

Ce este un IP?

Adresa logica asociata unui device

De ce asociem un IP unui device?

Dorim sa asiguram schimbul de mesaje intre echipamente

Ce este un protocol?

Un protocol este un set de reguli și convenții cu ajutorul căruia se realizează comunicarea într-o rețea. Protoalele determină formatul, timpul, secvențele și controlul erorilor în comunicarea de date.

Ce roluri indeplinește un protocol?

Protocoalele controlează toate aspectele comunicării datelor:

- cum este construită rețeaua fizică;
- cum sunt conectate calculatoarele la rețea;
- cum sunt formate datele pentru transmisie;
- cum sunt transmise datele;
- cum sunt conectate erorile.

Care este protocolul cel mai folosit pentru transmiterea datelor într-o rețea?

IP (Internet Protocol) este un protocol care asigură un serviciu de transmitere a datelor, fără conexiune permanentă.

Identifică fiecare interfață logică a echipamentelor conectate printr-un număr numit „adresă IP”(versiunea standard IPv4). În IPv4, standardul curent pentru comunicarea în Internet, adresa IP este reprezentată pe 32 de biți

Alocarea adreselor IP nu este arbitrară; ea se face de către organizații însărcinate cu distribuirea de spații de adrese (RIPE – Europa).

Ce roluri indeplinește un protocol?

Protocoalele controlează toate aspectele comunicării datelor:

- cum este construită rețeaua fizică;
- cum sunt conectate calculatoarele la rețea;
- cum sunt formate datele pentru transmisie;
- cum sunt transmise datele;
- cum sunt conectate erorile.

Care este protocolul cel mai folosit pentru transmiterea datelor într-o rețea?

IP (Internet Protocol) este un protocol care asigură un serviciu de transmitere a datelor, fără conexiune permanentă.

Identifică fiecare interfață logică a echipamentelor conectate printr-un număr numit „adresă IP”(versiunea standard IPv4). În IPv4, standardul curent pentru comunicarea în Internet, adresa IP este reprezentată pe 32 de biți

Alocarea adreselor IP nu este arbitrară; ea se face de către organizații însărcinate cu distribuirea de spații de adrese (RIPE – Europa).

IP protocol - detalii

Internet Protocol (IP) face parte din nivelul Internet al stivei TCP/IP.

În stiva OSI face parte din nivelul Network.

Protocol IP este folosit împreună cu un protocol de nivel superior, cel mai probabil

Cum funcționează?

Este proiectat să fie folosit peste o rețea dinamică.

Nu trebuie să depindă de un nod central și nu trebuie să depindă de alte resurse.

IP este un protocol *connectionless datagram-oriented* (fiecare pachet conține sursa și destinația).

Erorile de transmitere sunt tratate de un protocol de nivel superior (TCP connection-oriented protocol și UDP connectionless protocol).

Cea mai mare parte a traficului este TCP/IP.

Stiva OSI - rezumat

OSI Model

Layer #	Name	Mnemonic	Encapsulation Units	Devices or Components	Keywords/Description
7	Application	All	data	PC	Network services for application processes, such as file, print, messaging, database services
6	Presentation	People	data		Standard interface to data for the application layer. MIME encoding, data encryption, conversion, formatting, compression
5	Session	Seem	data		Interhost communication. Establishes, manages and terminates connection between applications
4	Transport	To	segments		End-to-end connections and reliability. Segmentation/desegmentation of data in proper sequence. Flow control
3	Network	Need	packets	router	Logical addressing and path determination. Routing. Reporting delivery errors
2	Data Link	Data	frames	bridge, switch, NIC	Physical addressing and access to media. Two sublayers: Logical Link Control (LLC) and Media Access Control (MAC)
1	Physical	Processing	bits	repeater, hub, transceiver	Binary transmission signals and encoding. Layout of pins, voltages, cable specifications, modulation

Stiva TCP/IP - rezumat

OSI comparision with TCP/IP Protocol Stack

OSI #	OSI Layer Name	TCP/IP #	TCP/IP Layer Name	Encapsulation Units	TCP/IP Protocols
7	Application	4	Application	data	FTP, HTTP, POP3, IMAP, telnet, SMTP, DNS, TFTP
6	Presentation			data	
5	Session			data	
4	Transport	3	Transport	segments	TCP, UDP
3	Network	2	Internet	packets	IP
2	Data Link	1	Network Access	frames	
1	Physical			bits	

IPv4 - detalii

Adresele IPv4 au o lungime de 32 de biți (4 octeți).

Fiecare adresă identifică o rețea (network) și o stație de lucru (work station) din cadrul rețelei.

Notăția obișnuită este obținută prin scrierea fiecărui octet în formă zecimală, separați între ei prin puncte.

De exemplu, $192.168.0.1_{(10)}$ este notația folosită pentru adresa $11000000.10101000.00000000.00000001_{(2)}$

De ce avem nevoie de o adresa de retea?

Intr-o retea TCP/IP de dimensiuni mari pentru a asigura eficient conectivitatea dintre retele, routerele folosesc adresele de retea in procesul de routare.

In felul acesta pachetele sunt transmise intre retele si abia dupa ce ajunge in retea de destinatie este folosita adresa de host.

Din acest motiv spunem ca un ip are doua parti: **network** + **host**

Exemplu: **192.168.123.132**

De ce avem nevoie de o adresa de broadcast?

De multe ori intr-o retea TCP/IP de dimensiuni mari exista anumite echipamente care au indeplinesc roluri special (server DHCP, server DNS, default gateway etc).

In unele situatii un echipament trebuie sa descopere un astfel de echipament “special”.

Ca sa nu fie obligat sa trimita cate un mesaj la fiecare adresa in parte, poate sa trimita catre adresa de broadcast (neassignabila) si astfel echipamentele care primesc vor trimite acest mesaj pe toate interfetele (**in cadrul aceleasi retea**).

Cate clase de adrese?

La începuturile Internetului, adresele IPv4 se împărțeau în 5 clase de adrese, notate de la A la E. Împărțirea se făcea în funcție de configurația binară a primului octet al adresei, astfel:

Clasa	Primul octet în binar	Prima adresă	Ultima adresă	Observații
A	0xxxxxxx	0.0.0.1	127.255.255.255	folosește 8 biți pentru rețea și 24 pentru stația de lucru
B	10xxxxxx	128.0.0.0	191.255.255.255	folosește 16 biți pentru rețea și 16 pentru stație
C	110xxxxx	192.0.0.0	223.255.255.255	folosește 24 biți pentru rețea și 8 pentru stație
D	1110xxxx	224.0.0.0	239.255.255.255	folosită pentru adresarea de tip multicast
E	1111xxxx	240.0.0.0	255.255.255.255	utilizată în scopuri experimentale

Clase de adrese

Adresele rețelelor au toți biții de stație 0 și nu pot fi folosite pentru o stație. În plus, mai există și adrese de difuzare, **care au toți biții de stație 1**.

Pentru identificarea stațiilor se folosesc numai adresele de clasă A până la C.

În plus, există două intervale de adrese de clasă A nefolosite în Internet:

- Intervalul 0.0.0.0 - 0.255.255.255 nu se folosește, pentru a nu fi confundat cu ruta implicită;
- Intervalul 127.0.0.0 - 127.255.255.255 este folosit numai pentru diagnosticarea nodului local (întotdeauna acesta va fi cel care va răspunde la apelul unei adrese din aceasta clasă).

Această metodă risipea multe adrese IP, pentru a soluționa această problemă, la începutul anilor '90 au fost concepute mai multe soluții: adrese private, CIDR (*Classless InterDomain Routing*), VLSM (*Variable Length Subnet Mask*)

Adrese private

Dispozitivele neconectate la Internet nu au nevoie de o adresă IP unică.

Pentru aceste dispozitive au fost standardizate adresele private.

Aceste adrese nu sunt unice la nivelul Internetului și de aceea nu sunt rutate de dispozitivele de nivel 3.

În RFC 1918 au fost definite trei intervale rezervate pentru adresare privată:

Adrese rezervate pentru clasa A: 10.0.0.0 - 10.255.255.255

Adrese rezervate pentru clasa B: 172.16.0.0 - 172.31.255.255

Adrese rezervate pentru clasa C: 192.168.0.0 - 192.168.255.255

Subretele

Adresele IPv4 folosesc subnetarea, care constă în împărțirea adresei IP în două părți: **adresa de rețea** și **adresa de stație**.

Folosind o mască de rețea, calculatorul poate determina unde să împartă adresa IP (conform standardului RFC 950).

Subnetarea a apărut ca soluție pentru problema epuizării spațiului de adrese IP. Odată cu subrețelele a apărut distincția între adresarea "classfull" (care ține cont de clasele de adrese) și adresarea "classless" (care oferă suportul pentru câmpul de subrețea).

Au fost introduse mecanisme de rutare pentru adresarea classless. Aceste mecanisme vizează CIDR, cât și VLSM.

VLSM (Variable Length Subnet Mask)

VLSM (Variable Length Subnet Mask) este un procedeu care presupune precizarea unei măști de rețea pentru fiecare adresă asociată unei interfețe.

Acest lucru permitea împărțirea unei clase de adrese în mai multe rețele de dimensiuni diferite, micșorând astfel irosirea de adrese IP.

De exemplu, pentru o rețea de 20 de calculatoare (stații) se puteau folosi acum doar 32 de adrese (o rețea /27), față de 256 de adrese (o rețea de clasă C, /24).

Link: <http://www.davidc.net/sites/default/subnets/subnets.html>

CIDR (*Classless InterDomain Routing*)

CIDR (Classless InterDomain Routing) se referă la modul de reprezentare a adreselor IP în tabela de rutare și la modul de trimitere a mesajelor de actualizare.

În notația CIDR, adresa IP este reținută întotdeauna împreună cu masca de rețea. De exemplu, o adresă IP de tipul 192.0.2.1, cu masca 255.255.255.0, ar fi scrisă în notația CIDR ca 192.0.2.1/24, deoarece primii 24 de biți din adresa IP indică subrețeaua.

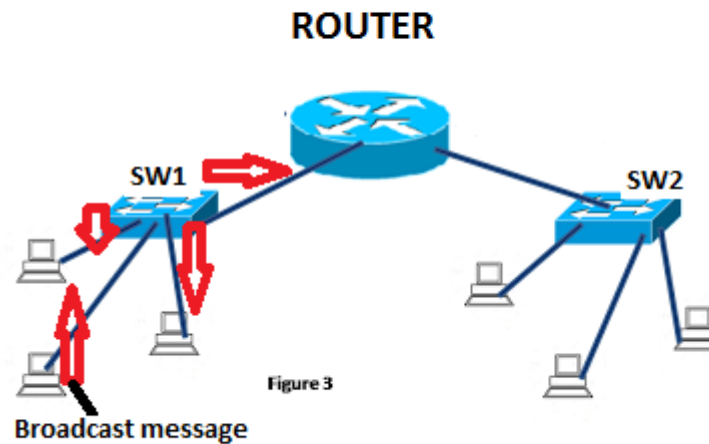
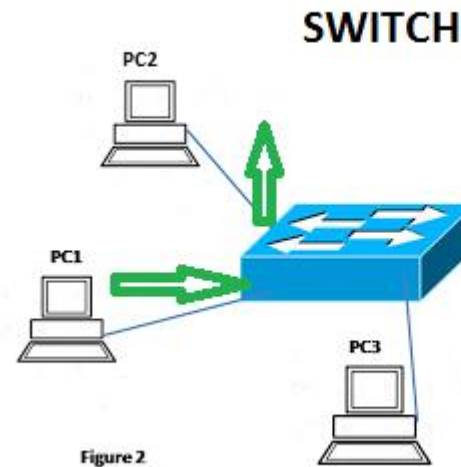
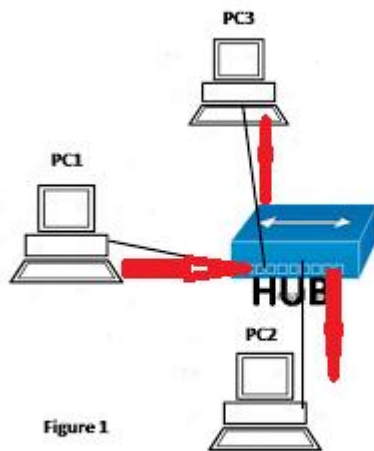
Faptul că în tabela de rutare este precizată și masca de rețea permite agregarea (unirea) rețelelor vecine, reducând dimensiunea tabelului de rutare. De exemplu, rețelele 192.0.2.0/24 și 192.0.3.0/24 vor fi reținute ca 192.0.2.0/23:

192.0.2.0/24 = 11000000.00000000.00000010. / 00000000

192.0.3.0/24 = 11000000.00000000.00000011. / 00000000

192.0.2.0/23 = 11000000.00000000.0000001 / 0.00000000

Domeniu de coliziune, domeniu de broadcast



Subnetting

- <http://www.network-calculator.com/m/>
- <http://www.ip-calc.com/>
- <https://play.google.com/store/apps/details?id=com.rain.divip&hl=en>
- <https://sourceforge.net/projects/divip/>
- <https://play.google.com/store/apps/details?id=uk.co.znder.subnetcalculator&hl=en>

Domain Name Service – DNS (1)

- Port: 53
- Protocol client - server
- Spațiul de nume DNS – structură logică arborescentă
- Fiecare nod reprezintă un domeniu = porțiune din spațiul de nume
- Domenii:
 - rădăcina: „.”
 - de nivel înalt: com, gov etc

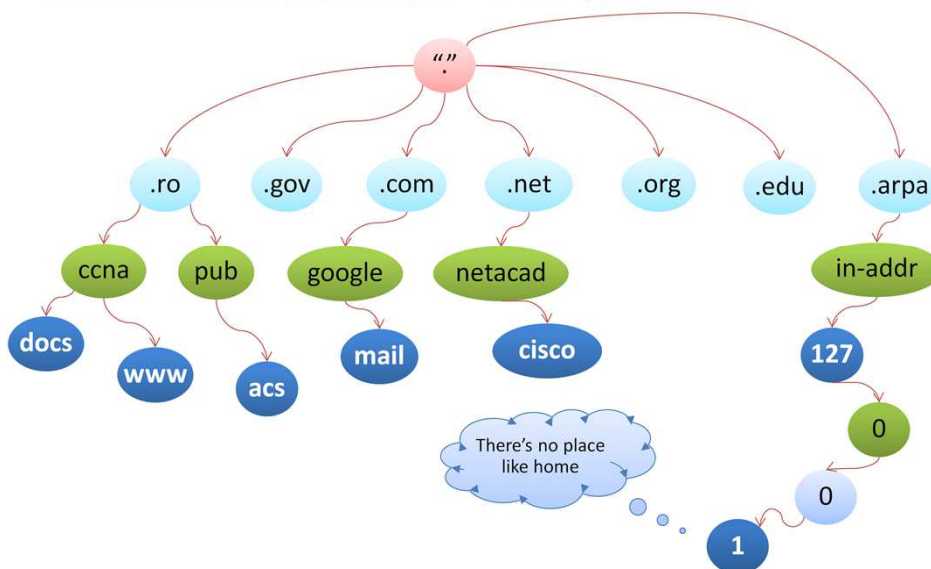


Un Domain Name Service reprezintă un sistem distribuit de date, de păstrare și interogare a unor date arbitrare, de obicei realizarea unei corespondențe între nume și adresa IP, într-o structură ierarhică de tip arborescentă. Cea mai cunoscută aplicație DNS este gestionarea ierarhică a domeniilor din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

DNS are rolul de a traduce 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 traducere a unui domeniu constituie o simplă mapare între nume și IP, un exemplu fiind `www.ccna.ro` - `141.85.227.20`.

Domain Name Service – DNS (2)

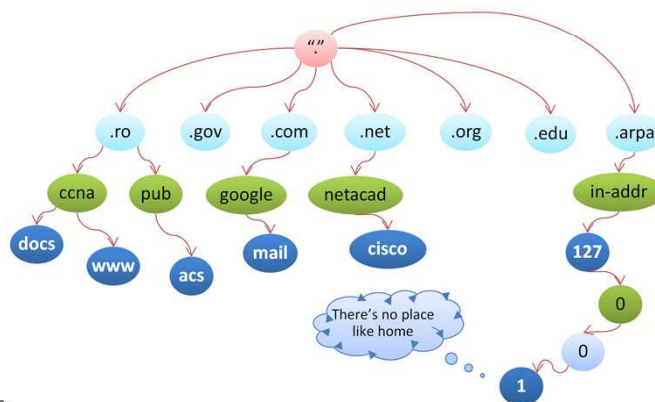


Structura DNS realizează administrarea numelor prin acordarea unor responsabilități diferite unui grup, fiecare nivel al arborelui constituie un domeniu. Sistemul de nume din Internet este structurat pe domenii și subdomenii. Un exemplu ar fi docs.ccna.ro, unde domeniul cel mai cuprinzător este „.ro”, 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 rețea ierarhică



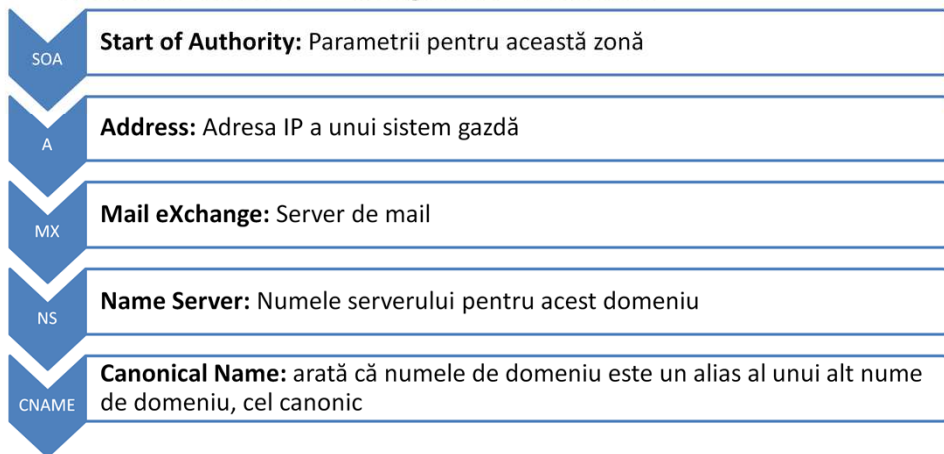
Serverele DNS reprezintă o bază distribuită pe toată rețeaua Internet. Se numește distribuită întrucât nu există un server care să conțină toată informația necesară traducerii oricărui domeniu existent într-o adresă IP. Fiecare server menține o bază de date cu propriile domenii pe care alte sisteme din Internet le poate interoga. Fiecare server DNS are un server DNS superior cu care face periodic schimb de informație, astfel într-un domeniu trebuie să existe două 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.

Domain Name Service – DNS (4)



- Informațiile sunt transmise de serverul DNS sub formă de “Resource Records” – înregistrări de resurse



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

Domain Name Service – DNS (5)



- DNS folosește un sigur format de mesaj pentru:
 - Toate tipurile de cereri de la client și răspunsuri de la server
 - Mesajele de eroare
 - Transferul înregistrărilor de resurse între servere

Header	Describe tipul mesajului
Question	Unul sau mai multe query-uri pentru server
Answer	RR care răspund la întrebarea din secțiunea Question
Authority	RR care trimit către serverul autoritativ
Additional	RR cu informații adiționale (care nu sunt neapărat necesare pentru a răspunde la întrebare)

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”

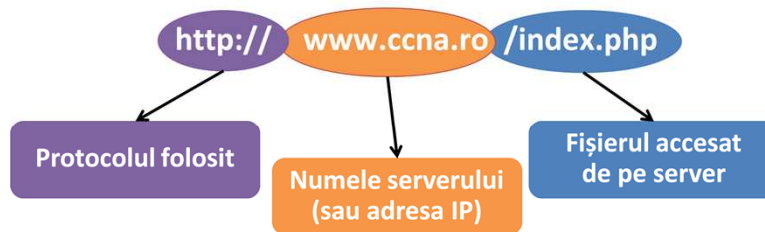
Modul în care se realizează o cerere DNS poate fi recursivă sau iterativă.

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 și 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



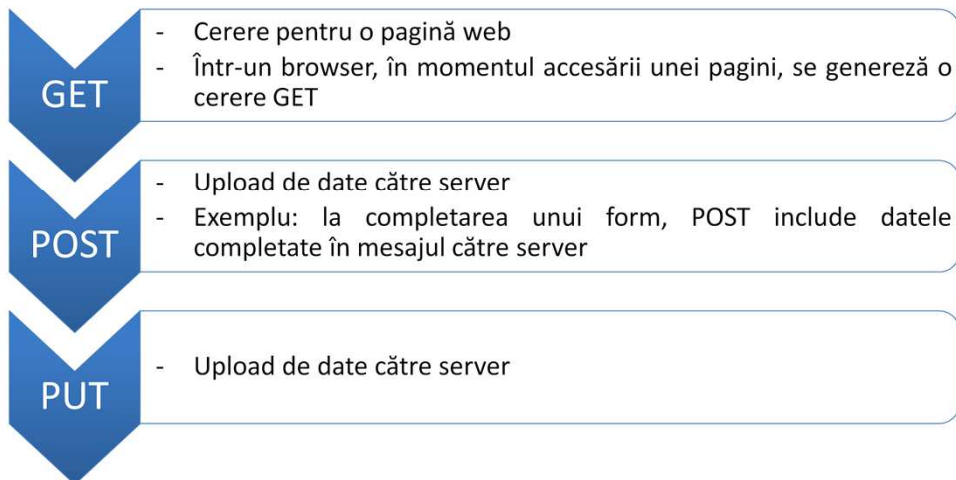
- **Hypertext Transfer Protocol**
- Face parte din stiva de protocoale TCP/IP (port 80)
- Original a fost conceput numai pentru transferul paginilor HTML
- În prezent este folosit pentru o gamă largă de tipuri de date
- Unul dintre cele mai folosite protocoale de nivel Aplicație

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 căreia un hypertext poate fi transmis de pe un server pe orice alt dispozitiv 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.

HTTP - Tipuri de mesaje



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 serverul HTTP va răspunde cu o serie de coduri de stare a operației solicitate:

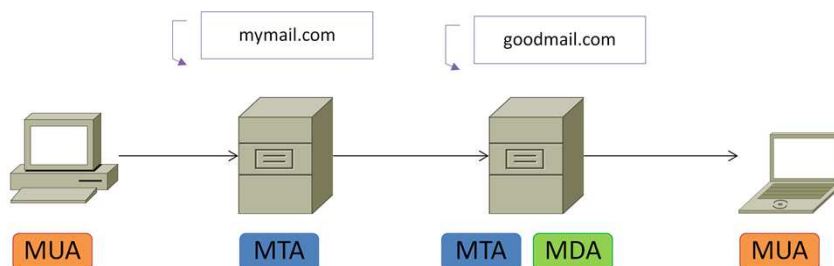
- 200 – cerere realizată cu succes
- 400 – bad request
- 403 – forbidden
- 503 – service unavailable

Unde semnificația fiecărei metode este următoarea:

- **Options** – prezintă o cerere de informații despre opțiunile 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 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 specificată de Request-URI.
- **DELETE** – Cere ca serverul să ștergă resursa identificată la Request-URI
- **TRACE** – Trimite o cerere de diagnosticare 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 „poșta electronică”, astfel e-mail-urile desemnează mesajele individuale trimise prin intermediul unor servere denumite servere de mail. Acest serviciu este descris în RFC 5322, care stabilește:

- Antetul (header) - include informații despre destinatar, subiect
- Corpul (body) - include informații 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 asigură transferul mesajelor de la un calculator al altul.
- **MUA** – denumit e-mail client – este programul folosit pentru citirea, compunerea și transmiterea de mesaje de poșta electronică. Citirea se face prin intermediul protocolului POP3 sau IMAP
- **MDA** – server folosit pentru copierea sau accesarea mesajelor stocate în casuța poștală, totodată 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



- **Dynamic Host Configuration Protocol**
- Permite configurarea dinamică a clienților (pentru accesul în rețea) folosind informații stocate pe un server
- Informații care pot fi primite de la un server de DHCP:
 - adresa IP
 - subnet mask (masca de rețea)
 - adresa gateway-ului
 - adresa serverului de DNS
 - alte informații opționale

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:

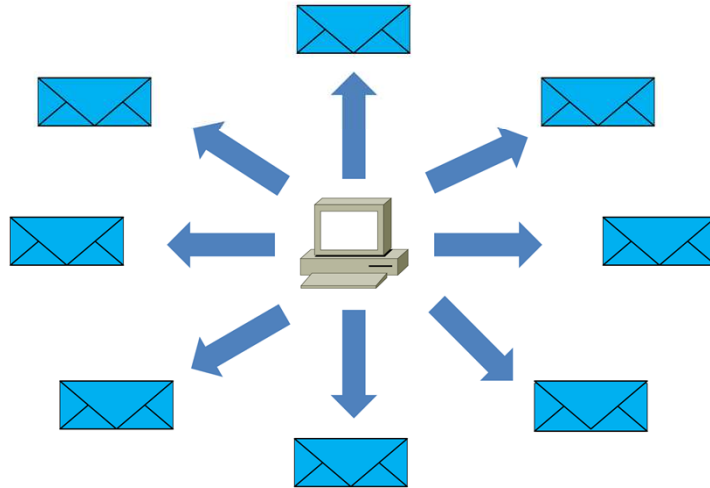
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Ack/Nack

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**)

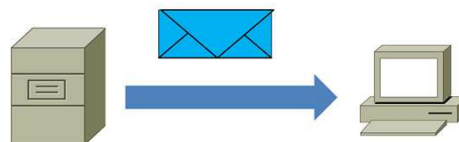


Un client ce dorește ca primească configurațiile necesare pentru a avea acces la resursele rețelei, trebuie să ceară aceste informații unei server DHCP, acest lucru realizându-se printr-un mesaj de tip broadcast UDP, numit „DHCP Discover”. La primirea acestui pachet fiecare server va rezerva pentru client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



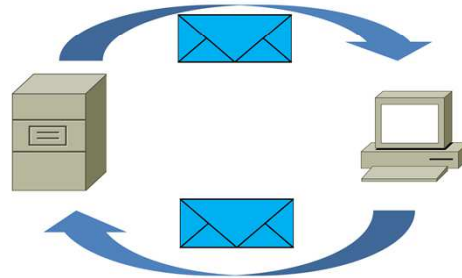
După procesarea cererii și rezervarea IP-ului, serverul va trimite un răspuns de tip unicast clientului, numit „DHCP Offer”.

În cele mai multe cazuri răspunsul va conține următoarele informații:

- 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”**



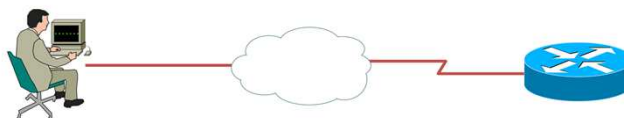
Odată ce pachetul „Offer” este primit de client acesta trimite un mesaj broadcast numit „DHCP Request” pentru a specifica serverului că oferta a fost acceptată. Pachetul este de tip broadcast, deoarece într-o rețea pot exista mai multe servere DHCP, astfel ele fiind informate să elibereze adresele IP 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 denumită 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 serverului
- 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 și de platforma hardware, transferă orice tip de fișiere, oferă posibilitatea gestionării unor restricții și drepturi asupra fișierelor. Modelul FTP folosește două conexiuni: una de control și una de date.

Acest protocol poate rula în două moduri diferite: pasiv și 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 și 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 următoarele caracteristici:

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