



Universitatea “Constatin Brâncuși” din Târgu-Jiu
Facultatea de Inginerie
Departamentul de Automatică, Energie și Mediu

Rețele de calculatoare

Lect. dr. Adrian Runceanu

An universitar 2013-2014

Curs 5

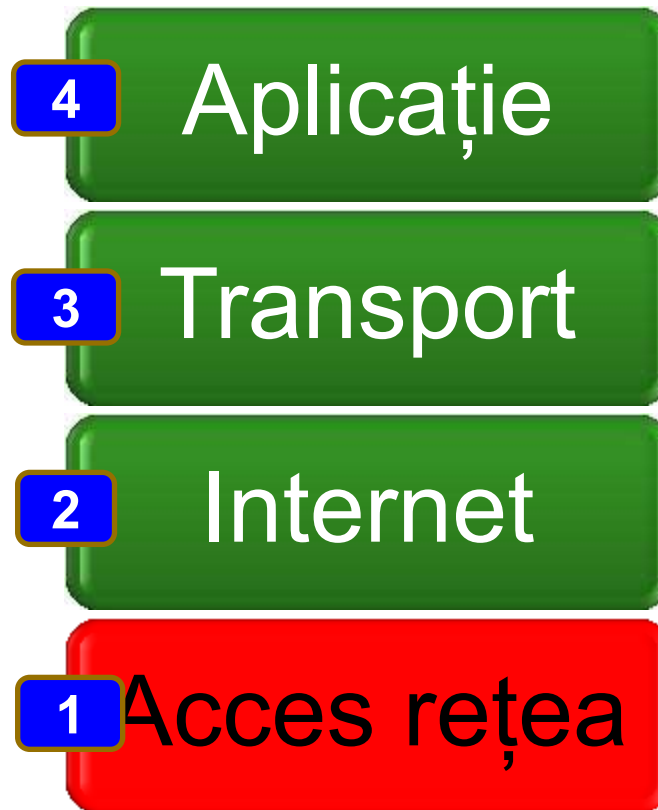
Modele de referință (continuare)

Modele de referință

1. Modelul de referință OSI/ISO

2. Modelul de referință TCP/IP

Nivelul Acces retea



1. Nivelul acces retea este nivelul inferior al stivei si face ca functionarea nivelului imediat superior (numit **Internet** si echivalent **nivelului retea** din modelul **OSI**) să nu depindă de rețeaua fizică utilizată pentru comunicatii si de tipul legăturii de date.

Se identifica in cadrul acestui nivel doua subnivele:

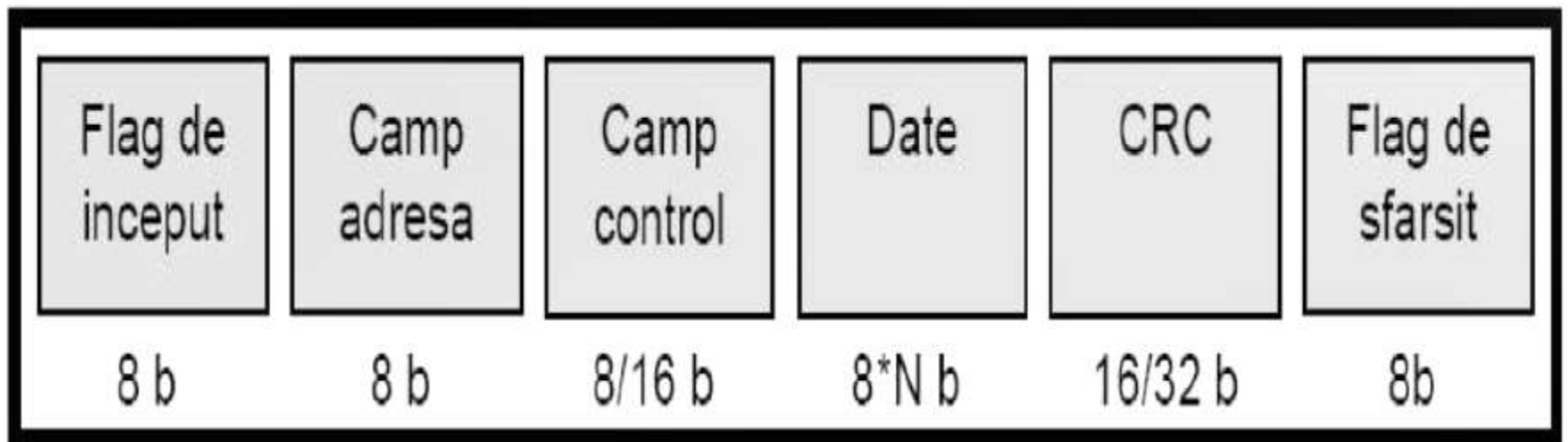
1. subnivelul hardware
2. subnivelul interfetei de retea

1.1. Subnivelul hardware include elemente de conectare fizica (conectica, semnale) care corespund nivelului fizic din modelul **ISO/OSI** respectiv interfetei hardware in modelul **TCP/IP**.

1.2. Subnivelul interfetei de retea se refera la elemente software cum ar fi driverele de retea (cand sistemul este conectat la o retea locală) sau alte subsisteme specifice de gestiune a interfetei.

Cadrul de date HDLC

Cadru de date HDLC



1.2. Subnivelul interfată rețea *intermediază* mesajele transmise între nivelul Internet și mediul fizic de comunicație.

- Pe baza analizei bitilor de control care însoțesc cadrele de date se determină protocolul de comunicație cu care se operează către nivelul următor.
- Către mediul de comunicație putem avea:
 - un acces de tip legătură de date de mare distanță (**circuite punct-la-punct**)
 - sau rețea locală bazată pe protocoale de subnivel **MAC**.

- Accesul la mediul de comunicare pune problema gestionarii traficului in conditiile in care, in mod obisnuit, mai multi clienti partajeaza aceiasi infrastructura.
- *Daca doua sau mai multe statii transmit in acelasi timp apare fenomenul de coliziune si unitatile de date nu mai sunt recuperabile decat prin retransmisie.*

Din acest motiv *la acest nivel se definesc metode si tehnologii de gestiune a accesului la mediul de comunicatie*, cele mai cunoscute fiind urmatoarele:

1. Retele **LAN** cu acces multiplu cu detectarea purtatoarei si a coliziunilor **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**

- ❑ fiecare statie dintr-o retea „asculta” mediul de comunicatie si nu initiaza nici o comunicatie pana cand nu detecteaza „liniste”
- ❑ inainte de a incepe o transmisie se asteapta un timp aleator pentru a evita ca doua statii care au sesizat simultan ca mediul este liber sa inceapa sa transmita in acelasi timp

❑ este o tehnologie specifica retelelor Ethernet 802.3

2. Retele **LAN** cu acces multiplu cu detectarea purtatoarei si evitarea coliziunilor **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance)

- ❑ se bazeaza pe „anuntarea” tuturor statiilor conectate asupra intentiei de a transmite astfel incat acestea evita initierea unei comunicatii in conditiile respective
- ❑ anuntarea prealabila inseamna un trafic suplimentar de tip broadcasting si deci o viteza de transfer utila mai scazuta; se foloseste in retelele Wireless, 802.11

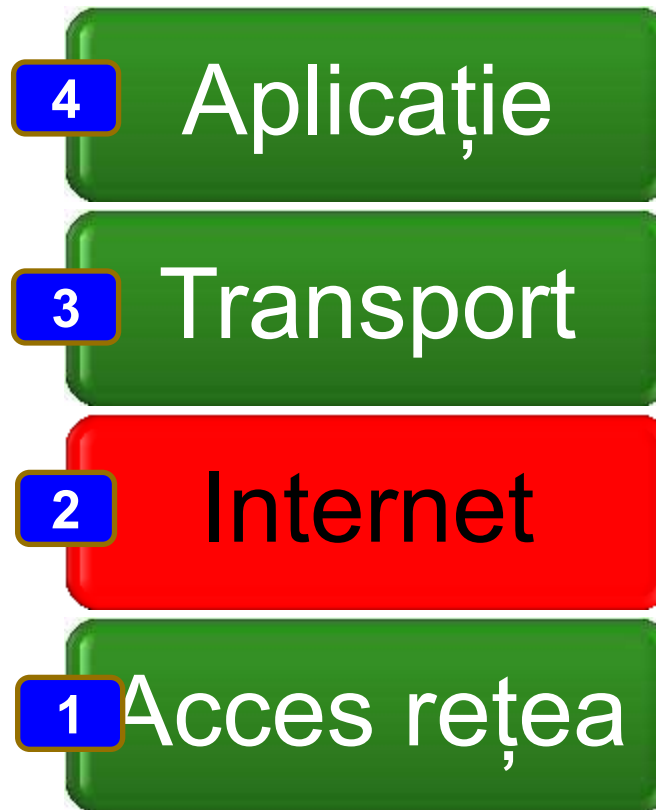
3. Retele **LAN** cu transfer de jeton pe magistrala (Token Bus, 802.4), rețele **LAN** cu transfer de jeton in inel (Token Ring, 802.5)

- gestioneaza accesul prin „tehnica jetonului”, accesul la mediul de comunicatie fiind permis numai statiei care detine jetonul (o secventa de date specifica) la un moment dat.

4. Retele **LAN** bazate pe cerere de prioritate; folosesc echipamente care primesc si analizeaza cererile de acces, avizand sau nu initierea unei transmisii

- permit definirea de prioritati pentru statii sau pentru un anumit tip de trafic
- se utilizeaza in retelele de tip 100VG - AnyLAN si folosesc medii de comunicatie full duplex cu patru perechi de conductoare

Nivelul Internet



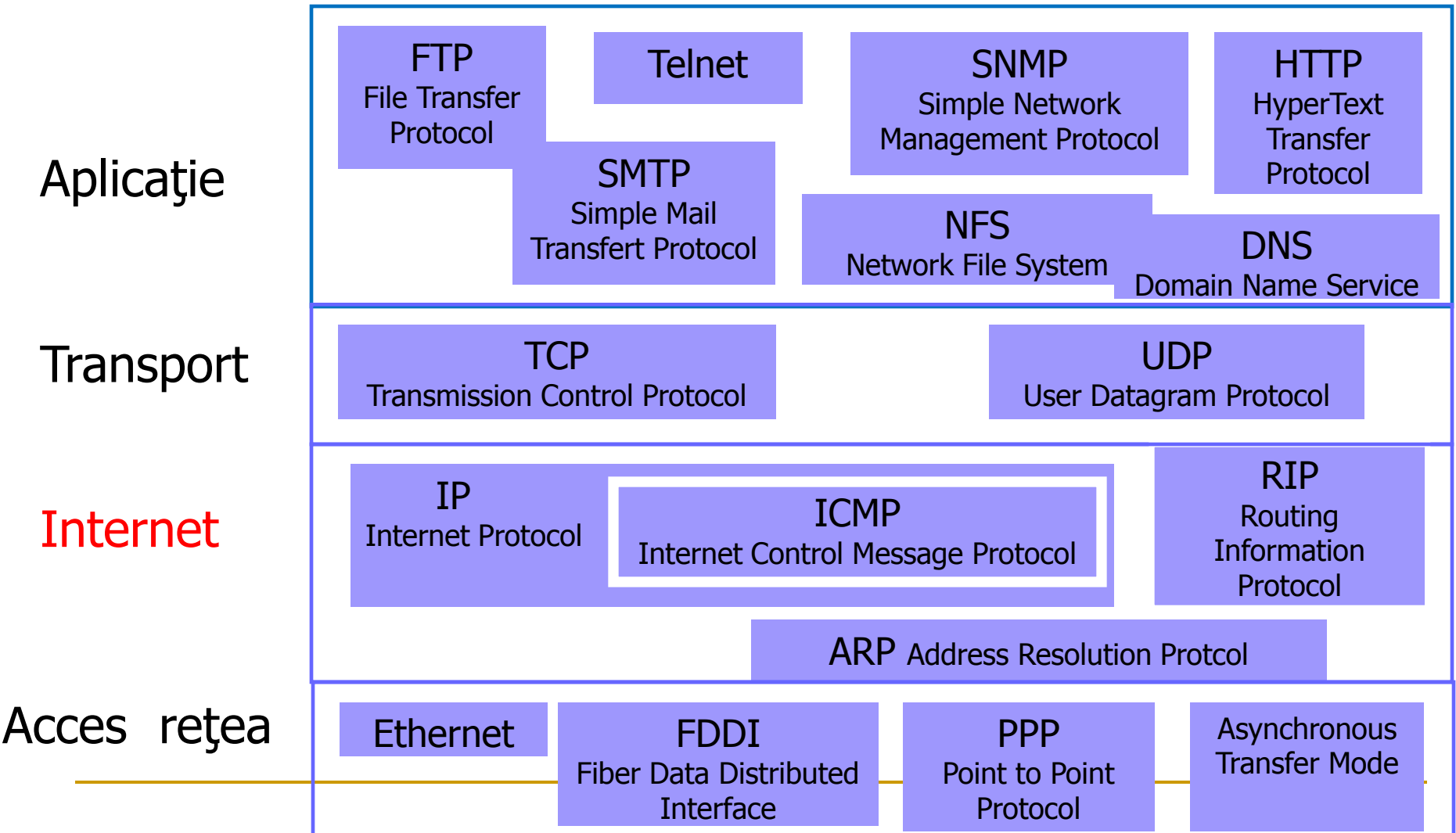
2. Nivelul internet *gestioneaza transmiterea pachetelor de la sistemul sursă la sistemul destinație, independent de conexiune.*

- El are rolul de a permite gazdelor sa emita pachete in orice retea si de a face ca pachetele sa circule independent pana la destinație.

- Pachetele pot chiar sa soseasca intr-o ordine diferita fata de cea in care au fost trimise, reordonarea lor fiind sarcina nivelurilor superioare.
- Nivelul internet defineste in mod particular un **format de pachet** si un protocol numit **IP - Internet Protocol**.
- *Sarcina nivelului internet este sa livreze pachete IP catre destinatie.*

- *Dirijarea pachetelor pe rutele necesare se face prin operatiunea de rutare.*
- La acest nivel opereaza diverse protocoale, toate operand cu o *metoda de identificare a gazdelor* bazata pe o adresare specifica numita *adresare IP*.

Principalele protocoale ale modelului TCP/IP



Principalele protocoale de nivel Internet sunt:

1. Protocolul IP (Internet Protocol) este protocolul de baza in arhitecturile Internet, este reglementat de IETC (Internet Engineering Task Force) RFC 791 si a fost publicat prima data in 1981.

- Acest protocol reglementează sistemul de adresare pe 32 de biți, organizați în patru câmpuri de câte 8 biți. Din acest motiv el se numește și **IPv4**.
- Pentru alocarea automată a adreselor IP s-a propus un alt protocol, **DHCP (Dynamic Host Control Protocol)** care alocă adresele **IP** gazdelor (alături de alte setări de rețea) pe baza adreselor fizice ale interfețelor de rețea.

- **IPv4** permite 4.294.967.296 de adrese independente, numar insuficient, ca urmare a exploziei Internetului si a numarului de gazde conectate.
- In 1994, IETC a adoptat sistemul de adresare cu 6 câmpuri, numit **IPv6**.

2. Protocolul ICMP (Internet Control Message Protocol) foloseste serviciile IP - *mesajul ICMP ocupă campul de date al IP.*

ICMP asigura *un mecanism prin care echipamentele de rutare si sistemele din retea comunică* informatii privind situatiile de functionare defectuasa.

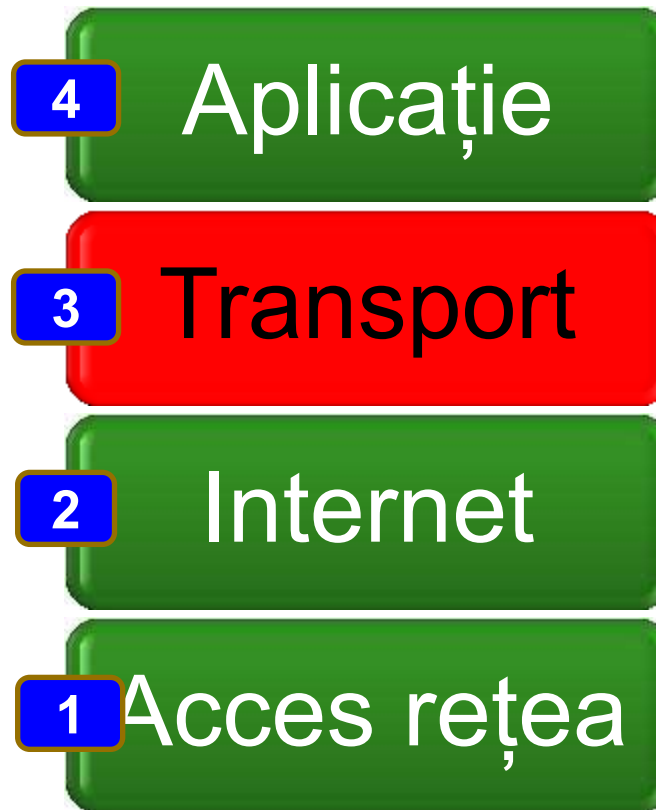
- *Acest protocol se bazeaza pe transferul de pachete ICMP.*
- În mod obisnuit nu este accesat de la nivelul aplicatie, cu exceptia comenzilor de tip **ping** care trimit cereri de ecou ICMP (**ICMP echo request**) si primesc mesaje de raspuns la ecou (**echo response messages**).

3. Protocolul ARP (Address Resolution Protocol) *permite unui sistem să determine adresa fizică (MAC) a unui alt sistem din aceeași rețea fizică cunoscând adresa **IP** (de nivel rețea) a acestuia.*

- ARP face posibil ca adresarea Internet să fie independentă de adresarea la nivel fizic.
- Pentru identificarea adresei **IP** proprii se folosește protocolul **RARP** (Reverse Address Resolution Protocol).

4. Protocolul IGMP (Internet Group Management Protocol) este utilizat pentru gestiunea apartenentei gazdelor la grupuri de distributie multipla.

Nivelul Transport

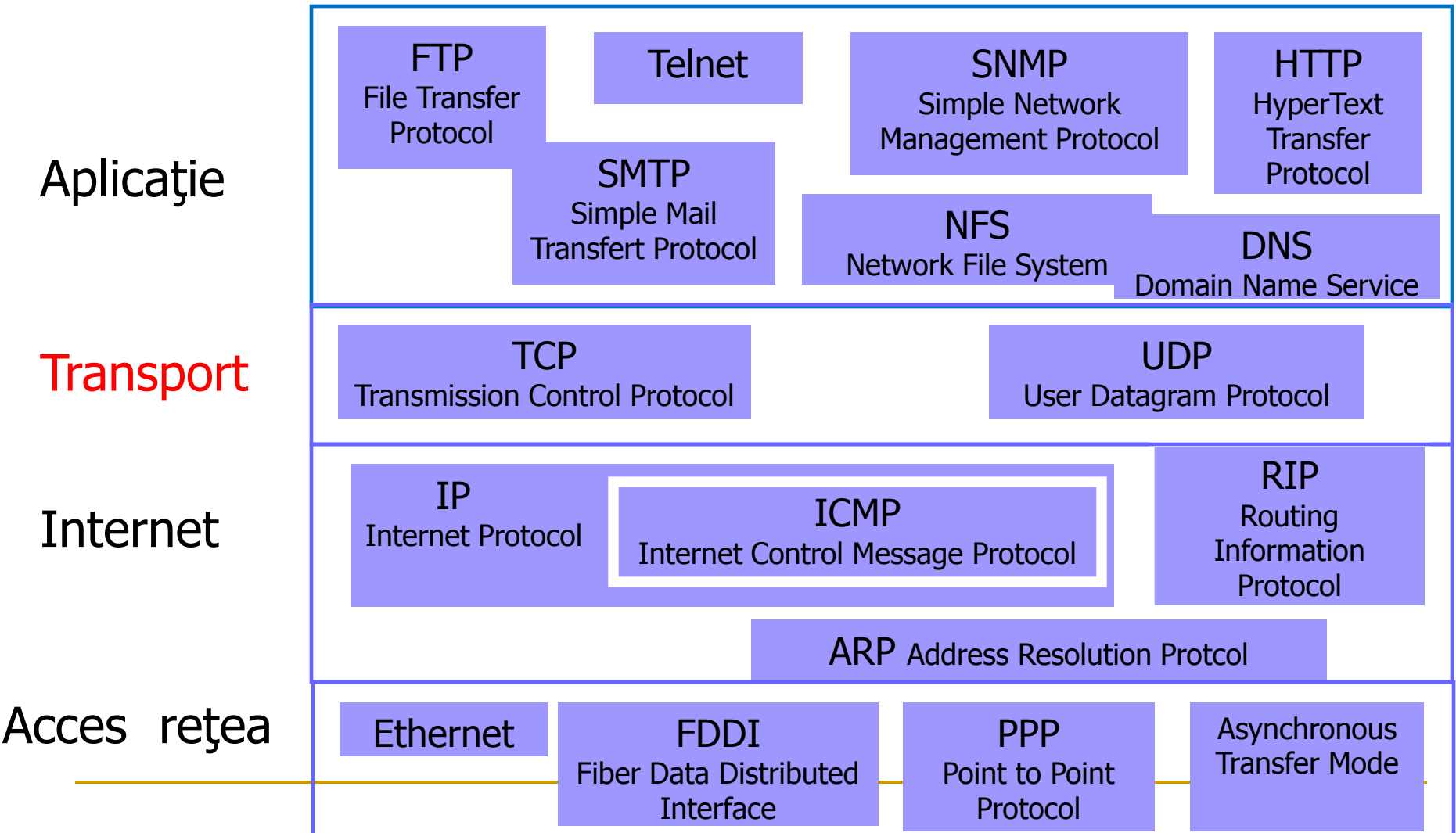


3. Nivelul transport asigură *comunicația între programele aplicație ocupându-se de reglarea fluxului de date și transferul fără erori a secvențelor de date.*

- La nivelul transport fluxul datelor ce trebuie transmise este divizat în pachete.

Cand mai multe programe de nivel aplicatie beneficiază, in acelasi sistem, de serviciile retelei, *nivelul transport trebuie să accepte datele de la acestea si să le transfere spre nivelul inferior*, adăugand fiecărui mesaj informatia necesară pentru identificarea programelor de aplicatie asociate.

Principalele protocoale ale modelului TCP/IP



Sunt folosite două protocoale principale de transport:

1. **UDP (User Datagram Protocol)**
2. **TCP (Transmission Control Protocol)**

dar alături de acestea există și altele.

1. Protocolul **UDP** asigură un serviciu fără conexiune folosind adresarea **IP** pentru transportul mesajelor.

- *Acest protocol*, mai simplu decat **TCP**, *nu garantează livrarea mesajului la receptie* fără erori, fără pierderi, fără duplicate si in ordinea in care a fost emis.
- **UDP** opereaza cu mesaje scurte organizate in datagrame.

- Din acest motiv este un *protocol rapid si eficient* dar care nu garanteaza transferul integral al informatiilor, adica este un *protocol nesigur*.
- Aplicatii uzuale care folosesc **UDP** sunt:
 - serviciile **DNS (Domain Name Services)**
 - aplicatiile multimedia
 - **VoIP (voice over IP)**
 - unele jocuri

2. Protocolul TCP ofera o alternativa de transfer sigur, in ordine si care *garanteaza transferul corect*, orientat pe conexiune.

- ❑ **TCP** este asociat cu majoritatea serviciilor Internet (http, mesagerie electronica, conectare la distanta)
- ❑ Acest protocol are capacitatea de a deservi mai multe aplicatii operand cu mai multe conexiuni numite porturi

- Porturile sunt identificate prin numere pe 16 biti, fiecare numar fiind asociat unei conexiuni.
- La randul lor porturile sunt de 3 categorii:
 - **porturi consacrate** - asociate in general cu aplicatii care „asteapta” in mod pasiv cereri:
 1. **FTP** - port 21
 2. **TELNET** – port 23
 3. **SMTP** – port 25
 4. **HTTP** – port 80sunt definite de **IANA – Internet Assigned Authority**

- **porturi inregistrate** (folosite de aplicatii end-user ca porturi sursa pentru contactarea serverelor)
- **porturi dinamice/private** (folosite tot de aplicatii end-user dar nu in mod sistematic).
- Numarul oficial de porturi recunoscute este **65.535**.

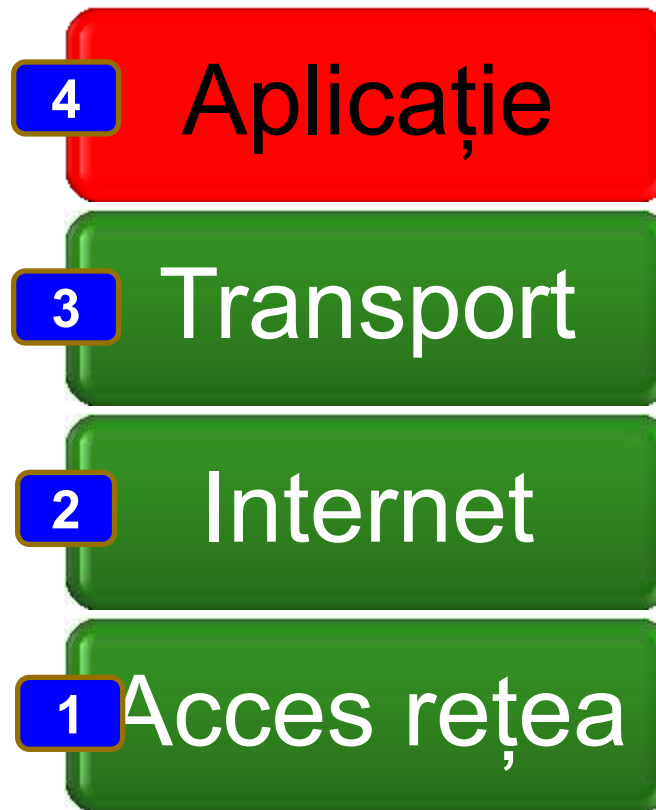
3. Protocolul SCTP (Stream Control Transmission Protocol) a fost definit in anul 2000 (IETF, RFC 2960), este asemanator cu **TCP** dar opereaza la nivel de cadre si nu la nivel de byte ca **TCP**.

- Contine facilitati de control a congestiilor.

4. Protocolul DCCP (Datagram Congestion Protocol) dezvoltat in anul 2005 este destinat aplicatiilor afectate de constrangeri temporale (time senzitive) fiind orientat pe mesaje.

- Scopul este acela de a evita ca unele fragmente de informatie sa ajunga la destinatie atunci cand nu mai sunt necesare.
- Contine specificatii de control a congestiilor.
- Aplicatiile tinta sunt cele din categoria telefoniei **IP** si a stream-urilor multimedia.

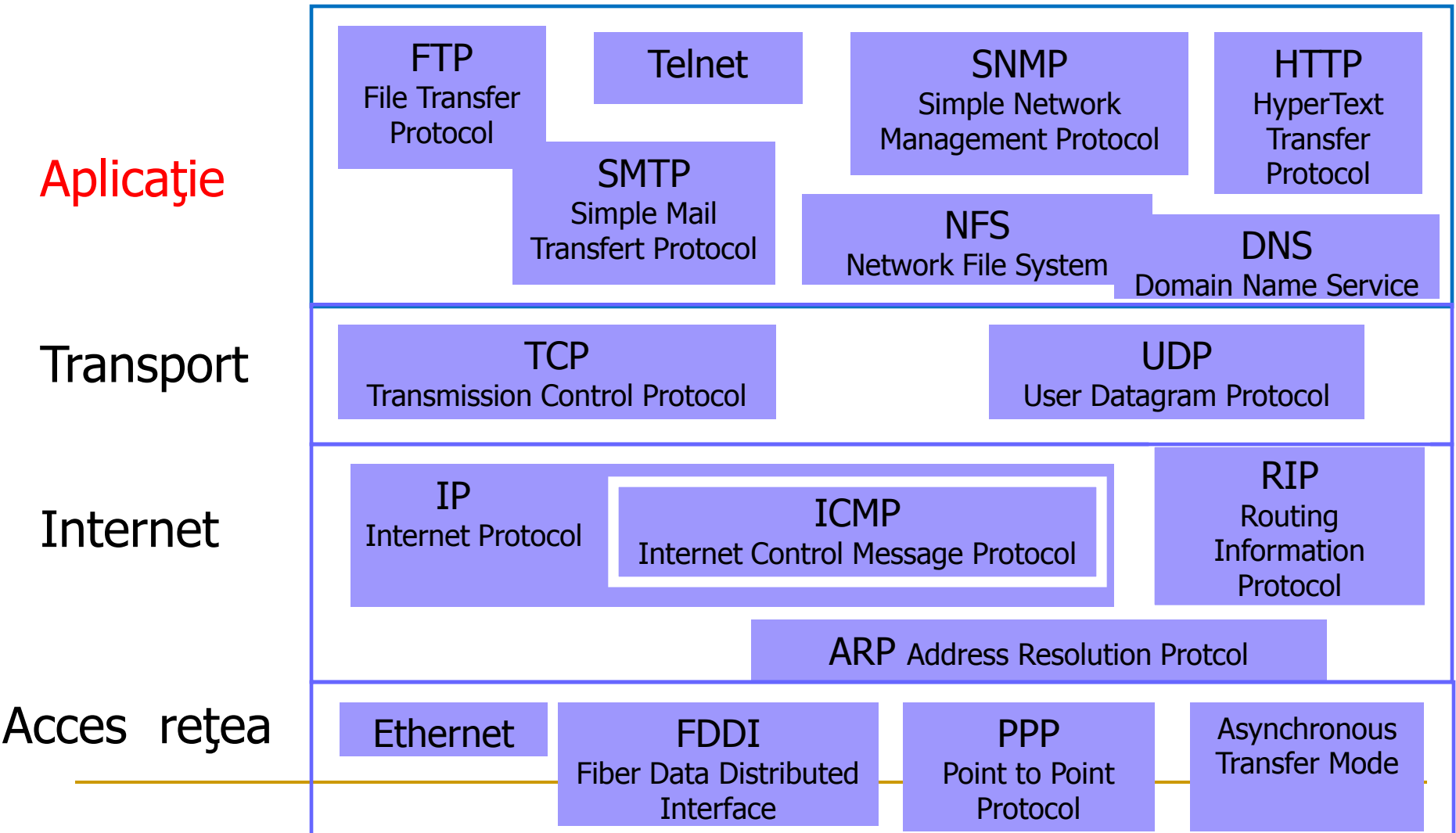
Nivelul Aplicație



4. Nivelul aplicatie asigură utilizatorilor rețelei, prin intermediul programelor aplicatie, accesul la servicii de retea.

- Protocoalele de la acest nivel se adreseaza conexiunilor de transport deci au asociate porturi specifice identificate prin valori numerice (in cazul in care se bazeaza pe **TCP**).

Principalele protocoale ale modelului TCP/IP



Cele mai frecvent folosite
protocoale sunt:

1. Protocolul HTTP (HyperText Transfer Protocol) - port 80 definește
maniera de transport pentru
informațiile de tip **www**, **World Wide
Web**.

2. Protocolul HTTPS (HyperText Transfer Protocol Secure) – port implicit 443 reprezinta *versiunea securizata a lui HTTP*.

- A fost propus de Netscape Communication Corporation pentru autentificarea si criptarea transferurilor de informatii.
- Sirurile tip text sunt criptate in vederea transferului folosind **SSL** (secure socket layer) sau **TLS** (transport layer security).

3. Protocolul SMTP (Simple Mail Transfer Protocol) – port 25 este folosit pentru *transferul (expedierea) in mod text a mesajelor de poștă electronică* către o destinație verificabilă.

- Sta la baza serviciului e-mail.

4. Protocolul FTP (File Transfer Protocol) – port 21 permite *utilizatorilor transferul de fisiere intre un sistem local si unul aflat la distanta.*

- Transferul se face in mod text (caractere **ASCII** sau **EBCDIC**) sau binar.

5. Protocolul Telnet – port 23 este utilizat pentru *conectarea la distanta pentru stabilirea de relatii tip client-server intre* sistemul local (client) si aplicatia Telnet distantă (server).

- In acest mod terminalul local functioneaza ca interfata virtuala de tip text sau terminal virtual (simuleaza local o interfata text VT-100 pentru un sistem distant).

6. Protocolul UUCP (Unix to Unix Copy Protocol) – port 540 este *destinat executiei de instructiuni la distanta si transferului de fisiere* intre masini **UNIX**.

- Este folosit in principal pentru comunicatii modem dar si pentru transferuri **TCP/IP**.

7. Protocolul NNTP (Network News Transfer Protocol) – port 119, NNTPS – port 563 *defineste transferul de informatii text de tip stiri electronice (e-news) intre servere.*

- Permite postarea si citirea de articole prin conectare la server si crearea de grupuri de stiri (newsgroup).

8. Protocolul SSH (Secure Shell Port) – port 22 definește *posibilitatea de conectare la distanță la un server și executarea de comenzi* în mod similar cu **telnet** (sau **rlogin**, **rsh**) oferind însă posibilitatea de criptare a transferului (conexiune securizată).

- Tunelul securizat astfel creat poate fi utilizat și de alte servicii sau transferuri de fișiere (cu funcțiile scp, sftp).
- O versiune mai nouă, SSH-2 oferă algoritmi superiori de criptare și identificare a partenerilor pe baza de adresă MAC precum și posibilități de a iniția mai multe sesiuni shell peste aceeași conexiune SSH.

9. Protocolul IRC (Internet Relay Chat) este *destinat comunicatiilor de tip text, on-line, in cadrul unor grupuri de discutie (forum-uri) sau pentru comunicatii unu-la-unu.*

- Fiind un protocol ce utilizeaza tranferul de tip text rezulta ca poate fi grefat pe orice sesiune **TCP** sau **SSL**.
- Necesita server **IRC** fara/cu identificarea utilizatorului (nick-name) si permite cascadata cu mai multe servere similare pentru expandarea retelei **IRC**.
- Un client uzual de **IRC** sub Windows este **mIRC**, care foloseste porturi intre 6667 si 7000.

10. SNMP (Simple Network Management Protocol) permite *gestiunea centralizata a echipamentelor care suporta acest protocol dintr-o retea.*

- Sunt cunoscute trei variante SNMP:
 - SNMP v1 este prima versiune (1988) si prezenta deficiente de securitate prin transmiterea necriptata a parolelor
 - SNMP v2 introduce noi functii de securitate / confidentialitate si administrare grupata fara insa se devina larg utilizat datorita unor inconsecvente ale standardului
 - SNMP v3 versiunea din 2004.

11. H323 – definește generic *protoacoale de comunicatie pentru sesiuni audio-video fiind utilizat de aplicatii ca NetMeeting (Windows), GnomeMeeting (Linux).*

- Un protocol alternativ este **SIP** (utilizat de **Skype**), mai nou si mai performant dar incompatibil cu H323.
- H323 este primul protocol **VoIP** (Voice over IP) care adopta **RTP** (Real Time Protocol) pentru transportul audio/video in retelele IP.

12. SIP (Session Initiation Protocol) este un protocol dezvoltat separat de H323, tot pentru transport VoIP dar incluzand functii care permit procesarea convorbirilor precum si functionalitati similare telefoniei publice.

- SIP se ocupa in principal de semnalizari si lucreaza in conjunctie cu alte protocoale, cum ar fi SDP (Session Description Protocol) care defineste continutul sesiunii, porturi utilizate, codec-uri.

13. RTP (Real-time transport Protocol) *definește formatul standard al pachetelor de transport a pachetelor audio/video peste Internet.*

- A fost elaborat în 1996 (RFC 1889) inițial ca protocol multicast dar folosit ulterior și în sesiuni unicast videoconferință, telefonie IP).
- Funcționează în conjuncție cu RTCP (RTP Control Protocol).

14. RTCP (RTP Control Protocol) este un *protocol complementar lui RTP* si asigura in special transportul feedback-urilor pentru RTP (important in gestiunea QoS, Quality of Services).

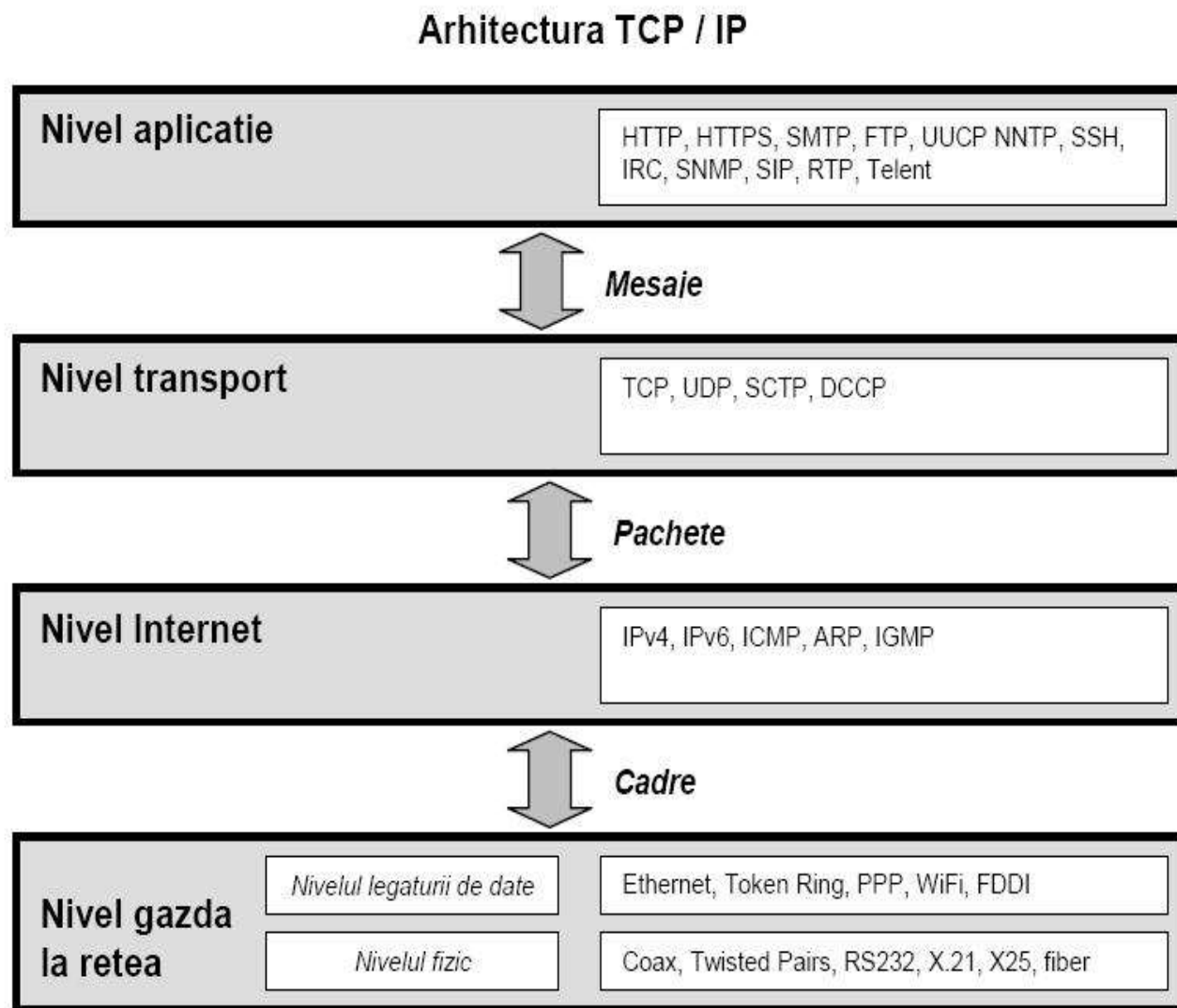
- Gestioneaza informatii referitoare la mediul de conectare, bytes transmisi, pachete pierdute, jitter, intarzieri date care permit aplicatiei sa eficientizeze transmisia (nivelul compresiei, de exemplu).
- Desi este implicat in impachetarea si furnizarea informatiilor multimedia, RTCP nu transporta date propriu-zise.

La **nivel aplicatie** exista o gama foarte larga de programe, functii, comenzi.

Cateva utilitare de retea uzuale sunt urmatoarele:

1. **Ipconfig** - afiseaza configuratia TCP/IP curenta
2. **Netstat** - asigura setarile si conexiunile protocolului TCP/IP
3. **Route** - afiseaza sau modifica tabela de rutare locala
4. **Tracert** - verifica ruta catre un sistem aflat la distanta

O structura de ansamblu a arhitecturii **TCP/IP** si a modului de interactiune a diverselor protocoale specifice:



Întrebări?