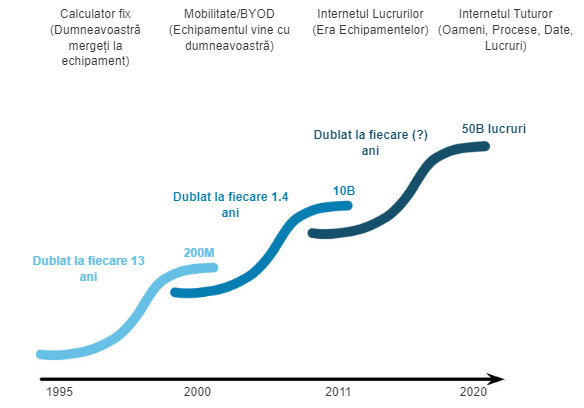
# Capitolul 1. Explorarea Reţelei

**Conectare globală**

## Interconectarea din ziua de astăzi



**Să schimbăm modul în care comunicăm**

Globalizarea internetului a vestit noi forme de comunicare care permit oamenilor să creeze informații ce pot fi accesate de către o audiență globală.

Unele forme de comunicare includ:

* **Mesageria instantă (IM)**Mesageria instantă permite comunicare în timp real între două sau mai multe persoane. Multe aplicații de IM încorporează facilități precum transfer de fișiere. Aplicațiile IM pot oferi facilități adiționale precum comunicare cu ajutorul vocii și a camerelor web.
* **Socializare Media** Socializarea media constă în site-uri web interactive unde oameni și comunități creează și partajează conținut generat de utilizatori cu prieteni, familie, parteneri și întreaga lume.
* **Unelte de colaborare**Uneltele de colaborare oferă oamenilor oportunitatea de a lucra împreună pe documente partajate. În lipsa constrângerilor de locație sau fus orar, persoanele conectate la un sistem comun pot vorbi unele cu celelalte, deseori prin intermediul clipurilor video interactive și în timp real. Prin intermediul rețelei, ei pot partaja text și grafice și pot edita documente împreună. Cu ajutorul uneltelor de colaborare disponibile, organizațiile pot să reacționeze rapid pentru a distribui informații și a atinge scopuri. Larga distribuție a rețelelor de date înseamnă că oameni din locații îndepărtate pot lucra în mod regulat cu oameni din centrul unor mari aglomerări urbane.
* **Bloguri**Blogurile sunt pagini web ușor de actualizat și editat. Spre deosebire de site-urile web comerciale, care sunt realizate de profesioniști experți în comunicare, blogurile permit oricui să își comunice gândurile unei audiențe globale fără a avea cunoștințe tehnice de web design. Există bloguri pe aproape orice temă, iar comunitățile oamenilor se formează deseori în jurul autorilor populari.
* **Wiki-uri**Wiki-urile sunt pagini web pe care grupuri de oameni le pot edita și vizualiza împreună. În timp ce un blog aparține unui individ, asemănător unui jurnal personal, un wiki reprezintă o creație de grup. De aceea, acesta poate fi supus unor editări și analize extensive. Asemenea blogurilor, wiki-urile pot fi create în etape, și de către oricine, fără sponsorizarea din partea unei mari companii comerciale. Wikipedia a devenit o resursă cuprinzătoare - o enciclopedie disponibilă pe internet - de subiecte rezultate în urma contribuției publicului. Organizații private și indivizi își pot crea propriile wiki-uri pentru a concentra toate cunoștințele din jurul unui subiect. Multe afaceri utilizează wiki-uri ca platforme de colaborare internă. Odată cu globalizarea internetului, oameni aparținând tuturor categoriilor sociale pot contribui la wiki-uri și își pot adăuga propriile perspective și cunoștințe unei resurse partajate.
* **Distribuire de fișiere multimedia în internet**Distribuirea de fișiere multimedia în internet (podcasting) reprezintă un mediu audio de calitate medie care inițial a permis oamenilor să înregistreze materiale audio și să le convertească pentru a fi utilizate. Podcasting-ul permite oamenilor să distribuie propriile înregistrări unei audiențe largi. Fișierul audio este încărcat pe un site web (sau blog, sau wiki) de unde alții îl pot descărca și îl pot asculta pe propriile calculatoare personale, laptopuri și alte dispozitive mobile.
* **Distribuirea de fișiere prin parteneri (Peer-to-Peer)**Distribuirea de fișiere prin parteneri permite oamenilor să partajeze fișiere între ei, fără a fi nevoiți să le stocheze și să le descarce de pe un server central. Utilizatorul se alătură rețelei P2P instalând o aplicație software P2P. Aceasta îi permite să delimiteze și să distribuie fișiere alături de alte persoane din rețeaua de parteneri. Diversificarea digitizării fișierelor media, precum muzică sau filme, a crescut interesul în partajarea de fișiere P2P. Distribuirea de fișiere P2P nu a fost adoptată de către toată lumea. Multe persoane sunt îngrijorate de încălcarea drepturilor de autor.

## Furnizarea de resurse într-o rețea

Rețelele sunt de diferite dimensiuni:

Rețelele simple instalate în gospodării permit partajarea resurselor precum imprimante, documente, fotografii și muzică între câteva calculatoare locale.



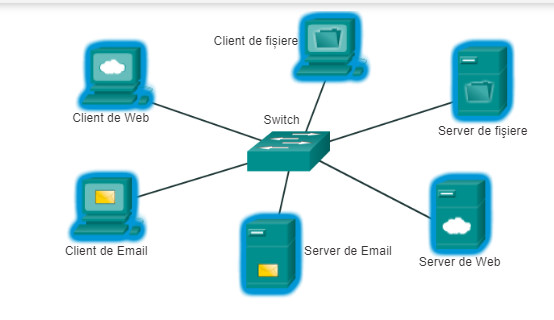
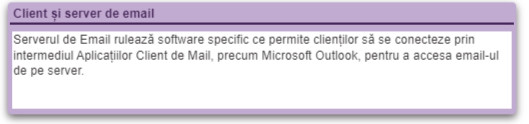
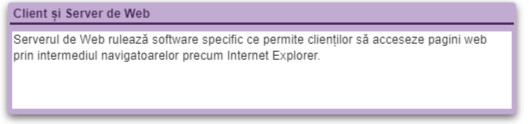
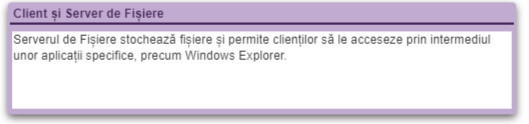
Rețelele mici pentru acasă și birou (SOHO) sunt deseori configurate de către indivizi care lucrează de acasă sau dintr-o locație la distață din nevoia de a se conecta la rețeaua de la serviciu sau la alte resurse centralizate.

Rețele de dimensiuni Medii sau Mari, precum cele folosite de către corporații sau școli, pot avea mai multe sublocații cu sute sau mii de calculatoare interconectate.



Internetul este o rețea de rețele interconectate ce conectează milioane de calculatoare din întreaga lume.

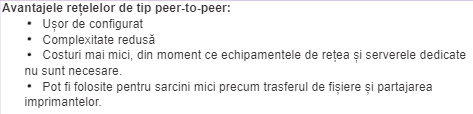
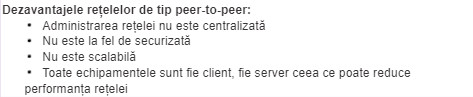
**Clienți și servere**

**** ****  

RR

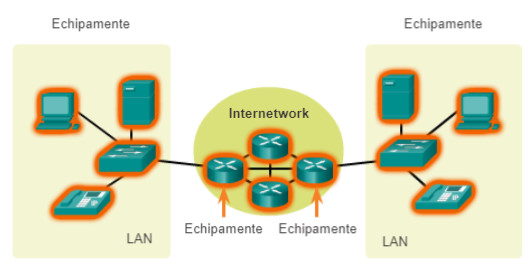
**Rețea de tip peer-to-peer**

Software-ul de tip client sau server rulează de obicei pe calculatoare diferite, dar este posibil ca un calculator să îndeplinească ambele roluri în același timp. În rețele mici și case, multe calculatoare funcționează ca servere și clienți în rețea. Acest tip de rețea este numit o rețea peer-to-peer.

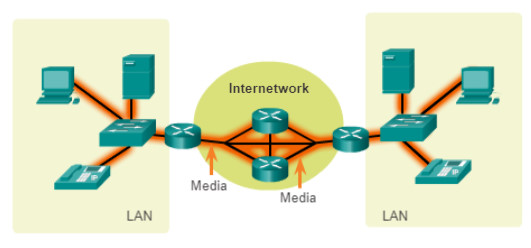
**** ****

## Componentele unei rețele

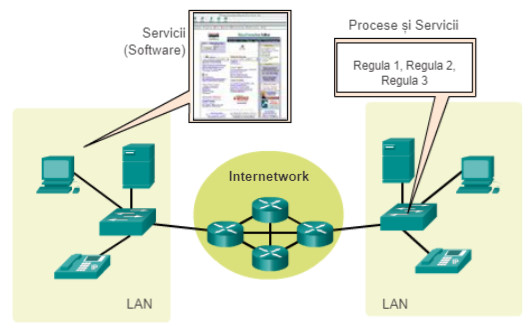
Echipamente:



Mediu:



Servicii:



**Echipamente finale**

Unele exemple de echipamente finale sunt:

* Calculatoare (stații de lucru, laptopuri, servere de fișiere, servere web)
* Imprimante de rețea
* Telefoane IP
* Terminal pentru TelePresence
* Camere video pentru securitate
* Dispozitive mobile (precum telefoane inteligente, tablete, PDA-uri, cititoare de carduri de credit/debit fără fir și cititoare de coduri de bare)

**Echipamente intermediare**

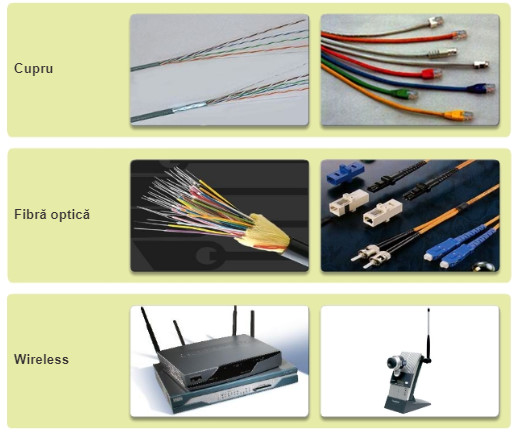
Iată câteva exemple de echipamente intermediare de rețea:

* Accesul la rețea (switch-uri și access point-uri wireless)
* Interconectarea rețelelor (routere)
* Securitate (firewall-uri)

Procesele care rulează pe echipamentele intermediare de rețea realizează aceste **funcții**:

* Regenerează și retransmit semnalele de date
* Mențin informații referitoare la căile existente în rețea și între rețele
* Înștiințează alte echipamente despre erori și eșuări de comunicare
* Direcționează datele pe alte căi atunci când există o legătură avariată
* Clasifică și direcționează mesaje conform cu prioritățile specificate de QoS (Quality of Service - calitatea serviciului)
* Permit sau interzic trecerea datelor pe baza setărilor de securitate

**Medii de transmisie**

****

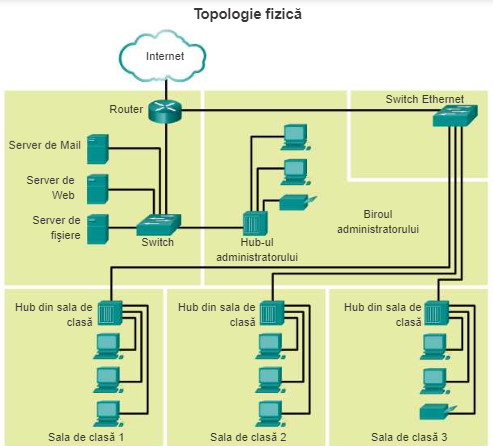
**Criteriile pe baza cărora alegem mediul de transmisiune sunt:**

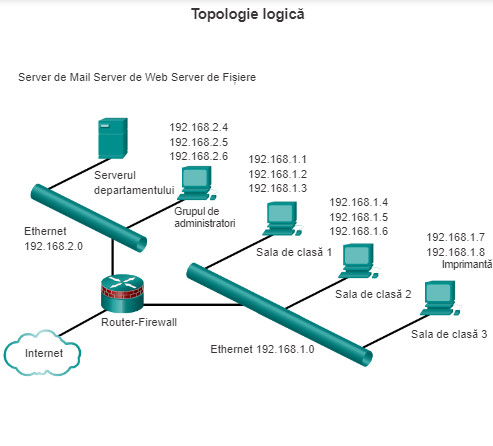
* Distanța pe care un mediu o poate acoperi pentru a transmite un semnal.
* Mediul fizic în care mediul de transmisiuni va fi instalat.
* Cantitatea de date și viteza la care trebuie să fie transmise.
* Costul mediului și instalarea

**Diagrame ale topologiilor**

Există două tipuri de diagrame ale topologiilor inclusiv:

* **Diagrame ale topologiilor fizice**- Identifică locația fizică a dispozitivelor intermediare, a porturilor configurate și a cablurilor .
* **Diagrame ale topologiilor logice**- Identifică dispozitive, porturi și scheme de adresare IP

****

****

## LAN-uri și WAN-uri

**Tipurile de rețele**

* **Rețea locală (Local Area Network - LAN)**- O infrastructură de rețea care asigură accesul utilizatorilor și echipamentelor finale într-o zonă geografică restrânsă.
* **Wide Area Network (WAN)**- O infrastructură de rețea care asigură accesul la alte rețele pe o arie geografică mare.
* **Metropolitan Area Network (MAN)**- O infrastructură de rețea care acoperă o arie fizică mai mare decât cea a unui LAN, dar mai mică decât cea a unui WAN (exemplu: un oraș) Rețelele de tip MAN sunt controlate de obicei de către o singură entitate precum o organizație mare.
* **Wireless LAN** **(WLAN)**- Similar unui LAN, acesta interconectează utilizatori și dispozitive finale dintr-o zonă geografică restrânsă fără fir.
* **Storage Area Network (SAN)**- O infrastructură de rețea concepută pentru a suporta servere de fișiere și a asigura stocare de date, dar și regăsire și replicare. Acestea implică servere de top, mai multe formații de de discuri și interconectări pe bază de fibră optică.

**LAN-uri**

Un LAN are o infrastructură care acoperă o zonă restrânsă de rețea. Anumite caracteristici ale LAN-urilor includ:

* **LAN-urile** interconectează echipamentele finale într-o zonă limitată precum școală, domiciliu, campus.
* **LAN-urile** furnizează lățimea de bandă de viteză mare către echipamentele finale interne și către cele intermediare.

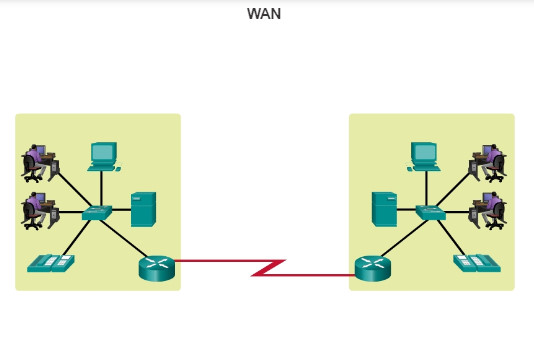
****

**Wide Area Networks**

Wide Area Networks (WAN-uri) sunt o infrastructură de rețea care se întind pe o zonă geografică de dimensiuni foarte mari. WAN-urile sunt gestionate de obicei de furnizorii de servicii (service providers-SP) sau de furnizorii de servicii de Internet (Internet Service Providers-ISP).

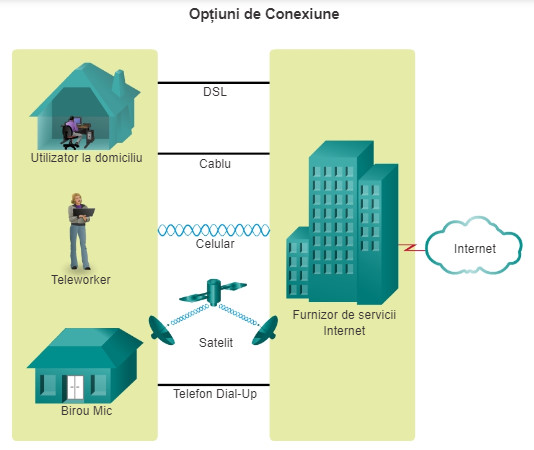
Caracteristicile specifice ale WAN-urilor includ:

* WAN-urile interconectează LAN-urile pe zone geografice de dimensiuni mari precum între orașe, țări, provincii sau continente.
* WAN-urile sunt de obicei administrate de mai mulți furnizori de servicii.
* WAN-urile furnizează de obicei link-uri de viteză scăzută între LAN-uri.

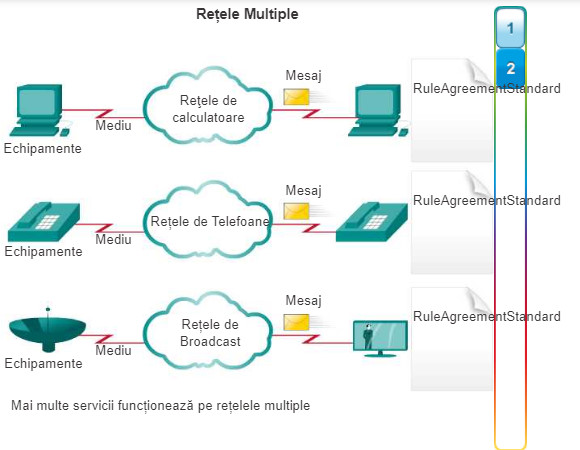
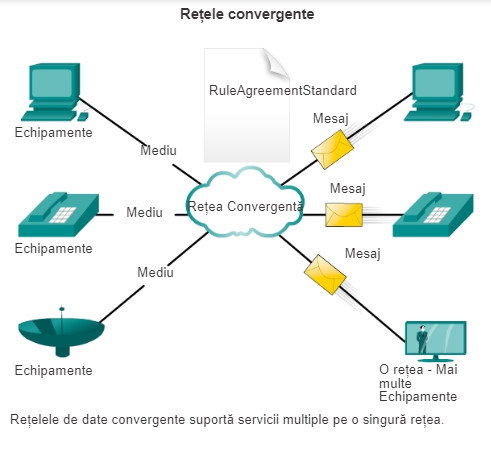
****

**Conectarea utilizatorilor Remote la Internet**

* **Cablu**Oferit de obicei de furnizorii de servicii de cablu TV, semnalul de date este transportat prin același cablu coaxial care furnizează și televiziunea prin cablu. Se oferă o lățime de bandă ridicată și o conexiune permanentă la Internet. Un modem de cablu special separă semnalul de date de pe Internet de celelalte semnale din cablu și furnizează o conexiune Ethernet la un host sau LAN.
* **DSL**Furnizează o lățime de bandă mare și o conexiune permanentă la Internet. Această opțiune de conectare folosește un modem de viteze ridicate ce separă semnalul DSL de semnalul de telefonie și asigură o conexiune Ethernet către calcuatorul local sau către un LAN. DSL folosește o linie telefonică ce se împarte în trei canale. Un canal este utilizat pentru apeluri telefonice cu voce. Acesta permite unei persoane să primească un apel telefonic fără a se deconecta de la Internet. Al doilea canal este un canal de descărcare mai rapidă, folosit pentru a primi infromații de la Internet. Al treilea canal este utilizat pentru încărcarea informațiilor. Acest canal este de obicei puțin mai lent decât cel de descărcare. Calitatea și viteza conexiunii DSL depinde în principal de calitatea liniei telefonice și de distanța până la sediul central al companiei telefonice. Cu cât sunteți mai departe de sediul central, cu atât este mai lentă conexiunea.
* **Celular**Accesul celular la Internet folosește o rețea de telefonice mobilă pentru conectare. De oriunde puteți obține un semnal celular, puteți obține și acces celular la Internet. Performanța va fi limitată de capacitățile telefonului și de turnul la care se conectează. Disponibilitatea accesului celular la Internet este un beneficiu real în acele zone în care nu ar exista altfel conectivitate la Internet sau pentru cei aflați în permanență în mișcare.
* **Satelit**-Serviciul prin satelit este o opțiune bună pentru locuințe sau birouri care nu au acces la DSL sau cablu. Satelitul are nevoie de o linie clară, lucru care ar putea fi dificil în zonele împădurite sau locurile cu construcții foarte înalte. Vitezele vor depinde în funcție de contract, deși de obicei sunt bune. Costurile cu instalarea și echipamentul pot fi ridicate (deși se verifică cu furnizorul pentru negocieri), iar apoi se aplică o taxă lunară moderată. Disponibilitatea accesului la Internet prin satelit este avantajoasă pentru acele zone în care nu există conectivitate la Internet.
* **Telefon Dial-Up** - O opțiune ieftină ce folosește liniile de telefonie și un modem. Pentru a se conecta la un ISP, un utilizator trebuie să sune la un număr de acces furnizat de ISP. Lățimea de bandă joasă este furnizată printr-o conexiune dial-up la modem și de obicei, nu este suficientă pentru transferul mare de date, în rest este util pentru accesul mobil în timpul călătoriei. O conexiune dial-up prin modem ar trebui să fie folosită atunci când nu sunt disponibile opțiuni de conexiune de mare viteză.

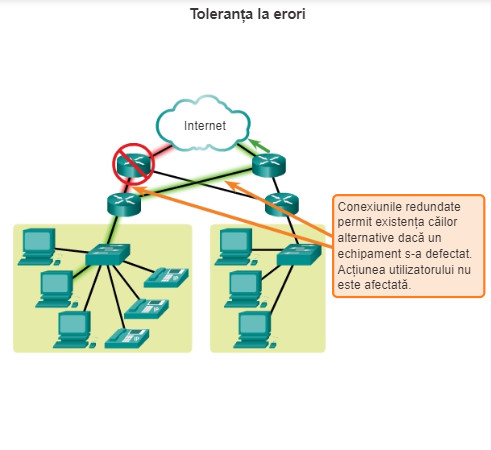
****

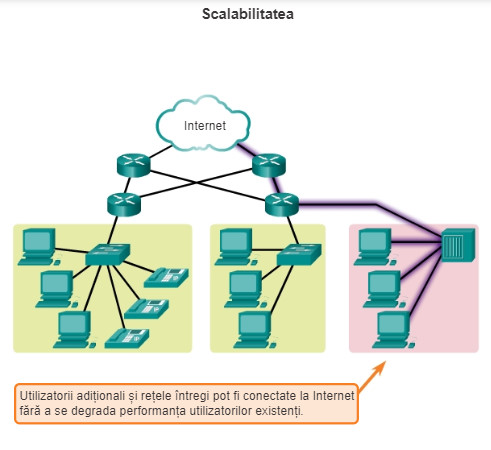
## Rețele convergente

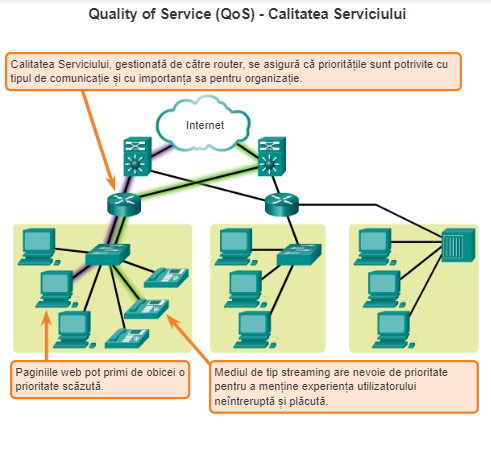
****

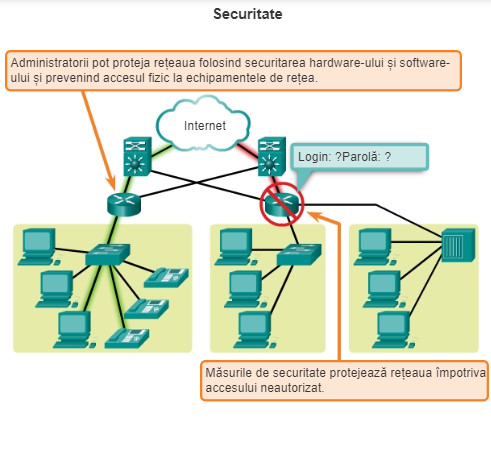
## Rețea Fiabilă

Pe măsură ce rețelele evoluează, descoperim că există patru caracteristici de bază pentru arhitecturile elementare, necesare să preîntâmpine așteptările utilizatorului:

****

****

****

****

## Tehnologii din domeniul Rețelisticii pentru Domiciliu

**WISP (Wireless Internet Service Provider)**

WISP este un ISP care conectează abonații la un punct de acces special sau hot spot folosind tehnologii wireless similare cu cele aflate în WLAN-uri. WISP se găsesc de obicei în mediile rurale unde DSL sau serviciile prin cablu nu sunt disponibile.

**Serviciul Broadband pentru Wireless**

O altă soluție wireless pentru domiciliu și companii mici este broadband-ul wireless. Acesta folosește aceeași tehnologie celulară folosită pentru a accesa Internetul cu un telefon inteligent sau tabletă. Antena este instalată în afara casei, aceasta furnizând fie conectivitate wireless, fie cablată pentru echipamentele din locuință. În mai multe zone, broadband-ul wireless este completat direct cu DSL sau servicii prin cablu.

**Amenințări de securitate**

* **Viruși, viermi și calul Troian** - cod malițios și arbitrar folosit pe echipamentele utilizatorului.
* **Spyware și adware** - software instalat pe echipamentul unui utilizator care colectează în secret informații despre utilizator
* **Atacuri zero-day, denumite și zero-hours** - un atac care apare în prima zi în care este cunoscută o vulnerabilitate
* **Atacuri ale hacker-ilor** - un atac asupra echipamentelor utilizatorilor sau resurselor de rețea efectuat de către o persoană cu multe cunoștințe
* **Atacuri de tip Denial of Service** - atacuri realizate pentru a încetini sau defecta aplicațiile și procesele unui echipament de rețea
* **Intercepția și furtul de date** - un atac de capturare a informației private de la rețeaua unei organizații
* **Furtul de identitate** - un atac prin care se fură credențialele de autentificare ale unui utilizator pentru a accesa date private

**Soluții de securitate**

Componentele de securitate pentru o rețea dintr-un domiciliu sau biroul mic ar trebui să includă, cel puțin:

* **Antivirus și antispyware** - pentru a proteja echipamentele utilizatorului împotriva software-ului malițios
* **Filtrarea prin intermediul firewall-ului**- pentru a bloca accesul neautorizat la rețea. Acest lucru ar putea include un sistem de firewall bazat pe host care este implementat să împiedice accesul neautorizat la echipamentul hostului, sau un serviciu de filtrare de bază pentru routerul de domiciliu pentru a împiedica accesul nedorit din exteriorul rețelei.

În plus, rețelele de dimensiuni mari și ale companiilor au de obicei și alte cerințe de securitate:

* **Sisteme de firewall dedicate** - pentru a asigura capacități avansate de firewall ce pot filtra cantități mari de trafic cu mai multă precizie
* **Access Control List (ACL)** - pentru a filtra în viitor accesul și traficul
* **Sisteme de prevenire a intruziunilor (IPS)** - pentru a identifica amenințările care se răspândesc rapid, cum ar fi atacuri zero-day sau zero-hour
* **Rețele private virtuale (VPN)** - pentru a furniza acces sigur pentru cei care lucrează remote

# Capitolul 2. Configurarea unui Sistem de Operare de Rețea

## Cisco IOS

Sistemele de operare de rețea sunt similare din multe puncte de vedere cu sistemele de operare ale calculatoarelor. Un sistem de operare efectuează un număr de funcții tehnice în spatele scenei care permit utilizatorului să:

* Folosească un mouse
* Să vizualizeze un output pe un monitor
* Să introducă comenzi cu text
* Să selecteze opțiuni dintr-o fereastră de dialog

Cisco IOS este un termen care întrunește un număr de sisteme de operare diferite care sunt utilizate pe mai multe echipamente diferite de rețea. Există multe variații diferite ale IOS-ului:

* IOS pentru switchuri, routere și alte echipamente de rețea Cisco
* Versiuni numerotate de IOS pentru anumite echipamente de rețea Cisco
* Seturi de caracteristici IOS care furnizează pachete distincte de caracteristici și servicii

**Funcțiile IOS-ului**

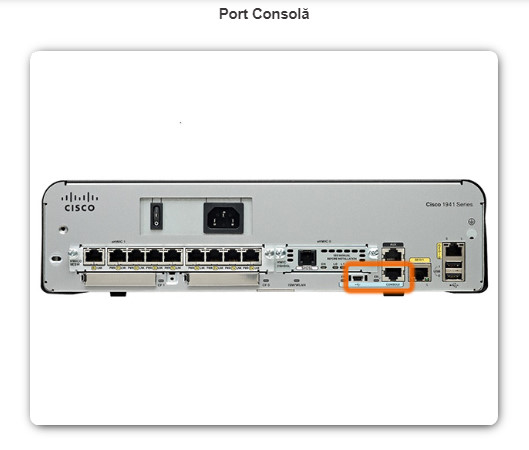
Majoritatea funcțiilor efectuate sau permise de routerele și switchurile Cisco includ:

* Asigurarea Securității Rețelei
* Adresarea IP pentru interfețele fizice și virtuale
* Permiterea configurărilor cu interfață specifică să optimizeze conectvitatea mediului respectiv
* Rutare
* Activarea tehnologiilor QoS
* Suportarea tehnologiilor de management al rețelei

## Accesarea unui Echipament cu IOS Cisco

Există câteva modalități pentru a accesa mediul CLI. Cele mai obișnuite metode sunt:

* Consola
* Telnet sau SSH
* Port AUX

****

****

**Programe de Emulare a Terminalului**

Câteva dintre acestea sunt:

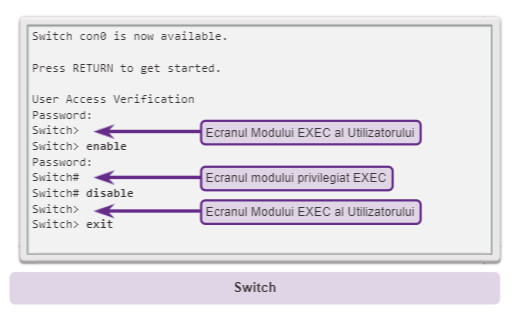
* PuTTY
* Tera Term
* SecureCRT
* HyperTerminal
* OS X Terminal

## Navigarea în IOS

**Modurile de Funcționare Cisco IOS**

În ordine ierarhică de la cel mai de bază la cel mai specializat, modurile principale sunt:

* modul executiv al utilizatorului (User EXEC)
* modul privilegiat EXEC (Privileged EXEC)
* Modul global de configurare
* Alte moduri de configurare, precum modul de configurare al interfeței

****

## Structura Comenzii

Sintaxa pentru utilizarea comenzii de descriere este: **description** este:

Switch(config-if)# **description** *string*

Pentru **ping** :

Switch> **ping** *IP-address*

Similar, sintaxa pentru introducerea comenzii **traceroute** este:

Switch> **traceroute** *IP-address*

Una din cele mai utilizate comenzi pe un switch sau router este:

Switch# **show version**

Câteva din informațiile arătate de această comandă sunt:

* **Versiunea software-ului**- versiunea software-ului IOS (stocată în flash)
* **Versiunea Bootstrap**- Versiunea Bootstrap (stocată în Boot ROM)
* **Disponibilitatea Sistemului**- Timpul care a trecut de la ultima pornire
* **Informații de repornire ale sistemului**- Metoda de repornire (crash, ciclu de alimentare)
* **Numele imaginii software**- Filename-ul IOS-ului stocat în flash
* **Tipul router-ului și al procesului**- Numărul modelului și tipul procesorului
* **Tipul memoriei și alocarea (main/partajată)**- Cantitatea de memorie RAM și Shared Packet I/O buffering
* **Caracteristici ale software-ului**- Seturi de protocoale/opțiuni suportate
* **Interfețe hardware**- Interfețe disponibile pe echipament
* **Registrul de configurare**- Setează specificăriile de pornire, setarea vitezei consolei și parametrii

## Hostname-uri

Hostname-urile permit echipamentelor să fie identificate de administratorii de rețea prin intermediul unei rețele sau a Internetului.

**Configurați Hostname-urile**

Din modul EXEC privilegiat, accesați modul de configurare global introducând comanda**configure terminal**:

Switch# **configure terminal**

După ce comanda este executată, prompt-ul se va modifica în:

Switch(config)#

Switch(config)# **hostname Sw-Floor-1**

După ce comanda este executată, prompt-ul se va modifica în:

Sw-Floor-1 (config)#

## Limitarea Accesului la Configurările de Echipamente

Parolele introduse aici sunt:

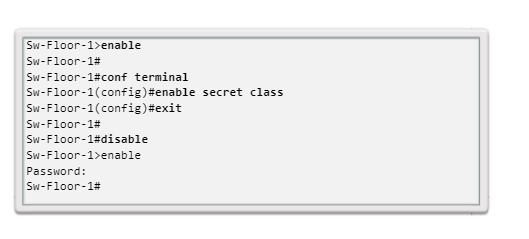
* **Parola Enable** - Limitează accesul la modul EXEC privilegiat
* **Enable secret** - Criptat, limitează accesul la modul EXEC privilegiat
* **Parola Consolei** - Limitează accesul al echipamente folosind conexiunea la consolă
* **Parola VTY** - Limitează accesul echipamentului prin Telnet

Considerați aceste puncte cheie atunci când alegeți parolele:

* Folosiți parole care au mai mult de 8 caractere în lungime.
* Folosiți în parole o combinație de litere mari și mici, numere, caractere speciale și/sau secvențe numerice.
* Evitați folosirea aceleiași parole pentru toate echipamentele.
* Evitați folosirea cuvintelor obișnuite precum parolă sau administrator, deoarece acestea sunt ușor de ghicit

**Exemple de comenzi pentru a seta parole:**

Switch(config)# **enable secret class**

****

Următoarele comenzi sunt utilizate în modul de configurare global pentru a seta o parolă pentru linia de consolă:

Switch(config)# **line console 0**

Switch(config-line)# **password cisco**

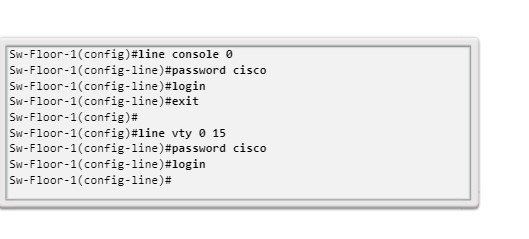
Switch(config-line)# **login**

Exemple de comenzi utilizate pentru a seta o parolă pe liniile vty:

Switch(config)# **line vty 0 15**

Switch(config-line)# **password cisco**

Switch(config-line)# **login**

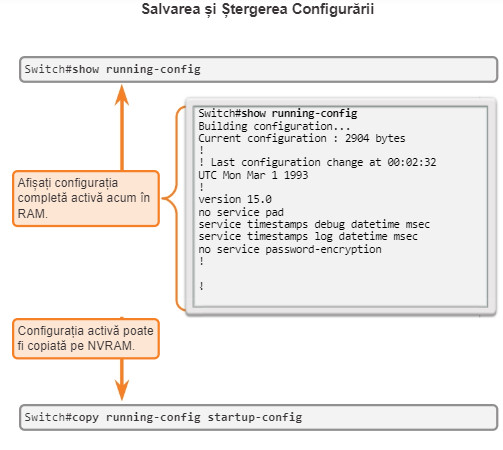
****

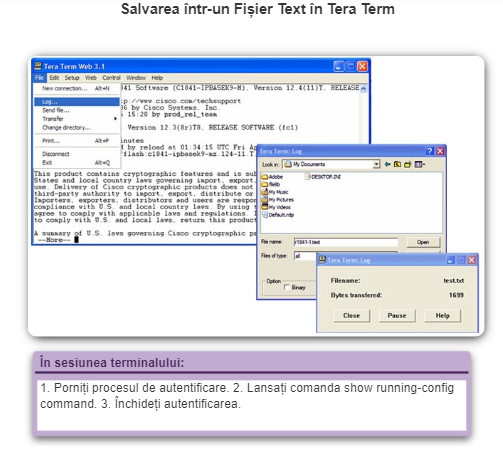
Sintaxa de configurare pentru MOTD, din modul de configurare global este:

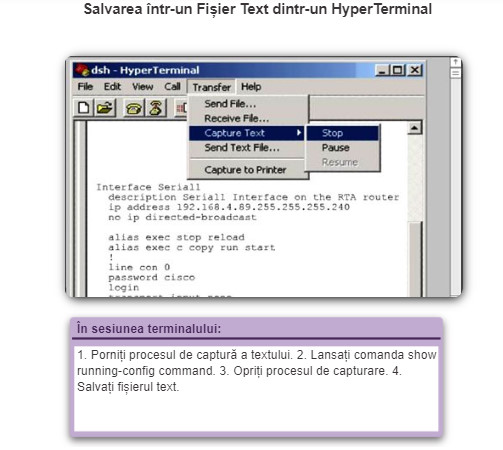
Switch(config)# **banner motd #** *message* **#**

****

## Salvarea Configurărilor

****

****

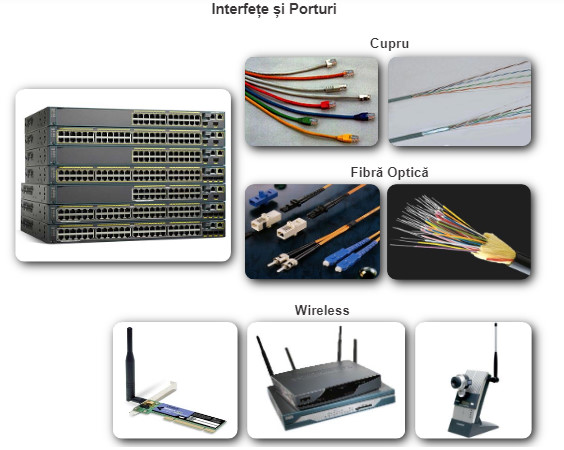
****

## Porturi și Adrese

Fiecare echipament final dintr-o rețea trebuie configurat cu adrese IP. Unele exemple de echipamente finale sunt:

* Calculatoare (stații de lucru, laptopuri, servere de fișiere, servere web)
* Imprimante de rețea
* Telefoane IP
* Camere video pentru securitate
* Telefoane inteligente
* Echipamente mobile de mână (scanner pentru codul de bare wireless)

Comunicațiile de rețea depind de interfețele echipamentului cu utilizator final, interfețelor echipamentului de rețea și de cablurile de conectare.

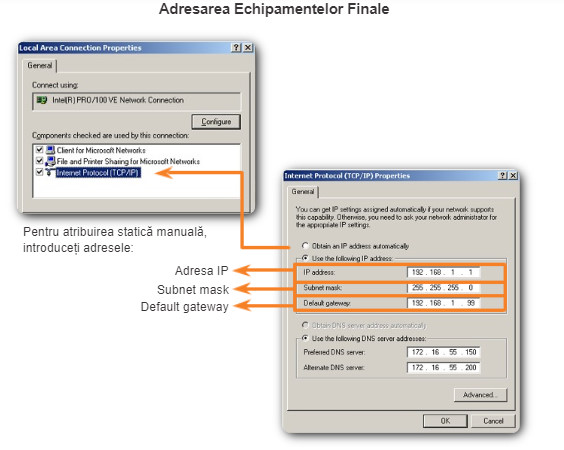
****

## Adresarea Echipamentelor

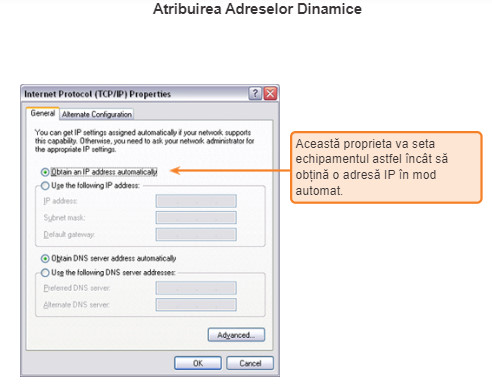
Pentru a accesa remote switch-ul, trebuie configurate o adresă IP și o mască de subrețea pe SVI:

* **Adresa IP** - Alături de masca de subrețea, identifică în mod unic echipamentul final din internetwork
* **Masca de subreţea** - Determină ce parte dintr-o rețea mai mare este utilizată de o adresă IP

**Configurarea manuală a adresei IP pentru echipamentele finale**

****

**Configurarea dinamică a adresei IP pentru echipamentele finale**

****

## Verificarea Conectivităţii

Comanda **ping** este utilizată pentru a verifica configurarea IP internă de pe hostul local.

Comenzile ping sunt introduse într-o linie de comandă pe hostul local folosind sintaxa:

C:\> **ping 127.0.0.1**

Răspunsul acestei comenzi va arăta cam așa:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

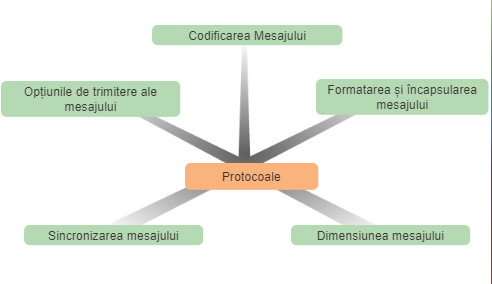
Rezultatele indică faptul că patru pachete de test de 32 octeți fiecare au fost trimise și returnate de la hostul 127.0.0.1 într-un timp mai scurt de 1 ms.

# Capitolul 3. Comunicații și protocoale de Rețea

## Regulile

Protocoalele folosite în comunicațiile de rețea partajează multe dintre trăsăturile fundamentale precum cele folosite de protocoale pentru a guverna conversațiile de succes ale oamenilor, vezi Figura 2. În plus, pentru a identifica sursa și destinația, protocoalele de rețea și calculatorul definesc detaliile cu privire la modul în care un mesaj este transmis prin intermediul unei rețele pentru a respecta cerințele de mai sus. În timp ce există mai multe protocoale care trebuie să interacționeze, protocoalele obișnuite ale calculatorului includ:

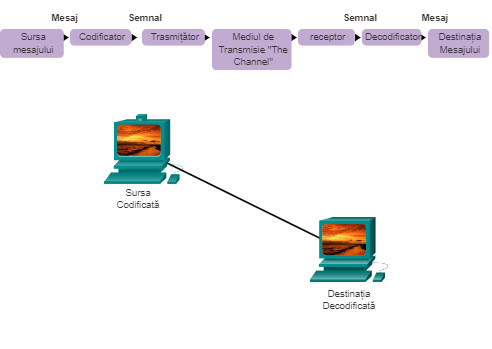
* Codificarea mesajului
* Formatarea și încapsularea mesajului
* Dimensiunea mesajului
* Timpul mesajului
* Opțiunile de trimitere ale mesajului



**Codificarea mesajului**

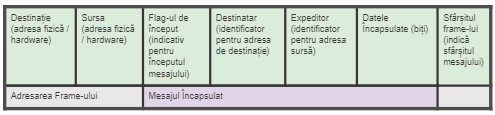
Codificarea este procesul de convertire a informației într-o altă formă acceptabilă de transmisie. Decodificarea inversează acest proces pentru a interpreta informația.

Codificarea între hosturi trebuie să fie într-o formă corespunzătoare pentru mediu. Mesajele trimise prin intermediul rețelei sunt primele convertite în biți de către hostul de expediere. Fiecare bit este codificat într-un pattern de sunete, unde de lumină sau impulsuri electrice care depind de mediul de rețea prin intermediul căruia sunt trimiși biții. Hostul de destinație primește și decodifică semnalele pentru a interpreta mesajul.

****

**Formatarea și încapsularea mesajului**

Atunci când un mesaj este trimis de la sursă la destinație, trebuie să se folosească un format sau o structură specifică. Formatul mesajului depinde de tipul mesajului și de canalul folosit pentru a trimite mesajul.

****

**Dimensiunea mesajului**

O altă regulă de comunicare este dimensiunea. Așadar, atunci când un mesaj lung este trimis de la un host la altul prin intermediul rețelei, este necesar să împărțiți mesajul în părți mai mici. Frame-urile de dimensiuni prea mari sau prea mici nu sunt trimise.

**Sincronizarea mesajului**

Un alt factor care afectează modul în care un mesaj este trimis și înțeles este sincronizarea. Oamenii folosesc sincronizarea pentru a determina momentul în care să vorbească, cât de repede sau cât de rar și cât de mult să aștepte un răspuns.

**Metoda de acces**

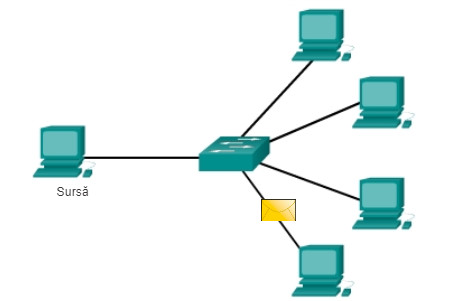
Metoda de acces determină momentul în care cineva poate trimite un mesaj. Aceste reguli de sincronizare sunt bazate pe mediu. De exemplu, ați putea vorbi de fiecare dată când aveți ceva de spus. În acest mediu, o persoană trebuie să aștepte până când nu mai vorbește nimeni pentru a putea vorbi. Dacă două persoane vorbesc în același timp, apare o coliziune de informație și este necesar ca amândoi să se oprească și să pornească din nou.

**Timp de răspuns maxim**

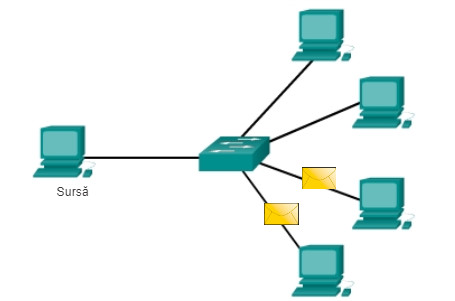
Dacă o persoană adresează o întrebarea și nu primește răspunsul într-un timp acceptabil, persoana presupune că nu va primi nici un răspuns și reacționează în consecință.

**Opțiunile de expediere a unui mesaj**

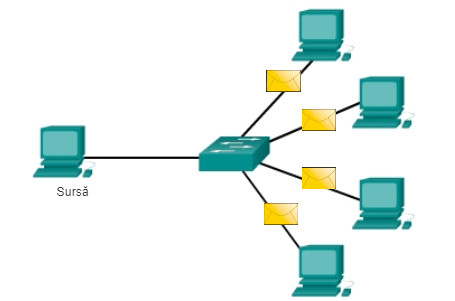
**Unicast**- de la o sursă la o destinație



**Multicast-** de la o sursă la mai mulți

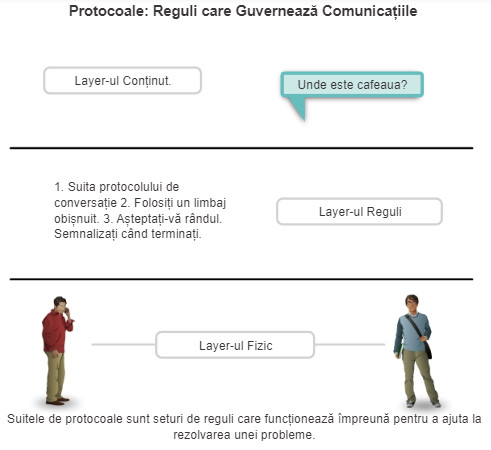


**Broadcast-** de la o sursă la toți destinatarii



## Protocoale

Ca și în cazul conexiunii dintre oameni, protocoalele diferite ale calculatorului și rețelei trebuie să poată interacționa și funcționa împreună pentru ca o comunicație de rețea să fie realizată cu succes. Un grup de protocoale inter-relaționate care trebuie să realizeze o funcție de comunicare se numește suită de protocoale. Suitele de protocoale sunt implementate de hosturi și de echipamentele de rețea în software, hardware sau ambele.



**Protocoalele de rețea** definesc un format comun și un set de reguli pentru interschimbarea mesajelor între echipamente. Câteva protocoale de rețea cunoscute sunt IP, HTTP și DHCP.

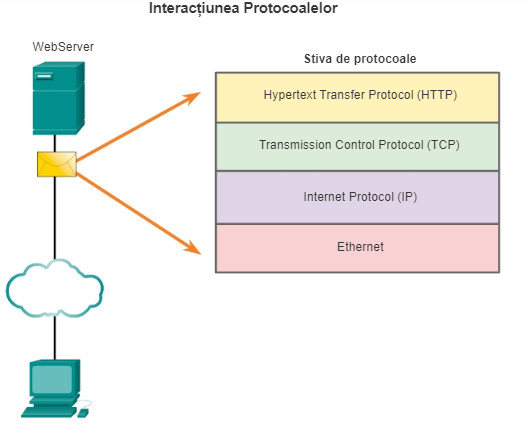
Protocoalele de rețea care descriu următoarele procese:

* Modul în care mesajul este formatat sau structurat
* Procesul în care echipamentele de rețea partajează informația despre căile de acces cu alte rețele
* Modul și timpul în care mesajele de eroare și cele de sistem sunt transmise între echipamente
* Configurarea și finalizarea sesiunilor de transfer de date

**Interacțiunea protocoalelor**

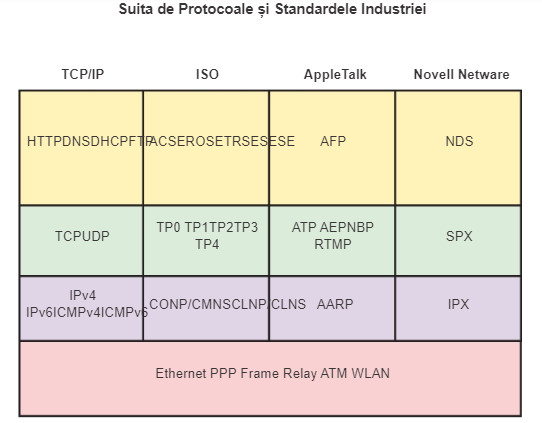
Această interacțiune folosește un număr de protocoale și standarde în procesul de interschimbare a informației.

* **Protocolul Aplicație**- Hypertext Transfer Protocol (HTTP) este un protocol care guvernează modul în care un server de web și un server de client interacționează.
* **Protocolul Transport**- Transmission Control Protocol (TCP) este protocolul de transport care gestionează conversațiile individuale între serverele de web și clienții de web.
* **Potocolul Internet**- IP este responsabil cu preluarea segmentelor formatate de la TCP, încapsularea lor în pachete, atribuirea loc către adresele corespunzătoare și trimiterea lor pe calea cea mai bună către hostul de destinație.
* **Protocoalele de Acces la Rețea**- Aceste protocoale descriu două funcții primare, comunicarea printr-un data link și transmisia fizică a datelor într-un mediu de rețea.

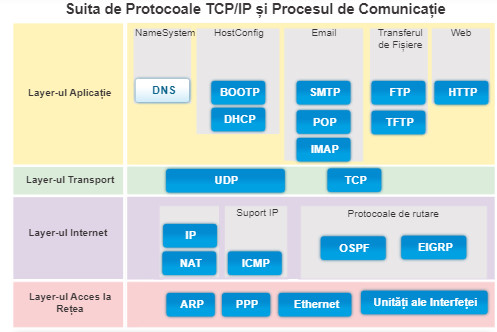


## Suita de Protocoale

Protocoalele IP, HTTP și DHCP sunt toate părți din suita de protocoale a Internetului cunoscută ca Transmission Control Protocol/IP (TCP/IP). Suita de protocoale TCP/IP este un standard deschis, ceea ce înseamnă că aceste protocoale sunt disponibile în mod gratis publicului și orice furnizor poate implementa aceste protocoale pe hardware-ul și software-ul lor.



Suita de protocoale TCP/IP este implementată ca o stivă TCP/IP pe hostul sursă și destinație pentru a furniza o expediere end-to-end a aplicațiilor în rețea. Protocoalele 802.3 sau Ethernet sunt folosite pentru a transmite pachetul IP în mediul fizic folosit de LAN.



## Organizaţii de standardizare

Organizațiile de standardizare de obicei nu au legătură cu furnizorii, sunt organizații non-profit stabilite pentru a dezvolta și promova conceptul de standarde libere.

Organizațiile de standardizare incluc:

* The Internet Society (ISOC)
* The Internet Architecture Board (IAB)
* The Internet Engineering Task Force (IETF)
* The Institute of Electrical and Electronics Engineers (IEEE)
* The International Organization for Standardization (ISO)



**The Internet Society (ISOC)** este responsabilă cu promovarea dezvoltării, evoluției și folosirii Internetului în mod liber în întreaga lume. ISOC facilitează dezvoltarea liberă a standardelor și protocoalelor pentru infrastructura tehnică a Internetului, incluzând și supraveghea celor de la Internet Architecture Board (IAB).

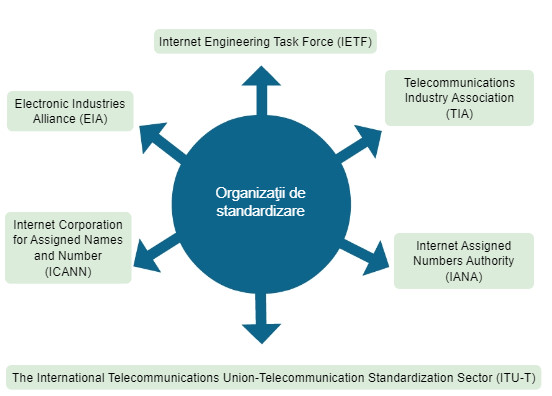
**The Internet Architecture Board (IAB)** este responsabil pentru dezvoltarea și managementul general al standardelor de Internet. IAB supravghează arhitectura protocoalelor și procedurilor folosite de Internet. IAB are 13 membri, incluzând și șeful de la Internet Engineering Task Force (IETF). Membrii IAB sunt individuali și nu reprezintă nici o companie, agenție sau altă organizație.

Misiunea celor de la **IETF** este să dezvolte, actualizeze și mențină tehnologiile TCP/IP și Internet. Una din responsabilitățile cheie ale celor de la IETF este producerea documentelor RFC (Request for Comments), care reprezintă un memorandum de descriere a protocoalelor, proceselor și tehnologiile pentru Internet.

**The Institute of Electrical and Electronics Engineers (IEEE)** este o organizație profesională pentru cei din domeniul electronicii și ingineriei electrice care se dedică avansării inovației tehnologie și creării standardelor. În 2012, IEEE era alcătuit din 38 de societăți, publica 130 de jurnale și sponsoriza mai mult de 1300 de conferințe din întreaga lume. IEEE are peste 1300 standarde și proiecte curente aflate în curs de dezvoltare.   
Standardele IEEE 802.3 și IEEE 802.11 sunt standarde IEEE importante în rețelistică. Standardul IEEE 802.3 definește MAC-ul (Media Acces Control) pentru Ethernet-ul cu fir. Această tehnologie este de obicei, pentru aplicații LAN, dar și pentru WAN. Standardul 802.11 definește un set de standarde pentru implementarea WLAN-urilor. Acest standard definește nivelul fizic OSI, dar și adresa MAC a nivelului data link pentru comunicații fără fir (wireless).

**ISO (The International Organization for Standardization)** este cel mai mare dezvoltator de standarde internaționale din lume, pentru o varietate de produse și servicii. ISO nu este un acronim pentru numele organizației, ci un termen bazat pe termenul grecesc “isos”, care înseamnă egal. Organizația Internațională de Standardizare a ales termenul ISO pentru a își afirma poziția de egalitate cu toate țările.

**Alte organizații de standartizare**

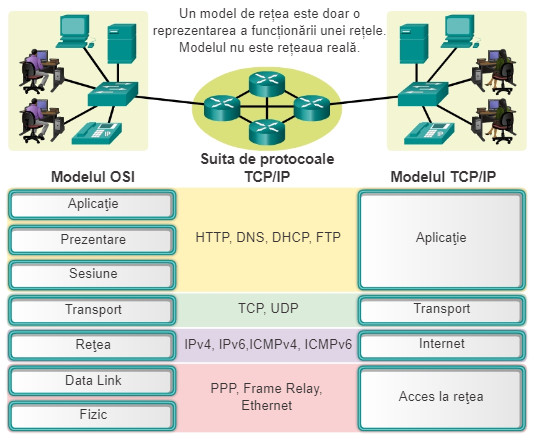
****

## Modele de referință

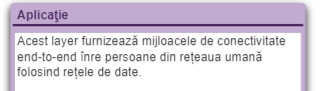
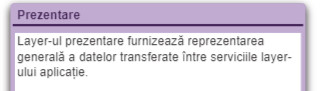
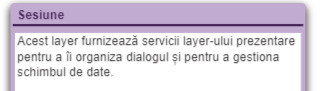
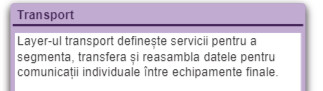
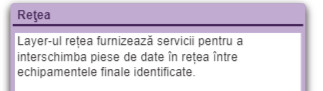
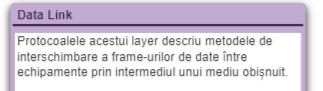
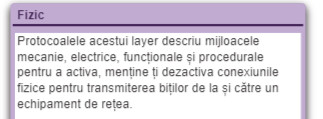
Un astfel de model precum TCP/IP este utilizat adesea pentru a ajuta la vizualizarea interacțiunii dintre protocoale diferite. Un model pe layere reprezintă funcționarea protocoalelor care apar în fiecare layer, precum și interacțiunea protocoalelor cu layer-ele superioare și inferioare.

Există două modele de bază ale modelelor din rețelistică:

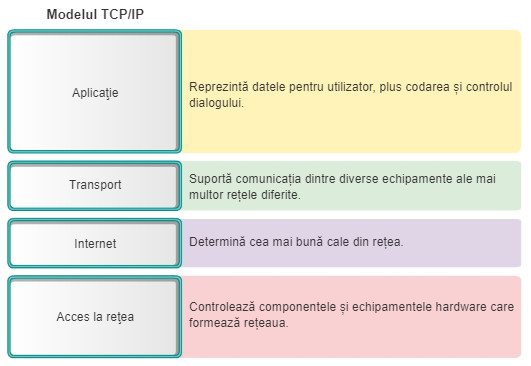
* **Modelul Protocolului** - Acest model se potrivește foarte mult cu structura unei suite de protocoale particulare. Setul ierarhic al protocoalelor relaționale dintr-o suită tipică reprezintă toate funcționalitățile necesare pentru a realiza o interfață între rețeaua umană și cea de date. Modelul TCP/IP este un model de protocol, deoarece descrie funcțiile care apar la fiecare layer al protocolului în cadrul suitei TCP/IP.
* **Modelul de referință** - Acest model furnizează consistența tuturor tipurilor de protocoale de rețea și servicii, descriind ce trebuie făcut la un anumit layer, dar nu se prescrie și modul în care trebuie să se procedeze. Un model de referință nu intenționează să fie o specificație de implementare sau să furnizeze un nivel de detaliu suficient pentru a defini în mod precis serviciile arhitecturii de rețea. Scopul principal al unui model de referință este să ajute la o mai bună înțelegere a funcțiilor și proceselor implicate.

****

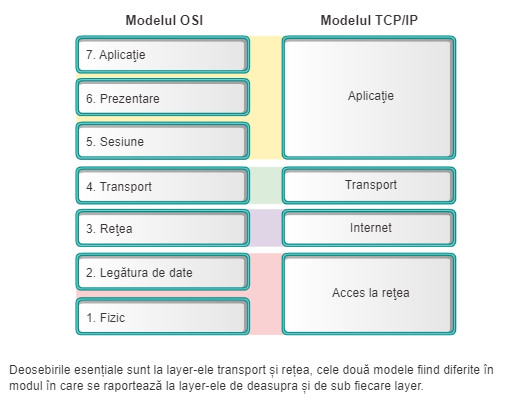
**Modelul OSI**

**** ****     

**Modelul TCP/IP**

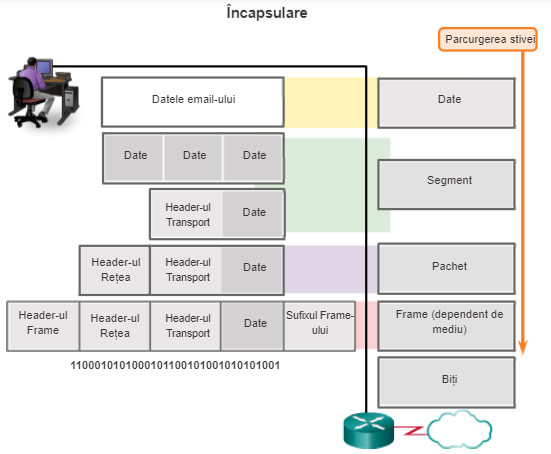
****

**Comparațiile între modelul OSI și TCP/IP**

****

## Încapsularea datelor

Pe măsură ce datele aplicației parcurg stiva de protocoale pentru a fi transmise în mediul de rețea, mai multe protocoale adaugă informație la fiecare nivel. Acest lucru este frecvent cunoscut ca proces de încapsulare.

****

Încapsularea datelor este procesul care adaugă informație adițională la header-ul protocolului de date înainte de transmitere. La majoritatea formelor de comunicații de date, datele originale sunt încapsulate în câteva protocoale înainte de transmitere.

**Decapsularea**

Acest proces este inversat la hostul de destinație, și este cunoscut ca decapsulare. Decapsularea este procesul folosit de un echipament de destinație pentru a îndepărta unul sau mai multe headere de protocoale. Datele sunt decapsulate pe măsură ce se parcurge stiva din aplicația cu utilizator final. Dați clic pe butonul Play din figură pentru a vedea procesul de decapsulare.

## Accesarea Resurselor Locale

**Adresa de rețea**

Layer-ul rețea sau Layer-ul 3, adresa logică conține informații necesare pentru a livra pachetul IP de la echipamentul sursă la cel destinație.

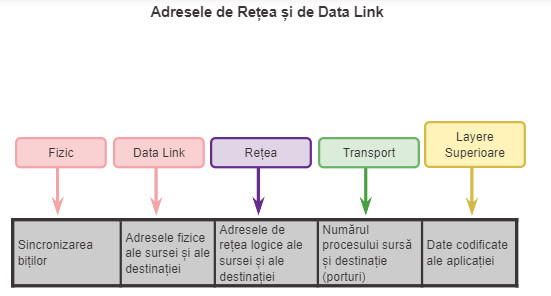
Un pachet IP conține două adrese IP:

* **Adresa IP Sursă** - Adresa IP a echipamentului transmițător
* **Adresa IP de Destinație** - Adresa IP a echipamentului receptor. Adresa IP de destinație este utilizată de routere pentru a înainta pachetul către destinația sa.

**Adresa Data Link**

Adresa fizică de Layer 2 sau Data Link are un rol diferit. Scopul acesteia este să trimită frame-ul de data link de la o interfață de rețea către altă interfață de rețea din aceeași rețea. Pachetul IP este încapsulat într-un frame de data link pentru a fi trimis către rețeaua de destinație.

* **Adresa data link a sursei** - Adresa fizică a echipamentului care trimite pachetul. Inițial, placa de rețea este sursa pachetului IP.
* **Adresa data link a destinației** - Adresa fizică a plăcii de rețea a următorului hop al routerului sau a echipamentului de destinație.



* **Adresa MAC a Sursei** - Aceasta este adresa de data link, sau adresa Ethernet MAC a echipamentului care trimite pachetul IP, PC1. Adresa MAC a plăcii de rețea Ethernet a lui PC1 este AA-AA-AA-AA-AA-AA.
* **Adresa MAC de destinație** - Atunci când echipamentul receptor se află în aceeași rețea cu cel transmițător, aceasta este adresa de data link a echipamentului receptor. În acest exemplu, adresa MAC de destinație este adresa MAC a serverului FTP: CC-CC-CC-CC-CC-CC.