Curs 1: Prezentare

Fundamentele retelelor de calculatoare
(Introduction to Networks)

Silviu Vasile
vsl@fmi.unibuc.ro

Planificare:

- Curs 1: Prezentare
- Curs 2: Retele de calculatoare - concepte generale
- Curs 3: Configurare IOS
- Curs 4: Protocoale in retelele de calculatoare
- Curs 5: Stiva OSI: Network Access
- Curs 6: Stiva OSI: Ethernet
- Curs 7: Stiva OSI: Network Layer
- Curs 8: Adresarea IP
- Curs 9: Subnetare
- Curs 10: Stiva OSI: Transport Layer
- Curs 11: Stiva OSI: Application Layer
- Curs 12: Managementul si mentenanta retelelor de calculatoare

Examen

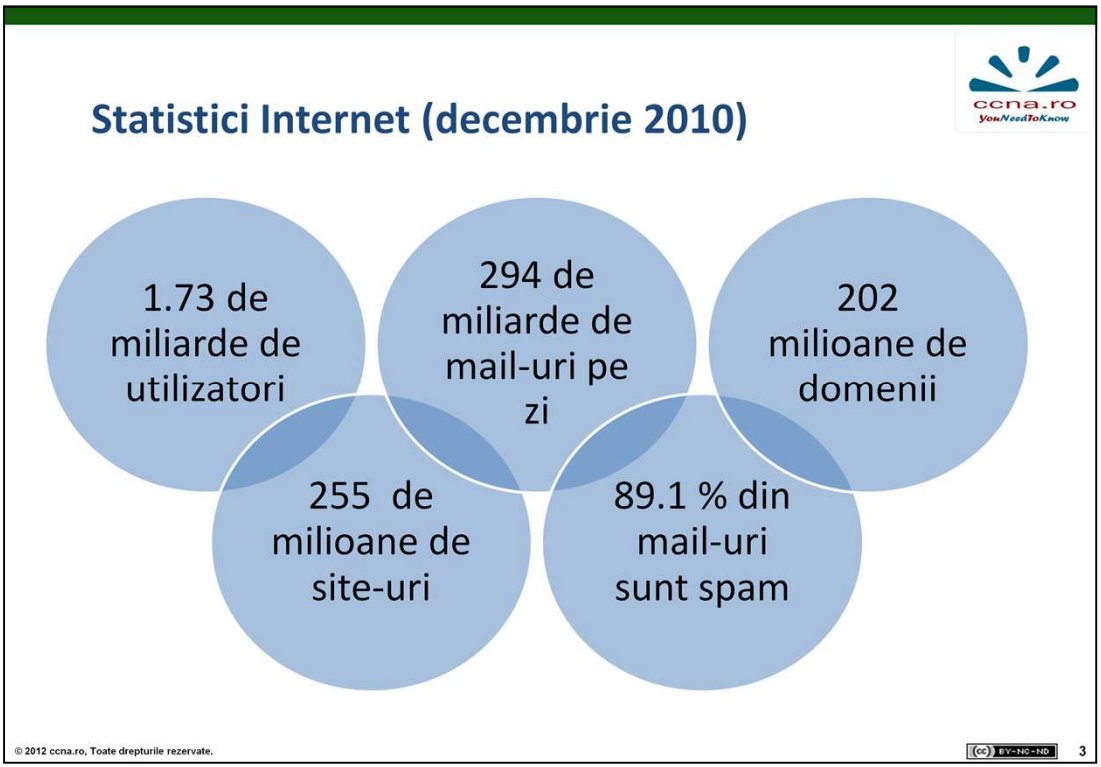
- Curs
- Laborator
- Platforma on-line

- Promovare - doar daca la oricare din cele 3 componente se obtin note de promovare;
- Prezenta optionala la curs, obligatorie la laborator;
- Examen – proba scrisa
- Materiale/teme la adresa: http://193.226.51.37

Capitolul 2:
Comunicații pe rețea

Obiective

- Platforma de comunicație
- LAN/WAN
- Protocoale
- Modele ierarhice
- Adresare

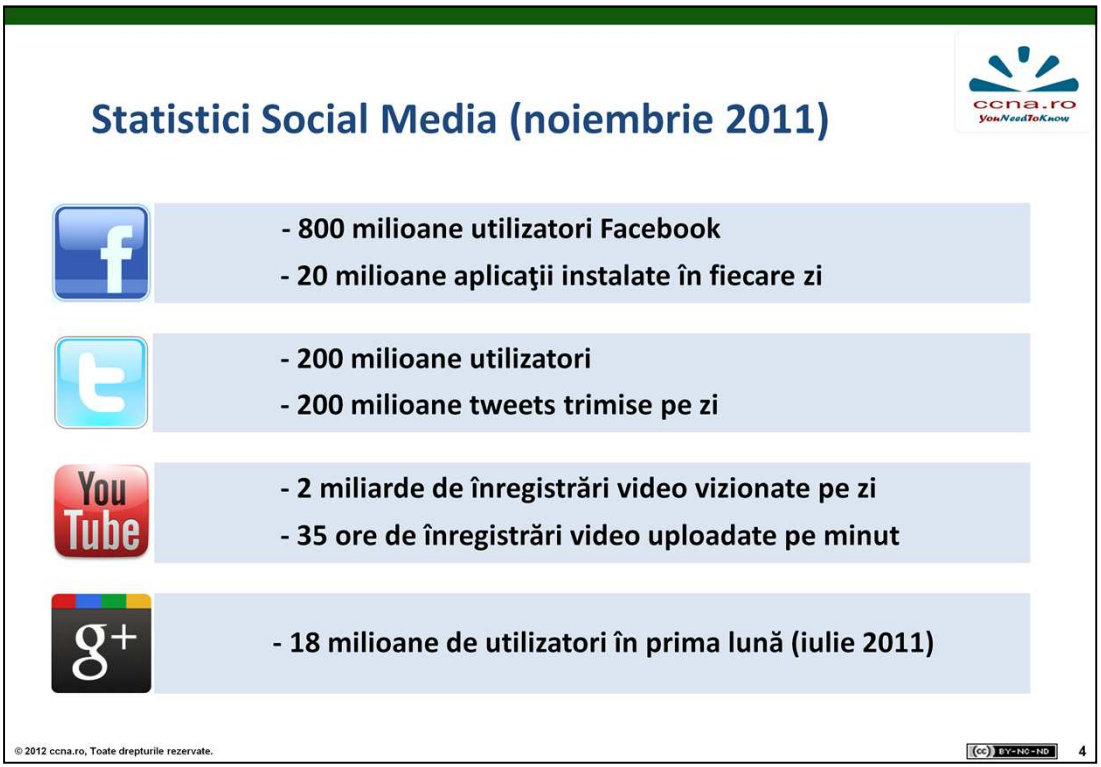


Termen necunoscut unui public larg de aproximativ un deceniu, Internetul a devenit azi una dintre principalele modalități de comunicare și de informare, a lumii moderne.

Statisticile actuale în legătură cu numărul de utilizatori și serviciile oferite de această rețea globală ne face să ne punem întrebarea ,,Cum și unde a luat naștere Internetul?".

Răspunsul este ARPAnet, o tehnologie dezvoltată în anul 1969 de către NASA sub forma unui proiect de cercetare. Datele sunt transmise sub formă de pachete, folosind tehnici de comunicare numite ,,protocoale de rețea".

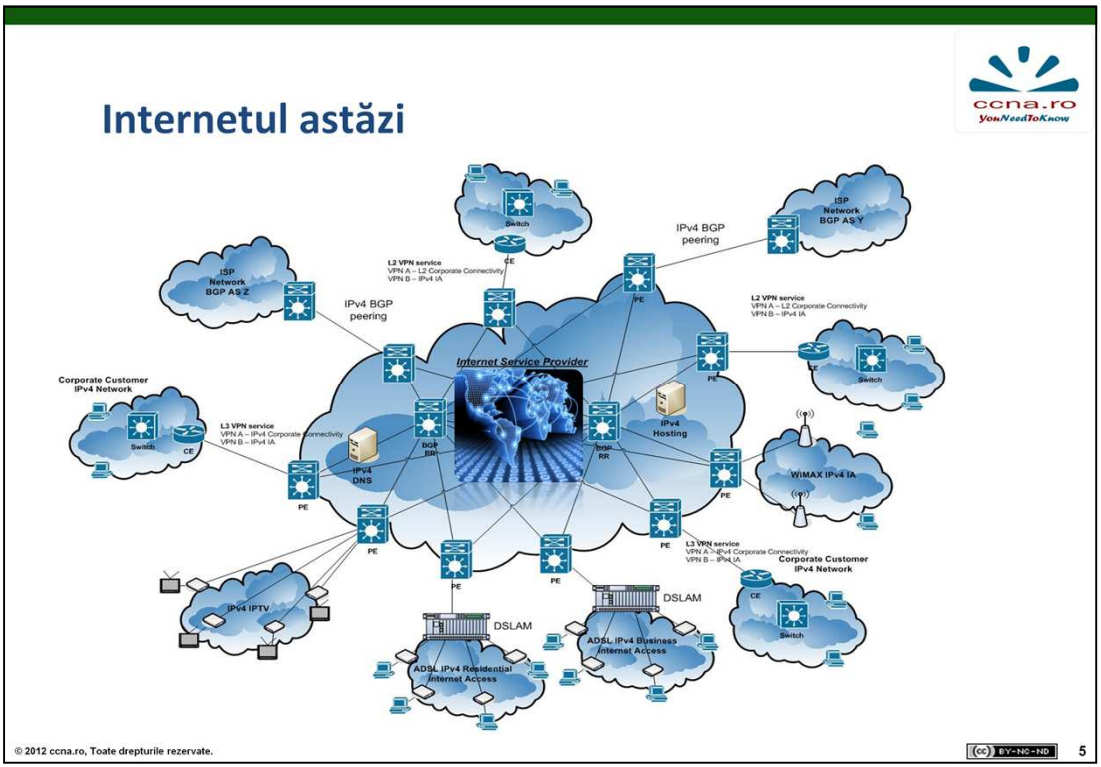
Una dintre cele mai importante părți ale Internetului a fost construită de către guvernul Statelor Unite pentru a permite cercetătorilor universitari să poată avea acces la centrele regionale de calcul.



În această lume a tehnologiei, unde Internetul este principalul coordonator al tuturor activităților umane, domeniul Social Media este cel mai des utilizat, conform unor statistici efectuate la nivel mondial.

Câteva cifre despre Social Media în 2011 la nivel mondial, conform prezentării de mai jos:

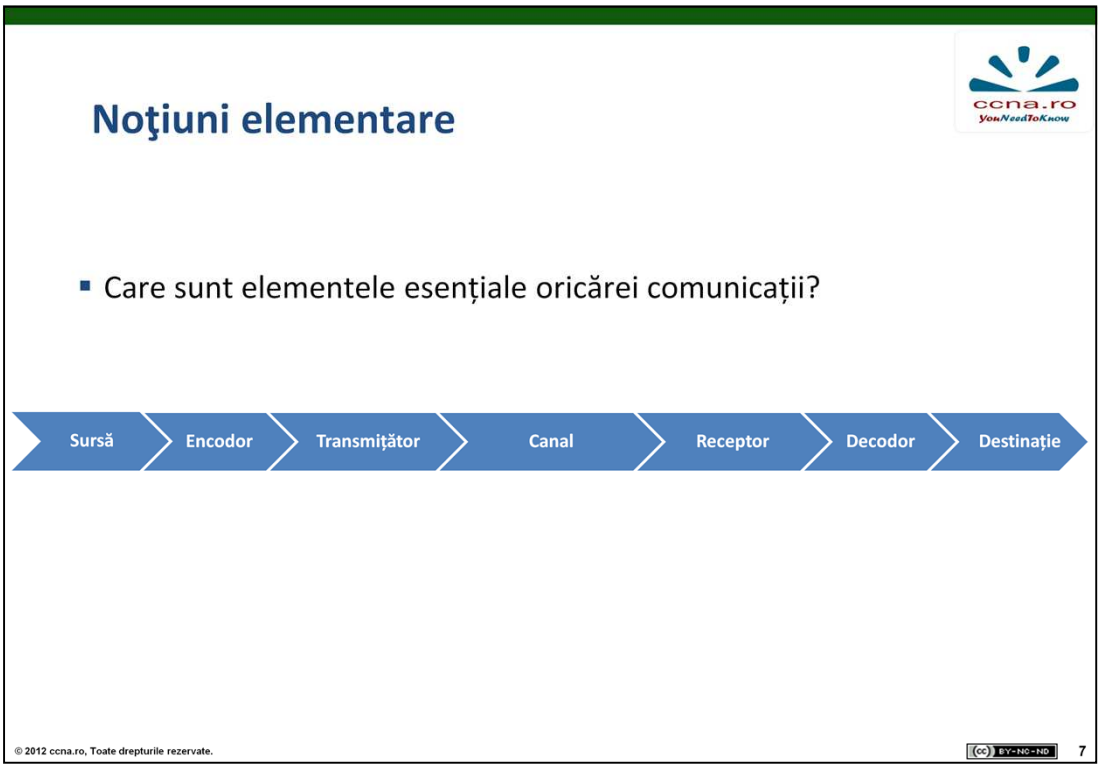
- 147 milioane bloguri (126 milioane în 2011)
- 800 milioane utilizatori Facebook
- 250 milioane utilizatori Twitter
- 150 milioane profile de Linkedin
- 2 miliarde videoclipuri vizionate pe Youtube într-o singură zi
- 40 milioane utilizatori de Flickr
- 45 milioane vizitatori lunari ai SlideShare



Astăzi, Internetul este folosit din ce în ce mai mult oferind posibilități multiple și diverse precum: accesarea unor pagini web, video streaming, instant messenger, verificarea conturilor bancare, cumpărături/vânzări online, jocuri, muzică, referate, bilete de avion, evenimente recente, informații despre locuri de muncă, etc. Analizând aceste caracteristici se observă că el a devenit o parte integrantă a societații noastre și a economiei.

Internetul este cel ce a adus informației un sens nou, aducând o abundență a acesteia, oferind libertatea de a naviga și selecta conținutul dorit. Un exemplu ce susține această afirmație este acela conform căruia majoritatea universitaților şi bibliotecilor oferă acces la Internet. În mod tradițional era nevoie de un computer pentru a te putea conecta la o rețea, fie ea locală sau globală, însă în prezent datorită progresului tehnologic există aceleași posibilități chiar și cu ajutorul televizorului sau al telefonului mobil.

Platforma de comunicație



Charles E. Osgood spunea: „O comunicare cu un sistem, respectiv o sursă, influențează un alt sistem, în speță un destinatar, prin mijlocirea unor semnale alternative care pot fi transmise prin canalul care le leagă”.

Elementele unei comunicări sunt:

- Emițător - cel care inițiază comunicația
- Receptor - cel care participă la comunicație
- Canal - mediul de transmisie
- Mesaj - informațiile efective

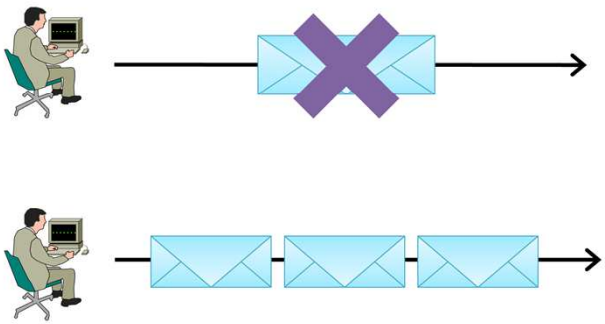
Emițătorul este inițiatorul comunicării, cel care elaborează mesajul. Tot el alege canalul de comunicare și limbajul astfel încât receptorul să-i înțeleagă mesajul formulat.

Mesajul reprezintă forma fizică în care emițătorul codifică informația, el fiind supus unui proces de codificare și decodificare.

Comunicația în plan tehnic (1)

- La baza comunicației pe rețea stau două principii fundamentale:

1. Segmentarea 2. Multiplexarea



La baza comunicației din rețea stau două mari principii:

- Segmentarea
- Multiplexarea

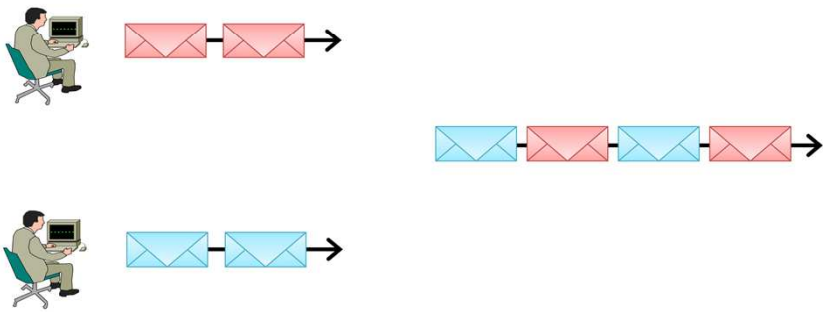
Segmentarea de pachete este un proces de divizare a unui pachet de date în unităţi mai mici pentru transmiterea lor eficientă prin reţea.

Segmentarea poate fi necesară în mai multe scenarii:

- În cazul în care pachetele de date au dimensiune mai mare decât dimensiunea maximă acceptată de reţea
- În cazul în care reţeaua nu este sigură şi se dorește împărţirea informaţiilor în segmente mai mici, pentru a maximiza probabilitatea ca fiecare dintre ele să poată fi livrate corect la destinație

Comunicația în plan tehnic (2)

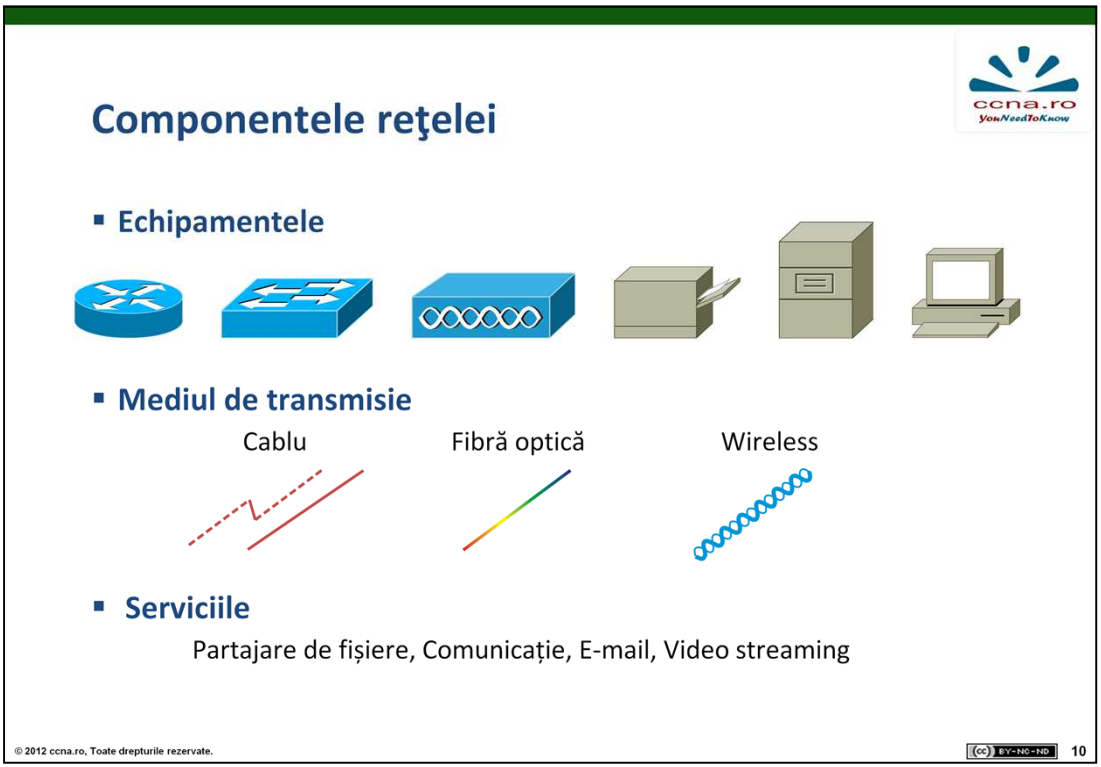
- La baza comunicației pe rețea stau două principii fundamentale:
  1. Segmentarea
  2. Multiplexarea



Multiplexarea este procedeul prin care mai multe canale de comunicare sunt combinate într-un singur canal fizic, în timp ce demultiplexarea este procesul invers.

Există numeroase tehnici de multiplexare, printre care se numără:

- FDM (Frequency Division Multiplexing): fiecare canal primește o anumită bandă de frecvență
- TDM (Time Division Multiplexing): informațiile transmise de fiecare canal li se oferă o cuantă de timp predefinită
- Statistical multiplexing: banda este alocată în mod dinamic fiecarui canal ce dorește să transmită informații la un moment dat
- DWDM (Dense Wavelength Division Multiplexing): este un mod de multiplexare dezvoltat pentru fibra optică, fiind echivalentul optic al multiplexării FDM



Rețeaua este un ansamblu de două sau mai multe echipamente legate între ele printr-un mediu de transmisie cu scopul de a schimba informații între ele.

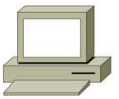
Echipamentele sunt o componentă elementară a unei rețele, ele având drept rol inițierea conexiunii și să se asigure că informația ajunge cu succes la destinație. După rolul pe care îl îndeplinesc, deosebim două categorii: echipamente terminale sau „end devices” și echipamente intermediare sau „intermediary devices”.

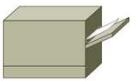
Interconectarea echipamentelor se realizează prin intermediul unui mediu de transmisie:

- Cablu de cupru
- Fibra optică
- Unde electromagnetice

Echipamente terminale (end devices)

- Exemple:
  - Computere (staţii de lucru, laptopuri, servere de fişiere, servere web)
  - Imprimante
  - Telefoane VoIP
  - Camere de securitate
  - PDA-uri
- Host
- Sunt de obicei controlate direct de un utilizator
- Reprezintă fie sursa, fie destinaţia unei comunicaţii pe reţea





Echipamentele terminale sunt acele componente ale rețelei cu care utilizatorul intră în contact direct:

- Computerele
- Telefoanele
- PDA-urile
- Imprimatele
- Camere video

În majoritatea cazurilor aceste dispozitive reprezintă fie sursa, fie destinația informației transmise pe rețea. Termenul sub care sunt întâlnite aceste echipamente în cărțile de specialitate de rețelistică este „host”. Un „host” este un dispozitiv dotat cu o placă de rețea care îi asigură conexiune fizică între mediul de transmisie și magistrala internă a sistemului.

Echipamente intermediare

- Exemple:
  - Ruter
  - Switch
  - Firewall

- Facilitează comunicaţia între echipamentele terminale
- Procesele ce rulează pe echipamentele intermediare:
  - Iau decizii legate de calea pe care urmează să transmită datele
  - Redirecţionează fluxul de date pe căi alternative în cazul căderii unei legături
  - Regenerează şi retransmit semnalele
  - Permit sau împiedică fluxul de date conform setărilor de securitate

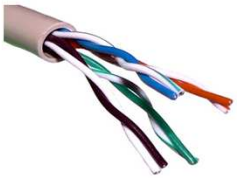
Comunicarea dintre echipamentele terminale nu ar fi posibilă fără existența unor echipamente intermediare, rolul lor fiind de a asigura conectivitatea şi lucrează ,,în spatele scenei" pentru a se asigura că fluxurile de date parcurg drumul corect de la sursă către destinație.

Aceste echipamente leagă dispozitive terminale diferite la rețea și le asigură posibilitatea de a accesa resurse locale sau globale.

Exemple de dispozitive de reţea intermediare:

- Ruter
- Switch
- Hub
- AP Wireless
- Firewall

Mediul de transmisie



- Transformarea biţilor în semnale este strâns legată de mediul fizic
- Alegerea mediului de transmisie ia în calcul:
  - Distanța maximă între două puncte din rețea
  - Interferența din mediu
  - Cantitatea de informații ce trebuie transmisă
  - Costul implementării

Mediile de transmisie au ca principală unitate de organizare a datelor biții. Biții pentru a fi transmiși printr-un canal de comunicație au nevoie de mediu fizic.

Cupru:

- Cablu coaxial: foarte folosit până la jumatatea anilor ’90
- Cablu torsadat: STP şi UDP, transferul de date la până 100 m

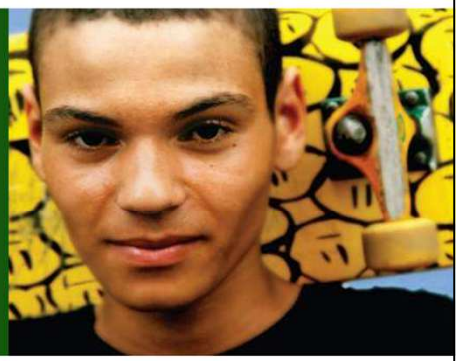
Fibră optică:

- Multimod (multi-mode): permite transmisia informației prin reflexie în pereții „core”-ului
- Monomod (single-mode): permite transmisia informației fără reflexie, fapt care permite distanțe mai mari de transmisie decât cea multimod

Unde electromagnetice: standardele wireless existente sunt a, b, g, n.

LAN, WAN,

Internetwork



Tipuri de Rețele

- Rețelele pot fi clasificate după:
  - Aria geografică pe care se întind
  - Numărul de utilizatori
  - Tipul de servicii asigurate
- În funcție de aceste criterii o rețea poate fi:
  - **LAN** (Local Area Network)
  - **MAN** (Metropolitan Area Network)
  - **WAN** (Wide Area Network)

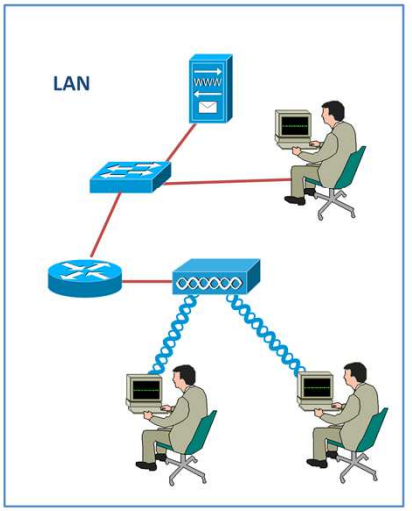
O rețea este reprezentată de o interconectare între mai multe dispozitive. Clasificarea se realizează în funcție de aria geografică și numărul de utilizatori:

- PAN (Personal Area Network) - imprimante, echipamente fax, telefoane
- LAN (Local Area Network)
- CAN (Campus Area Network)
- MAN (Metropolitan Area Network) - conectează două sau mai multe rețele de tip LAN/CAN și acoperă o suprafață de dimensiunea unui oraș
- WAN - Wide Area Network

Interconectarea tuturor acestor rețele reprezintă „Internetul” de azi.

LAN

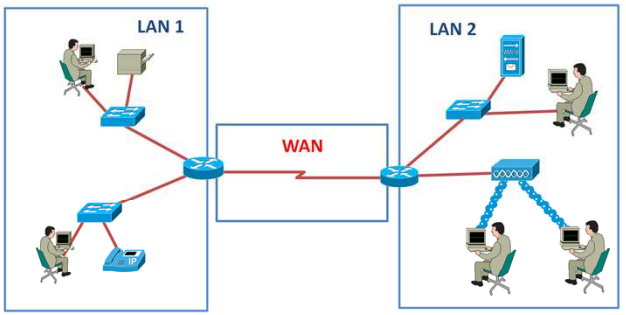
- Arie geografică restrânsă
- Management comun
- Politică de access și securitate uniformă



Rețele cu dimensiuni mici sau foarte mici, pot fi considerate următoarele:

- PAN (Personal Area Network) - imprimante, echipamente fax, telefoane, PDA
  - sunt echipamente de tip scanner
  - dimensiunea medie a rețelei este de 4-6 metri
- LAN (Local Area Network) - conexiunile se pot face prin cablu sau wireless
- Echipamentele pasive funcționează de regulă cu o lățime de bandă de aproximativ 100 Mbps
- CAN (Campus Area Network) - campusul unui colegiu, complexe industriale sau baze militare

WAN



- Arie geografică mare
- Interconectează multiple LAN-uri și MAN-uri
- Nu este obligatoriu să se afle sub același management

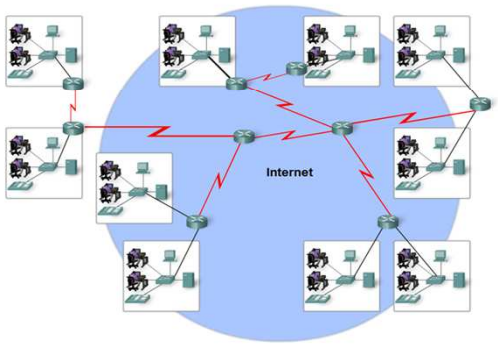
Un WAN este un ansamblu de două sau mai multe LAN-uri, principala diferență fiind că WAN-ul nu are o limitare spațială. WAN-urile pot fi extinse prin intermediul liniilor telefonice, cablurilor de fibră optică sau link-urilor prin satelit, astfel se poate afirma că Internetul este cel mai mare WAN.

Din punct de vedere al administrării și managementului, WAN-ul nu poate fi condus de o singură entitate care să aibă control suprem al acestuia.

Din moment ce el este alcătuit din multiple LAN-uri și MAN-uri, nu poate să aibă nici aceleași politici de securitate. WAN-ul este cea mai complexă și dezvoltată rețea din lume.

Internet

- Internetwork
  - Interconectarea unui număr mare rețele publice pe o arie globală
- Intranet
  - Interconectarea unor rețele private cu access restricționat pe o arie globală
- Internet
  - Este rețeaua de tip Internetwork a ISP-urilor (Internet Service Provider)

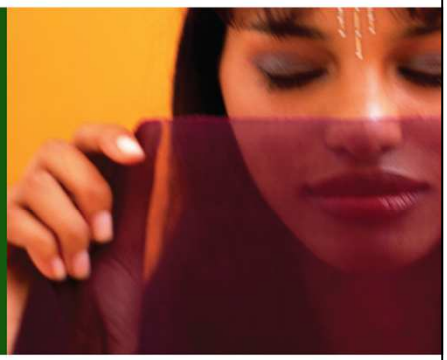


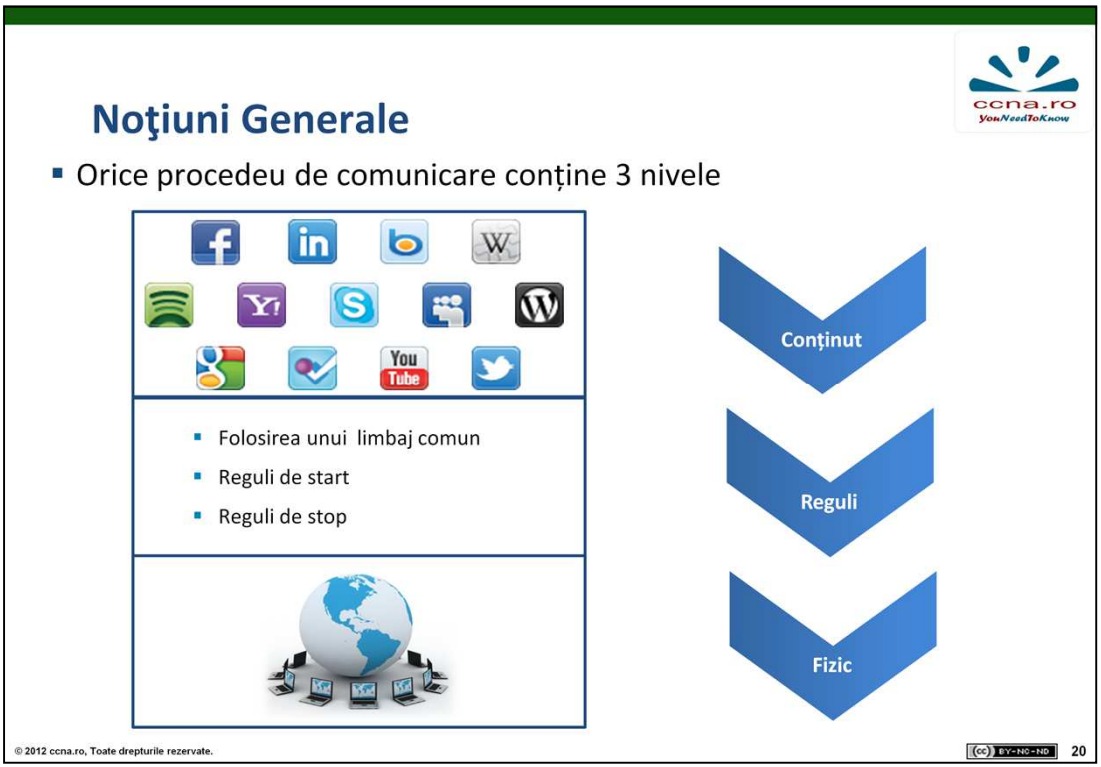
Într-o definiție succintă se poate considera că Internetul este cea mai mare rețea globală aflată în continuă creștere. Însă el este mai mult decât un WAN, constituind o rețea de rețele (comerciale, academice, militare, educaționale, universitare, etc.) și în plus, un imens mediu informațional ce oferă servicii și resurse din domenii vaste.

Acest sistem mondial de rețele interconectate aduce după sine posibilitatea ca utilizatorii situați în zone diferite ale planetei să socializeze, astfel Internetul devenind ce mai mare comunitate social-economică a lumii.

Socializarea prin intermediul Internetului, se poate realiza prin diferite moduri: forum-uri, blog-uri (prin intermediul web hosting) sau prin intermediul aplicațiilor dedicate: aplicații ce suportă Voice over IP, sau doar comunicația peste IP.

Protocoale

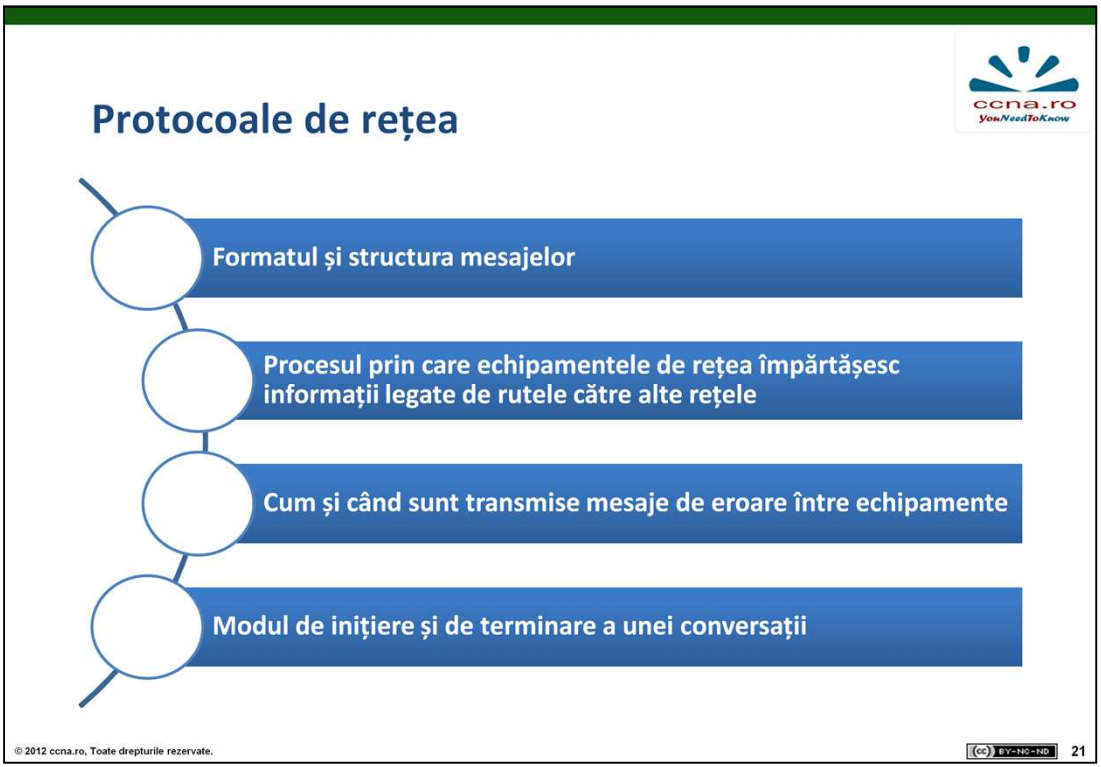




Un protocol reprezintă un standard sau o convenţie asupra modului de desfăşurare a unui anumit lucru, în cazul reţelelor, protocoalele permit echipamentelor să comunice între ele printr-un limbaj comun.

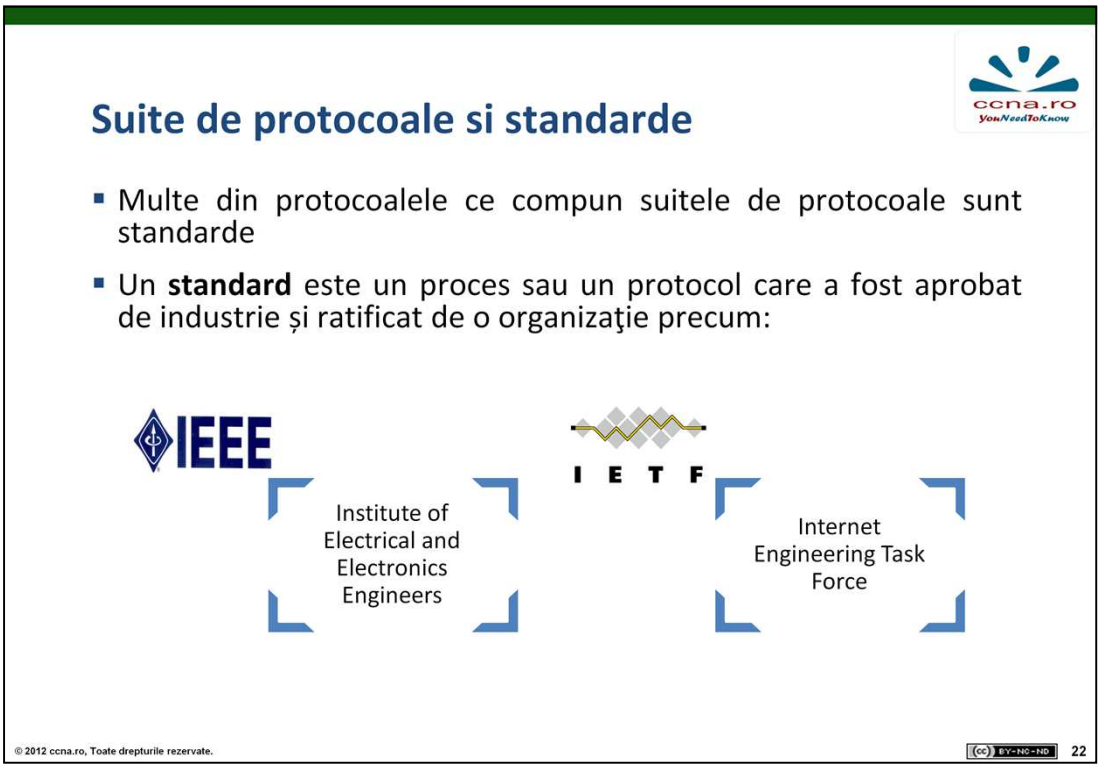
Prin model ierarhic se înţelege o suită (stivă) de protocoale ce lucrează împreună. Sarcinile şi activităţile asociate diferitelor nivele ale modelului, sunt îndeplinite de către protocoale implementate să funcționeze la respectivul nivel.

Fiecare nivel din stivă îndeplinește funcții diferite, ceea ce înseamnă că fiecare nivel administrează funcționalități diferite asupra pachetelor.



Protocoalele nu sunt identice din punctul de vedere al eficienţei, vitezei de lucru, consumului de resurse (în funcţie de dimensiunea antetului, de exemplu), uşurinţei în instalare și administrare.

Diferenţele sunt date de tipul reţelei, tipul infrastructurii acesteia, clienţilor din reţea Windows, Novell Netware, Apple Talk, tipul de echipamente existent și modul cum este utilizat protocolul.



În momentul în care este implementat un protocol, principala dificultate care se întâlnește este găsirea unui limbaj comun pentru a putea schimba informații.

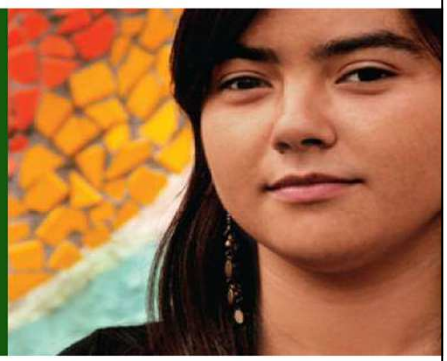
Rezolvarea acestei dificultăți presupune adoptarea unor standarde globale. Bazele stadardelor fiecărui protocol sunt descrise în documente denumite RFC (Request for Comments).

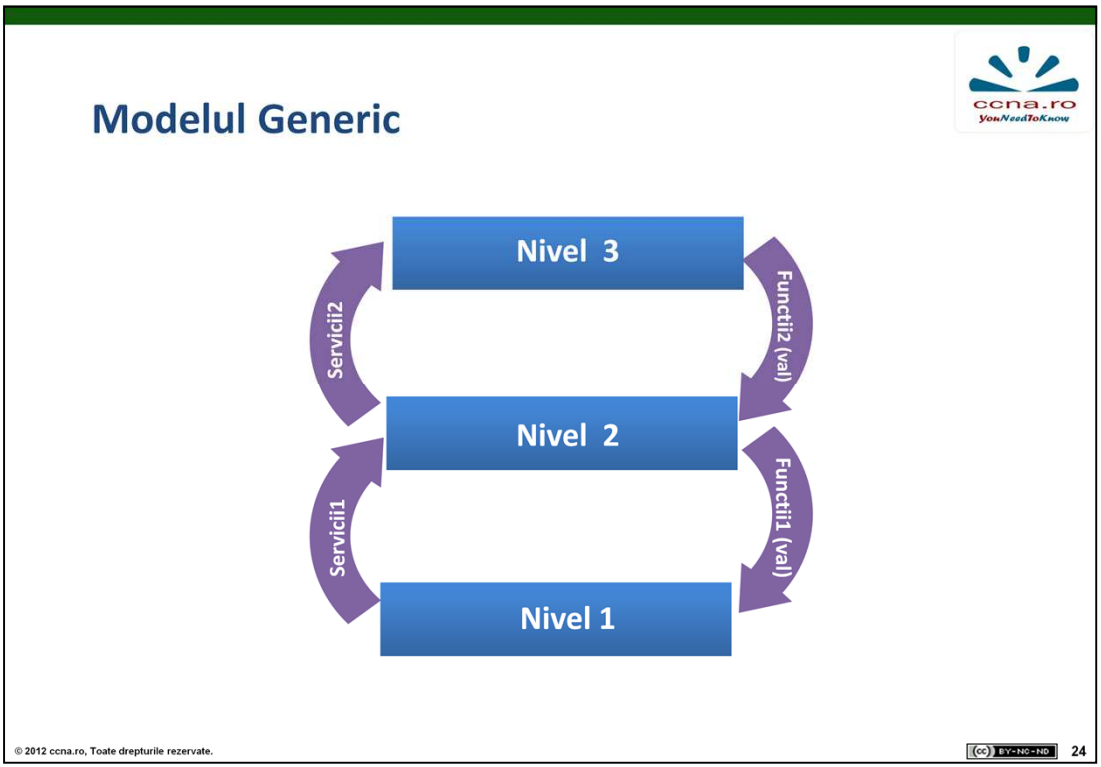
RFC-urile sunt aprobate și întreținute de două mari instituții: IEEE (Institute of Electrical and Electronics Engineers) și IETF (Internet Engineering Task Force).

Locul în care se pot găsi informații cuprinzătoare privind implementarea protocoalelor este la adresa: www.ietf.org/rfc.html.

Modele ierahice:

stive de protocoale





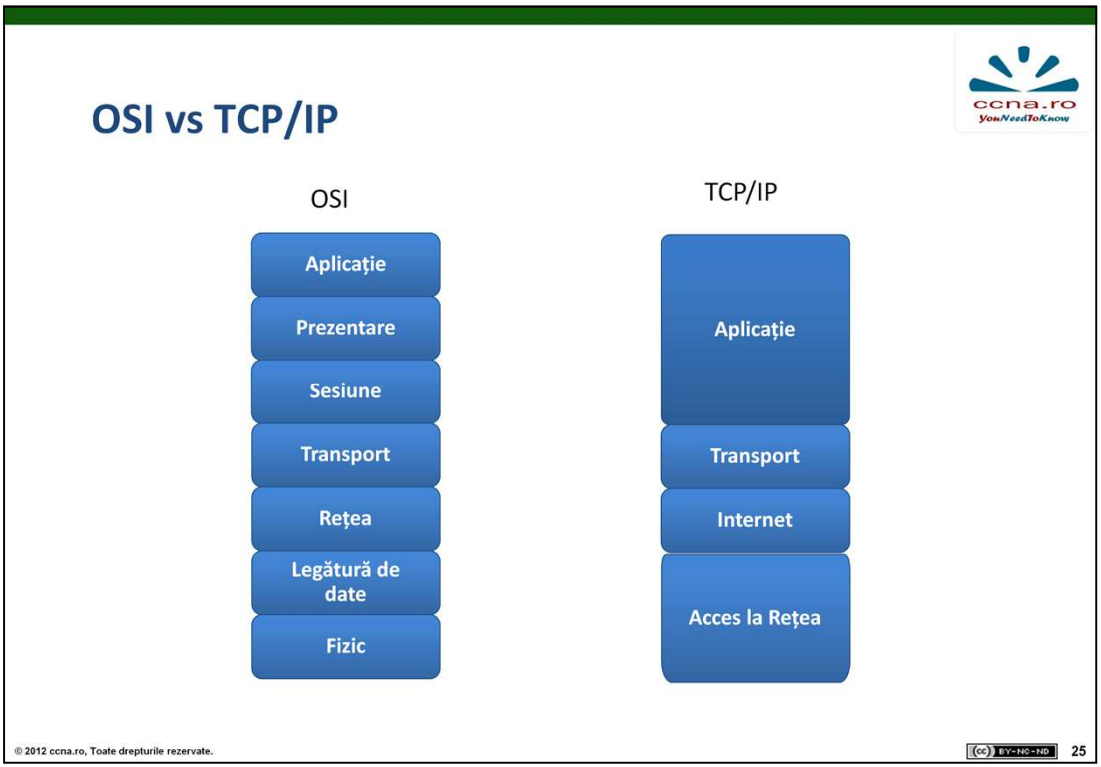
Protocolul de la fiecare nivel se implementează independent de nivelele vecine.

Sunt păstrate constante următoarele aspecte:

- Serviciile oferite nivelului superior
- Modul cum se apelează nivelul inferior

La nivelul 3 se adaugă adresă IP sursă și destinație, în timp ce la nivelul 2 adresa MAC, care este formată din două câmpuri: OUI care este echivalent cu *Company ID* și *Equipment ID*, fiecare având 24 de biți, în total alcătuind adresa MAC.

Nivelul 1 este cel care convertește informația în biți și o trimite pe mediu sub formă de semnal electric, astfel încât datele să fie transmise între echipamente.



În rețelistică când se vorbește de nivel al unei stive, se face referire la nivelul la care se află acesta în stivă. Se poate spune că cele două stive sunt identice din punct de vedere al funcționării, numele fiind diferit:

- *Open Systems Interconnection* – apărut 1984
- *Transmission Control Protocol/Internet Protocol*

Modelul OSI:

- Standard creat de ISO
- Datorită apariției târzii este folosit de puţine aplicații
- Este cel mai bun model teoretic

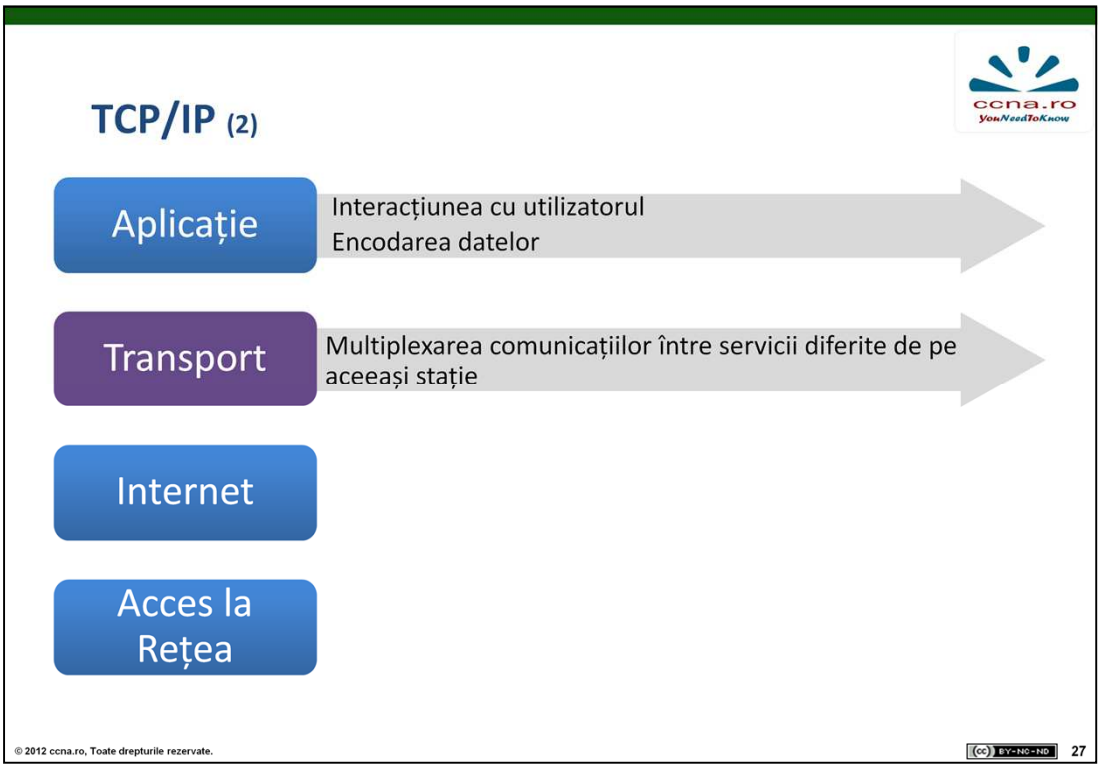
Modelul TCP/IP:

- Model creat de DARPA cu aplicație militară
- A fost adoptat inițial ca standard de facto
- Este modelul folosit în prezent

Nivelul Aplicație al TCP/IP gestionează problemele reprezentării, codării şi ale controlului dialogului. Stiva TCP/IP are prin intermediul nivelului Aplicație capacitatea de a oferi utilizatorului acces direct la serviciile oferite de rețea.

Acest nivel are în componență toate protocoalele de nivel înalt. Printre aceste protocoale se numără:

- TELNET - pentru conexiuni pe calculatoare la distanţă
- FTP - File Transfer Protocol - transfer de fişiere
- SMTP - Simple Mail Transmission Protocol (poşta electronică)
- DNS - Domain Name Service - pentru stabilirea corespondenţei între numele gazdelor şi adresa de reţea
- HTTP - HyperText Transfer Protocol - pentru vizualizarea paginilor web

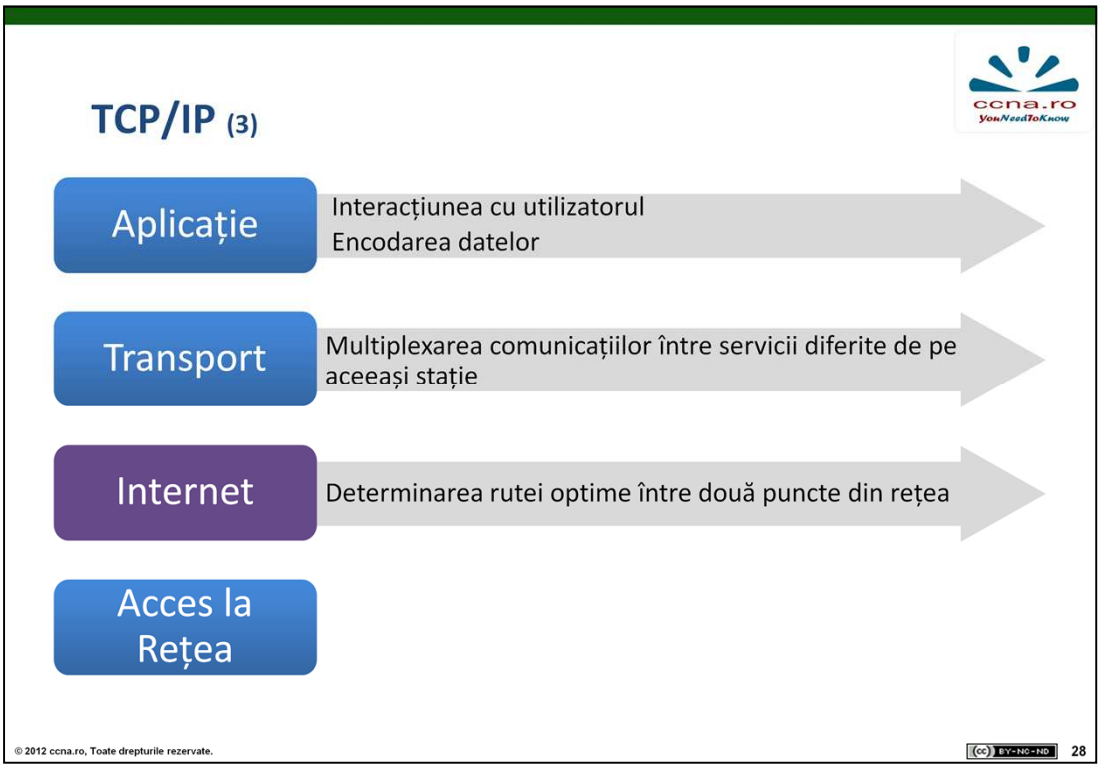


Nivelul Transport oferă servicii de transmisie de la stația sursă către stația destinație. El constituie o conexiune logică între cele două puncte ale rețelei. Protocoalele de transport au drept rol segmentarea și reasamblarea aplicațiilor de nivel superior în același flux de date între punctele comunicante.

La acest nivel se află implementate două protocoale:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

TCP este un protocol sigur și fiabil orientat pe conexiune care permite ca un flux de octeţi trimişi de la o sursă să ajungă la destinaţie fără erori, în timp ce UDP este un protocol nesigur, fără conexiune, destinat aplicaţiilor care doresc să utilizeze propria lor secvențiere şi control al fluxului.

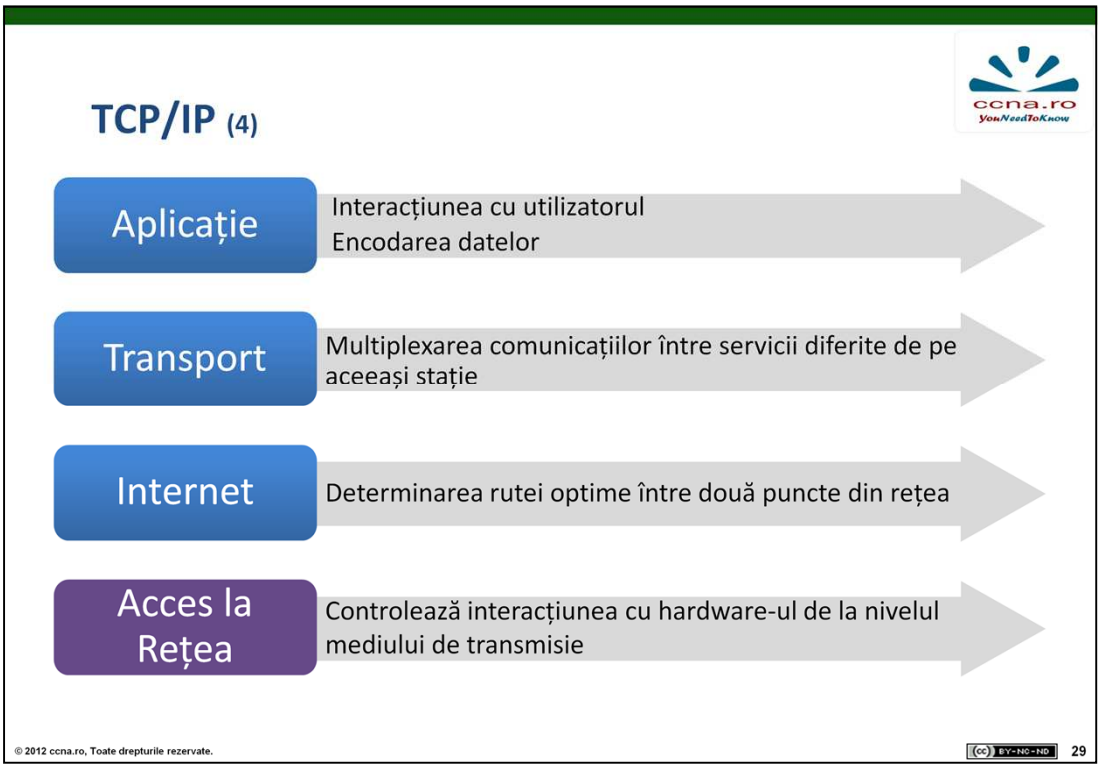


Scopul nivelului Internet este de a determina calea optimă între o sursă și o destinație situate în rețele diferite.

În cadrul stivei TCP/IP, funcțiile acestui nivel este asigurată de protocolul IP. Comunicarea prin intermediul IP-ului este nesigură, sarcina de corecție a erorilor fiind implementată la nivelul Transport.

Alături de protocolul IP la acest nivel mai putem enumera:

- ICMP - Internet Control Message Protocol
- ARP - Addess Resolution Protocol
- RARP - Reverse Address Resolution Protocol
- IPX - Internetwork Packet Exchange

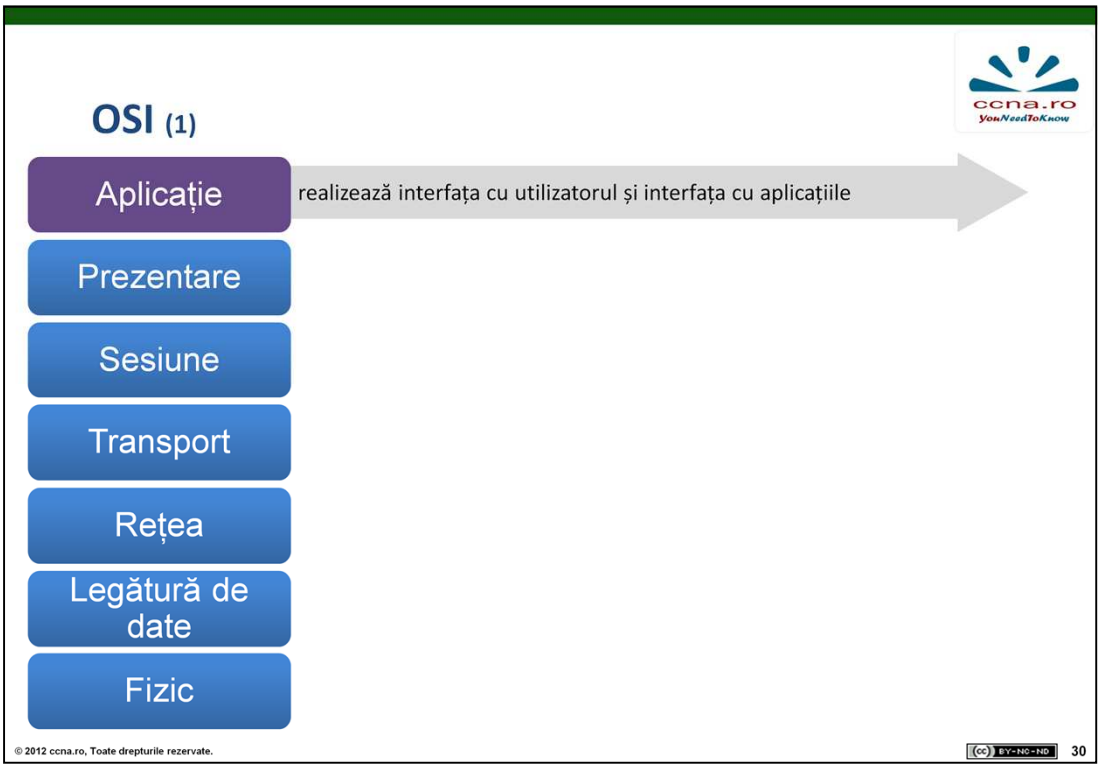


Nivelul Acces la Rețea se ocupă cu problemele legate de transmiterea efectivă a unui pachet primit de la nivel superior pe legătura fizică, incluzând astfel aspecte legate de tehnologii şi de medii de transmisie. De asemenea acest nivel prezintă detalii ale tehnologiilor LAN, WAN și toate detaliile conținute în nivelurile Fizic și Legăturii de Date din stiva OSI.

Serviciile ARP si RARP lucrează inclusiv la nivelul Acces la Rețea.

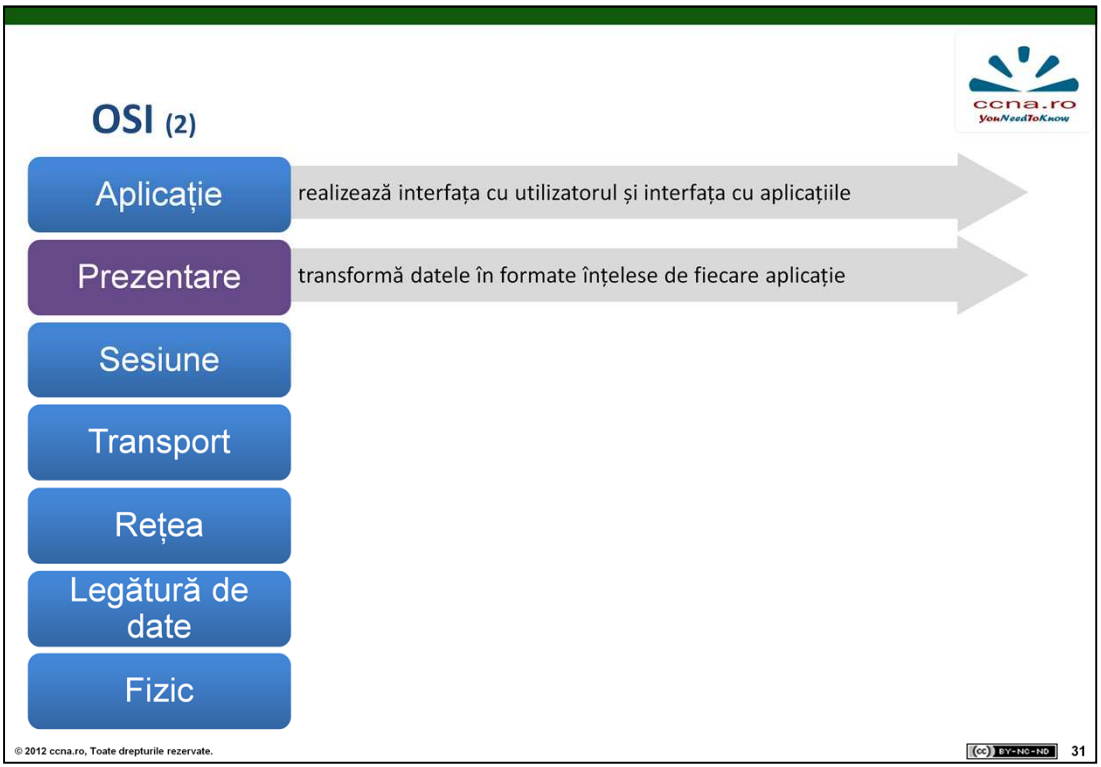
Nivelul acesta este împărțit în două subniveluri, cu funcționalități diferite, unul dintre ele face legătura cu nivelele superioare, cu partea software și celălalt subnivel cu partea hardware, realizând trecerea informației la nivel fizic.

Informația la nivel fizic este reprezentată sub formă de înșiruire continuă de biți.



Nivelul Aplicație realizează interfața cu utilizatorul și gestionează comunicația între aplicații. Acest nivel nu reprezintă o aplicație de sine stătătoare, ci doar interfața între aplicații și componentele sistemului de calcul.

Toate programele care utilizează comunicarea prin rețea fac parte din acest nivel. Exemplele de aplicații de rețea includ clienții și serverele de poștă electronică, clienții și serverele de http (client cunoscut sub numele browser web) sau baze de date distribuite dintre care cele mai cunoscute sunt cele asigurate de serverele DNS (Domain Name System), FTP sau servicii precum Telnet sau SSH care asigură posibilitatea de a accesa de la distanță echipamente.

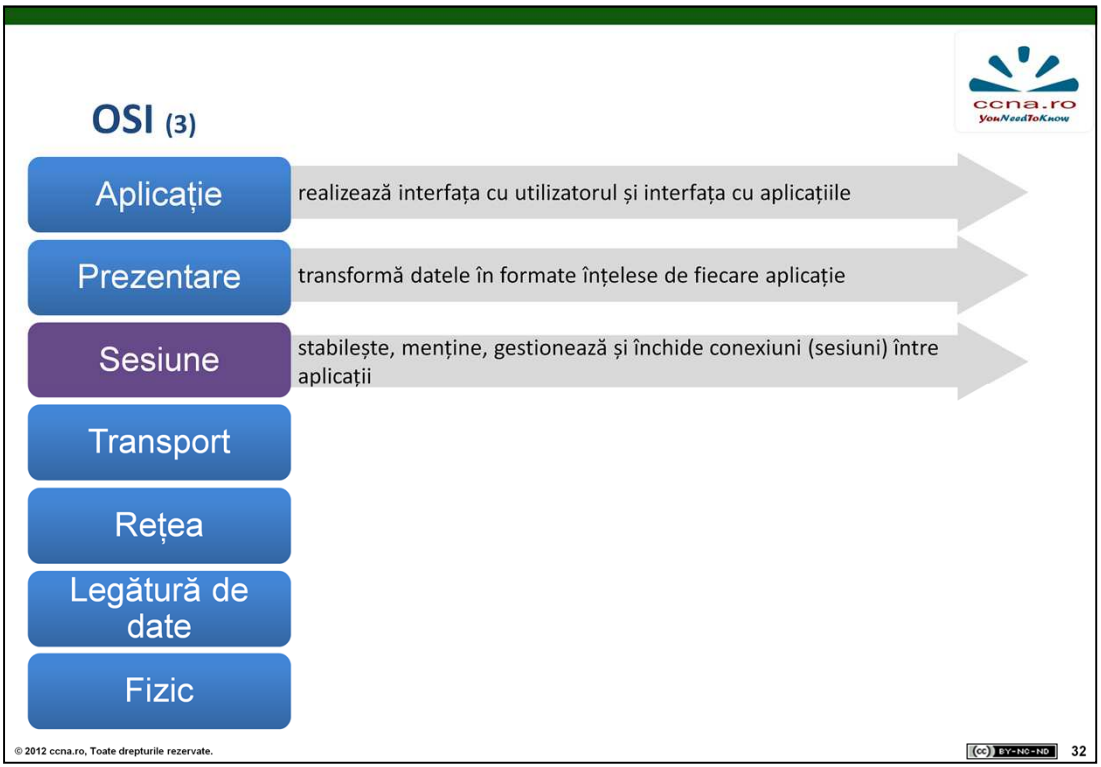


Nivelul Prezentare are rolul de a transforma datele în formate înțelese de fiecare aplicație și de calculatoarele respective, asigură compresia datelor și criptarea.

Nivelul Prezentare reunește funcții folosite în mod repetat în comunicațiile în rețea, realizând gestionarea detaliilor legate de interfațarea rețelei cu imprimantele, formatele fișierelor, etc.

Exemple de protocoale întâlnite la acest nivel:

- XDR - External Data Representation
- ASN.1 - Abstract Syntax Notation 1
- SMB - Server message block
- AFP - Apple Filing Protocol

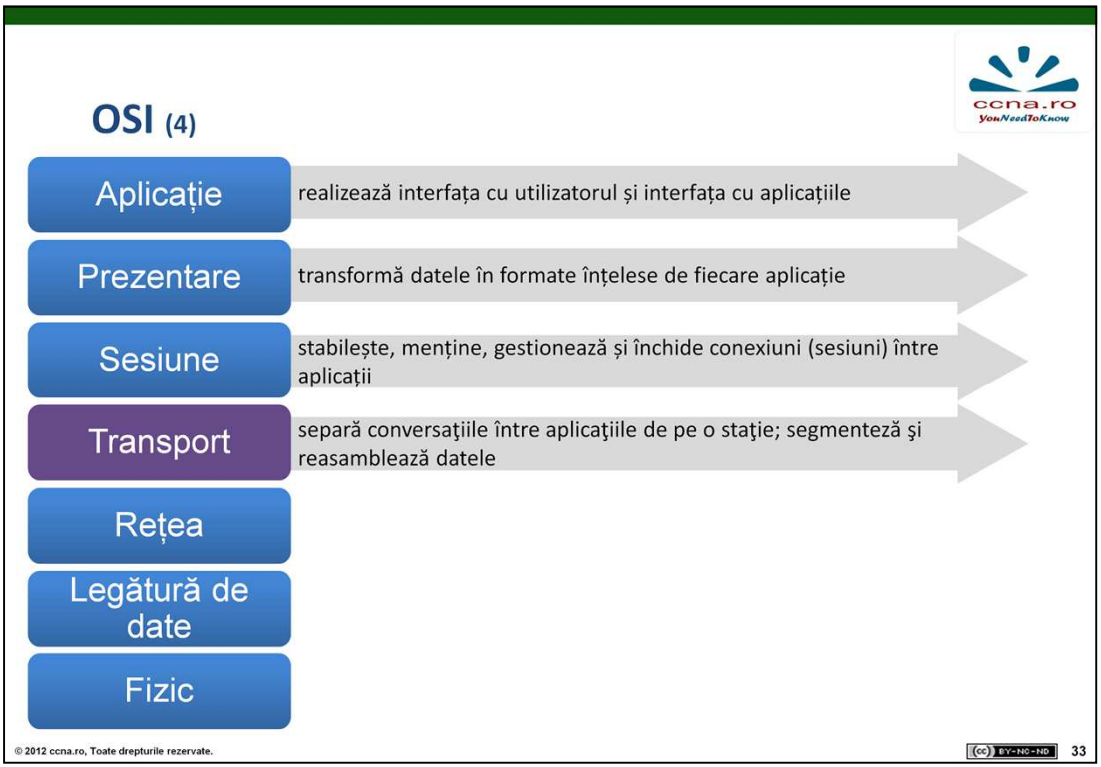


Nivelul Sesiune stabilește, administrează şi termină sesiunile dintre părțile implicate în comunicare. Acest nivel gestionează detalii precum: nume de cont, parole și autorizarea utilizatorilor.

O sesiune este deschisă la fiecare operație de autentificare a utilizatorului și încetează la cererea utilizatorului sau în cazuri bine stabilite, cum ar fi terminarea sesiunii la „n” minute după încetarea utilizării ei.

Protocoale implementate la acest nivel:

- ASAP - Aggregate Server Access Protocol
- SSL - Secure Sockets Layer
- TLS - Transport Layer Security
- SSH - Secure Shell

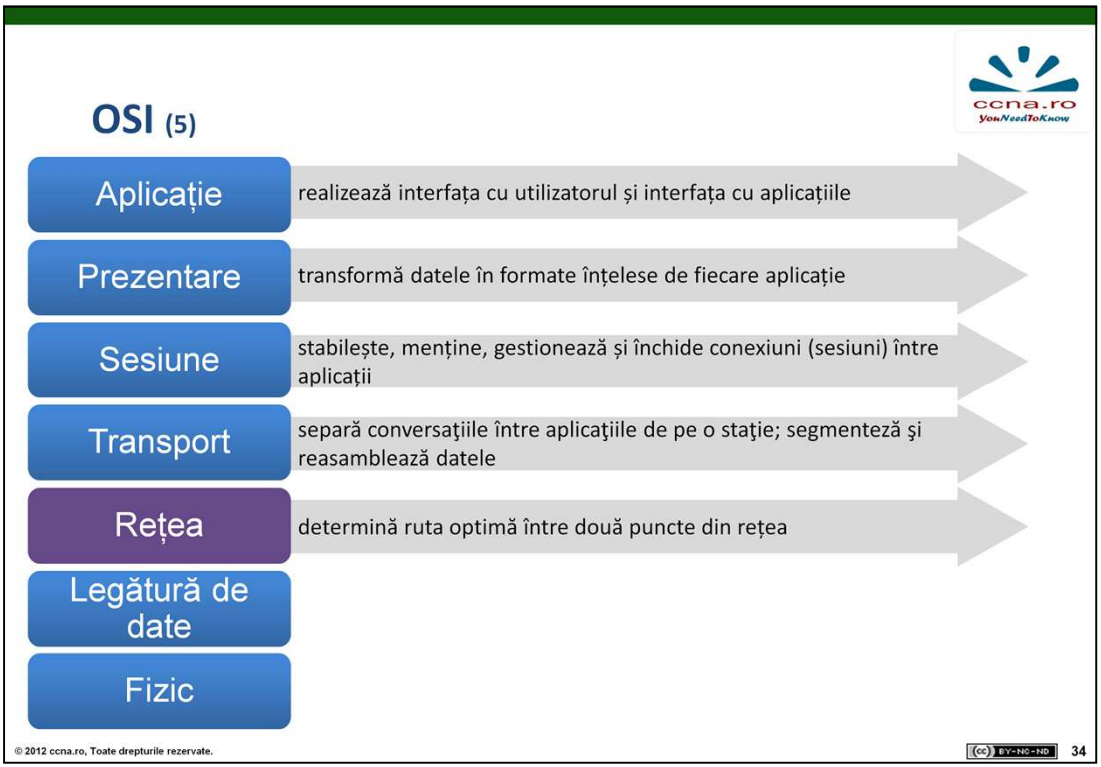


Rolul nivelului Transport este de a realiza transferul fiabil al informației între două sisteme terminale ale unei comunicații.

Acest nivel furnizează controlul erorilor și fluxului de date între două puncte terminale, asigurând ordinea corectă a pachetelor de date.

El oferă un serviciu de transport de date care izolează nivelurile superioare de orice specificități legate de modul în care este executat transportul datelor. Ca și în cazul stivei TCP/IP la acest nivel se află implementate cele două protocoale:

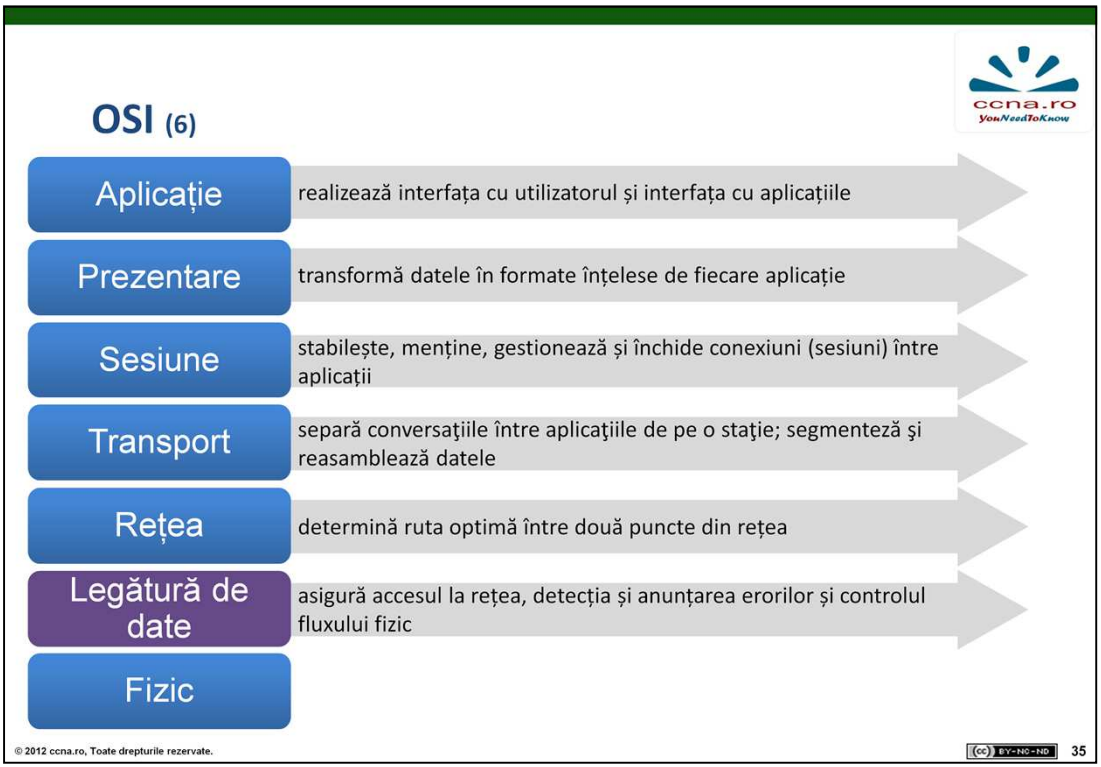
- TCP - Transmission Control Protocol
- UDP - User Datagram Protocol



Nivelul Rețea permite transferul de date între sistemele neadiacente (care nu partajează acelaşi mediu de acces). Unitatea de date utilizată este *pachetul*. Tot el asigură alegerea optimă a căilor de transmitere. Ca atare, nivelul rețea trebuie să gestioneze traficul în rețea, congestiile și rețele de transfer (vitezele) de-a lungul liniilor de transmisie.

Alegerea căilor spre destinație trebuie să se facă pe baza unei surse și destinație.

Pentru a se stabili sursa și/sau destinația este nevoie de o adresă IP. Completarea acestor câmpuri sursă și destinație în antetul IP este realizată de nivelul rețea .



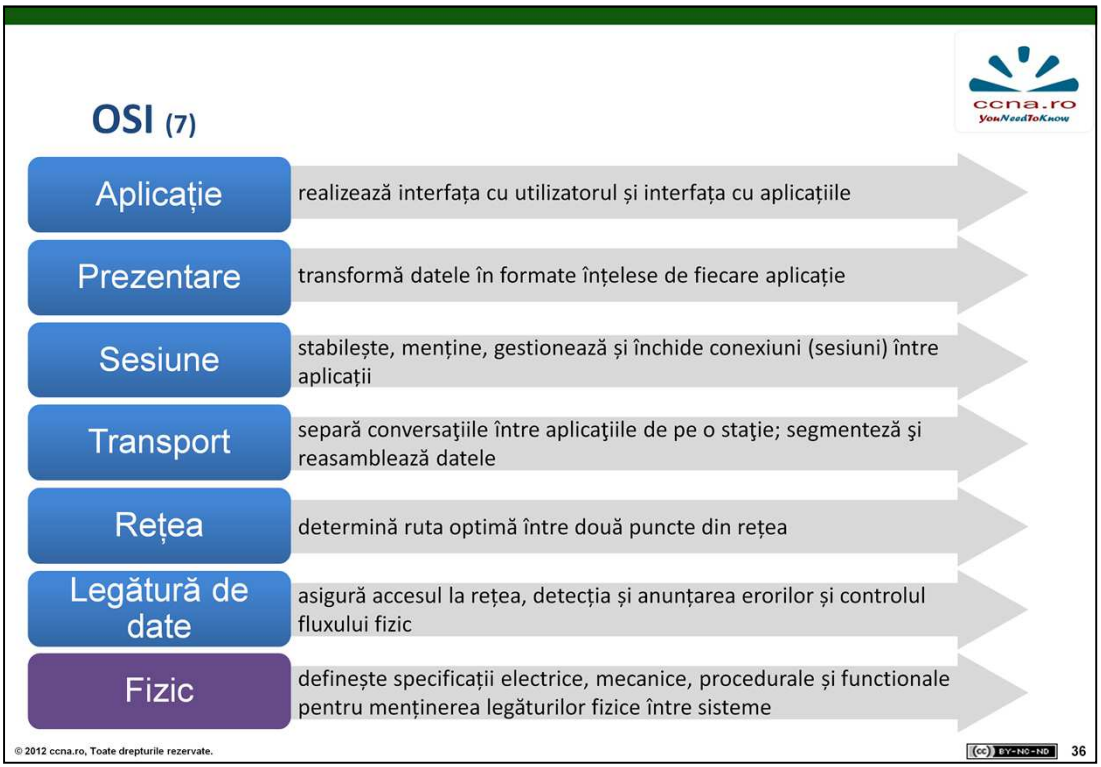
Nivelul Legătură de date asigură adresarea fizică, topologia rețelei, accesul la rețea, detecția și anunțarea erorilor și controlul fluxului fizic.

În cazul unui calculator placa de rețea constituie nivelul legăturii de date.

Ca exemplu de protocoalele întâlnite la acest nivel avem:

- Ethernet
- Frame Relay
- PPP - Point-to-Point Protocol
- ATM - Asynchronous Transfer Mode
- X.25
- 802.11

În funcție de protocolul folosit pot apărea diferite probleme, avantaje sau dezavantaje privind transmisia datelor.

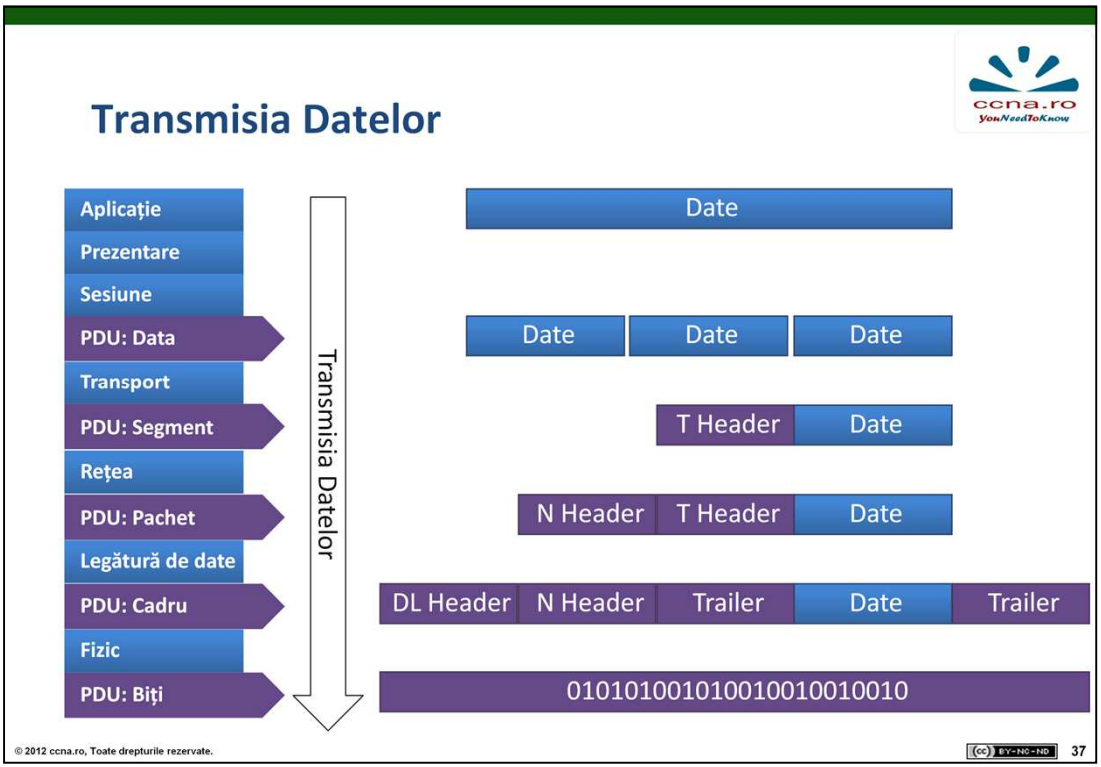


Nivelul Fizic este nivelul de bază care asigură serviciile fizice. El definește specificațiile electrice, mecanice, procedurale și funcționale pentru activarea, menținerea și dezactivarea legăturii fizice între sistemele finale. Este cel mai aproape de media și semnale.

El controlează specificațiile mediului de transmisie, controlează tensiunea, semnalele, viteza de transmisie, distanțele și conectorii.

Din punct de vedere al modului în care sunt codați biții de nivelul fizic, există mai multe tipuri de codificări:

- Manchester Diferențial
- Manchester IEEE 802.3
- Non-Return-To-Zero Level
- Multi-Level Transmit 3
- Pulse-Amplitude Modulation 5



În cadrul unei rețele datele sunt transmisie de la o gazdă la alta și fiecare nivel OSI comunică cu nivelul corespondent de la destinație. Forma de comunicare în cazul în care fiecare nivel realizează un schimb de date (așa numitul „protocol data units” - PDU) cu nivelul aflat la destinație poartă numele de comunicare corespondent-corespondent. În cadrul unei rețele fiecare nivel depinde de nivelul aflat sub el.

Începând cu transport, fiecare nivel încapsulează PDU-ul de la nivelul superior în câmpul său de date, îi adaugă „header”-ele și „trailer”-ele proprii, iar datele trec la nivelul următor.

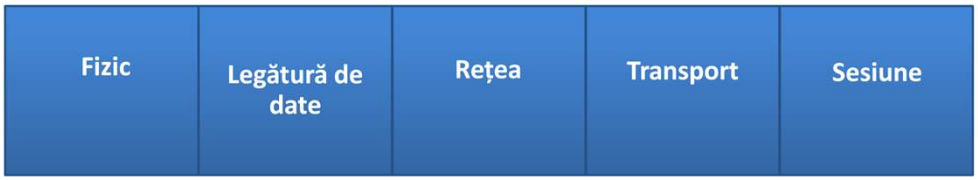
De exemplu nivelul 4 adaugă mai multe informații la datele provenite de la nivelul 5 și le grupează într-un segment. Nivelul 3 (rețea), trebuie să transmită datele prin rețea. Le atașează un „header” creând un PDU al nivelului 3. Acest procedeu continuă până când datele ajung la nivelul fizic, unde sunt transformate în biți și trimise către destinație.

Adresare

Necesitate

- Informația trimisă prin reţea este segmentată la sursă și reasamblată la destinație
- Segmentele ajung la destinație în mod independent
- Pentru a face transmisia cât mai sigură PDU-urile sunt asociate cu adrese

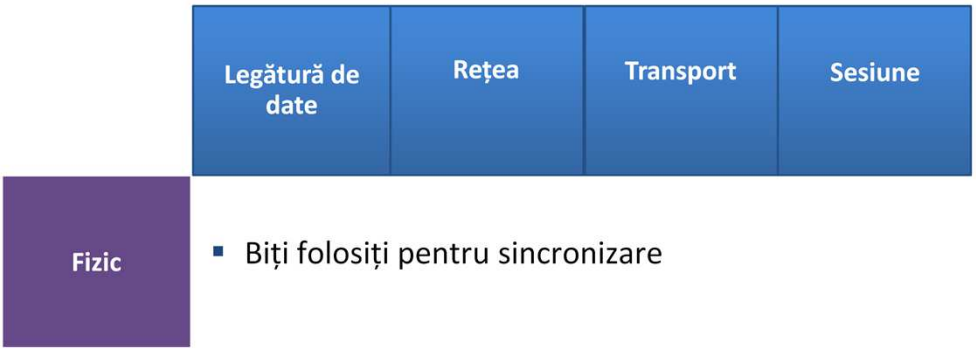
Adresare



Din punct de vedere al adresării rolul fiecărui nivel este:

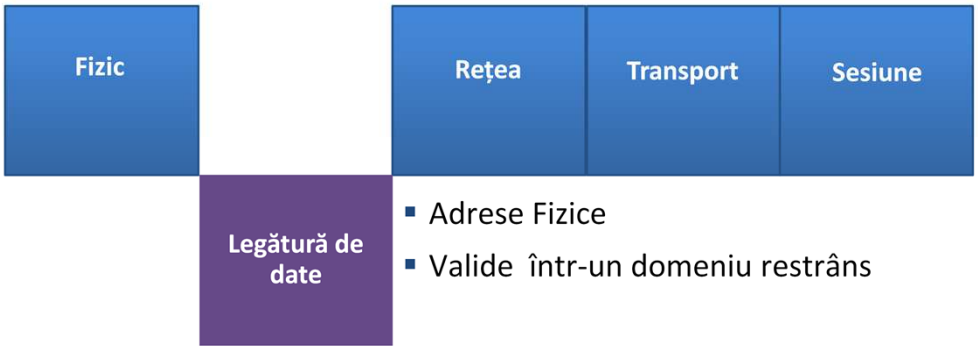
- Fizic: Biți folosiți pentru sincronizare
- Legătură de date: Adrese Fizice
  — valide într-un domeniu restrâns
- Rețea: Adrese Logice
  — valabile la nivel global
- Transport: Porturi
  —identifică traficul unei aplicaţii la nivelul sistemului de operare
- Sesiune:
  — identifică sesiuni multiple în cadrul aceleiași aplicații în cadrul aceluiași sistem de operare

Adresare: Nivelul Fizic



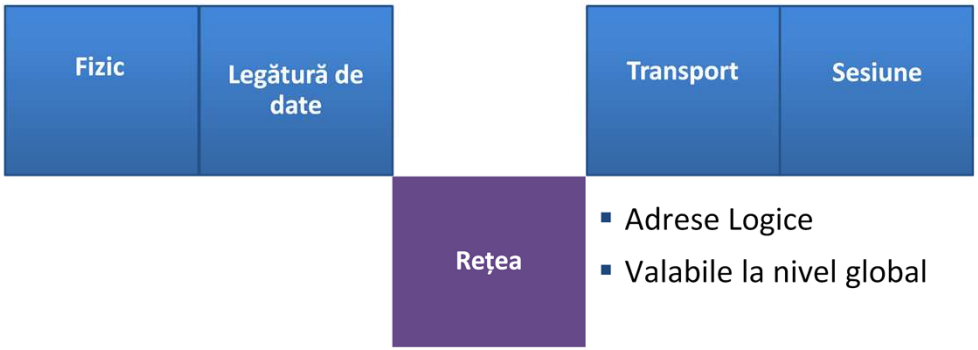
- Biți folosiți pentru sincronizare

Adresare: Nivelul Legătură de date



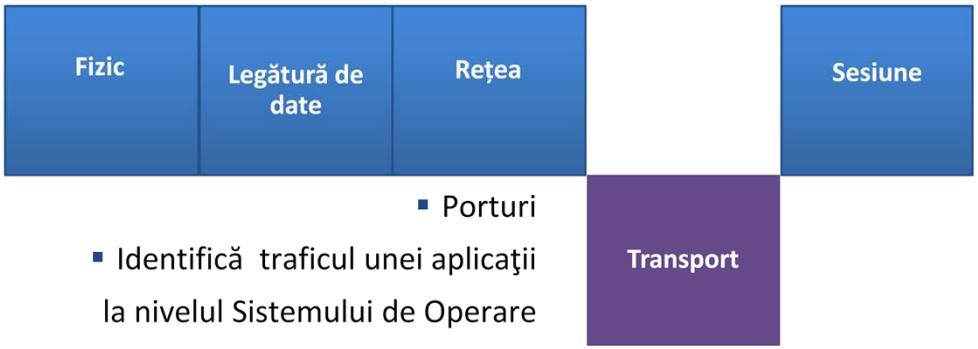
- Adrese Fizice
- Valide într-un domeniu restrâns

Adresare: Nivelul Rețea



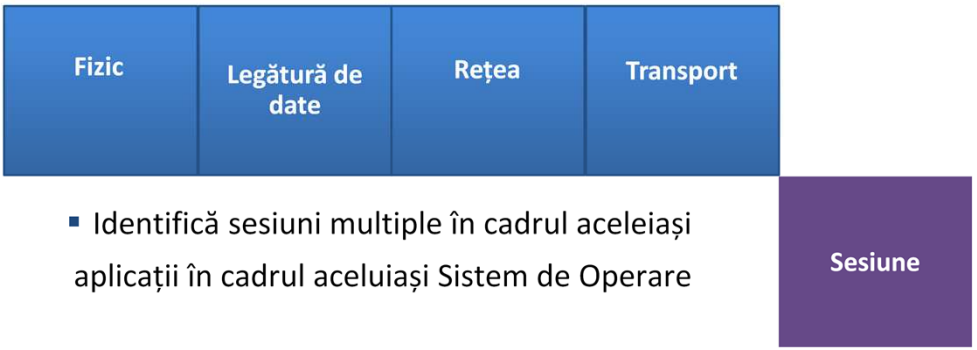
- Adrese Logice
- Valabile la nivel global

Adresare: Nivelul Transport



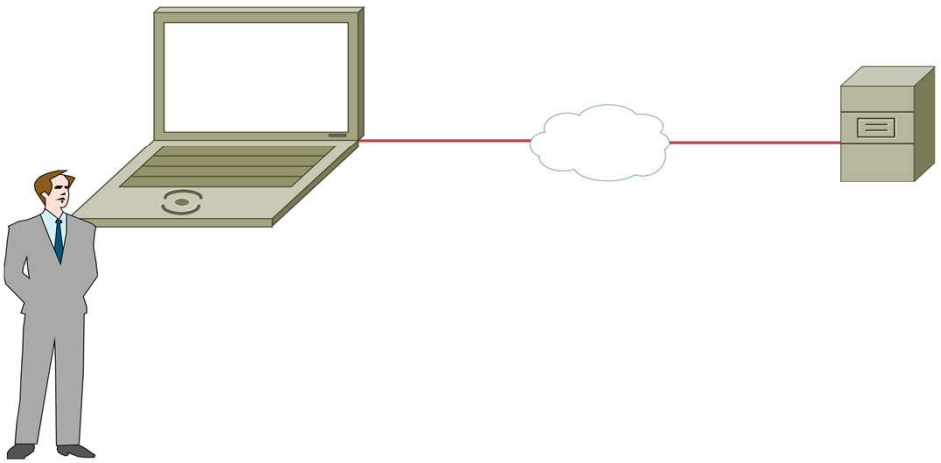
- Porturi
- Identifică traficul unei aplicaţii la nivelul Sistemului de Operare

Adresare: Nivelul Sesiune

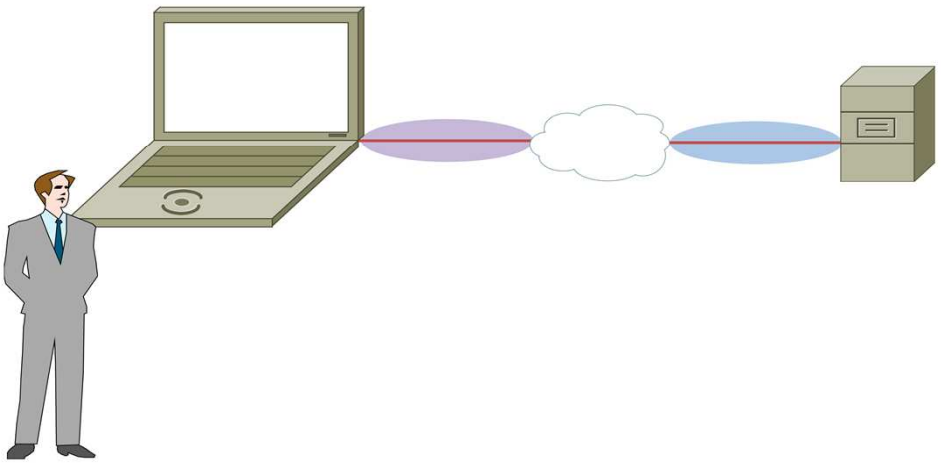


- Identifică sesiuni multiple în cadrul aceleiași aplicații în cadrul aceluiași Sistem de Operare

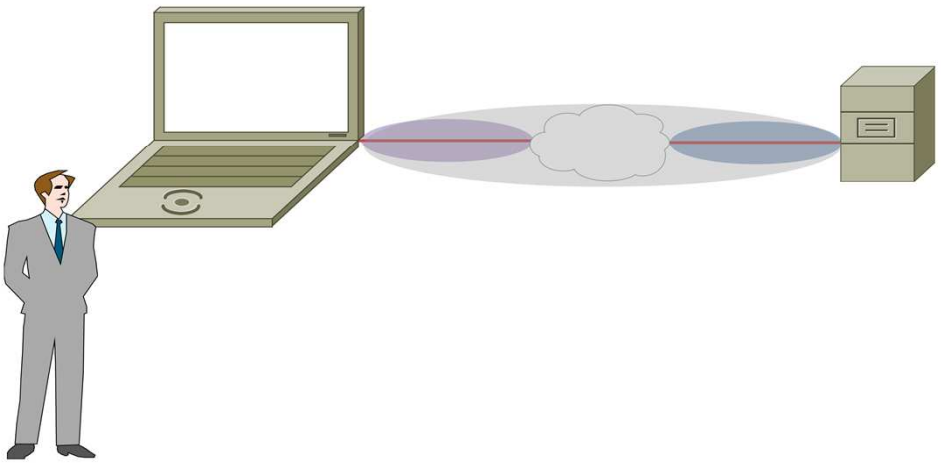
Adresare



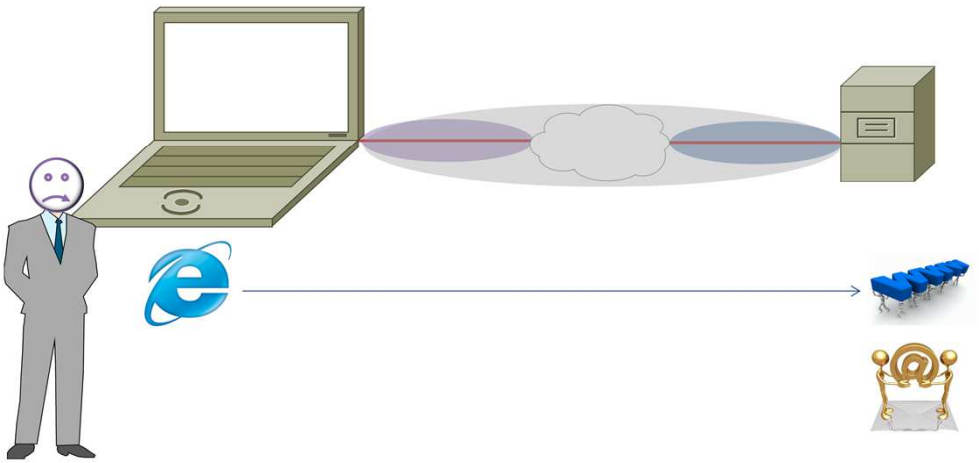
Adresare (Legătură de date)



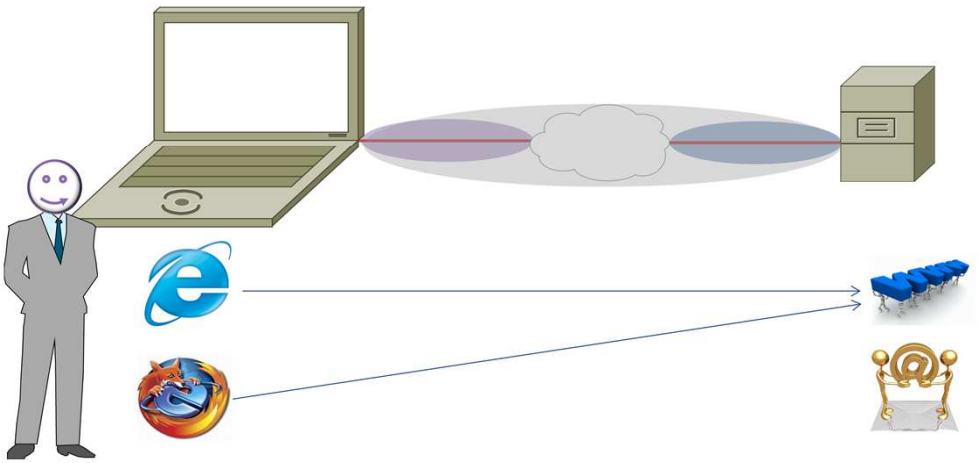
Adresare (Rețea)



Adresare (Transport)



Adresare (Sesiune)



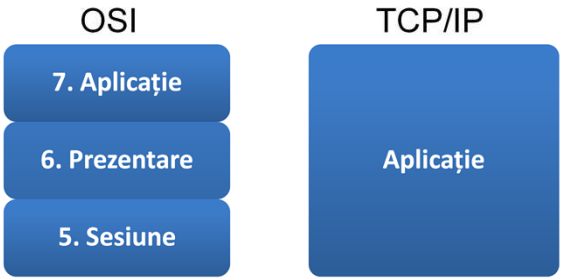
Capitolul 2: Nivelul Aplicație

Obiective

- OSI & TCP/IP
- Modele de comunicație
- Aplicații și servicii

OSI & TCP/IP

- Nivelul 4 al stivei TCP/IP îndeplinește funcțiile nivelelor 5, 6 și 7 ale stivei OSI



La baza stabilirii nivelelor arhitecturale ale modelului ISO-OSI au stat o serie de principii generale, cum ar fi: crearea unui număr redus de nivele cu puține interacțiuni între ele; colectarea funcțiilor înrudite în același nivel; crearea posibilității de modificare a funcțiilor unui nivel, fără afectarea celorlalte; crearea pentru fiecare nivel de linii de demarcație (interfețe) spre nivelul adiacent inferior și superior.

Din punct de vedere al funcționalității, cele două modele de stive: OSI (Open Systems Interconnection) și TCP/IP (Protocol de control al transmisiei/Protocol Internet), au elemente echivalente ce oferă aceeași funcționalitate.

Primele trei niveluri ale stivei OSI: Aplicație, Prezentare, Sesiune sunt echivalente cu nivelul Aplicație al stivei TCP/IP.

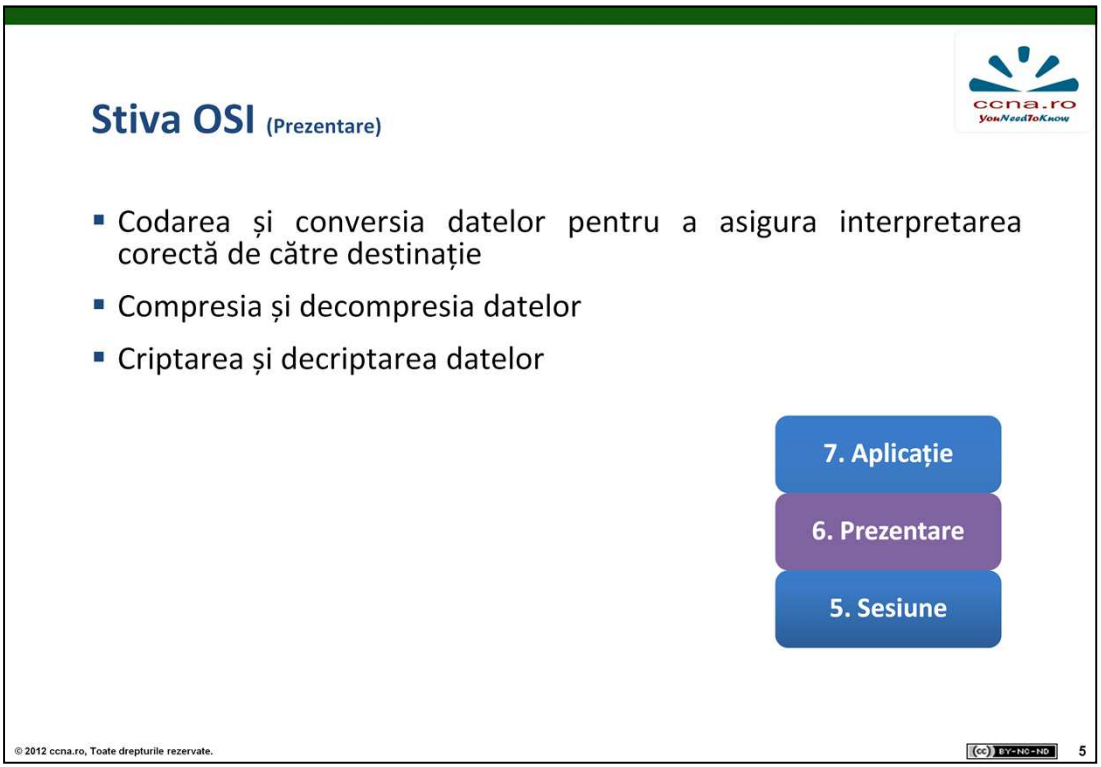
Diferența dintre cele două este că stiva OSI delimitează clar ce se întâmplă la nivelul aplicație, pe când TCP/IP înglobează totul în același nivel.

Stiva OSI (Aplicație)

- Interfața dintre aplicațiile folosite de utilizator și rețeaua peste care sunt transmise datele
- Protocoalele de la acest nivel sunt folosite pentru a transmite/primi date între programele care rulează pe mașinile sursă și destinație
- Ex.: HTTP, DNS, SMTP

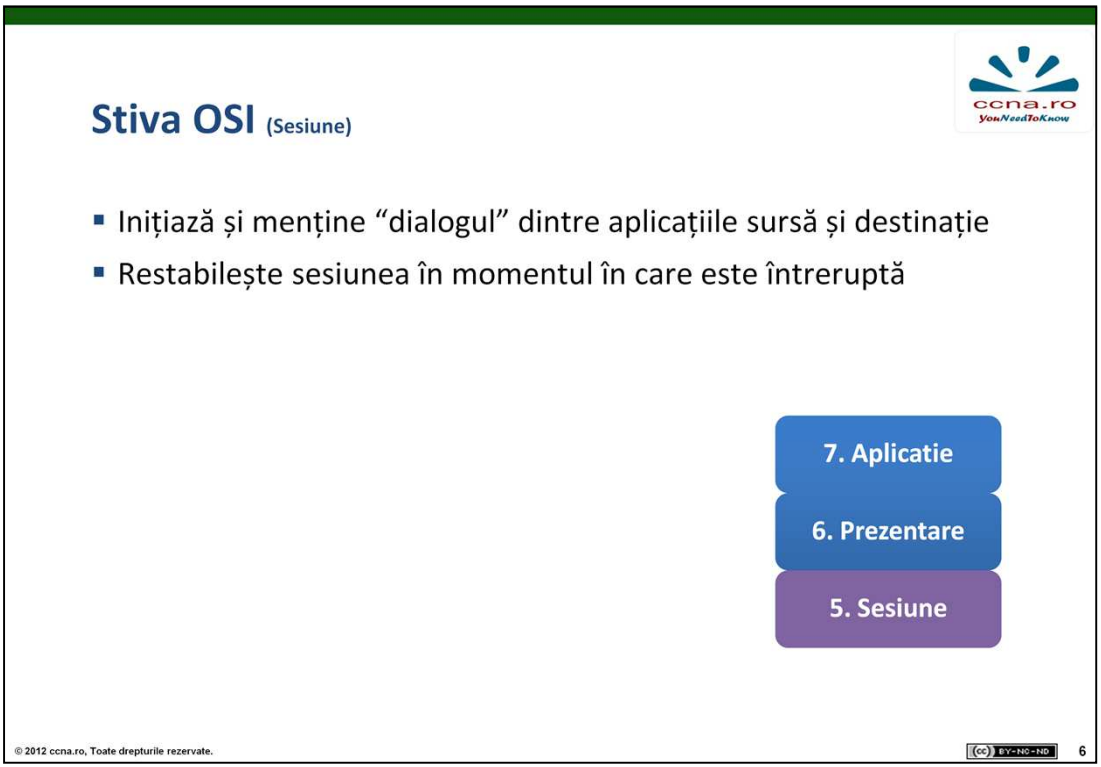
Nivelul acesta este cel mai aproape de utilizator, astfel interacţionează direct cu software-ul ce trebuie să aibă acces la reţea. Aici se identifică partenerii de comunicaţie, se determină câte resurse sunt disponibile şi se sincronizează comunicaţia. Diferența de celelalte niveluri este evidențiată prin inexistența unei dependențe de un alt nivel din cadrul stivei OSI.

Fiecare aplicație sau serviciu de rețea folosește protocoale care definesc standardele și formatul datelor ce urmează a fi folosite. Fără aceste protocoale formatul datelor nu vor avea un mod comun pentru a formata și directa datele în rețea.



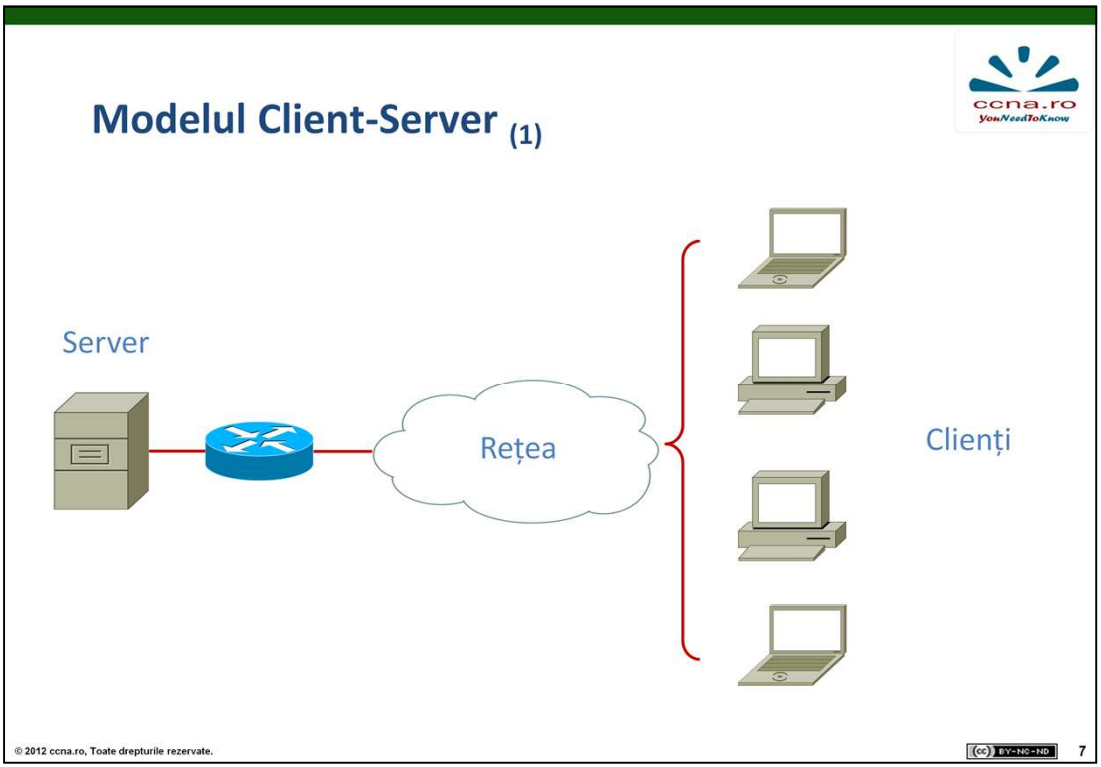
Nivelul Prezentare rezolvă diferenţele ce pot apărea din cauza diverselor aplicaţii ce pot folosi sintaxe şi semantici diferite. Un fişier video este diferit de unul audio dar trebuie ca ambele să fie convertite într-un format unic pentru reţea (mai ales restaurate la finalul transmisiei, trecând de la formatul de reţea la un format acceptat de programul ce trebuie să primească acele date).

De asemenea criptarea datelor se face tot la acest nivel.



Nivelul Sesiune controlează și administrează dialogul între două calculatoare (dintre aplicaţia locală şi cea la distanță). Se definesc proceduri de începere, terminare, menținere și resetare a convorbirilor (ce pot fi half-duplex/full-duplex).

Acesta include posibilitatea de control si management ale unor mesaje bidirecționale, anunțând astfel nivelul Aplicație despre datele ce au fost trimise cu succes.

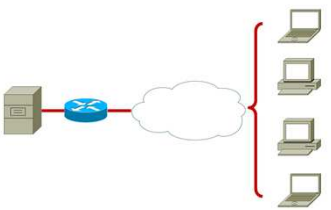


Modelul client-server este o structura distribuită care partajează procesarea între furnizorii de servicii, denumiți servere, și elemente ce solicită servicii numite clienți. Clienții și serverele comunică printr-o rețea având suport hardware, dar pot rula pe același suport fizic. Un server poate rula unul sau mai multe servicii pe care le partajează clienților.

Clientul nu partajează nicio resursă proprie ci doar apelează la cele oferite de server. Clienții sunt cei ce inițializează comunicația, menținerea legăturii între cei doi, aduce în prim plan conceptul de sesiune care de obicei este limitată în timp.

Modelul Client-Server (2)

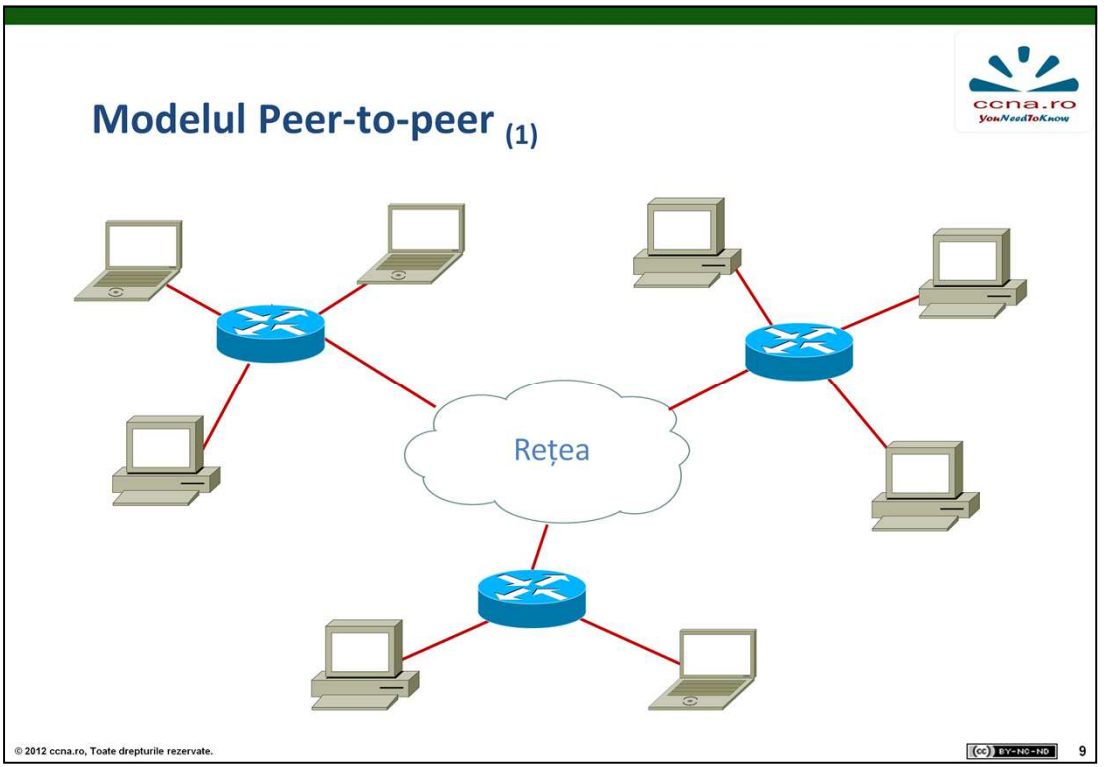
- **Client** = entitate care inițiază cereri pentru diverse resurse
- **Server** = entitatea care răspunde unei cereri inițiate de un client
  - poate fi un computer care conține informații accesate de mai mulți clienți (Ex.: server web)
  - de obicei pe acest computer rulează un proces numit "server daemon"
  - poate cere autentificarea utilizatorilor
- Se consideră că procesele client și server se află la nivelul Aplicație



În general un server este o aplicație ce oferă servicii utilizatorilor de Internet, în timp ce un client este o altă aplicație ce solicită un serviciu. Există aplicații alcătuite atât dintr-o parte client cât și dintr-o parte server, ce pot rula pe același sistem sau pe sisteme diferite.

Utilizatorii sunt cei ce inițializează partea client a aplicației, care efectuează o cerere la un serviciu pe care o trimite părții server a aplicației folosind protocoale de la nivelul Transport. Serverul este un software, ce primește o cerere, o soluționează și trimite rezultatul drept răspuns cererii.

Un server are capacitatea să rezolve mai multe cereri simultan. exemple de servere: DNS, Apache, Radius, PPPoE, FTP, MAIL , SSH, TFTP etc.



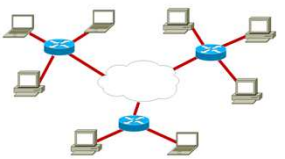
Rețelele „peer-to-peer” sunt o arhitectură de aplicații distribuite ce pornesc de la premisa împărțirii și încărcării egale între toți participanții (noduri). Aceste noduri au privilegii egale și au rol de participanți egali în cadrul unei aplicații. Rețelele „peer-to-peer” nu au servere dedicate și nicio ierarhie între calculatoare, toți participanții au drepturi egale (atât de client cât și de server) din acest motiv numindu-se „peers”.

În această rețea nu există un responsabil direct, utilizatorul fiecărui dispozitiv situat în comunicație decide datele ce vor fi partajate cu ceilalți participanți.

Un exemplu bine cunoscut de aplicații ce folosesc modelul de comunicație „peer-to-peer” sunt cele pentru torenți.

Modelul Peer-to-peer (2)

- Două sau mai multe calculatoare sunt conectate în rețea și pot accesa diverse servicii fără un server dedicat
- Fiecare echipament poate avea rol simultan de client sau server
- Accesul la resurse este descentralizat
- Securitate mai slabă și mai greu de implementat



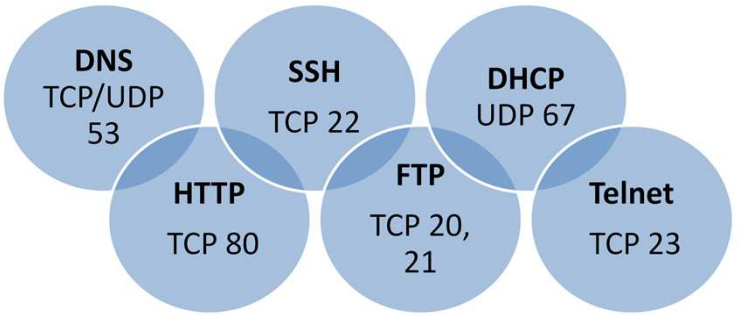
Rețelele „peer-to-peer” mai sunt denumite și grupuri de lucru (workgroups), ele fiind relativ simple întrucât fiecare dispozitiv funcționează atât ca server cât și ca un client, nefiind necesar un server central cu proprietăți hardware necesare pentru susținerea unei rețele de capacitate mare.

Din punct de vedere al costului în comparație cu modelul client-server, costul este scăzut deoarece nu există cerințe dedicate hardware sau software, comunicația prin rețea nu necesită standarde de securitate și performanțe ridicate.

În concluzie, o rețea „peer-to-peer” oferă ca avantaje administrarea proprie a securității, utilizatorii acționând ca administratori proprii asupra propriului sistem, implicat în comunicația de acest tip.

Porturi

- Nivelul Transport foloseşte o schemă de adresare folosind numere numite **porturi**
- Porturile oferă o metodă de a identifica aplicaţiile şi serviciile de la nivelul Aplicaţie care reprezintă sursa şi destinaţia comunicării

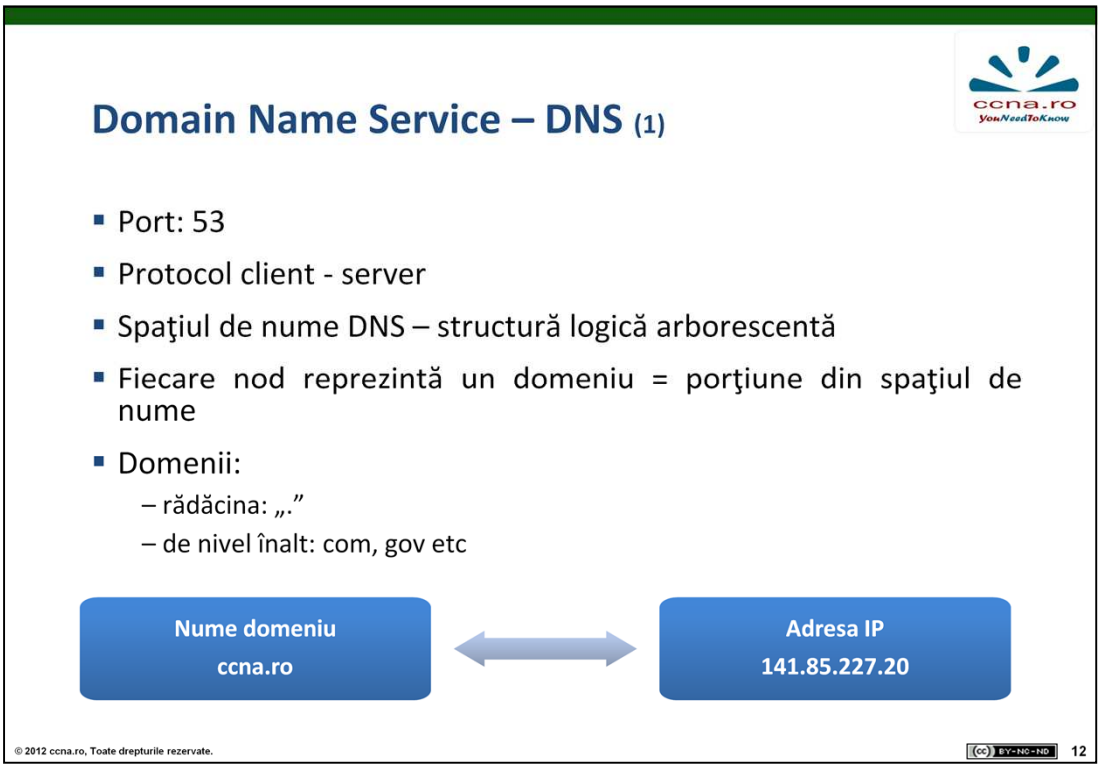


Aplicațiile de nivel înalt sunt marcate prin intermediul unui identificator numit port. Porturile sunt folosite pentru adresarea de nivel 4, identificând astfel sursa și destinația la nivel de Aplicație.

Porturile sunt reprezentate pe 16 biți având astfel valori între 0 și 65535.

Numerele de port cuprinse între 0-1023 corespund unor porturi bine cunoscute („well known ports”), acestea fiind alocate în general ca porturi destinație severelor de aplicații și pot fi utilizate doar de procese privilegiate, de exemplu „root” pe sisteme de operare bazate pe Linux, sau administrator pe Windows.

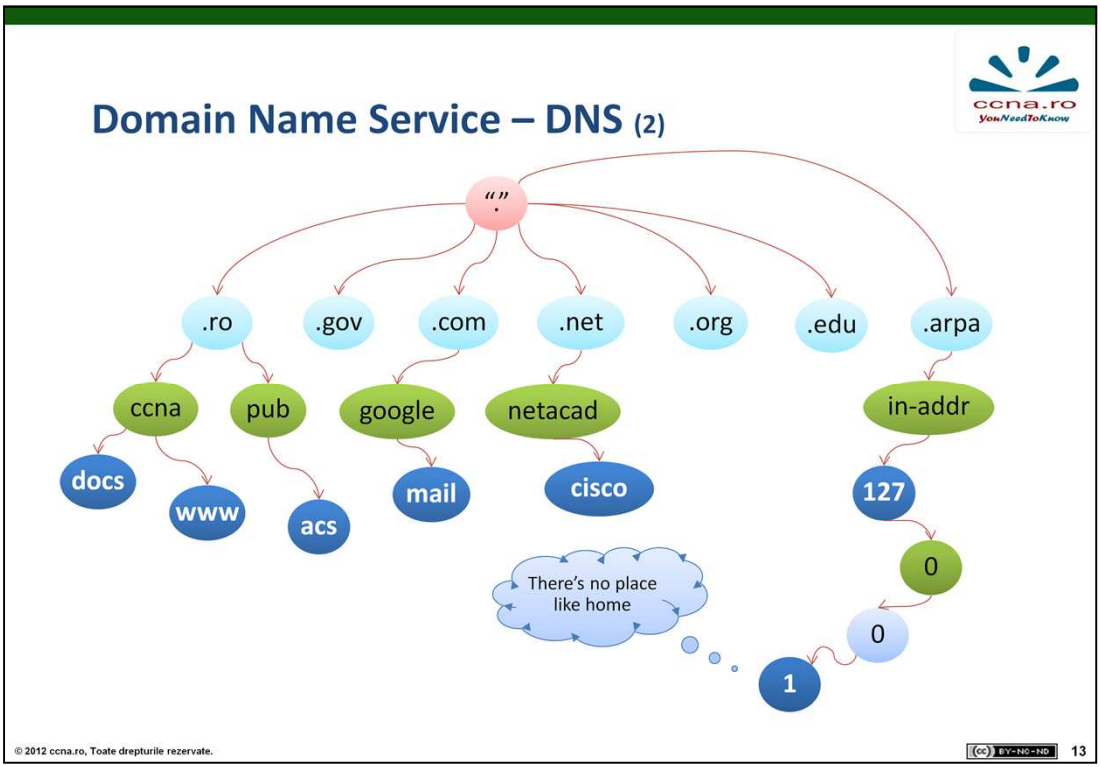
Exemple de porturi bine cunoscute: HTTP - 80, POP3 - 110, SNMP - 191, NTP - 37, IMAP - 143, SYSLOG - 514, Real Time Streaming Protocol - 554.



Un Domain Name Service reprezintă un sistem distribuit de date, de păstrare și interogare a unor date arbitrare, de obicei realizarea unei corespondențe între nume și adresa IP, într-o structură ierarhică de tip arborescentă. Cea mai cunoscută aplicație DNS este gestionarea ierarhică a domeniilor din Internet.

DNS are rolul de a translata din nume de domeniu în adrese IP, și din adrese IP în nume, acest proces numindu-se „rezolvarea numelui de domeniu”. Toate serviciile de Internet din zilele noastre se bazează pe servere de DNS, în situația în care acestea nu funcționează, livrarea informației nu este posibilă.

O translatare a unui domeniu constituie o simplă mapare între nume și IP, un exemplu fiind www.ccna.ro - 141.85.227.20.

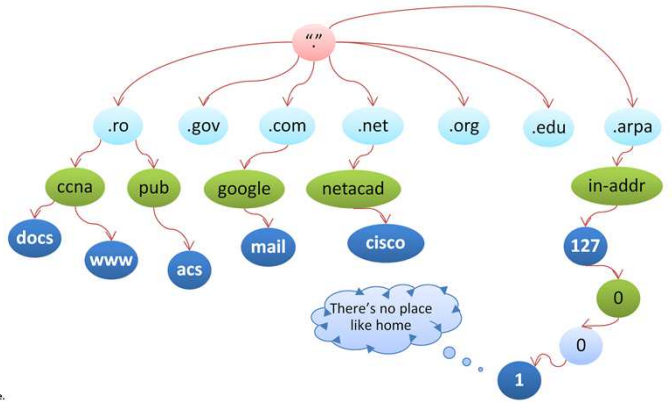


Structura DNS realizează administrarea numelor prin acordarea unor responsabilități diferite unui grup, fiecare nivel al arborelui constituie un domeniu. Sistemul de nume din Internet este structurat pe domenii și subdomenii. Un exemplu ar fi docs.ccna.ro, unde domeniul cel mai cuprinzător este „.ro”, care include la rândul lui domeniul „ccna”, iar „docs”, reprezintă resursele unui server intern evidențiat anterior.

În Internet există domenii dedicate (standardizate), toate dintre ele fiind legate printr-un server numit „.” (rădăcină) care se asigură că serverele DNS de pretutindeni au acces la aceeași informație privind adresele IP ale site-urilor și domeniilor web. Exemple de domenii dedicate: .com - desemnează domeniul comercial, .edu - domeniul educațional, .gov - domeniu guvernamental, .org - domeniul organizațional, .net - domeniul resurselor de rețea, .int - domeniul resurselor internaționale, etc.

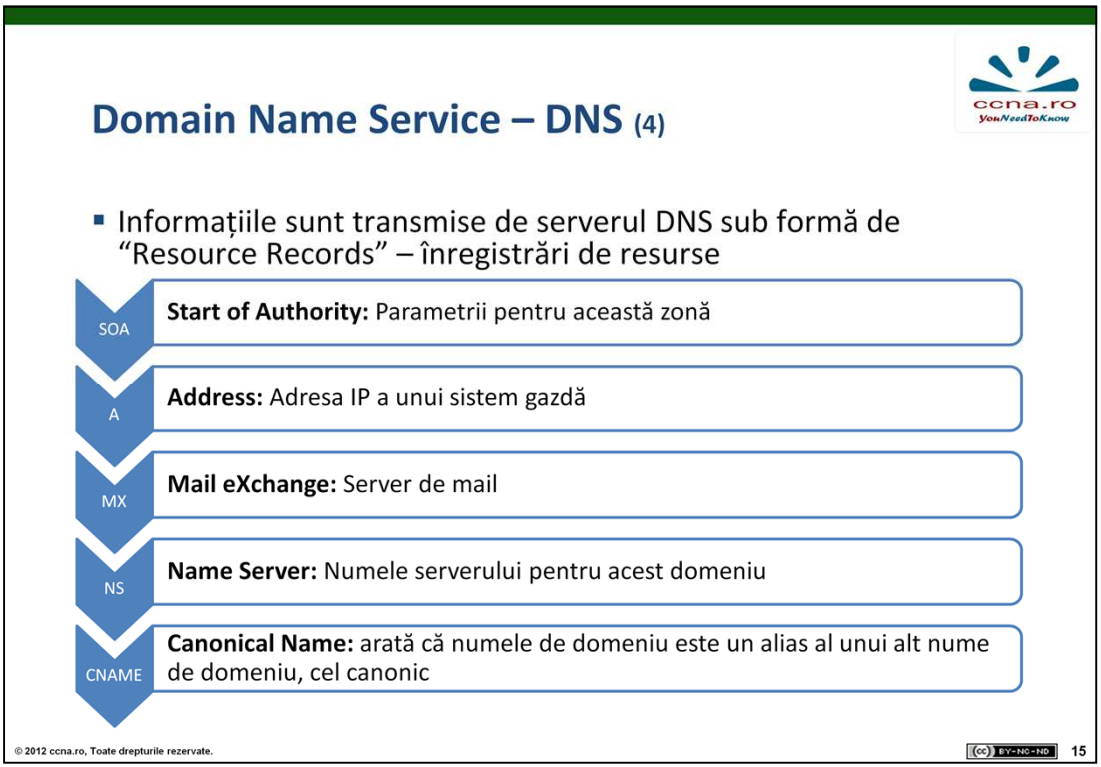
Domain Name Service – DNS (3)

- Domeniile sunt organizate în **zone DNS** pentru administrare
- Un **server DNS** administrează o zonă DNS
- Serverele DNS formează o reţea ierarhică



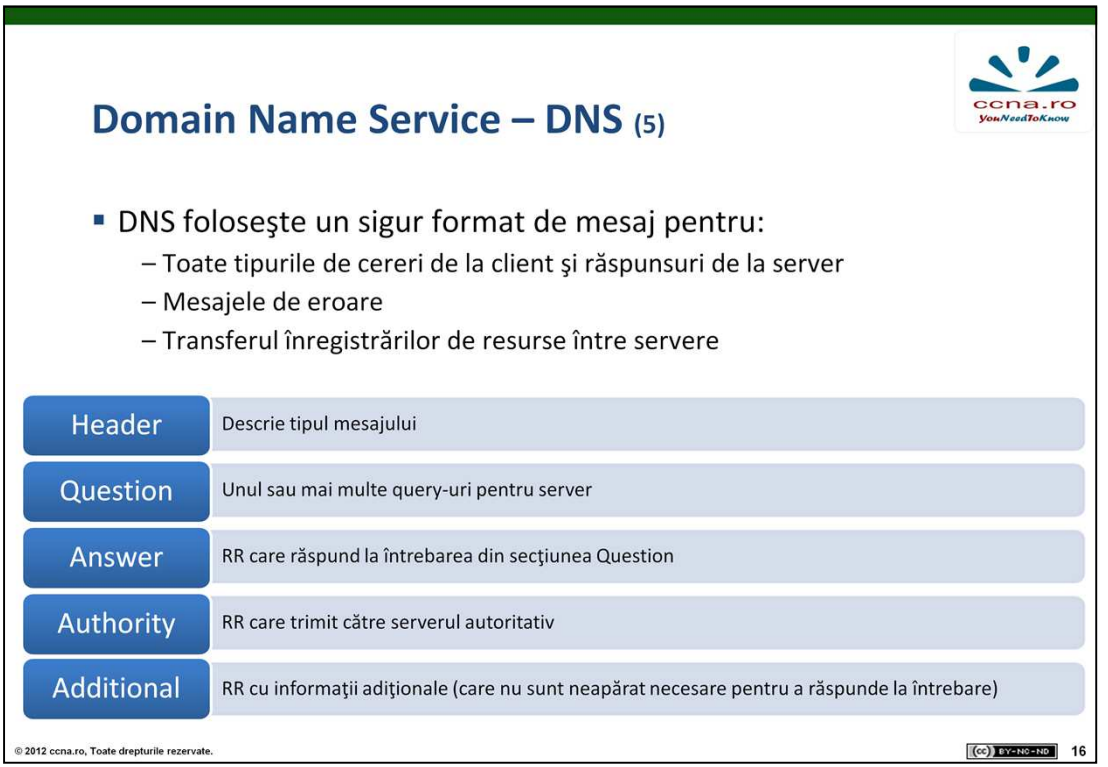
Serverele DNS reprezintă o bază distribuită pe toata rețeaua Internet. Se numește distribuită întrucât nu există un server care sa conțină toată informația necesară traducerii oricărui domeniu existent într-o adresa IP. Fiecare server menține o bază de date cu propriile domenii pe care alte sisteme din Internet le poate interoga. Fiecare sever DNS are un server DNS superior cu care face periodic schimb de informație, astfel într-un domeniu trebuie să existe doua servere DNS ce funcționează ca autoritar și primar.

Cel autoritar păstrează cea mai corectă și actualizată informație privind adresele IP din domeniu. În cele mai multe cazuri aceste echipamente sunt administrate de către deținătorii domeniilor în cauză, astfel alte servere de DNS din Internet se vor încrede în informațiile serverelor autoritare privind furnizarea informațiilor corecte pentru domeniile cunoscute lui.



Un sever DNS transmite informațiile sub formă de înregistrări:

- SOA - Parametrii pentru zonă (ex. Adresa de E-mail a administratorului de sistem)
- A - Adresa IP a sistemului gazdă
- MX - Legătura simbolică la un server de mail
- NS - Name Server
- CNAME
- PTR (Pointer) - Uzual constituie adresa unei adrese IP
- HINFO (HostInfo) - Informații despre sistemul gazdă în format ASCII
- TXT (Text ASCII) - Orice informație utilă despre entitate



DNS-ul are un format unic de mesaj pentru toate tipurile de cereri, exemplu fiind imaginea de mai sus, unde:

- „Header” - conține informații despre topul mesajului (întrebare sau răspuns), secțiunile ce sunt prezente în mesaj, cerere standard sau specială (folosește cod operație)
- „Question” - conține nume-domeniu, tip și clasă, iar câmpul „Answer” conține informații corespunzătoare răspunsului întrebării
- „Authority”
- „Additional”

Modul în care se realizează o cerere DNS poate fi recursivă sau iterativă.

Domain Name Service – DNS (6)

- Diferența dintre DNS și alte servicii client/server este că un client de DNS rulează ca un serviciu, nu ca o aplicație (DNS resolver)

- Pentru a transmite o cerere către un server DNS putem folosi utilitarele `nslookup`, `host`, `dig`

World Wide Web

- URL (Uniform Resource Locator) reprezintă o adresă web

- Browser web = aplicație client care se conectează la serverul web și face cereri pentru anumite pagini dorite de utilizator
- De obicei paginile sunt în format HTML (Hypertext Markup Language)

Termenul de World Wide Web cunoscut şi sub numele de „www”, reprezintă „rețea mondială” sau „țesătură răspândită în toată lumea”. Această figură de stil este sugestivă, întrucât serviciul este format dintr-o colecție de documente specifice conectate logic între ele numite „hypertext”.

Un „hypertext” este un document ce conține imagini, sunete, texte și legături către documente către același tip.

„Hypertext”-ul este denumit deseori pagini web, iar consultarea informațiilor organizate sub această formă se realizează prin intermediul unui browser web. Browser-ul, pentru a putea localiza resursele web, are nevoie de un URL (Uniform Resource Locator) ce poate fi privit ca o extindere a noțiunii „link către fișier”. Protocolul ce asigură comunicația dintre serverul web și browser poartă numele de HTTP (Hypertext Transfer Protocol).

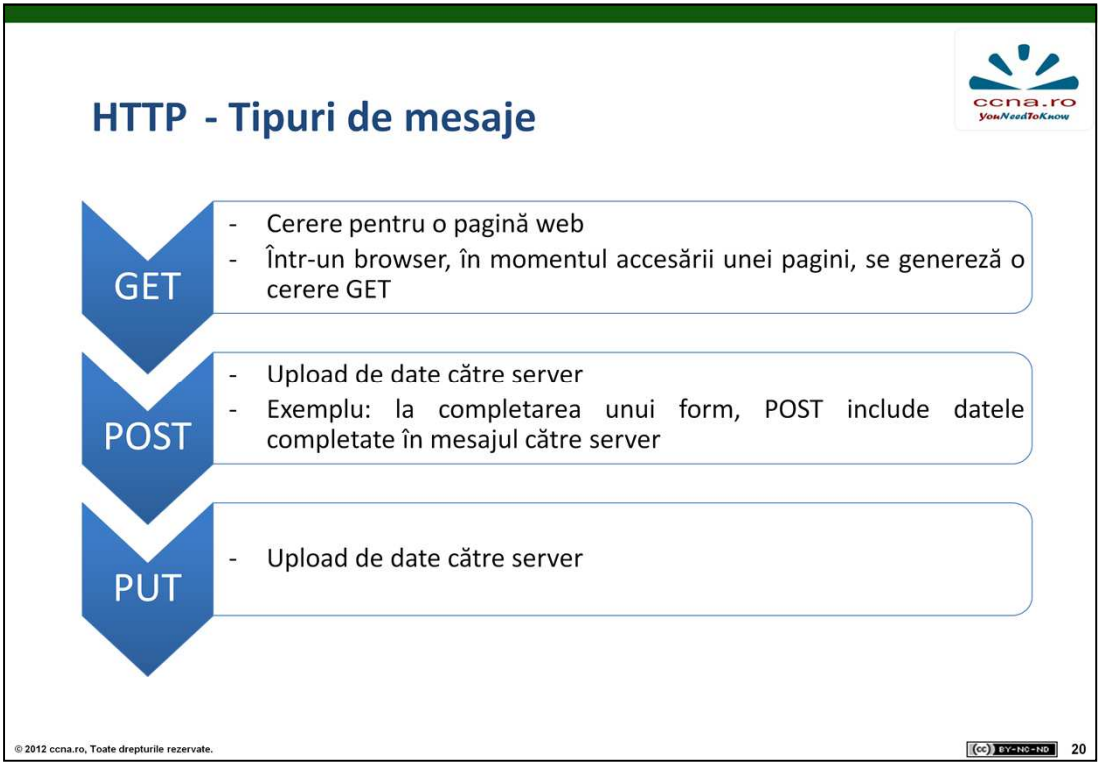
HTTP

- **Hypertext Transfer Protocol**
- Face parte din stiva de protocoale TCP/IP (port 80)
- Original a fost conceput numai pentru transferul paginilor HTML
- În prezent este folosit pentru o gamă largă de tipuri de date
- Unul dintre cele mai folosite protocoale de nivel Aplicație

HTTP este cel mai utilizat protocol de accesare a paginilor web, totodată și cel mai utilizat protocol de nivel Aplicație. Prima versiune HTTP a fost 0.9, care oferea doar posibilitatea de transfer de date printr-o rețea. Următoarea versiune HTTP 1.0 a fost definită de RFC 1945, definit ca un protocol sigur de tip cerere/răspuns, comunicațiile realizându-se peste conexiuni TCP folosind portul standard 80.

HTTP oferă o tehnică de comunicare cu ajutorul cărora un hypertext poate fi transmis de pe un server pe orice alt dipozitiv situat la distanță prin accesarea unui link care în cele mai multe cazuri este un URL.

HTTP-ul se bazează pe mai multe metode pentru a obține informații: POST, GET, HEAD, PUT, DELETE, TRACE.



Corpul unui mesaj HTTP va conține informațiile propriu-zise ale unei cereri sau răspuns, specificate ca o entitate. Formatul mesajului de cerere este de tipul:

Request-Line::=Method Separator Request-URI Separator HTTP-Version CRLF

Method::="OPTIONS"|"GET"|"HEAD"|"POST"|"PUT"|"DELETE"|"TRACE"

Request-URI ::= "*" | absolute-URI | abs_path .

Pentru fiecare cerere a clientului servereul HTTP va răspunde cu o serie de coduri de stare a operației solicitate:

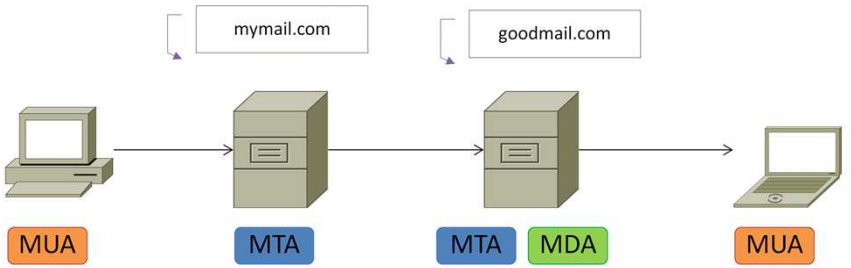
- 200 – cerere realizată cu succes
- 400 – bad request
- 403 – forbidden
- 503 – service unavailable

Unde seminficația fiecărei metode este urmatoarea:

- **Options** – prezintă o cerere de informații despre opținiile de comunicare disponibile
- **GET** – Reprezintă o cerere de accesare a unei informații identificate de Request-URI
- **HEAD** - Funcționalitate similară cu GET, diferența fiind aceea conform căreia sunt cerute informații din antetul antetul paginii web.
- **POST** – Metodă utilizată pentru a identifica dacă serverul acceptă entitatea înglobată în cadrul cererii.
- **PUT** – Specifică faptul că entitatea inclusă în mesaj va fi stocată pe serverul web la adresa specifictă de Request-URI.
- **DELETE** – Cere ca servereul să șterge resursa identificată la Request-URI
- **TRACE** – Trimite o cerere de diagnisticare a erorilor

E-mail

- Pentru transmiterea mesajelor se folosesc trei tipuri de agenți
  - MUA (Mail User Agent)
  - MTA (Mail Transfer Agent)
  - MDA (Mail Delivery Agent)



E-mail sau poșta electronică desemnează modalități pentru transmiterea și primirea de mesaje prin intermediul unei rețele. Termenul de „E-Mail" provine din engleză de la cuvântul „electronic mail", care în traducere liberă înseamnă „poștă electornică", astfel e-mail-urile desemnează mesajele individuale trimise prin intermediul unor servere denumite severe de mail. Acest serviciu este descris în RFC 5322, care stabilește:

- Antetul (header) - include informații despre destinatar, subiect
- Corpul (body) - include infomații despre mesajul propriu-zis

Două exemple de protocoale folosite pentru transferul de e-mail-uri sunt: Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP).

Deși funcționalitatea E-mail-ului este una de tip client-server peste TCP, mesajul parcurge mai multe stadii.

Componentele parcurse de mesaj de la sursă până la destinație poartă numele de agenți.

- ***MTA*** – denumit mail server sau mail exchange server, este un program sau agent software care aigură transferul mesajelor de la un claculator al altul.
- ***MUA*** – denumit e-mail client – este programul folosit pentru citirea, compunerea si transmiterea de mesaje de poșta electronica. Citirea se face prin intermediul protocolului POP3 sau IMAP
- ***MDA*** – server folosit pentru copierea sau accesarea mesajelor stocate în casuța poștală, totodata se ocupă și cu scanarea de viruși și filtrarea de spam-uri.

SMTP

- **Simple Mail Transfer Protocol**
- Folosește portul 25
- Intră în categoria “Mail Transfer Agent”
- Transmite mesajele de la client la server (outbound)
- Se ocupă și de transferul mesajelor între servere

SMTP este protocolul standard la nivelul aplicație, folosit pentru livrarea mesajelor de poștă electronică de la sursă la destinație folosind conexiuni TCP și un schimb de mesaje între client și server.

Determinarea adresei unui server SMTP se realizează pe baza înregistrării MX (MailExchange) din configurația serverului DNS. El oferă și posibilitatea transferului unui e-mail după un server pe altul.

MTA-ul ascultă pe portul specificat cererii de transmisie de mesaje de poștă electronică în format SMTP. SMTP este folosit în cadrul unei sesiuni de comunicație între MUA si MTA sau între două MTA-uri.

Un dezavantaj al SMTP-ului este ca el poate fi folosit doar pentru transmiterea de mail-uri nu și pentru recepționarea lor. În această situație SMTP este dependent de setările ISP-urilor.

POP3 / IMAP

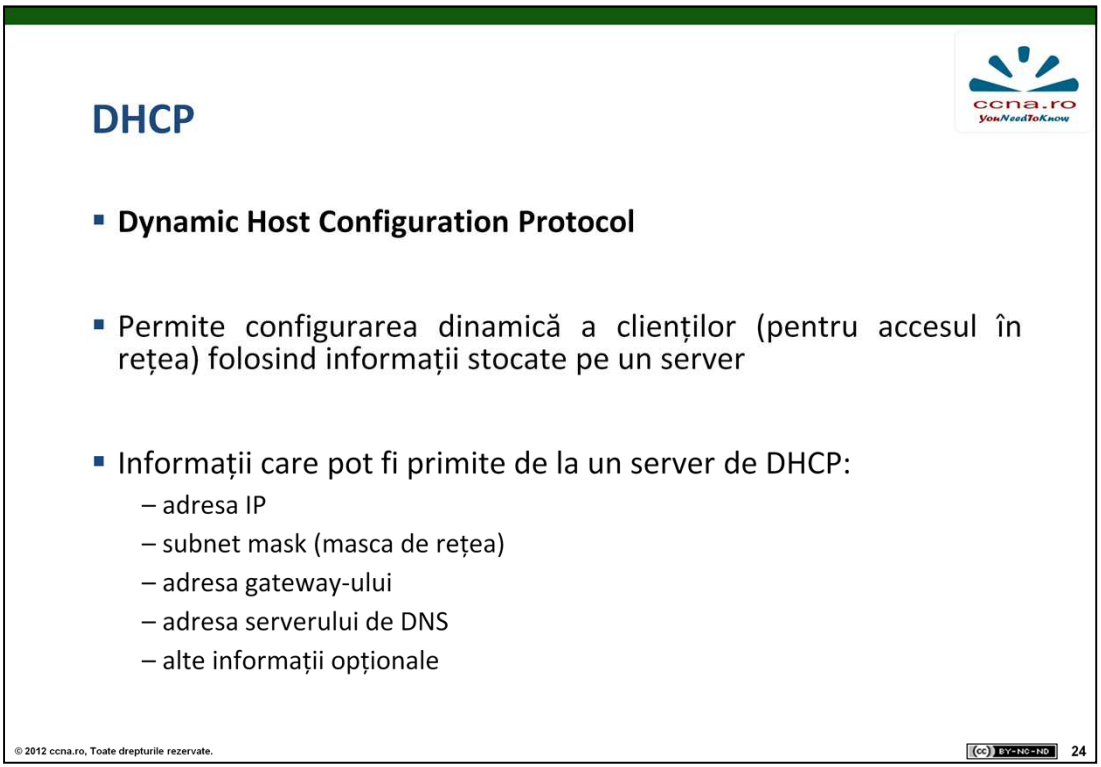
- Intră în categoria “Mail User Agent”
- POP/POP3 (Post Office Protocol)
  - transferă e-mailuri de la server către client (inbound)
  - folosește portul 110
- IMAP (Internet Mail Access Protocol)
  - permite clienților să își citească e-mailurile, fără a le muta de pe server pe mașina clientului
  - folosește portul 143

POP3 alături de IMAP este unul din protocoalele folosite de dispozitivele terminale pentru recepționarea e-mail-urilor.

POP3 este protocolul utilizat de clientul de e-mail (MUA) pentru a descărca mesaje de poștă electronică de pe un server.

IMAP este compatibil cu standardele de transmisie de e-mail-uri permițând accesul și managementul mesajelor de pe mai multe stații de lucru. Spre deosebire de POP3, oferă acces la e-mail-uri fără a folosi un protocol de transferul de fișiere.

IMAP oferă suport pentru modurile de lucru, „online”, „offline” „disconect”, iar accesul la căsuțele poștale publice se realizează într-un mod concurent.



DHCP este un protocol client-server prin intermediul căruia serverul furnizează stației client parametrii de configurare necesari funcționării într-o rețea. Pentru realizarea configurării unei stații folosind un server DHCP au loc următoarele schimburi de pachete:

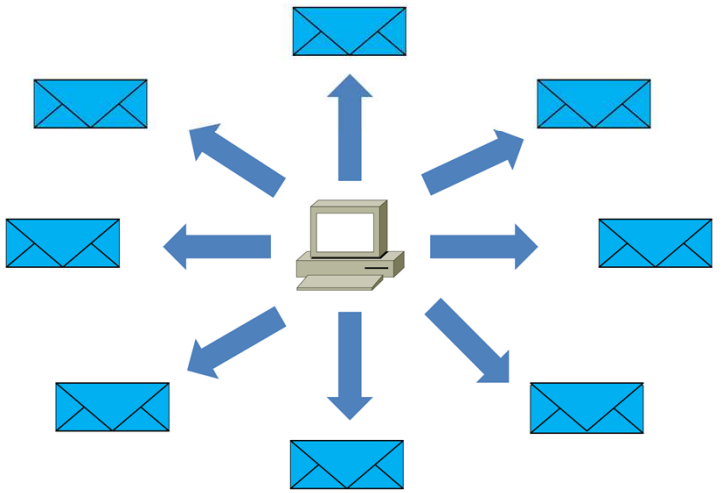
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Ack/Nack

În funcție de modul de configurare, un server DHCP poate oferi trei moduri de alocare a adreselor IP:

- alocare dinamică
- alocare automată
- alocare statică

DHCP (Discover)

- Clientul face broadcast pentru a căuta un server (**Discover**)

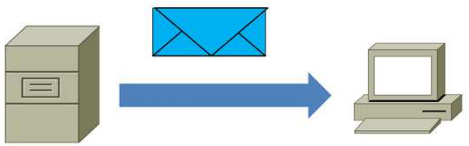


Un client ce dorește ca primească configurațiile necesare pentru a avea acces la resursele rețelei, trebuie sa ceară aceste informații unei server DHCP, acest lucru realizându-se printr-un mesaj de tip broadcast UDP, numit „DHCP Discover”. La primirea acestui pachet fiecare server va rezerva pentru client o adresă IP.

Pe un server pot exista mai multe pool-uri de adrese IP. Rețeaua din care va fi asignată adresa IP se va alege în funcție de interfața după care s-a primit cererea.

DHCP (Offer)

- Serverul DHCP răspunde cu o propunere de configurație (**Offer**)
- Propunerea făcută nu este permanentă (clientul poate solicita altă adresă)



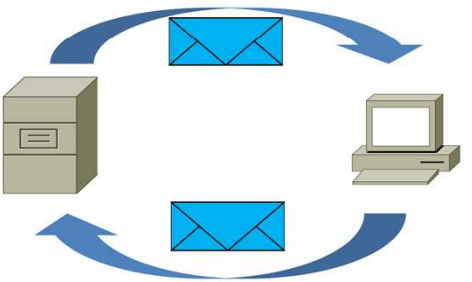
După procesarea cererii şi rezervarea IP-ului, serverul va trimite un răspuns de tip unicast clientului, numit „DHCP Offer”.

În cele mai multe cazuri răspunsul va conține urmatoarele infomații:

- Adresă IP
- Masca de rețea
- Adresa IP a serverului DHCP
- Timpul de închiriere
- Adresa MAC a clientului

DHCP (Request, Ack, Nack)

- Clientul trimite un răspuns de tip "**Request**" serverului, specificând adresa dorită
  - poate fi cea propusă sau una preferată de client
- Serverul răspunde cu "**Ack**" dacă adresa este disponibilă sau cu "**Nak**" altfel
- La deconectare, clientul trimite o cerere "**Release**"



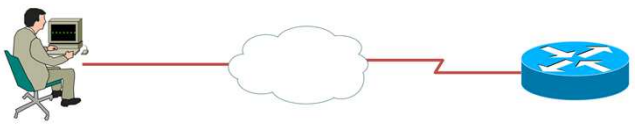
Odată ce pachetul „Offer" este primit de client acesta trimite un mesaj broadcast numit „DHCP Request" pentru a specifica serverului că oferta a fost acceptată. Pachetul este de tip broadcast, deoarece într-o rețea pot exista mai multe servere DHCP, astfel ele fiind informate să elibereze adresele IP rezervate. Acest mesaj poate cuprinde de asemenea și alte specificații: adresa default gateway, adresa IP a serverului DNS sau alte specificații.

După acest proces serverul trimite clientului ACK cu informațiile cerute și confirmarea că adresa IP a fost rezervată pe durata închirierii.

În cazul în care un client trimite o cerere de prelungire a închirierii, aceasta se poate realiza doar după trecerea a jumătate din timpul închirierii.

Telnet (1)

- Oferă posibilitatea de conectare pe un echipament aflat la distanță prin emularea liniei de comandă (Command Line Interface – CLI)
- Port: 23
- Conexiunea realizată folosind protocolul Telnet este denumita VTY (Virtual Terminal)



Telnet este un serviciu de conexiune la distanță nesecurizat, având următoarele caracteristici:

- Nu necesită putere de procesare din partea calculatorului client
- Comenzile scrise la tastatura clientului sunt transmise către server și acesta transmite rezultatul către client
- Procesarea și păstrarea informațiilor au loc pe partea server-ului
- Permite autentificarea utilizatorilor
- Pachetele sunt transmise necriptat (plain text)
- SSH (Secure Shell) - alternativă securizată la Telnet (datele sunt criptate) care folosește portul 22
- O aplicație ce suportă serviciul de Telnet este Putty, iar informațiile nu sunt criptate.

Telnet (2)

- Funcționarea Telnet nu necesită putere de procesare din partea calculatorului client
- Comenzile scrise la tastatura clientului sunt transmise către server și acesta transmite rezultatul către client
- Procesarea și păstrarea informațiilor au loc pe partea server-ului
- Permite autentificarea utilizatorilor
- Datele sunt transmise necriptat (plain text)
- SSH (Secure Shell)
  - alternativă securizată la Telnet (datele sunt criptate) care folosește portul 22

File Transfer Protocol (1)

- Protocol folosit pentru transferul de fișiere
- Se stabilesc două conexiuni între client și server

FTP este un standard pentru transferul de fișiere descris în RFC 959, fiind un protocol general cu următoarele caracteristici: funcționează independent de sistemele de operare şi de platforma hardware, transferă orice tip de fișiere, oferă posibilitatea gestionării unor restricții şi drepturi asupra fișierelor. Modelul FTP folosește două conexiuni: una de control și una de date.

Acest protocol poate rula în două moduri diferite: pasiv şi activ.

File Transfer Protocol (2)

- Conexiunea de date se termină automat după ce se termină transferul unui fișier
- Sesiunea de control se închide când utilizatorul se deconectează
- Transferul datelor se poate face în mod ASCII sau binar
- Poate autentifica utilizatorii

Modul Pasiv presupune conectarea clientului la server, cerând serverului să asculte la o adresă și un port specificat de server.

În cazul modului Activ, serverul se poate conecta la client.

FTP este un protocol nu suportă criptarea datelor, dar exista FTP over SSH care poartă denumirea de SFTP şi BBFTP.

Server Message Block

- Protocol folosit pentru transferul de fișiere de IBM în 1980
- După conectarea la server, clienții pot accesa resursele partajate (fișiere, imprimante, etc.)
- Este suportat atât pe sisteme de operare Windows, cât și pe Linux (Samba) sau pe MacOS
- Protocolul definește
  - inițierea, autentificarea și terminarea sesiunilor
  - controlul accesului asupra fișierelor, imprimantelor
  - modul în care o aplicație permite transmiterea de mesaje între clienți

SMB este un protocol de tip client server, și are urmatoarele caracteristici:

- Conectarea și deconectarea de la fișiere sau imprimante partajate
- Citirea sau scrierea fisierelor partajate
- Crearea sau ștergerea de directoare

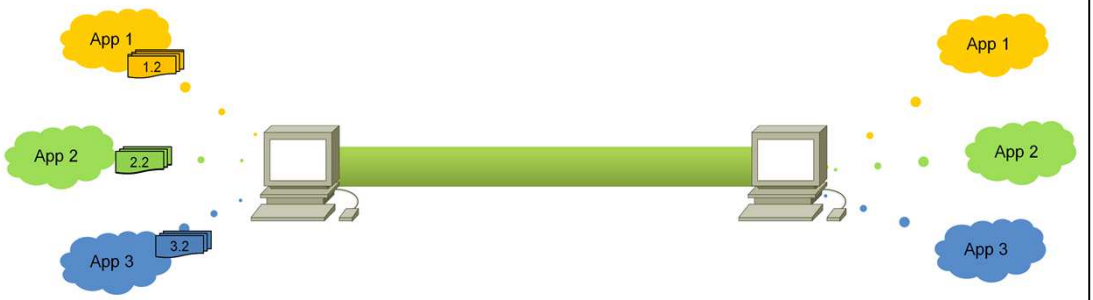
Capitolul 4:
Nivelul Transport

Obiective

- Necesitatea nivelului Transport
- Funcţiile nivelului Transport
- Protocoale specifice nivelului Transport
  - TCP
  - UDP

Comunicaţii concurente

- De cele mai multe ori, activitatea unui utilizator implică existenţa mai multor **fluxuri simultane** de informaţie
- Rolurile nivelului Transport:
  - a organiza acestor conversaţii
  - a oferi o mapare consistentă între **aplicaţii** şi **fluxurile de transport** corespunzătoare



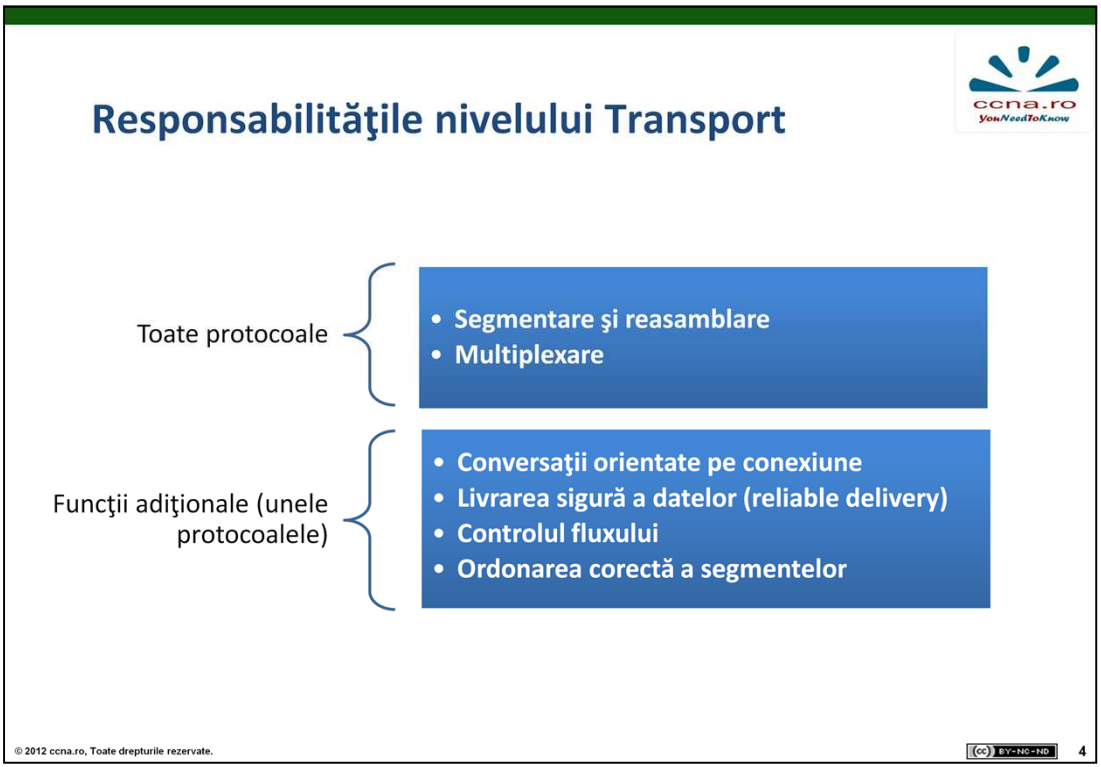
Nivelul Transport este un nivel intermediar care delimitează nivelul hardware de nivelul software.

El oferă un set standard de servicii, independent de tipul reţelei utilizate:

- Transfer sigur de date pe o reţea de comunicaţii considerată nesigură
- Corectarea erorilor când această operaţie nu se realizează pe nivelurile inferioare
- Negocierea calităţii serviciului

Sarcina principală a nivelului Transport este aceea de refacere a fluxului de date la destinaţie, deoarece un pachet poate fi segmentat în mesaje mai mici, cu rute diferite prin reţeaua de comunicaţie.

PDU-ul întâlnit la acest nivel poartă numele de segment.



Nivelul Transport se ocupă de transferul datelor de la sursă către destinație, cât și de la o aplicație la alta.

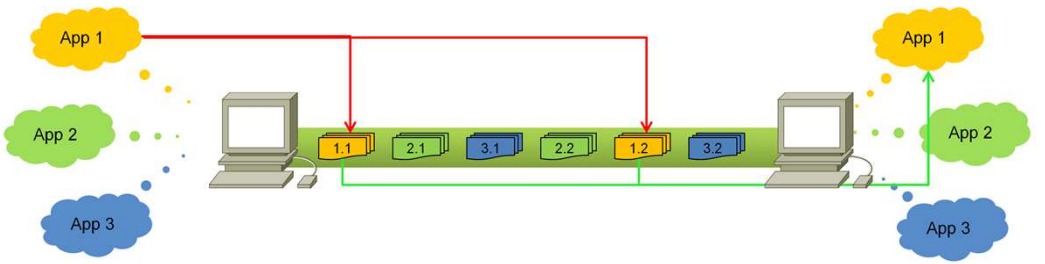
El poate fi sau nu orientat pe conexiune asigurându-se că fluxurile de octeți ajung într-un mod fiabil la destinație, de aici evidenţiându-se caracterul său de reliable.

Pe lângă caracteristicile precizate mai sus putem evidenția existența unor mecanisme de detecție şi corectare a erorilor, dar totodată el oferă posibilitatea conectării prin circuite virtuale, transfer de date prin zone tampon (buffers) și comunicații orientate pe flux de date (stream-uri).

Analizând funcțiile nivelului Transport, putem concluziona că sarcina acestui nivel este de a transporta datele de la sursă la destinație într-un mod sigur, eficient din punct de vedere al costurilor și independent de caracteristicile fizice ale rețelei.

Segmentare şi reasamblare

- Segmentarea este procesul de împărţire a datelor în unităţi mai mici şi de trimitere a acestora la destinaţie
- Când datele ajung la destinaţie, sunt reasamblate şi trimise aplicaţiei corespunzătoare
- Protocol Data Unit-ul (PDU-ul) specific nivelului Transport este **segmentul**.



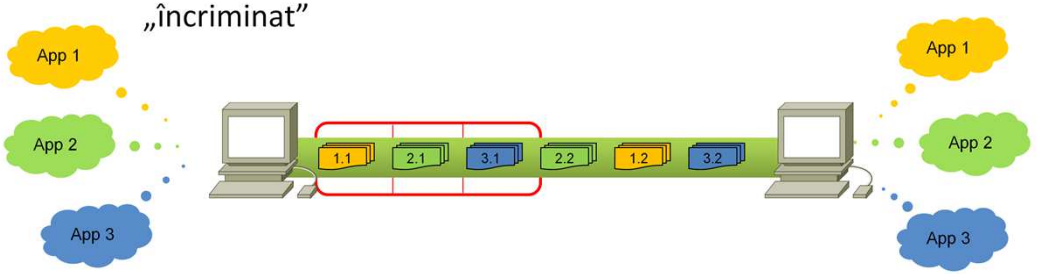
Din punctul de vedere al aplicației, nivelul Transport nu transferă un șir (stream) continuu de octeți prin rețea.

Aplicația nu trebuie să-și facă griji cu segmentarea datelor în blocuri de bază sau datagrame, rolul acesta revenindu-i nivelului Transport prin gruparea octeților în fragmente, care sunt transferate nivelului Rețea pentru a fi transmise la destinație. De asemenea, însuși nivelul Transport, prin protocoalele sale, decide cum să segmenteze datele și cum pot fi trimise cât mai convenabil mai departe.

Reasamblarea segmentelor se realizează la destinație tot de către nivelul Transport, însă modul în care vor fi procesate informațiile depinde de tipul de protocol folosit, TCP-ul realizează reasamblare în ordine, pe când UDP-ul nu.

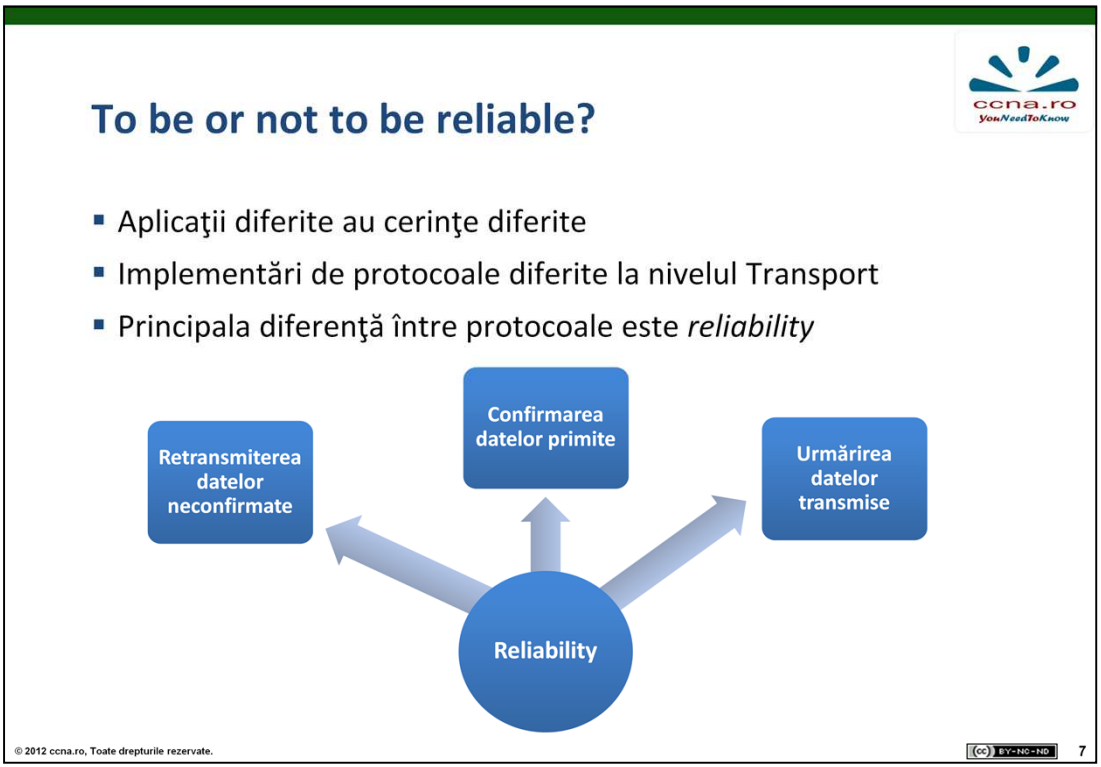
Multiplexare

- Multiplexarea este o metodă prin care mai multe fluxuri de date pot fi transmise peste aceeaşi legătură
- Un beneficiu important al segmentării şi multiplexării îl reprezintă
  - **conservarea lăţimii de bandă**
  - în cazul apariţiei unei erori, este retransmis numai segmentul „încriminat”



Multiplexarea este un proces de transmitere simultană a semnalelor multiple, dar separate, pe un singur canal. Deoarece semnalele sunt trimise într-o singură transmisie complexă, receptorul trebuie să separe semnalele diferite. Două metode principale de multiplexare sunt: multiplexarea cu divizare de timp (TDM) şi multiplexarea cu divizarea frecvenţei (FDM).

În prima metodă (folosită pentru semnale digitale), unui dispozitiv i se acordă un interval de timp în care el poate folosi canalul. În cea de-a doua metodă (folosită pentru semnale analogice), canalul este împărţit în subcanale, fiecare cu o frecvenţă diferită specifică unui singur semnal. Reţelele pe bază de fibră optică pot opera DWDM (multiplexare cu diviziunea simultană a lungimii de undă), în care semnale diferite sunt trimise în mediul din fibră optică, sub forma razelor de lumină cu lungimi de undă diferite.



Protocoalele întâlnite la acest nivel sunt :

- TCP (Transmision Control Protocol)

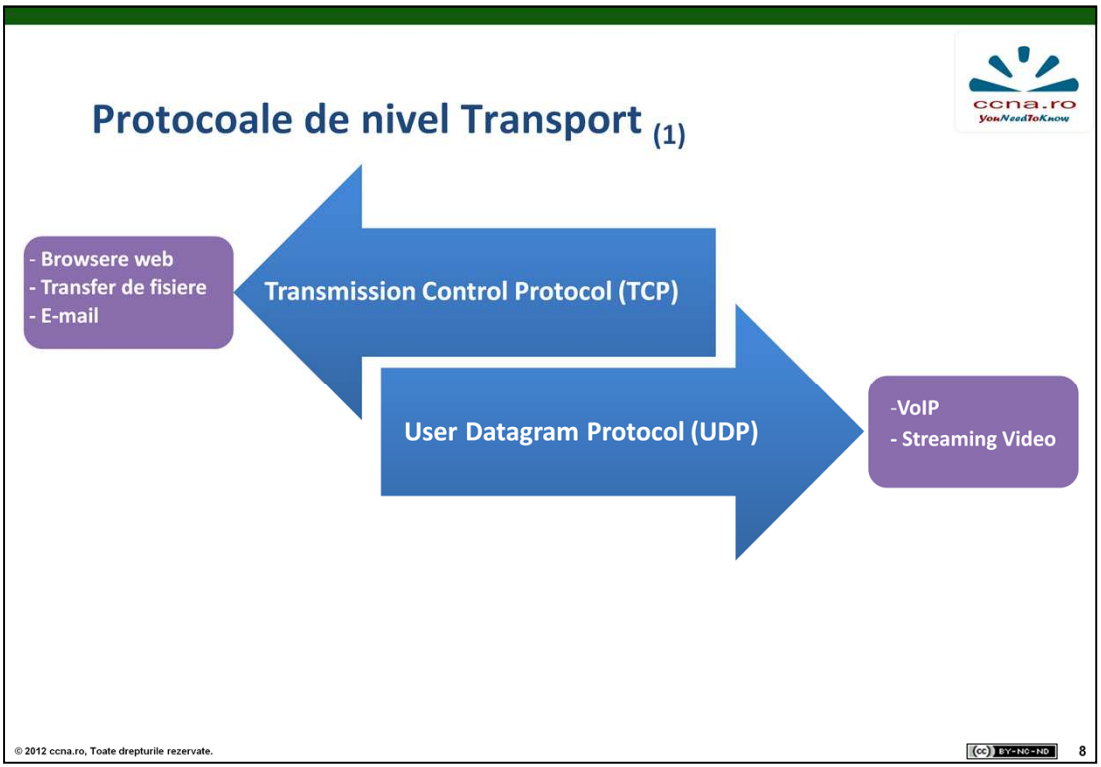
  — este un protocol bazat pe conexiune, unde pentru fiecare pachet transmis se aşteaptă o confirmare din partea echipamentului destinaţie

  — transmisia următorului pachet nu se realizează dacă nu se primeşte confirmarea pentru pachetul transmis anterior

- UDP (User Datagram Protocol)

  — este folosit în situaţiile în care eficienţa şi viteza transmisiei sunt mai importante decât corectitudinea datelor, un exemplu ar fi transmiterea către clienţi a informaţiilor de voce sau imagine, unde viteza este mai importantă decât calitatea

  — este un protocol fără conexiune, semnalarea erorilor sau retransmiterilor fiind asigurată de nivelul superior



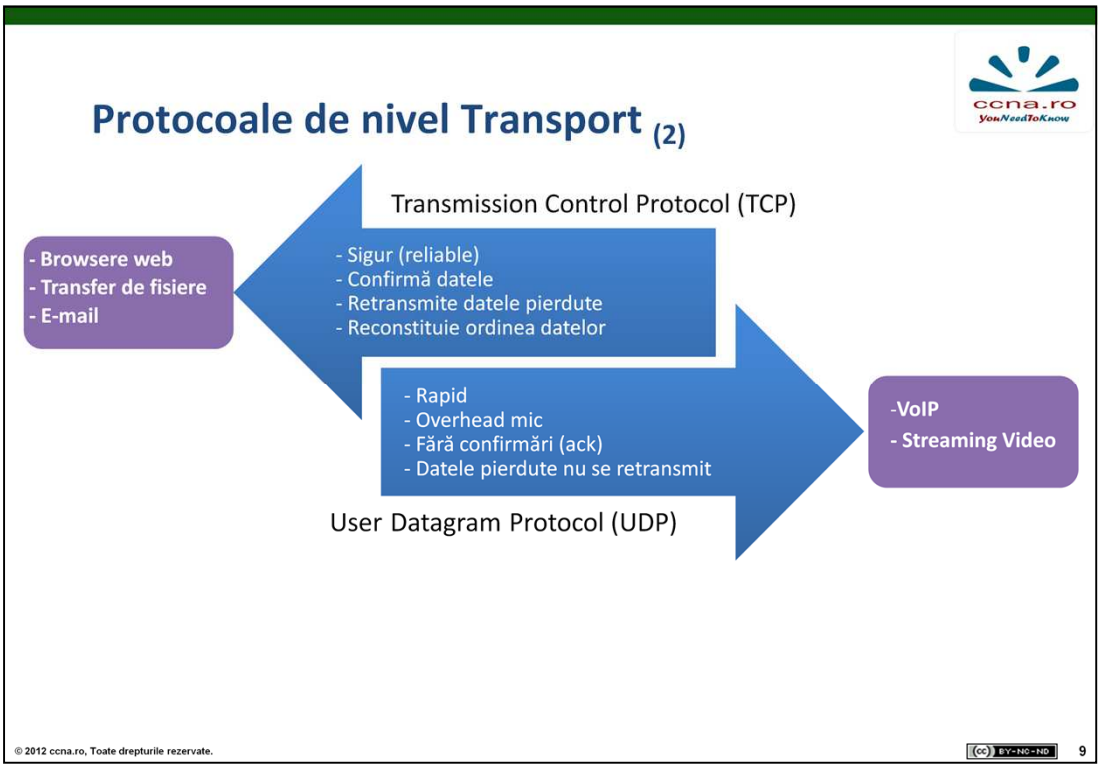
Analizând serviciile ce au luat naștere înaintea comunicației prin rețea, putem face o scurtă comparație cu cele două protocoale.

Astfel UDP-ul este similar poștei terestre deoarece:

- Nu garantează ordinea recepționarii mesajelor
- Mesajul se poate pierde pe rețea

TCP-ul este similar telefoniei întrucât:

- Realizează o conexiune înainte ca datele să fie transmise
- Se asigură de terminarea convorbirii
- Prezintă un dialog între părți, idee evidențiată prin faptul că sursa trimite un pachet și apoi așteaptă confirmarea de primire de la destinatar înainte de a trimite pachetul următor



TCP asigură considerabil mai multe facilităţi pentru aplicaţii decât UDP-ul, mai ales recuperarea erorilor, controlul transmisiei și siguranță.

TCP este un protocol orientat pe conexiune, spre deosebire de UDP, fapt pentru care cele mai multe aplicații protocol, precum Telnet, FTP, ș.a. utilizează TCP.

UDP-ul nu adaugă niciun fel de siguranță, control al transmisiei sau recuperare de erori.

El foloseşte portul drept multiplexor/demultiplexor pentru trimiterea și primirea datagramelor. Antetul UDP conține puține câmpuri pentru transmiterea rapidă a informației, însă necesită ca aplicația să-și asume responsabilitatea pentru recuperarea erorilor.

Porturi (1)

- Porturile reprezintă mecanismul prin care se disting conversaţii multiple la care participă un calculator
- Segmentele TCP şi UDP conţin în antete numere de porturi sursă şi destinaţie
- La crearea unui segment, acestuia i se ataşează un număr de port destinaţie pe care se ştie că destinatarul „ascultă”
- Portul sursă ataşat segmentului se alege aleator
- Portul sursă este folosit de către destinatar pentru a-i putea răspunde expeditorului

Porturile sunt modalități de adresare asemănătoare adresei IP din cadrul nivelului Rețea. Ele se asociază unei aplicații (serviciu) şi nu unei gazde, un proces putând oferi mai multe servicii, deci poate utiliza mai multe porturi.

Un port este asociat în mod diferit celor două protocoale de la acest nivel, ca exemplu: portul 50 UDP este diferit de portul 50 TCP.

Un port este reținut în memoria unui dispozitiv terminal pe 16 biți, astfel valorile lor sunt cuprinse între 0 și 65535.

În funcție de aceste valori sunt clasificate în trei categori: porturi bine cunoscute (Well Known Ports), porturi înregistrate (Registered Ports), și porturi dimamice și/sau private (Dynamic și/sau Private Ports).

Porturi (2)

- Clasificarea porturilor:

Număr port	Tip port
De la 0 la 1023	Porturi bine-cunoscute
De la 1024 la 49151	Porturi înregistrate
De la 49152 la 65535	Porturi private şi dinamice

Înregistrarea porturilor s-a realizat de către Internet Assigned Number Authority în RFC 1700 după cum urmează:

- Porturi rezervate (Well-known ports) - între 0-1023 :
  - SSH
  - Telnet
  - HTTP
- Porturi înregistrate (Registred ports) - între 1024 și 49151:
  - Kazza
  - MySQL
  - RMI Registry
- Porturi dinamice și private (private and dynamic ports) - între 49152 și 65535:
  - testare locală

Porturi (2)

Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
443	TCP	SSL/HTTPS

Un port poate fi înregistrat atât pentru TCP cât și pentru UDP. Unele protocoale folosec doar portul TCP: FTP (20 pentru transmiterea datelor și 21 pentru control), SSH (port 22), Telnet (port 23), HTTP peste SSL (port 443), etc.

Alte protocoale folosesc în transmiterea informației doar portul UDP: DHCP (porturile 67, 68) sau TFTP (port 69). Cu toate acestea, sunt protocoale care au implementări pentru ambele protocoale de transport, cum este protocolul DNS, care funcționează fie pe TCP port 53, fie UDP port 53.

Lista completă de porturi se găsește la adresa:

www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.

Pe sistemele Linux, această listă se poate găsi în fișierul /etc/services.

Porturi (3)

- Corespondenţa dintre adresa IP şi numărul de port identifică în mod unic o aplicaţie care rulează pe un anumit calculator dintr-o reţea
- Această asociere se mai numeşte socket

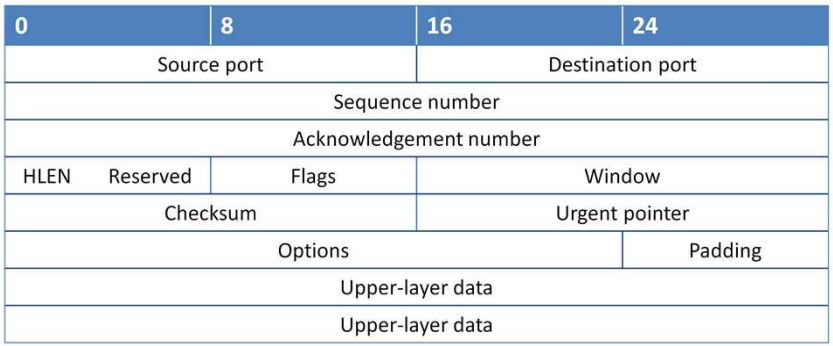
Multiplexarea presupune ca două sau mai multe procese de pe același dispozitiv să acceseze simultan resursele rețelei. Pentru aceasta se realizează o asociere între adresa de port și adresa IP care poartă numele de socket.

Astfel o conexiune este identificată într-un mod unic de socket, însă există posibilitatea ca la intervale de timp diferite să fie folosit același socket de mai multe conexiuni.

Cu alte cuvinte un socket este o abstracțiune software folosită pentru a reprezenta fiecare din cele două „capete” ale unei conexiuni între două procese ce rulează într-o rețea. Fiecare socket este atașat unui port astfel încât să poată identifica unic programul căruia îi sunt destinate datele.

TCP - Overview

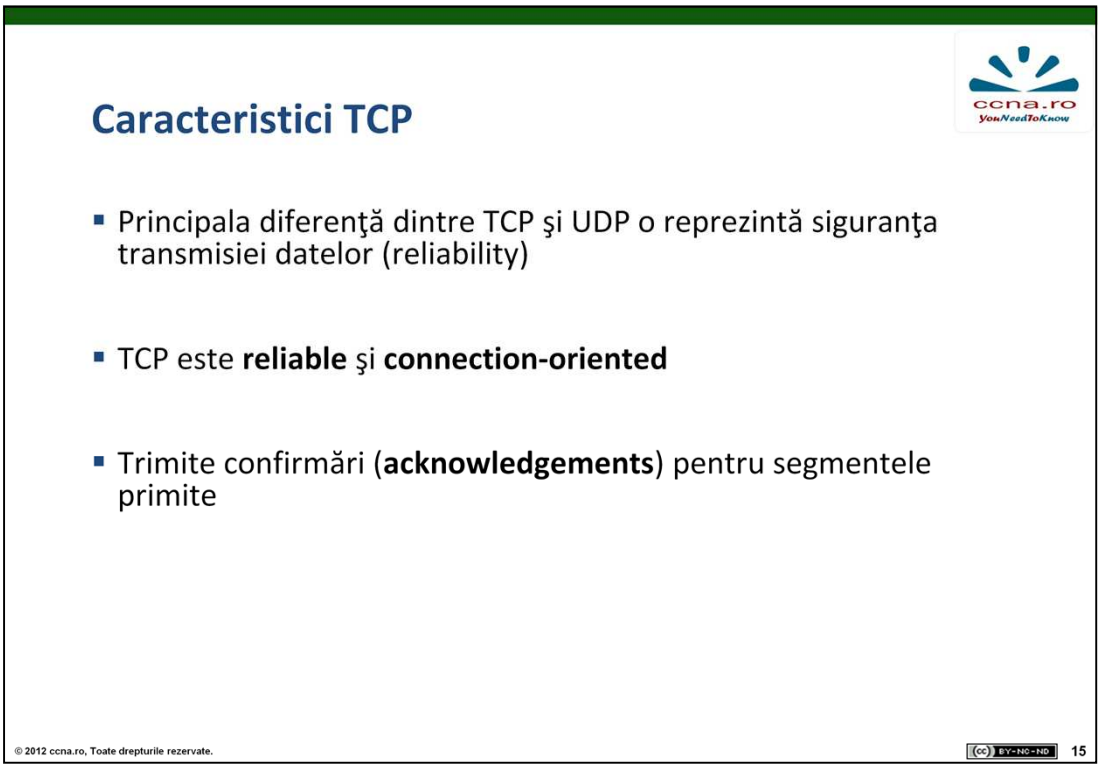
- Deziderатul principal al TCP-ului este transmisia **corectă** şi în ordine a mesajelor
- Pentru a putea efectua acest lucru sunt necesare mai multe câmpuri în cadrul antetului, care introduc **overhead**



0	8	16	24
Source port		Destination port	
Sequence number			
Acknowledgement number			
HLEN Reserved	Flags	Window	
Checksum		Urgent pointer	
Options			Padding
Upper-layer data			
Upper-layer data			

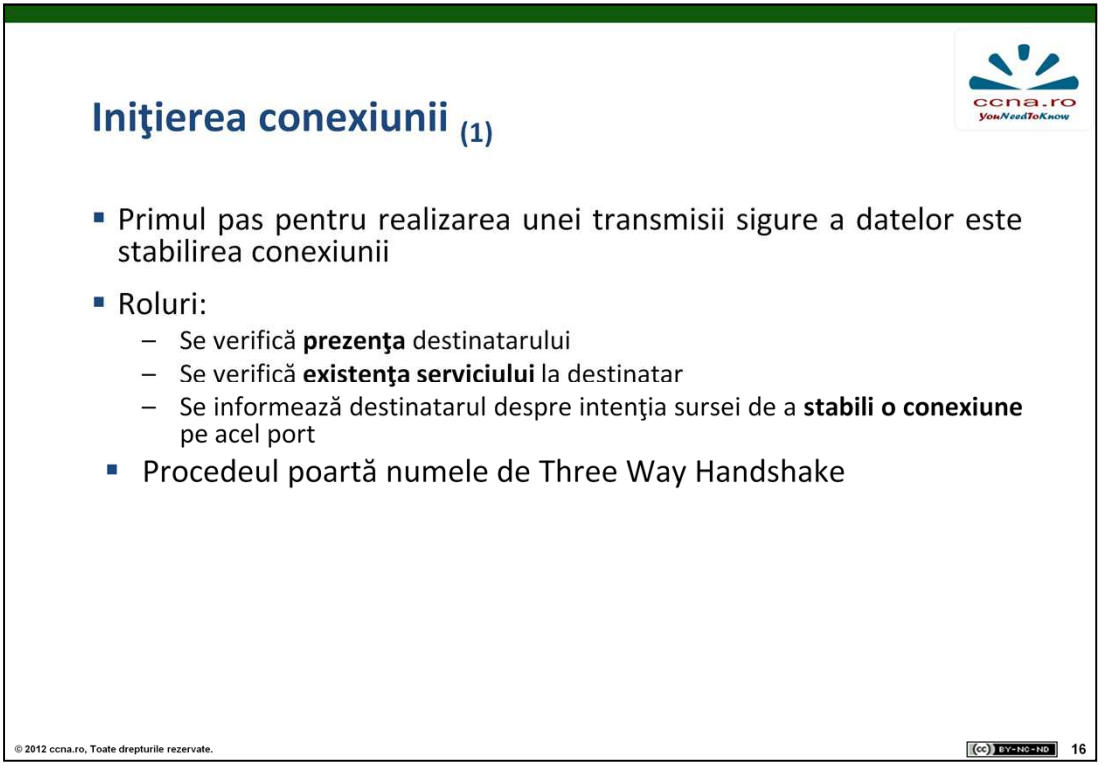
Semnificația câmpurilor din antetul TCP este următoarea:

- Source port **-** numărul portului sursă
- Destination port **-** numărul portului destinație pe 16 biți
- Sequence number - numărul de secvență al primului octet de date
- HLEN - el indică unde încep datele
- Reserved - șase biți rezervați pentru utilizare în viitor
- Window - indică numărul de segmente după care se așteptă ACK
- Checksum - folosit pentru identificarea erorilor
- Padding - pentru completarea lungimii minime a cadrului
- Flags - identifică tipul flag-ului (ACK, FIN, SYN, etc)
- Options - câmp folosit pentru adăugarea de opțiuni protocolului



Principalul scop al TCP este de a asigura un circuit logic sigur sau serviciu de conexiune între două procese pereche. El nu se bazează pe siguranța altor protocoale de nivel inferior, așa că trebuie să garanteze el însuși siguranța transmisiei. TCP este caracterizat prin următoarele facilități pe care le asigură pentru aplicațiile care îl utilizează:

- Siguranță (reliable) - atribuie un număr de secvență fiecărui octet transmis și așteaptă o confirmare
- Controlul transmisiei (Flow Control) - aplicația TCP destinație, când transmite o confirmare (ACK) către sursă, indică și numărul de octeți pe care îi poate recepționa fără să apară depășirea memoriilor tampon (internal buffers) ale sale
- Multiplexare - prin utilizarea porturilor
- Orientare pe conexiune - stabilește o conexiune între sursă și destinație înainte să transmită informațiile

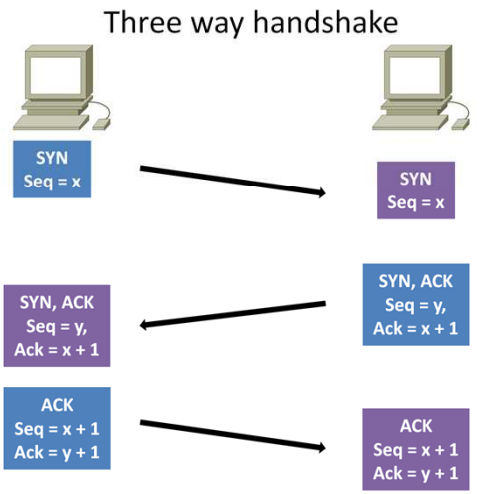


După cum s-a constatat, TCP-ul este un protocol orientat pe conexiune, iar stabilirea conexiunii şi determinarea erorilor au la bază principiul ferestrei glisante modificat astfel:

- Deoarece TCP asigură o conexiune de flux de octeți (byte-stream connection), numerele de secvență sunt atribuite fiecarui bit din flux
- Principul ferestrei glisante este folosit la nivel de octet, adică segmentele trimise și confirmările vor transporta numere de secvență pentru octet, iar dimensiunea ferestrei va fi exprimată în număr de biţi în loc de număr de pachete
- Dimensiunea ferestrei este determinată de către receptor când conexiunea este stabilită și variază în timpul transferului de date

Iniţierea conexiunii (2)

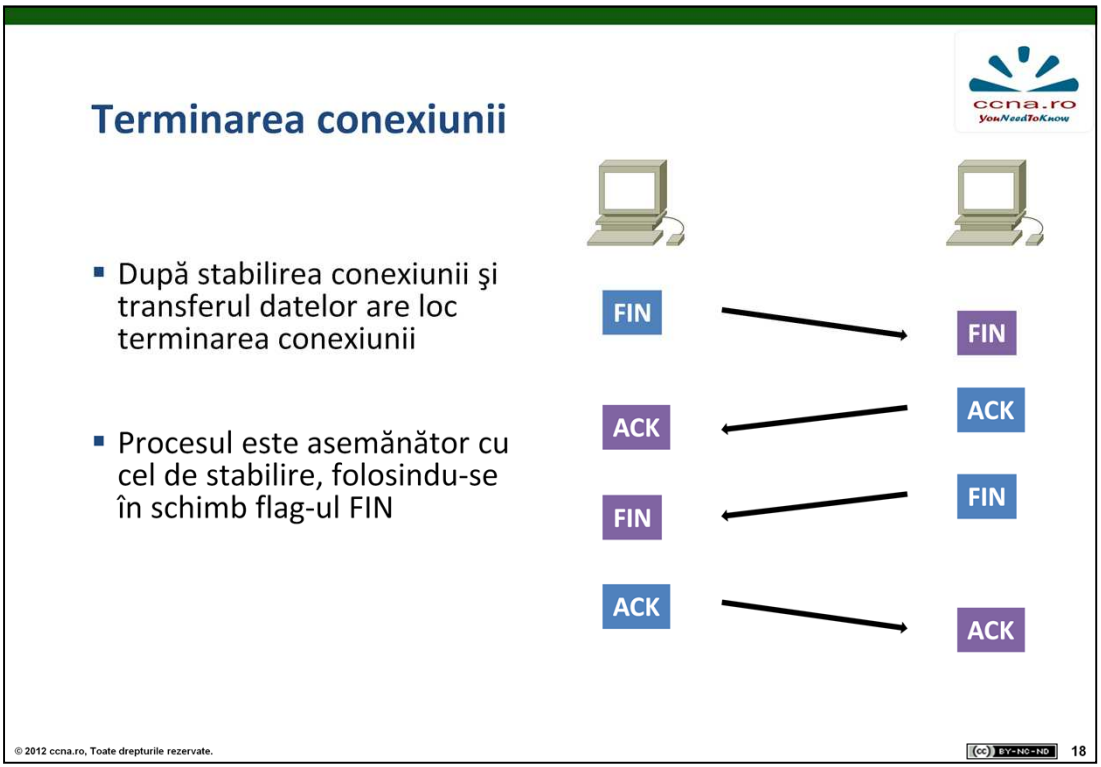
- Sequence number (Seq)
- Acknoledgment number (Ack)
- Flags:
  - SYN
  - ACK



Inițierea conexiunii, este realizată în cele mai multe cazuri de către client, moment în care antetul TCP are bitul de SYN este activat.

Protocolul de inițiere de conexiune (three way handshake) funcționează astfel:

- Pachet are bitul de SYN activat și stabilește Initial Sequence Number (ISN) pentru comunicația de la sursă la destinație
- Al doilea pachet are activat SYN-ul și ACK-ul, având drept rol confirmarea primului pachet și determinarea ISN pentru comunicația de la destinație la sursă
- Cel de-al treilea pachet are activat ACK-ul, confirmând primirea celui de-al doilea pachet și încheie stabilirea conexiunii



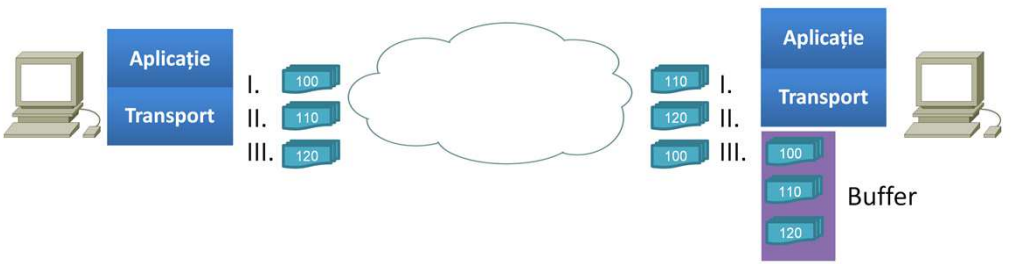
Terminarea conexiunii se realizează prin activarea bitului FIN în cadrul antetului TCP și, spre deosebire de inițiere, ea poate fi cerută de orice capăt al comunicației.

Modul de funcţionare al închiderii este următoarea:

- Primul pachet conţine câmpul FIN activat
- Al doilea pachet este o confirmare a primului, dar totodată conţine și bitul de FIN activat, astfel, în acest moment, conexiunea este pe jumătate închisă (HALF CLOSED)
- Ultimul pachet este o confirmare a celui de-al doilea, marcând terminarea conexiunii

TCP – segmentare şi reasamblare

- Există posibilitatea ca pachetele asociate unui flux TCP să urmeze căi diferite până la destinaţie, ajungând în altă ordine decât cea de la sursă
- Pentru a permite reasamblarea, TCP foloseşte **numerele de secvenţă(Seq)** din cadrul antetului
- Destinaţia menţine un buffer în care segmentele sunt reasambate şi apoi trimise nivelului Aplicaţie



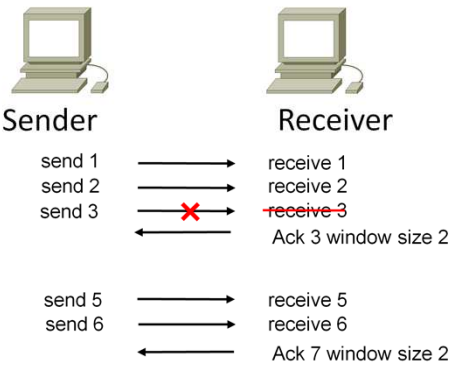
Numerele de secvență sunt folosite de către TCP pentru a se asigura că datele care se pierd datorită problemelor apărute în rețea, pot fi recuperate.

TCP ordonează segmentele într-o anumită ordine prin transmiterea către destinație a unei confirmări prin intermediul ACK-ului. Fiecare pachet este numerotat înainte de a fi transmis, iar la destinație TCP reasamblează segmentele pentru a forma mesajul inițial.

În cazul în care numărul unei secvențe lipsește din cadrul seriei pe care trebuia să o recepționeze destinația, segmentul va fi retransmis. De asemenea segmentele a căror recepție nu este confirmată într-o perioadă de timp vor fi retransmise.

Controlul fluxului în TCP (1)

- În antetul TCP se transmite numărul de confirmare
  - numărul următorului segment aşteptat (expectational acknowledgement)
- Conexiunea este stabilită two-way, deci se transmit confirmări în ambele sensuri
- În cazul pierderilor de date, ACK-ul va conţine numărul primului segment pierdut



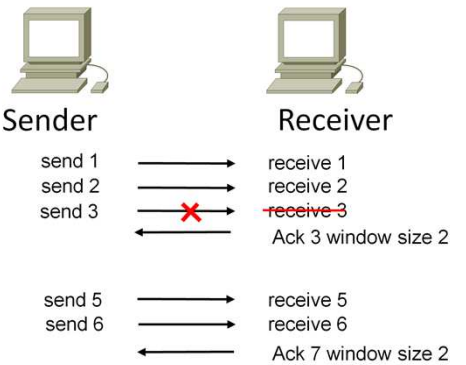
Un al rol al TCP este de control al fluxului, adică de a încetini emiţătorul în cazul în care nu este capabil să proceseze datele suficient de repede. O metodă extremă ar fi neconfirmarea de către receptor a octeților ce nu sunt procesați. Însă această metodă are ca dezavantaj generarea unui trafic inutil.

Soluția utilizată de TCP este ca receptorul să semnalizeze prin valoarea câmpului Window din antet, numărul de octeți pe care receptorul este capabil să-i recepționeze în acel moment.

Controlul fluxului este folosit pentru a evita ca expeditorul să nu trimită prea multe date către receptor. Acest mecanism este util datorită diferențelor cu care un dispozitiv poate prelucra informația la un moment dat.

Controlul fluxului în TCP(2)

- Viteza de transmisie este stabilită de mărimea unei „ferestre” (fereastră glisantă)
  - numărul de segmente ce pot fi trimise înainte de a se aştepta o confirmare
- Destinatarul poate să „negocieze” o mărime mai mică a ferestrei de transmisie dacă este nevoie
- În funcție de calitatea transmisiei informaţiilor (pierderi sau consum de resurse) sursa poate să crească mărimea ferestrei



Viteza de transmisie este stabilită de mărimea unei „ferestre” (sliding window) prin care se specifică numărul de segmente ce pot fi trimise înainte de a se aştepta o confirmare.

Destinatarul poate să „negocieze” o mărime mai mică a ferestrei de transmisie dacă este nevoie. După o perioadă în care transmisia se desfăşoară fără pierderi și fără un consum mare de resurse, sursa va începe să crească mărimea ferestrei.

Pe lângă mecanismul menționat mai sus, emiţătorul TCP reduce debitul de date emise și în cazul în care constată pierderi de pachete. Ideea este că pachetele se pot pierde fie ca urmare a erorilor la nivel fizic, fie ca urmare a congestiei nodurilor intermediare.

Congestia reprezintă degradarea performaţelor unei rețele în urma încărcării acesteia cu un număr foarte mare de pachete.

Antetul UDP

- UDP oferă mult mai puţine facilităţi decât TCP, antetul fiind simplificat şi redus doar la câmpurile strict necesare, ajungând la o mărime de 8 octeţi

0	16	32	48	64 ...
Source Port	Destination Port	Length	Checksum	Data

- UDP este un protocol simplu, neorientat pe conexiune, cu puţin overhead
- Segmentele UDP se numesc **datagrame** iar transmisia lor se consideră că este de tip **best effort**

UDP asigură un mecanism pentru ca o aplicație să trimită o datagramă unei alte aplicaţii. În limbajul curent unitățile de transmisie a informației pentru UDP se numesc datagrame UDP. Cu toate că datagrama poate fi fragmentată în timpul transmisiei, implementarea IP a calculatorului destinație o va reasambla înainte de a o prezenta nivelului Transport. Semnificația câmpurilor din antetul UDP este urmatoarea:

- Source port - indică portul procesului emitent
- Destination port - precizează portul procesului destinație
- Length - evidențiază lungimea în octeți a datagramei
- Checksum - este un câmp pe 16 biți utilizat pentru detectarea unor modificări ale segmentului

UDP Pros & Cons

- Protocol simplu
- Neorientat pe conexiune
- Nu dispune de mecanisme de retransmisie, numere de secvenţă sau fereastră glisantă
- Antetul UDP este mai mic decât cel al TCP-ului şi este preferabil în reţele în care pierderile sunt foarte reduse
- Nu foloseşte niciun sistem pentru a le reorganiza sau a retransmite datele pierdute pe reţea

În concluzie analizând antetul UDP-ului se observă că el nu asigură siguranța livrării, controlul transmisiei și recuperarea erorilor, astfel încât acestea trebuie asigurate de către aplicație.

Dintre aplicațiile standard care utilizează UDP enumerăm:

- Trivial File Transfer Protocol (TFTP)
- Serverul de nume DNS (Domain Name System)
- Remote Procedure Call (RPC), utilizat de către NFS (Network File System)
- Simple Network Management Protocol (SNMP)
- Lightweight Directory Access Protocol (LDAP)

Capitolul 4: Nivelul Rețea

Obiective

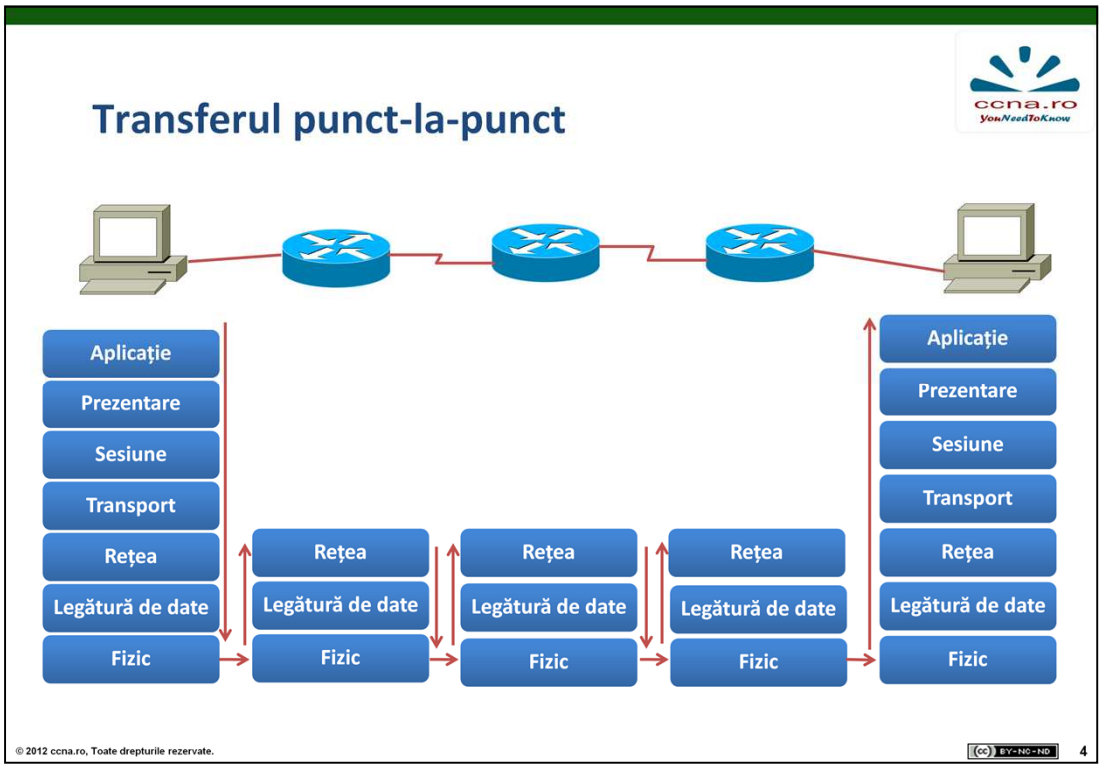
- Rolul nivelului Rețea
- Protocolul IP
- Rutarea pachetelor

Nivelul Rețea

- Reprezintă nivelul 3 din stiva de protocoale OSI și este echivalent cu al doilea nivelul din stiva de protocoale TCP/IP (Internet)
- La acest nivel au loc împachetarea și transportarea datelor provenite de la nivelul Transport
- Transferul punct-la-punct este alcătuit din trei etape
  - încapsularea
  - rutarea
  - decapsularea

Nivelul Rețea este nivelul 3 din modelul OSI responsabil cu transmiterea pachetelor incluzând rutarea între sisteme intermediare fără gestionarea fluxului datelor sau verificarea erorilor apărute în timpul comunicației. Entitățile de transport se identifică prin adresele de rețea, în mod unic. Nivelul rețea are următoarele funcții:

- Încapsularea/decapsularea datelor primite
- Rutarea și livrarea pachetelor în cadrul rețelelor
- Adresarea pachetelor
- Segmentarea pachetelor pentru a respecta dimensiunea cadrului impusă de către protocoalele de la nivel inferior
- Diferențierea pachetelor în funcție de tipul serviciului
- Verificarea integrității antetului



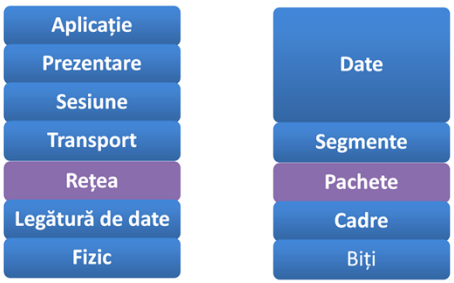
Dacă în capitolele 3 si 4 s-a observat cum aplicațiile și serviciile de pe o stație pot comunica eficient cu aplicațiile și serviciile de pe o altă stație, în continuare este prezentat modul în care sunt transmise datele prin intermediul rețelei de la o stație sursă la o stație destinație, realizându-se rutarea pachetelor.

Protocoalele de rețea specifică modalitatea de adresare a pachetelor cât și procesele care permit transportul și încapsularea datelor primite de la nivelul superior.

În timpul transmisiei datelor pe rețea, fiecare echipament intermediar care realizează funcția de rutare, decapsulează PDU până la nivelul Rețea pentru citirea adresei stației destinație și pe baza acestei informații alege calea optimă.

Încapsularea

- PDU-urile de la nivelul Reţea se numesc „pachete”
- Protocoalele de la nivelul Rețea definesc structura și modul de procesare al pachetelor
- Fiecare pachet conține un antet (header) în care se regăsesc adresele IP sursă și IP destinație

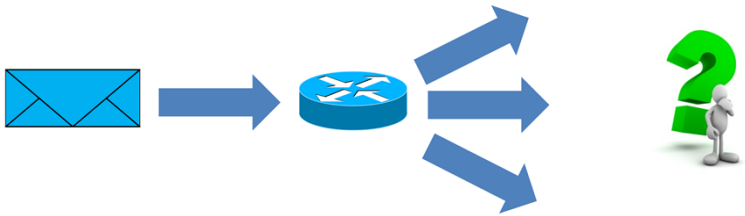


Când o stație transmite informații pe rețea, datele trec printr-un proces numit ***încapsulare*** care reprezintă adăugarea unor informații la diferite nivele ale stivei OSI. În funcție de nivelul la care informațiile sunt încapsulate, sunt create diferite tipuri de PDU (Protocol Data Units). La nivelul Rețea PDU-urile poartă numele de ***pachete.*** Nivelul Rețea primește segmentul încapsulat de la nivelul superior și îi adaugă un antet care conține, pe lângă alte informații, adresarea logică, respectiv adresele IP sursă și destinație. În final, pachetul este transmis mai departe nivelului Legătură de date. Procesul de transmitere a datelor:

- Generarea datelor la nivelul Aplicație, Sesiune și Prezentare
- Crearea ***segmentelor*** (antet TCP sau UDP)
- Crearea ***pachetelor*** (adăugarea unui antet IP)
- La nivelul Legătură de date, crearea ***cadrelor***
- Transmiterea informației pe mediu (encodarea informațiilor)

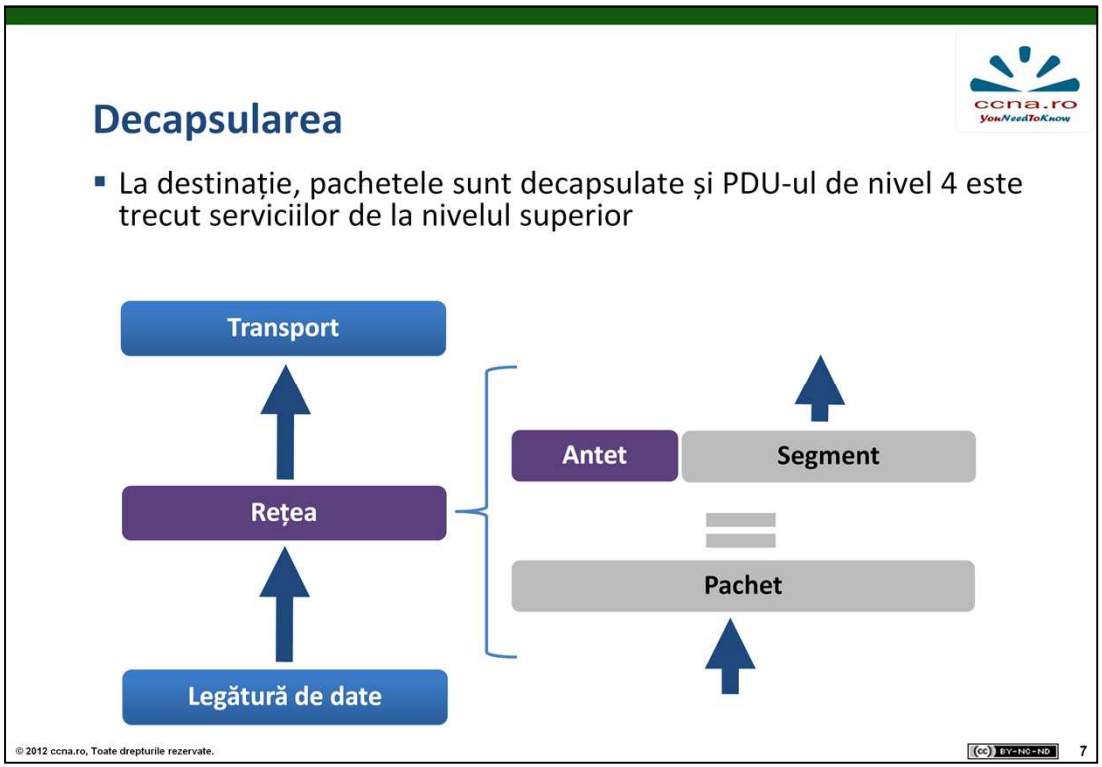
Rutarea

- Serviciile de rețea se ocupă cu direcționarea pachetelor prin Internet către adresa destinație
- Ruterele sunt dispozitive intermediare care au rolul de a selecta căile pe care pachetele sunt trimise
- *Hop*: reprezintă trecerea unui pachet de date între două noduri de rețea
- Datele încapsulate în PDU de la nivelele superioare rămân intacte în timpul proceselor de la nivelul rețea



Rutarea este procesul de selectare a căii de transmitere a informației între mai multe rețele. Stațiile sursă și destinație nu sunt întotdeauna conectate la aceeași rețea. Pe parcursul traseului fiecare pachet trebuie să fie ghidat prin diferite rețele pentru a ajunge în final la rețeaua destinație. Echipamentele care decid calea cea mai bună sunt ruterele care în funcție de adresa IP a destinației aleg portul pe unde va fi transmis pachetul.

Rutarea pachetelor se face pe baza unei tabele de rutare care specifică pentru fiecare rețea destinație în parte, interfața de ieșire sau next hop-ul spre rețea, dar și alte informații suplimentare precum distanța sau costul spre rețea.



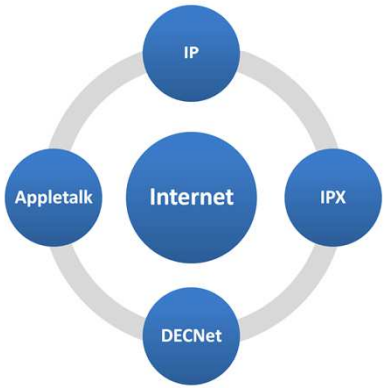
Decapsularea este procesul invers încapsulării și reprezintă extragerea informațiilor din PDU (Protocol Data Units), prin înlăturarea antetelor. Pachetul este primit de la nivelul Legătură de date, este analizată adresa IP destinație, și dacă aceasta corespunde cu adresa IP a stației, este extras segmentul din pachet și transmis mai departe nivelului superior.

În momentul primirii unui pachet, ruterul extrage din antet IP-ul destinație.

Pe baza acestui IP caută în tabela de rutare pentru a afla dacă există vreo rută către rețeaua destinație. Dacă nu are rețeaua în tabela de rutare, ruterul aruncă pachetul, iar dacă rețeaua există în tabela de rutare, echipamentul încapsulează pachetul cu informațiile de nivel 2 și transmite mai departe datele.

Protocoalele nivelului Rețea

- Dispozitivele intermediare de nivel 3
  - pot implementa în același timp mai multe protocoale de nivel 3
  - nu iau în considerare decât informația din antetul pachetelor



Echipamentele de nivel 3, pot ruta diferite protocoale. Acestea oferă mecanisme de identificare a sursei și a destinației.

DECnet: Suita de protocoale DECnet a fost implementată de Digital Equipment Corporation în 1970. Rutarea DECnet era implementată pe diferite tehnologii ca Ethernet, Token Ring, FDDI, HDLC, PPP, Frame Relay. DECnet suportă atât rețele orientate pe conexiune cât și rețele neorientate pe conexiune.

Appletalk: AppleTalk este seria de protocoale dezvoltată de Apple Inc, în anul 1984, dar în prezent nu mai este suportată de echipamente fiind înlocuită de stiva TCP/IP din 2009.

IPX: Internetwork Pachet Exchange este protocol de rețea din suita de protocoale IPX/SPX.

IP (Internet Protocol) face parte din suita de protocoale TCP/IP, protocol folosit pentru adresare logică.

Internet Protocol (1)

- IPv4, IPv6 – cele mai cunoscute protocoale de nivel 3
- Stiva TCP/IP implementează la nivelul „Internet” protocolul IP
- IPv6 nu este implementat, deocamdată, decât în zone izolate
- Nu implementează tehnici de controlul fluxului

Internet Protocol este cel mai răspândit protocol de rețea și a fost proiectat în special pentru rutarea pachetelor în rețea de la sursă la destinație folosind exclusiv adresa IP a destinației. A fost definit în RFC 791 ca parte a stivei TCP/IP.

Cele mai cunoscute versiuni ale acestui protocol sunt IPv4 și IPv6. Adresele IPv4 sunt formate din patru octeți, existând o parte de rețea și o parte de host. Cea mai nouă versiune este versiunea IPv6 care are o adresare de 16 octeți (128 biți).

Protocolul IP a fost conceput ca având un overhead foarte mic, realizând doar funcțiile necesare transmisiei pachetelor de la sursă la destinație. Protocolul nu urmărește sau gestionează fluxul de pachete, aceste funcții fiind realizate de către protocoale de la alte nivele.

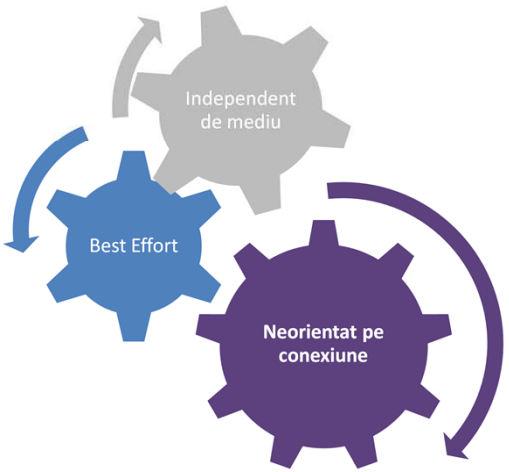
IP nu asigură posibilitatea că o stație care trimite date cu o viteză mai mare ca maximul acceptat de destinație, să se realizeze cu succes.

Internet Protocol (2)

- Protocolul IP este considerat

un protocol:

  - Neorientat pe conexiune
  - Best Effort (unreliable)
  - Independent de mediu



Connectionless:

- Nu se stabilește o conexiune anterior trimiterii pachetului
- Nu necesită schimbul prealabil de informații de control
- Există posibilitatea ca pachetele să nu ajungă în ordine, să se piardă sau să fie amestecate cu alte pachete
- Când este trimis pachetul, sursa nu știe dacă stația destinație există în rețea, dacă pachetul a ajuns la destinație

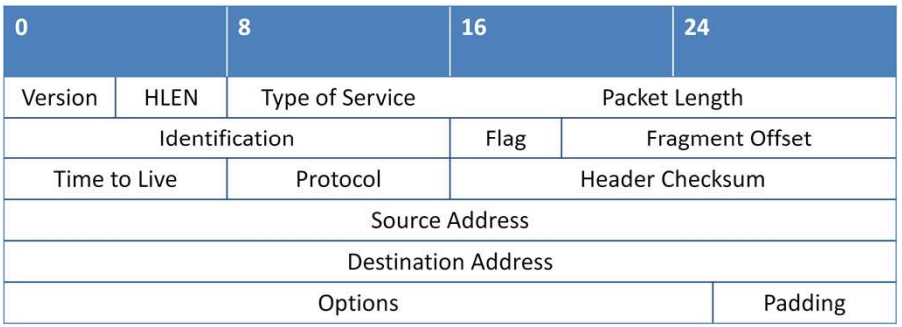
Best Effort:

- Nu se garantează ajungerea pachetelor la destinație
- Protocolul IP nu are posibilitatea de a recupera pachetele care nu au ajuns la destinație sau care au fost eronate.

Media independent:

- Poate fi implementat peste mai multe tipuri de dispozitive fizice

Antetul IPv4



Antetul IPv4 conține următoarele câmpuri:

- Version: Tipul versiunii IP (4-IPv4, 6-IPv6)
- Header Length: Numărul de octeți ai antetului IP în cuvinte de 32 biți
- Type of Service: Indică prioritatea datagramei, QoS
- Total length: Numărul de octeți ai pachetului
- Identification: Necesar pentru reasamblarea la recepție a pachetului
- Flags: Indică fragmentarea pachetului
- Fragment offset: Definește poziția fragmentului în cadrul datagramei
- Time To Live (TTL): Folosit pentru evitarea buclelor de rutare
- Protocol: Indică tipul următorului antet (1 - ICMPv4, 6 - TCP, 17 - UDP)
- Header checksum: Verificarea corectă a transmisiei antetului IP
- Padding: Câmp folosit pentru completarea antetului atunci când acesta nu conține un număr întreg de cuvinte de 32 biți.

Organizarea rețelelor (1)

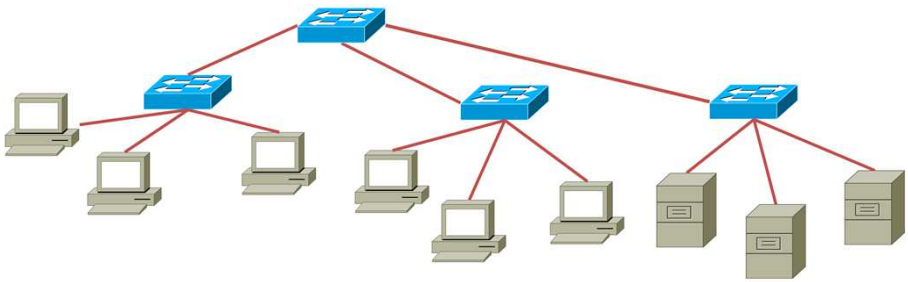
- Factori
  - locația geografică
  - scop
  - administrarea rețelei
- Motive
  - performanța numărului de calculatoare influențează gradul de utilizare al resurselor rețelei
  - posibilitatea de a face **broadcast** (trimiterea unui pachet către toate stațiile din rețea)
  - securitate
  - managementul adreselor

Una din funcțiile nivelului Rețea este de a suporta un mecanism de adresare a calculatoarelor. Istoric, prima rețea IP a fost o singură mare rețea. Cu cât rețeaua a crescut, cu atât și administrarea era din ce în ce mai dificilă. De aceea, a fost necesară împărțirea în subrețele. Când se realizează divizarea rețelei se pot lua în considerare unul dintre următorii factori:

- Locația geografică - gruparea calculatoarelor din aceeași locație (ex. campus, etaje diferite ale clădirilor, etc.)
- Scopul rețelei - gruparea calculatoarelor în funcție de rolul pe care îl au în rețea
- Administrarea rețelei - gruparea calculatoarelor pentru divizarea responsabilității personalului de management

Organizarea rețelelor (2)

- Fără organizare în subrețele
  - adresarea este plată
  - este greu de monitorizat și securizat



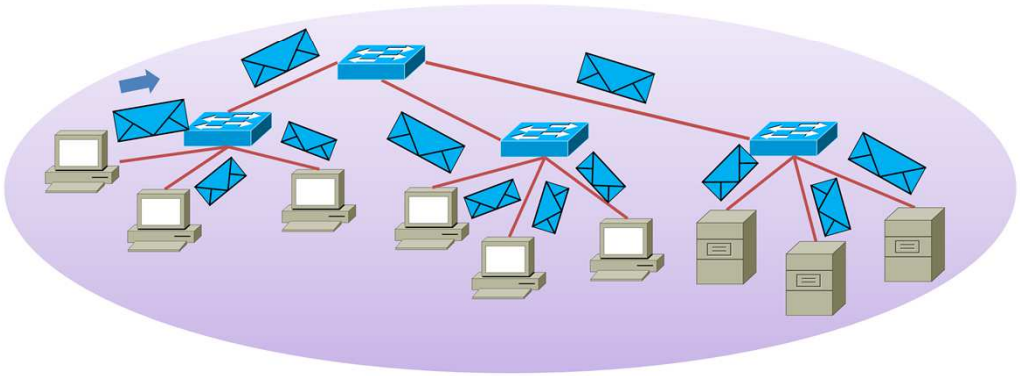
Adresarea plată se realizează luând la rând adresele (ex. adresele MAC) fără nici o structurare. Deși ușor de implementat, adresarea plată nu furnizează informații privind localizarea unui calculator într-o rețea de aceea este greu de realizat rutarea într-o astfel de rețea.

O singură rețea reprezintă un singur domeniu de broadcast prin urmare pachetele de tip broadcast vor ajunge în toată rețeaua existând astfel un surplus de trafic inutil în rețea.

Un alt mare dezavantaj pe lângă cel al procesării broadcast-urilor, este gradul de securitate foarte scăzut, deoarece un atacator se poate afilia foarte ușor rețelei.

Organizarea rețelelor (3)

- Fără organizare în subrețele
  - un singur domeniu de broadcast (un pachet de broadcast ajunge în toată rețeaua)



Din moment ce nu există un echipament care să poată să filtreze broadcast-urile, toate calculatoarele conectate la acea rețea fac parte din același domeniu de broadcast.

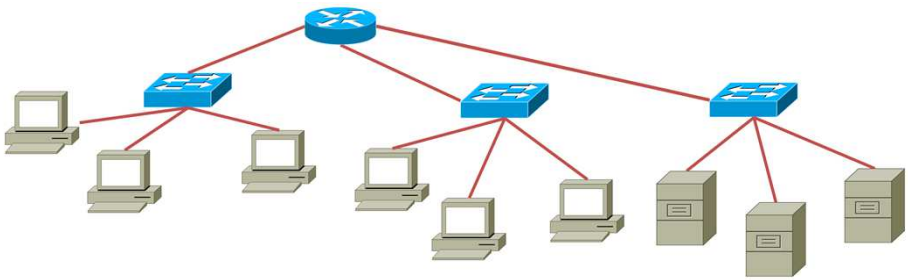
Acest lucru implică o creștere a semnificativă a traficului, chiar dacă acesta este inutil.

Echipamentele trebuie să fie din ce în mai puternice din punct de vedere al procesării, aplicațiile necesită o lățime de bandă mai mare .

O soluție pentru eliminarea acestor probleme ar fi segmentarea rețelei în domenii de broadcast sau chiar și în domenii de coliziune dacă în rețea sunt existente hub-uri.

Organizarea rețelelor (4)

- Cu organizare în subrețele
  - adresarea este ierarhică
  - fiecare subrețea poate fi monitorizată mult mai ușor



Odată ce rețeaua poate fi segmentată în domenii de broadcast diferite apar si avantaje:

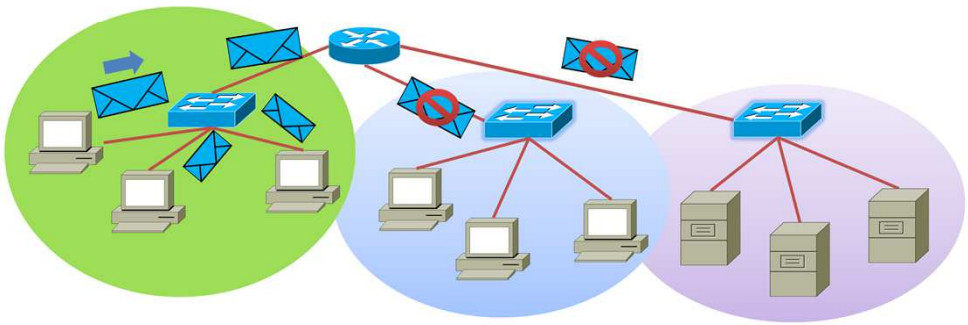
- Eficientizarea rutării pachetelor
- Sumarizarea rutelor către rețele destinație, astfel micșorând tabelele de rutare
- Simplificarea managementului și depanării proceselor

Din moment ce există un punct în rețea, prin care tot traficul spre exterior trece, se poate administra și monitoriza din punctul de vedere al securității mult mai bine și ușor tot ce se întâmplă în rețeaua locală.

Adresarea ierarhică presupune și folosirea de adrese de rețea diferite pentru fiecare domeniu de broadcast.

Organizarea rețelelor

- Cu organizare în subrețele
  - multiple domenii de broadcast (un pachet de broadcast ajunge doar în subrețeaua destinată)
  - se elimină traficul redundant



Cu cât crește numărul de domenii de broadcast, cu atât se poate vorbi despre o administrare mai ușoară și sigură din prisma securității.

Domeniile de broadcast fiind mult mai restrânse, traficul redundant se elimină, ceea ce înseamnă că viteza este mai ridicată.

Broadcast-urile sunt filtrate de echipamentele de nivel trei, astfel aceste pachete nu pot trece dintr-un domeniu în altul de broadcast.

Unele servicii folosesc adresa de broadcast - DHCP (Dynamic Host Configuration Protocol), dar problema este ce se întâmplă dacă serverul DHCP nu este în același domeniu de broadcast? De această problemă se ocupă echipamentul ce realizează segmentarea domeniilor de broadcast.

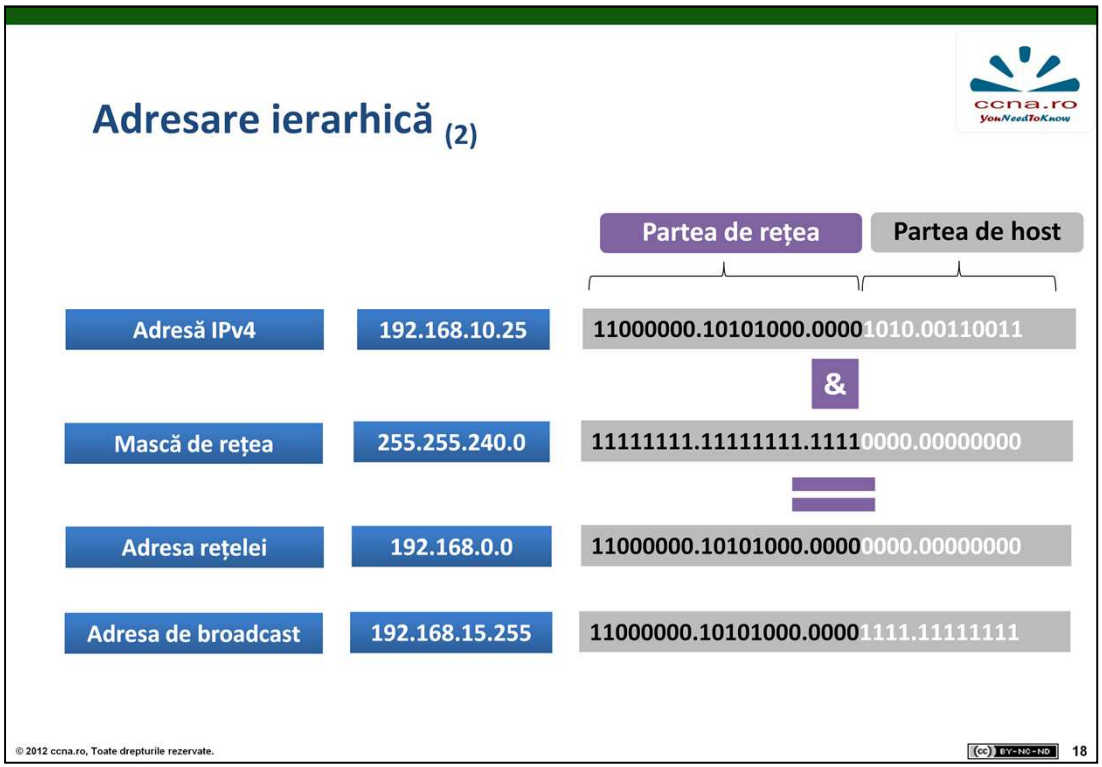
Adresare ierarhică (1)

- Fiecare calculator este identificat în mod unic
- IANA – organizația care se ocupă cu administrarea IP-urilor
- Adresa IPv4
  - reprezentată pe 4 octeți (32 de biți)
  - notația cea mai cunoscută este cea scrisă sub formă de 4 numere zecimale, separate prin punct (“dot-decimal notation”)
- Masca de rețea
  - delimitează partea de rețea de partea de stație

O adresă IPv4 este un șir de 32 de biți care identifică în mod unic stațiile. Având o adresare de tip ierarhic, o adresă IPv4 este formată dintr-o parte de rețea, care identifică domeniul în care se aflată stația, și o parte de alocare pentru utilizator, unică în cadrul rețelei respective.

Pentru a determina fiecare parte a adresei este necesară specificarea unui alt tip de adresă, respectiv masca de rețea, care delimitează partea de rețea de parte de stație.

Masca de rețea se poate nota și după lungimea prefixului (ex.: dacă prefixul conține 24 de biți masca se poate nota cu /24).



Masca de rețea este secvența de 32 de biți care are pe pozițiile corespunzătoare identificatorului de rețea valoarea „1” și valoarea „0” pe pozițiile corespunzătoare identificatorului stației.

Adresa rețelei este adresa IPv4 care are numai biți cu valoarea „0” în partea de stație.

Adresa de broadcast este adresa IPv4 care are valoarea „1” pe pozițiile corespunzătoare identificatorului stației iar identificatorul rețelei identic cu adresa de rețea.

Adresare ierarhică (3)

- Subrețele
  - o rețea poate fi împărțită în mai multe subreţele
  - se creează mărind lungimea prefixului (împrumutând biți de staţie)
  - numărul de calculatoare per subrețea va fi mai mic

Principiul de alocare a adreselor IP a devenit inflexibil pentru a permite modificări ale configurațiilor rețelelor locale. Astfel este necesară divizarea rețelelor în subrețele.

O subrețea se realizează prin împrumutarea de biți din partea de stație crescându-se astfel lungimea prefixului dar micșorându-se numărul de calculatoare per subrețea.

Adresarea ierarhică oferă avantaje spre deosebire de cea plată, deoarece se pot agrega subrețelele, ceea ce înseamnă că din subrețele se poate crea o rețea cu o mască mai mare decât măștile tuturor subrețelelor, acest proces poartă numele de supernetare.

Procesul invers este cunoscut sub numele de sumarizare.

Rute

- Rutele către destinații indică doar adresa next-hop, nu calea efectivă pe care pachetul o va lua
- Pe fiecare stație este adăugată automat în tabela de rutare o rută către destinațiile din afara rețelei cu next-hop adresa gateway-ului
- Pe fiecare ruter, rețelele direct conectate se introduc automat în tabela de rutare

În interiorul unei rețele, stațiile pot comunica fără existența unui echipament de nivel 3. Pentru comunicația cu alte rețele, este necesară folosirea unui echipament intermediar de nivel 3, respectiv un ruter, care este gateway-ul spre acele rețele. Adresa „Default Gateway" reprezintă adresa interfeței ruterului la care este conectată rețeaua locală și trebuie să fie cunoscută de către stații pentru a permite comunicarea în afara rețelei. După definirea gateway-ului, în tabela de rutare a stației apare o rută către rețele externe unde adresa next-hop este adresa gateway-ului. Pe ruter rutele pot fi:

- Către rețele direct conectate
- Introduse manual
- Învățate prin intermediul unui protocol dinamic de rutare

Dacă ruta către rețeaua destinație nu există, pachetul nu poate fi trimis mai departe și este astfel aruncat.

Tabela de rutare (1)

- Parametrii unei rute sunt:
  - Reţeaua destinaţie
  - Adresa next-hop
  - Metrica
- Un calculator poate adăuga automat în tabela sa de rutare toate rețelele direct conectate şi o rută default către gateway
- Comenzi uzuale pentru monitorizarea şi administrarea tabelei de rutare a unui calculator:
  - **`netstat -r`**
  - **`route, route PRINT`**
  - **`route ADD/DELETE/CHANGE`**

Tabela de rutare este cea pe baza căreia se iau decizii pentru directarea pachetelor spere rețeaua destinație.

Reţeaua destinaţie:

- Apare în tabela de rutare sub formă de adresă de reţea
- Se compară adresa destinaţie cu adresele stocate în tabela de rutare și dacă nu se găsește nici o potrivire, pachetul este aruncat

Adresa next-hop:

- Reprezintă adresa ruterului la care va fi trimis un pachet pentru a ajunge într-o anumită rețea
- Nu este specificată pentru rețelele direct conectate

Metrica:

- Indicator de preferință a unei rute după anumite criterii
- O metrică mai mică este mai bună

Tabela de rutare (2)

- O intrare din tabela de rutare se refera la o rețea generală sau doar la o subrețea din rețeaua generală
- Comanda pentru afișarea tabelei de rutare a unui router este:
  - **show ip route**
- Comenzi pentru aflarea configurației pe un calculator:
  - **ipconfig**
  - **ipconfig /all**
  - **route PRINT**
  - **ifconfig**

Pentru verificarea tabelei de rutare există diferite comenzi, în funcție de sistemul de operare și de echipamentele dedicate folosite.

Ca particularități ale tabelei de topologie se regăsesc în fiecare mediu, după cum urmează:

- Adresă destinație, adresa de rețea nex-hop, metrica, interfața de ieșire.

Parcurgerea tabelei de rutare se realizează de la cea mai specifică adresă de rețea până la cea mai nesemnificativă adresă.

Cea mai puţin specifică adresă de rețea este 0.0.0.0/0, ceea ce înseamnă că se face potrivire pe orice destinație.

În cazul în care, în tabela de rutare nu exista o rută pe care să se potrivească pachetele vor fi aruncate.

Tabela de rutare (3)

- Exemplu de tabelă de rutare

```
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demand routing, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O 172.150.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
D 172.17.10.0 [90/128] via 10.119.254.244, 0:02:22, Ethernet2
```


Pentru o mai bună clasificare și depanare a rețelei, tabela de rutare reține rutele învățate din diferite protocoale de rutare, și totodată, modul prin care aceste rute au fost adăugate.

În funcție de rețelele pe care le are tabela de rutare, ruterul va lua decizii.

Fiecare echipament din rețea va lua independent decizii, bazându-se pe propria tabelă de rutare.

În funcție de modul prin care ruterul a învățat acele rute (dinamic), acestea pot trece prin diferite tabele până ca ele să fie instalate în tabela de rutare.

În cazul în care în tabla de rutare nu sunt adăugate sau învățate rute, aceasta va conține doar rețelele direct conectate.

Rutarea pachetelor

- Fiecare pachet este tratat individual
- În urma procesării unui pachet se poate decide
  - trimiterea către ruterul next-hop
  - trimiterea către calculatorul destinație
  - aruncarea pachetului
- În procesul de trimitere a unui pachet, ruterul va alege calea cea mai specifică – cu cel mai lung prefix
- Pachetul este procesat de ruter la nivelul 3
  - se elimină încapsularea de nivel 2
  - se ia o decizie pe baza tabelei de rutare
  - dacă pachetul se trimite mai departe se reface încapsularea de nivel 2

Rutarea necesită ca toate ruterele de pe calea de comunicație de la sursă la destinație, să aibă o rută pentru a transmite mai departe fiecare pachet care apare în rețea.

Ruterele din rețea nu trebuie să cunoască câte o rută către toate rețele ci doar adresa next-hop sau interfața spre care va trimite pachetul către destinație.

Dacă ruterele sunt direct conectate, nu este nevoie să se cunoască adresa de rețea next-hop ci doar interfața de ieșire. Un astfel de mediu poartă numele de Point-to-Point. În cazul unui mediu cu acces multiplu este necesară cunoașterea adresei next-hop către destinație.

Ruta implicită

- Este imposibilă introducerea în tabela de rutare a tuturor rutelor existente în Internet
- Soluția: Ruta default („Default Gateway” sau „Gateway of Last Resort”)
  - către toate rețelele posibile
  - are adresă și masca de rețea 0.0.0.0
  - utilizată pentru pachete a căror destinație nu sunt în tabela de rutare
  - îi este asociată o adresă next-hop
- Se reduce simțitor mărimea tabelei de rutare

Ruta implicită, denumită și *gateway of last resort*, este o rută folosită de către un ruter atunci când nicio altă rută către o anumită rețea nu există în tabela de rutare. Pentru IPv4, ruta implicită este 0.0.0.0/0. Masca de rețea fiind /0 va fi de fapt cea mai scurtă masca de rețea, deci ultima rută posibil aleasă în procesul de rutare. În mod similar, pentru IPv6 rută implicită este ::/0. Această rută implicită mai poartă și numele de „quad-zero”.

Acest tip de rută este folosită în special pe ruterele din cadrul unei organizații, având next-hop ruterul conectat la rețeaua ISP-ului. Astfel pachetele cu destinația în afară LAN-ului vor fi trimise către acest ruter.

Această rută poate fi de asemenea și ea învățată dinamic prin intermediul protocoalelor dinamice sau poate fi asignată static de către administrator.

Rutarea statică

- Denumește configurarea manuală a rutelor
- Trebuie efectuată configurația pe toate ruterele
- Avantaje
  - nu utilizează resursele rețelei (lățime de bandă) şi nici ale ruterului (procesor, memorie)
  - oferă un control riguros asupra următorului hop ales la un moment dat
- Dezavantaje
  - nu este deloc scalabilă

Rute către rețele îndepărtate pot fi configurate manual pe ruter specificând o adresă next-hop spre care trebuie transmise datele. Dacă între stațiile ce comunică se află mai multe rutere este necesară configurarea rutelor statice pe fiecare echipament care participă la transferul informațiilor între acele entități. Dacă apar schimbări în topologie rutele trebuie reconfigurate manual pe fiecare ruter.

După cum se știe, fiecare rută are propria distanță administrativă. Aceasta înseamnă că se poate modifica această valoare, prescurtată AD, care prioritizează ruta în tabela de rutare.

Cum fiecare obiect are avantaje și dezavantaje, așa și rutarea statică are avantajul că este stabilă, consumă puține resurse de procesare, nu folosește lățimea de bandă deoarece nu este învățată dinamic dar marele dezavantaj este scalabilitatea, pentru fiecare nouă rută trebuie adăugată propria rută statică.

Rutarea dinamică

- Ruterele schimbă între ele informații despre rețelele cunoscute
- Dacă au loc modificări în rețea, pe măsură ce ruterele află de acestea, vor distribui informația către ceilalți vecini
  - tabelele sunt mereu actualizate şi conțin informații coerente și precise
- Necesită cunoștinte avansate pentru o configurare eficientă
- Utilizează atât un procent din lățimea de bandă cât și din procesor
- Este o soluție scalabilă și tolerantă la defecte
- Exemple de protocoale de rutare: RIP, EIGRP, OSPF, IS-IS, BGP

Protocoalele de rutare dinamice reprezintă un set de reguli prin care ruterele schimbă informații de rutare. Astfel la fiecare modificare a topologiei sunt transmise informații între ruterele care rulează respectivele protocoale și tabelele de rutare sunt actualizate conform modificărilor apărute.

Cele mai răspândite protocoale de rutare sunt:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)

Spre deosebire de rutarea statică, rutarea dinamică mărește traficul în rețea. De asemenea, în cazul unor protocoale, este necesară suficientă capacitate de procesare și lățime de bandă.

Capitolul 5: Adresarea IP

Obiective

- Anatomia adresei IP
- Tipuri de adrese IP
- Modele de comunicație
- Modele de adresare
- Configurarea reţelei

Anatomia adresei IP (1)

01111011001011010000101000100101

- O adresă IPv4 este reprezentată în memorie ca un număr pe 32 de biţi
- Orice transformare asupra adresei se reduce la o operaţie binară

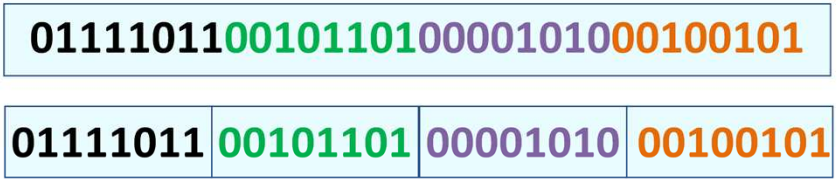
Biții sunt combinați în grupări de câte 8, apoi fiecare grupare este convertită pe rând într-un număr zecimal (în exemplu, 123.45.10.37).

Șirul 01111011001011010000101000100101 are 32 de biți.

Pentru conversia din binar în zecimal este nevoie de a cunoaște puterile lui 2.

- $2^0 = 1$
- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 8$
- $2^4 = 16$
- $2^5 = 32$
- $2^6 = 64$
- $2^7 = 128$

Anatomia adresei IP (2)



- Trecerea în zecimal facilitează lucrul cu adrese IP
- Primul pas reprezintă împarţirea valorii pe octeţi

Adresa IP se separă în 4 grupări de câte 8 biți – 01111011.00101101.00001010.00100101. Se aplică transformarea din baza 2 în baza 10 asupra fiecărui octet pentru a ajunge la formatul „dotted-decimal” - 123.45.10.37.

Fiecare octet este notat în format big endian: bitul cel mai semnificativ este cel mai din stânga.

Din perspectiva echipamentului și a sistemului de operare nu interesează numărul zecimal, această transformare este realizată pentru o înțelegere ușoară și intuitivă a adresei IP, din prisma omului.

O altă caracteristică pentru care se face transformarea este depanarea.

Anatomia adresei IP (3)

01111011001011010000101000100101			
01111011	00101101	00001010	00100101
123	45	10	37

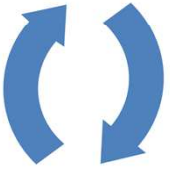
- Al doilea pas constă în trecerea octeţilor din binar în zecimal

Ultimul pas din această operație constă în calcularea fiecărui octet în zecimal.

De exemplu 00001010 înseamnă:

$$0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 0 \cdot 2^7 = 10$$

Anatomia adresei IP (4)



01111011001011010000101000100101

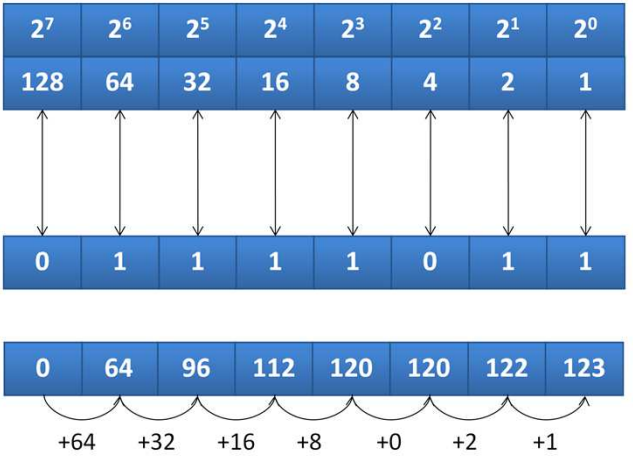
- Un inginer în reţele trebuie să stăpânească perfect această transformare

123.45.10.37

Orice persoană din domeniul IT, cu atât mai mult în rețelistică, trebuie să aibă capacitatea de a face aceste operații foarte rapid şi să aibă un spirit de observație foarte bun, deoarece o singură greșeală poate duce la probleme foarte mari.

Modificarea unui singur bit, reprezintă propagarea și utilizarea unei alte adrese de rețea, adresa ce nu face parte din spațiul de adrese cumpărat de la Internet Assigned Numbers Authority (IANA).

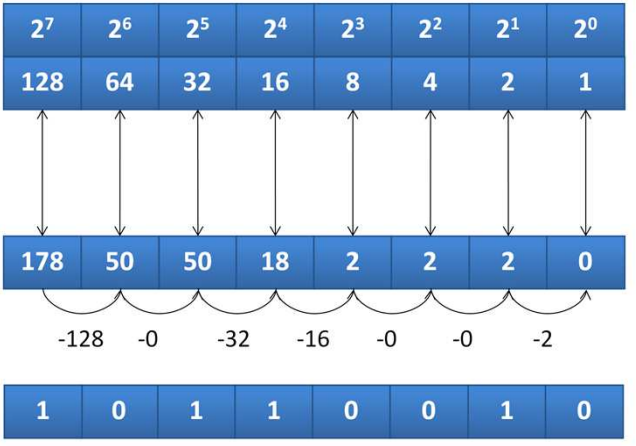
Binary Magic (2)



Transformarea din binar în zecimal se face adunând valorile asociate pozițiilor biților care au valoarea 1 dintr-un octet.

În exemplul de stânga sus, primul bit de 1 este pe poziția 2^6. Se va reține valoarea 64, următorul bit de 1 este pe poziția 2^5, deci se va aduna 32 la 64 de unde 96 și așa mai departe.

Binary Magic (3)



Transformarea din zecimal în binar se face comparând numărul cu cea mai mare putere a lui 2 cu valoare mai mică sau egală și scăzând-o pe aceasta din număr. În același timp pe poziția din octet corespunzătoare acelei puteri se va pune un bit de 1. Dacă nu s-a făcut nicio scădere cu o anumită putere, se va pune 0.

În exemplul de mai sus, avem numărul 178. Cea mai mare putere a lui 2 mai mică sau egală este reprezentată de 2^7. În continuare se scade 178 – 128 = 50 se pune 1 pe poziția 2^7 și se caută cea mai mare putere a lui 2 mai mică sau egală decât 50 etc.

Masca de reţea

123.45.10.37	01111010001001010010110100001011
255.255.0.0	11111111111111110000000000000000

- Orice adresă IPv4 are asociată o mască de reţea
- Aceasta constă într-un șir continuu de „1” completat cu un șir continuu de „0” până la 32 de biţi
- O mască de reţea /16 conţine un set continuu de 16 biţi cu valoarea „1”

Măștile de rețea sunt folosite pentru clasele A, B și C. Adresele de multicast nu folosesc măști de rețea.

O mască de rețea este un număr de 32 biți în care biții de 1 reprezintă partea de rețea și biții de 0 identifică partea de stație adresei.

O mască de rețea trebuie să aibă un șir continuu de 1 în partea stângă a măștii; biții setați pe 0 trebuie să fie în partea dreaptă a măștii.

Masca de rețea este de forma X.X.X.X. Pentru a simplifica scrierea se poate folosi și formatul prefix/Y, unde Y este numărul de biți de 1 din masca de rețea.

Adresa de reţea (1)

123.45.10.37	01111010001001010010110100001011
	ŞI
255.255.0.0	11111111111111110000000000000000

- Dacă efectuăm o operaţie de ŞI logic între IP şi masca de reţea se va obţine adresa de reţea

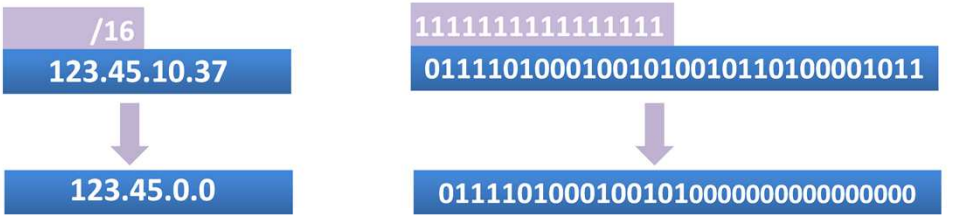
Modul în care se poate afla adresa de rețea din care face parte un IP, este o operație logica.

Această operație este un ŞI logic între adresa IP scrisă în forma binară și masca de rețea scrisă tot in formă binară.

Operația de ŞI logic este definită astfel:

- 1 & 1 = 1
- 1 & 0 = 0
- 0 & 1 = 0
- 0 & 0 = 0

Adresa de rețea (2)



- Partea de stație dintr-un IP reprezintă ultimii „X” biți, unde:

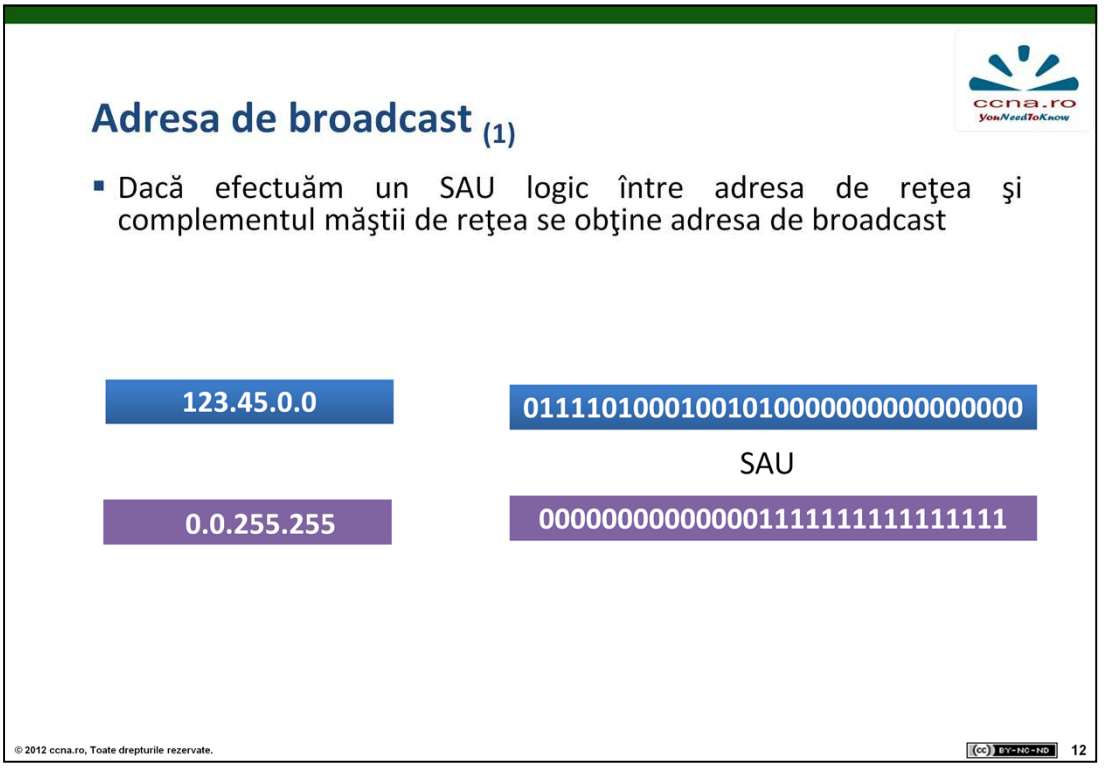
X=32-mărimea măștii de rețea

Adresa de rețea va identifica în mod unic o rețea locală. Toate stațiile din acea rețea vor avea acești biți comuni.

După biții de rețea pe care i-am determinat prin intermediul dimensiunii măștii de rețea, urmează biții de stație, ce identifică unic un stație în cadrul rețelei.

În exemplul de mai sus, dacă prefixul adresei este /16 rezultă că sunt 16 biți de rețea și atunci vor rămâne 32 – 16 = 16 biți de stație.

În total în această rețea vor putea exista maxim $2^{16} – 2$ stații (adresa de rețea și adresa de broadcast nu sunt asignabile).



O altă operație la fel de importantă este SAU logic.

Această operație ajută administratorul să afle adresa de broadcast a adresei de rețea, aflate cu ajutorul opeației de ȘI logic.

Operația de SAU logic este definită astfel:

- 1 | 1 = 1
- 1 | 0 = 1
- 0 | 1 = 1
- 0 | 0 = 0

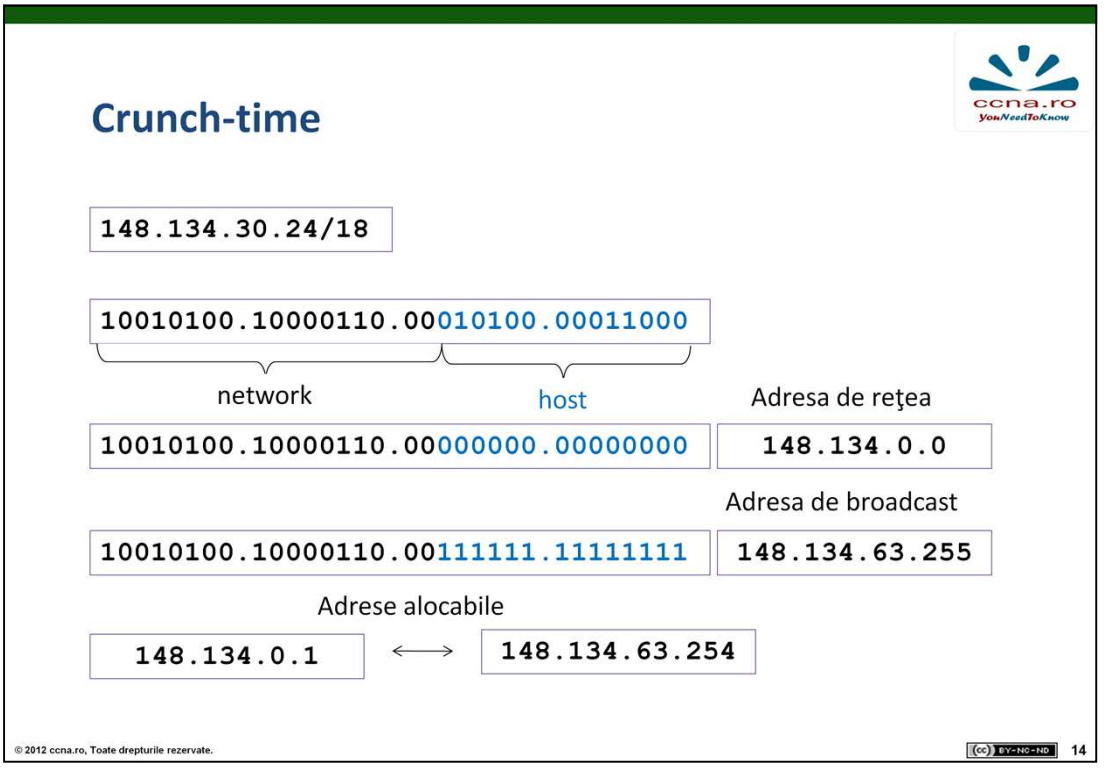
Adresa de broadcast (2)

- Adresa de reţea şi adresa de broadcast nu pot fi alocate unui echipament

O rețea are o singură adresă de broadcast – ultima adresă din spațiul de adrese al rețelei. Aceasta adresă nu poate fi asignată niciunei stații. Un pachet trimis către această adresă din rețeaua locală va fi primit de către toate stațiile din acea rețea.

Adresa de broadcast are în partea de stație toți biții cu valoarea 1, păstrând intacți biții din partea de rețea.

În figura de mai sus, masca de rețea este 255.255.0.0. Dacă se complementează masca de rețea se va obține 0.0.255.255. Cu această valoare și adresa IP se face operația SAU logic pentru a afla adresa de broadcast specifică rețelei.

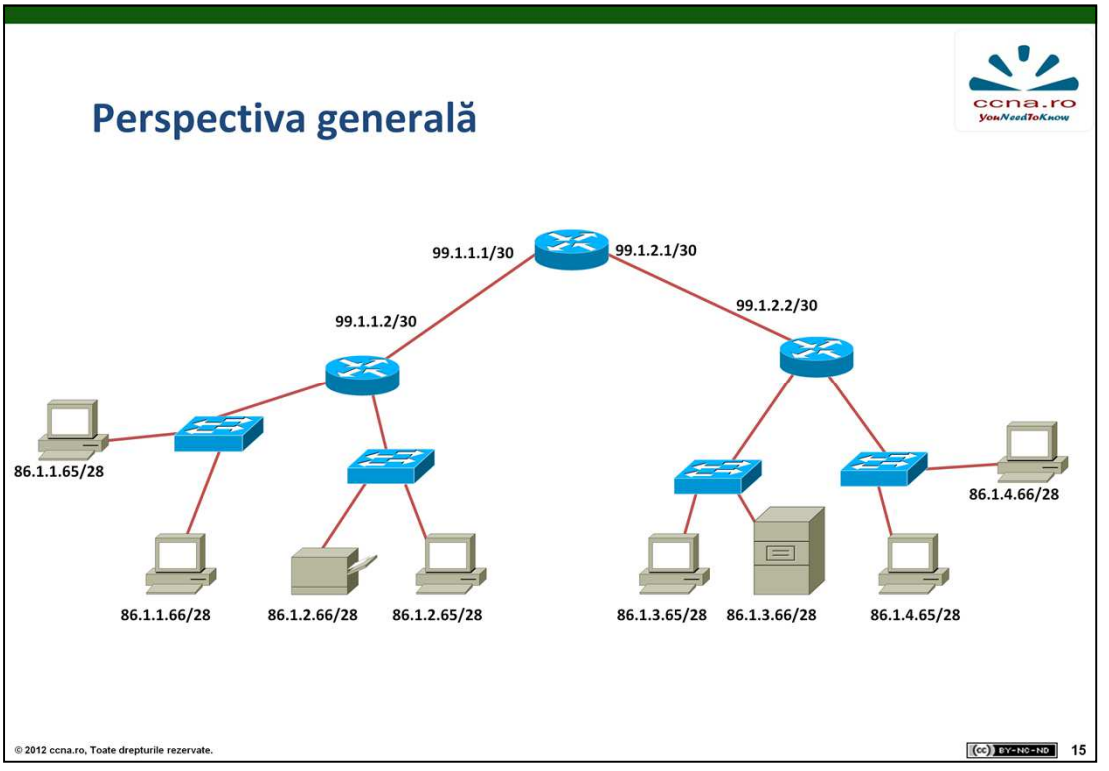


Având o adresă IP și o mască de rețea se poate afla partea de rețea și partea de stație a adresei. Înlocuind partea de stație a adresei cu biți de 0 se va obține adresa de rețea pentru respectiva adresă.

Înlocuind partea de stație a adresei cu biți de 1 se va obține adresa de broadcast pentru respectiva adresă.

Valorile între cele două adrese aflate în acest fel vor reprezenta adresele alocabile din rețea.

În exemplul de mai sus prefixul adresei este /18, ceea ce înseamnă că primii 18 biți vor reprezenta partea de rețea și deci vor rămâne neschimbați. Următorii 32 – 18 = 14 biți vor fi înlocuiți după cum urmează: 0 pentru adresa de rețea, 1 pentru adresa de broadcast. Se aplică transformarea din binar în zecimal pentru simplitate în scriere.

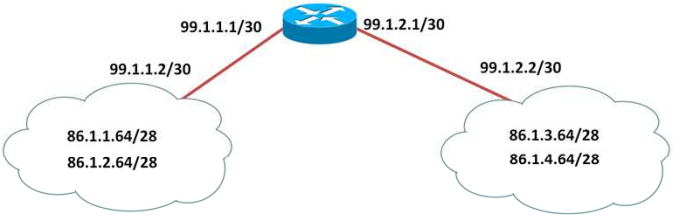


În lumea reală, organizarea rețelelor este ierarhică. Fiecare echipament de rețea va comunica de fiecare dată când este necesară comunicația cu echipamente din alte rețele, cu Internetul.

Din punct de vedere al organizării unei rețele, aceasta trebuie să aibă un model ierarhic.

Astfel fiecare echipament, în cazul în care nu cunoaște o adresă destinație să aibă un alt echipament direct conectat cu el astfel încat să îi trimită lui cererile pe care nu le cunoaște, urmând acest procedeu, până se ajunge în nucleul Internetului.

Perspectiva ruterului

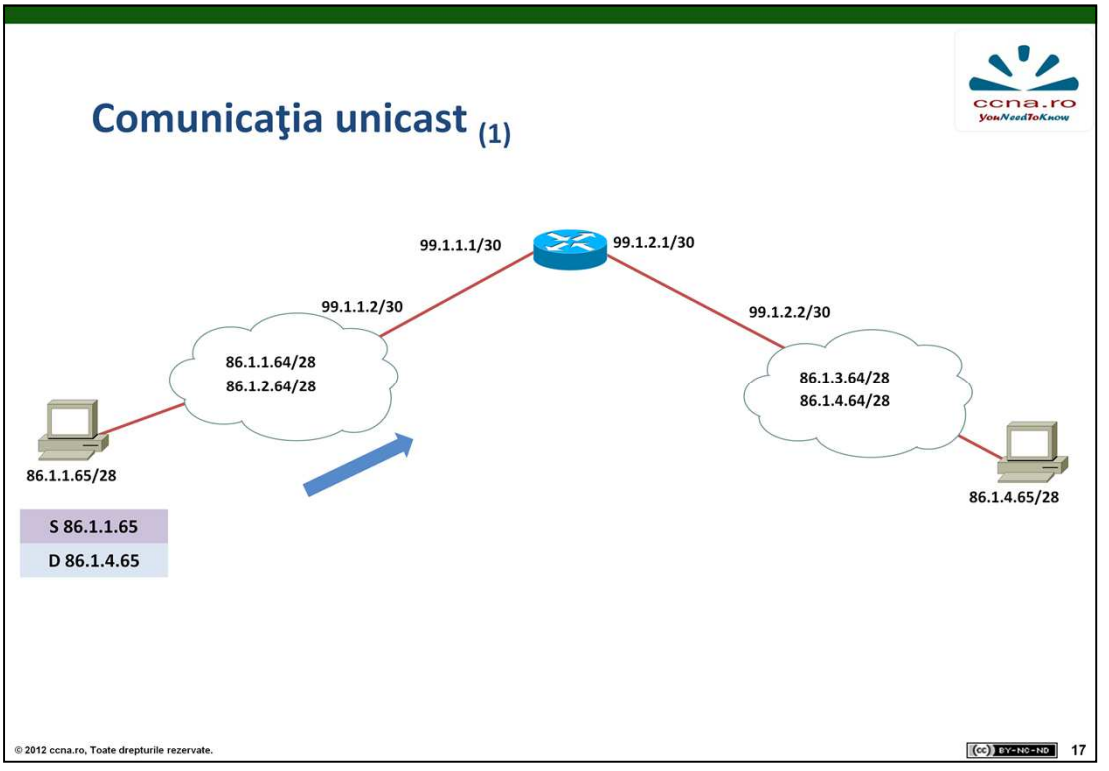


- Ruterele nu memorează decât adresele de reţea
- Fiecare ruter are o tabelă de rutare
- Tabela de rutare reţine asocieri de forma:
  - adresă de reţea ↔ next-hop

Din perspectiva echipamentelor de rețea, există o altă vedere asupra modului de comunicare între echipamente: fiecare ruter are o tabelă de rutare care conține adresele de rețea și IP-ul nodului următor spre acea rețea.

Tabela de rutare este populată cu adresele de rețea direct conectate, adrese ce sunt specificate static, cât și cu adrese de rețea învațate dinamic din protocoale de rutare.

Fiecare ruter ia alegeri privind calea pe unde să fie trimis un pachet, bazându-se doar pe tabela de rutare .



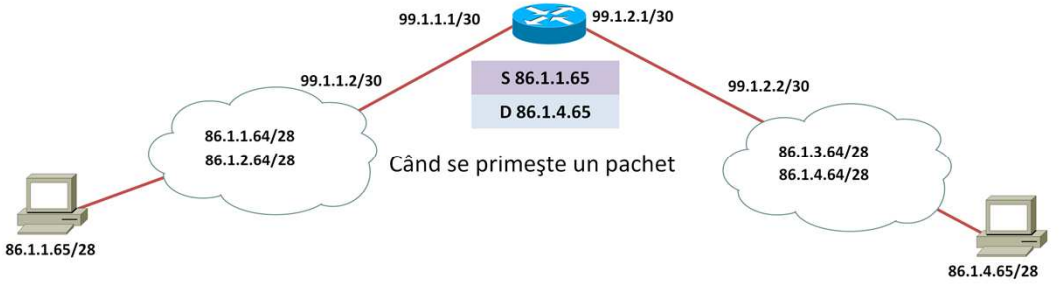
Una dintre cele mai folosite comunicații este comunicația unicast. Aceasta are rolul de a specifica faptul că un pachet este trimis de o singură sursă către o singură destinație.

Comunicația unicast poate fi întâlnită fie la comunicarea între două stații, fie este folosită de către protocoalele de rutare pentru a crea legături cu vecini.

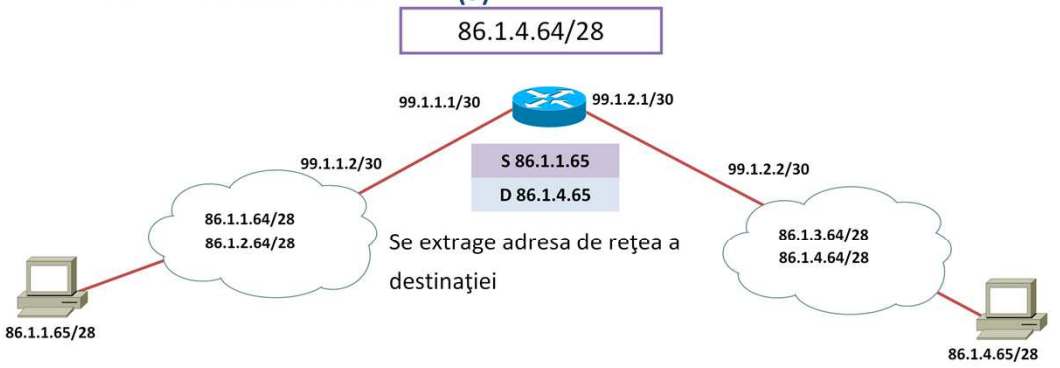
Comunicația unicast este o relație de 1:1.

La fiecare hop se verifică tabela de rutare pentru a ști pe unde trebuie să fie trimis acel pachet. În cazul în care nu exista o intrare în tabela de rutare spre destinație pachetul va fi aruncat.

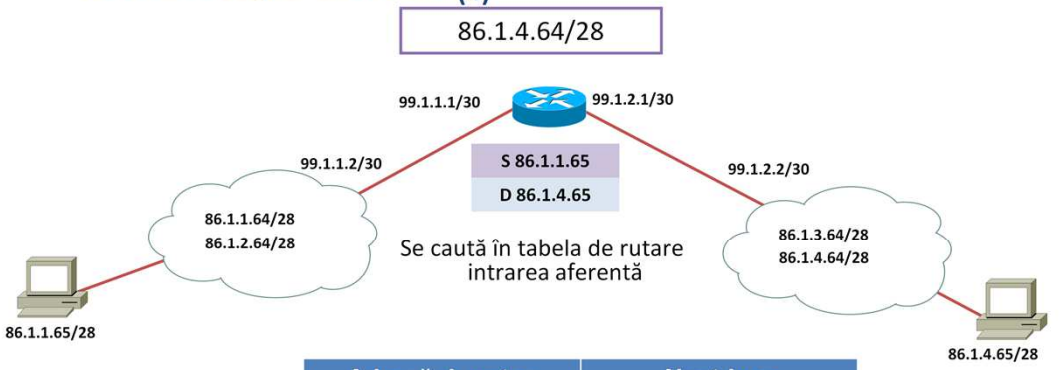
Comunicaţia unicast (2)



Comunicaţia unicast (3)

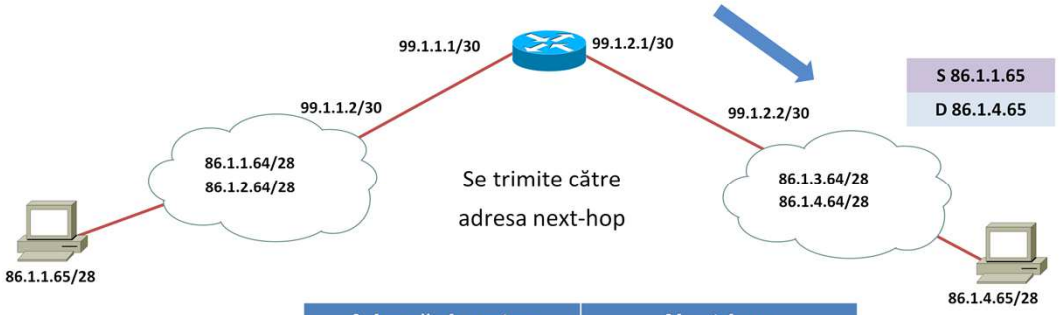


Comunicaţia unicast (4)



Adresă de reţea	Next-hop
86.1.1.64/28	99.1.1.2
86.1.2.64/28	99.1.1.2
86.1.3.64/28	99.1.2.2
86.1.4.64/28	99.1.2.2

Comunicaţia unicast (5)



Adresă de reţea	Next-hop
86.1.1.64/28	99.1.1.2
86.1.2.64/28	99.1.1.2
86.1.3.64/28	99.1.2.2
86.1.4.64/28	**99.1.2.2**

Comunicaţia broadcast (1)

- Toate staţiile care au aceeaşi adresă de reţea sunt în acelaşi Domeniu de Broadcast
- Interfaţa unui ruter poate fi asociată cu o singură adresă de reţea
- Un ruter nu rutează pachete broadcast implicit
- Ruterul este singurul echipament de reţea care segmentează domenii de broadcast

Comunicația broadcast este specifică în rețeaua proprie, deoarece pachetele cu adresa destinație de broadcast sunt filtrate de către ruter.

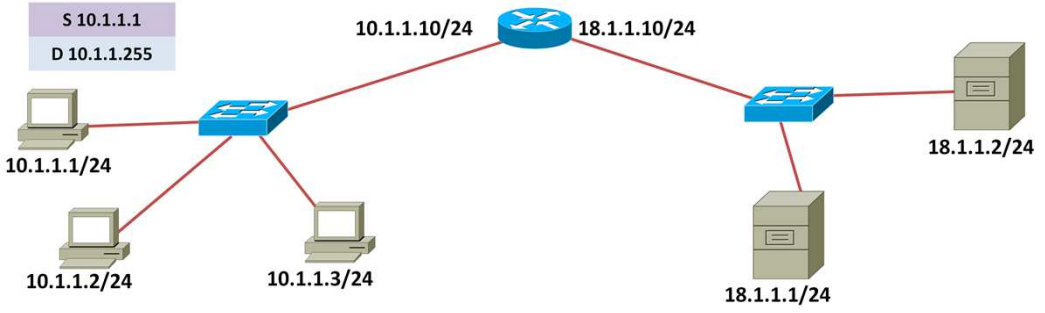
Acestă comunicație este folosită în general pentru a cere anumite informații unor stații a căror adresă IP nu este cunoscută, sau în cazul în care se dorește trimiterea unui pachet la toate staţiile din rețea.

Adresa de broadcast este ultima adresă din domeniul adresei de reţea.

Această adresă nu poate fi asignată unei stații.

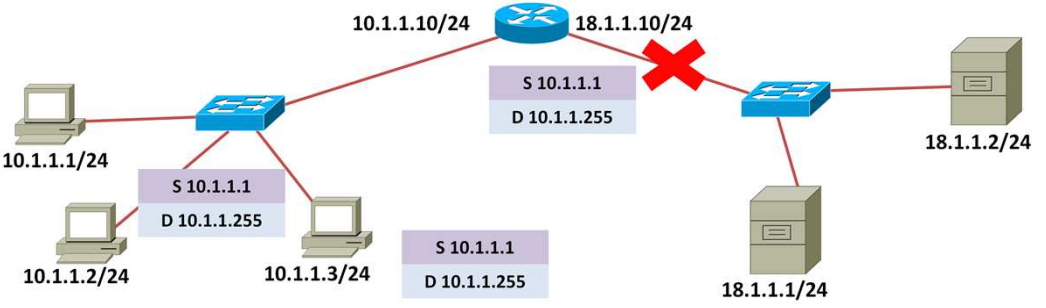
Comunicaţia broadcast (2)

- Un pachet de broadcast are ca adresă destinaţie adresa de broadcast



Comunicaţia broadcast (3)

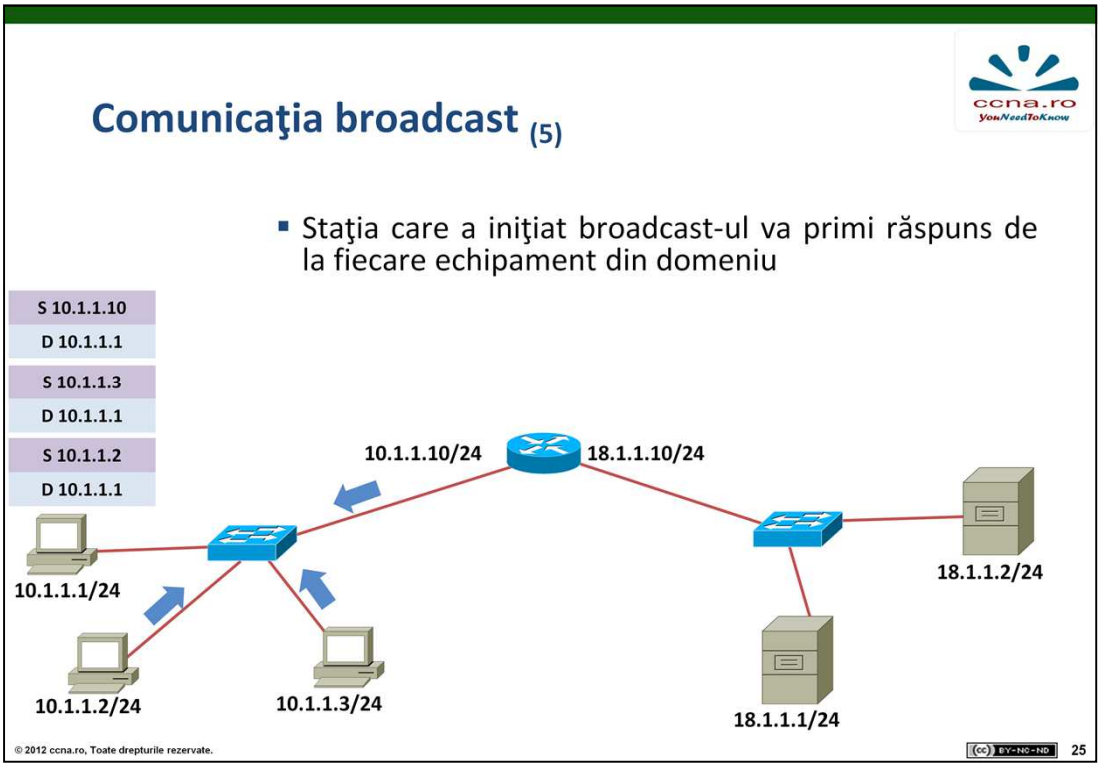
- Ruterul nu va trimite pachetul pe celelalte interfeţe segmentând broadcast-ul



În imaginea de mai sus, este un exemplu în care staţia cu adresa IP 10.1.1.1 doreşte sa timită un pachet în toată reţeaua locală; modul prin care acestă staţie trimite acest pachet este de a folosi adresa de broadcast, fără a fi nevoită să trimită pachetul la fiecare staţie folosind comunicaţia de tip unicast.

Ruterul este echipamentul ce nu permite trecerea pachetului de broadcast spre alte reţele.

Acestă comunicaţie este de tipul 1:N.



Staţia care a iniţiat broadcast-ul, va primi răspuns de la fiecare echipament.

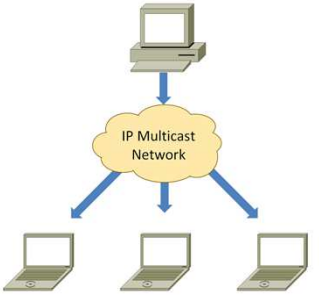
Privind din alta perspectivă, aceasta comunicaţie face ca reţeaua să fie încărcată cu pachete, ceea ce duce la o scădere a performanţei întregii reţele.

Exploatând acest tip de comunicaţie se pot crea atacuri de reţea.

La prima vedere pare că nu ar fi necesară comunicaţia de tip broadcast, dar sunt unele servicii care nu pot rula fără acest tip de serviciu. Un exemplu este DHCP (*Dynamic Host Configuration Protocol*).

Comunicaţia multicast (1)

- Este un model de comunicaţie de tipul many-to-many
- Foloseşte un model de adresare plată
- Adresa IP destinaţie este folosită ca o etichetă pentru a marca un flux de trafic
- Toate staţiile care ascultă pe un anumit flux de trafic aparţin unui grup de multicast

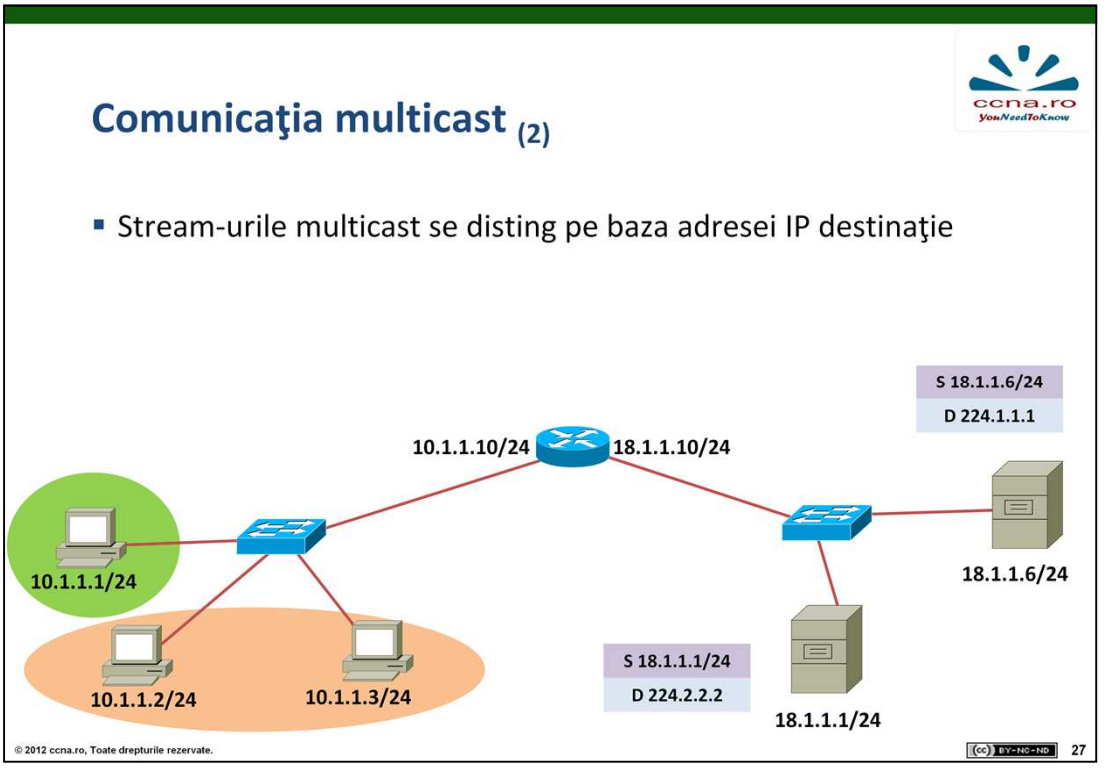


Comunicația de tip multicast este folosită în general de un grup restrâns de oameni.

Adresele de multicast aparțin unei clase speciale și anume clasa D.

Unele adrese de multicast sunt rezervate pentru un anumit tip de trafic, de exemplu unele protocoalele de rutare folosesc: 224.0.0.5 sau 224.0.0.10, etc.

O altă utilizare a acestui tip de comunicație este pentru video streaming, deoarece scade lățimea de bandă folosită de întreaga rețea.



Spre deosebire de comunicația de tip broadcast, pachetele ce au ca destinație o adresa de multicast nu vor fi filtrate de către rutere. Acesta este și motivul pentru care unele protocoale de rutare folosesc acest tip de comunicație.

Un alt avantaj este că o stație poate aparține mai multor grupuri de multicast, ceea ce aduce un mare avantaj privind traficul din reţea.

Pe aceste adrese de multicast pot fi transmise filme de la o sursă către un grup stabilit, este foarte folositor într-o rețea locală, sau se poate face video conferință.

Adresarea classful

- Iniţial adresele au fost grupate în 5 clase
- Apartenenţa unui IP la o anumită clasă este stabilită de valoarea primului octet
- La început masca de reţea era stabilită tot pe baza primului octet
  - Clasa A - /8
  - Clasa B - /16
  - Clasa C - /24

Adresarea classful se bazează pe împărțirea adreselor IP în 5 clase, de la A la E.

Clasele A, B și C sunt folosite pentru alocare de adrese IP stațiilor, clasa D este folosită pentru adrese de multicast (transmiterea unică a unui pachet către mai multe destinații) și clasa E pentru uz experimental.

Clasa A de adrese este de format N.H.H.H, unde N este partea de reţea a adresei și H este partea de stație. Clasa B de adrese va fi de format N.N.H.H, iar clasa C de format N.N.N.H.

De măștile acestor clase nu se mai ține cont pentru asignare directă de adrese IP datorită risipei prea mare de adrese ce pot fi folosite per rețea (exemplu în cadrul clasei A unde un singur octet era folosit pentru rețea, restul pentru stații).

Clase IP

Clasa	primul octet zecimal	primul octet binar	masca de rețea	nr de rețele	nr de stații/ rețea
A	1-127	00000000-01111111	/8	2^7 128	2^{24}-2 16,677,214
B	128-191	10000000-10111111	/16	2^{14} 16,384	2^{16}-2 65,534
C	192-223	11000000-11011111	/24	2^{21} 2,097,150	2^8-2 254
D	224-239	11100000-11101111	N/A	N/A	N/A
E	240-255	11110000-11111111	N/A	N/A	N/A

Clasa A de adrese cuprinde adrese de rețea asignabile de la 1.0.0.0 la 126.0.0.0 (rețelele 0.0.0.0 și 127.0.0.0 sunt rezervate).

Clasa B de adrese cuprinde adrese de rețea de la 128.0.0.0 la 191.255.0.0 având un prefix de rețea /16.

Clasa C de adrese cuprinde adrese de rețea de la 192.0.0.0 la 223.255.255.0 având un prefix de rețea /24.

Clasa D de adrese cuprinde intervalul 224.0.0.1 - 239.255.255.255. Acestea nu au parte de rețea sau de stație. Unele adrese de multicast din acest interval sunt deja asignate (exemplu 224.0.0.10 este folosit de ruterele cu EIGRP).

Clasa E de adrese cuprinde intervalul 240.0.0.0 – 254.255.255.255 și este rezervată pentru utilizare experimentală.

Rețeaua 255 este folosită pentru broadcast.

Not so great expectations...

1970

- 32 biti ~ 4 miliarde de adrese
- ARPANET
- „Rețeaua mondială nu va depăși niciodată 1000 de stații”

2012

- 2 miliarde de utilizatori
- Adresele alocabile de către IANA au fost epuizate, au mai rămas cele alocabile la nivel regional
- 2014 consumarea completă

Advanced Research Projects Agency Network (ARPANET) este prima rețea de tip comutare de pachete de la care a plecat Internetul de azi care avea doar câteva calculatoare conectate prin modemuri ce ajungeau la maxim 50 kbps.

Spațiul întreg de adrese IP este administrat de IANA (Internet Assigned Numbers Authority) și de cinci RIR (Region Internet Registries) responsabile în teritoriile desemnate pentru asignarea lor utilizatorilor sau ISP (Internet Service Providers). Odată cu terminarea adreselor în ianuarie 2011 la IANA și în aprilie 2011 la APNIC RIR, s-a pus mai multă presiune pe adoptarea de noi tehnologii, incluzând Classless Inter-Domain Routing (CIDR) din 1993, Network Address Translation (NAT) și noua versiune Internet Protocol, IPv6 din 1998.

Soluţii: Adresarea classless

- În modelul **classful** nu se propagă informaţii despre masca de reţea în pachetul IP
- Datorită condiţiei de unicitate al adreselor IP modelul classful este limitat şi inflexibil
- În modelul **classless** :
  - masca de reţea poate avea orice lungime
  - valoarea măştii se propagă în pachetul IP

IP Address Subnet Design. Dezvoltarea unui plan de asignare a adreselor IP sau de design al unei subrețele este un concept important pentru un proiectant de rețele.

Trebuie să se țină cont de mai mulți factori în momentul în care se folosește modelul de adresare classless (care nu se mai bazează pe clasele prezentate anterior):

- Numărul de locații
- Numărul de echipamente din fiecare locație
- Cerințele de adresare IP pentru fiecare locație individuală
- Numărul de echipamente din fiecare rack de echipamente
- Cerințe de VoIP, wireless LAN, video
- Mărimea subrețelei

Soluţii: Adrese private

- Adrese rezervate care nu trebuie să respecte condiţia de unicitate
- Nu sunt rutate în domeniul public

Masca	Range
/8	10.0.0.0 - 10.255.255.255
/12	172.16.0.0 - 172.31.255
/16	192.168.0.0 - 192.168.255.255

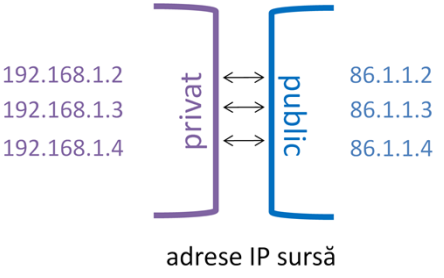
Unele rețele din spațiul de adrese IPv4 sunt rezervate pentru folosire privată. Aceste adrese nu sunt rutate în Internet. Multe organizații folosesc astăzi în rețeaua internă adrese private. Protocolul cu care acestea ajung translatate în Internet se numește NAT.

Spațiul de adrese rezervat pentru rețelele private este 10/8, 172.16/12 și 192.168/16. Include o clasă A, 16 rețele din clasa B și 256 rețele din clasa C. Folosind adresarea classful, marile organizații pot folosi clasa 10.0.0.0/8 pentru asignarea de adrese IP în rețea.

Cele de dimensiune medie pot folosi o rețea din clasa B, de la 172.16.0.0/16 la 172.31.0.0/16. Organizațiile cu puține cereri de adrese IP pot folosi rețele din clasa C – care încep cu 192.168 şi care au o capacitate de maxim 254 de stații fiecare.

NAT (1)

- Este un protocol folosit pentru a face trecerea între adrese publice şi adrese private
- Are variantele:
  - **static NAT - one-to-one**
  - DNAT - many-to-many
  - PAT - multiplexare cu porturi



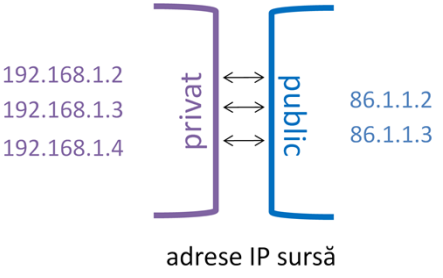
Echipamentele ce folosesc NAT convertesc adrese IP interne în adrese IP globale unice în Internet și vice versa.

Static NAT: mapează o adresă privată la o adresă IP înregistrată, relația fiind de 1 la 1, pentru fiecare adresă privată va fi folosită o adresă publică.

Un avantaj este că, deși este o translatare 1:1, nu este permisă accesarea echipamentelor din rețeaua locală din exterior (Internet). Acest procedeu nu este considerat o regulă de firewall.

NAT (2)

- Este un protocol folosit pentru a face trecerea între adrese publice şi adrese private
- Are variantele:
  - static NAT - one-to-one
  - **DNAT - many-to-many**
  - PAT - multiplexare cu porturi

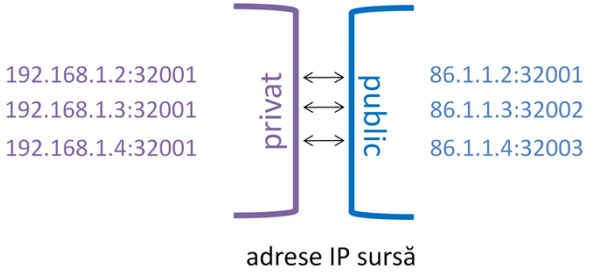


Dynamic NAT**:** mapează o adresă IP privată pe un grup de adrese IP publice. Există două subseturi ale acestui mod:

- Overlapping: Mapează adrese IP private la adrese IP publice configurate într-un grup. Poate de altfel mapa adresele externe la adrese interne.
- Overloading: Mapează mai multe adrese IP private la o singură adresă publică folosind porturi diferite. Aceasta se mai numește și PAT – Port Address Translation.

NAT (3)

- Este un protocol folosit pentru a face trecerea între adrese publice și adrese private
- Are variantele:
  - static NAT - one-to-one
  - DNAT - many-to-many
  - **PAT - multiplexare cu porturi**



Adrese speciale - Ruta default

- Este folosită pentru a specifica unde se vor trimite pachetele dacă acestea nu corespund cu alte intrări din tabela de rutare
- Destinaţia implicită este de forma 0.0.0.0/0
- Implică rezervarea blocului 0.0.0.0/8

Ruta implicită este cunoscută sub numele de poartă de acces de ultimă instanţă, aceasta rută este adăugată manual sau învățată dinamic.

Ea este adăugată ultima în tabela de rutare deoarece are cel mai mic prefix. Această rută trebuie folosită doar în cazul în care nu există în tabelă o rută cu un prefix mai specific spre destinație.

Această rută mai poartă și numele de „quad-zero”

Adrese speciale - Loopback

- Este de forma 127.0.0.1/32
- Folosită pentru a testa stiva TCP/IP proprie
- Nu se apelează hardware-ul de acces la mediu
- Poate fi utilizată în comunicaţie între servicii de pe acelaşi echipament

O interfaţă loopback este doar o interfaţă soft care este folosită pentru a simula o interfaţă fizică. Ca şi alte interfeţe, acesteia din urmă îi putem asocia o adresă IP.

Interfeţele de tip loopback sunt de asemenea folosite de alte protocoale de rutare, ca RIP, EIGRP, OSPF, în diferite scopuri. Într-un mediu de laborator, interfeţele loopback sunt utile pentru crearea reţelelor adiţionale fără a adăuga mai multe interfeţe fizice la ruter.

O interfaţă loopback poate fi anunțată în update-uri și învățate de alte rutere prin intermediul protocoalelor de rutare.

Adrese speciale - Link local

- Sunt in spațiul 169.254.0.0 - 169.254.255.255
- Sunt adrese generate automat de sistemele de operare
- Sunt folosite daca pe mediu nu exista DHCP sau adrese statice
- Aceste pachete nu trebuiesc rutate
- De obicei se trimit cu TTL 1

În RFC 3927, Internet Engineering Task Force (IETF) a rezervat blocul adrese 169.254.0.0 - 169.254.254.255 pentru legăturile inter-locale în abordarea Internet Protocol Version 4. Astfel în procesul de configurare automată a adresei IP, staţia alege o adresă oarecare din domeniul rezervat şi cu ajutorul protocolului ARP testează că adresa nu este folosită în reţea. Dacă staţia primeşte un răspuns la cererea ARP, atunci adresa este deja folosită şi alege o nouă adresă.

Adresele link-local IPv6 au prefixul fe80::/64 şi, spre deosebire de cazul IPv4, este obligatorie configurarea lor pe fiecare interfaţă activă chiar dacă există configurate adrese rutabile.

Internet Assigned Numbers Authority

- Este organizaţia care asigură unicitatea adreselor IP publice
- Alături de IANA există 5 RIR (Regional Internet Registries)
  - AFRNIC - Africa
  - APNIC - Asia, Pacific
  - LACNIC - America de Sud si Caraibe
  - ARIN - America de Nord
  - RIPE NCC - Europa Centrală şi de Est, Orientul Mijlociu
- Oricine doreşte să aibă asociat un IP public trebuie să se înregistreze

IANA este în mare măsură responsabilă pentru alocarea de nume la nivel global unic şi numerele care sunt utilizate în protocoale Internet, care sunt publicate ca documente RFC . IANA menţine, de asemenea, o strânsă legătură cu Internet Engineering Task Force (IETF) şi echipa editorială RFC pentru a îndeplinii această funcţie.

IANA gestionează datele din serverele de nume rădăcină, care formează partea de sus a arborelui ierarhic DNS (root). Această sarcină implică asigurarea legăturii cu domeniul de nivel superior (operatori), operatorii de rădăcină corespunzătoare serverelor de nume.

Internet Service Providers

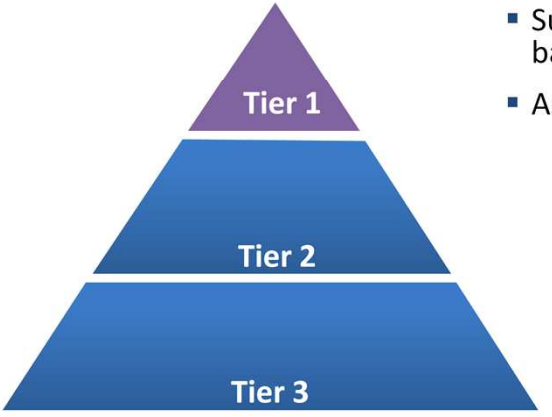
- Adresele IP sunt rareori închiriate direct de la IANA sau RIR
- De obicei IP-urile publice sunt închiriate de la ISP
- Folosind acest model:
  - Companiile sunt vizibile imediat în domeniul public
  - Se centralizează procesul de rutare

Furnizorii de servicii Internet sunt firme sau organizații care oferă conexiune și acces la Internet și servicii. Deseori ei sunt numiți „ISP", inițialele provin din limba engleză *Internet Service Provider*.

Accesul fizic la Internet se poate realiza prin linie de telefon comutată (*dial-up*), acces prin linie închiriată, linie de telefon ISDN, linie de telefon ADSL, cablu (de TV), radio, sistemul de telefonie mobilă GSM, sistemul de telefonie mobilă UMTS și satelit.

Legăturile între diverșii ISP sunt făcute de obicei printr-o rețea de tip „backbone“, capabilă să transmită un volum imens de informații, folosind deseori fibră optică.

Ierarhia ISP



- ISP-uri naţionale sau regionale
- Sunt conectate direct la backbone
- Asigură cele mai bune servicii

Nivelul 1, furnizorii de internet sunt cei mai mari ISP din lume, care formează împreună backbone-ul Internetului.

Nivelul 1 are multiple legături cu backbone-ul, asigurând cea mai mare viteza a traficului. Garantează 99.671% disponibilitate.

Nivelul 2 ISP achiziţionează serviciul de Internet de la Nivel 1. Nivelul 2, în general, se concentrează pe clienţii de business, oferind mai multe servicii decât celelalte două niveluri de ISP.

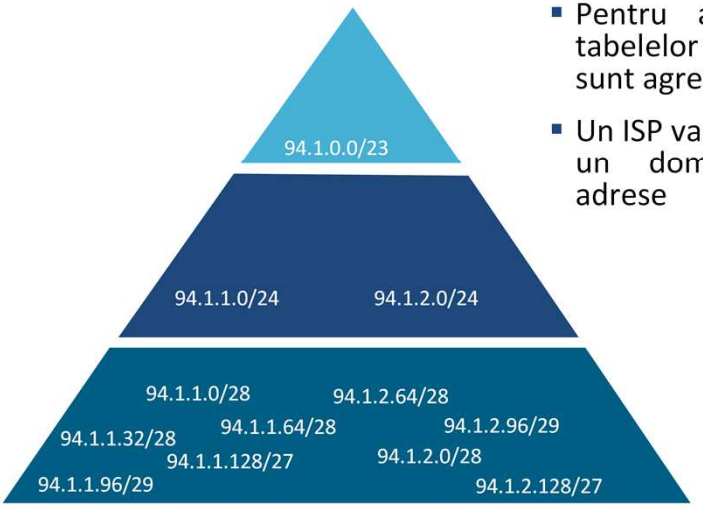
Nivel 2 tinde să dispună de resursele IT, să opereze propriile servicii, cum ar fi DNS, servere de e-mail, şi servere de web

Nivelul 3 sunt cei face oferă acces la internet, sunt legați direct la Romtelecom, RoEdu, sunt acele rețele de cartier.

Cu cât baza piramidală crește cu atât mai mult apar mai multe probleme, complexitatea rețelei crește.

.

Agregare



- Pentru a micșora mărimea tabelelor de rutare rețelele sunt agregate
- Un ISP va da de obicei clienților un domeniu continuu de adrese

O consecința a agregării este micșorarea tabelei de rutare. Pe scurt agregarea se referă la sumarizarea rutelor. Pe măsură ce se vorbește de un Nivel mai specific, cu atât rutele au o mască de rețea mai mică.

Pentru o bună distribuire și administrare, ISP-ul oferă spații de adrese continue.

Un Nivel 3 de obicei nu prea poate agrega rute deoarece și la rândul său este legat la un alt ISP (Nivel 2), Nivel 2 este cel care agregă rutele celor de Nivel 3.

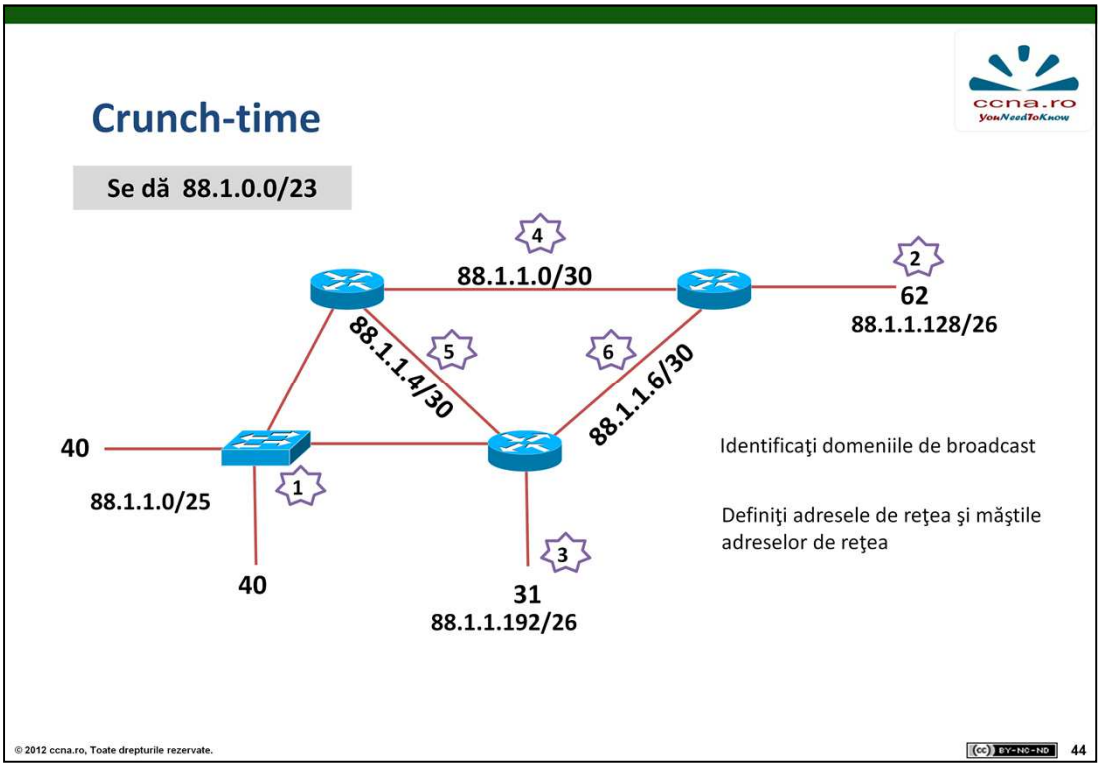
Subnetare - Reguli

- Un domeniu de broadcast corespunde cu o singură adresă de reţea
- Nu trebuie sa existe două domenii de broadcast cu aceeaşi adresă de reţea
- Intervalul de adrese alocabile din două domenii diferite nu trebuie să se suprapună

Un domeniu de broadcast este reprezentat de echipamentele care au aceeași adresă de rețea și primesc și transmit mesaje de tip broadcast numai în limitele acelei rețele. Un domeniu de broadcast este limitat de echipamente de Nivel 3. Echipamentele de Nivel 2 nu delimitează domeniile de broadcast.

Odată alocată o subrețea unui domeniu de broadcast, adresele din cadrul acesteia nu pot fi refolosite în altă subrețea și trebuie să fie unice în subrețeaua respectivă.

În cazul telefoniei IP, echipamentele de VoIP se plasează de obicei într-un VLAN, care este într-un alt segment logic separat de celelalte stații. Separarea echipamentelor de voce de cele de date prin VLAN-uri ajută și la implementarea QoS pentru traficul de voce. Aceasta regulă de design facilitează și depanarea eventualelor probleme.



Având un spațiu de adrese dat (88.1.0.0/23), subnetarea pentru o anumită rețea începe cu identificarea domeniilor de broadcast și a cerințelor fiecăruia (numărul de stații necesar). În cazul acestei subnetări se vor împărți adresele astfel încât să se conserve cât mai multe adrese pentru subrețele adăugate ulterior, deci minimizând numărul de adrese alocabile per subrețea.

Fiecare interfață a ruterului reprezintă un domeniu de broadcast diferit și deci va aparține unei subrețele diferite. În figură sunt 6 domenii de broadcast deci vor fi necesare 6 subrețele.

Subrețeaua 1 va necesita 80 de adrese IP asignabile deci va începea în /25 (vor fi de fapt 126 de adrese asignabile în acea subrețea). Subrețeaua 2 va necesita 62 de adrese IP asignabile deci /26, subrețeaua 3 va necesita 31 de adrese IP asignabile deci /26, subrețelele 4, 5 și 6 sunt conexiuni punct la punct între două rutere deci se vor folosi rețele cu prefixul /30.

Best practice

- Nu alocaţi mai multe adrese decât sunt necesare pentru un domeniu de broadcast
- Alocaţi subneturi în ordinea crescătoare a numărului de utilizatori
- Folosiţi întâi intervalele cele mai mici numeric (ex: 1.1.1.1 < 1.1.1.2)

Nu există o singură regulă de subnetare, subnetarea se poate face în mai multe moduri și poate avea mai multe rezultate. Totuși este recomandat să se înceapă subnetarea de la rețelele cu cel mai mare număr de stații ce necesită IP-uri alocabile.

De altfel, este bine să se înceapă subnetarea cu adresa clasei de la care s-a plecat și să se aloce subrețele consecutive pentru o predictibilitate mai ușoară când vine vorba de proiectarea rețelei.

Luând exemplul anterior de subnetare, este recomandat ca asignarea IP-urilor să înceapă de la Subrețeaua 1 deoarece are cel mai mare număr de stații, după care Subrețeaua 2 cu al doilea de mare număr de stații, etc. De altfel, este recomandat ca asignarea pentru Subrețeaua 1 să pornească cu adresa 88.1.0.0.

ICMP

- Versiunea curentă este ICMPv4
- Funcţioneaza la nivelul 3 pe stiva TCP/IP
- Raportează informaţii sau erori despre reţelele IP
- Nu asigură corecţia problemelor, ci doar raportarea lor
- Are un comportament hop-by-hop

Mesaje ICMP:

Host Confirmation: se confirmă conectivitatea folosind o pereche de mesaje Echo-Request , Echo-Reply.

Time Exceeded: mesaj trimis către echipamentul care a inițiat traficul anunțând că TTL este 0, înainte ca pachetul să ajungă la destinație.

Route Redirection: notifică echipamentul că există o rută mai bună către destinaţie. Se trimite doar dacă sursa traficului este în acelaşi domeniu de broadcast cu gateway-ul.

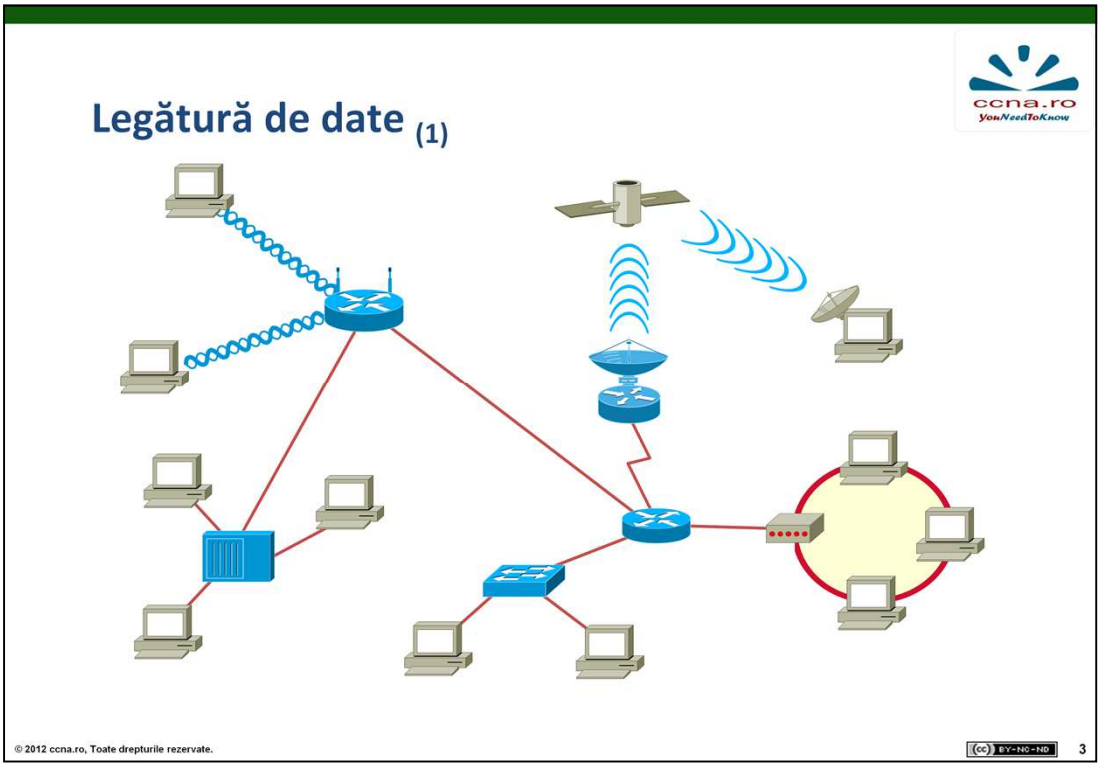
Unreachable Destination or Service: *net unreachable, host unreachable* se trimit la originea traficului când un ruter nu poate ruta un pachet. *Protocol unreachable:* se trimit la originea traficului când pachetele nu pot fi interpretate de nivele superioare.

Source Quench: se trimit către originea traficului dacă aceasta suprasolicită destinaţia.

Capitolul 7:
Nivelul Legătură de date

Obiective

- Rolul nivelului Legătură de date
- Modalități de accesare a mediului
- Topologii
- Standarde



Nivelul Legătură de Date este al doilea nivel din stiva OSI sau o parte din primul nivel din stiva TCP/IP, Acces la reţea.

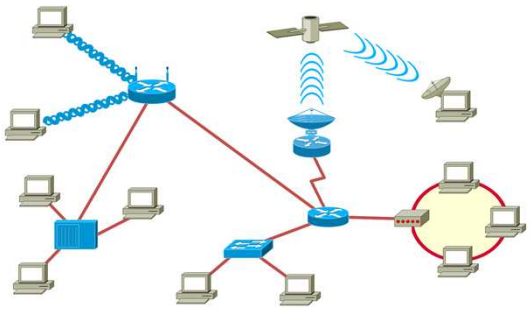
Dacă discutăm despre Local Area Network, tehnologia IEEE 802 este standardul ce definește conexiunea dintre software și mediu fizic. Acest nivel din stiva OSI poartă numele de Legătură de Date.

Nivelul Legătură de Date oferă mijloace funcţionale şi procedurale pentru a transfera date între entităţile de reţea şi poate oferi mijloacele pentru a detecta şi corecta erorile care pot apărea la nivel fizic.

Acest nivel, indiferent de tipul de mediu (cu sau fără fir), are un rol foarte important prevenind așa numitele coliziuni care apar în momentul în care mai multe stații încearcă să comunice simultan.

Legătură de date (2)

- Transmisia de date poate avea loc peste diferite tipuri de echipamente, fiecare cu particularitățile sale
- Cum se înțeleg echipamentele pentru a putea transmite date?

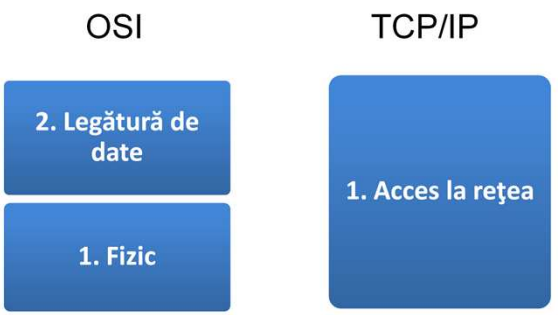


Pentru a realiza conexiunea între două puncte din zone geografice diferite, informația trebuie să parcurgă un drum, acesta purtând numele de mediu. Nivelul Legătură de Date efectuează o serie de activități precum:

- Adresarea fizică – definește modul în care dispozitivele sunt marcate la nivelul Legătură de date, cel mai des este numit Media Access Control (MAC)
- Topologia reţelei – definește modul în care un dispozitiv este fizic conectat la mediu (ex: bus, ring)
- Notificarea erorilor – anunță nivelul superior că a avut loc o eroare în transmisia datelor datorită nivelului fizic (semnal pierdut, clock rate - interfețe seriale)
- Controlul fluxului – administrează fluxul de date între rețea și echipamente

OSI & TCP/IP

- Nivelul 1 al stivei TCP/IP îndeplinește funcțiile nivelelor 1 și 2 ale stivei OSI



În domeniul rețelisticii există mai multe tipuri de stive:

- OSI
- TCP/IP
- IPX
- Appletalk
- NetBEUI

Fiecare dintre aceste stive are aproximativ același comportament, de exemplu stiva OSI are 7 niveluri echivalente cu 4 ale stivei TCP/IP; primele 3 niveluri, 5, 6, 7 ale stivei OSI sunt echivalente cu nivelul Aplicație al stivei TCP/IP.

Nivelul 4 este identic cu nivelul 3, și anume, Transport;

Nivelul 3 (Reţea) este echivalent cu nivelul 2, Internet, iar Fizic și Legătură de date sunt echivalente cu Acces la reţea al stivei TCP/IP.

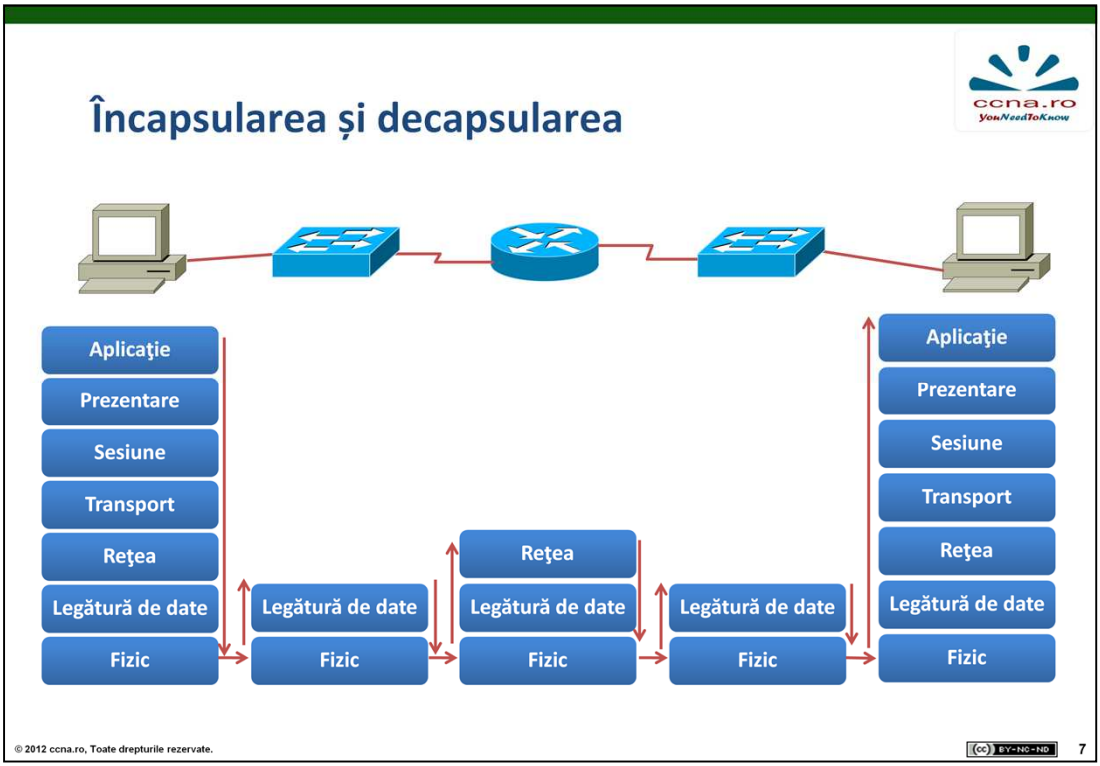
Serviciile oferite nivelurilor superioare

- Încapsularea pachetelor (nivel 3) în cadre (nivel 2)
- Controlul modului în care datele sunt transmise sau primite pe mediu folosind **Media Access Control**
- Detecția erorilor
- Cadrele sunt transmise între stații aflate în aceeași rețea
- Diferențele de mediu sunt transparente pentru nivelurile superioare

Încapsularea reprezintă procesul de adăugare de antete şi „trailer”-e în jurul aceleiași infomații (date).

Un exemplu ar fi transferul de date de la un calculator la altul. Datele sunt încaspulate; la nivel Aplicație sunt datele, pe măsură ce stiva OSI este parcursă, asupra datelor sunt aduse mici modificări: la nivel 4 datele sunt segmentate și este adăugat un antet ce conține informații despre ce proces trebuie să ruleaze pe mașina destinație, cea care trebuie să primească mesajul. De asemenea conține și informații care permit destinației să reasambleze datele în formatul original transmis de sursă. La nivelul Internet, segmentele sunt încapsulate în pachete, care conțin IP-urile sursă și destinație ale echipamentului cu care se realizează transferul.

La nivelul Legătură de date are loc împărțirea în cadre unde este adăugată adresa fizică, adresa MAC, care trebuie să fie unică în rețeaua locală, și în ultima fază informația este transformată în biți.



Încapsularea are loc de la nivelul superior, Aplicaţie la cel inferior, Fizic, în timp ce decapsularea este procesul invers, realizându-se de la nivelul Fizic la nivelul Aplicaţie.

În funcţie de echipamentele de reţea prin care merg spre destinaţie, datele sunt decapsulate la niveluri diferite. De exemplu, un switch decapsulează până la nivelul doi deoarece el are nevoie, pentru a putea trimite pachetul spre destinaţie, de adresa MAC. Ruterul are nevoie de adresa IP destinaţie, așa că pachetele vor fi decapsulate până la nivelul Rețea.

Încapsularea

- Informațiile de control adăugate la nivelul Legătură de date
  - ce noduri comunică în rețea
  - când începe și când se termină comunicarea între două noduri
  - au apărut erori?
  - cine urmează să comunice
- PDU-ul de la nivelul Legătură de date include
  - un prefix (header) – informații de control (de exemplu adresarea)
  - datele – pachetul primit de la nivelul Rețea
  - un trailer – informații adăugate la sfârșitul cadrului (un cod CRC)

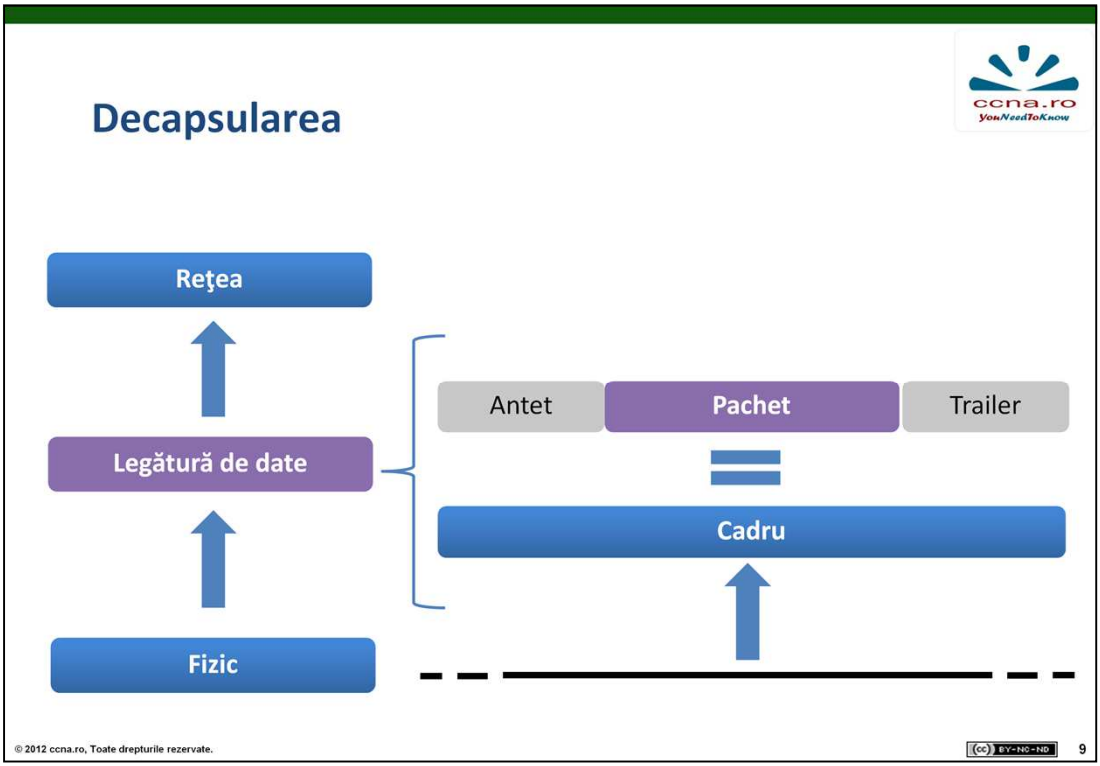
Cele două câmpuri specifice încapsulării de nivel Legătură de Date, Antet și Trailer, conțin următoarele secvențe:

Antet:

- Frame Start – anunță începerea transmisiei datelor
- Addressing – mai poartă și denumirea de Naming
- Type – specifică tipul protocolului sau dimensiunea cadrului
- Control – controlul fluxului de date

Trailer:

- Error Detection – pentru detectarea erorilor de nivel 2
- Frame Stop



Dupa cum s-a precizat și anterior, decapsularea este procesul invers încapsulării și are loc în momentul în care pachetul ajunge la destinație.

În funcție de informațiile adăugate pe parcursul încapsulării, echipamentul de rețea va ști exact cum să reconstruiască datele astfel încât acestea să fie valide pentru aplicația ce le va folosi.

Rolul trailer-ului

- Conține o sumă de verificare a datelor (**Frame Checksum**)
- Marchează sfârșitul unui cadru – **End of Frame** (folosit pentru sincronizare)

Trailerul are doua câmpuri:

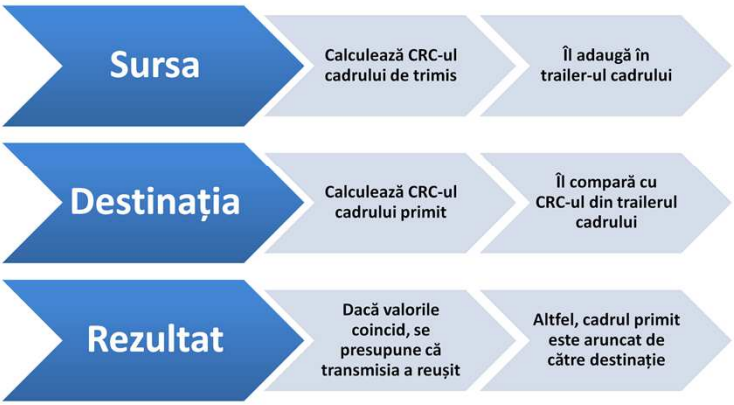
- FCS
- Stop Frame

Principala calitate a trailerului este să determine dacă cadrul ajunge fără erori la destinație. Acest proces este numit *„error detection”.*

Sursa calculează un număr bazat pe dimensiunea cadrului, cunoscut sub numele de CRC (cyclic redundancy check) şi transmis în câmpul FCS. Când destinația primește cadrul calculează și ea CRC-ul și verifică dacă valoarea calculată este egală cu valoarea din FCS trimisă de sursă. Dacă aceste două valori nu coincid, cadrul va fi șters.

Stop Frame este un câmp opțional, folosit când lungimea cadrului nu este specificată în câmpul Type/Length.

Cyclic Redundancy Check



În cadrul Trailer-ului există un câmp numit Frame Check Sequence (FCS) care are rolul de a determina dacă au avut loc erori în transmisia sau receptarea cadrelor.

Mecanismul de detectare a erorilor furnizat de FCS, descoperă erorile cauzate de mediu și asigură validitatea cadrelor. Se creează o sumă logică asupra conținutului cadrului, această sumă purtând numele de Cyclic Redundancy Check (CRC).

Când cadrul ajunge la destinație, se calculează iar CRC-ul și se verifică dacă este identic cu cel primit în cadru.

Dacă este egal înseamnă că acel cadru nu a fost alterat pe drum.

Framing (1)

- Exemplu: structura unui cadru Ethernet

Nr. Octeți	2	1	6	6	2	46-1500	4
Câmp	Preambul	Delimitare început de cadru	Adresă destinație	Adresă sursă	Tip/ Lungime	Payload	Sumă de control

Preambul – este folosit pentru sincronizare, conține de asemenea un delimitator pentru a marca sfârșitul de informații.

Adresa destinaţie – conține adresa MAC destinație.

Adresa sursa – conține adresa MAC sursă.

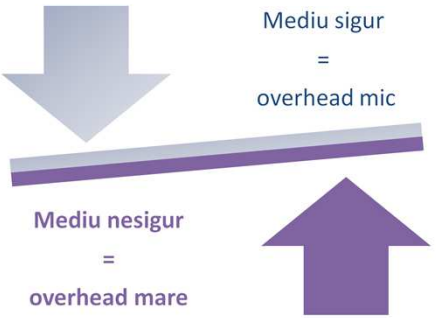
Tip/Lungime – valoare care face referire la protocolul superior, dacă valoarea este 0x0600 (hex) sau, dacă este mai mică, face referire la dimensiunea cadrului.

În 802.3 o valoare cuprinsă între 46-1500 în decimal este lungimea protocoalelor interioare, header-ul LLC indică tipul protocolului interior.

Payload – acesta este PDU, specific IPv4 care vor fi transportate peste mediu.

Framing (2)

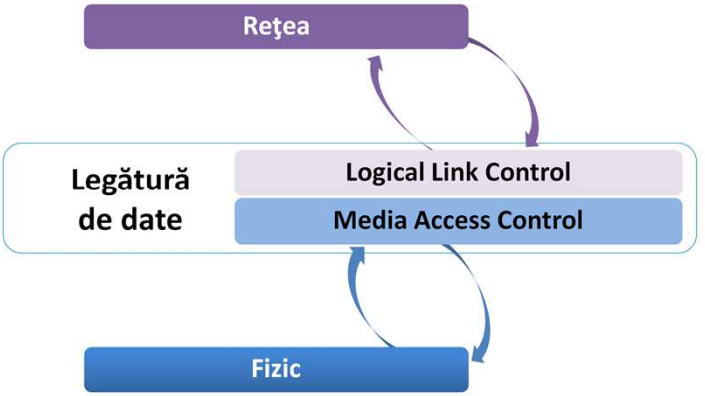
- Informațiile de control depind de mediul de transmisie
  - într-un mediu nesigur e nevoie de mai multe informații de control
  - într-un mediu sigur (ex.: rețea locală) sunt folosite mai puține informații



În general, pentru a crește securitatea este nevoie de mai mulți parametri, ceea ce înseamnă un overhead mai mare, pe de altă parte dacă în rețeaua locală se dorește o viteză mai mare.

Nu este nevoie de securitate, este recomandat să se folosească cât mai puțini parametri de control.

Subnivelurile Legătură de date (1)



Legătură de Date este nivelul ce face trecerea dintre software și mediu fizic, acesta fiind împărțit în două componente:

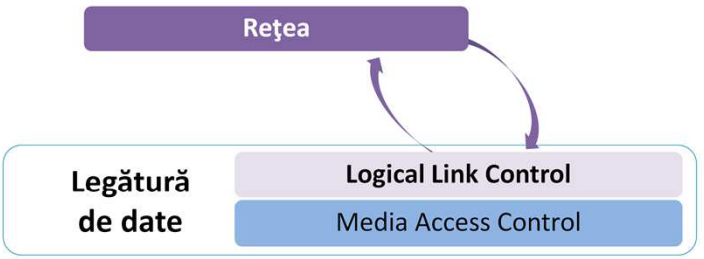
- Logical Link Control
- Media Access Control

Standardul ce definește Logic Link Control este 802.2, fiind subnivelul ce prezintă o interfață uniformă pentru utilizator a serviciului Legătură de Date.

802.3 este standardul pentru MAC, subnivel ce este dependent de mediu (Ethernet, token ring, FDDI, 802.11).

Subnivelul MAC are ca rol principal identificarea într-un mod unic a dispozitivelor în cadrul rețelei locale.

Subnivelurile Legătură de date (2)



- Logical Link Control (LLC) – 802.2
  - definește partea software care permite comunicarea nivelurilor superioare cu mediul fizic
  - realizează încapsularea datelor
  - adaugă informații ce permit mai multor protocoale de nivel 3 să comunice folosind aceeași legătură fizică

Logical Link Control este subnivelul superior al Legăturii de date. Când un echipament primește un cadru și analizează antetul LLC, el găsește protocolul de nivel superior la care să transporte cadrul, de exemplu protocolul IP la nivelul Network sau IPX.

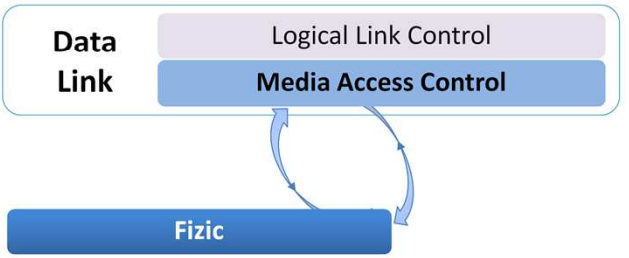
Acest standard oferă două conexiuni de tip neorientat pe conexiune și una de tip orientat de conexiune.

- Tipul 1: unacknowledged connectionless, permite trimiterea unor cadre unicast, multicast sau broadcast
- Tipul 2: connection-oriented – cadrele sunt reasamblate în ordinea în care au fost trimise
- Tipul 3: ack connectionless – suportă doar comunicația punct-la-punct

O altă funcționalitate a Logical Link Control este să administreze și să asigure integritatea datelor transmise.

Subnivelurile Legătură de date (3)

- Media Access Control (MAC)
  - definește partea hardware a procesului de acces la mediu
  - se ocupă de problemele de adresare
  - realizează delimitarea cadrelor



Pentru ca o comunicație să se realizeze cu succes, fiecare stație trebuie să aibă propria adresă Media Access Control, unică în rețeaua locală.

Adresa MAC este memorată pe 48 de biți.

Standardul 802.3 definește mai multe componente care specifică tipul și viteza diferitelor cabluri și tehnologii.

Ca exemplu putem avea:

- **802.3a** – apărut în anul 1985, 10BASE2 10Mbit/s (1.25 MB) pe cablu coaxial
- **802.3b** – apărut în anul 1985, 10BROAD36
- **802.3u** – Full duplex
- **802.3z** – aparut in 1998, 1000BASE-X Gbit/s Ethernet pe fibră optică

Media Access Control

- Reprezintă procesele prin care echipamentele pot accesa rețeaua
- Mediile prin care sunt transmise informațiile pot să difere de la o rețea la alta
- Cine realizează acest control?
  - pentru calculatoare
    - placa de rețea
    - modem-ul (de telefon, cablu etc.)
  - în cazul echipamentelor intermediare (rutere) – fiecare interfață se ocupă de accesul la mediu potrivit pentru fiecare rețea

Media Access Control este mecanismul care oferă accesul la rețea. El este unic în rețeaua locală, acest lucru asigură că pachetele destinate unei stații nu vor ajunge și la alte destinații. Adresa MAC este arsă pe placa de rețea, este furnizată direct de către producător, însă ea poate fi schimbată la nivel software.

Dacă două dispozitive de rețea au aceeași adresă MAC, situație destul de des întâlnită și nedorită de administratorii de rețea, atunci rețeaua este compromisă.

Pot exista adrese MAC identice fără a cauza probleme, când adresele MAC fac parte din rețele diferite.

Accesul la mediu

- Factori care influențează accesul la mediu
  - mediul este sau nu partajat - cum se realizează această partajare
  - topologia - modul de conectare a stațiilor
- Existența regulilor
  - este necesară prezența unor reguli de acces la mediu
  - regulile prea stricte pot produce un overhead prea mare
  - regulile prea puțin stricte pot permite pierderi de informații

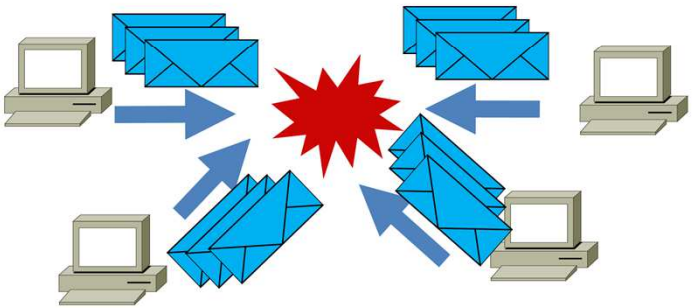
În funcție de modul în care informația accesează mediul poate exista un overhead mai mare.

Dacă se dorește filtrarea anumitor pachete este novoie de un mecanism care să permită inspecția datelor la nivel 7, ceea ce înseamnă un timp de procesare mai lent față de o soluție care nu implementează reguli de firewall.

Cu cât se încearcă o filtrarea a pachetelor la un nivel mai ridicat în stiva OSI cu atât este nevoie de timp de procesare, de echipamente dedicate, cât și de un administrator care să le configureze cât mai optim. Un alt criteriu este costul ridicat de implementare, și viteza traficului, deoarece orice nouă regulă de securitate încetinește viteza de acces la resurse.

Scenariul 1: Fără reguli

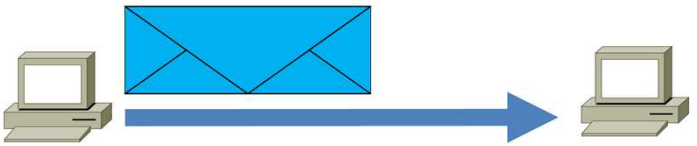
- Oricare stație transmite când vrea, cât vrea, cum vrea



Dacă în rețea nu ar exista niciun fel de reguli de firewall, fiecare stație ar putea oricând să trimită orice tip de informație, indiferent de mărimea ei, ceea ce ar provoca o supraîncărcare a mediului, acest lucru putând duce la incapacitatea de a mai putea accesa resursele.

Scenariul 2: Reguli prea stricte

- Pentru transmiterea datelor se folosesc multe informații de control și verificare
  - overhead mare
  - siguranță mai mare a datelor



Dacă administratorul de rețea consideră că datele sunt de o valoare însemnată, trebuie impuse diferite reguli care sa asigure securizarea informaţiei.

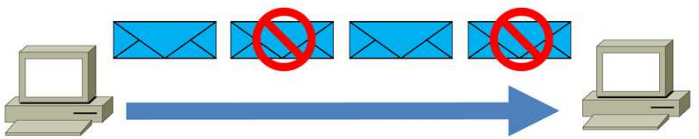
Cu cât aceste reguli sunt mai stricte cu atât overhead-ul crește, dar oferă în continuare o siguranță sporită a datelor.

Securizarea datelor se poate realiza cu diferite tool-uri (ACL) sau cu echipamente dedicate (Firewall - ASA).

Un firewall dedicat este folosit pentru a proteja rețeaua de atacuri din exterior, dar există posibilitatea ca atacatorul să obțină acces fizic la rețea. În această situație a fost implementat protocolul 802.1X care realizează protejarea rețelei de atacurile de la toate nivelurile prin securizarea nivelului Legătură de Date.

Scenariul 3: Reguli prea puțin stricte

- Pentru transmiterea datelor se folosesc mai puține informații de control și verificare
  - overhead mic
  - siguranță mai mică a datelor

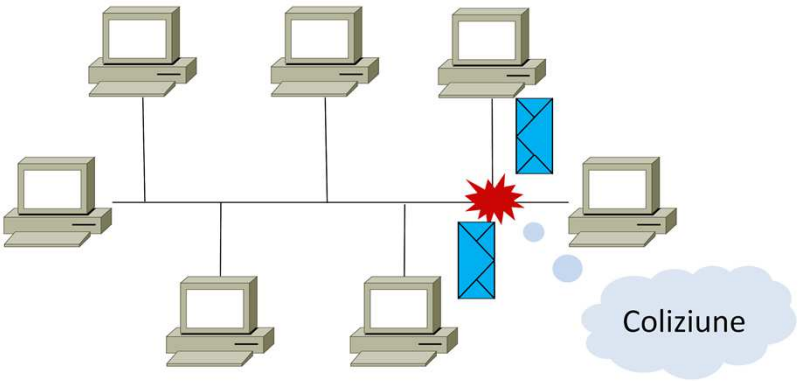


În cazul in care nu există securitate sau aceasta are un nivel foarte mic, pot apărea probleme, deoarece unele pachete pot fi alterate, de o altă persoană din rețea.

Există mai multe tipuri de atacuri de rețea, fiecare dintre ele testând vulnerabilitați diferite ale rețelei, ca exemplu putem avea:

- De recunoaștere:
  - ping sweep, Sniffing, Port scan
- De DoS (Denial of Service) sau DDoS (Distributed DoS):
  - smurf attack, SYN flood
- De acces:
  - atacarea unei parole (cu dicționar sau brute-force)
  - buffer overflow sau Man-in-the-middle

Mediul partajat



Din punct de vedere al securității, mediul partajat nu poate oferi un grad minim de securitate, dar ofera o imunitate bună la interferențele electromagnetice.

Într-un mediu partajat, toate stațiile care comunică în același timp produc o coliziune.

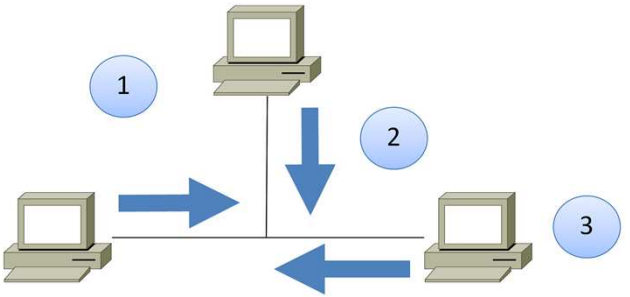
Coliziunea este rezultatul compunerii a două sau mai multe semnale electrice, în urma căruia informația transmisă este deteriorată.

Pentru detectarea și soluționarea coliziunilor sunt folosite mai multe tehnici, ca exemplu:

- CSMA/CD – folosită pentru comunicații pe fir
- CSMA/CA – folosită pentru comunicațiile fără fir

Acces la mediul partajat (1)

- Modul de acces controlat
  - se folosește o abordare de tip round-robin
  - acces determinist – se știe cine are dreptul să transmită
  - poate fi ineficient deoarece fiecare stație are rezervată o cuantă de timp chiar dacă nu are nimic de transmis



Mediul partajat este caracterizat de coliziuni, fapt pentru care trebuie să existe metode de control a acestei probleme.

Ca soluție oferită este modul de acces la mediu:

- Controlat
- Concurențial

Din punctul de vedere al accesului la mediu accesul controlat, de tip round-robin, este o soluție.

Pe de altă parte în cazul în care este o topologie cu un număr ridicat de utilizatori, datorită faptului că pentru fiecare stație îi este rezervat un cuantum de timp, chiar dacă este nevoie ca o singură stație să trimită informație, aceasta trebuie să își aștepte rândul.

Acces la mediul partajat (2)

- Modul de acces concurențial
  - acces nedeterminist
  - fiecare stație poate încerca să transmită când are nevoie
  - se folosește ***Carrier Sense Multiple Access (CSMA)***
  - se poate întâmpla ca două calculatoare să transmită în același timp → coliziune (datele trebuie retransmise)
  - mai multe stații conectate în rețea → probabilitate de coliziune mai mare

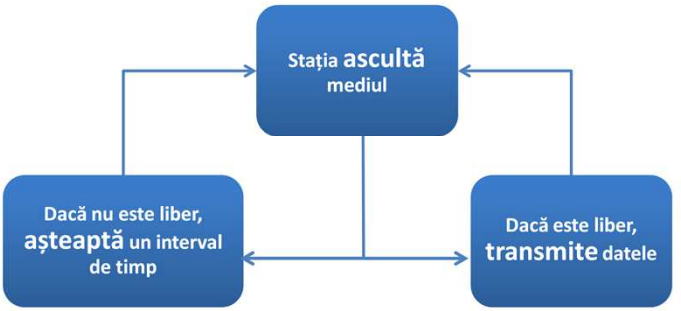
Pentru acest model soluția oferită este CSMA/CD. Acest mecanism spre deosebire de accesul controlat, permite accesul nedeterminist, nu mai este nevoie ca fiecare stație să aibă o cuantă de timp pentru a transmite informații pe mediu.

Principiul de bază este ca, după ce sursa transmite pachetul, aşteaptă un interval foarte scurt de timp (dependent de întârzierile de propagare şi de sistem) apoi îşi ascultă propria transmisie.

Dacă sursa, atunci când acţionează ca receptor al propriei transmisii, detectează o diferenţă între informaţia recepţionată faţă de cea transmisă, va deduce că s-a produs o coliziune pe canal, va trunchia pachetul în curs de transmisie şi va căuta să rezolve coliziunea, organizând, după un algoritm specific, retransmiterea ulterioară a acestuia.

CSMA/Collision Detection

- Folosit în Ethernet



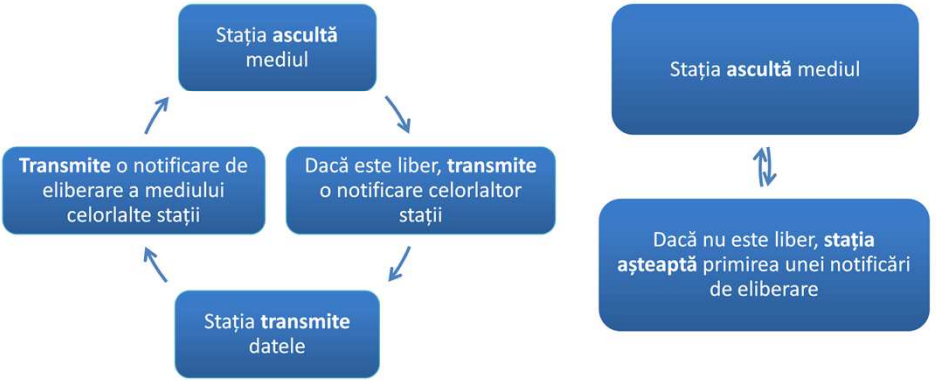
Când o stație dorește să transmită, ea urmează următorul procedeu: „ascultă” pe fir să vadă dacă nu cumva mai transmite cineva în acel moment.

Dacă „aude” că mai transmite cineva, stația așteaptă o perioadă de timp aleatoare după care încearcă să transmită din nou. Dacă nu transmite nimeni, stația începe să transmită, însă în același timp continuă să și asculte, pentru a fi sigură ca nu a mai început nimeni să transmită.

O coliziune are loc când biții de la stații diferite sunt pe același mediu în același timp.

CSMA/Collision Avoidance

- Folosit în Wireless



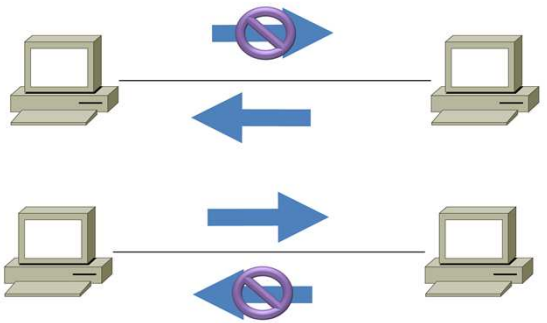
Pentru mediul wireless, nu se poate folosi CSMA/CD pentru acces la mediu. O explicație este ca un emiţător radio nu poate transmite si recepţiona în acelaşi timp. Așa că o staţie nu poate asculta mediul în timp ce transmite, pentru a vedea dacă a apărut o coliziune.

Soluția pentru a remedia aceasta problemă este *„Carrier sense multiple access with collision avoidance”*. Funcţionarea acestui mecanism se bazează pe trimiterea unui cadru special de ACK de la destinaţie la sursă, după fiecare cadru 802.11 primit la destinaţie. Dacă după trimiterea unui cadru, nu se primeşte ACK, se aşteaptă un timp după care se încearcă să se trimită cadrul pentru care nu s-a primit ACK.

Deoarece în wireless pentru fiecare cadru transmis, se aşteaptă ACK, banda efectivă de care se dispune este de la început înjumătăţită.

Acces la mediu nepartajat (1)

- În această categorie intră topologiile punct-la-punct
- Comunicația poate fi **full-duplex** sau **half-duplex**
- **Half-duplex**



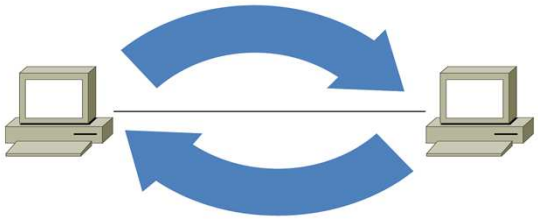
Din perspectiva a două stații direct conectate mediul este nepartajat deoarece în comunicație nu intră și o a treia stație. Comunicația între cele două stații poate fi atât full-duplex cât și half-duplex.

Comunicația half-duplex oferă posibilitatea ca un dispozitiv la un moment dat fie să transmită fie să recepționeze informații. Dat fiind aceste caracteristici putem trage concluzia că în cadrul acestui model de comunicații apar coliziuni.

Dat fiind faptul că o stație nu poate transmite și primi date simultan, în rețea trebuie să existe niște reguli pentru cazurile în care mai multe stații vor să transmită.

Acces la mediu nepartajat (2)

- **Full-duplex** = ambele stații pot transmite și primi date în același timp, deci nu e nevoie de reguli pentru reglarea traficului



În cazul full-duplex există căi dedicate pentru transmiterea și recepționarea informației, fapt ce duce la eliminarea coliziunilor.

Conexiunea full-duplex sau double-duplex system este cea mai răspândită, deoarece are mult mai multe facilități, cât şi viteza superioară transmisiei de tip half-duplex.

De exemplu, cablul coaxial este, prin definiţie, un mediu pentru half-duplex, pentru că transmisia şi recepţia se realizează pe acelaşi fir. Pe cablurile torsadate însă, prin folosirea unei perechi separate pentru transmisie (numită Tx) şi unei alte perechi pentru recepţie (numită Rx) se poate asigura suport de comunicaţie full-duplex.

Atunci când se folosește full-duplex nu se mai foloseşte modul de acces la mediu CSMA/CD pentru că aceasta nu mai este o reţea de tip mediu partajat. Mai exact, dacă este posibilă transmiterea şi primirea de date în acelaşi timp, nu mai pot avea loc coliziuni.

Topologii logice și topologii fizice

- Ce înțelegem prin topologie?
- Există două niveluri la care putem privi topologia unei rețele
  - **fizic** – aranjarea echipamentelor și a conexiunilor dintre ele (corespunde nivelului Physical din stiva OSI)
  - **logică** – se referă la modul de transfer al cadrelor de la un echipament la celălalt. Are în vedere conexiunile virtuale dintre echipamente. Se situează la nivelul Data Link
- Topologia fizică poate fi diferită de cea logică
- Exemple de topologii
  - Point-to-Point
  - Multi-Access
  - Ring

Topologia reprezintă design-ul unei rețele, aceasta fiind realizată în momentul în care este creată rețeaua.

Din punct de vedere al unei topologii există două niveluri:

- Fizic
- Logic

De cele mai multe ori topologia logică este diferită de cea fizică, deoarece există diferite protocoale care necesită un anumit tip de topologie logică.

Un exemplu în care topologia fizică diferă de cea logică este atunci când se folosesc protocoale ce implementează circuite virtuale, ca exemplu: VPN, PPP, Frame Relay, GRE, ATM, etc.

Point-to-point

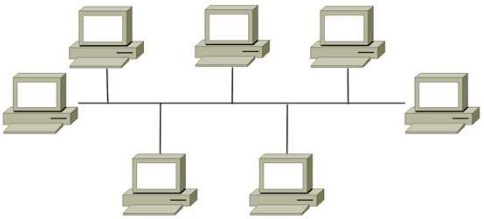
- Două stații sunt conectate direct
- Protocolul de control al accesului la mediu este simplu
- Poate funcționa half-duplex sau full-duplex
- Din punct de vedere al topologiei logice
  - nu este influențată de modificări ale topologiei fizice deoarece topologia logică se referă la circuite virtuale
  - echipamentele pot fi interconectate folosind mai multe echipamente intermediare

Legăturile punct-la-punct, sunt reprezentate în general de legăturile seriale.

Din punct de vedere al nivelului Legătură de Date, pot exista mai multe tipuri de încapsulare, astfel:

- High-Level Data Link Control
- Frame Relay
- Point-to-point protocol
- ISDN

Acces multiplu



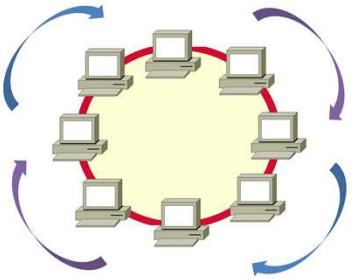
În cadrul topologiei de tip acces multiplu doar una dintre stații poate transmite la un moment dat, astfel este nevoie de o metodă de acces a mediului mai avansată pentru a reduce numărul posibilelor coliziuni.

Toate celelalte stații văd cadrul transmis dar numai destinația va putea prelucra pachetul.

De obicei se folosește CSMA/CD sau CSMA/CA, dar se poate folosi și token passing (determinist).

O topologie de tip multiaccess poate fi determinată de o comunicație pe fir sau fără fir, însă în prezent cea mai întâlnită comunicație de acest tip este wireless-ul, mai general formulat comunicația pe bază de unde (electromagnetice).

Ring



Stațiile primesc pe rând cadrul transmis și dacă nu le este adresat îl trimit mai departe, se poate folosi o metodă controlată de acces la mediu numită „token passing”.

Când nu se transmit date, pe mediu există un semnal numit „token” (jeton).

O stație nu poate transmite decât în momentul în care are jetonul.

Acest tip de topologie a fost folosit pentru prima dată în implementarea algoritmilor de alegere a liderului. În cadrul unei rețele de servere există necesitatea ca informația să fie transmisă într-un mod centralizat pentru un management mai ușor și o evitare a supraîncărcării rețelei. Liderul este echipamentul care va primi informația de la celelalte dispozitive din rețea o va prelucra și va răspunde.

Adresarea fizică

- Datele de adresare se găsesc în header: adresa destinație și adresa sursă
- Este un tip de **adresare plată** → un echipament poate fi mutat în altă rețea fără a schimba adresa fizică
- Are relevanță numai în rețeaua locală
- La trecerea dintr-un segment de rețea în altul (la trecerea printr-un ruter) adresele sursă și destinație de nivel 2 se modifică
  - cadrul va fi recapsulat cu informațiile de adresare corecte pentru noul segment de rețea
- Adresarea depinde de topologia logică folosită

Adresele MAC sunt folosite pentru realizarea adresării fizice.

Acest tip de adrese folosesc o schemă de adresare plată (spațiul de adresare este ocupat treptat și complet).

Mulțimea adreselor fizice este neordonată, fapt pentru care nu poate fi folosit integral spațiul de adrese MAC disponibil. Cu toate că această schemă de adresare fizică nu a fost modificată și nici măcar actualizată pe parcursul ultimilor 20 de ani, IEEE a anunțat că cel puțin până în 2100 spațiul de adrese fizice nu va fi epuizat.

Standarde pentru nivelul Legătură de date

- În general, protocoalele de la nivelul 2 nu sunt definite în RFC-uri
- Implementarea acestor protocoale se face atât în hardware cât și în software
- Pentru mai multe detalii despre standardele utilizate de nivelul 2
  - http://www.iso.org → HDLC (High Data Level Control)
  - http://www.ieee.org → 802.2, 802.3, 802.5, 802.11
  - http://www.ansi.org → Frame Relay, ISDN, HDLC
  - http://www.itu.org

Ethernet

- Definit de standardele 802.2 și 802.3
- Tehnologie de LAN
- Bandwidth de 10, 100, 1000, 10000 Mbps
- Foloseşte CSMA/CD deoarece reprezintă un mediu partajat
- Adresa MAC
  - 48 de biți (12 cifre)
  - 2 componente: OUI (24 de biți), ID interfață(24 de biți)
  - Exemplu: 00:11:43:A4:1C:99, 00:C0:00:BE:EE:FF

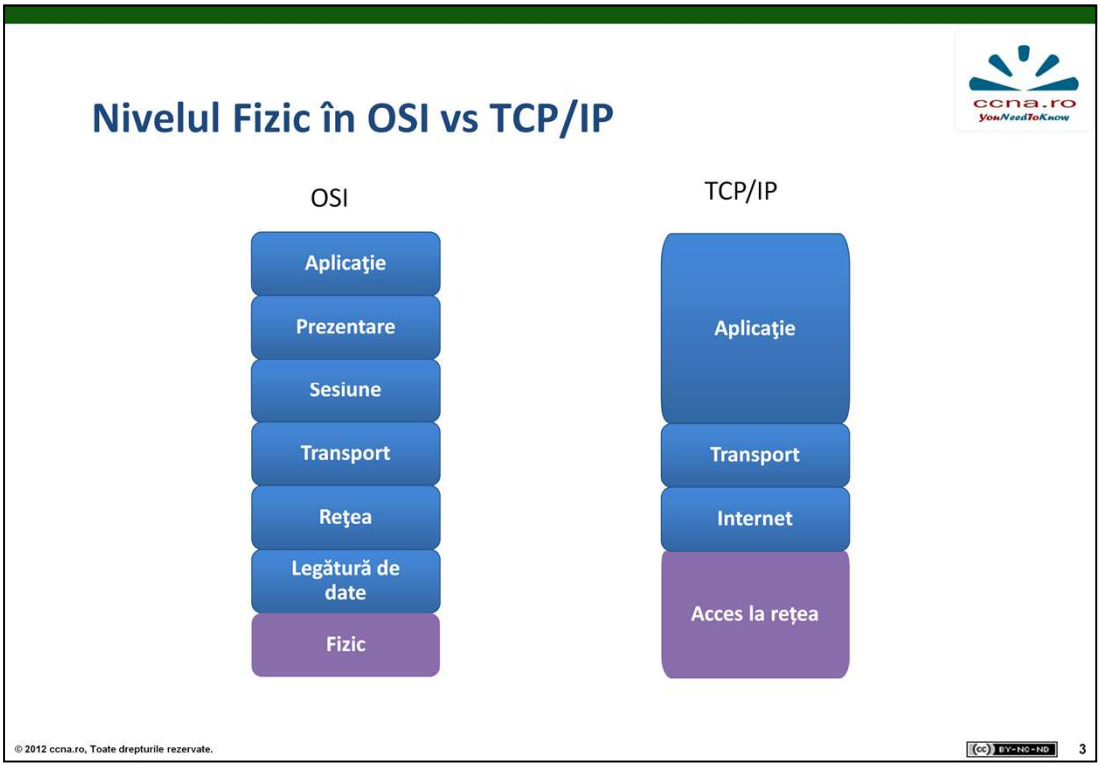
Wireless

- Standardizat ca 802.11 (Wi-Fi)
- Ca și pentru Ethernet se folosește LLC 802.2 și schema de adresare pe 48 de biți
- Mediul de transmisie este aerul/atmosfera, mediu nesigur
- Folosește CSMA/CA
- Folosește acknowledgments: fiecare cadru transmis trebuie confirmat, altfel va trebui retransmis
- Alte servicii definite în standardul 802.11 sunt autentificarea, asocierea și criptarea

Capitolul 7: Nivelul Fizic

Obiective

- Semnale de comunicare
- Reprezentarea biţilor
- Tipuri de medii fizice
- Conectori



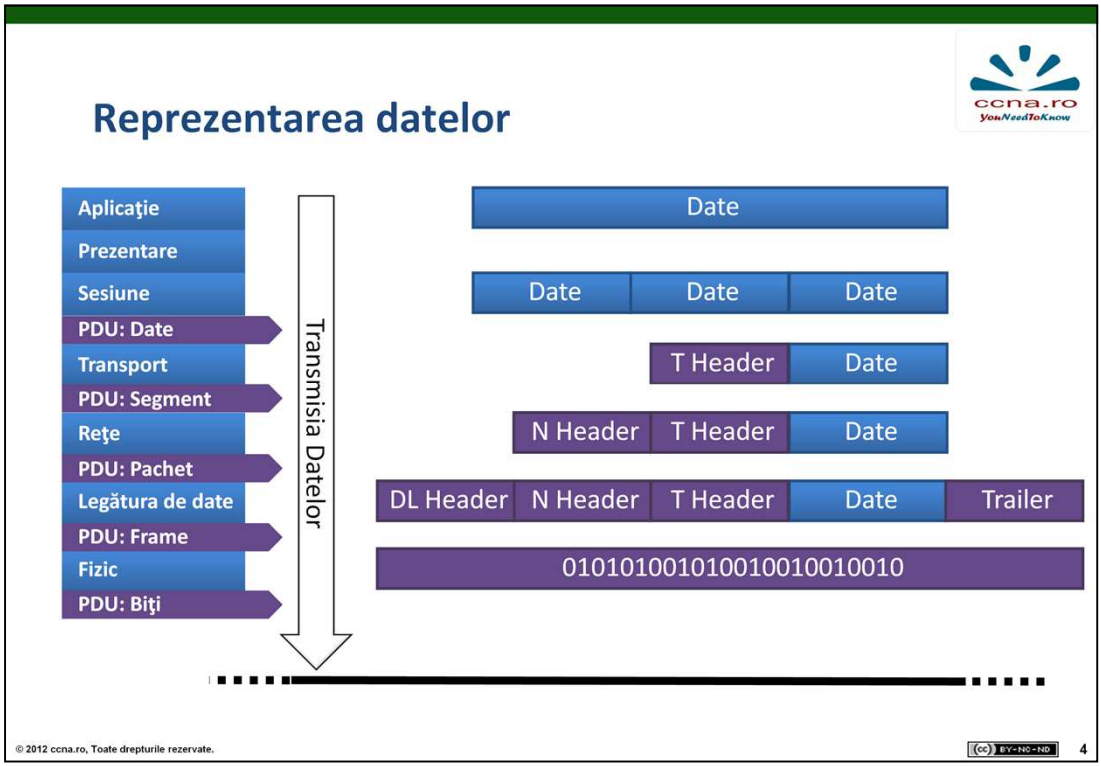
Nivelul Fizic este primul nivel în cele două modele de stive, OSI și TCP/IP. Nivelul „Acces la rețea” descris în stiva TCP/IP este echivalent cu două din nivelurile stivei OSI, cel „Fizic” și „Legătură de date”. Unitatea de date utilizată la nivel Fizic este *bitul*.

Nivelul Fizic stabileşte proprietăţile cablurilor şi ale conectorilor, defineşte protocoalele necesare pentru transmisia datelor pe o linie de comunicaţie.

În cadrul nivelului Fizic se definesc următoarele funcţii:

- Transmisia asincronă
- Transmisia sincronă

Dintre tipurile de medii de transmisiune folosite amintim cablu coaxial, UTP, fibră optică sau „aerul”. La acest nivel se realizează codificarea şi decodificarea şirurilor de biţi (repetoare, media-convertoare).



Dacă pentru primele nivele ale stivei OSI datele erau încapsulate, adăugându-se antete și „trailere”, nivelul Fizic se ocupă cu convertirea informațiilor. Primul pas realizat la acest nivel este aplicarea unui algoritm de codificare a datelor, urmând procesul de serializare.

Procesul de serializare este definit ca fiind procesul de conversie al datelor stocate în memorie, sub forma de biți, în semnale. În funcție de mediu de transmisie folosit aceste semnale pot fi electrice, optice sau sub formă de unde.

O parte a procesului de serializare este reprezentată de modul de sincronizare. O parte din biți transmiși sunt folosiți pentru specificarea începutului de transmisie a datelor, sau pentru semnalizarea încheierii operației de transmitere.

Biţi

- Datele sunt reprezentate în toate spaţiile de stocare şi de transmisie în mod binar
- Biţii sunt cea mai mică unitate de informaţie

Un bit reprezintă unitatea de bază a informației în telecomunicații. Un bit poate avea două stări posibile, 0 sau 1. Aceste stări pot fi reprezentate ca fiind două stări a unui flip-flop, două poziții al unui switch, două nivele de tensiune sau curent, două nivele de intensitate luminoasă sau două direcții ale magnetizării sau polarizării.

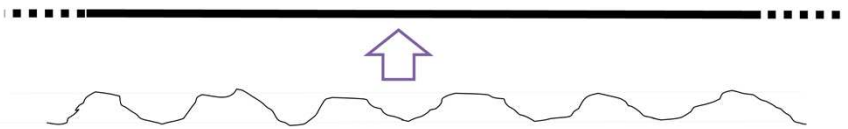
Opt biți reprezintă un octet, denumirea în engleză fiind „Byte (B)”. Foarte important este reprezentarea acestora. Un „kilobyte (Kb)” reprezintă 1024B, iar un „megabyte (MB)” 1024Kb.

Pentru mediile de stocare reprezentarea se face în octeți (B), spre deosebire de viteza de transfer care este reprezentată în biți (b). Presupunem un fișier de 10MB și o legătură de transfer de 100Mbps. Acest fișier va fi transferat în:

- 10MB = 1024 * 10Kb = 1024 * 1024 * 10B = 1024 * 1024 * 10 * 8b / 100 * 1024 * 1024 => 0,8 secunde

Semnale electrice

- Biţii sunt convertiţi în semnale electrice
- Electronii (curentul electric) sunt purtători ai informaţiei
- Convertirea trebuie să fie identică atât la sursă cât şi la destinaţie
- Tensiunile de pe fir pot varia în funcţie de tipul conversiei

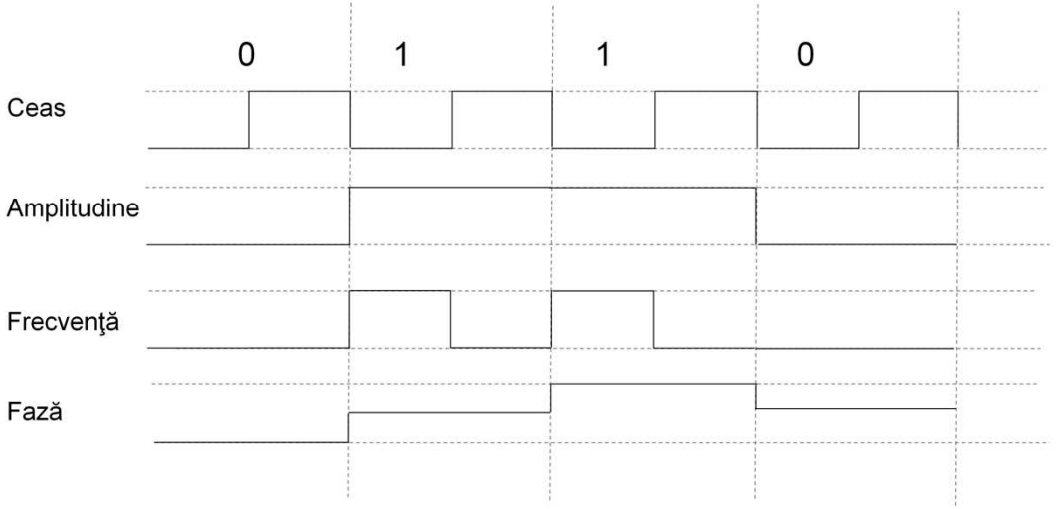


Dacă se folosește un cablu de tip coaxial, UTP sau STP informația va fi transmisă sub formă de semnal electric. De obicei aceste tipuri de cabluri sunt realizate din materiale bune conductoare electrice, precum aluminiu sau fierul.

Semnalul electric este predispus la interferențe. Aceste „zgomote” externe pot afecta reprezentarea unui bit. Un alt factor care poate influența transmiterea folosind semnale electrice este rezistența. Cu cât un cablu este mai lung, cu atât acesta va opune o rezistență mai mare.

În funcție de modul de conversie, tensiunile folosite pentru reprezentarea unui bit pot avea diferite valori.

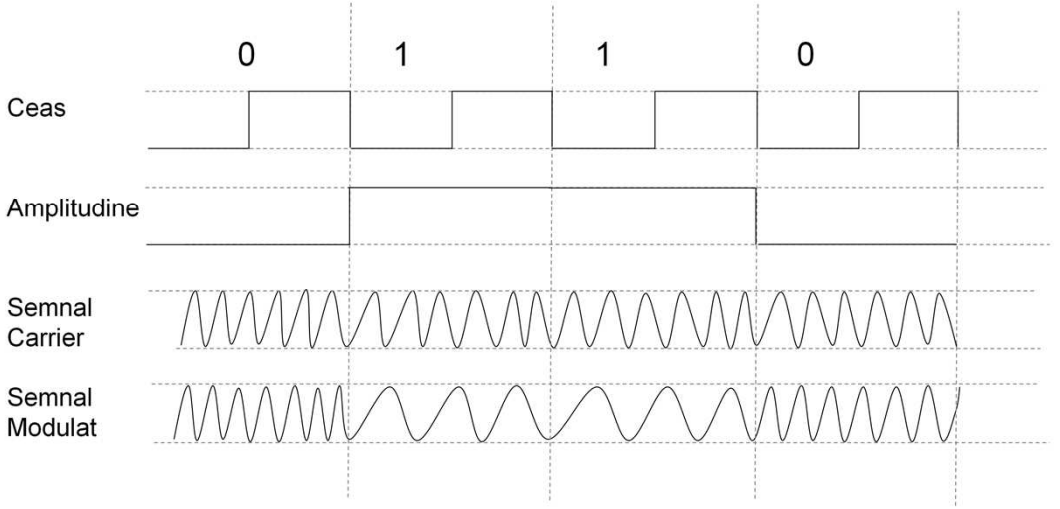
Metode de reprezentare digitală



Informațiile transmise pe rețea se pot reprezenta în semnale prin mai mulți parametri, respectiv prin amplitudine, frevenţă sau fază.

Pentru ca datele să fie sincronizate între sursă și destinație este necesară folosirea unui semnal de ceas iar decodările se fac în funcție de acest semnal.

Frequency-shift keying (FSK)

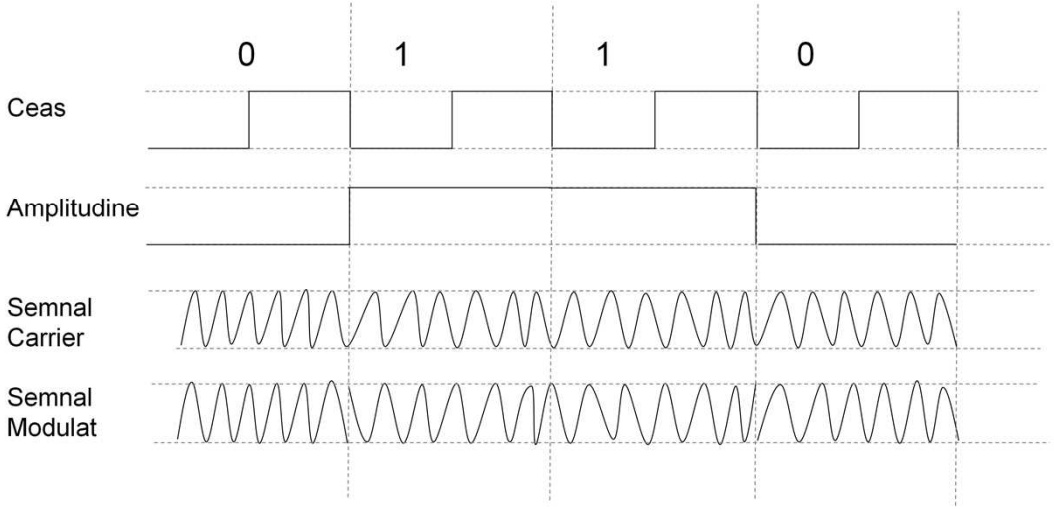


„Frequency-shift keying” este o schemă de modulație în frecvență unde informația digitală este transmisă prin intermediul schimbării discrete a frecvenței folosind un semnal de referință sau purtător.

Cea mai simplă modulație FSK este modulația FSK binară (BFSK) (exemplificată în slide) care utilizează o pereche de frecvențe discrete pentru a transmite informație binară (0 și 1). În această schemă 1 este numită „mark-frequency”, iar 0 este denumită „space frequency”.

Alte exemple de modulații în frecvență sunt MSK (minimum-shift keying) care este folosită în comunicații GSM și AFSK (audio frequency-shift keying).

Phase-shift keying (PSK)

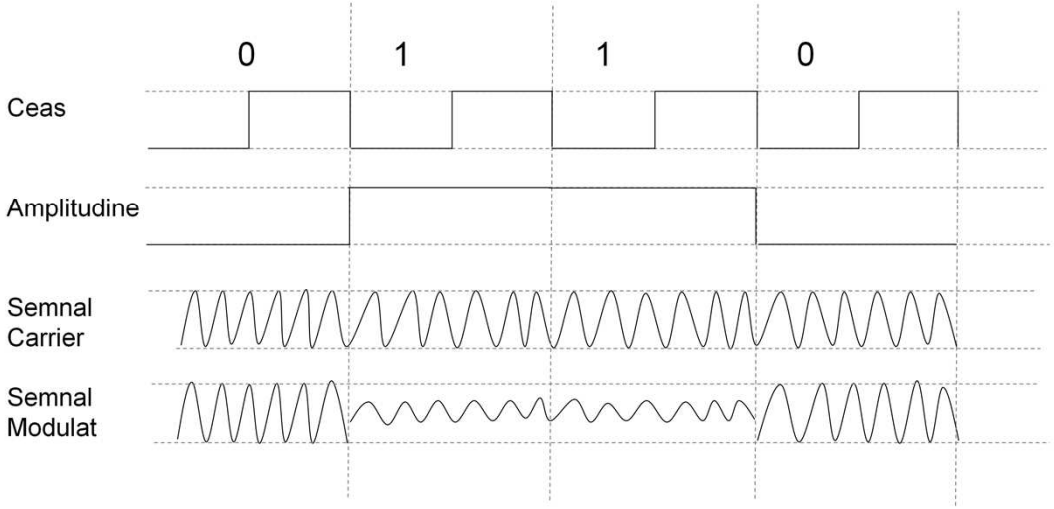


„Phase-shift keying” (PSK) este o schemă de modulație în care se modifică sau se modulează faza semnalului purtător. PSK folosește un număr finit de faze, fiecare asignată unui anumit flux de biți.

Aplicațiile acestor modulații:

- IEEE 802.11b - 1999 (standard Wireless LAN) folosește variante ale PSK respectiv DBPSK (differential binary PSK), DQPSK (differential quadrature PSK)
- Bluetooth 2 folosește π/4-DQPSK și 8-DPSK

Amplitude-shift keying (ASK)

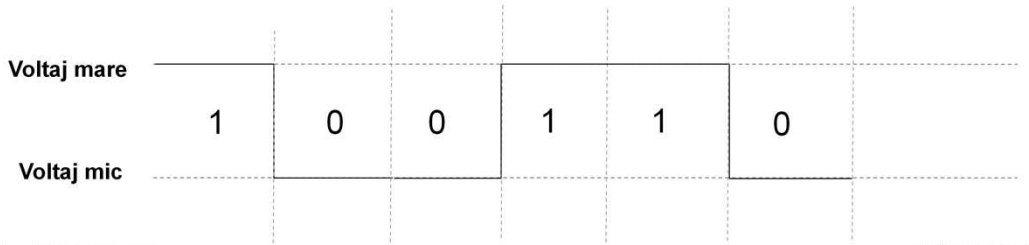


„Amplitude-shift keying” este o modulație care reprezintă informații digitale ca variații ale amplitudinii unui semnal purtător.

ASK folosește un număr finit de valori ale amplitudinii, fiecare asignat unui segment de cifre binare. Spre deosebire de PSK și FSK, ASK este mult mai susceptibilă la zgomot și la interferențe.

Reprezentarea NRZ

- NRZ = Non Return to Zero
- Un voltaj mic reprezintă 0 logic
- Un voltaj mare reprezintă 1 logic
- Voltajul depinde de standardul folosit
- Exemplu: RS232 foloseşte [5V 12V] pentru 0 logic, [-12V -5V] pentru 1 logic



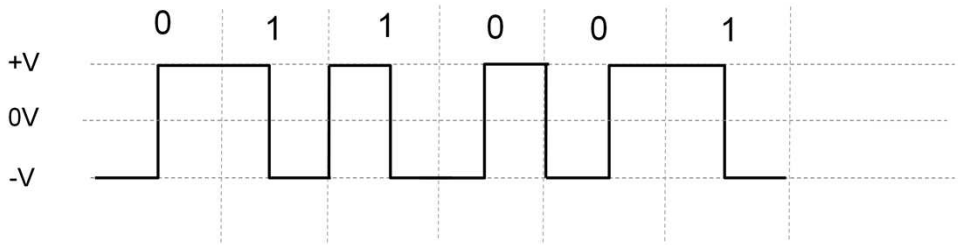
Reprezentarea „Non Return to Zero” este o codificare binară în care biții de valoare 1 sunt reprezentați printr-un anumit nivel al tensiunii electrice iar biții de 0 sunt reprezentați de o altă valoare. Valorile folosite pentru reprezentarea biților depind de standardul folosit.

Această metodă de semnalizare este folosită doar pentru legături de viteze mici.

NRZ nu folosește în mod eficient lățimea de bandă și este susceptibilă la interferențe electromagnetice. În plus se pot pierde din biții transmiși dacă există șiruri continue de biți de 1 sau 0, astfel neaparând tranziții pe mediu.

Codarea Manchester

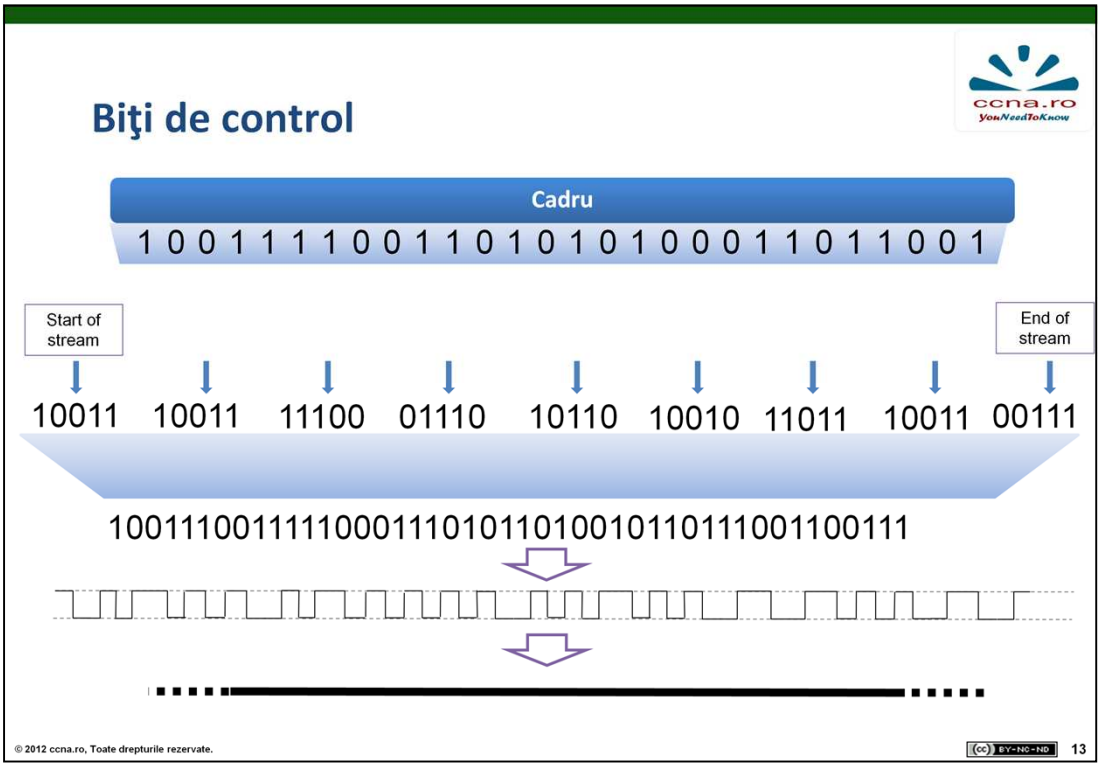
- Folosită în standardul Ethernet
- O tranziţie jos sus reprezintă 0 logic
- O tranziţie sus jos reprezintă 1 logic
- Foloseşte varierea voltajului la jumătatea perioadei de ceas



Codarea „Manchester” nu folosește reprezentarea biților printr-un anumit nivel al tensiunii, ci folosește tranzițiile tensiunii pentru a reprezenta datele.

De exemplu o tranziție de la un nivel mic la un nivel mare al tensiunii reprezintă bit de valoare 0 și invers bit de valoare 1.

Codarea Manchester nu este destul de eficientă pentru a putea fi folosită pe legături de viteze mari. Cu toate acestea a fost folosită în standardul 10BaseT Ethernet (legătură Ethernet cu debit de 10Mbps).



Pe lângă datele primite de la nivelele superioare, la nivelul Fizic se adaugă biți suplimentari de control pentru a mări robustețea transmiterii datelor pe rețea.

Sunt adăugați biți de control pentru delimitarea diferitelor sectoare din fluxul de date precum biții început de flux (11000), sfârșit de flux eroare (01101), de transmitere (00100).

Dacă sunt recepționate date care nu prezintă aceste informații de control, nu sunt transmise mai departe la nivelul Lagătură de Date. Deși mecanismul introduce un „overhead”, asigură robusteţe prin folosirea codurilor de detecţie a erorilor în loc de implementarea mecanismelor de sincronizare.

Throughput, Goodput, Bandwidth

- Medii diferite de transmisie suportă transferul biților la viteze variabile
- Viteza de transfer a datelor poate fi măsurată în 3 moduri:
  - throughput
  - goodput
  - bandwidth

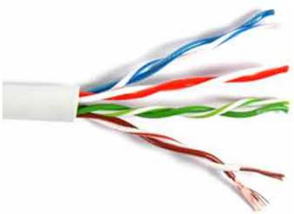
În funcție de câțiva parametri, viteza datelor este influențată:

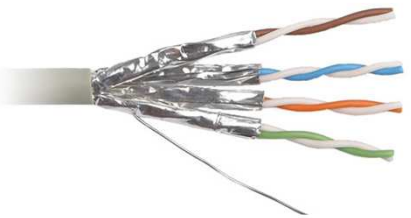
- **Throughput**: reprezintă cantitatea de informaţie determinată practic care poate circula printr-un mediu fizic, măsurată în bps. Este influenţat de trafic, tipul de date sau de numărul de dispozitive intermediare întâlnite
- **Goodput**: reprezintă cantitatea de date care tranzitează mediul fizic măsurată în bps. Este calculat extrăgând „overhead”-ul protocoalelor de comunicaţie din „Throughput”
- **Bandwidth:** reprezintă capacitatea maximă teoretică a unui mediu fizic de transmisie a datelor măsurată în bps

1 Tbps = 10^3 Gbps = 10^6 Mbps = 10^9 Kbps = 10^{12} bps

Copper media (1)

- Fiecare din standarde utilizează nivele de voltaj proprii
  - **UTP**
    = Unshielded Twisted Pair
  - **STP**
    = Shielded Twisted Pair





Cablul „Unshielded Twisted Pair” (cablu torsadat neecranat) este un tip de cablu Ethernet folosit pentru interconectarea echipamentelor de rețea. Pot exista mai multe tipuri de standarde de cablare pentru diferite situații. Există următoarele 3 tipuri de cabluri:

- Straight-through
- Crossover
- Rollover

Folosirea incorectă a acestor cabluri poate duce la deteriorarea echipamentelor dar și comunicația între dispozitive nu este posibilă.

Folosirea unui cablu Ethernet conectat la portul de consolă duce la arderea acestuia. Cablul Shielded Twisted Pair combină tehnicile de ecranare, compensarea efectelor interferențelor și torsadarea firelor.

Ambele standarde folosesc mufă RJ45 drept conector (Straight-through și Crossover)

Copper media (2)

	10BASE-T	100BASE-TX	1000BASE-CX	1000BASE-T
Media	EIA/TIA UTP Cat 3,4,5 - 2 perechi	EIA/TIA UTP Cat5 - 2 perechi	STP	EIA/TIA UTP Cat5 - 4 perechi
Lungime max	100m	100m	25m	100m
Conector	RJ-45	RJ-45	RJ-45	RJ-45

Primele două standarde Ethernet au fost 10BASE2 și 10BASE5 care defineau specificațiile la nivelul Fizic și Legătură de Date.

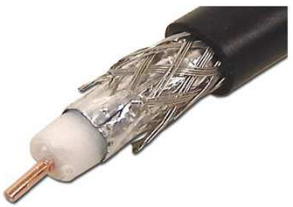
Cu aceste două tipuri de cabluri se realizau rețelele Ethernet fără să fie nevoie de folosirea unor echipamente ca hub-ul sau switch-ul. Rețeaua Ethernet era deci o colecție de NIC-uri (Network Interface Controller) Ethernet ale stațiilor și conexiunile coaxiale. Astfel se realiza rețeaua de tip BUS.

A apărut mai târziu standardul 10BASE-T, 100BASE-TX (Fast Ethernet) și 1000BASE-CX și 1000BASE-T(Gigabit Ethernet). Pentru a suporta aceste standarde au fost create noi echipamente, respectiv hub-uri și switch-uri. Aceste noi standarde presupun folosirea cablării torsadate (twisted-pair).

Indiferent de tipul de cablul folosit, se folosește tot același conector și anume RJ45, în schimb pentru modem conectorul folosit este RJ11.

Copper media (3)

- Cablu Coaxial



Acest tip de cablu a fost folosit pentru prima dată în transmisia de date.

Cablul coaxial este realizat dintr-un conductor din cupru înconjurat de un strat de izolație flexibilă înconjurată la rândul ei de un strat conductor tubular. Ultimul strat de material conductor servește ca un scut conductorului central, reducând interferențele electromagnetice exterioare.

Acest tip de cablu este folosit pentru atașarea antenelor la echipamentele wireless, pentru transportul de semnale de radiofrecvență, în special pentru semnalele de televiziune prin cablu.

Fibra optică (1)

- Nu este afectată de interferenţele electromagnetice
- Cost şi dificultate ridicate în implementarea şi mentenanța soluţiei
- Pierderi foarte mici de semnal şi deci poate fi folosită la frecvenţe mai mici şi la distanţe mai mari
- Durata de timp până la deteriorarea fibrei este de circa 10 ani

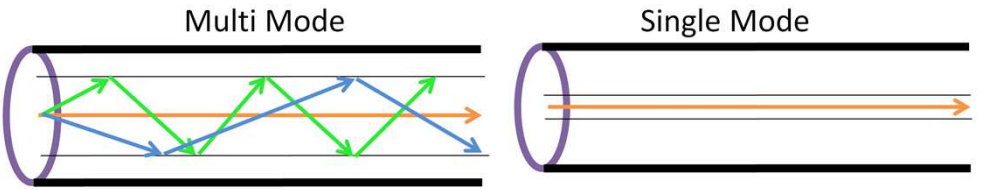
Cablarea cu fibră optică folosește atât sticlă cât și fibrele plastice ca ghiduri de undă pentru transmitere de impulsuri de lumină de la sursă la destinație. Biții sunt codați pe fibră în impulsuri de lumină cu o bandă de frecvențe mari.

În prezent standardele de transmisie nu folosesc la maxim capabilitățile acestui mediu de transmisiune. Pentru că fibra optică nu este formată din conductor electric, acest mediu este imun la interferențe electromagnetice.

În prezent fibra optică este folosită în special în cablările „backbone” pentru conexiuni de mare viteză. Rata de transfer variază de la 51.84 Mbps la 9953.28 Mbps. Folosește standardul SONET și necesită un repetor la maxim 100 km.

Fibra optică (2)

	10BASE-FX	100BASE-SX	1000BASE-LX	1000BASE-ZX	1000BASE-ZR
Mediu	50/62.5 µm fibră multimod	50/62.5 µm fibră multimod	50/62.5fibră multimod sau 9 µm fibră monomod	9 µm fibră monomod	9 µmfibră monomod
Lungime maximă	2km	550m	550m (MMF) 10km (SMF)	70km	80km



În comunicația optică, fibra monomod (single mode fiber) este tipul de fibră care transportă un singur semnal luminos. Nucleul fibrei optice monomod are un diametru suficient de mic astfel încât să permită razelor de lumină să călătorească pe o singură cale, au dispersia mai mică, sunt potrivite pentru distanţe mari (până la 3 km și chiar 100km fără amplificare la 50Gbps), utilizează laserul ca sursă de lumină.

La fibra multimod, diametrul nucleului este suficient de mare pentru a permite mai multe căi de pe care să se poată deplasa lumina în interiorul fibrei, sunt utilizate pentru distanţe mai mici decât cele monomod (până la 2 km) și utilizează LED-urile ca sursă de lumină.

Wireless

- Mediu half duplex
- Se folosesc undele electromagnetice (microunde şi unde radio)
- Riscuri mari de securitate

Standard	Bluetooth (802.15)	802.11 (a,b,g,n)	MMDS, LMDS, 802.16	GPRS, GSM
Viteză	1 Mbps	1-54 Mbps	22 Mbps	10-384 Kbps
Rază	1-10 m	32-95 m	15-100 km	40km
Aplicare	Dispozitive p2p	Reţele	Fixe, acces la distanţă	PDA, Telefoane Mobile

Rețelele fără fir sunt rețele de aparate și dispozitive interconectate prin unde radio, infraroșii, etc. În ultimii ani ele au cunoscut o dezvoltare semnificativă pe plan mondial, reprezentând o soluție alternativă la legăturile cu fir.

Tehnologiile moderne fără fir pot interconecta echipamentele (sau și rețelele locale, LAN-urile) atât la distanțe mici cât și la distanțe mari. Spre deosebire de Ethernet, mediul de transmisie aduce probleme de securitate suplimentară. Dacă în Ethernet, accesul la cablu se putea restricționa, undele radio sunt mult mai dificil de controlat.

Există mecanisme de bruiaj, care generează un zgomot electromagnetic ce acoperă frecvențele folosite de rețelele wireless, dar acestea nu pot funcționa perfect, fără a afecta comunicațiile legitime. Cum la nivel Fizic securitatea este dificil de asigurat, pentru obținerea unui nivel de securitate acceptabil este obligatorie criptarea datelor și controlul accesului la nivelele superioare celui Fizic.

802.11 (1)

- Standard de comunicaţii wireless
- Operează cu frecvenţe nelicenţiate (2.4, 3.7, 5 Ghz)
- Rata de transfer şi raza depind de obstacole
- Este afectat de alte dispozitive electromagnetice

802.11 face parte dintr-o familie de standarde pentru comunicațiile în rețele locale, elaborate de IEEE în anii 1990, prima versiune a acestuia fiind definitivată în 1997, însă în 1999 au început să fie implementate două standarde, respectiv 802.11a și 802.11b.

Din punct de vedere al securității, IEEE și Wi-Fi Alliance recomandă utilizarea standardului de securitate 802.11i, respectiv a schemei WPA2. Alte tehnici simple de control al accesului la o rețea 802.11 sunt considerate nesigure, cum este și schema WEP, dependentă de un algoritm de criptare simetrică, RC4, nesigur.

Limitările standardului provin din mediul fără fir folosit, care face ca rețelele IEEE 802.11 să fie mai lente decât cele cablate, dar și din folosirea benzii de frecvență de 2,4 GHz, împărțită în 12 canale care se suprapun parțial două câte două. Limitările date de consumul mare de energie, precum și de reglementările privind puterea electromagnetică emisă, nu permit arii de acoperire mai mari de câteva sute de metri.

802.11 (2)

Protocol	Data	Frecvență (Ghz)	Perioada de ceas (Mhz)	Mbps	Nr. antene (MIMO)	Modulare	Raza înăuntru (m)	Raza afară (m)
a	Sep 1999	5	20	6-54	1	OFDM	35	120
b	Sep 1999	2.4	20	1-11	1	DSSS	38	140
g	Iun 2003	2.4	20	1-54	1	DSSS OFDM	38	140
n	Oct 2009	2.4 5	20 40	7-72.2 15-150	4	OFDM	70	250

În 1999 au fost publicate două standarde: 802.11a și 802.11b. Primul standard lucra la frecvență de 5GHz și cu viteze de transmisie care ajungeau până la 54Mbps. Folosirea frecvenței de 5Ghz prezintă un avantaj important întrucât este o bandă mult mai puțin folosită de către alte echipamente în comparație cu bandă de 2.4GHz care este aglomerată de numeroase echipamente: cuptoare cu microunde, telefoane wireless, echipamente Bluetooth, etc.

Standardul 802.11b, publicat tot în 1999, lucra la frecvență de 2.4Ghz și atingea viteze de maxim 11Mbps. Deși performanțele acestui standard erau mult mai slabe decât ale 802.11a, a fost preferat deoarece lucra la frecvențe mai mici, deci echipamentele folosite erau mai ieftine.

Un alt dezavantaj al primului standard, datorat tot frecvenței mai mari, era faptul că semnalul era mai atenuat decât cele de frecvență de 2.4. Standardul 802.11g publicat în 2003 este compatibil cu 802.11b.

802.11n - MIMO

- 802.11n este cel mai recent standard Wireless
- MIMO = multiple-input multiple-output
- Atât transmiţătorul cât şi receptorul deţin un sistem de antene folosind multiplexarea spaţială prin transmiterea semnalelor în mod independent pentru fiecare antenă
- Creşte rata de transfer la 72.2 Mbps pentru frecvenţa de 2.4 GHz şi la 150 Mbps pentru 5GHz

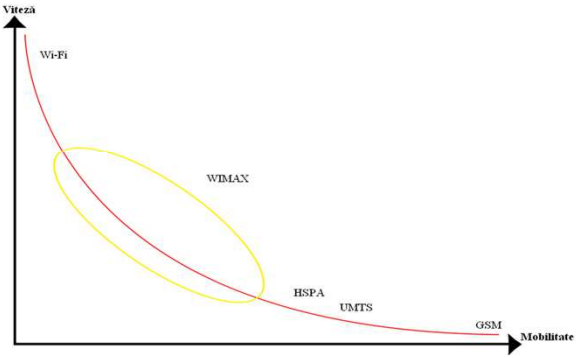
Standardul 802.11n este cel mai nou standard WiFi care îmbunătățește performanța standardelor anterioare funcționând la o viteză de până la 600Mbps. Acest lucru este realizat cu ajutorul unui sistem de antene de transmisie și recepție.

Standardul permite folosirea a patru antene de transmisie și patru antene de recepție realizând astfel patru transmisiuni simultane. Configurațiile folosite cele mai comune sunt: 2x2:2 (două antene de transmisie, două de recepție, două fluxuri), 2x3:2 și 3x3:2.

Standardul este compatibil atât cu 802.11b/g cât și cu 802.11a, funcționând atât în banda de 2.4GHz cât și în cea de 5GHz.

WiMAX (802.16)

- Conectează locaţii la distanţă prin broadband
- Este prima tehnologie 4G
- Utilizează frecvenţele 2.3, 2.5 şi 3.5 GHz atât licenţiate cât şi nelicenţiate
- Rază de maxim 50 km şi o rată de transfer de 70 Mbps

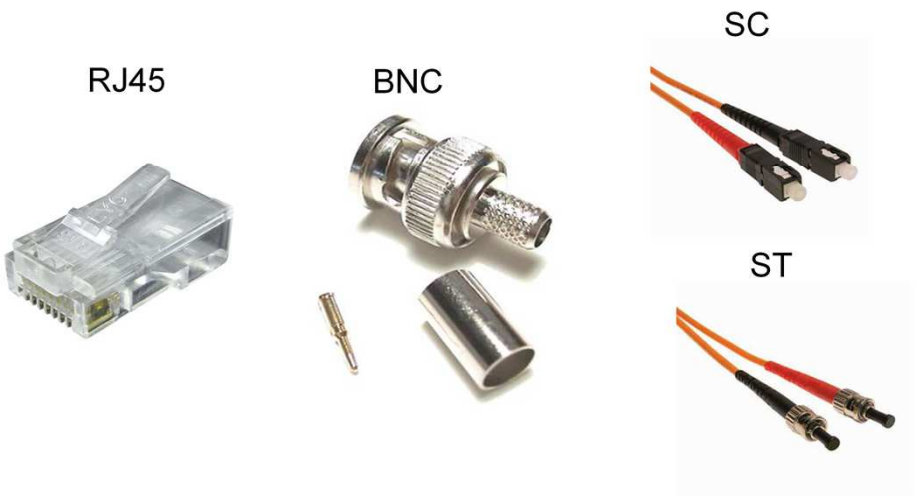


Protocolul WiMAX este o tehnologie broadband care prezintă performate similare cu tehnologiile 802.11 dar cu acoperirea și QoS rețelelor celulare. WiMAX poate furniza acces wireless de mare viteză pe o arie de până la 50km pentru stații fixe și 15km pentru stații mobile.

Cu WiMAX se pot atinge vitezele suportate de tehnologia WiFi dar interferențele sunt diminuate. WiMAX operează atât în benzi de frecvențe licențiate cât și frecvențe nelicențiate.

Cel mai recent standard rival al standardului WIMAX este Long Term Evolution (LTE) care lucrează în mod similar, acesta din urmă reprezentând tot o tehnologie 4G.

Tipuri de conectori



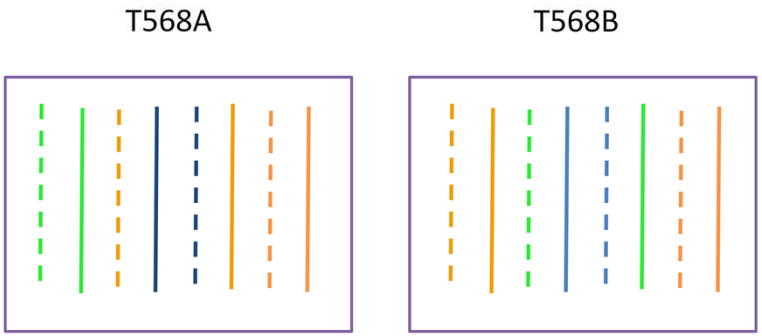
Mufa RJ45 este un conector standard pentru rețelele de comunicații. Conectorul 8P8C (8 pini cu toții conectați) este folosit atât pentru rețele Ethernet cât și pentru rețelele de tip „token ring”.

Mufa BNC a fost folosită în rețele vechi ce foloseau cablu coaxial cu impedanță de 52 de ohmi și aveau conectori sub formă de „T” la calculatoare dinspre capete pentru a „închide” electric rețeaua.

Conector ST (straight-tip) este un un conector standard folosit pentru fibră optică multimod. Conectorul SC (Subscriber connector) este un conector care folosește mecanismul de „push-pull” implementat în cazul fibrei monomod.

Tipuri de conectări (1)

- T568A – Europa
- T568B – America



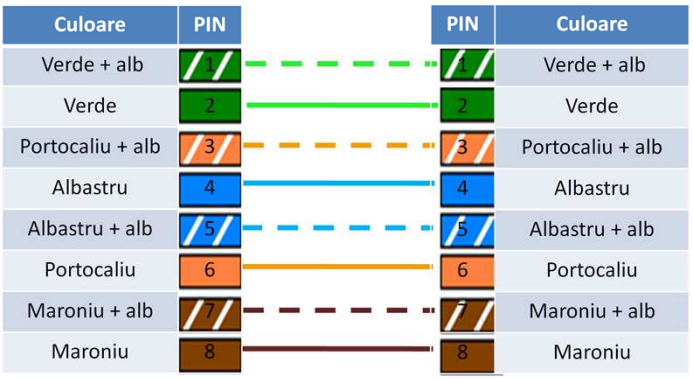
Standardele T568A și T568B sunt două standarde publicate de Telecommunications Industry Association și fac parte din standardul TIA/EIA-568-B.1.2001, publicat în 2001. Ele definesc ordinea conexiunilor firelor într-un modul de tip 8P8C (8 Position 8 Contact). Numerotarea perechilor de fire este următoarea:

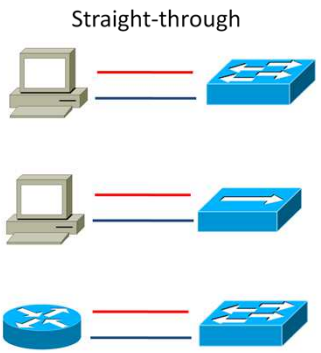
- Perechea 1: albastru
- Perechea 2: portocaliu
- Perechea 3: verde
- Perechea 4: maro

Ordinea firelor depinde de tipul standardului folosit.

Tipuri de conectări (2)

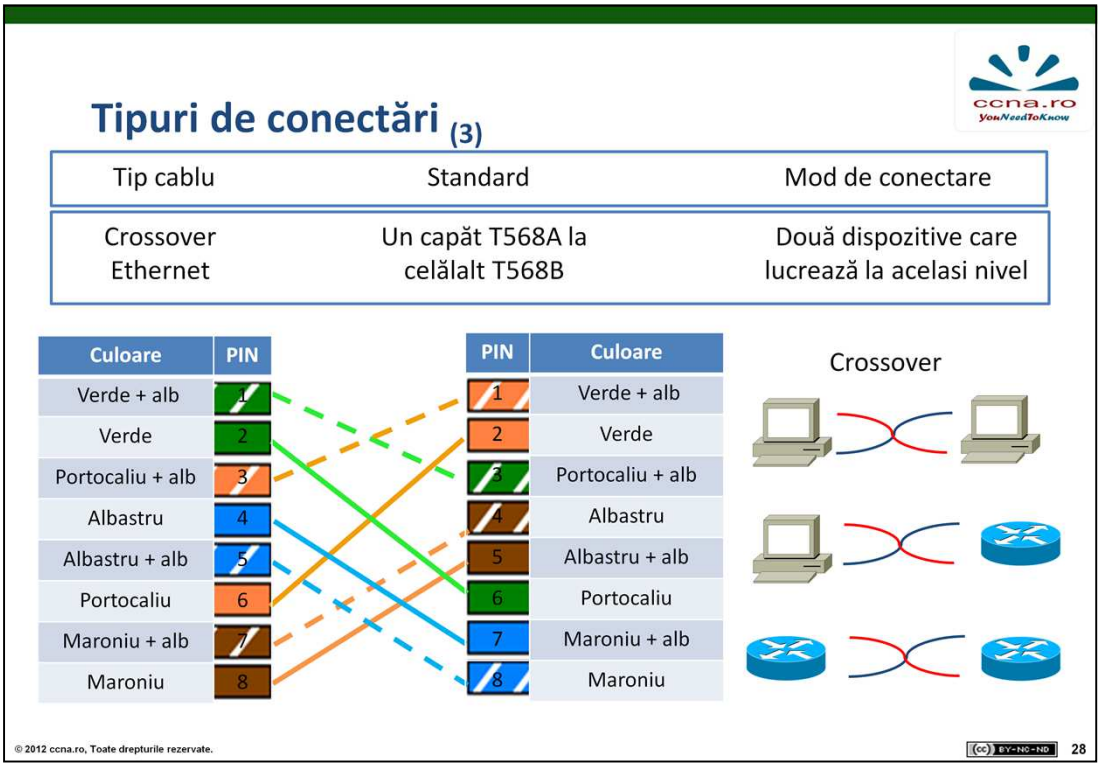
Tip cablu	Standard	Mod de conectare
Straight-through Ethernet	Ambele capete sunt identice (T568A sau T568B)	Dispozitiv nivel 3 la dispozitiv nivel 2





Cablul straight-through este un cablu torsadat folosit în rețelele locale la care ambele capete respectă același standard. Dacă pinii 1 și 2 sunt de transmisie și pinii 3 și 6 sunt de recepție, la cablul straight-through informațiile transmise de un dispozitiv ajung tot în pinii TX la recepție, echipamentul terminal realizând intern schimbul TX-RX. Conectorul folosit este mufă RJ-45.

Acest tip de cablare este folosit de la un dispozitiv de nivel 3, respectiv ruter, PC la un dispozitiv de nivel 2, respectiv switch, hub.



Cablul crossover este un cablu torsadat folosit în rețelele locale la care fiecare capăt este mufat după un anumit standard. Transferul de informație se face în modul următor:

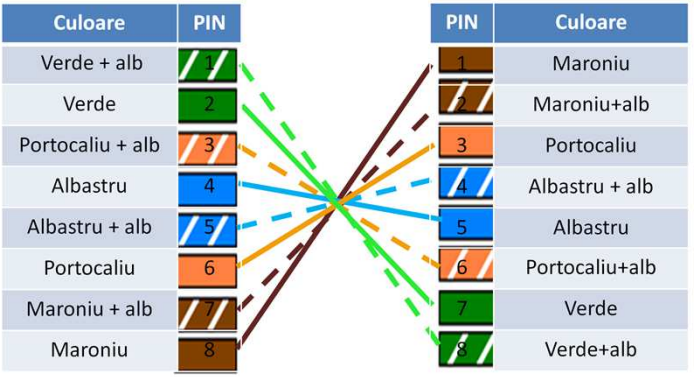
- Pin1 (TX) ↔ Pin3 (RX)
- Pin2 (TX) ↔ Pin6 (RX)

Astfel transferul de la pinii de transmisie la pinii de recepție se face prin cablu. Acest tip de cablare este folosit pentru conectarea dispozitivelor care lucrează la același nivel, respectiv:

- PC-ruter
- PC-PC
- Ruter-ruter
- Switch-switch
- Switch-hub

Tipuri de conectări (4)

Tip cablu	Standard	Mod de conectare
Rollover	Ordinea unui capăt exact opusă celuilalt	O staţie la un port serial de consolă



Cablul rollover este un standard proprietar Cisco folosit pentru conectarea portului serial al unei stații la portul de consolă. Această conectare se folosește pentru configurarea directă a dispozitivelor.

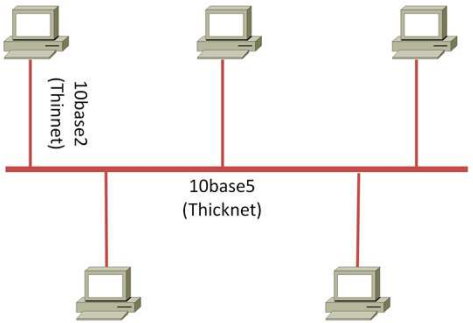
Deoarece că se folosește la porturile seriale, mufarea trebuie să respecte acest standard, de aceea mufarea cablului rollover se face inversând ordinea pinilor de la un capăt la celălalt.

Capitolul 9: Ethernet

Obiective

- Ethernet Legacy
- Ethernet Frame
- MAC
- Ethernet Fizic
- Comunicare
- ARP

Topologii



- Topologie Logică: Bus
- Topologie Fizică: Bus
- Bandwidth partajat 10Mb/s
- Conexiune half-duplex
- Cablu coaxial

În rețelele locale în care este folosită topologia de tip BUS, fiecare stație este conectată la un singur cablu. Dacă un echipament terminal încearcă să comunice cu un altul, semnalul de la sursă va ajunge la toate stațiile din rețea, însă doar destinația specificată de sursă va prelucra informația.

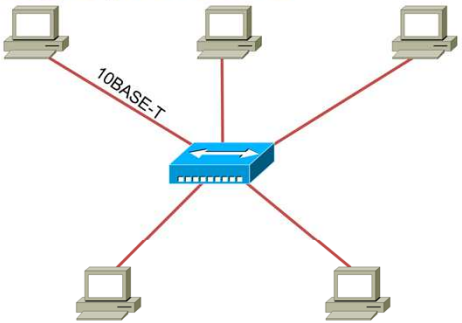
Pentru acest tip de rețea, predominant este cablul coaxial gros RG-62, sau cablul coaxial subțire RG-58.

Unul din dezavantajele majore ale acestui tip de topologie este că, dacă în orice punct al rețelei cablul are o problemă, întreaga rețea nu va mai putea fi folosită.

Există două tipuri de rețele de tip BUS:

- Linear bus - are în componență un singur cablu coaxial
- Distributed bus - are în componență cel puțin două cabluri coaxiale

Topologii – Legacy Ethernet



- Topologie Logică: Bus
- Topologie Fizică: Star
- Bandwidth partajat 10Mb/s
- Conexiune half-duplex
- Cablu UTP

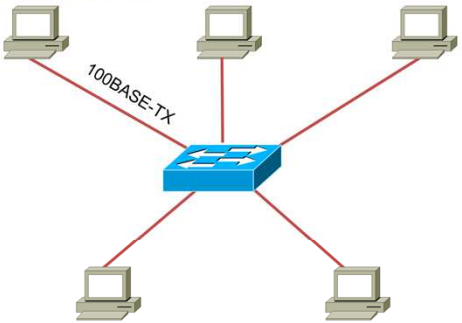
Spre deosebire de topologia de tip “bus”, în cea de tip “star” fiecare stație este conectată la un nod (hub) central, cu o conexiune de tip punct-la-punct.

Topologia de tip “star” nu trebuie să aibă o asemănare cu o stea pentru a fi star, fiecare sistem trebuie să fie conectat la un punct central.

În cazul topologiei de tip star, toate pachetele vor trece prin același punct central înainte de a ajunge la destinație. Dezavantajul unei astfel de topologii poartă de numirea de “single point of failure”. În cazul în care se pierde conectivitatea la echipamentul central, toate echipamentele vor pierde conectivitate.

Avantajul acestei topologii este că se pot adăuga cu ușurință noi noduri în rețea. Cablul folosit de acest tip de topologie este cablul de tip UTP (neecranat) sau de tip STP (ecranat).

Topologii – Switched



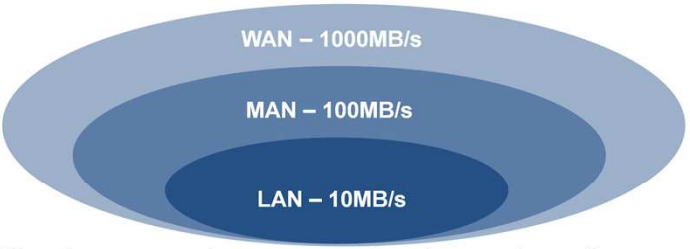
- Topologie Logică: Star
- Topologie Fizică: Star
- Bandwidth dedicat 100Mb/s
- Conexiune full-duplex
- Cablu UTP

Topologia de tip switched respectă aceeasi structură ca topologia de tip star; diferența principală constă în echipamentul central care realizează legătura între stații, în acest caz fiind reprezentat de un switch.

Un mare avantaj adus de un switch îl reprezintă folosirea porturilor de tip full-duplex. Acest tip de legătură nu permite apariția coliziunilor, folosind perechi de cabluri diferite pentru trimiterea și primirea de date.

Un alt avantaj este viteza de transfer. Față de o viteză de 10Mbps, cât suportă un hub, un switch poate transfera informații la viteze de peste 100Mbps. Cel mai mare switch produs de Cisco, CISCO 6500, poate suporta viteze de până la 10Gbps.

Evoluţie



- La ora actuală Ethernet a devenit o tehnologie cheie în orice zonă a reţelei
- S-a impus prin:
  - simplitate
  - cost scăzut de implementare
  - abilitatea de a încorpora uşor tehnologii noi

Datorită fiabilității și a costurilor scăzute de implementare, standardul Ethernet a ajuns să fie folosit și în rețelele de tip Wide Area Network. Principala problemă pe care a întâlnit-o acest standard a fost folosirea sa doar pe medii de transport pe bază de cupru. Odată cu utilizarea standardului Ethernet peste medii de transport optic, vitezele de transfer au crescut semnificativ.

O altă caracteristică la fel de importantă este aceea că standardul Ethernet îmbunătățește metodele Media Access Control, oferind posibilitatea de a funcționa pe diferite medii de transport.

Cadrul Ethernet

7	1	6	6	2	46-1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Type/ Length	Data	FCS

- Standardul IEEE 802.3 defineşte mărimea unui cadru între 64 și 1518 octeți
- Standardul IEEE 802.3ac stabileşte mărimea maximă la 1522 de octeţi

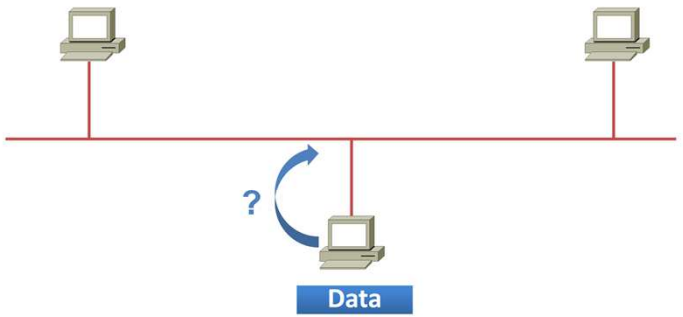
Primul câmp al pachetului este câmpul “Preamble”, cu o lungime de 7 octeți. Acest câmp este necesar stațiilor care primesc pachetul pentru a se sincroniza cu ceasul stației transmițătoare.

Urmează câmpul SFD (*Start Frame Delimiter*), delimitator de început de cadru, care conține biți de non-informație (10101011).

Adresa sursă și destinație sunt folosite pentru trimiterea pachetului, iar cei doi octeți folosiți pentru tip, specifică protocolul de nivel superior. Câmpul “Type/Length” este interpretat ca și lungime a cadrului dacă valoarea sa este mai mică de 1536 (0x600 în hexazecimal). Dacă valoarea sa este mai mare de 1536, el reprezintă protocolul de nivel superior folosit.

Câmpul de date trebuie să fie mai mare de 46 de octeți. Dacă dintr-un motiv sau altul acest câmp are o valoare mai mică se adaugă “padding”, biți de 0. Suma de control, atașată la sfârșitul cadrului, are rolul de a detecta erorile de transmisie.

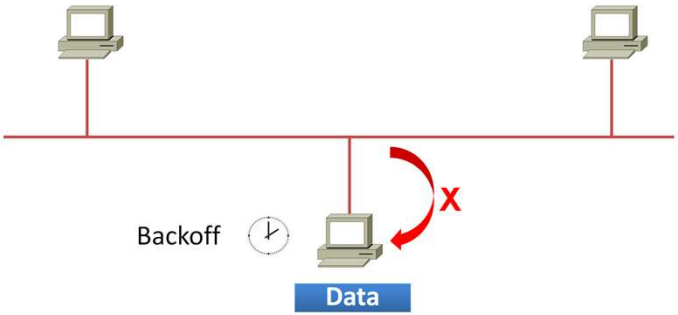
CSMA/CD (1)



- Înainte ca o staţie să transmită informaţii verifică dacă se desfăşoară comunicaţii pe mediul fizic

În toate rețelele în care algoritmul “Carrier Sense Multiple Access with Collision Detection” este utilizat dispozitivele care au de transmis mesaje mai întâi vor asculta mediul de transmisie. Doar în cazul o altă stație nu transmite în același timp, mediul nu este “ocupat”, stația va transmite date.

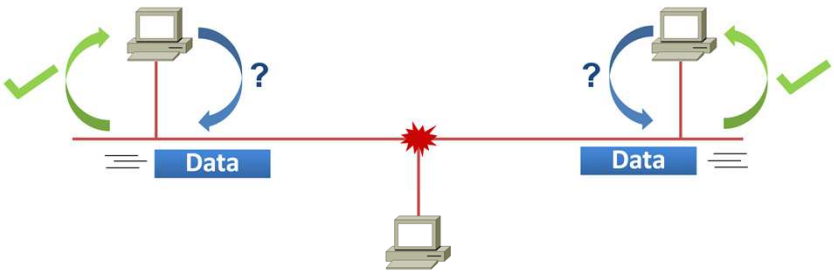
CSMA/CD (2)



- Dacă momentan se desfăşoară o comunicaţie staţia alege o valoare aleatoare - **timp de backoff** cât timp va aştepta până să verifice din nou mediul

Dacă stația detectează un semnal de la o altă stație, ea va aștepta o perioadă de timp până va încerca să transmită din nou. Acest timp de așteptare poartă numele de timp de “back-off”.

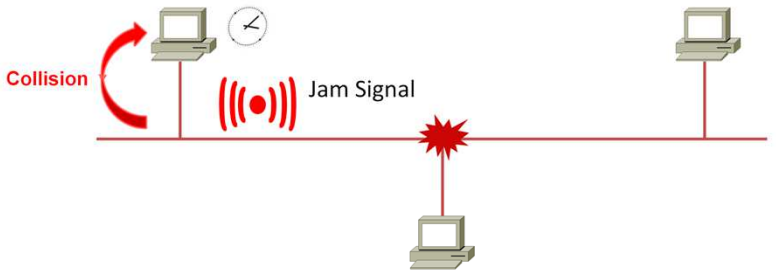
CSMA/CD (3)



- Dacă două staţii interoghează mediul simultan, vor începe să transmită date simultan
- Se va produce o coliziune

Dupa ce o stație a verificat disponibilitatea mediului, ea poate începe să transmita date dacă acesta este “liber”. Dacă două echipamente trimit în același timp are loc o coliziune.

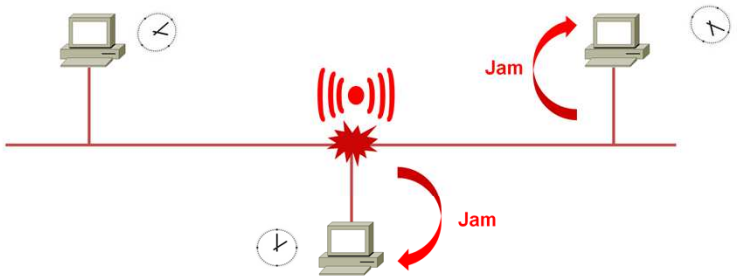
CSMA/CD (4)



- Coliziunea se detectează prin creşterea tensiunii la nivelul mediului fizic partajat
- Staţia implicată în coliziune va începe să transmită prima o secvenţă de 32 de biţi, numită **Jam Signal** şi va porni procedura de backoff

La apariția unei colizuni are loc o creștere a tensiunii semnalului. În acest moment stația care a detectat coliziunea va trimite o secvență de 32 de biți, denumită secvență de bruiaj (“Jam”), urmând ca apoi să fie inițiată procedura de „back-off”.

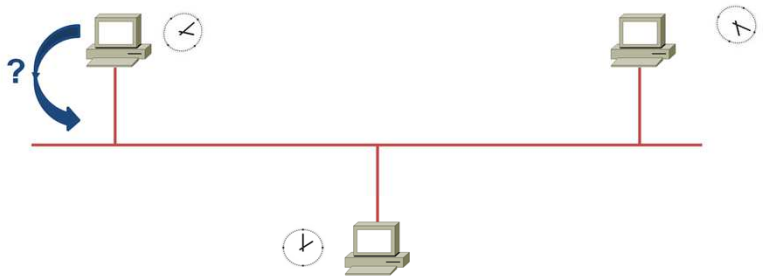
CSMA/CD (5)



- Orice staţie care detectează semnalul de Jam va iniţia algoritmul de backoff
- Semnalul de jam se propagă în tot mediul fizic până când toate staţiile au iniţiat procedura de backoff

Stațiile care au produs coliziunea vor aștepta o perioadă mai mare decât celelalte stații din rețea. Astfel, fiecare dintre echipamentele ce transmiteau în momentul în care a avut loc coliziunea va adăuga la timpul de “back-off” un timp suplimentar generat la întâmplare. Acest comportament va garanta că următoarea stație ce transmite date nu face parte din echipamentele ce au generat o coliziune.

CSMA/CD (6)



- Pentru staţiile care au cauzat coliziunea valoarea intervalului de backoff va fi mai mare
- Dupa expirarea timpului de backoff se va relua procedura de transmisie

După ce acest algoritm este parcurs, se va relua tot procesul la următoarea coliziune.

Ethernet Timing – Bit time

- **Bit time:** intervalul de timp necesar pentru ca un bit să fie emis pe mediul fizic

Bandwidth	Bit time
10 Mbs	100 ns
100Mbs	10 ns
1Gbs	1ns
10Gbs	0.1ns

Calculul bit time-ului se face în funcție de viteza plăcii de rețea (NIC - Network Interface Card) după următoarea formulă:

- $Bit\ time = \frac{1}{viteza\ plăcii\ de\ rețea}$

De exemplu, pentru a calcula bit time-ul unei plăcii de rețea cu o viteză de 10 Mb/s, folosim formula:

- $Bit\ time = \frac{1}{10 \cdot 10^6} = 100\ ns$

Ethernet Timing – Slot time

- **Slot Time:** intervalul de timp necesar pentru ca un impuls electric să parcurgă distanţa maximă într-un mediu fizic
- Dându-se o anumită viteză de transmisie trebuie ca mărimea unui frame să fie mai mare decât un slot time
- Coliziunea trebuie detectată înainte să se termine transmisia frame-ului care a cauzat-o
- Pentru staţiile care au fost implicate în coliziune, la intervalul de backoff se adaugă un slot time

Slot time-ul este de două ori timpul necesar unui impuls electric să parcurgă distanța teoretică maximă între două noduri ale rețelei.

În cazul rețelelor ce folosesc CSMA/CD un dispozitiv așteaptă cel puțin un timp egal cu *slot time*-ul înainte de a pune informații pe mediu.

Din moment ce un impuls nu va depăşi niciodată *slot time*-ul, NIC-ul așteaptă un număr minim de *slot time*-uri înainte de a transmite, cu scopul de a permite semnalului electric să ajungă la destinație. Folosirea acestui principiu ajută la evitarea coliziunilor.

Ethernet Timing – Slot time

- Stabilirea slot time-ului este un trade-off între reducerea timpului de recuperare după o coliziune şi capacitatea de a acomoda reţele mari

Bandwidth	Slot time (bit time)	Interval de timp (µs)
10 Mbs	512	51,2
100Mbs	512	5,12
1Gbs	4096	4096
10Gbs	N/A	N/A

Slot time-ul este folosit doar în rețelele de tip half-duplex. Dat fiind că el definește timpul necesar de recuperare după o coliziune, în rețelele de tip full duplex nu există această noțiune. Deoarece 10 Gbs/s este o tehnologie full duplex, nu putem vorbi de o aplicabilitate a *slot time*-ului.

Ethernet Timing – Interframe spacing

- **Interframe spacing**: intervalul de timp între două frame-uri transmise cu succes
- Este necesar pentru a permite procesarea frame-ului precedent şi pentru stabilizarea mediului fizic

Bandwidth	Interframe Spacing (bit time)	Interval de timp (µs)
10 Mbs	96	9.6
100Mbs	96	0.96
1Gbs	96	0.096
10Gbs	96	0.0096

Moduri de funcţionare

- Ethernet a devenit o tehnologie fundamentală, folosită peste UTP şi Fibră optică
- Cu toate că există o multitudine de standarde se folosesc doar patru moduri de funcţionare
  - 10 Mbs - Legacy Ethernet
  - 100 Mbs - FastEhernet
  - 1000 Mbs - Gigabit Ethernet
  - 10 Gbs - 10 Gigabit Ethernet

Dintre tehnologiile implementate pentru comunicația pe cablu care respectă standardul Ethernet 802.3, putem aminti: 10BASE-T, 100 BASE-TX (cunoscută și sub numele de Fast Ethernet deoarece dezvoltă o lățime de bandă mai mare decât precedenta), 1000BASE-T (cunoscută și sub numele de Gigabit Ethernet), 10BASE-FL, 100BASE-FX, 1000BASE-SX, 1000BASE-LX.

Semnificația reprezentări standardelor este următoarea:

- Numărul din partea stângă a simbolului ilustrează valoarea în Mbps a lățimii de bandă a aplicației
- Termenul BASE ilustrează faptul că transmisia este baseband – întreaga lățime de bandă a cablului este folosită pentru un singur tip de semnal
- Ultimele caractere se referă la tipul cablului utilizat (T-indică un cablu torsadat, F ,L și S indică fibra optică)

Standarde (1)

Tip	Bandwidth	Cablu	Duplex	Distanţă Maximă
10BASE2	10Mbs	Thinnet coaxial	half	200 m
10BASE5	10Mbs	Thicknet coaxial	half	500 m
10BASE-T	10Mbs	Cat3/Cat5 UTP	half	100 m

Avantajele utilizării standardului 10BASE sunt:

- Costuri de instalare mici
- Ușurința în instalare, comparativ cu fibra optică
- Echipamentul și cablurile sunt ușor de schimbat

Iar dezavantajele sunt următoarele:

- Lungimea maximă a unui segment de cablu este de doar 50m
- Cablurile sunt susceptibile la interferențe electromagnetice
- Oferă o lățime de bandă redusă de doar 10 Mbs
- Transmisia este de tip half duplex

Acest standard nu mai este folosit în rețelele actuale.

Standarde (2)

Tip	Bandwidth	Cablu	Duplex	Distanţă Maximă
100BASE -TX	100Mbs	Cat5 UTP	full	100 m
100BASE-FX	100Mbs	Multimode Fiber	full	400 m
100BASE-BX	100Mbs	Singlemode Fiber	full	40 km

Avantajele utilizării unui standard 100BASE sunt:

- Costuri de instalare mici
- Ușurința în instalare, comparativ cu fibra optică
- Echipamentul și cablurile sunt ușor de schimbat
- Oferă o lațime de bandă de 10 ori mai mare față de tehnologiile 10BASE

Iar dezavantajele sunt următoarele:

- Cost mai mare al echipamentelor capabile să suporte tehnologia

Standarde (3)

Tip	Bandwidth	Cablu	Duplex	Distanţă Maximă
1000BASE -T	1000Mbs	Cat6 UTP	full	100 m
1000BASE-SX	1000Mbs	Multimode Fiber	full	550 m
1000BASE-LX	1000Mbs	Singlemode Fiber	full	5 km
1000BASE-ZX	1000Mbs	Singlemode Fiber	full	70km

Avantajele utilizării unui standard 1000BASE sunt:

- Lățimea de bandă de până la 1 Gbps

Iar dezavantajele sunt următoarele:

- În cazul tipului T cablurile sunt susceptibile la interferențe electromagnetice

Standarde (4)

Tip	Bandwidth	Cablu	Duplex	Distanţă Maximă
10GBASE –T	10Gbs	Cat7 UTP	full	100 m
10GBASE-SR	10Gbs	Multimode Fiber	full	300 m
10GBASE-LR	10Gbs	Singlemode Fiber	full	26 km

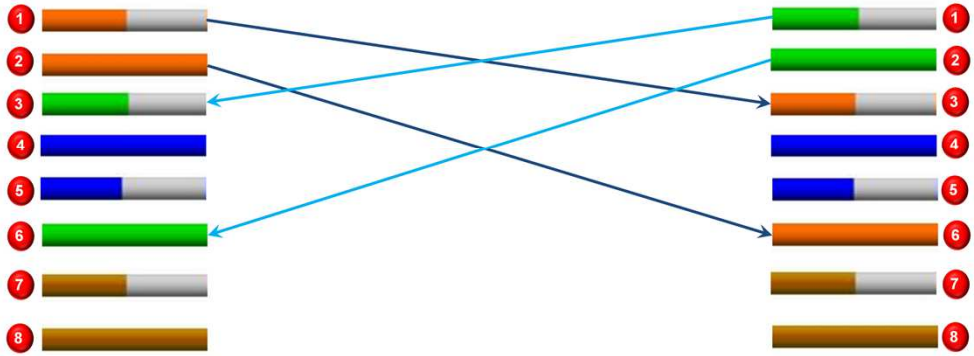
Avantajele utilizării unui standard 10GBASE sunt:

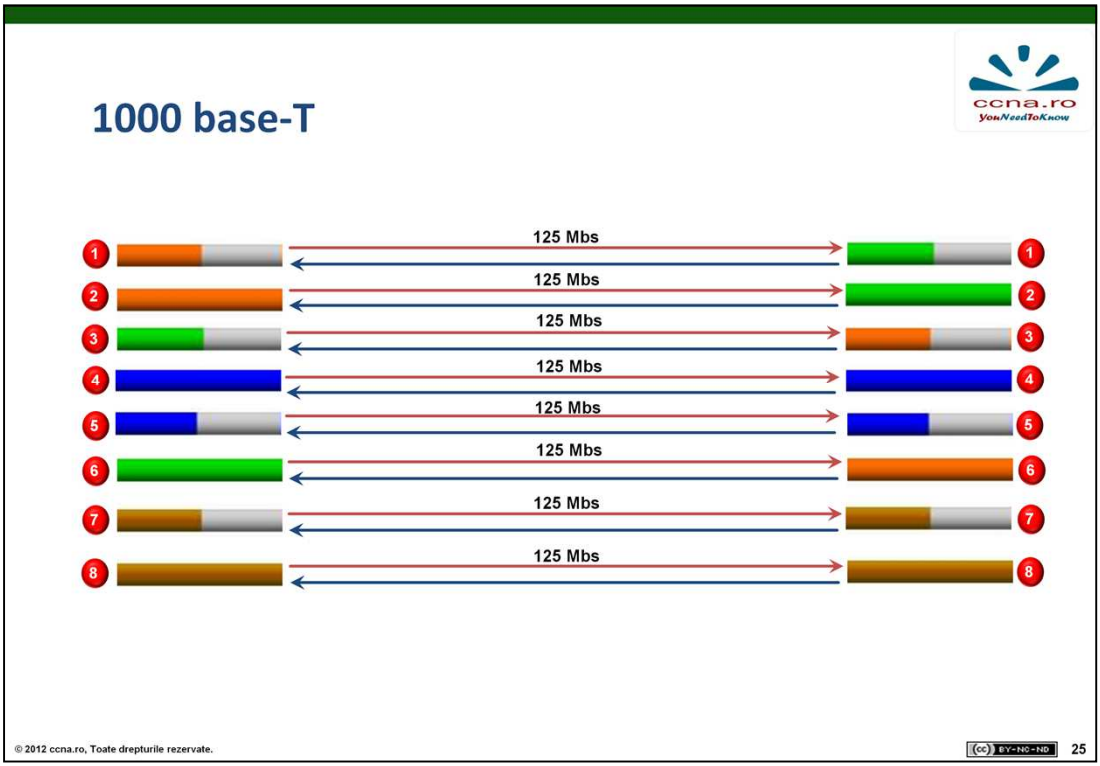
- Lățimea de bandă de până la 10 Gbps

Iar dezavantajele sunt următoarele:

- În cazul tipului T cablurile sunt susceptibile la interferențe electromagnetice
- Cost ridicat pentru placi de rețea și switch
- Necesită echipament suplimentar

100 base-T





Spre deosebire de celelalte standarde (10BASE-T și 100BASE-T), care foloseau în comunicație două perechi, standardul folosit pentru Gigabit Ethernet, 1000BASE-T impune utilizarea a 4 perechi de fire torsadate. Astfel, standardul de Ethernet ales pentru infrastructură specifică numărul de perechi folosite în comunicație și nu standardul de cablu.

Un exemplu de cabluri UTP capabile să suporte standardul Gigabit Ethernet sunt:

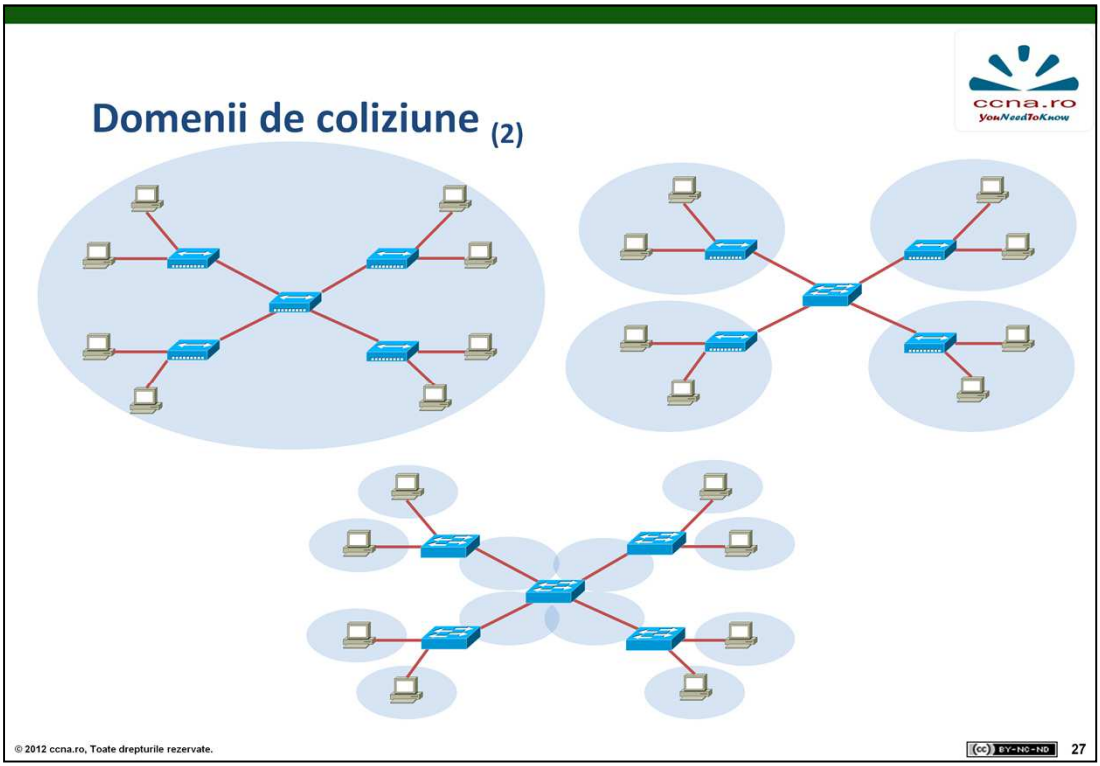
- CAT5e
- CAT6
- CAT6a
- CAT7
- CAT8

Domenii de coliziune (1)

- Reprezintă un set de echipamente care comunică pe un mediul fizic comun
- Comunicaţia în interiorul unui domeniu este half-duplex
- Switchurile şi ruterele segmentează domeniile de coliziune
- Huburile extind domeniul de coliziune

Porțiunea de rețea în care pachetele transmise de către două stații pot genera coliziuni poartă denumirea de “domeniu de coliziune”. Acest fenomen apare în toate cazurile în care mediul de transmisie este partajat între mai multe echipamente. Toate conexiunile care se fac prin intermediul dispozitivelor de nivel 1 fac parte dintr-un domeniu de coliziune.

Despre huburi (repetoare) am spus că sunt dispozitivele care regenerează traficul unei reţele fără însă a filtra în vreun fel informaţiile pe care le recepţionează/transmit. Informaţiile primite de un port al unui hub sunt transmise tuturor celorlalte porturi. Prin urmare folosirea acestor dispozitive conduce la extinderea unui domeniu de coliziune. Spre deosebire de hub-uri, switch-urile și ruterele segmentează domeniile de coliziune.



În exemplul de mai sus este evidențiat pe o topologie fizică modul cum se comportă un hub din punct de vedere al domeniilor de coliziune. Astfel, se poate observa că există doar un singur domeniu de coliziune.

În momentul în care un hub este înlocuit cu switch, are loc o segmentare a domeniilor de coliziune, acest lucru realizând o creștere a performanței rețelei.

Modelul Switched

- Pe lângă segmentarea domeniilor de coliziune se oferă și alte beneficii
- Bandwidth dedicat pentru fiecare echipament conectat la switch
- Fiecare staţie conectată la switch beneficiază de un mediu full-duplex

Fiecare nod beneficiază de aceeași lățime de bandă pe legătura dintre nod și switch. Dat fiind faptul că hub-urile trimit informația primită pe toate porturile, mai puțin pe cel de pe care a primit-o, face ca dispozitivele legate prin acest echipament să partajeze același lățime de bandă.

Conexiunea punct-la-punct pe care o determină conectarea prin intermediul unui switch aduce cu sine un mediu full-duplex, deci coliziunile sunt eliminate.

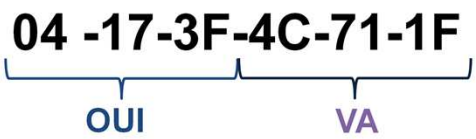
Adresa MAC

- Este un model de adresare plată
- Se mai numeşte BIA (burnt-in address) deoarece este encodată la nivel hardware şi nu poate fi schimbată
- Adresele MAC trebuie să respecte condiţia de unicitate doar în cadrul unui domeniu de broadcast
- Se reprezintă folosind 6 cifre hexazecimale

Adresa Media Access Control (MAC), cunoscută și sub numele de adresă hardware sau adresă fizică, este un identificator unic asignat plăcilor de rețea de către producători. Ea este reprezentată pe 48 de biți, însă în practică este o secvență numerică formată din 6 grupuri de câte 2 cifre hexazecimale (în baza 16) de tipul: 00:11:22:33:44:55.

Pe baza acestei adrese se realizează adresarea fizică. Adresa MAC identifică unic o stație într-o rețea locală. Adresele MAC pot fi modificate la nivel de sistem de operare, recomadat este să se folosească adresa inscripționată pe placa de rețea, adresă denumită BIA (Burn-In-Address).

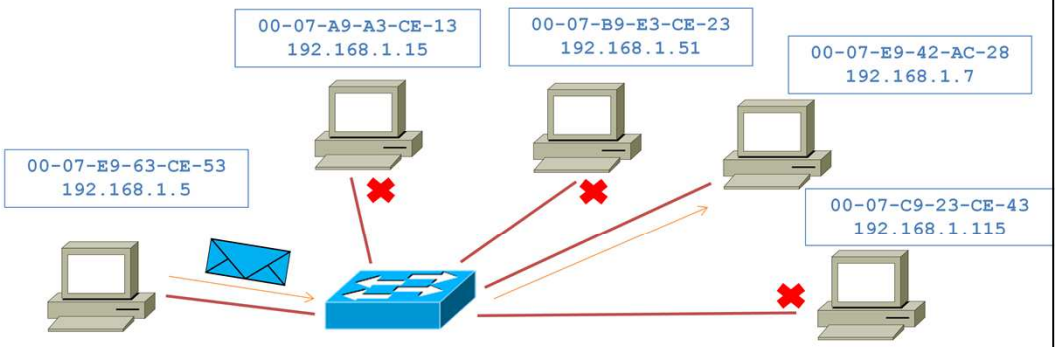
Structura MAC



- **OUI** (Organizational Unique Identifier) – este un număr specific fiecărui producător de NIC-uri
- **VA** (Vendor Assigned) – este generat automat de fiecare producător

După cum s-a specificat anterior adresa MAC este reprezentată pe 48 de biți dintre care 24 (în acest caz 04-17-3F) identifică întotdeauna producătorul plăcii de reţea (RealTek, Cisco, SUN Microsystems etc.), iar următorii 24 de biți identifică dispozitivul în sine și sunt denumiți VA (vendor assigned).

Modele de Comunicare - Unicast



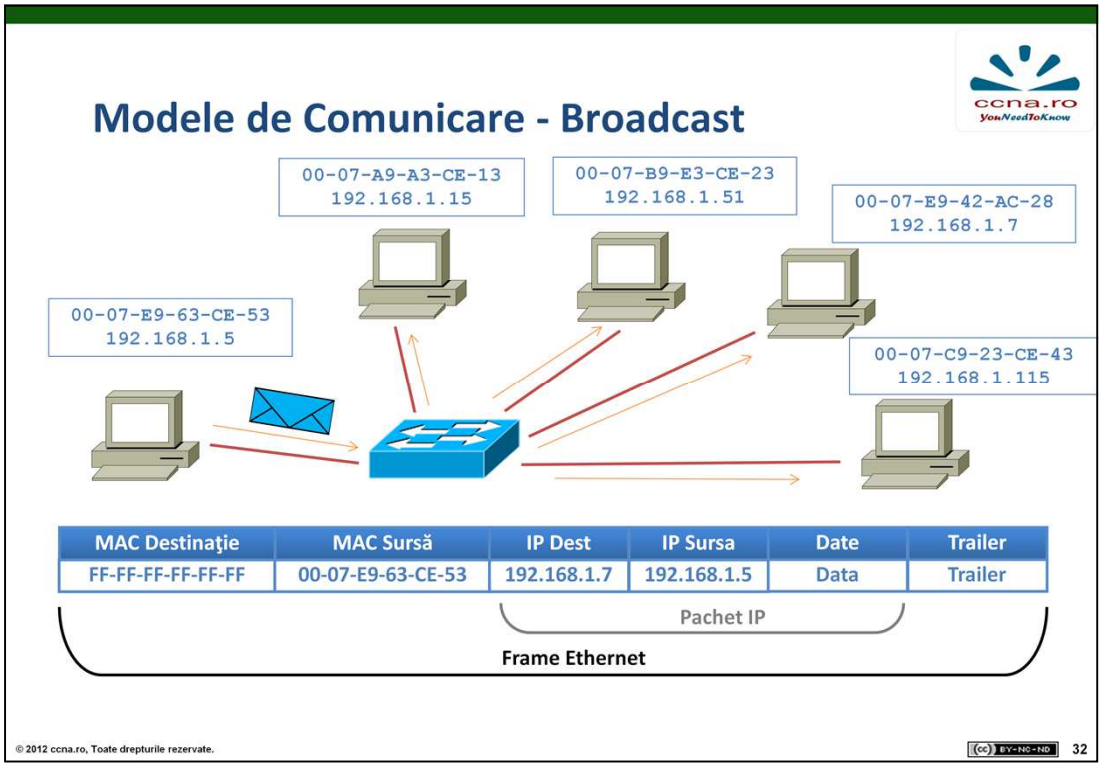
MAC Destinaţie	MAC Sursă	IP Dest	IP Sursa	Date	Trailer
00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.7	192.168.1.5	Data	Trailer

Pachet IP

Frame Ethernet

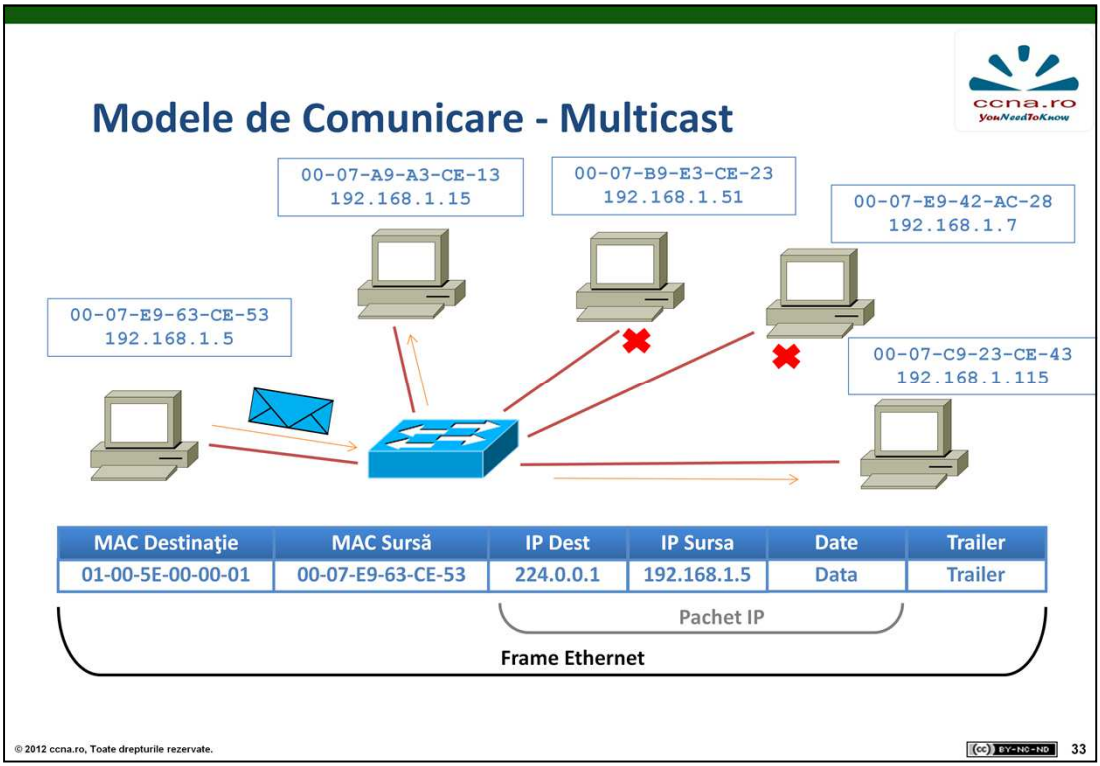
Adresa MAC de tip unicast identifică o destinație unică existentă într-o rețea locală. În această situație informațiile sunt transmise de către o sursă către o singură destinație, atât adresa sursă cât și destinație fiind de tip unicast.

Adresa de nivel 2 de tip unicast poate avea orice formă, diferită de cea de broadcast și multicast. Componența adreselor specificate anterior vor fi descrise în slide-urile următoare.



Adresa MAC de tip broadcast identifică toate destinațiile existente într-o rețea locală. În această situație informațiile sunt transmise de către o sursă către toate destinațiile, adresa sursă fiind de tip unicast, iar adresa destinație de tip broadcast.

Adresa de nivel 2 de tip brodcast este în format binar, fiind alcătuită din 48 de biți de 1, iar în hexazecimal este de forma: FF-FF-FF-FF-FF-FF.



Adresa fizică de tip multicast identifică un grup de echipamente. În acest caz avem o sursă ce trimite mesaje mai multor echipamente din aceeași rețea cu ea. Adresa sursă este de tip unicast, pe când adresa destinație este de multicast. Identificarea unei adrese de tip multicast se face știind că ultimul bit al primului octet este 1, un exemplu ar putea fi: 01-00-0C-00-02-03.

Funcţionarea switchurilor

- Swithurile efectuează 5 operaţii fundamentale:
  - forwarding:
  - flooding
  - learning
  - aging
  - forwarding selectiv

Semnificaţia operaţiilor este următoarea:

- Forwarding - switch-urile fac asocieri de tipul MAC-port pe baza adresei sursă şi le memorează în tabela CAM (Contenet Addressable Memory)
- Flooding - dacă un switch nu recunoaşte destinaţia transmite cadrul pe toate porturile
- Learning - tabela CAM se populează dinamic pe baza adreselor sursă din cadru
- Aging - fiecare intrare dinamică are asociat un timer

  - dacă timer-ul expiră înainte să mai fie înregistrat trafic pentru MAC-ul respectiv, intrarea aferentă este ştearsă
- Forwarding Selectiv - dacă deţine intrarea în tabela CAM , switch-ul va replica cadrul doar pe portul aferent

CCNP Preview: MAC-address filtering

- Există diverse metode de filtrare pentru adresa MAC la nivel de switchuri:
  - asocierea unui port cu o singură adresă MAC, astfel încât o altă adresă MAC să nu poată folosi acel port
  - filtrarea accesului pe un port pentru o anumită adresă MAC sursă/destinație
  - filtrarea accesului pe un VLAN pentru o anumită adresă MAC sursă/destinație

Una dintre problemele cele mai mari ale unei rețele interne este securitatea. Varianta optimă într-o rețea bazată pe “switching” este limitarea clienților care se pot conecta la infrastructură, pornind de la datele de identificare ale stației de lucru. Soluția cea mai simplă este de a configura un switch să accepte pachete de date doar dacă provin de la un anumit grup de adrese MAC.

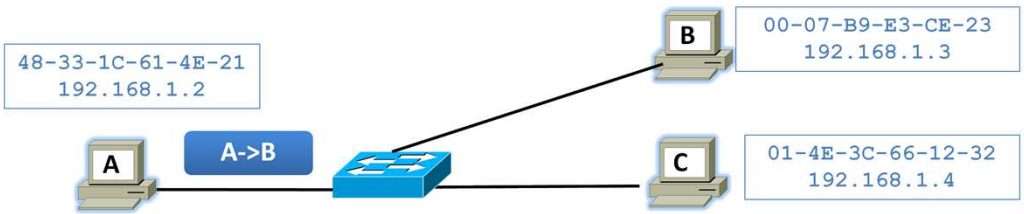
Un exemplu de astfel de soluție este conceptul de “port security”, care oferă posibilitatea de configurare a echipamentului astfel încât să filtreze adresele MAC statice sau învățate dinamic.

Address Resolution Protocol

- Pentru a comunica într-un mediu Ethernet este nevoie atât de adresa destinaţie IP cât şi cea MAC
- Fiecare entitate care comunică pe reţea are o tabelă cu asocieri MAC-IP
- Nu scalează bine ca această tabelă să fie extensivă
- Este mai eficient să se poată afla adresa MAC a destinaţiei în momentul când trebuie transmise date
- Protocolul ARP asigură următoarele funcţii:
  - rezolvarea adreselor IPv4 în adrese MAC
  - menţinerea mapărilor în cache

Comunicarea dintre două dispozitive într-o rețea presupune ca dispozitivul care transmite să cunoască atât adresa MAC, cât şi adresa IP a dispozitivului destinaţie. În cele mai multe cazuri, echipamentul sursă cunoaște adresa IP a destinației, pe baza acesteia dorește să identifice adresa MAC. În această situație protocolul ARP este soluția. Acest protocol ajută la obținerea automată a adresei MAC pentru o staţie cu un adresa IP cunoscut. Fiecare staţie va ţine o tabelă cu toate adresele IP şi MAC ale calculatoarelor din aceeaşi reţea locală, aceste tabele se numesc tabele ARP. Spre deosebire de stații, un ruter ține câte o tabelă ARP pentru fiecare interfață activă. Aceste mapări sunt memorate în memoria RAM a dispozitivului, fapt pentru care la restartare se vor pierde.

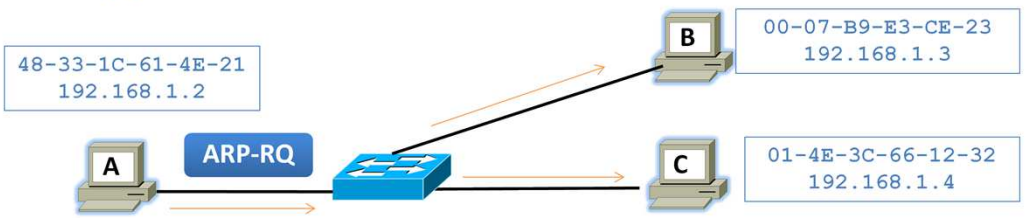
ARP (1)



MAC Destinaţie	MAC Sursă	IP Dest	IP Sursa
??-??-??-??-??-??	48-33-1C-61-4E-21	192.168.1.3	192.168.1.2

În momentul în care o sursă află adresa IP a destinației cu care doreşte să comunice, va căuta adresa de MAC a acestuia în tabela ARP proprie. Dacă nu poate găsi adresa în această tabelă, staţia va iniţia o procedură numită cerere ARP.

ARP (2)

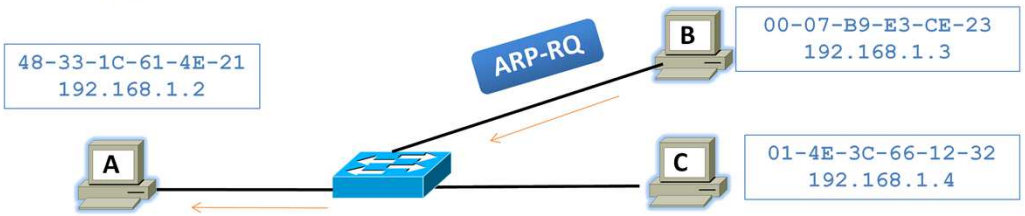


MAC Destinaţie	MAC Sursă	Date	Trailer
FF-FF-FF-FF-FF-FF	48-33-1C-61-4E-21	ARP Request	Trailer

Un pachet de tip “ARP-Request” se foloseşte pentru a afla adresa MAC pentru o anumită adresă IP. Acest pachet va conţine adresa MAC destinaţie adresa de broadcast, FF-FF-FF-FF-FF-FF. Cea mai importantă informaţie din câmpul de date este adresa IP pentru care se solicită adresa MAC. Echipamentul se va identifica punând în cadrul câmpului “MAC Sursă”, adresa MAC proprie.

Dat fiind că pachetul a fost trimis pe adresa de broadcast, toate staţiile din reţeaua locală îl vor primi şi îl vor trimite nivelului reţea pentru a fi analizat.

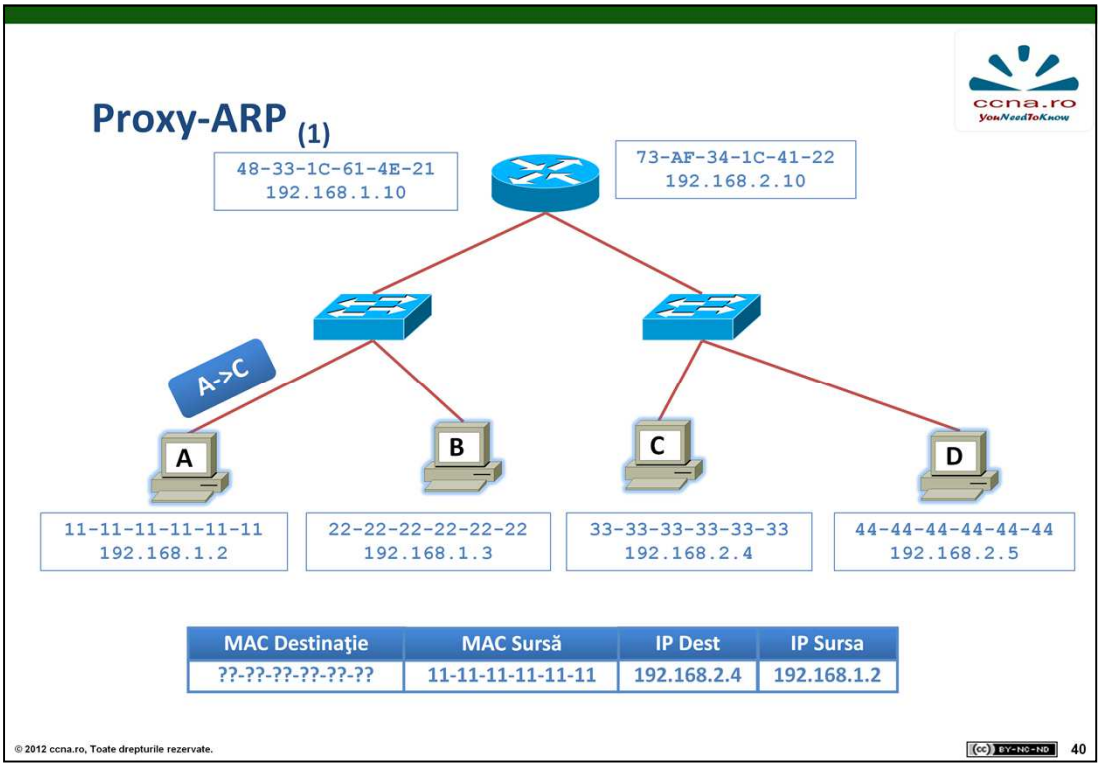
ARP (3)



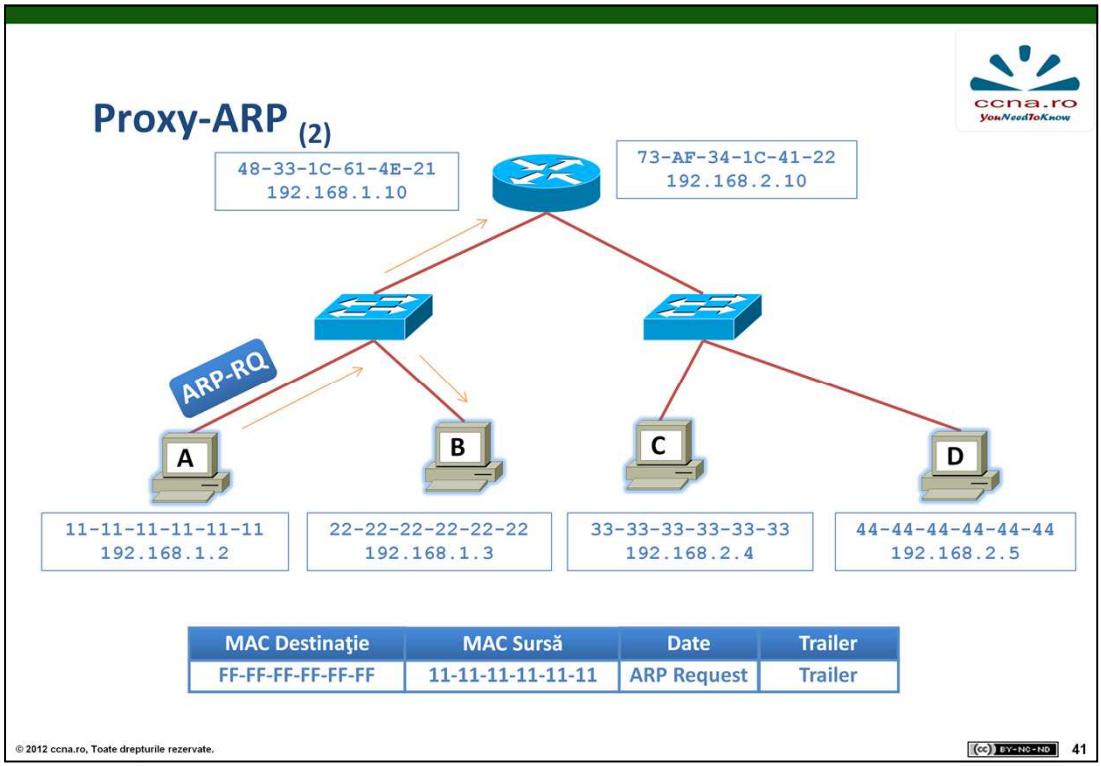
MAC Destinaţie	MAC Sursă	Date	Trailer
48-33-1C-61-4E-21	00-07-B9-E3-CE-23	ARP Reply	Trailer

Dacă adresa IP a dispozitivului corespunde adresei destinaţie din pachet, dispozitivul va răspunde. În momentul în care dispozitivul a luat decizia că este destinatarul pachetului, va pregăti un pachet de răspuns ARP. Acest pachet va avea ca adresă IP destinaţie adresa IP a staţiei care a iniţiat cererea ARP, iar adresa IP sursă va fi egală cu adresa IP pentru care se dorea găsirea adresei MAC corespunzătoare, deci cea a staţiei care trimite pachetul de răspuns ARP. Frame-ul care încapsulează acest pachet va fi adresat către adresa MAC a dispozitivului care a făcut cererea ARP , iar ca adresă MAC sursă va fi utilizată adresa MAC a staţiei care răspunde.

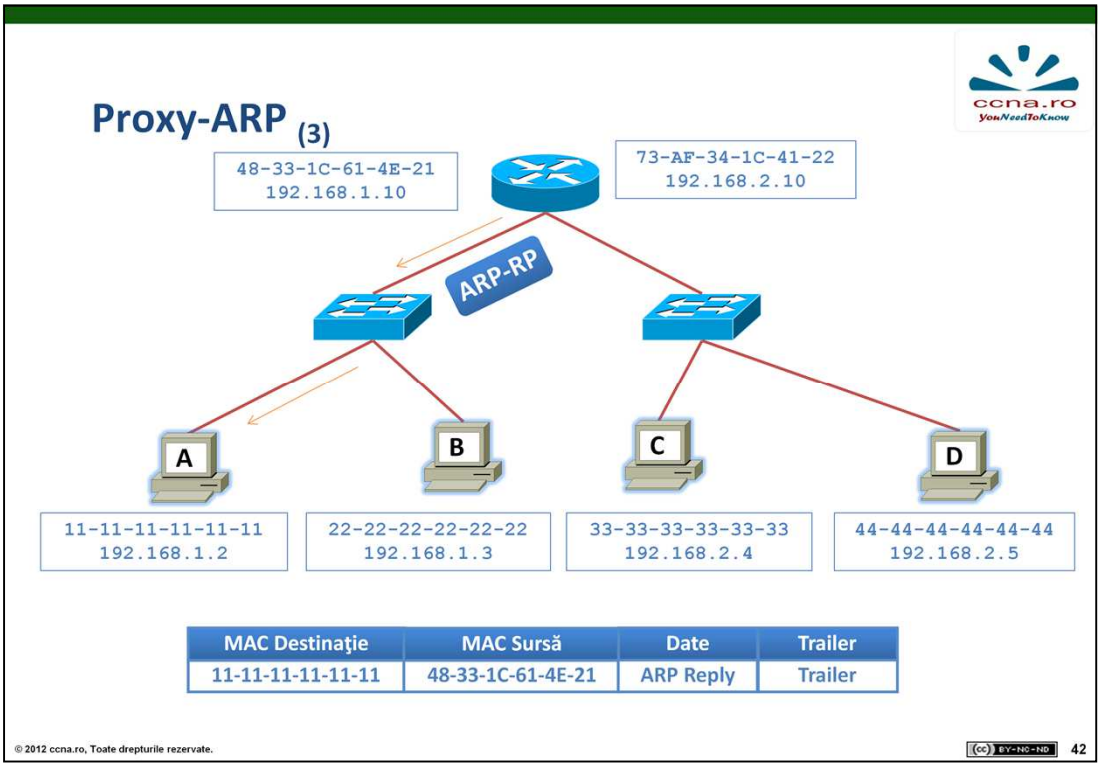
În cazul unei neconcordanțe a adreselor IP, dispozitivul va ignora pachetul.



Protocolul Proxy-ARP a apărut ca o necesitate pentru asigurarea conectivității atunci când în rețeaua locală nu se folosește un "default gateway". Deși aceste cazuri sunt rar întâlnite, astăzi protocoul Proxy-ARP joacă un rol important în rutarea statică. Acest protocol se bazează pe faptul că o cerere de tip ARP-Request este trimisă la o adresă de broadcast și nu există un mecanism de verificare a unui răspuns. Un ruter care rulează proxy-arp va răspunde la pachete de tip ARP-Request ce au ca destinație o adresă IP aflată în altă rețea decât cea pe care a fost primit pachetul. În acest mod un ruter poate "extinde" o rețea locală, jucând rolul unui "default gateway" pentru nivelul 2 din stiva OSI.



Stația A trimite o cerere ARP cu adresa de nivel 2 destinație de tip broadcast, astfel toate dispozitivele din rețea inclusiv ruterul vor primii și procesa cererea.

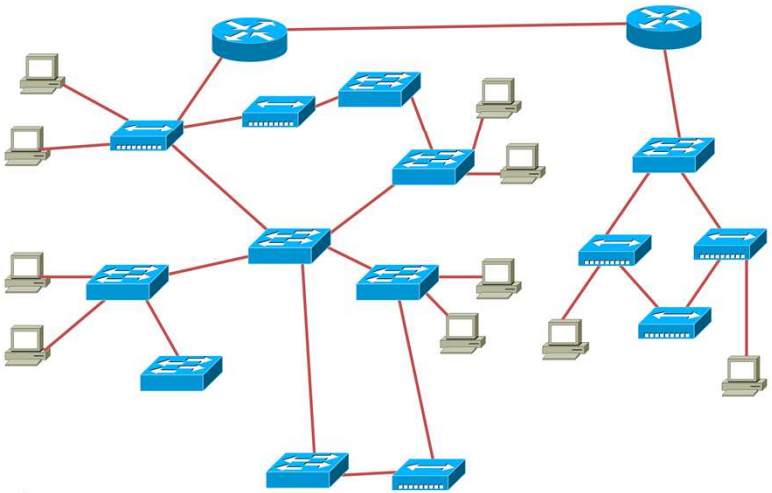


Dat fiind faptul că adresa IP a destinației este dintr-o altă rețea, stațiile situate în rețea cu A vor ignora pachetul. În această situație este imposibil ca cele doua stații să poată comunica, soluția este dată de activarea protocolului Proxy-ARP pe ruter. Proxy-ARP-ul determină ruterul să caute în tabela de rutare informații despre adresa IP pentru care s-a făcut cererea ARP.

Dacă ruterul are în tabela de rutare, rețeaua din care face parte stația C va pregăti un pachet de răspuns ARP, asemănător cu cel descris anterior, singura diferență fiind adresa MAC destinație care va fi adresa MAC a interfeței ruterului de pe care a primit cererea ARP.

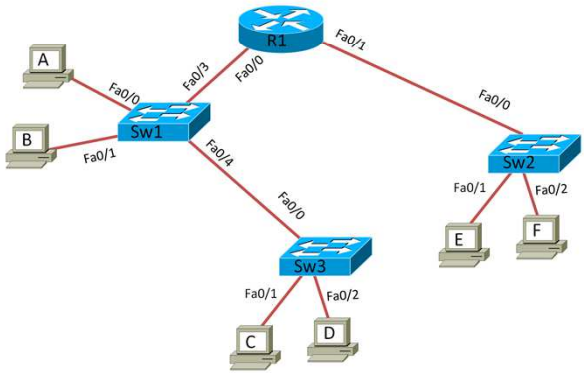
Întrebări

- Identificaţi numărul de domenii de broadcast şi numărul de domenii de coliziune din reţeaua următoare



Întrebări

- Se dă topologia următoare. Cum arată tabela MAC a Sw1 după următoarele schimburi de pachete:
  - A-B
  - A-C
  - C-B
  - D-A
  - A-F
  - E-R1



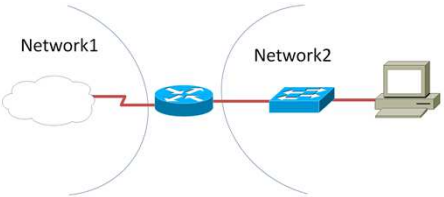
Capitolul 9:
Cablare și proiectarea rețelelor

Obiective

- Echipamente de rețea: alegere și considerente
- Cablare și conexiuni LAN / WAN
- Adresarea echipamentelor

Dispozitive de rețea (1)

- Ruter
  - interconectează ***rețele*** (WAN și LAN)
  - limitează domeniile de coliziune și de broadcast
  - determină calea la nivel 3



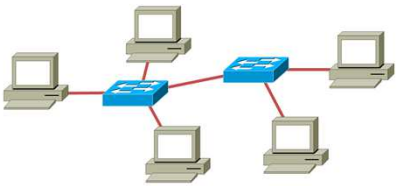
Un ruter este un dispozitiv care conectează două sau mai multe rețele fie ele LAN-uri sau WAN-uri.

La începutul perioadei utilizării rutării (de la mijlocul anilor ‘70 până la mijlocul anilor ‘80), pe post de rutere erau folosite minicalculatoare. Chiar dacă calculatoarele obișnuite pot fi folosite ca rutere, dispozitivele moderne sunt dispozitive extrem de specializate, de multe ori cu hardware dedicat construit să accelereze atât funcțiile de bază (comutarea pachetelor) cât și funcțiile speciale (de exemplu criptarea datelor).

Deși sistemul de operare pentru rutere de la Cisco (numit IOS) a fost creat de la 0 special pentru dispozitive de rețea, alte sisteme de operare pentru rutere, precum cele de la Juniper și Extreme Networks sunt variante extrem de modificate de Unix. Pentru cercetare și alte aplicații sunt folosite în continuare rutere făcute din calculatoare cu Linux și Unix.

Dispozitive de rețea (2)

- Switch
  - limitează domeniile de coliziune
  - extinde domeniile de broadcast
  - ia decizii la nivel 2, în funcție de adresele MAC



Un switch este un dispozitiv care realizează conexiunea diferitelor segmente de rețea pe baza adreselor MAC. În cadrul unei rețele switch-ul are drept scop eliminarea coliziunilor și determinarea unei căi între sursă și destinație.

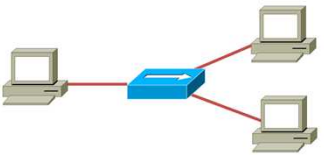
Clasificarea switch-urilor se poate face pe baza a două criterii:

- După formă: montabile în rack-uri și nemontabile
- După posibilitatea de configurare: neconfigurabile și configurabile

Switch-urile neconfigurabile nu posedă interfață de configurare și se regăsesc uzual în mediile SOHO (Small office/Home office), iar cele configurabile, în rețele de dimensiuni medii/mari. Sarcina de configurare necesită de obicei înțelegerea nivelului 2 (Legătura de Date) al rețelelor.

Dispozitive de rețea (3)

- Hub
  - extinde domeniile de coliziune și de broadcast
  - regenerează semnalul
  - nu foloseşte adresare

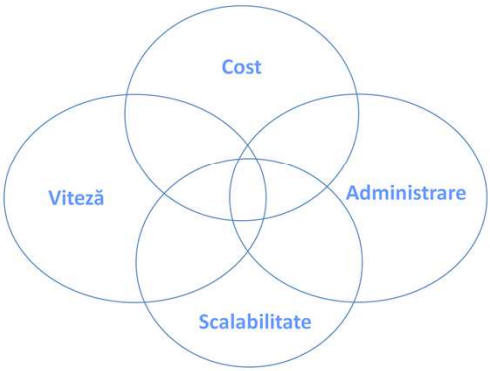


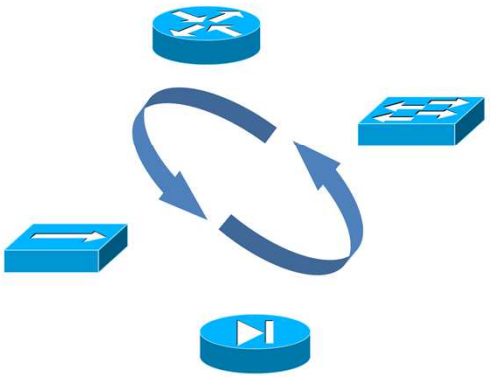
Un hub de rețea este un dispozitiv pentru conectarea altor dispozitive fie prin cablu răsucit (de tip twisted pair), fie prin cablu de fibră optică; legătura permite ca rețeaua să se comporte ca un singur segment. Hub-urile funcționează la nivelul 1 fiind responsabile și pentru retransmiterea semnalului spre toate porturile sale.

Deseori hub-urile dispun de conectoare de tip BNC (conector pentru cablu coaxial) și/sau AUI (conector pentru cablu serial), pentru a permite conectarea la astfel de segmente de rețele de tipul 10BASE2 și 10BASE5 (rețele dezvoltate pe cablu coaxial).

Apariția switch-urilor a înlocuit practic pe piață hub-urile, dar ele mai sunt întâlnite la conexiuni mai vechi și în aplicații speciale.

Alegerea echipamentelor





În funcție de gradul de securitate, gradul de utilizare și viteza rețelei locale echipamentele sunt alese astfel:

- În cazul în care care nu se dorește o filtrare a pachetelor la nivel hardware se poate alege un ruter
- Dacă în rețea se dorește împărțirea pe departamente se poate alege un switch de nivel 3, care are ca facilitate rutarea pachetelor

În general alegerea echipamentelor se realizează după ce design-ul a fost construit, și accentul este pus pe securitatea informațiilor. Dar în cele mai multe cazuri este recomandată o implementare care să cuprindă atât echipamente de nivel 2 cât și de nivel 3 pentru diminuarea costurilor și sporirea securității.

Alegerea echipamentelor: Switch (1)

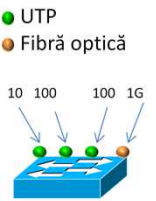
În cadrul rețelelor actuale, switch-urile sunt bazate pe protocolul Ethernet și suportă fie 10MB, 100MB și 1000MB, însă ultima generație de switch-uri poate suporta până la 10 GB/s.

Switch-urile se pot conecta și în rețele ce suportă Fiberchannel, ATM sau Wireless. Legătura prin aceste echipamente se poate face fie la nivelul 2, fie la nivele superioare, această ultimă proprietate determinând apariția unor switch-uri „multilayer”.

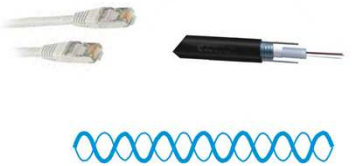
Pe lângă aceste caracteristici cel mai important factor în procesul de alegere a unui switch este determinat de existența sau inexistența unei posibilități de management, astfel deosebindu-se echipamentele SOHO de cele profesionale.

Alegerea echipamentelor: Switch (2)

- Alegerea switch-urilor
  - capacitate
    - numărul de porturi
    - viteză
  - caracteristici speciale
    - capacitate back-plane
    - medii de transmisie suportate
    - PoE(Power over Ethernet)
    - arhitectură modulară



Doua tipuri, viteze diferite



Managementul este o altă caracteristică de selecție, el fiind dependent direct de sistemul de operare și serviciile pe care un switch le oferă, dintre care amintim:

- VLAN – posibilitatea de a împarți o rețea fizică în mai multe subrețele logice
- Static MAC Forwarding – stabilirea unei adrese MAC ce poate accesa un anumit port
- Spanning Tree Protocol – asigură redundanța, prevenind buclele de nivel 2
- Link Aggregation – presupune gruparea unor porturi fizice într-unul logic de capacitate mai mare
- Port Security – permite doar pachetelor cu adresa MAC învațată dinamic și/sau adresa MAC statică configurată să treacă prin switch.

Alegerea echipamentelor: Ruter (1)

Ruterele sunt echipamentele indispensabile din cadrul unei rețele. În funcție de domeniul în care sunt utilizate ele pot fi împărțite în 3 categorii: individuale, pentru companii și pentru rețele de telecomunicații (ruterele folosite de ISP-uri).

Ruterele individuale sunt folosite pentru conectarea reședințelor individuale și a firmelor mici la serviciile de Internet prin cablu sau la rețelele de cartier.

Ruterele pentru companii se împart în trei subnivele:

- Rutere de nivel acces - oferă lățime de bandă divizată între utilizatori și filtrare la nivelul 2 al stivei OSI
- Rutere de nivel distribuție - agregă traficul de la mai multe rutere de acces, către nodul central al rețelei companiei
- Rutere de core - trebuie să asigure rutarea cu cea mai mare viteză a pachetelor, realizând legătura cu exteriorul

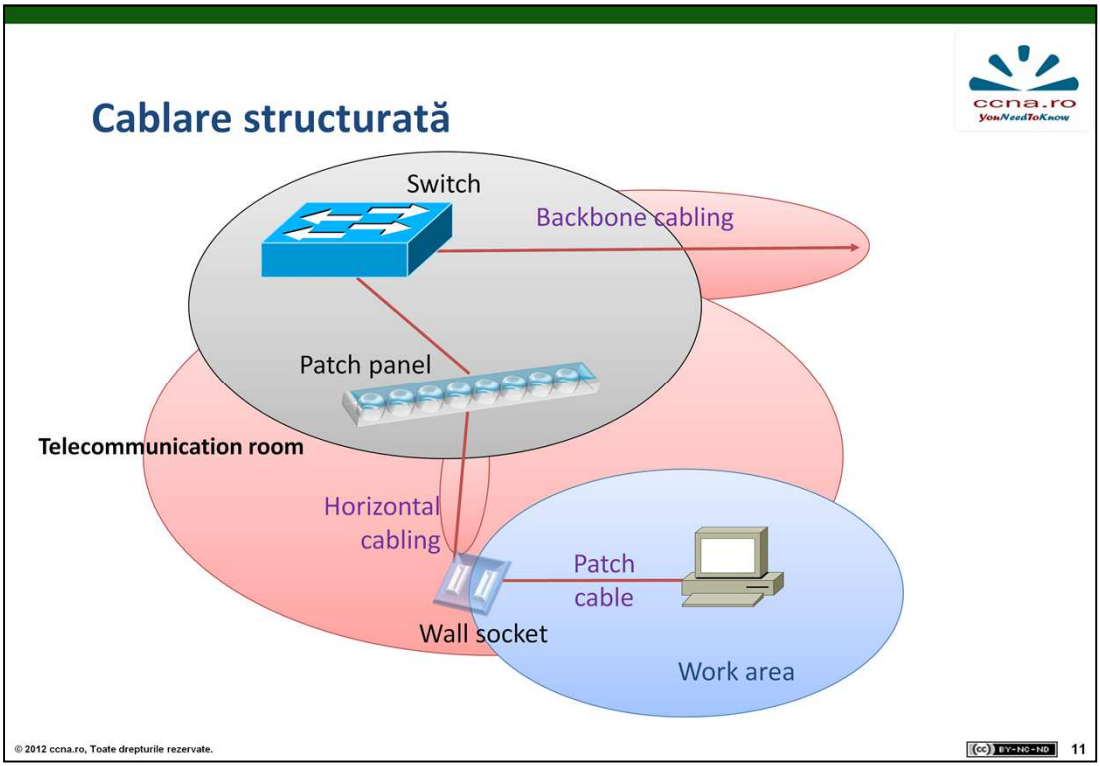
Alegerea echipamentelor: Ruter (2)

- Alegerea ruterelor
  - tipuri de interfețe
  - extensibilitate
    - capacitate backplane
    - arhitectură modulară (WIC, HWIC, NME)
  - caracteristici IOS:
    - securitate (firewall, VPN, inspecția traficului)
    - servicii integrate (firewall, Network Address Translation(NAT), Dynamic Host Configuration Protocol (DHCP), telefonie analogică, ISDN, telefonie IP)
    - Quality of Service
    - protocoale de rutare suportate (RIP, RIPng, EIGRP, EIGRP for IPv6, OSPFv2, OSPFv3, BGP, BGP for IPv6, etc.)

În momentul în care se dorește alegerea unui ruter CISCO, există numeroase caracteristici ce pot ajuta la alegerea celei mai bune soluții pentru compania pe care o reprezentați. O primă caracteristică este performanță exprimată prin numărul de pachete transmise pe secundă. Ca exemplu un ruter 2610 trimite aproximativ 15000 de pachete pe secundă, pe când unul 7500 poate transmite peste 2 milioane de pachete pe secundă.

Posibilitatea de upgrade este un alt factor ce diferențiază modelele, referindu-se în principal la memoria RAM și Flash. Expandabilitatea aduce în prin plan o altă diferențiere a echipamentelor în funcție capacitatea și numărul de interfețe pe care le poate suporta un ruter.

După o analiză hardware este recomandată o evaluare software pentru a putea decide dacă echipamentul corespunde cerințelor necesare. Caracteristicile software sunt evidențiate mai sus.



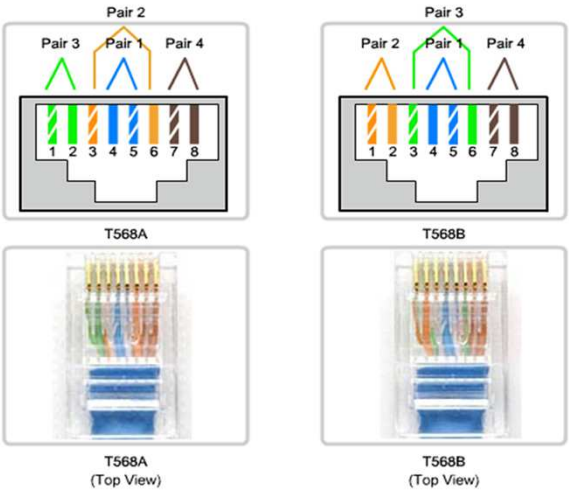
Cablarea structurată reprezintă un set de standarde ce determină modalitatea de instalare a cablurilor ce intră în componența rețelelor de date sau voce din centre de date, birouri sau clădiri.

Aceste standarde determină modul de cablare în formație „stea”: prizele de date sunt conectate la un patch panel central de unde se determină modul în care vor fi utilizate aceste conexiuni.

Cablarea structurată este alcătuită din următoarele subsisteme: instalaţia de intrare, dulapul de telecomunicaţii (conţine echipamentele), backbone-ul (transportă semnalul între componentele definte anterior), cablarea orizontală (cablurile de la camerele de telecomunicaţii la prizele individuale) și componentele zonei de lucru (conectează echipamentul utilizatorului la prizele subsistemului de cablare orizontală).

Conexiuni LAN folosind cabluri UTP

- Standarde
  - mufa RJ-45
  - EIA-TIA T568A / T568B
  - MDI / MDIX
- Tipuri
  - straight-through
  - crossover
  - rollover



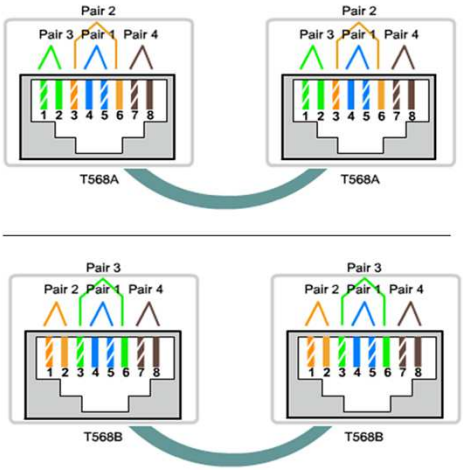
Standardul 802.3 cuprinde protocoalele ce definesc nivelul fizic și subnivelul MAC al nivelului legătură de date. Procedura de fixare a firelor într-un conector se numește sertizare. Standardul TIA/EIA 568 A/B specifică modul în care pot fi ordonate firele la o terminație a cablului.

Pentru a putea fi identificate ușor cele opt fire sunt grupate în patru perechi colorate diferit. Astfel tehnologiile 100BaseTX și 10BaseT folosesc doar două perechi din cele patru: una pentru transmisie și una pentru recepție. Conform standardelor de mai sus, aceste tehnologii pot folosi doar perechile verde și portocaliu.

În funcție de corespondența perechilor dintr-un capăt cu pinii de la celălalt capăt, cablurile se împart în trei categorii: crossover, straight-through și rollover.

Straight-through (1)

- Ambele capete sunt mufate folosind același standard



Cablul straight-through are ambele capete conform aparținând aceluiași standard (T568-T568 în SUA sau T568B-T568B în Europa). Se folosește atunci când se conectează echipamente de tipuri diferite.

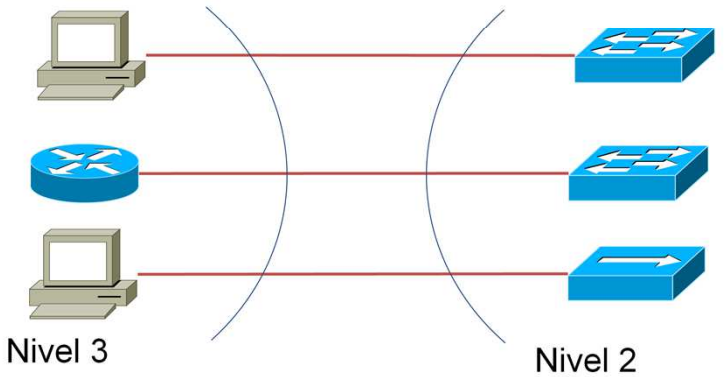
Cele două capete având aceeași ordine a firelor, fiecare pin al conectorului dintr-un capăt comunică direct cu pin-ul corespunzător al conectorului de la celălalt capăt al cablului.

Dacă nu se folosește tipul corect de cablu comunicația nu poate să aibă loc.

Referința la un cablu straight-through este relevantă doar pentru tehnologiile ce folosesc ca mediu de transmisie cablul UTP.

Straight-through (2)

- Ambele capete sunt mufate folosind același standard
- Folosit între echipamente care operează la niveluri diferite din stiva OSI



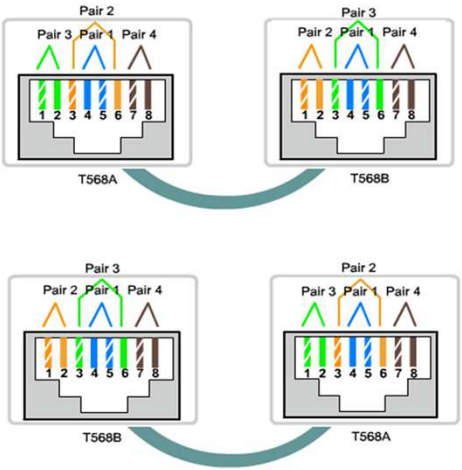
Echipamentele ce pot fi conectate folosind un cablu UTP de tip straight-through sunt:

- Dispozitiv terminal - switch
- Ruter - switch
- Dispozitiv terminal - hub

Categoria dispozitivelor terminale este reprezentată de orice echipament cu care utilizatorul are contact direct (calculator, laptop, imprimantă, pda, smartphone, IP phone, tabletă, smart TV, playstation, etc). Deși de managementul unui server se ocupă un administrator de rețea, acesta intră tot în aceași categorie a echipamentelor terminale.

Crossover (1)

- Capetele sunt mufate folosind standarde diferite



Cablul crossover se foloseşte pentru conectarea a două echipamente capabile să interpreteze până la același nivel al stivei OSI informația, excepție fiind legătura directă dintre un ruter și un calculator. Prin modul în care este construit acest cablu două echipamente de același tip pot transfera date între ele fără a mai trece printr-un alt echipament, dacă placile lor de rețea sunt conectate printr-un cablu crossover.

Pentru standardele 10BASE-T sau 100BASE-T se inversează cele două perechi (portocaliu și verde), însă pentru standardul 1000BASE-T trebuie inversate în oglindă toate cele patru perechi.

Crossover (2)

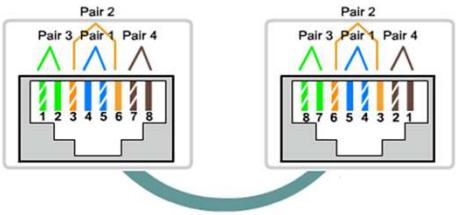
- Capetele sunt mufate folosind standarde diferite
- Folosit între echipamente care operează la același nivel din stiva OSI

Echipamentele ce pot fi conectate folosind un cablu UTP de tip crossover sunt:

- Dispozitiv terminal – dispozitiv terminal
- Switch - switch
- Switch - hub
- Ruter - ruter
- Dispozitiv terminal - ruter
- Hub - hub

Rollover

- Un capăt este mufat folosind un standard iar celălalt capăt este mufat în ordine inversă
- Folosit pentru echipamente Cisco
- Folosit pentru administrarea echipamentelor (Ex.: rutere, switchuri etc.)
- Se conectează pe portul serial al calculatorului

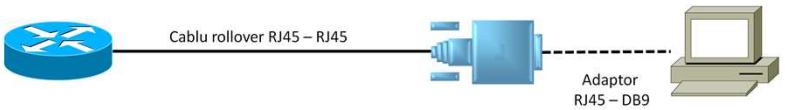


Cablul de consolă, sau cablu rollover este folosit când se dorește conectarea printr-un port de consolă la un echipament de rețea. Există mai multe tipuri de cabluri ce pot face legatura între un echipament terminal și un echipament intermediar (ruter, switch etc.).

Întodeauna, portul dispozitivului terminal este o legatură de tip serial (DB9 sau DB25). Portul dintre ruter și dispozitiv terminal poate fi DB25 sau RJ45, astfel încât pot apărea ca conectori o mufă cu DB9 și una RJ45 sau un cablul de tip rollover și un adaptor de tip RJ45-DB9.

Conectarea prin portul de consolă (1)

- Se folosește un adaptor RJ45-DB9 pentru a face legătura între portul de consolă și portul serial al unui calculator
- Setări pentru comunicația serială
  - 9600 bps
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: none



Comunicația serială presupune ca datele să fie transmise bit cu bit.

Cu toate că transferul paralel este mai rapid, încă mai există transmisii de date între echipamente terminale făcute pe o cale serială pentru a reduce costul cablului și a conectorilor. Toate comunicațiile seriale sunt caracterizate de trei elemente:

- Date – scheme de codificare
- Temporizări – sincronizare între receptor și emiţător
- Semnale – tratarea erorilor, rutare și control al fluxului

În cazul comunicării seriale dintre un echipament de rețea și un echipament terminal este necesar un cablu rollover cu adaptor pentru DB9 și un soft pe echipamentul terminal capabil să realizeze accesul la portul serial.

Un exemplu de astfel de soft este Putty.

Conectarea prin portul de consolă (2)

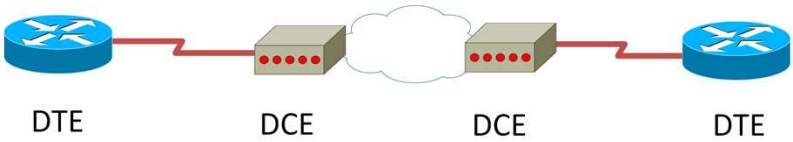
- Necesară pentru:
  - management out-of-band
  - configurarea inițială a routerului (out of the box)
  - monitorizare
  - system recovery (inclusiv password recovery)

Folosirea portului de consolă oferă pe lângă avantajele menționate mai sus și dezavantaje:

- Accesul fizic neautorizat la portul de consolă al echipamentului ce aduce după sine compromiterea totală a securității
- Conectarea unei interfețe Ethernet la portul de consol aduce cu sine distrugerea totală a portului
- În cazul în care sistemul de operare este șters și în rețea nu există un server de TFTP, copierea fișierelor se face lent

Conexiuni WAN

- **DCE** = Data Communication Equipment
  - la granița provider-ului
  - impune frecvenţa semnalul de ceas (clocking)
- **DTE** = Data Terminal Equipment
  - contactul utilizatorului cu WAN-ul
  - adaptează semnalul de ceas la frecvenţa DCE-ului



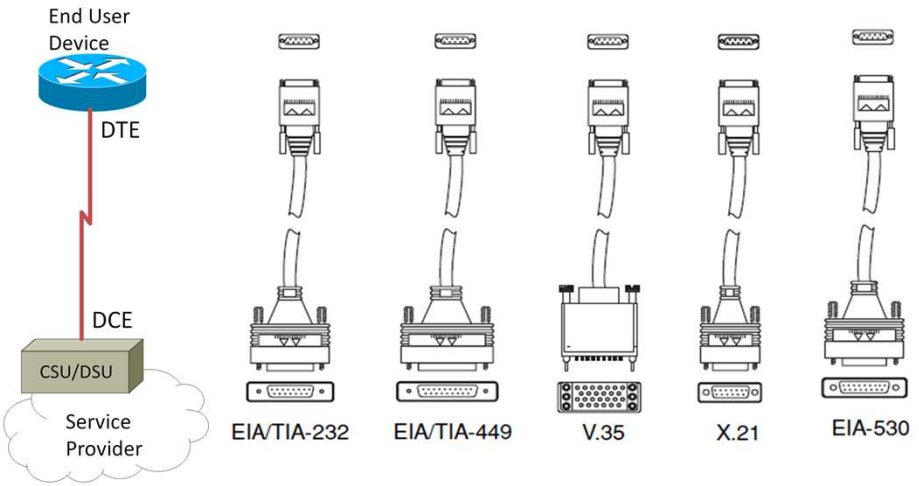
DTE-ul este un echipament ce converteşte informaţiile primite în semnale electrice, de aceea mai este denumit și ,,circuit coadă”.

După cum indică numele complet, DTE, aceasta este un dispozitiv care termină o linie de comunicare, pe când DCE-ul prevede prelungirea unei căi de comunicare. Ca exemplu, să presupunem că avem un calculator care vrea să comunice în Internet prin intermediul unui modem şi o conexiune de tip dial-up. Pentru a ajunge la Internet modemul va apela numărul furnizorului, acesta va răspunde cerând datele de autentificare ale clientului, iar după verificarea informației de autentificare, calculatorul va avea acces la Internet.

În acest exemplu, calculatorul și furnizorul de Internet sunt un DTE, iar modemul este un DCE.

Interfețe WAN (1)

- Conexiuni seriale



Interfețele seriale simulează liniile închiriate în cadrul laboratorului, acest tip de cablu este folosit pentru conectarea unui echipament al ,,Internet Service Provider-lui” (ISP) cu ruterul din reţeaua locală.

Liniile închiriate sunt o tehnologie în care clientul primește un canal dedicat de la ISP. Clientul având control deplin asupra canalului.

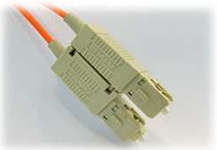
Echipamentul ISP-ului este de tip DCE (Data Communication Equipment) , cel care setează „clock rate-ul” interfeței seriale.

„Clock rate-ul” este viteza maximă suportată de acea legătură serială, valorile vitezei fiind o sumă de puteri ale lui doi.

Data Equipment Terminal-ul este reprezentat de echipamentul ce realizează legătura între rețeaua locală și ISP, acesta configurează viteza legăturii cu parametrii primiți de la DCE.

Interfețe WAN (2)

- Conexiuni fibră optică
  - SC (Standard Connector)
  - ST (Straight Tip)
  - MIC (Media Interface Connector)



SC

ST

MIC

Principalele caracteristici ale conectorilor de fibră optică menționați mai jos sunt:

- Domenii de aplicație: reţele de telecomunicaţii, reţele de CATV, LAN, MAN, WAN
- Parametrii tehnici:

  - șlefuire PC (physical contact)

  - carcasă conector din plastic pentru SC și carcasă conector din metal anticoroziv pentru ST

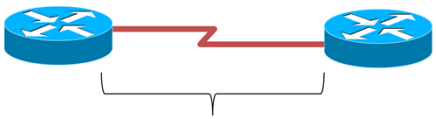
  - mecanism de fixare prin înşurubare pentru ST și mecanism de fixare Push & Pull pentru SC

  - montabil pe fibră şi cablu moultimod de 50 şi 62,5 mm

Pentru mai multe informații despre conectori de fibră optică consultați site-ul: http://www.en.atl-fo.eu.

Adresarea IP într-o rețea (1)

- Înainte de începerea planificării cablajului trebuie să se realizeze împărțirea în subrețele
- Împărțirea în subrețele trebuie să țină cont de tipul rețelelor și de evoluția lor în viitor („planning for future growth”)
- Pentru LAN-uri, se preconizează un număr maxim acceptabil de calculatoare ce vor avea nevoie de adrese IP în acel subnet
- Pentru WAN-uri point-to-point, alocarea a mai mult de două adrese reprezintă o irosire de adrese (rețele /30)



Subnet /30 cu 2 adrese alocabile

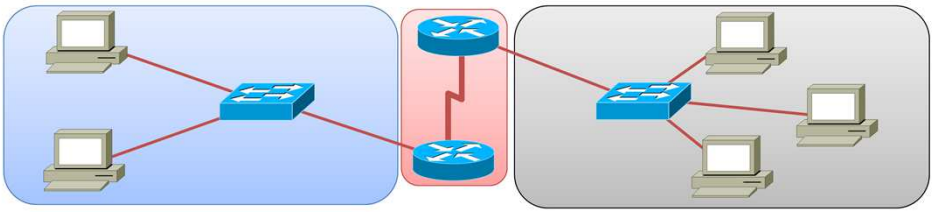
Dezvoltarea unui plan de alocare a adreselor IP sau de proiectare a unei subrețele este un concept important pentru un administrator de rețea.

Trebuie să se țină cont de mai mulți factori în momentul în care se folosește modelul de adresare classless:

- Numărul de locații
- Numărul de echipamente din fiecare locație
- Cerințele de adresare IP pentru fiecare locație individuală
- Numărul de echipamente din fiecare rack de echipamente
- Cerințe de VoIP, wireless LAN, video
- Mărimea subrețelei

Adresarea IP într-o rețea (2)

- Împărțirea în subrețele
  - reduce traficul de broadcast
  - segmentează rețeaua pe domenii de funcționalitate (fiecare cu cerințele și serviciile sale)
  - permite o implementare a securității corespunzătoare cu cerințele fiecărei rețele



După cum știm un domeniu de broadcast este reprezentat de echipamentele care au aceeași adresă de rețea, primesc și transmit mesaje de tip broadcast numai în limitele acelei rețele. Un domeniu de broadcast este limitat de echipamente de nivel trei și extins de unul de nivel 2.

Odată alocată o subrețea unui domeniu de broadcast, adresele din cadrul acesteia nu pot fi refolosite în altă subrețea și trebuie să fie unice în subrețeaua respectivă.

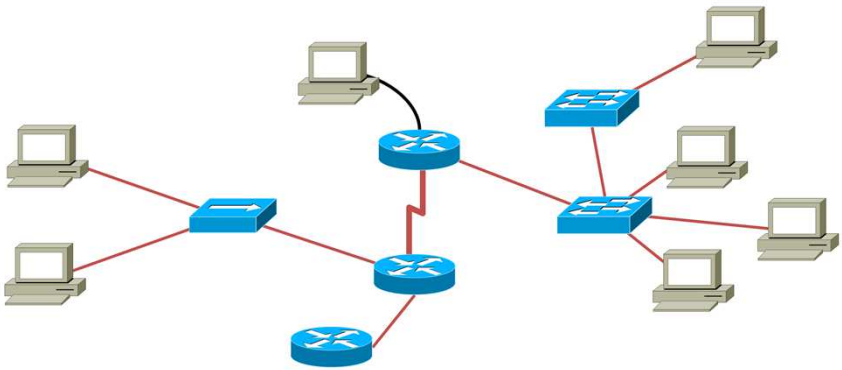
În cazul telefoniei IP, echipamentele de VoIP se plasează de obicei într-un VLAN, care este într-un alt segment logic separat de celelalte stații. Separarea echipamentelor de voce de cele de date prin VLAN-uri ajută și la implementarea QoS pentru traficul de voce. Aceasta regulă de proiectare facilitează și depanarea eventualelor probleme.

Întrebări

1. Se dorește implementarea unei rețele cu un mediu nesusceptibil la interferențe electromagnetice. Ce tip de mediu se folosește?

a. Wireless b. Fibră optică c. Cablu coaxial d. Cablu UTP categoria 5

2. Realizați cablarea urmatoarei rețele specificând tipul de cablu și conectorul folosit.



Capitolul 10: Configurarea și testarea rețelei

Obiective

- Cisco IOS
- Configurarea IOS
- Verificarea conectivității
- Monitorizarea rețelei

IOS

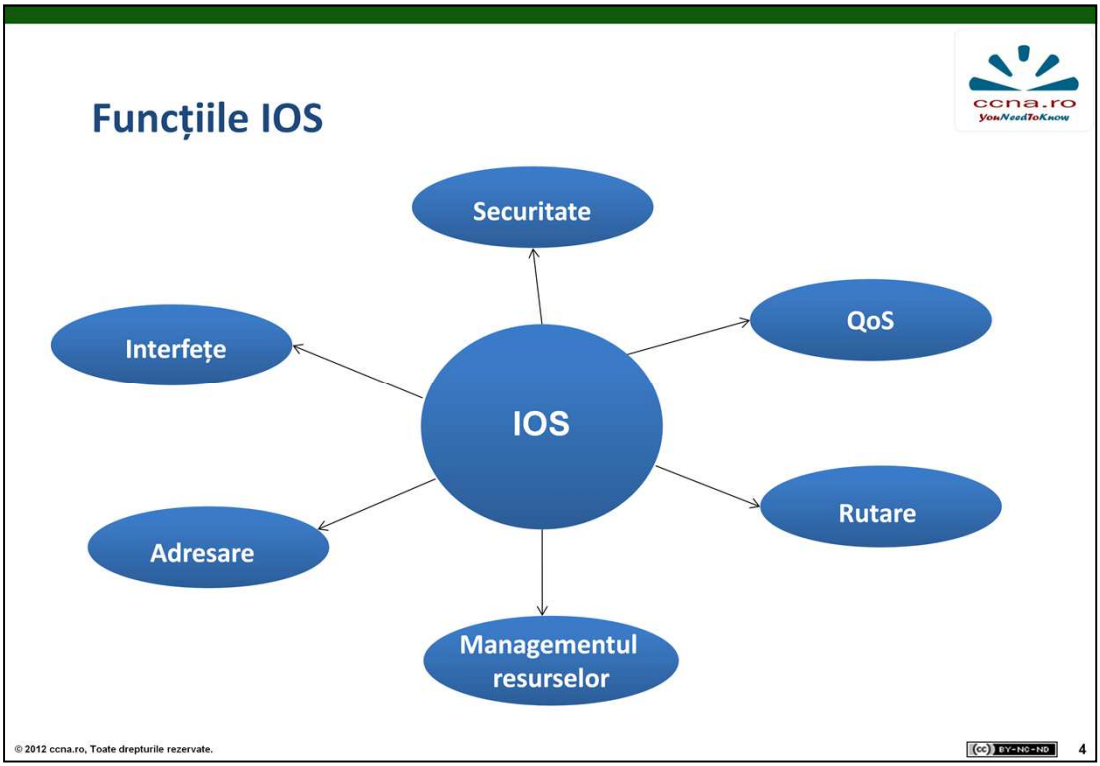
- IOS = Internetwork Operating System
- Sistemul de Operare multitasking care funcționează pe echipamente Cisco
- Conține un set de funcții de switching, rutare și comunicare
- Principalul mod de interacțiune este prin CLI (Command Line Interface)

Cisco IOS este sistemul de operare, closed-source, proprietar Cisco folosit pe majoritatea ruterelor și switch-urilor Cisco. Prima versiune a fost scrisă în 1986.

Cisco IOS este stocat în Flash (memorie nevolatilă), putând fi salvat și în format de arhivă, caz în care este mai greu încărcat de echipament. La fiecare pornire a echipamentului este copiat în memoria RAM și apoi rulat.

În funcție de platforma folosită, IOS-ul poate avea diferite opțiuni, ceea ce înseamnă că, în funcție de necesitate, se pot alege versiuni diferite.

Cea mai folosită versiune de IOS este 12. În prezent CISCO a lansat versiunea 15 care este modulară și poate rula pe orice tip de echipament.



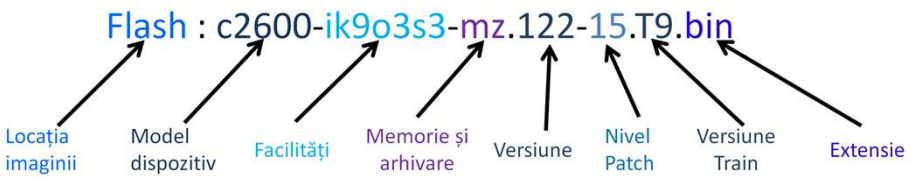
Caracteristici IOS sunt:

- Securitate: Access list (ACL), Firewall, Virtual Private Networks (VPN), Intrusion Prevention System (IPS), Quality of Service (QoS), Media streaming, VoIP, Video-conferințe
- Protocoale de rutare dinamice: RIP, EIGRP, ISIS, OSPF, BGP
- Interfețe: Ethernet, Seriale, virtuale sau logice
- Adresare: IPv4 și IPv6

Aceste funcționalități pot fi administrate dintr-un mod global de configurare. Managementul IOS-ului este unul arborescent, acest model permite navigarea și înțelegerea rapidă a structurii sistemului. O altă caracteristică ce vine în ajutorul utilizatorului este autocompletarea.

Numele unei imagini IOS

- Fiecare imagine este compilată pentru familii de dispozitive
- Facilitățile includ IP base, Voice, Security, tipuri de criptări suportate (AES, 3DES), Firewall
- Versiunile sunt : XE(2.4-2.6), XR(3.7-3.9), NX-OS (4.0-4.2), 12.2S, 12.3, 12.4 si 15



Cisco IOS are numele versiunii de tipul a.b(c.d)e, unde:

- a reprezintă numărul versiunii majore
- b este numărul versiunii minore
- c este numărul de „release”, care începe cu valoarea 1 și este incrementat la fiecare „release” publicat în aceași suită a.b
- d (omis în „release”-urile generale, nesemnificativ pentru utilizatori) este numărul compilării
- e (0, una sau două litere) este identificatorul suitei: T (pentru Technology), E (pentru Enterprise), S (pentru Sevice Provider), XA (pentru suite de funcționalități speciale), etc.

Metode de acces (1)

Port Consolă

- **Port Consolă**: conexiune serială de mică viteză (9600 bps), configurare out-of-band, se folosește cablul rollover
- Folosirea unui cablu Ethernet pe portul de consolă va duce la distrugerea acestuia

Portul de consolă este un port de management, accesibil chiar dacă nu au fost configurate servicii de rețea.

Exemple de folosire a portului de consolă:

- Configurare inițială a echipamentului
- Depanarea echipamentelor atunci când accesul de la distanță nu este posibil
- Recuperarea parolei

Accesul la portul de consolă este nesecurizat în mod implicit, totuși, este recomandat configurarea unei parole pentru a preveni accesul persoanelor neautorizate. În cazul pierderii parolei, există posibilități de accesare a echipamentului evitând folosirea acesteia, doar dacă există acces fizic.

Metode de acces (2)

Port Auxiliar

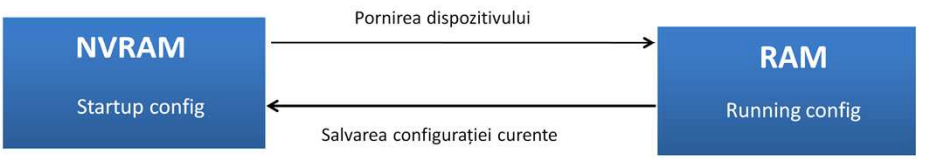
- **Port AUX**: conexiune dialup prin intermediul unui modem, configurare out-of-band

Un alt port de management este portul auxiliar. Nu toate echipamentele au un port auxiliar. Acesta poate fi folosit ca înlocuitor al portului de consolă.

În cazul defectării acestuia poate fi atașat un modem, astfel realizându-se o conexiune la distanță prin intermediul unei conexiuni dial-up.

Similar cu portul de consolă, această metodă de acces nu necesită configurarea de servicii de rețea și este de preferat evitarea folosirii ei.

Fișierul de configurare



NVRAM este memorie nevolatilă. „Nevolatilă” specifică ideea conform căreia conținutul din NVRAM nu se pierde atunci când ruterul este oprit sau restartat.

Memoria RAM deţine fişierul de configurare curent, iar NVRAM deţine fişierul de configurare la pornire. Dacă NVRAM este gol, atunci când se porneşte ruterul, se va solicita introducerea modului de autoconfigurare.

RAM este memorie cu acces aleatoriu şi stochează informaţii operaţionale, cum ar fi tabelele de rutare şi fişierele de configurare. Conţinutul RAM este pierdut atunci când echipamentul este oprit sau restartat.

Moduri de operare (1)

User EXEC : *Router>*
`ping, show (limitat), enable, etc.`

```
Router> ping IP_address
Router> show (limited) [arp | flash: | version etc.]
Router> enable
Router> telnet IP_address
Router> ssh IP_address
Router> traceroute IP_address
```


Din punct de vedere al securității, echipamentele de rețea au diferite moduri din care se pot monitoriza sau configura diferite servicii oferite de acesta.

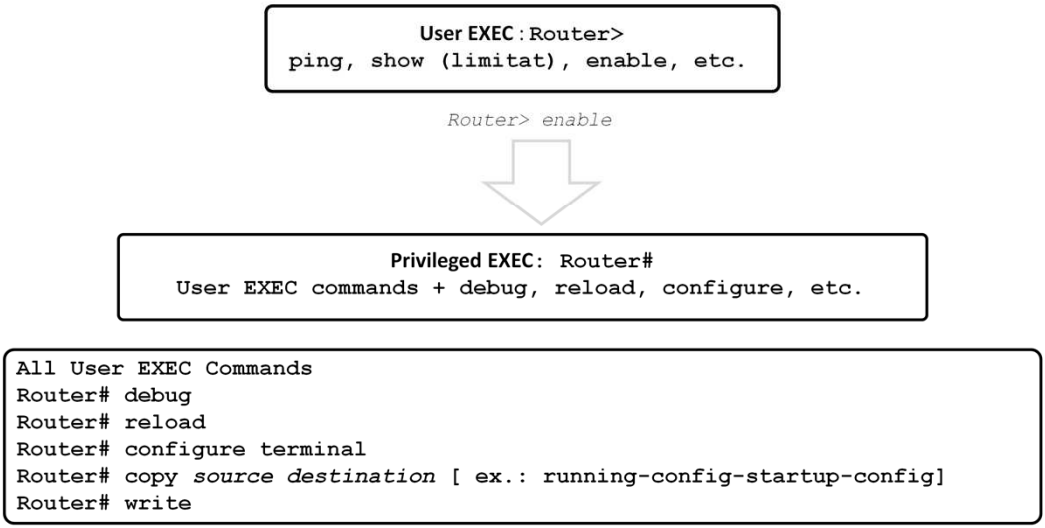
Primul și cel mai restrictiv mod este „User EXEC”, modul implicit în care pornește un IOS fără configurare inițială, astfel utilizatorul având privilegii limitate. Se mai numește „view-only mode” şi nu este protejat de parolă în mod implicit.

Din acest mod se pot verifica şi monitoriza toate serviciile de pe un echipament.

Promptul specific „User EXEC” în CLI este: `Router>`.

Pentru a trece la un nivel nivel superior de privilegii este nevoie de comanda „enable”, moment în care promptul„>” se transformă în „#”.

Moduri de operare (2)



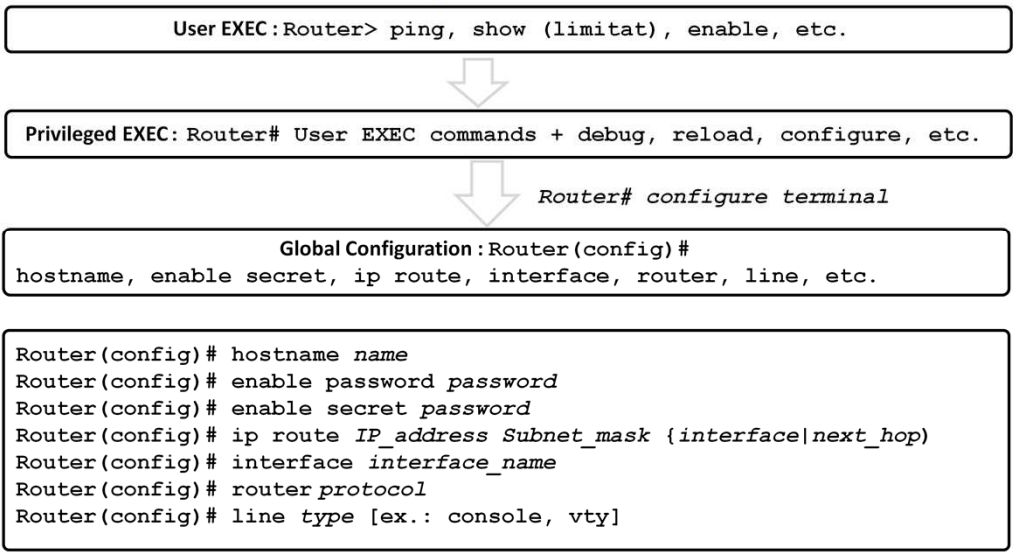
Modul ce oferă privilegii în plus fața de „User EXEC” este „Privileged EXEC”.

În cadrul acestui mod de operare, utilizatorul are acces deplin la toate comenzile de testare și vizualizare, incluzând comenzile conţinute de modul EXEC. Din acest mod se accesează modul global de configurare cu ajutorul comenzii „configure terminal”.

Ruterele CISCO au mai multe nivele de privilegii, de la nivelul 0 la nivelul 15. „Privileged EXEC” este echivalent cu nivelul de privilegiu 15 în timp ce „User EXEC” este de privilegiu 1.

Privilegiul de nivel 0, este rar folosit și include 5 comenzi: disable, enable, exit, help și logout.

Moduri de configurare (1)



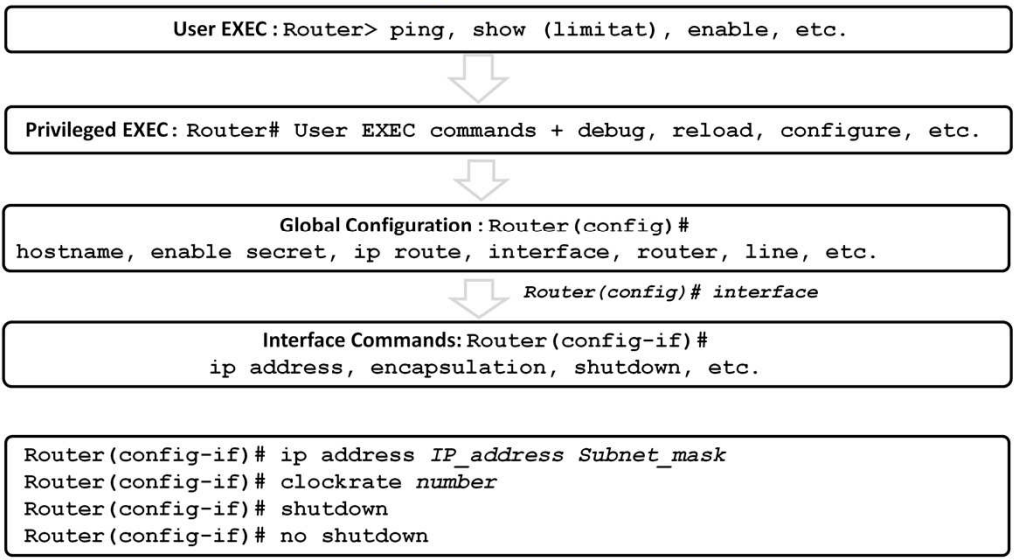
Singurul mod ce permite configurarea echipamentului este „global configuration”.

Se accesează prin comanda „configure terminal” din modul privilegiat. Este folosit pentru configurarea persistentă a echipamentului şi pentru accesarea modurilor specifice de configurare (line, route, interface etc.).

Spre deosebire de User şi Privileged orice comandă din acest mod se va salva în configurația curentă (running configuration).

Tot de aici se pot introduce toate comenzile din modul privilegiat, doar cu condiția ca înaintea comenzii să fie introdus cuvântul cheie „do”. Din acest mod se configurează interfețele, linia de consola, liniile de acces de la distanță, etc.

Moduri de configurare (2)



Din modul global de configurare, trebuie să se acceseze un mod specific de configurare al interfețelor. Se accesează prin comanda „interface *[if-name]"* din modul *Global de configurare.* Se utilizează pentru configurarea interfețelor (IP address, mask, encapsulation, etc.)

Promptul este de forma: **Hostname(config-if)#**

Comenzi:

– configurarea unei adrese IPv4 pe interfaţă

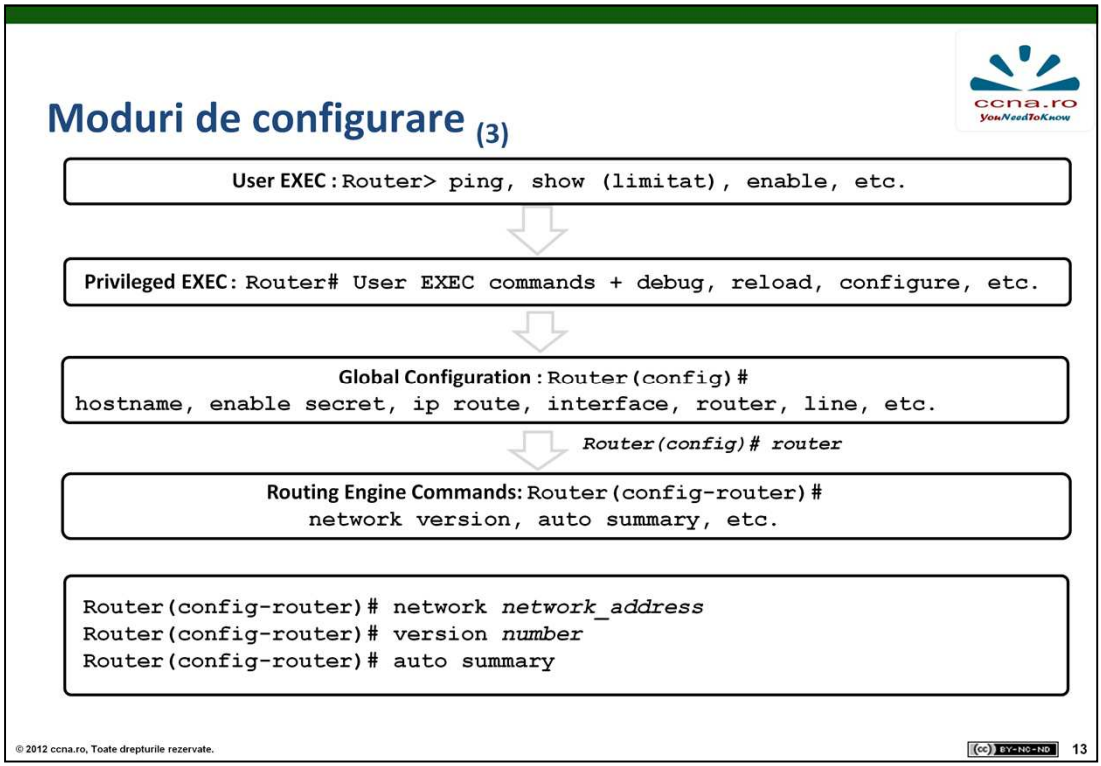
R1(config-if)#ip address *IP_address Subnet_mask*

– configurarea frecvenţei de transfer pentru legăturile seriale

R1(config-if)#clockrate *number*

– închiderea interfeţei: **R1(config-if)#shutdown**

– deschiderea interfeţei: **R1(config-if)#no shutdown**



Pentru configurarea protocoalelor dinamice se foloseşte comanda „router [protocol]”.

Se accesează din modul global de configurare şi se utilizează pentru configurarea protocoalelor de rutare. Protocoale suportate: RIP, OSPF, IGRP, EIGRP, IS-IS, BGP etc.

Promptul este de forma: **Hostname(config-router)#**

– pentru majoritatea protocoalelor de rutare, comanda network se foloseşte pentru activarea pe interfeţe a protocolului de rutare

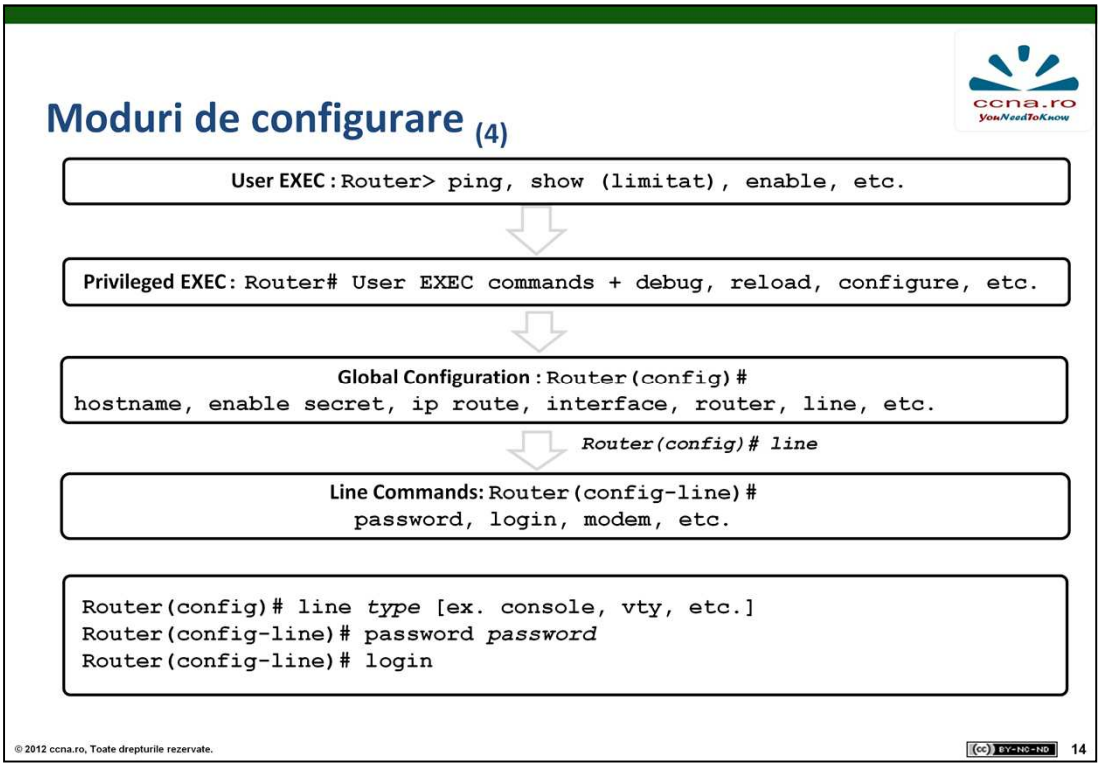
Router(config-router)#network *network_address*

– setarea versiunii protocolului

Router(config-router)#version *number*

– setarea sumarizării automate

Router(config-router)#auto summary

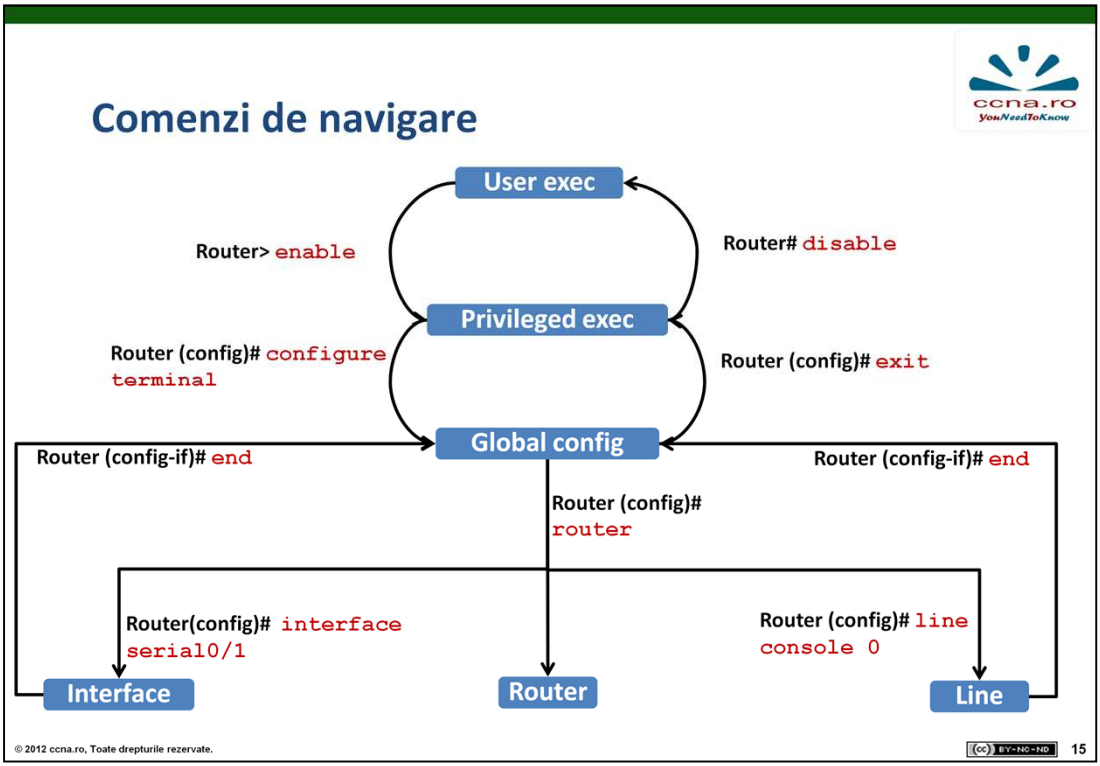


Modul de configurare a liniilor de consolă se accesează prin comada *„line [type]”* din modul global de configurare. Este folosit pentru configurarea accesului pentru conexiunile ce sunt destinate echipamentului.

Tipuri suportate sunt:

- vty (terminal virtual)
- console
- tty
- async

Promptul este de forma **`Hostname(config-line)#`**. Se poate configura accesul simultan atât telnet cât și ssh sau în mod independent.



Prin diferite combinații de taste se poate ajunge direct în modul „User EXEC” sau prin comanda exit se aduce utilizatorul în modul anterior.

În cazul în care, din diferite motive, sunt operații ce durează prea mult, există diferite combinații de taste care pot ajuta administratorul să iasă din acel timp mort fără a fi nevoit să aștepte ca operația respectivă să se încheie.

Una din cele mai folosită comandă este Ctrl+C.

CLI Help (1)

- Context sensitive help:

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection

Router>show ?
  arp             Arp table
  cdp             CDP information
  clock           Display the system clock

Router>show p?
policy-map  privilege  protocols
```

- Command Syntax Check

```
Router>s
% Ambiguous command: "s"

Router>show
% Incomplete command.

Router>show iinterface
             ^
% Invalid input detected at '^' marker.
```


- Context sensitive help:
  - se afişează o listă de comenzi specifice modului curent sau o listă de argumente specifice comenzii curente
- Command Syntax Check
  - mesaje de eroare:
    - comandă ambiguă
    - comandă incompletă
    - comandă incorectă

CLI Help (2)

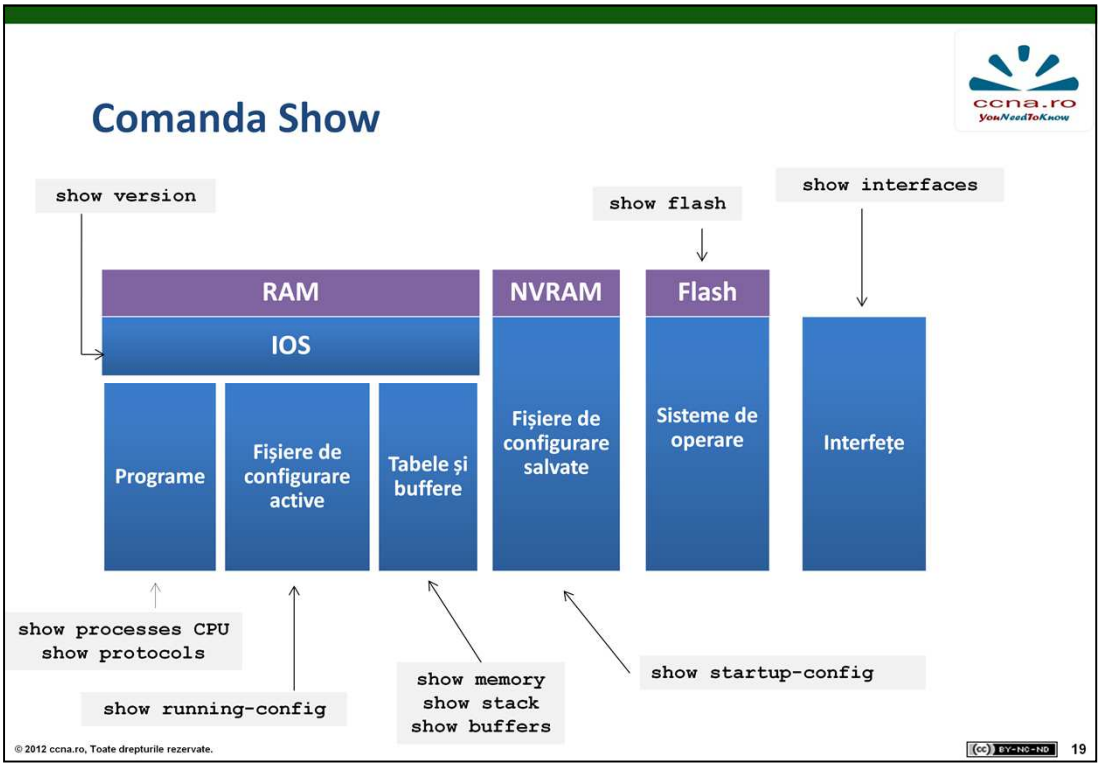
- Taste rapide: Line edit

Tastă	Acțiune
Ctrl-D	șterge un caracter la dreapta cursorului
Backspace	șterge un caracter la stânga cursorului
Esc-D	șterge caracterele din dreapta cursorului până la sfârșitul cuvântului
Ctrl-W	șterge un cuvânt la stânga cursorului
Ctrl-K	șterge caracterele din dreapta cursorului până la sfârșitul liniei
Ctrl-U sau Ctrl-X	șterge caracterele din stânga cursorului până la începutul liniei
TAB	termină o comandă parțială
Ctrl-A	mută cursorul la începutul liniei
Ctrl-E	mută cursorul la finalul liniei
Ctrl-R	reafișează o linie
Up/Down Arrow	permite căutarea de comenzi care au mai fost date

CLI Help (3)

- Taste rapide: Break keys

Tastă	Acțiune
Ctrl-C	Părăsește modul global în modul privileged, afisează promptul dacă suntem intr-un mod de setup
Ctrl-Z	Părăsește modul global în modul privileged
Ctrl+Shift+6	Permite căutarea de comenzi care au mai fost date.



Pentru a face verificări sau eventuale depanări, trebuie examinată operarea dispozitivelor, acest lucru realizându-se folosind comanda show.

Există o multitudine de parametrii pentru comanda „**show**”, cei mai frecvent folosiți fiind:

- **`show version`** - pentru vizualizarea versiunii IOS-ului și altor parametri ai dispozitivului

```
1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"
```

- **`show running-config / startup-config`** - pentru vizualizarea configurării actuale / inițiale a echipamentului

Show ip interface [brief]

```
Router# show ip interface brief
Interface          IP-Address    OK?   Method   Status                  Protocol
FastEthernet0/0    192.168.0.1   YES   NVRAM    up                      up
FastEthernet0/1    unassigned    YES   unset    administratively down   down
Serial0/0          unassigned    YES   unset    down                    down
Serial0/1          10.0.1.1      YES   NVRAM    up                      down
```


Această comandă este utilă pentru a vizualiza în mod centralizat starea și unele configurări ale interfețelor. Afișează starea interfețelor la nivel fizic (Status) și nivel legătură de date (Protocol).

Statusul poate fi: up, down sau administratively down.

Protocolul poate fi: up sau down.

Pot apărea urmatoarele situații:

- *Status: down* și *Protocol: down* – erori nivel 1 (lipsă cablu, tip de cablu greșit, clockrate diferit, etc.)
- *Status: up* și *Protocol: down* – erori nivel 2 (încapsulare)
- *Status: administratively down* și *Protocol: down* – interfața configurată cu shutdown

Ping

```
Router# ping 192.168.0.1
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)

Router# ping
Protocol[ip]:
Target IP address: 192.168.0.1
Repeat count [5]:
Datagram size[100]:
Timeout in seconds[2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
```


Acest utilitar verifică conectivitatea între două dispozitive, starea stivei de protocoale (ping 127.0.0.1). Serviciul folosește protocolul ICMP.

Tipuri de mesaje:

- Echo Request: o cerere la care se așteaptă un pachet cu aceleași date
- Echo Reply: răspunsul la o cerere
- Destination Unreachable: un mesaj care este trimis de un ruter sau gateway pentru a anunța că destinația nu este accesibilă
- Time Exceeded: mesaj trimis de un ruter sau gateway pentru a anunța că TTL a ajuns la valoarea 0

Comanda ping extinsă: atunci când o comandă ping simplă este introdusă pe un ruter, adresa sursă este adresa IP a interfeței de ieșire a pachetului. Dacă este folosită o comandă ping extinsă, adresa IP sursă poate fi schimbată cu orice adresă IP a lui.

Pachetul de ICMP

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (160 bits OR 20 Bytes)	Version/IHL	Type of service	Length	
	Identification		*Flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (64+ bits OR 8+ Bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

Pachetul ICMP conţine câmpurile:

- Versiunea: poate fi 4 respectiv 6
- Type of service: specifică indicații despre QoS, este format din 8 biți
- TTL (Time to Live): numărul maxim de hopuri pe care un pachet îl poate avea, se decrementează la fiecare hop. Când TTL este egal cu 0 pachetul va fi aruncat
- Header Checksum: verifică denaturarea datelor, se face o sumă de control, iar la destinație de verifica printr-un algoritm dacă suma pe care o calculează destinația este echivalentă cu cea trimisă de sursă
- Source: specifică adresa IP a stației sursă
- Destination: specifică adresa IP a stației destinație

Monitorizare (1)

- La nivel fizic: culoarea LED-urilor de pe dispozitive
- La nivel legatură de date: gestionarea tabele CAM, arp –a
- La nivel reţea: gestionarea tabelei de rutare, ping, tracert
- La nivel transport: port scanner (nmap)
- La nivel aplicaţie: gestionarea proceselor, permisiuni
- Aplicaţii complexe: Wireshark
- Recomadare: includerea unui sistem de raportare şi jurnalizare

Pentru o monitorizare de bază trebuie cunoscute câteva lucruri de bază, depanarea realizându-se pe nivele:

- La nivel fizic: este importată cunoașterea culorilor LED-urilor
- La nivel legătură de date: tabela CAM reține o asociere între un port și o adresa MAC, această asociere putând fi fie statică fie dinamică
- La nivel reţea: este importantă înțelegerea tabelei de rutare, cât și a utilitarelor ping și tracert (Windows)
- La nivel transport: unul dintre cele mai puternice utilitare este nmap ce are rol de scanare a porturilor
- Aplicații complexe: Wireshark este analizor de pachete, open source, folosit pentru depanarea rețelei care permite capturarea și afișarea traficului de pe o stație

Rezumat

- IOS
- Port Consolă, Port AUX, Telnet, SSH
- User EXEC
- Privileged EXEC
- Global Configuration
- CLI Help
- Gateway
- Monitorizarea reţelei

- Care este versiunea imaginii următoare? Dar modelul dispozitivului?

flash:c3640-j-mz_112-6_P.bin

- Ce tip de port se foloseşte pentru configurarea la distanță a unui ruter?
- Cu ajutorul cărei comenzi se realizează trecerea de la modul privilegiat la modul global de configurare?
- De ce apare mesajul de eroare la tastarea comenzii următoare?

```
Router#show serial 0/0/0
```

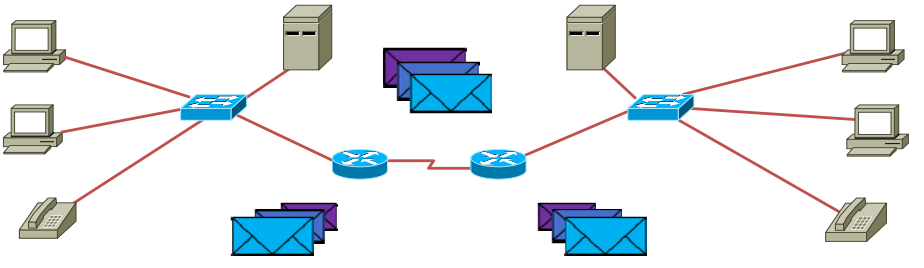
- La ce nivel se realizează monitorizarea folosind comanda următoare?

```
Router# show arp
```

Introducere în concepte de rutare

Ce funcții oferă un ruter?

- Interconectează două sau mai multe rețele
- Are două funcții principale
  - determinarea căii optime
  - trimiterea pachetelor către destinație, folosind calea optimă determinată
- Multiple funcții secundare: manipulare, filtrare și modificare a pachetelor

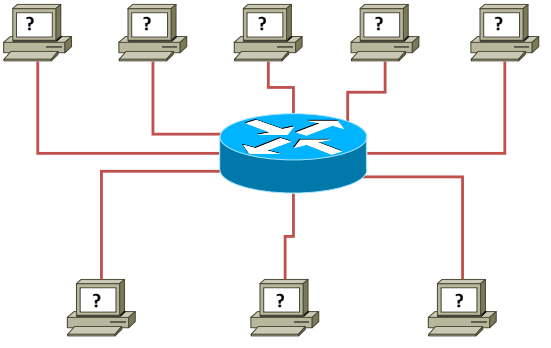


Principalul scop al unui ruter este procesul de „routing” al pachetelor între mai multe rețele. „Routing” înseamnă analizarea antetelor pachetelor de nivel 3 și luarea, pe baza a multiple reguli, a unei decizii cu privire la interfața pe care va fi trimis acesta. Determinarea căii se face prin mai multe metode, și anume rutare statică și rutare dinamică.

În cazul rutării statice administratorul decide calea pe care o va urma un pachet, iar în cazul celei dinamice calea este decisă automat pe baza unor protocoale de rutare. Din punct de vedere practic, un ruter poate fi considerat un dispozitiv care funcționează pana la nivelul 7 (nivelul Aplicație), deoarece poate avea și funcții de filtrare ale pachetelor, asigurarea unei anumite calități a serviciilor și modificarea antetelor pachetelor de nivel 4 (nivelul Transport).

De ce avem nevoie de rutare?

- Transmiterea pachetelor între rețele
  - criterii de eficiență
  - criterii de politică internă sau externă



Principalul rol al unui ruter într-o topologie este rutarea pachetelor între mai multe rețele. Rutarea este procesul prin care dispozitivul de rețea analizează antetul de nivel 3 al unui pachet primit (adresa IP destinație) și apoi, pe baza anumitor reguli clar definite manual sau de protocoale specializate, decide ce să facă cu pachetul mai departe. Un ruter de nivel „enterprise” trebuie să fie capabil să proceseze în jur de 10.000 pachete pe secundă, iar acest lucru este posibil doar prin implementarea unor circuite hardware dedicate foarte rapide.

Deși din punct de vedere teoretic, rutarea pachetelor se desfășoară doar la nivelul 3, un ruter este capabil să citească informații din antete până la nivelul 7. Acest lucru este în special folositor în aplicații „mission-critical” cum ar fi VoIP sau aplicații care necesită latență extrem de mică, cu ajutorul unor sisteme de QoS (Quality of Service). QOS este un serviciu oferit de anumite rutere avansate care permite prioritizarea traficului în funcție de conținut sau destinație.

Criterii de rutare

- Informațiile cu privire la rețelele cunoscute sunt stocate în tabela de rutare
  - se stochează adresele rețelelor și următorul hop către fiecare destinație
  - în cazul conexiunilor punct-la-punct se poate stoca direct interfața de ieșire
  - același lucru se face automat pentru rețelele direct conectate
- Rute statice
  - configurate de administrator
  - au prioritate în procesul de rutare
- Rute dinamice
  - învățate prin intermediul unor protocoale specializate
  - algoritmii folosesc criterii de eficiență sau criterii de politică

Fiecare ruter are o bază de date salvată în RAM care conține regulile setate manual sau automat folosite pentru luarea deciziilor de rutare; această bază de date se numește tabelă de rutare.

Tabela de rutare a unui ruter stochează informații multiple cu privire la rețelele adiacente unui ruter și la calea pe care un pachet trebuie să o urmeze pentru a ajunge în rețeaua destinație. Astfel, pentru o destinație oarecare tabela de rutare stochează:

- masca de rețea
- metoda prin care calea respectivă a fost aflată
- adresa IP next-hop sau interfața de ieșire prin care aceasta poate fi accesată

Rutele pot fi învățate de un ruter prin două metode:

•Static, configurate de un administrator; acest tip de rută va fi întotdeauna preferată față de o rută dinamică

•Dinamic, cu ajutorul unui protocol de rutare specializat; în acest caz se folosesc algoritmi avansați pentru determinarea căii optime

Rutare statică vs. Rutare dinamică (1)

- Rutare statică
  - oferă control mult mai riguros administratorului asupra următorului hop ales
  - este foarte ușor de învățat
  - nu este deloc scalabilă

Rutarea statică se configurează manual pe rutere și oferă un management mai riguros asupra modului de stabilire a următorului hop către o anumită destinație. Un avantaj al folosirii rutării statice este efortul necesar scăzut pentru configurarea și administrarea rețelelor restrânse. Pe de altă parte, rutarea statică nu scalează optim în cazul rețelelor de dimensiuni mari, fiind necesară implementarea rutării dinamice. De asemenea, rutarea statică consumă puține resurse hardware, permițând rularea în paralel a altor aplicații performante dacă este necesar.

Rutare statică vs. Rutare dinamică (2)

- Rutare dinamică
  - necesită cunoștinte avansate pentru o configurare eficientă
  - utilizează atât un procent din bandwidth cât și o parte din procesor
  - calea aleasă de pachete nu e cunoscută în mod clar
  - este o soluție scalabilă și tolerantă la defecte
  - exemple: RIP, IGRP, EIGRP, OSPF, IS-IS, BGP

În cazul protocoalelor de rutare dinamice, informația despre rute este propagată automat în întreaga rețea, rutele fiind distribuite cu ajutorul unui algoritm specific. Protocoalele de rutare dinamice oferă scalabilitate și flexibilitate mărită față de metoda statică, însă consumă mai multe cicluri de procesor și utilizează o cantitate mai mare de memorie RAM. Protocoalele de rutare dinamice sunt responsabile cu păstrarea tabelei de rutare sincronizată peste toate ruterele din domeniul de rutare în cazul unei modificări în topologie. Astfel, informațiile că o rețea este invalidă sau afectată de anumite probleme hardware se propagă foarte rapid în toată rețeaua, fără intervenția administratorului. Exemple de protocoale de rutare dinamice sunt RIPv1, RIPv2, IGRP, EIGRP, OSPF, IS-IS, RIPng, EIGRP IPv6 si BGP. RIPv1 și IGRP nu mai sunt utilizate, ele fiind înlocuite integral de versiunile lor îmbunătățite – RIPv2 și EIGRP. RIPng și EIGRP IPv6 sunt variantele bazate pe IPv6 ale protocoalelor de rutare asociate prin denumire.

_____

_____

_____

_____

_____

Metrici, determinarea căii optime

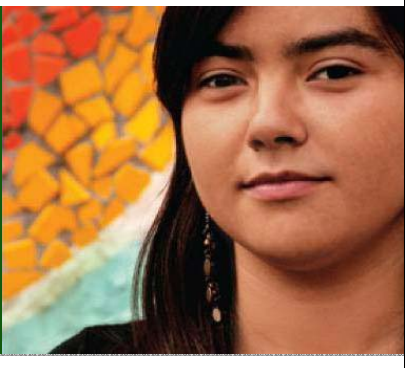
- Metrică
  - indicator de preferință a unei rute după anumite criterii
  - se calculează în funcție de hop-count, delay, bandwidth etc.
  - o metrică mai mică este mai bună
- Determinarea căii optime
  - fiecare rută din tabel are atribuită o metrică
  - ruterul alege ruta cu metrica cea mai mică

Determinarea celei mai bune căi către destinație implică evaluarea căilor disponibile în funcție de anumite criterii, dintre care se remarcă metrica. Metrica este o valoare calculată în funcție de anumite variabile asociate drumului dintre două puncte într-o rețea:

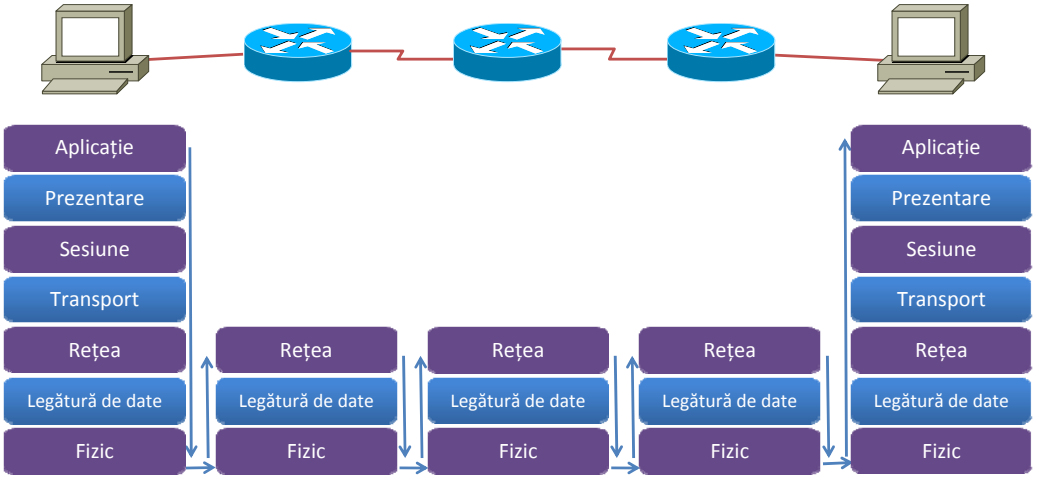
- Hop-count: numărul de rutere parcurse de pachet până la destinație
- Delay: latența specifică elementelor de legătură care alcătuiesc calea
- Bandwith: viteza legăturilor dintr-o cale
- Load: încărcarea cu date a unei conexiuni
- Reliability: gradul de siguranță oferit de o anumită legătură

Protocoalele de rutare dinamice pot utiliza una sau mai multe din aceste variabile în calculul metricii unui drum sau a unei destinații. Ulterior acestui calcul, protocolul de rutare va selecta ruta cu metrica cea mai mică și o va introduce în tabela proprie de rutare.

Manipulareaa pachetelor



Rutarea în cadrul stivei OSI



În cazul transmiterii de date între două stații, pachetele aflate în tranzit vor fi prelucrate de echipamentele terminale și intermediare folosind protocoalele definite în cadrul fiecărui nivel al stivei OSI. Astfel, un pachet va trece prin mai multe procese de încapsulare și decapsulare. La sursă, PDU-ul (Packet Data Unit) va fi încapsulat, la fiecare nivel adăugându-se noi informații specifice.

În cazul rutării, pachetul va fi decapsulat în fiecare ruter prin care trece până la nivelul 3, deoarece un ruter are nevoie doar de adresa IP destinație pentru a lua decizia de trimitere mai departe. Adresele IP sursă și destinație nu se vor schimba niciodată de-a lungul traseului. La nivelul Legătură de date, fiecare hop va modifica adresa MAC sursă, respectiv adresa MAC destinație. Antetul de nivel 2 se va modifica doar la trecerea într-o altă rețea, și nu la trecerea printr-un switch sau alt echipament de nivel 2. Când ajunge la destinație, pachetul este decapsulat și informația conținută este prezentată utilizatorului.

_____

_____

_____

_____

_____

Manipularea pachetelor (1)

- Adrese MAC
  - adrese de nivel 2
  - folosite pentru identificarea fizică a dispozitivelor în cadrul unei rețele locale
  - se modifică la trecerea dintr-o rețea în alta

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	**Start of frame delimiter**	**Destination Address**	**Source Address**	Length Type	802.2 Header and Data	Frame check sequence

Pentru o comunicație eficientă în interiorul rețelei locale nu este nevoie de o adresă la nivel 3, fiind suficient antetul unui pachet la nivelul 2. Acesta conține adresa MAC sursă cât și cea destinație, acestea fiind suficiente pentru transmiterea pachetului cu succes la destinație. Deoarece adresele fizice au numai relevanță locală, ele se vor modifica când pachetul părăsește rețeaua în care se află la un moment dat.

Cadrul 802.3 (Ethernet) este alcătuit din următoarele câmpuri:

•Preamble: 7 biți de 1 și 0 care alternează și au rol de sincronizare

•Start of frame Delimiter: un octet care semnalizează începutul cadrului

•Destination Address: adresa MAC a destinatarului

•Source Address: adresa MAC a expeditorului

Manipularea pachetelor (2)

- Adrese MAC
  - adrese de nivel 2
  - folosite pentru identificarea fizică a dispozitivelor în cadrul unei rețele locale
  - se modifică la trecerea dintr-o rețea în alta

IEEE 802.3						
7	1	6	6	**2**	**46 to 1500**	**4**
Preamble	Start of frame delimiter	Destination Address	Source Address	**Length Type**	**802.2 Header and Data**	**Frame check sequence**

- Length/Type: doi octeți care pot reprezenta ori lungimea cadrului (dacă valoarea este mai mică decât 0x600 – echivalentul 1536 în zecimal) sau tipul protocolului de nivel superior (dacă valoarea este mai mare de 0x600)
- Data: datele încapsulate în pachet
- Frame Check Sequence: 4 octeți cu rolul de a verifica integritatea datelor recepționate.

Manipularea pachetelor (3)

- Adrese IPv4
  - adrese de nivel 3
  - folosite pentru identificarea rețelelor și a stațiilor din rețea
  - se păstrează neschimbate în timpul rutării între rețele
  - time-to-live poate fi folosit pentru a opri buclele de rutare

0			16		31
Version	Header Length	Service type	Total length		
Identification			Flags	Fragment offset	
Time to live		Protocol	Header checksum		
Source address					
Destination address					
IPv4 options (if any)					Padding
Data					

Antetul de nivel 3 este utilizat de ruter pentru a determina calea pe care trebuie să trimită pachetul în drumul spre destinație. Adresele de nivel 3 IP sursă și destinație nu se modifică niciodată în tranzit, fiind afectate alte câmpuri din antet, cum ar fi TTL (time to live) și Header Checksum. Câmpul TTL al fiecărui pachet IP se decrementează cu o unitate la fiecare trecere printr-un ruter. Decrementarea valorii TTL poate fi considerată o măsură de siguranță la nivel 3 permițând eliminarea rapidă a buclelor de rutare (în general considerând că un pachet este trimis cu o valoare TTL egală cu 16, aceasta nu este prins într-o buclă de rutare deoarece pachetul va fi aruncat după parcurgerea a 16 hopuri).

Tabela de rutare și principiile rutării

Tabela de rutare

- Este folosită de ruter pentru a alege interfața de ieșire în transmiterea unui pachet
- Este stocată în RAM, deci se pierde la fiecare repornire
- Conține informații de tip rețea – interfață de ieșire (sau rețea – rețea intermediară)
  - rețele direct conectate, adăugate implicit
  - rețele la distanță: rute statice sau dinamice

Tabela de rutare a unui ruter reprezintă o structură de date ierarhică, unificată și organizată care stochează informații despre destinațiile cunoscute. Este stocată în RAM și nu se memorează la salvarea configurației unui ruter – ea se va reconstrui la fiecare repornire. Pe baza informațiilor conținute în tabela de rutare ruterele iau decizii cu privire la transmiterea unui pachet pe o anumită interfață de ieșire.

Tabela de rutare poate conține mai multe tipuri de rețele:

•Rețele direct conectate: sunt introduse automat în tabela de rutare, reprezentând rețelele care aparțin interfețelor active ale ruter-ului; ele nu pot fi șterse sau modificate fără o schimbare a adresării IP sau a dezactivării interfeței

•Rețele remote: configurate cu ajutorul rutelor statice sau a protocoalelor dinamice de rutare

Tabela de rutare

- Exemplu de tabelă de rutare

```
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demand routing, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route  change change change

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O 172.150.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E 172.17.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
```


În momentul în care un ruter primește un pachet IP pe una din interfețe, adresa destinație din antetul pachetului va fi căutată în tabela de rutare pornind de la ruta cea mai specifică din tabelă (masca de rețea cea mai lungă) și până la ruta cea mai puțin specifică. Tabela de rutare prezintă informații despre următorul hop unde trebuie trimis un pachet pentru ca acesta să ajungă la destinația dorită. De asemenea este prezent și un timer, care în cazul protocoalelor de rutare dinamice reprezintă timpul rămas până la declararea unei anumite rute invalide din cauza lipsei de activitate. Fiecare tip de rută din tabela de rutare este reprezentată de un simbol: O – OSPF, R – RIP, D – EIGRP, B – BGP, făcând mai ușoară parcurgerea acesteia și efectuarea de „troubleshooting” în caz de nevoie.

Principiile de rutare

- Fiecare ruter ia decizii bazându-se doar pe propria tabelă de rutare
- Nu toate ruterele au aceeași tabelă de rutare
- Rutarea se face asimetric
  - rutele stocate se referă doar la drumul spre o rețea, nu și invers
  - pachetele pot folosi alte căi la comunicarea în sens invers

Pentru asigurarea unei funcționări optime a procesului de rutare sunt respectate următoarele 3 principii:

•Ruterele iau decizii de rutare independent bazându-se numai pe informațiile din propria lor tabelă de rutare; astfel, problemele de rutare sunt împiedicate de a se propaga în întreaga topologie, iar puterea de procesare pentru găsirea unei destinații este împărțită în mod egal tuturor nodurilor

•Tabela de rutare este unică pentru fiecare ruter deoarece aceasta conține următorul hop pentru fiecare destinație în parte; tabela de rutare a unui ruter nu va descrie niciodată întreaga cale pe care un pachet trebuie să o urmeze pentru a ajunge la destinația cerută

•Rutarea este asimetrică deoarece tabela de rutare nu descrie un „next hop” valabil pentru un drum dus-întors

Clasificarea rețelelor la rutare

- Conectate
  - rețele direct conectate la interfețe ale ruterului
  - rutele sunt adăugate automat după pornirea și configurarea interfeței
- Cunoscute
  - acele rețele către care sunt definite rute statice sau dinamice
- Necunoscute
  - nu există rute definite pentru aceste rețele
  - se folosește ruta default, dacă e definită, sau se aruncă pachetul
- Rută implicită
  - se definește static de către administrator sau este propagată dinamic
  - se aplică pentru toate rutele necunoscute

Tabela de rutare a unui ruter poate fi populată de mai multe tipuri de rețele:

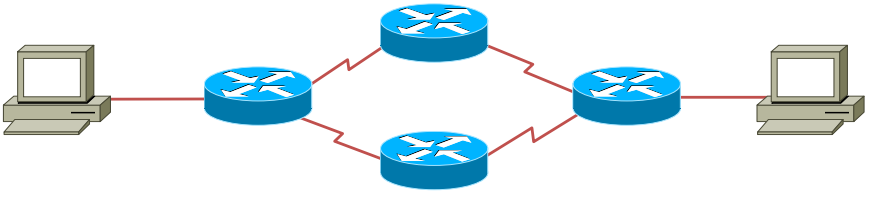
•Conectate – rețelele care aparțin interfețelor active ale ruterului, fiind introduse automat în tabela de rutare alături de interfețele de ieșire corespunzătoare

•Cunoscute – rețelele care au fost instalate în tabela de rutare prin rute statice sau prin protocoale de rutare dinamice

•Necunoscute – rețelele pentru care nu a fost găsit nici un „next hop” sau o interfață de ieșire în urma procesului de parcurgere a tabelei de rutare; în cazul definirii unei rute implicite, ruterul va folosi această rută pentru trimiterea pachetelor destinate respectivelor rețele, altfel, vor fi aruncate

•Rută implicită – este ruta spre care se trimit toate pachetele pentru care nu se cunoaște o destinație specifică

Load balancing



- Pot exista mai multe rute cu aceeași metrică și către aceeași rețea
- În acest caz pachetele pot fi repartizate în mod egal între rutele respective
  - se obține o mai bună repartizare a traficului în rețea
- Procesul se numește „Load balancing”

Există situații în care sunt introduse în tabela de rutare mai multe rute către aceeași destinație având aceeași valoare a metricii. În acest caz, ruterul va repartiza pachetele trimise către destinație în mod egal între rutele respective. Astfel, tabela de rutare va conține pentru o anumită rețea destinație mai multe interfețe de ieșire (sau adrese IP next-hop).

Utilizarea corectă a procesului de „load balancing” poate îmbunătății eficiența și performanța rețelei. În cazul în care traficul este împărțit în mod egal între rutele către destinație, ruterul realizează procesul de „equal cost load balancing”, dar există situații în care pachetele pot fi trimise pe căi multiple chiar dacă metrica nu are aceeași valoare. Acest proces este cunoscut sub numele de „unequal cost load balancing” și poate fi realizat în cadrul protocolului de rutare EIGRP.

Configurarea ruterului prin CLI

Configurare prin CLI

- Există 2 moduri de lucru în CLI
- Modul User Exec
  - este evidenţiat de prompt-ul „**>**”
  - modul implicit în care avem acces imediat după autentificarea pe ruter
  - are doar drepturi de interogare a unor informaţii, nu şi de configurare
- Modul Privileged Exec
  - este evidenţiat de prompt-ul „**#**”
  - are drepturi de configurare a setărilor echipamentului
  - trecerea din modul User în modul Privileged se face cu comanda **`enable`**

Interfața în linie de comandă presupune existența a două moduri principale în care se pot introduce comenzi:

• Modul user Exec: oferă drepturi limitate utilizatorului; identificat prin prompt-ul „>”, se pot accesa doar comenzi elementare de afișare a informațiilor cu privire la funcționarea ruterului

• Modul privileged Exec: se activează prin comanda **`enable`** în modul user Exec și oferă acces la funcții de configurare mai avansate și la informații mai detaliate cu privire la procesele ruterului; accesarea modului privileged Exec se poate observa prin schimbarea prompt-ului de la caracterul „**>**” în caracterul „**#**”

Comanda show

- Informaţii generale despre ruter
  - **#show version**
- Informaţii generale despre interfeţele ruterului
  - **#show interfaces**
- Informaţii despre adresarea interfeţelor
  - **#show ip interface [brief] [tip_interfață număr_interfață]**
- Afişarea tabelei de rutare
  - **#show ip route**
- Afişarea configuraţiei curente
  - **#show running-config**

Una dintre cele mai utilizate comenzi pentru vizualizarea și inspectarea diferitelor configurații existente pe un ruter este comanda **show**. Această comandă suportă numeroși parametrii cu rolul de a afișa:

•informații generale despre ruter (modelul ruterului, versiunea de IOS, capacitatea memoriei, ș.a.)

•informații generale despre funcționalitatea și numărul interfețelor existente pe un ruter

•ip-urile configurate pe interfețe

•conținutul tabelei de rutare

•configurația curentă salvată în fișierul running-config (în memoria RAM) sau configurația permanentă salvată în fișierul startup-config (în memoria NVRAM)

Configurări de bază (1)

- Intrarea în modul de configurare
  - **#configure terminal**
  - prompt-ul se schimbă din **#** în **(config)#**
- Setarea numelui echipamentului
  - **(config)#hostname <nume_router>**
- Setarea unei parole pe modul privilegiat
  - **(config)#enable secret <parola>**
- Setarea unui banner pe router (mesaj afişat la accesare)
  - **(config)#banner motd # Accesul strict interzis ! #**

Majoritatea comenzilor pentru realizarea configurărilor de bază ale unui ruter sunt introduse din modul global de configurare (global configuration mode). Modul global de configurare este accesat prin comanda **configure terminal** introdusă în privileged Exec mode și se identifică prin afișarea promtului **(config)#**. Acest mod de configurare reprezintă interfața principală pentru implementarea a numeroase funcționalități ale unui ruter. Astfel se remarcă o serie de configurări de bază:

•setarea numelui echipamentului

•setarea unei parole criptate sau „plain text” pentru modul privilegiat

•setarea unui banner, adică un mesaj care este afișat de fiecare dată când ruterul este accesat în linia de comandă

Configurări de bază (2)

- Setarea unei parole pentru accesul la consolă
  - `(config)#line console 0`
  - `(config-line)#password <parola>`
  - `(config-line)#login`
- Configurarea ruter-ului pentru acces de la distanță (telnet)
  - `(config)#line vty 0 4`
  - `(config-line)#password <parola>`
  - `(config-line)#login`

Accesarea unui ruter poate fi realizată prin conectare directă la consola ruterului sau la distanță folosind protocoalele telnet sau ssh.

Pentru a oferi un anumit grad de securitate al ruterului, există posibilitatea configurării unei parole de acces. Astfel, pentru accesul la consolă se setează o parolă din modul **`config-line`**. În acest caz, la fiecare conectare la linia de comandă a ruterului, se va solicita utilizatorului introducerea parolei setate.

În cazul accesului de la distanță, se pot configura liniile vty (Virtual Terminal lines) cu o parolă comună pentru toți utilizatorii, o parolă diferită pentru fiecare utilizator definit local, sau se poate folosi un server de autentificare.

Configurarea unei interfeţe (1)

- Intrarea în modul de configurare al interfeţei
  - **(config)#interface <tip_interfață> <număr_interfață>**
  - prompt-ul se schimbă din **(config)#** în **(config-if)#**
- Pornirea/oprirea unei interfețe
  - **(config-if)#[no] shutdown**
  - implicit toate interfețele sunt oprite pe rutere

Configurarea caracteristicilor unei interfețe se realizează din modul de configurare al unei interfețe semnalat de schimbarea promptului din **(config)#** în **(config-if)#** la introducerea comenzii **interface** urmată de numele și numărul interfeței.

Dezactivarea unei interfețe se efectuează utilizând comanda **shutdown**. Pentru pornirea acesteia, se anulează comanda **shutdown** prin negare: **no shutdown**.

În general, o interfață este denumită respectând următorul format: tip interfață urmat de 3 numere separate prin „/”, spre exemplu FastEthernet 0/1/1 unde prima valoare identifică modulul, a doua slotul, iar ultima, portul. Prima valoare este menționată doar în cazul utilizării ruterelor modulare.

Configurarea unei interfeţe (2)

- Setarea unei adrese IP pe interfaţă
  - **(config-if)#ip address <adresă> <mască>**
- Setarea unei descrieri pe interfață
  - **(config-if)#description <descriere>**
- Configurarea parametrului `clock-rate` pe interfețele seriale
  - interfeţele seriale necesită, pentru a putea funcţiona, configurarea vitezei de comunicaţie (clock rate)
  - **(config-if)#clock rate <valoare>**

Ulterior accesării modului de configurare a unei interfețe se poate seta o adresă IP prin specificarea adresei respective urmată de masca de rețea din cadrul rețelei din care face parte adresa IP configurată.

O informație utilă pentru facilitarea documentării sau depanării unei rețele este configurarea unei descrieri pe interfețe. Aceasta este setată prin utilizarea comenzii **`description`** urmată de un text limitat la 240 de caractere.

În cazul utilizării unei legături seriale de tip punct-la-punct, un capăt al legăturii este de tip DTE (data terminal equipment), iar celălalt, de tip DCE (data communications equipment). Pentru a se realiza comunicația de date pe o astfel de legătură, ruterul conectat la capătul DCE trebuie să asigure sincronizarea transmisiei semnalului prin folosirea unei valori numerice configurate prin comanda **`clock rate`** urmată de o valoare exprimată în biți pe secundă.

Salvarea sau ştergerea configurărilor

- Reunește configurările din memorie cu cele salvate în fișierul de configurare (configurările din memorie nu se pierd!)
  - **#copy startup-config running-config**
- Salvarea configurării curente pentru a fi încărcată la repornire
  - **#copy running-config startup-config**
- Ştergerea configurării salvate (startup-config)
  - **#erase startup-config**

Toate configurațiile realizate pe un ruter sunt salvate în RAM, în fișierul de configurare running-config. Pentru ca setările să devină permanente, acestea trebuie salvate într-o memorie nevolatilă, și anume în NVRAM. Astfel, în cazul restartării accidentale a unui ruter, configurațiile curente vor fi încărcate la boot-are. Salvarea setărilor se face prin copierea fișierului running-config în fișierul startup-config. O comandă mai scurtă și mai rapidă decât comanda **copy**, cu cei doi parametrii fișier sursă și fișier destinație, este comanda **write** fără parametri, având același efect.

Ștergerea configurațiilor anterioare existente pe un ruter se realizează prin comanda **erase** urmată de numele fișierului de șters, în cazul de față, startup-config.

Rutare statică

CDP

- Cisco Discovery Protocol
  - proprietar Cisco
  - trimite CDP advertisements echipamentelor direct conectate
  - operează la Nivelul 2
- Cu ajutorul său, un ruter află informații despre vecini:
  - tipul de echipament (Ruter, Switch)
  - interfețele ruterelor cu care este conectat
  - interfețele sale folosite pentru conexiunile cu vecinii
  - modelul echipamentelor vecine

CDP este una dintre cele mai puternice unelte puse la dispoziția unui administrator de rețea de către Cisco. Acesta este folosit pentru monitorizarea și depanarea rețelelor.

Periodic, dispozitivele din rețea trimit vecinilor lor mesaje care conțin informații proprii, cum ar fi: tipul de dispozitiv (router, switch etc.), modelul dispozitivului sau interfața prin care se conectează cu vecinul. În funcție de sistemul de operare de pe un echipament și de tipul acestuia, CDP mai poate trimite informații despre hostname, versiunea de IOS, IP etc. Aceste mesaje se numesc CDP advertisements.

Este important de reținut faptul că CDP lucrează numai la Nivelul 2. În funcție de nivelul la care ne raportăm, conceptul de vecin diferă. Astfel:

•La Nivelul 3, două dispozitive sunt vecine dacă au aceeași adresă de rețea

•La Nivelul 2, două dispozitive sunt vecine dacă sunt direct conectate

Cum operează CDP

- Pornește automat după ce ruterul bootează
- Furnizează o serie de informații (hardware și software) despre vecinii echipamentului care folosește CDP:
  - identificatorii echipamentelor (numele)
  - identificatorii porturilor (locale și remote)
  - lista capabilităților (tipul de echipament)
  - platforma hardware

Comezile **`show cdp neighbors`** și **`show cdp neighbors detail`** oferă informații detaliate despre dispozitivele direct conectate. Acestea includ: hostname-ul, numele interfeței conectate, numele interfeței la care se conecteză, modelul dispozitivului și altele. CDP arată, de asemenea, adresa IP a dispozitivului vecin, chiar dacă un **`ping`** către dispozitivul respectiv nu are succes. Având în vedere faptul că, în multe situații, IP-ul unui dispozitiv este un lucru necesar pentru a începe o sesiune de telnet, CDP poate fi folosit cu succes pentru desenarea topologiei logice a unei rețele.

Pe de altă parte, informațiile oferite de CDP pot reprezenta o vulnerabilitate pentru o rețea. De aceea, este indicat, în unele situații, să se oprească protocolul CDP. Acest lucru se face cu ajutorul comenzii **`no cdp run`**, în modul global pentru întregul dispozitiv, sau pe o singură interfață prin comanda **`no cdp enable`**.

Exemplu CDP

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Ser 0/0            129        R S I      3640      Ser 1/0
Sw               Fas 0/0            133          S I      WS-2950   Fas 0/0
```

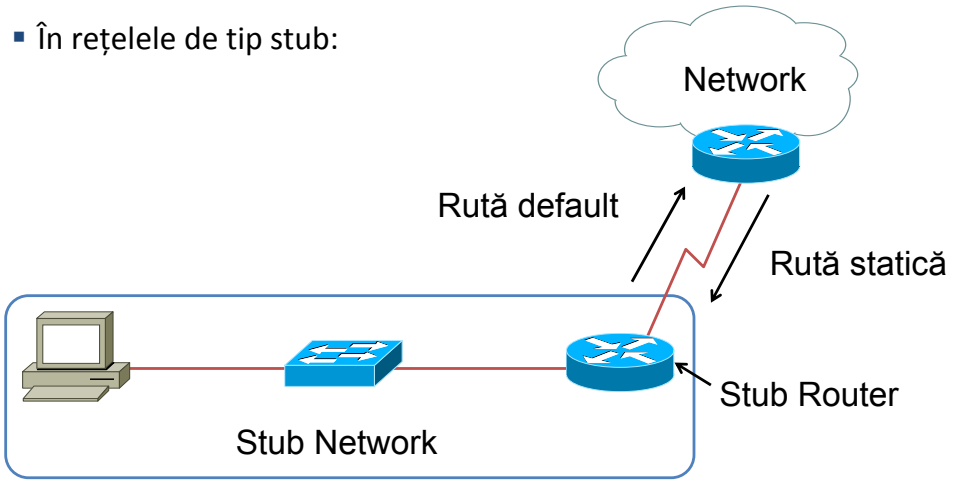
Output-ul comenzii **`show cdp neighbors`** oferă informații despre:

- Device ID: hostname-ul device-ului vecin
- Local interface**:** interfața locală la care este conectat dispozitivul vecin
- Holdtime: intervalul de timp în care ruterul va ignora update-urile primite despre o rețea care a devenit inaccesibilă
- Capability: tipul dispozitivului
- Platform: modelul dispozitivului
- Port ID: interfața vecinului la care este conectat echipamentul

Dacă între R1 și R2 ar exista un hub, acesta nu ar fi detectat de protocolul CDP.

Rol rute statice

- În rețelele de tip stub:



O rețea stub este o rețea care poate fi accesată doar printr-o singură rută. Astfel, în exemplu, dacă host-ul vrea să acceseze o destinație din afara rețelei sale, singurul mod de a face acest lucru este prin ruta R1-R2. De asemenea, dacă un host din afara rețelei stub vrea să acceseze un dispozitiv din interiorul rețelei, va putea face acest lucru numai prin intermediul rutei R2-R1.

În astfel de situații, folosirea unui protocol de rutare între cele două rutere ar fi redundant, deoarece există un singur mod prin care R1 poate trimite pachete în afara rețelei stub. Așadar, se va configura câte o rută statică pe fiecare ruter: o rută statică implicită din rețeaua stub spre ruterul vecin, iar apoi o rută statică de pe ruterul vecin spre rețeaua stub.

Principii de rutare

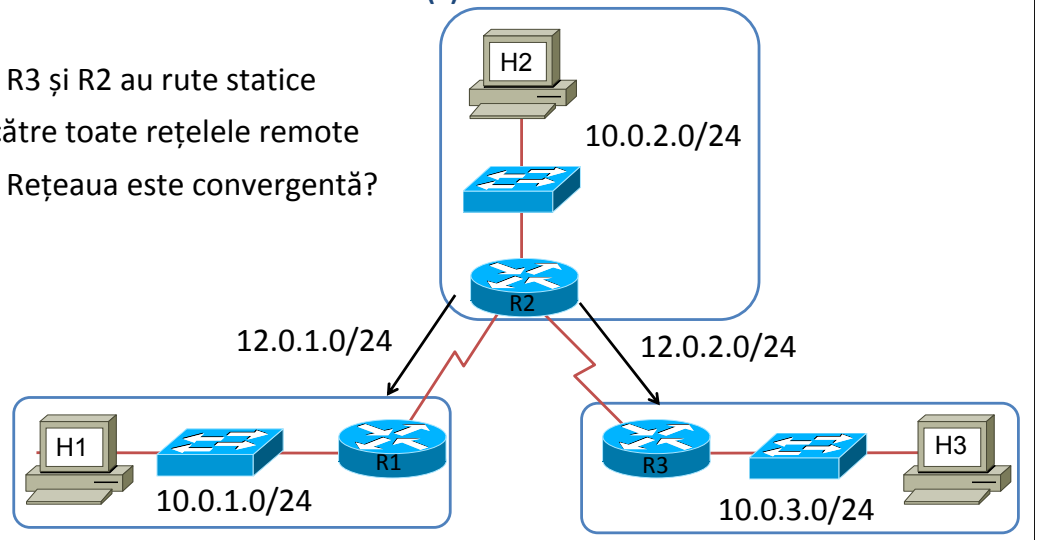
- Fiecare ruter ia deciziile de rutare independent, bazându-se pe informațiile aflate în tabela sa de rutare
- Dacă un ruter are anumite informații în tabela de rutare nu înseamnă că alte rutere au aceeași informație
- Informațiile de rutare despre o cale nu trebuie să fie aceleași pentru calea de întoarcere

Presupunând că un ruter R1 conține în tabela sa de rutare o serie de rute spre diverse destinații, orice decizie de transmitere a pachetelor va fi luată pe baza informațiilor deținute. R1 nu consultă tabelele de rutare ale vecinilor și nici nu cunoaște dacă ruterul la care va trimite pachetul are configurată o rută către destinație. În caz că adresa IP destinație a unui pachet face parte dintr-o rețea existentă în tabela de rutare, R1 va cunoaște doar către ce echipament vecin să trimită mai departe pachetul și eventual distanța până la destinație.

Dacă pachetul trimis trece printr-un ruter intermediar R2 pentru a ajunge la destinație, nu se garantează faptul că R2 va folosi aceeași cale de întoarcere prin R1. Există și posibilitatea ca R2 să nu cunoască nici o rută de întoarcere către expeditor. De aceea, este rolul administratorului de rețea să se asigure că toate destinațiile sunt accesibile.

Aplicarea principiilor (1)

- R3 și R2 au rute statice către toate rețelele remote
- Rețeaua este convergentă?



Dacă H2 trimite un pachet către H1, acesta va ajunge la destinație deoarece R2 are configurate rute statice către toate rețelele remote. Pachetul va ajunge la R1 care, fiind direct conectat cu H1, va ști să îl transmită. Totuși, dacă H1 vrea să îi răspundă lui H2, pachetul va fi aruncat fiindcă R1 nu are o rută configurată către rețeaua lui H2.
Se respectă așadar principiile de rutare: dacă R2 și R3 au rute configurate către toate rețelele remote, nu înseamnă că R1 știe despre acestea. Astfel, dacă R2 are o rută către rețeaua lui R1 nu înseamnă că R1 va ști să transmită un răspuns către R2. Aceeași problemă este valabilă și în cazul comunicației între dispozitivele H2 și H3.

În concluzie, nu există conectivitate între oricare două puncte ale rețelei, rețeaua nefiind convergentă. Soluția optimă pentru rezolvarea problemei de conectivitate este configurarea unei rute statice pe ruterele R1 și R3 cu destinația 10.0.2.0/24 sau a unei rute implicite spre ruterul R2.

Aplicarea principiilor (2)

- Tabelele de rutare corespunzătoare topologiei

```
R1#show ip route
  ***output omitted***
10.0.1.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C       12.0.1.0 is directly connected, Serial1/0
```

```
R2#show ip route
  ***output omitted***
10.0.0.0/24 is subnetted, 3 subnets
S       10.0.1.0 is directly connected, Serial1/0
C       10.0.2.0 is directly connected, FastEthernet0/0
S       10.0.3.0 is directly connected, Serial1/1
12.0.0.0/24 is subnetted, 2 subnets
C       12.0.1.0 is directly connected, Serial1/0
C       12.0.2.0 is directly connected, Serial1/0
```


Vizualizarea rutelor configurate se face prin afișarea conținutului tabelei de rutare. Astfel, comanda **`show ip route`** oferă multiple informații despre rutele existente:

•tipul rutei, identificat printr-un caracter, de exemplu caracterul S înseamnă rută statică, iar caracterul C înseamnă rețea direct conectată; orice alt caracter alfabetic diferit de S sau C semnifică protocolul de rutare dinamic prin care ruta a fost introdusă în tabela de rutare

•adresele rețelelor din tabela de rutare împreună cu masca de rețea folosită; masca de rețea va fi afișată în dreptul rețelei classful părinte sau în dreptul fiecărei rute

•tipul interfeței de ieșire sau adresa IP a următorului hop; în unele cazuri, vor fi afișate ambele elemente (atât interfața de ieșire cât și adresa IP a următorului hop)

Aplicarea principiilor (3)

```
R3#show ip route
  ***output omitted***
10.0.0.0/24 is subnetted, 3 subnets
S       10.0.1.0 is directly connected, Serial1/0
S       10.0.2.0 is directly connected, Serial1/0
C       10.0.3.0 is directly connected, FastEthernet0/0
12.0.0.0/24 is subnetted, 2 subnets
S       12.0.1.0 is directly connected, Serial1/0
C       12.0.2.0 is directly connected, Serial1/0
```

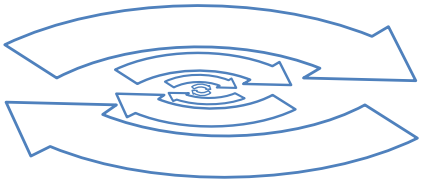

Din output-ul comenzii **`show ip route`**, introdusă pe ruterele R2 și R3, se observă faptul că acestea au configurate rute către toate rețelele din topologie, spre deosebire de R1 care cunoaște numai rețelele direct conectate cu acesta.

În momentul în care R1 trebuie să trimită un pachet drept răspuns la conexiunea inițializată cu ruterul R2, adresa IP destinație va face parte din rețeaua 10.0.2.0/24. Analizând tabela de rutare a ruterului R1, se observă că nu există nici o rută definită către această rețea. În absența configurării unei rute implicite, pachetul va fi ignorat, deci nu există conectivitate între rețeaua 10.0.1.0/24 și alte rețele remote.

Căutare recursivă în tabela de rutare

- Procesul are loc doar la instalarea rutei în tabela de rutare

Ruta statică este specificată prin următorul hop



Se caută următorul hop în tabela de rutare

```
 10.0.0.0/24 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
S       10.0.1.0 [1/0] via 10.0.0.2
```


Pentru ca un pachet să fie trimis mai departe de către un ruter, acesta trebuie, mai întâi, să găsească o cale a cărei adresă de rețea să corespundă adresei IP destinație a pachetului. Dacă un ruter primește un pachet destinat unei rețele care nu este direct conectată, acesta va căuta în tabela de rutare rețeaua destinație, iar apoi interfața pe care trebuie să trimită pachetul. Când ruterul trebuie să desfășoare mai multe căutări în tabela de rutare înainte să trimită un pachet, efectuează un proces cunoscut sub numele de căutare recursivă.

Eliminarea procesului de căutare recursivă se poate face prin definirea unei rute statice prin interfața de ieșire către destinație. Astfel, pentru descoperirea căii pe care un ruter trebuie să trimită un anume pachet se va realiza doar o singură căutare în tabelă. În cazul definirii unei rute cu adresa IP a următorului hop, ruterul va mai realiza o căutare în tabelă pentru a descoperi interfața de ieșire atașată acestuia.

Interfață de ieșire căzută

- Ruta statică este ștearsă din tabela de rutare dacă interfața de ieșire pentru aceasta nu funcționează

```
RT: interface FastEthernet0/0 removed from routing table
RT: del 10.0.0.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 10.0.0.0/24
RT: del 10.0.1.0/24 via 10.0.0.2, static metric [1/0]
RT: delete subnet route to 10.0.1.0/24
%LINK-5-CHANGED: Interface FastEthernet0/0,changed state to administratively down
```


Se poate întâmpla, din diverse motive, ca o interfață să devină inutilizabilă. În acest caz, rutele statice care aveau ca interfață de ieșire pe cea căzută vor fi șterse din tabela de rutare. Pentru instalarea și menținerea unei rute în tabela de rutare trebuie să existe în prealabil o configurație IP pentru cel puțin o interfață activă.

Procesul de ștergere a unei rute statice se poate urmări cu ajutorul comenzii **`debug ip routing`**. Se observă faptul că toate rutele care aveau ca interfață de ieșire pe cea căzută sunt șterse din tabela de rutare. Aceste rute vor fi reinserate în tabela de rutare doar dacă interfața va redeveni funcționabilă.

O rută poate fi configurată în așa fel încât să aibă asociată o interfață de ieșire, indiferent dacă rețeaua este direct conectată sau nu. Acest lucru micșorează timpul de căutare a căii destinație în tabela de rutare.

Rute statice

- Un router care decide să trimită pachete la următorul hop precizat într-o rută statică trebuie să seteze adresa MAC destinație a pachetului

În situația în care între două rutere există o conexiune de tip Ethernet, cadrul unui pachet va include câmpuri pentru adresarea MAC.

Când un ruter trebuie să trimită un pachet pe o interfață Ethernet, el va căuta adresa MAC corespunzătoare IP-ului destinație sau a ruterului „next-hop” în tabela sa ARP. Dacă nu este găsită nici o corespondență, ruterul va trimite un ARP request pe interfața Ethernet. Acest request este, de fapt, un broadcast care cere adresa MAC a dispozitivului destinație sau a „next-hop”-ului. Răspunsul va fi un pachet de tip ARP reply ce conține adresa MAC căutată, informație ce va fi introdusă în tabela ARP a dispozitivului care a solicitat request-ul. Pachetul este apoi încapsulat, folosind adresa MAC obținută, și trimis mai departe.

Rețelele seriale (point-to-point) conțin numai două dispozitive legate între ele, deci nu vor avea nevoie de o adresă de nivel 2 în momentul în care se trimite un pachet pe o interfață serială.

Ruta default

- Adăugând o rută default pachetele nu vor mai fi aruncate
  - orice pachet face match pe ruta default
- Când se folosește?
  - când nici o altă rută nu decide rutarea unui pachet
  - când un ruter are un singur punct de ieșire spre restul rețelei (stub router)

La primirea unui pachet, un ruter va compara adresa destinație cu adresele pe care le conține în tabela de rutare, verificând astfel dacă aceasta face parte din cadrul unei rețele cunoscute. Pachetul va fi trimis pe ruta cea mai specifică. De exemplu, dacă un pachet are destinația 192.168.0.3 și ajunge la un ruter care are în tabela sa de rutare rețelele: 192.168.0.0/24 și 192.168.0.0/16, pachetul va fi trimis spre prima rețea, deoarece 24 de biți se potrivesc cu adresa destinație, în comparație cu 16 biți în cazul celei de-a doua rețele.

O rută default este o rută care se potrivește oricărei destinații. Astfel, în momentul în care nici o rută din tabela de rutare nu se potrivește cu adresa destinație, pachetul va fi trimis pe ruta default în loc să fie aruncat. De asemenea, ruta default poate fi folosită și în cazul unei rețele de tip „stub”, deoarece orice pachet va fi trimis pe o singură cale de ieșire.

Comanda show interfaces

- Verificarea configurării interfețelor
  - **#show interfaces [tip_interfață număr_interfață]**

```
R1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is cc00.140c.0000 (bia cc00.140c.0000)
  Internet address is 10.0.0.1/24

R1#show interface serial 1/0
Serial1/0 is administratively down, line protocol is down
```


Comanda **show interfaces** oferă informații detaliate despre starea interfețelor existente pe un ruter. Comanda poate fi introdusă fără parametri suplimentari, caz în care va afișa, sub forma unei liste, detalii despre toate interfețele instalate pe echipament, sau se poate specifica denumirea unei interfețe ca argument pentru un output mai specific. În primul rând, comanda va verifica dacă interfața este activă și dacă protocolul de nivel 2 funcționează. În output se mai afișează și adresa IP asociată interfeței, adresa MAC și modelul fizic al acesteia.

Pentru un output mai succint și mai bine organizat se poate folosi comanda **show ip interface brief**. Informațiile afișate astfel reprezintă o modalitate utilă pentru verificarea funcționalității interfețelor și corectitudinii configurării adreselor IP.

Comanda show interfaces (2)

- Probleme Layer1
  - cablu deconectat

```
R1#show interface serial 1/0
Serial1/0 is down, line protocol is down
```

- Probleme Layer2
  - interfața serială nu primește semnal de ceas

```
R1#show interface serial 1/0
Serial1/0 is up, line protocol is down
```


Comanda **`show interfaces`** poate fi folosită cu succes pentru depanarea problemelor de conectivitate dintr-o rețea, datorate unei interfețe inactive sau unor inconsistențe în configurarea IP-urilor.

Dacă în output este specificat că interfața este „down” atât la nivel de linie, cât și la nivel de protocol, înseamnă fie că un cablu este deconectat sau defect, fie că interfața dispozitivului de la celălalt capăt al legăturii este în modul „shutdown”.

În cazul în care output-ul indică doar protocolul de linie ca fiind „down”, acest lucru reprezintă o problema la nivelul 2, de exemplu faptul că nu a fost setată valoarea clock-rate-ul pentru sincronizarea interfețelor seriale HDLC.

Examinarea interfețelor seriale

- Verificarea DCE/DTE
  - **#show controllers [tip_interfață număr_interfață]**

```
R1#show controllers serial 1/0
M4T: show controller:
PAS unit 0, subunit 0, f/w version 1-45, rev ID 0x2800001, version 1
idb = 0x64090F0C, ds = 0x64091FD4, ssb=0x64092390
Clock mux=0x0, ucmd_ctrl=0x0, port_status=0x7B
Serial config=0x8, line config=0x200
maxdgram=1608, bufpool=78Kb, 120 particles
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
line state: down
cable type : V.11 (X.21) DCE cable, received clockrate 2015232
```


Conexiunile seriale sunt realizate considerând un capăt al legăturii de tip DCE (Data Comunications Equipment) și celălalt capăt de tip DTE (Data Terminal Equipment). Interfețele seriale Cisco sunt, în mod normal, DTE, dar pot fi configurate pentru a se comporta ca DCE.

Pentru a configura interfața unui ruter ca DCE se conectează capătul DCE al cablului la interfață, pe care apoi se va stabili o valoare numerică pentru clockrate.

În general, conectorii cablurilor seriale sunt marcați vizual ca fiind de tip DCE sau DTE. Un alt mod de a deosebi cele două modele este faptul că DTE are conector de tip „male”, iar cel DCE, de tip „female”.

Comanda folosită pentru a vizualiza dacă un capăt al unei conexiunii seriale este de tip DTE sau DCE este **show controllers** menționând ca parametru identificatorul interfeței respective.

Configurarea interfețelor seriale

- Configurarea parametrului **clock-rate** pe interfețele seriale
  - interfeţele seriale necesită configurarea vitezei de comunicaţie (clockrate), pentru a putea funcţiona
  - echipamentul care dă tactul de ceas trebuie sa fie DCE
  - **(config-if)#clock rate <valoare>**

Configurarea parametrului clock-rate, adică a vitezei de transmisie a datelor pentru sincronizarea echipamentelor de la cele două capete ale legăturii seriale va avea efect numai în cazul interfețelor de tip DCE. Dacă se setează o valoare pentru clock-rate pe interfața DTE, sistemul de operare va ignora comanda introdusă.

Valorile numerice care pot fi atribuite clock-rate-ului (în biți pe secundă) sunt: 1.200, 2.400, 9.600, 19.200, 38.400, 56.000, 64.000, 72.000, 125.000, 148.000, 500.000, 800.000, 1.000.000, 1.300.000, 2.000.000, 4.000.000 sau 8.000.000. Nu este necesară reținerea valorilor exacte a ceasului, deoarece în cadrul configurării acesteia, poate fi introdusă orice valoare non standard între 300 și 8.000.000, iar sistemul de operare va ajusta numărul introdus la cea mai apropiată valoare suportată de către echipamentul hardware. În mod implicit, o interfață DCE nu are configurat semnalul de ceas, acest lucru fiind semnalat prin starea „down” a protocolului de linie.

Troubleshooting

- Verificarea introducerii rutelor în tabela de rutare
  - **#debug ip routing**

```
R1#debug ip routing
IP routing debugging is on
R1#configure terminal
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
 RT: interface FastEthernet0/0 removed from routing table
 RT: delete subnet route to 10.0.0.0/24
 RT: NET-RED 10.0.0.0/24
 %LINK-5-CHANGED: Interface FastEthernet0/0,changed state to
        administratively down
R1(config-if)#no shutdown
 RT: interface FastEthernet0/0 added to routing table
 %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,changed state
         to up
```


Spre deosebire de comanda **show**, comanda **debug** este folosită pentru monitorizarea operațiilor efectuate de ruter în timp real. Comanda **debug ip routing** urmărește fiecare schimbare făcută de ruter, în procesul de rutare.

Astfel, dacă o interfață din rețea devine inactivă, **debug ip routing** va arăta faptul că orice rută care folosea interfața de iesire respectivă a fost ștearsă. De asemenea, comanda va afișa și fiecare interfață/rută nou adăugată în tabela de rutare.

Procesele **debug** consumă o mare parte din procesor atunci când sunt activate. De aceea este recomandat să fie folosite numai la depanarea rețelelor și să se păstreze un număr cât mai mic de procese **debug** pornite, dezactivându-se cele care nu sunt necesare.

Pentru a închide toate procesele **debug** activate se folosește comanda **no debug all**, sau comanda cu același efect, **undebug all**.

Comenzi CDP

- Afișarea vecinilor

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Ser 1/0            129        R S I      3640      Ser 1/0
R2               Fas 0/0            178        R S I      3640      Eth 0/0
```

- Afișarea informațiilor de Layer3 și a capabilităților vecinilor

```
R1#show cdp neighbors detail
-------------------------
Device ID: R2
Entry address(es):
  IP address: 10.0.0.2
Platform: Cisco 3640,  Capabilities: Router Switch IGMP
Interface: Serial1/0,  Port ID (outgoing port): Serial1/0
Holdtime : 160 sec

Version :
Cisco IOS Software, 3600 Software (C3640-JS-M), Version 12.4(12)
```


CDP reprezintă o unealtă puternică pentru monitorizare și depanare care lucrează la nivelul 2 al stivei OSI (nivelul legătură de date). Cu ajutorul CDP se pot descoperi și monitoriza vecinii de nivel 2 ai unui dispozitiv de rețea. Așadar, nu este necesară configurarea unei adrese IP pe interfețe, protocolul CDP funcționând atâta timp cât interfețele nu se află în modul „administratively down”.

Comanda **`show cdp neighbors`** va afișa informații despre vecinii de nivel 2 ai echipamentului în formatul: numele dispozitivului vecin, interfața conectată către vecin, timpul, în secunde, până la expirarea informației învățate prin mesaje de tip cdp advertisments, tipul dispozitivului, modelul și interfața vecinului la care se conectează echipamentul.

Comanda **`show cdp neighbors detail`** va returna și informații de nivel mai înalt, de exemplu adresa IP sau versiunea sistemului de operare existent.

Comenzi CDP (2)

- Pornirea protocolului pe interfață
  - `(config-if)#cdp enable`
- Pornirea protocolului din modul global
  - `(config)#cdp run`
- Oprirea protocolului pe interfață
  - `(config-if)#no cdp enable`
- Oprirea protocolului din modul global
  - `(config)#no cdp run`

Protocolul CDP poate fi pornit atât pentru o singură interfață cât și pentru întregul echipament. Pentru pornirea sa numai pe o interfață, din modul **`configure interface`** se va folosi comanda **`cdp enable`**. Pentru a porni CDP pe tot dispozitivul, în modul global de configurare se tastează comanda **`cdp run`**.

Având în vedere faptul că informațiile furnizate de CDP se pot dovedi o vulnerabilitate față de siguranța rețelei, protocolul poate fi oprit, pe o interfață sau la nivel global, pe întregul dispozitiv. Pentru a opri CDP pe o interfață se va folosi **`no cdp enable`** în modul de configurare al interfeței dorite iar pentru a opri CDP în totalitate, se utilizează comanda **`no cdp run`** din modul global de configurare.

CDP trimite implicit informații despre dispozitivul local pe toate interfețele și poate fi folosit la explorarea unei rețele nedocumentate, permițând detectarea echipamentelor și conexiunilor dintre acestea.

Configurarea rutelor statice

- Sintaxa comenzii **ip route**
  - **(config)#ip route adresă-rețea subnet-mask {adresă-ip | interfață-de-ieșire}**
- Configurarea rutei statice default
  - **(config)#ip route 0.0.0.0 0.0.0.0 {adresă-ip | interfață-de-ieșire}**
- Nu se pune doar interfața de ieșire în cazul rețelelor multi-acces, trebuie obligatoriu next-hop

Pentru a adăuga o rețea remote în tabela de rutare a unui ruter în mod static, se va folosi comanda **ip route**. Aceasta va primi ca parametri adresa rețelei remote, masca ei de rețea, și adresa ip a ruter-ului „next-hop” sau interfața de ieșire.

Se poate verifica adăugarea noii rute prin activarea procesului **debug** sau prin folosirea comenzii **show ip route** după adăugarea rutei.

În cazul unei rețele „stub” este recomandată configurarea unei rute default deoarece pachetele pot ieși din rețea doar pe o singură cale. Ruta default va avea adresa de rețea 0.0.0.0 și masca /0.

În cazul rețelelor multi-access se va configura adresa IP a următorului hop deoarece doar prin configurarea interfeței de ieșire ruterul nu va avea suficiente informații pentru a determina dispozitivul „next-hop”. Așadar, fără a cunoaște ip-ul „next-hop-ului”, ruterul nu va ști ce adresă MAC destinație să încapsuleze în cadrul Ethernet de nivel 2.

Rute statice cu interfețe Ethernet

- Rețeaua Ethernet este multi-acces
  - nu se poate specifica doar interfața de ieșire pentru că pot exista mai multe destinații pe aceeași interfață
  - trebuie să se specifice next-hop

- Configurarea rutei

```
R1(config)#ip route 10.0.1.0 255.255.255.0 fastEthernet 0/0 10.0.0.2
```

- Afișarea rutei

```
S       10.0.1.0 [1/0] via 10.0.0.2, FastEthernet0/0
```


Spre deosebire de o rețea point-to-point, cu interfețe seriale, care include doar două device-uri (cele două rutere conectate între ele), o rețea Ethernet poate conține, pe lângă rutere, și alte dispozitive (switch-uri, host-uri), ceea ce înseamnă că rețeaua Ethernet este o rețea multi-acces. În aceste condiții, trebuie ca rutele statice către rețelele remote să fie făcute prin adresa IP „next-hop”. Pentru o bună funcționare a rutelor statice configurate, se recomandă specificarea ambelor căi de ieșire pentru o anumită rută (interfață de ieșire și adresă IP „next-hop”).

Comanda **`ip route`** va include la parametri adresa rețelei remote, masca acesteia, interfața pe care se trimite pachetul către rețea și IP-ul interfeței. Specificarea interfeței este opțională. În cazul în care nu este specificată interfața, ruterul va căuta rețeaua următorului hop în tabela de rutare și va folosi interfața direct conectată la acesta.

Rutele statice în tabela de rutare

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 2 subnets
S       172.16.0.0 is directly connected, Serial1/0
S       172.16.1.0 is directly connected, Serial1/0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
S       10.0.1.0 [1/0] via 10.0.0.2
     12.0.0.0/24 is subnetted, 1 subnets
C       12.0.0.0 is directly connected, Serial1/0
S*   0.0.0.0/0 is directly connected, Serial1/0
```


Tabela de rutare se vizualizează cu ajutorul comenzii **`show ip route`**, care produce afișarea tuturor rutelor existente, fie ele direct conectate, învățate în mod static sau prin protocoale de rutare.

Output-ul generat include tipul rutei, adresa rețelei accesibile prin ruta menționată, tipul conexiunii, interfața pe care se realizează conexiunea și, dacă este cazul, metrica. Tipul unei rute existente în tabelă este specificat prin prezența unui caracter alfabetic în dreptul fiecărei rute. Astfel, o rută statică este indicată de caracterul „S” a cărui semnificație este prezentată în legenda afișată în prima parte a output-ului comenzii introduse.

În cazul configurării unei rute statice default, aceasta va fi indicată de cararterul „S” urmat de caracterul „*” la începutul liniei pe care este afișată, dar și de prezența mesajului **`Gateway of last resort is 0.0.0.0 to network 0.0.0.0`**.

Modificarea unei rute statice

- Nu se poate modifica o rută statică deja creată
  - se va șterge și se va crea o alta

```
R1(config)#no ip route 172.16.1.0 255.255.255.0 serial 1/0
R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.0.1
```


Odată creată o rută statică, singurul mod în care i se pot aduce modificări este ștergerea și recrearea acesteia. Pentru a șterge o rută statică se folosește aceeași comandă prin care a fost adăugată, precedată de negația **no**. Se va crea, apoi, o nouă rută statică specificând modificările dorite.

Verificarea configurării corecte a rutelor se poate face prin două metode: afișarea fișierului de configurare „running-config” sau vizualizarea tabelei de rutare. Comanda introdusă pentru setarea unei rute statice va fi prezentă în running-config chiar dacă ea nu apare în tabela de rutare (posibil din cauză că interfața atașată ruterului nu este activă, sau nu are configurată în prealabil o adresă IP).

Rute statice sumarizate

- Se sumarizează, acolo unde este posibil, pentru a avea tabele de rutare cu mai puține intrări
  - rutele nesumarizate trebuie șterse

```
ip route 172.16.1.0 255.255.255.0 Serial0/0/1
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

```
ip route 172.16.0.0 255.255.252.0 Serial0/0/1
```


Conceptul de sumarizare a fost introdus pentru a ajuta la micșorarea tabelelor de rutare, eficientizând astfel procesul de dirijare a pachetelor. Acest concept constă în reducerea mai multor rețele mici la o rețea mai mare, păstrând astfel o singură rețea echivalentă în tabela de rutare. Este important de reținut faptul că sumarizarea se face doar pentru acele rute care au asociată aceeași interfață de ieșire sau aceeași adresă IP „next-hop”.

Procesul de sumarizare se face conform următoarelor reguli:

•Se scriu adresele de rețea în binar

•Se numără biții comuni de la stânga la dreapta

•Masca noii rețele va reprezenta numărul de biți comunii între rețelele inițiale

•Rețeaua rezultată reprezintă rețeaua sumarizată a rutelor inițiale

Troubleshooting pentru rute statice

- Afișarea tabelei de rutare
  - **show ip route**
- Afișarea statusului interfețelor de pe router
  - **show ip interface brief**
- Verificarea conectivității Layer2 cu vecinii
  - **show cdp neighbors detail**
- Testarea accesului între sursă și destinație
  - **ping**
- Testarea traseului de la sursă la destinație
  - **traceroute**

Există multe probleme care pot apărea într-o rețea, de la căderea unei interfețe până la o comandă greșit introdusă de administrator. În aceste cazuri conectivitatea rețelei poate fi ușor compromisă. Rolul administratorului de rețea este să rezolve astfel de potențiale situații apărute. În acest scop există mai multe unelte care pot ajuta la depanarea rețelei:

• **show ip route** – oferă informații detaliate despre starea interfețelor și a rutelor active din tabela de rutare

• **show ip interface brief** – afișează sumar starea interfețelor

• **show cdp neighbours detail** – oferă informații detaliate despre toate dispozitivele direct conectate cu echipamentul local

• **ping** - testează conectivitatea dintre două dispozitive

• **traceroute** – identifică locația unde se poate bloca un pachet între sursă și destinație, afișând adresele parcurse de pachet

Mesaje de logging

- Mesaje privind schimbări în configurație, erori, alerte, etc.
- Sincronizarea afișării logurilor cu promptul
  - **(config-line)#logging synchronous**

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
                 administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
                 changed state to down
R1(config-if)#
```


De multe ori, sistemul de operare afișează diverse mesaje informative fără a fi solicitate de administrator (schimbarea descrierii unei interfețe generează un mesaj). Aceste mesaje pot crea unui administrator de rețea posibile dificultăți de vizualizare în momentul introducerii diferitelor comenzi de configurare. Deși aceste mesaje nu afectează comenzile utilizatorului în nici un fel, ele pot fi derutante, lucru pentru care se obișnuiește să se separe mesajele sistemului de operare de comanda care este scrisă. Acest lucru se realizează automat după introducerea comenzii **`logging synchronous`** în modul **`config-line`** accesat prin comanda **`line console 0`**.

Tabela de rutare (clasificare rute)

Tabela de rutare (1)

- Organizare ierarhică
- Rutele sunt stocate pe nivele
- Conține:
  - adresele rețelelor direct conectate
  - rute statice
  - rute învățate prin protocoale de rutare dinamice

Tabela de rutare (2)

- Exemplu

```
Router#show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demand routing, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2   10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E      10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
    172.110.0.0 is variably subnetted, 2 subnets, 2 masks
C      172.110.232.32/28 is directly connected, Ethernet0
S      172.110.0.0/16 is directly connected, Ethernet0
```

Tabela de rutare (3)

- Deși tabela suportă atât adresare classful cât și classless, structura ei este bazată pe adresarea classful
- Ierarhizarea tabelei ajută la determinarea rapidă a căii pe care să fie trimis pachetul
- Rutele sunt organizate pe două niveluri

Level 1 Routes

- Au masca de rețea mai mică sau egală cu masca classful a rețelei
- Pot funcționa ca:
  - „Default Route”

```
S*    0.0.0.0 [1/0] via 192.168.1.2
```

  - „Supernet Route” (masca de rețea strict mai mică decât masca classful)

```
C    192.168.2.0/22 is directly connected, Ethernet0
```

  - „Network Route” (masca de rețea egală cu masca classful)

```
C    128.137.0.0/16 is directly connected, Ethernet0
```

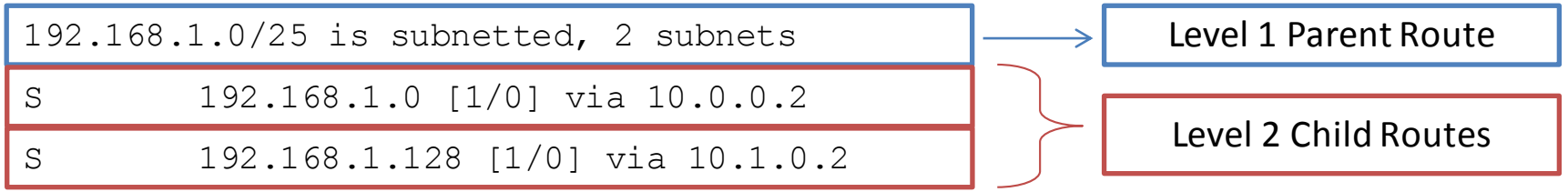
Ultimate Routes

- Rutele care includ:
  - o adresă next-hop
  - și/sau o interfață de ieșire
- Pot fi atât rute Level 1 cât și rute Level 2
- Exemplu

```
S*   192.168.2.0 [1/0] via 192.168.1.2
                  is directly connected, FastEthernet1/0
```

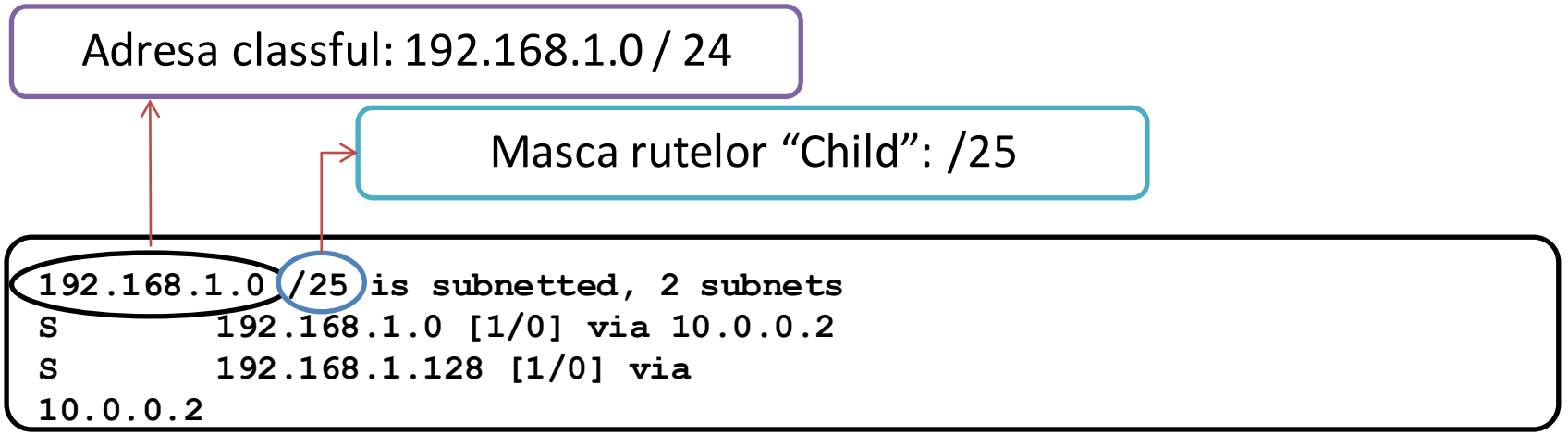
Parent & Child Routes

- Parent route
  - rută Level 1
  - nu conține o adresă destinație sau o interfață de ieșire
  - este adăugată automat când este introdusă în tabelă o subrețea a unei rețele classful (rută Level 2)
- Child route
  - rută Level 2
  - reprezintă o subrețea a unei rețele classful
  - conține o adresă destinație și/sau o interfață de ieșire



Parent & Child Routes: Classful

- Adresa rețelei din ruta „Parent” este adresa clasei majore
- Masca de rețea a rutei „Parent” este masca pentru rutele sale „Child”

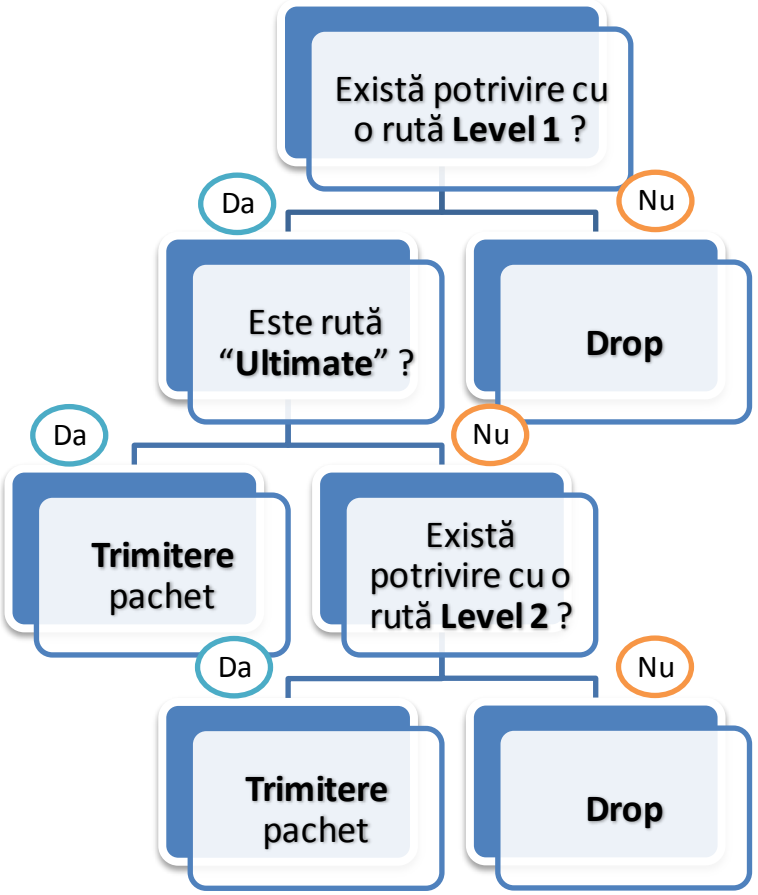


Parent & Child Routes: Classless

- Adresa și masca rețelei din ruta „Parent” corespund clasei majore
- Este precizat numărul de subrețele și numărul de măști folosit
- Fiecare subrețea specifică adresa subrețelei și masca

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.4/30 is directly connected, Serial0/0/0
C       172.16.1.8/30 is directly connected, Serial0/0/1
C       172.16.1.16/24 is directly connected, Serial0/1/0
```

Căutarea în tabela de rutare (Classful)



Căutarea în tabela de rutare (Classless)