înlătură neajunsurile mai esențiale ale comutării de mesaje: se reduce durata transmisiei și capacitatea necesară a memoriei nodurilor de comunicație.

Compararea metodelor de comutare în rețele		
Criteriu	Comutarea datagramă	Comutarea cu circuite virtuale
Stabilirea circuitului	Nu este necesară	Obligatorie
Adresare	Fiecare pachet conține adresa sursă și adresa destinație	Fiecare pachet conține numărul CV (este mult mai mic)
Informații de stare	Ruterele nu păstrează informații despre conexiuni	Fiecare CV necesită spațiu pentru tabelul rutelui per conexiune
Dirijare	Fiecare pachet este dirijat independent	Calea este stabilită la inițierea CV, toate pachetele o urmează
Efectul defectării rutelui	Nici unul, cu excepția pachetelor în timpul defectării	Toate CV-urile care trec prin rutelul defect sunt terminate
Calitatea serviciului	Dificil	Simplu, dacă pentru fiecare CV pot fi alocate în avans suficiente resurse
Controlul congestiei	Dificil	Simplu, dacă pentru fiecare CV pot fi alocate în avans suficiente resurse

29. Rețele cu difuzarea de pachete [1/14; 9].

Rețelele cu difuzare au un singur canal de comunicație (mediu de transmisie) partajat între stațiile atașate. Când o stație (calculator, terminal) transmite, toate celelalte pot recepționa informațiile respective. Destinatarul este indicat printr-un identificator special (în RC – adresă). În asemenea rețele este necesară coordonarea accesului stațiilor la mediu pentru transmisie.

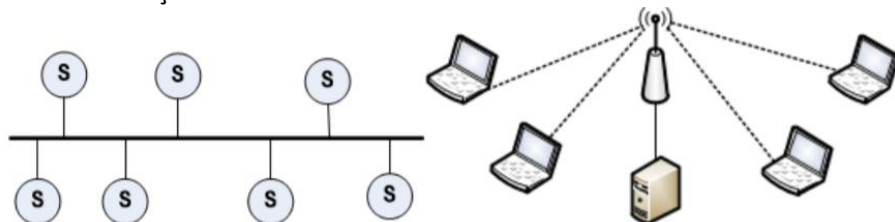
În funcție de mediul de transmisie utilizat și aria de cuprindere se deosebesc:

- ♣ rețele radio cu difuzare; ♣ rețele de sateliți cu difuzare (cosmice); ♣ rețele locale cu difuzare.

Metode acces la mediu, cablat (ghidat), radio,

Ca exemplu de rețea radio cu difuzare poate servi rețeaua ALOHA, lansată la Universitatea din Honolulu în 1971. La rețele locale cu difuzare se referă rețelele conforme standardului IEEE 802.11.

Scheme de rețele de calculatoare cu difuzare:



30. Caracterizarea generală a tehnologiei de rețea Ethernet [1/59-61; 2].

Ethernet-ul a fost inventat pe baza ideii că pentru a lega computerele între ele astfel ca să formeze o rețea este nevoie de un mediu de transmisie central cum ar fi un cablu coaxial partajat.

Ethernet-ul constituie fundamentul majorității LAN-urilor actuale. În loc de un mediu (cablu) central, tehnologiile moderne utilizează legături de tipul „punct-la-punct”, *hub*, *switch*, *bridge* și *repeater*, bazate pe fire electrice de cupru torsadate care reduc costurile instalării, măresc fiabilitatea și înlesnesc managementul și reparațiile rețelei.

La nivelele de deasupra nivelului fizic, aparatele dintr-o rețea *Ethernet* comunică între ele prin împărțirea mesajelor în multe pachete mici, care se transmit și se recepționează unul câte unul (dar foarte repede). Fiecare aparat legat la rețea primește o adresă de la protocolul *Media Access Control* (Adresă MAC), unică, alcătuită din 48 biți, și care se folosește la identificarea atât a sursei cât și a destinației pachetelor.

31. Metoda (protocolul) de acces la mediu CSMA/CD [1/232-233].

CSMA(Carrier Sense Multiple Access) este un protocol care ascultă canalul înainte de a transmite. Dacă acesta este liber, transmite tot frame-ul. Dacă este ocupat, reține transmiterea. Dar totuși există posibilitatea coliziunii. Din cauza întârzierilor, două noduri poate să nu audă transmisiunea reciprocă.

CSMA/CD este protocolul CSMA cu CD(detectarea de coliziuni), care le detectează în timp scurt și stopează transmiterea celor două noduri pentru a reduce utilizarea canalului. Acest protocol este mai ușor în transmiterea prin cablu, și fac dificil prin transmiterea wireless, unde semnalul primit poate să fie copleșit de puterea transmiției locale.

Principiul de funcționare a CSMA/CD este de a transmite doar când canalul este liber, dacă acesta este ocupat, el așteaptă și ascultă. După ce începe să transmită pe canalul liber, el monitorizează apariția coliziunilor. Dacă apare coliziune, el se duce la procedura “coliziune detectată” și retransmite după frame-ul de la început.

32. Controlul legăturilor logice IEEE 802.2 [1/260-261].

Există sisteme în care este de dorit un protocol de legătură de date cu control al erorilor și al fluxului. IEEE a definit un astfel de protocol care poate funcționa peste Ethernet și peste cele-lalte protocole 802. Acest protocol, numit **LLC (Logical Link Control)**, ascunde diferențele între diferitele tipuri de rețele 802, oferind un singur format și o singură interfață pentru nivelul rețea.

Nivelul rețea de pe calculatorul emițător trimite un pachet către LLC, folosind primitivele de acces LLC. Subnivelul LLC adaugă apoi un antet LLC, conținând numere care indică secvența și mesajul de confirmare. Structura rezultată este inserată apoi în câmpul de informație utilă al unui cadru 802 și apoi transmisă. Când cadrul ajunge la receptor se desfășoară procesul invers.

LLC oferă trei opțiuni de **servicii**: servicii pentru datagrame nesigure, confirmarea serviciului de datagrame, și un serviciu sigur orientat spre conexiuni. Antetul LLC conține trei **câmpuri**: un punct de acces de destinație, un punct de acces sursă și un câmp de control. Punctul de acces spune din partea cărui proces a sosit cadrul și unde trebuie transportat, înlocuind câmpul „tip” DIX. Câmpul de control conține numere de secvență și de confirmare.

33. Protocolul ARP, actualizarea tabelului ARP [2; 6/42-43].

Caracteristica **ARP** (Address Resolution Protocol) îndeplinește o funcție necesară în rutarea IP. ARP găsește adresa hardware, cunoscută și sub numele de adresă MAC, a unei gazde de la adresa IP cunoscută. ARP menține o memorie cache (tabel) în care adresele MAC sunt mapate la adresele IP. Deci protocolul ARP are două funcții de bază:

- Aflarea adreselor IPv4 cu ajutorul adreselor MAC
- Menținerea unui tabel de asocieri

Tabelul ARP este menținut în mod dinamic. Intrările din tabelul ARP sunt înregistrate în timp în aceeași manieră în care intrările din tabelul MAC sunt înregistrate în switchuri. Dacă un echipament nu primește un frame de la un anumit echipament până când expiră timpul sau termenul limită, intrarea pentru acel echipament este ștearsă din tabelul ARP.

34. Comutarea cadrelor Ethernet. Caracterizarea generală a comutatoarelor Ethernet [2].

Hub - Este, în principiu, un repetor multiport. Un hub conectează mai multe fire provenind din ramuri diferite. Hub-urile nu pot filtra date, astfel încât pachetele de date sunt trimise tuturor dispozitivelor conectate. De asemenea, nu au inteligență pentru a afla cea mai bună cale pentru pachetele de date, ceea ce duce la ineficiențe și pierderi.

Bridge – un bridge funcționează la nivelul liniei de date. Un bridge este un repetor, care adaugă funcționalitatea de filtrare a conținutului prin citirea adreselor MAC ale sursei și destinației. Este, de asemenea, utilizat pentru interconectarea a două LAN-uri care lucrează pe același protocol. Are un singur port de ieșire și un singur port de ieșire, făcându-l astfel un dispozitiv cu 2 porturi.

Switch - un switch este un bridge multi-port cu un tampon și un design care îi poate spori eficiența și performanța. Switch-ul este un dispozitiv cu strat de legătură de date. Switch-ul poate efectua verificarea erorilor înainte de redirecționarea datelor, ceea ce îl face foarte eficient deoarece nu transmite pachete care au erori și transmite pachete bune selectiv pentru a corecta numai portul.

35. Noțiuni generale și clasificarea rețelelor fără fir [6/275-276].

Rețelele fără fir sunt rețele de aparate și dispozitive interconectate prin unde radio, infraroșii, optice și alte metode fără fir. Conexiunile fără fir devin tot mai populare, deoarece ele rezolvă probleme ce apar în cazul când avem multe cabluri, conectate la multe dispozitive. Tehnologiile moderne fără fir pot interconecta echipamentele (sau și rețelele locale, LAN-urile) la distanțe mici, dar și la distanțe mari.

Clasificarea rețelelor fara fir:

- Rețele locale de calculatoare (LAN – Local Area Network)
- Rețele de întindere mare (WAN – Wide Area Network)
- Rețele fara fir (WLAN – Wireless Local Area Network)

36. Particularitățile accesului la mediul fără fir [6/71-72, 276-278].

Medii de transmisie a datelor fără fir – transmit datele sub formă de unde radio, microunde, raze infraroșii sau raze laser - în cadrul conexiunilor fără fir (wireless);

Rețele WLAN sunt rețele locale la care transmisia datelor se face prin medii fără fir. Într-un WLAN, stațiile, care pot fi echipamente mobile – laptop – sau fixe – desktop - se conectează la echipamente specifice numite puncte de acces. Stațiile sunt dotate cu plăci de rețea wireless. Punctele de acces, de regulă routere, transmit și recepționează semnale radio către și dinspre dispozitivele wireless ale stațiilor conectate la rețea. În prezent există mai multe moduri de a capta datele din eter: Wi-Fi, Bluetooth, GPRS, 3G ș.a. Acestora li se adaugă o nouă tehnologie care poate capta datele de șapte ori mai repede și de o mie de ori mai departe decât populara tehnologie Wireless Fidelity (WiFi), numită WiMAX.

Avantaje:

1. Simplitate în instalare;
2. Grad ridicat de mobilitate a echipamentelor;
3. Tehnologia poate fi utilizată în zone în care cablarea este dificil sau imposibil de realizat;
4. Costul mai ridicat al echipamentelor wireless este nesemnificativ raportat la costul efectiv și costul manoperei în cazul rețelelor cablate;
5. Conectarea unui nou client la o rețea wireless nu implică folosirea unor echipamente suplimentare.

Dezavantaje:

1. Securitate scăzută;
2. Raza de acțiune în cazul folosirii echipamentelor standard este de ordinul zecilor de metri. Pentru extinderea ei sunt necesare echipamente suplimentare care cresc costul;
3. Semnalele transmise sunt supuse unor fenomene de interferențe care nu pot fi controlate de administratorul de rețea și care afectează stabilitatea și fiabilitatea rețelei – motiv pentru care serverele sunt rareori conectate wireless;

37. Arhitectura rețelelor IEEE 802.11 [6/284-286].

IEEE 802.11 definește controlul legăturii între echipamentele din rețea și este independent de mediul de transmisie sau de implementările substratului de control al accesului la mediul de transmisie.

Topologia rețelelor IEEE 802.11 este compusă din așa numitele seturi (sets), cu scopul de a oferi stațiilor mobilitate. IEEE 802.11 definește următoarele trei seturi topologice:

1. Setul de servicii de bază BSS (Basic Service Set). Reprezintă topologia de bază în rețele 802.11. Constă din cel puțin un punct de acces AP (Access Point) conectat la o rețea cablată și mai multe noduri wireless. Mai este cunoscut și sub numele de mod infrastructură.

2. Setul independent de servicii de bază IBSS (Independent Basic Service Set). Topologia IBSS mai este cunoscută și sub numele de modul ad-hoc.

3. Setul de servicii extins ESS (Extended Service Set). Topologia ESS conține mai multe seturi topologice BSS suprapuse (numite celule), fiecare fiind deservită de către un AP.

38. Moduri de operare și setarea rețelelor IEEE 802.11, inclusiv WDS și punctele de acces [6/287-289].

Retelele wireless pot opera în două moduri: **Ad-hoc** și **Infrastructure**.

- **Modul Ad-hoc** asigură conexiunea wireless directă între două calculatoare (dotate cu plăci de rețea wireless), fără comunicare cu rețeaua cablată. Funcționarea în acest mod permite doar transferul fișierelor între calculatoare.
- În **modul Infrastructure** întreg traficul trece printr-un echipament wireless numit access-point (nu există conexiune directă între calculatoare) care realizează și legătura cu rețeaua cablată. Funcționarea în modul infrastructură permite conectarea la Internet, transferul fișierelor, accesul la un printer sau alte servicii disponibile în rețeaua cablată.

Routerele wireless funcționează ca **access-point-uri**.

Un sistem de distribuție fără fir (**WDS**) este un sistem care permite interconectarea wireless la puncte de acces într-o rețea cu tehnologie de tip IEEE 802.11. Acesta permite o rețea fără fir pentru a se extinde cu ajutorul a mai multor puncte de acces fără cerința tradițională de a fi conectate cu fir. Avantajul notabil pentru WDS peste alte soluții se păstrează la adresele MAC de cadre-client din legături între puncte de acces.

39. Securitatea rețelelor fără fir [6/289-295].

Securitatea rețelelor wireless este cu atât mai greu de obținut mai ales datorită vulnerabilității legăturilor, protecției fizice limitate a fiecărui dintre noduri, conectivității sporadice, topologiei care se schimbă dinamic, absența autorității de certificare și lipsa unei monitorizări centralizate sau a unui punct de management. Pentru securizarea rețelelor wireless au fost definite suita de protocoale IEEE 802.11a/b/g/n cunoscute ca și Wi-Fi sub securitatea WEP și WPA și 802.16 cunoscut ca WiMax cu securitatea DES și AES.

40. Esența și oportunitatea divizării în subrețele. Esența, folosirea și beneficiile măștilor VLSM [2, 6/45-48].

Administratorii de rețea pot grupa echipamentele și serviciile în subrețele care sunt determinate de locația geografică (cum ar fi al treilea etaj al unei clădiri), de unitatea organizațională (departamentul de vânzări), tipul echipamentului (imprimante, servere, WAN) sau orice alte diviziuni care fac sens într-o rețea. Subnetizarea poate reduce traficul total de rețea și poate duce la îmbunătățirea performanței rețelei.

Subnetizarea tradițională creează subrețele de dimensiuni egale. **VLSM** permite ca un spațiu de rețea să fie împărțit în părți inegale. Cu VLSM, masca de subrețea va varia în funcție de câți biți au fost împrumutați pentru o subrețea particulară, de aici și partea cu "variabil" din VLSM.

Subnetizarea VLSM este similară cu cea tradițională în care biții sunt împrumutați pentru a crea subrețele. Formulele folosite la calculul numărului de hosturi pentru fiecare subrețea și la calculul numărului de subrețele create încă se aplică. Diferența este aceea că subnetizarea nu este o activitate singulară. Cu VLSM, rețeaua este mai întâi subnetizată, iar apoi subrețelele sunt subnetizate din nou. Acest proces poate fi repetat de mai multe ori pentru a crea subrețele de dimensiuni diferite.

41. Esență și metode de rutare în rețele [6/340-242].

În rețelele de calculatoare, termenul **rutare** se referă la selectarea căilor într-o rețea, pe care să se trimită anumite date. Rutarea directează drumul pachetelor ce conțin adrese logice dinspre sursă spre destinația finală prin noduri intermediare (numite rutere). Procesul de rutare directează de obicei pe baza unor tabele de rutare pe care le gestionează ruterele, care mențin o înregistrare a celor mai bune rute către diferite destinații din rețea.

Există două mari tipuri de rutare în rețea:

- **Rutarea statică** descrie un sistem care rutează într-o rețea de date în funcție de căi fixe.
- **Rutarea dinamică** construiește dinamic tabelele de rutare, bazându-se pe informațiile purtate de protocoale, permițând rețelei să acționeze în mod aproape automat pentru a evita erori și blocaje în rețea.

Datorită proprietăților sale, rutarea dinamică domină în momentul actual internetul. Avantajele rutării dinamice față de cea statică sunt scalabilitatea și adaptabilitatea. O rețea rutată dinamică poate crește mult mai repede și este capabilă să se adapteze schimbărilor din topologia rețelei aduse tocmai de această creștere sau de erorile din una sau mai multe componente ale rețelei. Într-o rețea dinamică, ruterele învață despre topologia rețelei comunicând cu alte rutere. Rutarea dinamică are însă și dezavantaje, cum ar fi creșterea complexității.

42. Interconectarea în rețele. Protocoale ale stratului Internet [2; 6/30-32].

Scopul inițial al nivelului rețea ("Internet Protocol") era să asigure rutarea pachetelor în interiorul unei singure rețele. Odată cu apariția interconexiunii între rețele, acestui nivel i-au fost adăugate funcționalități de comunicare între o rețea sursă și o rețea destinație.

În stiva TCP/IP, protocolul **IP** asigură rutarea pachetelor de la o adresă sursă la o adresă destinație, folosind și unele protocoale adiționale, precum **ICMP** sau **IGMP**. Determinarea drumului optim între cele două rețele se face la acest nivel.

43. Caracterizarea generală a protocolului IP [2; 6/32-33]

Internet Protocol este un protocol prin care datele sunt trimise de la un calculator la altul prin intermediu Internetului. Fiecare calculator „gazdă”, are pe Internet cel puțin o adresă IP unică, care îl identifică între toate computerele din rețea. Când cineva trimite sau primește informații (de ex.: poștă electronică, pagini web) 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.

44. Caracterizarea generală a protocolului IPv6 [2, 6/51-53].

IPv6 este un protocol de nivel internet TCP/IP (respectiv nivel rețea din Modelul OSI) pentru rețelele cu comutare de pachete, inclusiv pentru Internet.

IPv6 a fost proiectată pentru a oferi fiecărei rețele de pe glob mai multe adrese ce pot fi [rutate](#) în întregul Internet; adresele pot fi folosite pentru o largă varietate de dispozitive, inclusiv telefoane mobile, PDA-uri, vehicule cu suport IP, electrocasnice și multe altele.

45. Trecerea de la IPv4 la IPv6 [2, 6/61-62].

Este probabil că Internetul va folosi IPv4 și IPv6 în paralel pentru o perioadă destul de lungă. Cele două protocoale nu pot comunica direct, fiind nevoie de un gateway dedicat sau de unul din mecanismele de tranziție implementate.

În plus față de asigurarea spațiului mai mare de adrese, IPv6 are următoarele avantaje în comparație IPv4:

- Managementul și delegarea adreselor devine mai ușoară;
- Autoconfigurarea ușoară a adreselor;
- [IPsec](#) încorporat;
- Rutare optimizată;
- Depistarea adreselor duble.

46. Protocoalele ICMP și ECN [2, 6/33-34].

ICMP este un protocol din suita [TCP/IP](#) care folosește la semnalizarea și diagnosticarea problemelor din [rețea](#). Mesajele ICMP sunt încapsulate în interiorul pachetelor [IP](#). Versiunea ICMP pentru IPv4 este adesea cunoscută ca ICMPv4; în schimb [IPv6](#) dispune de un protocol similar cunoscut sub abrevierea ICMPv6.

Probabil cele mai utilizate programe care se bazează pe ICMP sunt [ping](#) și [traceroute](#). Ping trimite mesaje ICMP de tip *echo request* ("cerere de [ecou](#)") către [calculatorul](#) țintă și așteaptă de la acesta mesaje ICMP de tip *echo reply* ("răspuns de tip ecou"). Dacă acestea nu sunt primite, se poate presupune că ceva este în neregulă cu conexiunea dintre cele două calculatoare.

ECN este o extensie a protocolului de Internet și a protocolului de control al transmisiei. ECN permite notificarea end-to-end a congestiei rețelei fără a lăsa pachete. ECN este o caracteristică opțională care poate fi utilizată între două puncte finale activate de ECN atunci când infrastructura de rețea de bază o acceptă.

47. Concepte și protocoale de rutare în Internet [6/340-345].

Rutarea directează drumul pachetelor ce conțin adrese logice dinspre sursă spre destinația finală prin noduri intermediare (numite rutere). Procesul de rutare directează de obicei pe baza unor tabele de rutare pe care le gestionează ruterele, care mențin o înregistrare a celor mai bune rute către diferite destinații din rețea.

Există două mari tipuri de rutare care stau la baza tuturor celorlalte tipuri de rutare: **rutarea statică** (descrie un sistem care rutează într-o rețea de date în funcție de căi fixe) și **rutarea dinamică** (construiește dinamic tabelele de rutare, bazându-se pe informațiile purtate de protocoale, permițând rețelei să acționeze în mod aproape automat pentru a evita erori și blocaje în rețea).

Protocoale cu rutare internă (IGP)

RIP este un protocol mai vechi de rutare cu vectori-distanță

IGRP - protocol de rutare cu starea legăturilor. Este brevetat și acceptat doar pe routere Cisco.

EIGRP - protocol de rutare bazat pe protocolul IGRP, predecesorul său. Este proprietate Cisco.

OSPF - protocol cu starea legăturilor, cu un standard deschis.

IS-IS este un protocol bazat pe OSI

Protocoale cu rutare externă (EGP)

EGP (Exterior Gateway Protocol)

BGP este un protocol de rutare modern, utilizat între sisteme autonome.

48. Caracterizarea generală a rutelor Cisco. Exemple de rutere [2].

Un **ruter** este un dispozitiv hardware sau software care conectează două sau mai multe rețele de calculatoare bazate pe „comutarea de pachete” (packet switching). Ruterele operează la nivelul 3 al modelului OSI (rețea). Aceste rețele pot fi cu fir sau fără fir. Funcția îndeplinită de rutere se numește rutare.

Îndiferent de funcția, dimensiunea sau complexitatea lor, toate modelele de router sunt de fapt calculatoare. Precum și calculatoarele, tablete și echipamentele inteligente, routerele necesită și ele:

- Sisteme de operare (OS)
- Unitățile de procesare centrale (CPU)
- Memoria RAM (Random-access memory)
- Memoria ROM (Read-only memory)

Un router are și o memorie specială care include Flash și memorie NVRAM (nonvolatile random-access memory).

Există mai multe **tipuri de routere** de infrastructură disponibile. De fapt, routerele Cisco sunt proiectate pentru a adresa nevoile următorilor:

- Sucursala - Muncitori de la distanță, companii mici și sucursale de dimensiuni medii. Include Routerele Integrate Cisco 800, 1900, 2900 și 3900 (ISR) G2 (a doua generație).
- WAN - Companii și organizații mari. Include Seria de Switchuri Cisco Catalyst 6500 și Cisco Aggregation Service Router (ASR) 1000.
- Furnizorul de Servicii - Furnizori mari de servicii. Include Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System și Seria de routere 7600.

49. Funcțiile de bază și protocoale ale stratului Transport în Internet [2, 6/28].

[TCP](#), [UDP](#), [RTP](#), [SCTP](#), [SPX](#), [ATP](#), [IL](#)

Transferul fiabil al informației între două sisteme terminale (*end points*) ale unei comunicații. Furnizează controlul erorilor și controlul fluxului de date între două puncte terminale, asigurând ordinea corectă a pachetelor de date. Oferă un serviciu de transport de date care izolează nivelurile superioare de orice specificitații legate de modul în care este executat transportul datelor.

50. Protocolul TCP [2, 6/28-29].

TCP este un protocol folosit de obicei de aplicații care au nevoie de confirmare de primire a datelor. Efectuează o conectare virtuală full duplex între două puncte terminale, fiecare punct fiind definit de către o adresă IP și de către un port TCP.

51. Protocolul UDP [2, 6/29-30].

UDP este un protocol de comunicație pentru calculatoare ce aparține nivelului Transport (*nivelul 4*) al modelului standard OSI. Împreună cu Internet Protocol (IP), acesta face posibilă livrarea mesajelor într-o rețea. Spre deosebire de protocolul TCP, UDP constituie modul de comunicație fără conexiune.

52. Alegerea între protocoalele TCP și UDP *2+.

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge sequencing	No acknowledgment

53. Numere de porturi și perechi de socluri în Internet [2].

Porturile și soclurile reprezintă mecanismul prin care se realizează legătura cu un server. **Porturile** reprezintă o poartă la care sunt primiți clienții pentru un anumit serviciu. De exemplu la aceeași adresă se pot oferi diferite servicii, acestea oferindu-se la porturi diferite. Același calculator (cu o singură adresă IP) poate să ne ofere oricate servicii dorește. Clienții care apelează la serviciile acestui calculator vor utiliza aceeași adresă, indiferent la care serviciu apelează, și toți clienții care doresc utilizarea unui anumit serviciu vor utiliza același port.

Un **număr de port** este un număr înreg din intervalul 1-9999. IETF definește serviciile oferite pe porturile 1-1024. De obicei serviciile HTTP sunt oferite la portul 80, cele de FTP la portul 21, Telnet la 23 etc.

Un **soclu** este de fapt un nod abstract de comunicație. Soclurile reprezintă o interfață de nivel scăzut pentru comunicarea în rețea. Soclurile permit comunicarea între procese aflate pe același calculator sau pe calculatoare diferite din rețea. Mecanismul de socluri a fost definit prima dată în BSD UNIX. Java suportă trei tipuri de socluri. Clasa Socket utilizează un protocol orientat pe conexiune (TCP), clasa DatagramSocket utilizează protocolul UDP la nivelul transport, care este un protocol neorientat pe conexiune. O altă variantă a DatagramSocket este MulticastSocket utilizat pentru a trimite date deodată la mai mulți receptori. Soclurile utilizează fluxuri de date (streamuri) pentru a trimite și a recepționa mesaje.

54. Funcțiile de bază și protocoale ale stratului Aplicație în Internet [6/26-28, 74-76, 78-80].

[HTTP](#), [SMTP](#), [SNMP](#), [FTP](#), [Telnet](#), [SIP](#), [SSH](#), [NFS](#), [RTSP](#), [XMPP](#), [Whois](#), [ENRP](#)

realizează interfața cu utilizatorul și interfața cu aplicațiile, specifică interfața de lucru cu utilizatorul și gestionează comunicația între aplicații.

55. Protocoalele de e-poștă SMTP, POP și IMAP [2, 6/81-84].

SMTP este un protocol simplu din suită de protocoale de Internet, care este folosit la transmiterea mesajelor în format electronic în rețea de calculatoare. SMTP folosește portul de aplicație 25 TCP și determină adresa unui server SMTP pe baza înregistrării MX (*Mail eXchange*) din configurația serverului DNS.

Protocolul SMTP specifică modul în care mesajele de poștă electronică sunt transferate între proces 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.

POP este unul din protocoalele utilizate de un calculator gazdă pentru recepționarea poștei electronice (e-mail).

IMAP permite accesul la mesaje din foldere de e-mail de pe un server. Spre deosebire de POP, care este proiectat pentru a transfera și șterge e-mail-urile de pe server, scopul IMAP este de a le stoca pe toate pe server, pentru a putea fi oricând accesate din orice loc.

56. Accesul și transferul de hypertexte WWW în Internet [6/84-87].

WWW este totalitatea site-urilor / documentelor și informațiilor de tip [hipertext](#) legate între ele, care pot fi accesate prin rețeaua mondială de [Internet](#). Documentele, care rezidă în diferite locații pe diverse calculatoare server, pot fi regăsite cu ajutorul unui identificator univoc numit [URL](#). Hipertextul inclusiv imagini etc. este afișat cu ajutorul unui program de navigare în web numit [browser](#), care [descarcă paginile web](#) de pe un [server](#) web și le afișează pe un terminal „client” la utilizator.

57. Serviciul VoIP [6/88-92].

VoIP (*Voice over Internet Protocol*, **VoIP**), numită și **Telefonie IP** sau **Telefonie Internet** este procesul de transmitere a conversațiilor vocale umane prin legături de date de tip [IP](#) sau prin rețele în care este folosit acest protocol.

Avantajul principal al VoIP față de [telefonia clasică](#) este prețul redus, datorat faptului că se utilizează rețeaua IP care poate fi folosită în același timp și pentru alte servicii, precum navigare web, e-mail, e-banking și multe altele. Utilizatorul își poate folosi serviciul VoIP indiferent de locul unde se conectează la Internet.

58. Protocoalele de securizare a conexiunilor SSL și TLS [6/101-102].

Secure Sockets Layer (SSL) și **Transport Layer Security** (TLS), succesorul său, sunt protocoale criptografice care permit comunicații [sigure](#) pe [Internet](#). Între SSL 3.0 și TLS 1.0 există anumite diferențe, dar protocolul rămâne aproximativ același.

SSL reprezintă un [protocol web](#) dezvoltat pentru a transmite fără risc documente private prin [Internet](#). Pentru a cripta datele, SSL utilizează un sistem criptografic cu două chei: una publică, cunoscută de oricine, și una privată, secretă, cunoscută numai de destinatarul mesajului. Majoritatea [browserelor](#) web suportă SSL, și multe [situri web](#) utilizează protocolul de utilizator pentru a transmite informații confidențiale, cum ar fi numerele de [carduri de credit](#). Prin convenție, [URL](#)-ul care are nevoie de o conexiune SSL începe cu [https](#): (în loc de [http](#):).

TLS este un protocol criptografic care asigură securitatea comunicațiilor end-to-end prin rețele și este utilizat pe scară largă pentru comunicații pe internet și tranzacții online. Este un standard IETF destinat să prevină interceptarea, manipularea fraudelor și falsificarea mesajelor. Aplicațiile obișnuite care utilizează TLS includ browserele Web, mesageria instantanee, e-mail și voice over IP.

59. Protocoalele DNS și DHCP [6/103-107].

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](#).

Caracteristicile sistemului de nume (DNS) sunt:

- 1) folosește o structură ierarhizată;
- 2) delegă autoritatea pentru nume;
- 3) [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.

DHCP (**Dynamic Host Configuration Protocol**) este un [protocol de rețea](#) de calculatoare folosite de gazde (clienți DHCP) care atribuie adrese IP și alte informații de configurare de rețea importante în mod dinamic. DHCP automatizează alocarea parametrilor de rețea la dispozitive de către unul sau mai multe [fault-tolerant](#) servere DHCP. Chiar și în rețele mici, DHCP este folositor, deoarece simplifică adăugarea unor noi echipamente în rețea.

60. Tehnologiile de rețea ISDN [9].

Într-o rețea ISDN nodurile de comunicație realizează comutarea de canale, pentru transmiterea vocii și a datelor la distanță, cât și comutarea de pachete pentru transmisia de informații de serviciu.

Se folosesc următoarele **variante de acces** – tuburi de biți:

- ♣ BRI – acces de bază 2B+D
- ♣ PRI – acces primar 30B+D (se folosește în Europa).
- ♣ PRI – acces primar 23B+D (SUA, Canada, Japonia);

Canalele B sunt destinate transferului de voce și date prin comutare de canale, iar cele D – transferului de informații de serviciu prin comutarea de pachete.

Rețelele de tehnologie ISDN:

- 1) prima implementare – 1987 (rețeaua NUMERIS în Franța);
- 2) sunt conforme modelului OSI ISO (cuprinde straturile 1-3); și cu setul de protocoale X.25 al ITU-T;
- 3) sunt destinate transmiterii vocii și datelor pe fire de cupru telefonice ordinare;
- 4) folosesc comutarea de canale pentru voce și date și comutarea de pachete pentru informații de serviciu;
- 5) viteze de transfer date de până la 2 Mbps;
- 6) serviciile relativ scumpe;

61. Tehnologiile de rețea Frame Relay [9].

FR folosește comutarea de pachete cu circuite virtuale DLCI (data-link connection identifier). O rețea FR constă din noduri de comunicație FR, interconectate prin trunchiuri de comunicație. Stațiile se conectează la o rețea FR prin intermediul concentratoarelor de date (FRAD) sau direct la nodurile de comunicație.

Rețelele de tehnologie Frame Relay:

- 1) primele implementări – 1989;
- 2) sunt conforme modelului OSI ISO (cuprind straturile 1-2 OSI/ISO)
- 3) sunt orientate la folosirea canalelor de calitate înaltă;
- 4) efectuează detectarea de erori, dar nu și corectarea acestora.
- 5) pot opera prin canale D ale BRI și PRI;
- 6) operează la viteze de transfer date de până la 45 Mbps; servicii ieftine, mai ieftine decât cele X.25 și ISDN;
- 7) sunt folosite pentru conectarea rețelelor locale la rețele magistrale de transfer date;
- 8) pot fi folosite și ca rețele magistrale de interconectare a stațiilor și rețelelor locale;

62. Tehnologia de rețea ATM [9].

Rețelele ATM (Asynchronous Transfer Mode) realizează o tehnologie de comutare și transfer date ultrarapidă pentru utilizare și interconectarea transparentă a rețelelor locale și de arie largă. ATM se bazează pe tehnologia de comutare pachete Cell Relay. Tehnologia ATM suportă și transferul de date în regim izocron. Ca mediu de transmisie a fost utilizată fibra optică, cablul torsadat și coaxial.

Rețelele de tehnologie ATM:

- 1) primele implementări – 1992; orientate la folosirea canalelor de calitate înaltă;
- 2) sunt conforme modelului OSI ISO, cuprind straturile 1-2 OSI/ISO și stratul ATM Adaptation Layer;
- 3) destinate transferului oricărui tip de date, inclusiv trafic izocron (date, voce și video – triple play);
- 4) operează la viteze de transfer date de până la 10 Gbps;
- 5) folosesc metoda de comutare cu circuite virtuale, folosesc căi virtuale (Virtual path);
- 6) dimensiunea cadrelor (celule) este fixă – 53 octeți, din care 5 octeți pentru antet;
- 7) efectuează detectarea de erori în date, dar nu și corectarea acestora. Pachetele eronate se aruncă;
- 8) calitatea înaltă a serviciilor, inclusiv fiabilitatea de funcționare, servicii relativ scumpe;
- 9) sunt folosite pentru rețele magistrale de transfer date

63. Tehnologia de rețea MPLS [9].

Multiprotocol Label Switching îmbină flexibilitatea rețelelor IP cu beneficiile oferite de tehnologiile orientate pe conexiune ca ATM.

Alegerea următorului nod pentru transmiterea de mai departe a pachetului: La prima etapă, pachetele se grupează în Forwarding Equivalence Classes – FEC. La a doua etapă, pentru fiecare FEC se determină canalul de

ieșire. Toate pachetele, ce aparțin unei clase FEC concrete și pleacă de la același nod (cu aceeași etichetă), vor urma prin rețea aceeași cale comutată prin etichete.

Rețelele de tehnologie MPLS :

- 1) primele implementări – 1999 (1996);
- 2) sunt relativ conforme modelului OSI ISO; cuprind straturile 1-3 OSI/ISO. Se consideră de nivel 2,5 OSI;
- 3) sunt destinate transferului oricărui tip de date, inclusiv trafic izocron (date, voce și video – triple play);
- 4) folosesc metoda de comutare prin etichete (LSP).
- 5) pot transporta date pentru rețele de diferite tehnologii (multiprotocol);
- 6) operează inclusiv cu IP, FR și ATM, fără a necesita modificări în echipamente;
- 7) oferă calitate înaltă a serviciilor; sunt flexibile; sunt folosite pentru rețele magistrale de transfer date