Sisteme de operare
Rețele (2)

Sorin Milutinovici
sorinmilu@gmail.com

Recapitulare

- Un dispozitiv conectat la rețea are un adaptor de rețea care funcționează pe baza următoarelor informații:
- Adresa Hardware - un fel de număr de serie al adaptorului determinat în timpul procesului de fabricație, independent de utilizator
- Adresa IP - un număr de 32 de biți parte dintr-un sistem internațional de adrese finit. În rețelele locale, adresele IP sunt convertite în adrese hardware prin protocolul ARP
- Netmask - un sistem de separare a adreselor IP locale (care se pot trimite direct către adresele hardware) de celelalte adrese pentru care pachetele trebuie trimise la router.
- Gateway - adresa IP a unui computer sau alt fel de dispozitiv la care se vor trimite pachetele care nu sunt destinate

Adresa IP a dispozitivului poate fi de două feluri: adresă IP rutabilă sau adresă IP nerutabilă.

Dispozitivele cu adrese nerutabile pot accesa internetul folosind un protocol special implementat în routere, numit NAT (Network Address Translation).

Marea majoritate a rețelelor private, care conțin dispozitive care nu au instalate pe ele programe de tip server, au acum adrese nerutabile.

Open Systems Interconnect (OSI)

Pentru a putea transmite informație unui computer aflat la distanță, avem nevoie de un set de standarde care să conlucreze. Aceste standarde se ocupă de fiecare “strat” al sistemului electric/logic/informatic.

Stratul 7 (aplicații)	Standarde de comunicare informațională (HTTP, FTP).
Stratul 6 (prezentare)	Standarde de transfer al informației și de serializare: XML, JSON, la care se poate adăuga criptare, compresie etc.
Stratul 5 (sesiune) NetBios, RPC	Deschide conexiuni, închide conexiuni, asigură securitatea mesajelor
Stratul 4 (transport) TCP, UDP (porturi)	Proceduri de control al transferului de mesaje, sisteme de testare a eficienței și calității transferului de date
Stratul 3 (network) Adresa IP	Transmitere primară de informații încapsulate în seturi de semnale, sisteme de direcționare a informației în funcție de sursă și destinație (ex: rutere)
Stratul 2 (data link) Adresa MAC	Adresare primară: mai multe dispozitive conectate pe același fir pot transmite informații între ele cunoscându-și adresele. Aici se găsesc și dispozitivele de multiplexare (switchuri)
Stratul 1 (fizic)	Cabluri, conectori, fire, semnale

https://osi-model.com/

Ce înseamnă www.google.com ?

- Protocolul IP se ocupă de transferul și rutarea informației pe internet. Imediat după primele implementări ale acestuia, a devenit evident faptul că este foarte dificil pentru oricine să țină minte adrese IP.
- Prima încercare de rezolvare a acestei probleme a fost apariția unui fișier (numit hosts) în care se puteau da nume diferitelor adrese IP.
- Rețeaua ARPANET distribuia un fișier hosts care era întreținut de o singură persoană. Fiecare nou computer trebuia să se înregistreze în fișierul care trebuia redistribuit tuturor computerelor existente. Destul de rapid această metodă și-a dovedit limitele.
- Paul Mockapetris a propus un sistem distribuit de completare automată a relației dintre nume și adrese IP.
- Sistemul propus de el este unui ierarhic care permite delegarea responsabilităților întreținerii tabelelor de corespondență între nume și ip.
- Acest sistem se numește Domain Name System și este utilizat în continuare, într-o arhitectură nu foarte diferită de cea propusă de Mockapetris.

Paul Mockapetris

DNS (Domain Name System)

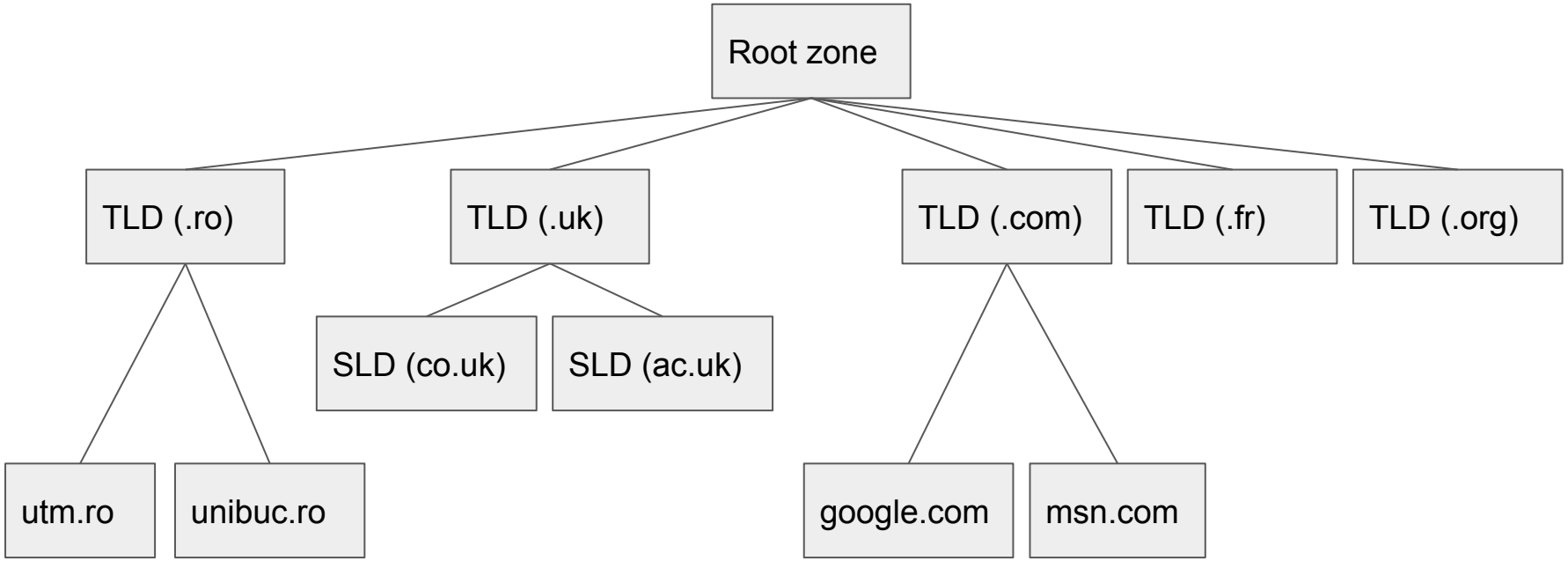
- Toate comunicațiile între computere se fac pe baza adreselor IP.
- Majoritatea solicitărilor făcute însă de utilizatori, prin intermediul programelor, se fac pe baza numelor.
- Sistemul DNS este o agendă globală care returnează aplicațiilor adresa IP corespunzatoare unui anumit nume.
- Fiecare dispozitiv conectat la internet are, pe lângă cele necesare comunicării prin IP (adresa IP, netmask etc.) și unul sau mai multe IP-uri ale unui nameserver.
- Un nameserver este un computer care rulează un software special care se ocupă de “rezolvarea” numelor și returnează adrese IP corespunzatoare.

Serverul DNS utilizat pentru interogare

Răspunsul serverului

```
root@student:~# nslookup google.com

Server:         62.149.128.4
Address:        62.149.128.4#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.205.110
```

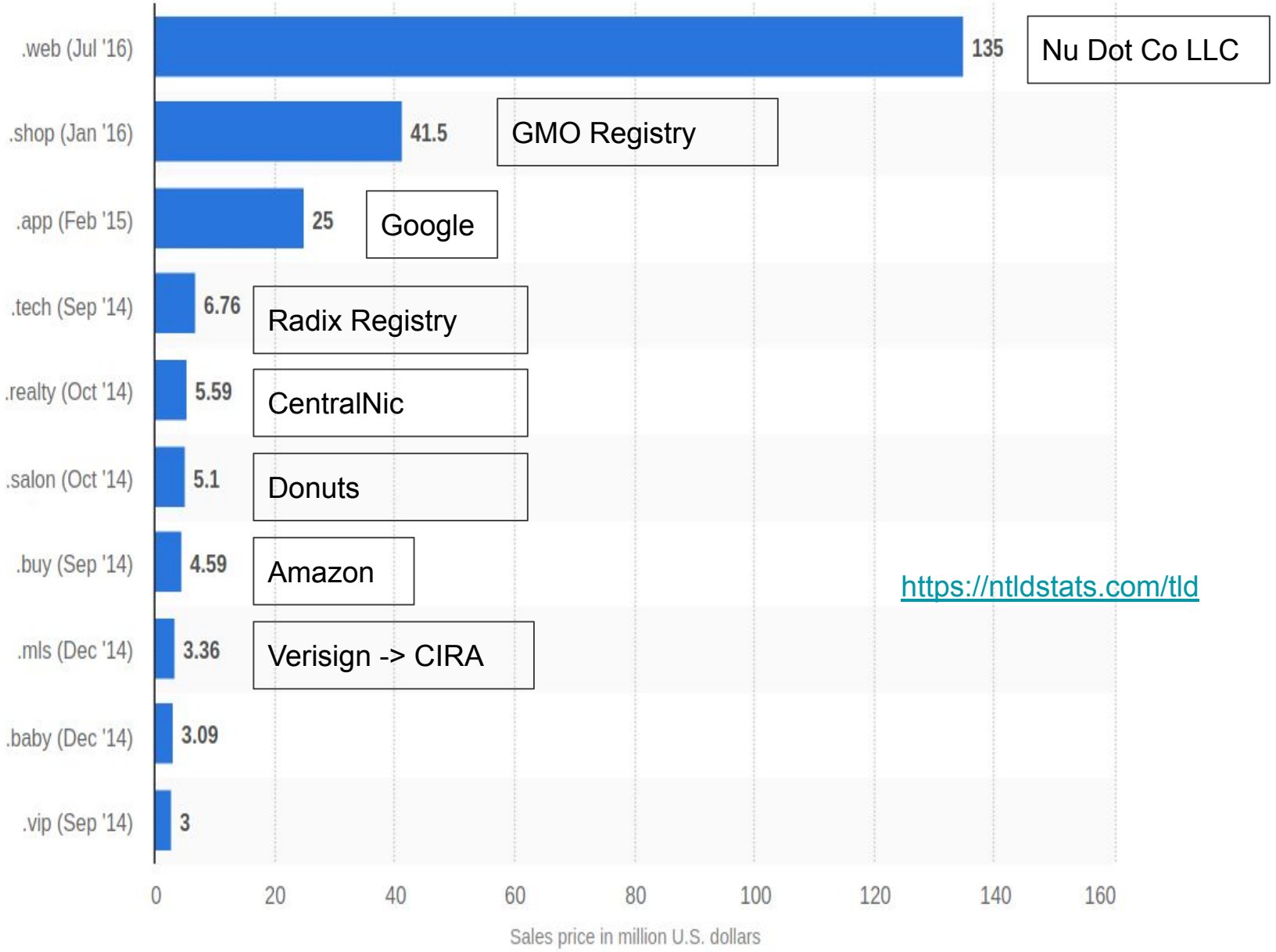
Serverele de nume principale (root name servers)



- Fiecare zonă are cel puțin un nameserver principal.
  Zonele care sunt imediat subordonate zonei principale se numesc “Top Level Domains”
  TLD-utile sunt de mai multe feluri:
  - TLD-uri generice (.com, .org, .info)
  - TLD-uri pentru fiecare țară (doua litere: .ro, .uk, .fr)
  - TLD-uri sponsorizate de anumite organizații (.aero, .cat, .asia)
- Anumite țări au Secondary Level Domains (SLD): ex: Marea britanie

- 1998 - information.ca din Toronto a plătit 50 de milioane de dolari țării Tuvalu pentru cedarea dreptului de folosință a TLD-ului atribuit (.tv) până în 2048. Tuvalu a folosit prima tranșă de 1 milion de dolari pentru a intra în Organizatia Națiunilor Unite.

GTLD

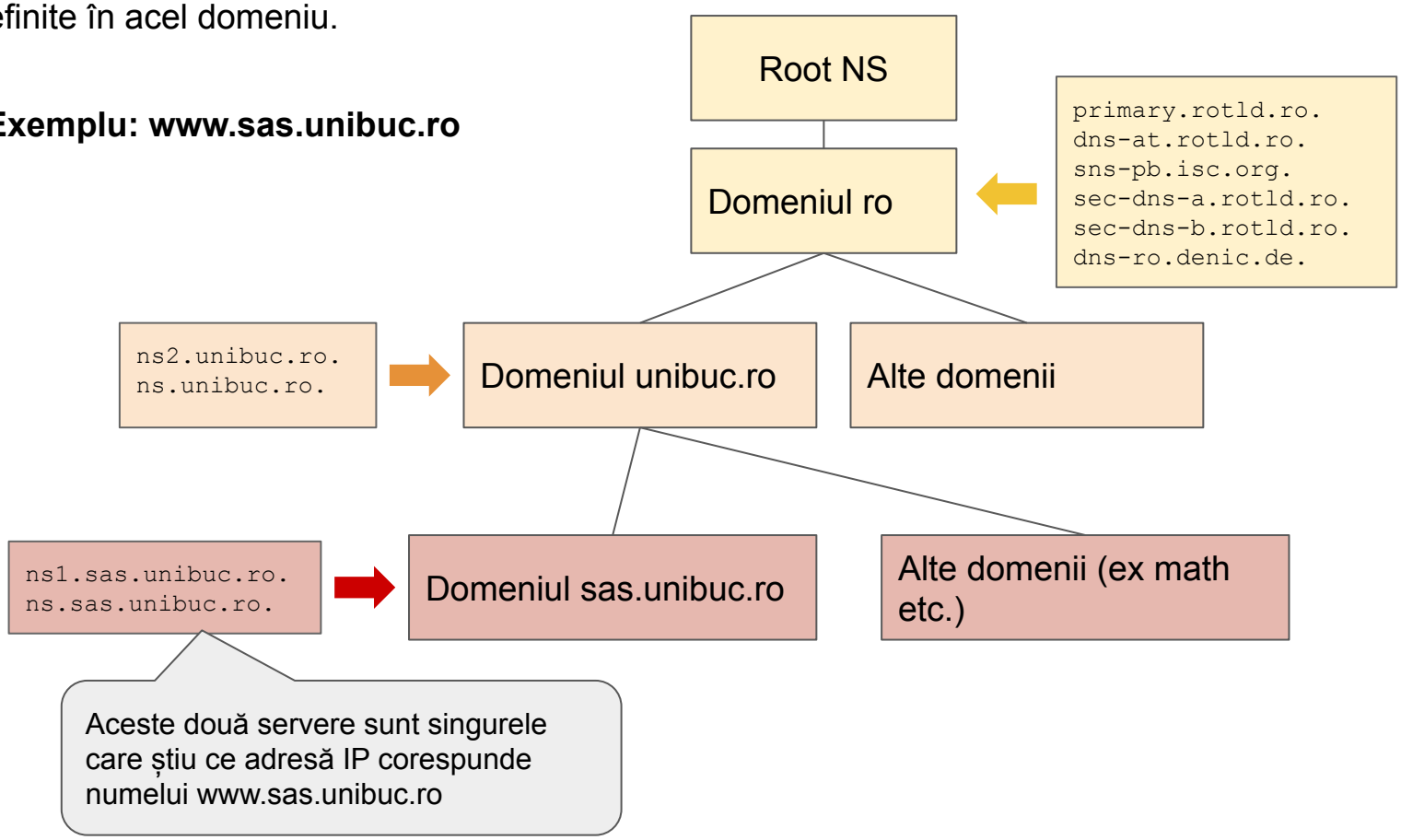


https://ntldstats.com/tld

DNS (Domain Name System)

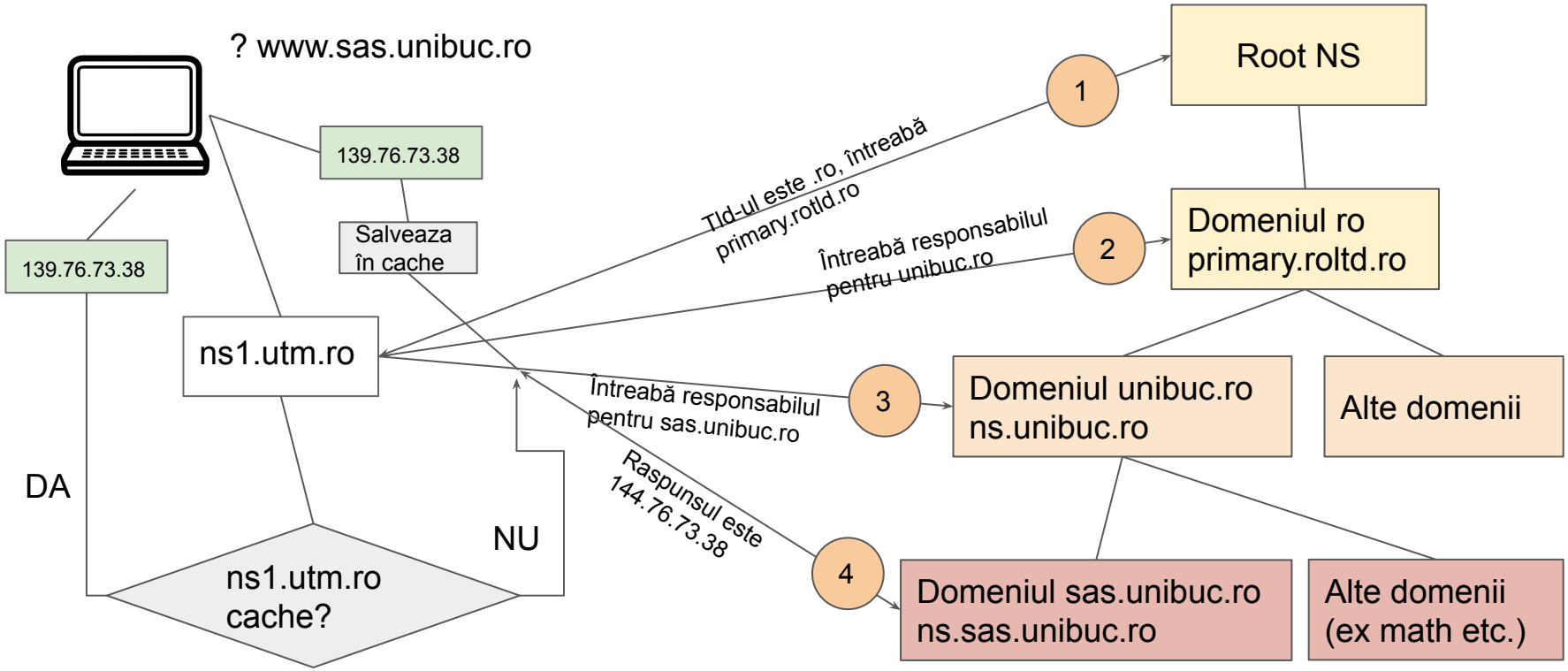
- DNS se bazează pe noțiunea de “domeniu”. Un domeniu este un șir care identifică în mod unic o anumită “zonă” a internetului. Fiecare nume înregistrat în sistemul DNS este un domeniu.
- Fiecare domeniu este compus din mai multe componente. Fiecare component reprezintă o zonă.
- Fiecare zonă are cel puțin un nameserver care este responsabil de a menține lista tuturor numelor definite în acel domeniu.

Exemplu: www.sas.unibuc.ro



DNS (Domain Name System)

- În încercarea de a afla adresa IP a unui anumit nume, un computer poate interacționa cu două tipuri de servere de nume:
- Serverele care conțin liste de nume și care reprezintă sursa autoritară pe un anumit domeniu (authoritative servers)
- Serverele care sunt folosite doar pentru a oferi serviciul de rezolvare a adreselor, fără să conțină în realitate nici o lista proprie (recursive servers).



Propagarea modificărilor

- Toate serverele de nume mențin un cache al tuturor interogărilor reușite. De asemenea, fiecare server de nume are o listă a tuturor serverelor de nume principale (root name servers).

- Relația dintre numele de domeniu și IP-uri nu este însă fixă. Un anumit domeniu (ex: www.google.com) poate să se mute de pe un IP pe altul. Dacă aceasta se întâmplă, toate serverele care au IP-ul vechi în cache vor returna dispozitivelor care le întreabă un răspuns greșit.

  Pentru ca răspunsul să devină corect, este nevoie ca înregistrarea respectivă să fie ștearsa din cache. Ștergerea din cache se întâmplă în două cazuri:

  - Administratorul serverului de nume solicită în mod expres golirea cacheului
  - Înregistrarea expiră.

- Expirarea înregistrării este posibilă pentru că serverul autoritar pe domeniul respectiv publică, împreună cu relația domeniu - IP, și un interval în secunde care informează toate celelalte servere de nume cât să țină înregistrarea în cache.

- Pentru a minimiza traficul DNS (care este semnificativ), multe companii publică intervale foarte mari - de ordinul zilelor. De aceea, propagarea mutării unui domeniu de pe un IP pe altul poate să dureze până la câteva zile.

Serverul de nume - fișier de zonă (bind)

SOA - Start of Authority.
Fiecare domeniu trebuie să aibă o înregistrare de tip SOA

```
$TTL      86400
@    IN   SOA  ns1.greencore.ro. postmaster.greencore.ro. (
                        2017111701     ; serial,
                        28800               ; refresh, seconds
                        7200           ; retry, seconds
                        604800              ; expire, seconds
                        86400 )             ; minimum, seconds


*               86400 A            193.228.153.170
agora           86400 A            193.228.153.170
aqua            86400 A            193.228.153.170
bell            86400 A            193.228.153.170
laborator         300 A            94.130.12.51
student          3600 A            80.211.136.82
mail            86400 A            193.228.153.170
ns1             86400 A            193.228.153.170
talk            86400 A            91.199.243.5
templates       86400 A            193.228.153.170
www             86400 A            193.228.153.170
www2            86400 CNAME        www.greencore.ro
greencore.ro. 86400  MX  10  mail.greencore.ro.
greencore.ro. 86400  NS       ns1.greencore.ro.
```

A - address - cele mai comune tipuri de înregistrări, cele pentru care s-a inventat DNS-ul

CNAME: un alias al altei înregistrări; interogarea va fi refacută cu noua valoare

MX: Mail exchanger, IP-ul serverului responsabil pentru a primi emailuri pentru adresele acestui domeniu

NS: numele serverului care are autoritate asupra acestui domeniu

Transfer al zonelor

- Clienții serverelor de nume interoghează serverele pentru a obține informații. Fiecare tip de înregistrare (A, NS, MX, SOA) poate fi apelată prin specificarea tipului de înregistrare pe care o dorim

```
sorin@student:~$ host -t MX google.com

google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
```

- Pentru a putea avea mai multe servere de nume sincronizate automat pentru același domeniu, pe lângă interogările obișnuite, există un tip special numit interogare AXFR (Asynchronous Full Transfer Zone).
- AXFR este o tranzacție care folosește TCP, nu UDP. Pentru a putea obține o anumită zonă prin AXFR, trebuie ca serverul responsabil de ea să accepte acest gen de interogări. În general, serverele NU acceptă interogari AXFR decât de la alte servere secundare.
- 19 Sept 2016, serverul de nume principal din Corea de nord a fost prost configurat să accepte interogări AXFR de la orice alt server. Astfel, zonele au fost copiate și s-a constatat că în Coreea de Nord exista 28 de site-uri web.

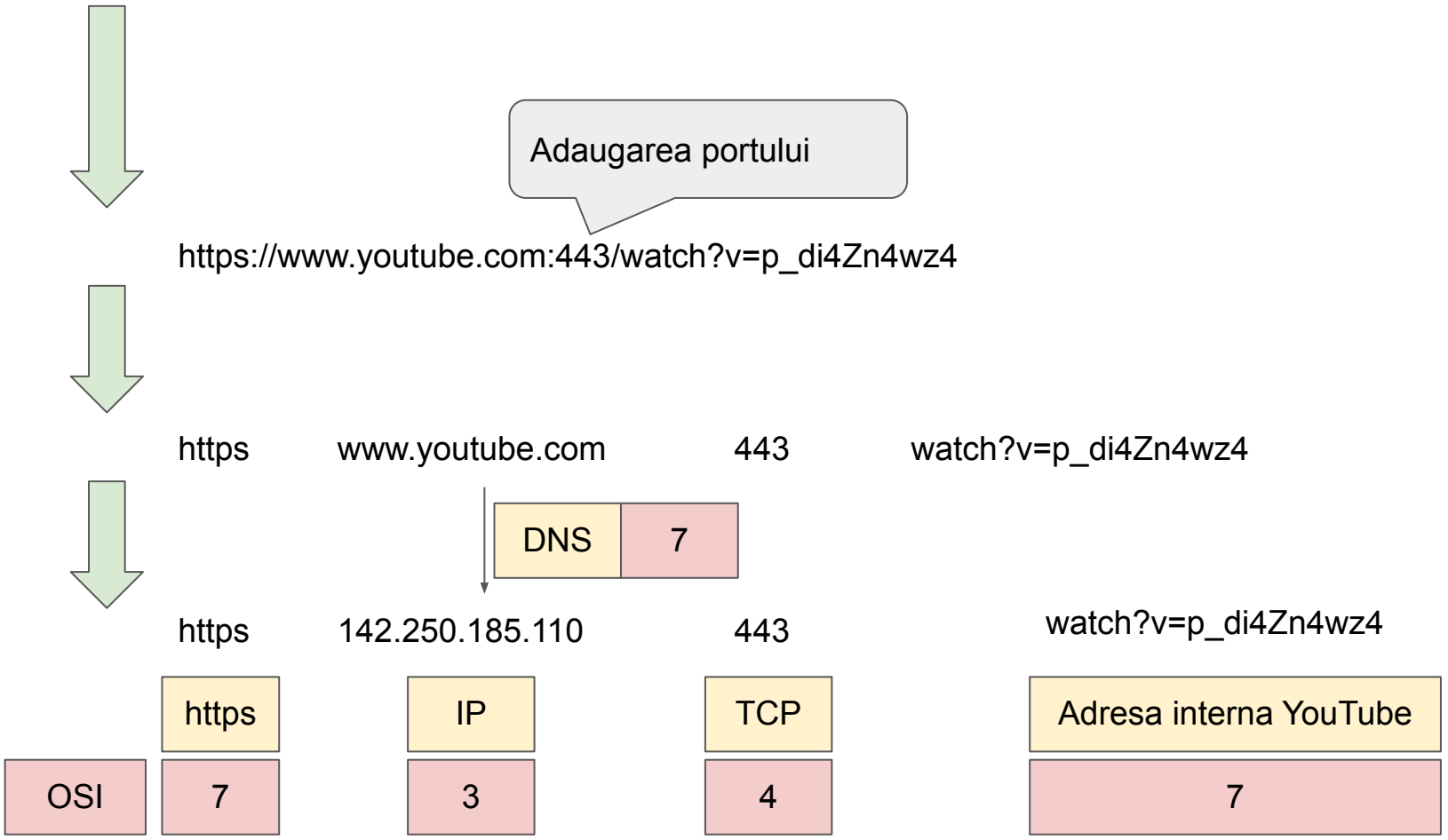
Zonele se gasesc la https://github.com/mandatoryprogrammer/NorthKoreaDNSLeak

Interogare generală

```
[root@isp named]# host -a greencore.ro

Trying "greencore.ro"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49922
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;greencore.ro.                  IN    ANY

;; ANSWER SECTION:
greencore.ro.             86400    IN      MX    10 mail.greencore.ro.
greencore.ro.             86400    IN      NS    ns1.greencore.ro.
greencore.ro.             86400    IN      A     193.228.153.170
greencore.ro.             86400    IN      SOA   ns1.greencore.ro.
postmaster.greencore.ro. 2017111701 28800 7200 604800 86400

;; ADDITIONAL SECTION:
mail.greencore.ro.        86400    IN      A     193.228.153.170
ns1.greencore.ro.         86400    IN      A     193.228.153.170

Received 164 bytes from 193.228.153.170#53 în 9 ms
```

Nameserverele sunt programe care ascultă pe portul 53, protocolul UDP. Majoritatea comunicării este făcută prin pachete UDP, cu excepția tranzacțiilor care depășesc 512 octeți și a tranzacțiilor AXFR

https://www.youtube.com/watch?v=p_di4Zn4wz4



DHCP

- Majoritatea dispozitivelor care se conectează la rețele, în special cele care au conexiuni temporare (wireless, 3G - 4G) nu solicită utilizatorului să completeze detaliile cu privire la adresa IP.
- Adresa IP, gateway-ul, netmaskul și toate celelalte informații se obțin automat de către dispozitive.
- Sistemul care permite această automatizare se numește DHCP (Dynamic Host Configuration Protocol).
- DHCP este un protocol care permite atribuirea automată a adreselor IP dispozitivelor care solicită aceasta.
- Tot protocolul DHCP oferă celelalte informații necesare pentru funcționarea pe rețea a dispozitivului (gateway, netmask, server DNS etc.)
- Protocolul DHCP funcționează în sistemul client-server. Orice rețea pe care DHCP funcționează are cel putin un program software special numit DHCP server. Serverul deschide portul 67 UDP iar fiecare client va deschide portul 68 UDP.

TCP, UDP

Ethernet și IP sunt protocoale proiectate să asigure transmiterea informației între dispozitive, în mod uniform.

TCP și UDP sunt protocoale de comunicare între aplicații software.

TCP

- Implica deschiderea unei conexiuni persistente între client și server
- Asigură ajungerea informațiilor la destinație, este capabil să solicite retransmisia acestora
- Asigură ordinea corectă a mesajelor

UDP (User Datagram Protocol)

- Nu implică deschiderea unei conexiuni persistente
- Ajungerea la destinație a mesajelor trimise nu poate fi verificată
- Mesajele nu ajung în ordine
- UDP poate trimite mesaje în sistem broadcast, TCP nu

Cum arată o sesiune DHCP

- În momentul în care noul dispozitiv se conectează fizic la rețea (fie că e vorba de rețea cu fir, fie că e vorba de rețele fără fir), acesta nu are adresa IP și nu știe nimic despre rețeaua în care s-a conectat.
- Interfața de rețea a dispozitivului respectiv este configurată astfel încât să încerce să își ia elementele de configurare folosind protocolul DHCP.
- Serverele de DHCP ascultă pe portul 67 și așteaptă pachete UDP.
- Dar portul este o specificație a standardului TCP/IP, deci portul are nevoie de IP.
- **Cum trimitem pachete către un IP fără să avem o adresă de IP? Fără să avem nici o cunoștință despre adresele IP ale dispozitivelor din rețea?**

Network, broadcast

Adresa rețelei locale în format decimal → 80.211.136.0

Adresa maximă în format decimal → 80.211.136.255

IP-urile rețelei locale sunt între 80.211.136.0 și 80.211.136.255. Pentru orice alt IP sistemul trebuie să trimită pachetele către router.

- Aplicând netmaskul 255.255.255.0 reușim să izolăm un număr de 255 de posibile adrese IP pentru rețeaua locală. Din ele însă, nu putem atribui dispozitivelor decât 254.
- 80.211.136.0 este adresa rețelei. Ea este folosită de către routere pentru a trimite pachetele către alte rețele. Fiecare router are o tabelă de rețele însoțită de un anumit gateway. În orice grup de adrese stabilit pe baza netmaskului, prima adresă este a rețelei și nu poate fi folosită.
- 80.211.136.255 de asemenea nu poate fi folosită: ea este utilizată pentru trimiterea pachetelor către toate IP-urile din clasa curentă. Ultima adresă se numește “Broadcast” și nu poate fi atribuită unui computer pentru că există comunicații extrem de importante (ex: arp) care trebuie să poată fi trimise către toate IP-urile din clasă.

Adresa 255.255.255.255 va funcționa ca adresă de broadcast în orice rețea, indiferent de IP-urile din acea rețea. Indiferent de IP-ul serverului DHCP, acesta va primi pachetele trimise către adresa 255.2555.255.255. IP-ul sursă este 0.0.0.0.

Cum arată o sesiune DHCP (principiul DORA)

DHCP**D**ISCOVER

MAC sursa:	02:F2:d6:68:3f:0f
MAC destinatie:	FF:FF:FF:FF:FF:FF
IP sursa:	0.0.0.0
IP dest:	255.255.255.255

Clientul trimite pe rețea pachete către toate dispozitivele exprimând dorința de a primi un IP.

DHCP**O**FFER

MAC sursa:	90:eB:34:dC:93:B4
MAC destinatie:	02:F2:d6:68:3f:0f
IP sursa:	192.168.1.1
IP dest:	255.255.255.255

Serverul rezervă o adresă IP dintr-un grup disponibil și trimite mesajul DHCP OFFER care conține acest IP și perioada în care clientul are voie să folosească acest IP înainte de a reface cererea. Mesajul este trimis către toata rețeaua

DHCP**R**EQUEST

MAC sursa:	02:F2:d6:68:3f:0f
MAC destinatie:	FF:FF:FF:FF:FF:FF
IP sursa:	0.0.0.0
IP dest:	255.255.255.255

Clientul trimite mesajul DHCP REQUEST către toată rețeaua în care întreabă dacă poate utiliza IP-ul oferit de serverul respectiv.
Aceasta folosește pentru eventualitatea în care sunt mai multe servere DHCP pe rețea.

DHCP**A**CK

MAC sursa:	90:eB:34:dC:93:B4
MAC destinatie:	02:F2:d6:68:3f:0f
IP sursa:	192.168.1.1
IP dest:	255.255.255.255

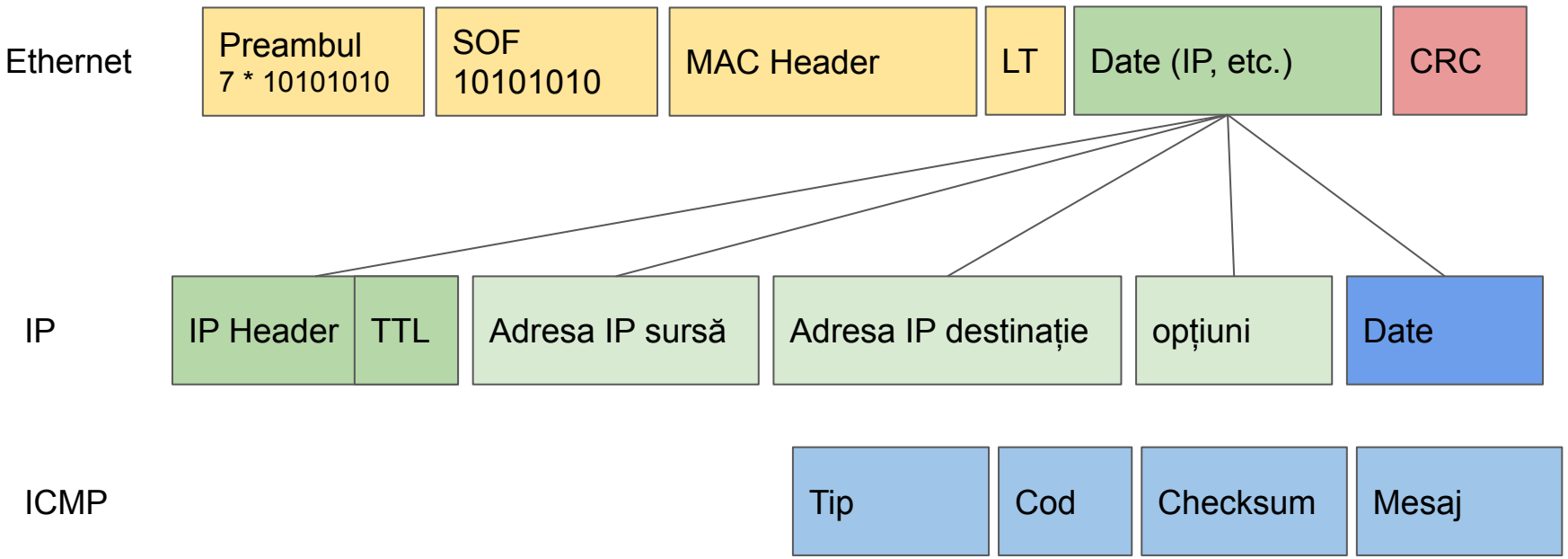
Serverul confirmă faptul că IP-ul este utilizabil și rezervat pentru MAC-ul clientului.

Cum arată o sesiune DHCP

- Fiecare IP care este trimis către un dispozitiv este “inchiriat” pe o durată specificată în configurarea serverelor.
- Când perioada de timp depașește jumătate din timpul de închiriere, clientul trimite direct un pachet DHCPREQUEST către server (posibil pentru că acum clientul are IP). Serverul răspunde cu un pachet de tip DHCPACK (afirmativ), caz în care IP-ul se reînchiriază, sau DHCPNACK (negativ) , caz în care dispozitivul trebuie să reînceapă procesul cu un pachet de tip DHCPDISCOVER.
- Dacă la trecerea a 87.5% din timpul de închiriere clientul NU poate comunica direct cu serverul DHCP, acesta va trimite un pachet de tipul DHCPREQUEST dar nu doar către serverul care i-a “închiriat” IP-ul ci în sistem broadcast.
- Un al server poate răspunde cu DHPCACK sau DHPCNACK, caz în care clientul păstrează IP-ul reținând IP-ul noului server care i-a acordat noul lease.

Internet Controls Message Protocol (ICMP)

- ICMP este un protocol IP, la fel ca TCP și UDP.
- ICMP nu este conceput pentru transferul de date între rețele/dispozitive, este un protocol utilitar care permite verificarea funcționării corecte a rețelelor și a dispozitivelor.
- Pachetele ICMP sunt tratate diferit de către sistemele conectate la rețea. De regulă, driverele sistemului de operare direcționează pachetele TCP sau UDP către aplicațiile ale căror porturi sunt specificate în headerul TCP, în cazul ICMP-ului pachetele sunt desfăcute, conținutul lor este verificat la nivelul nucleului și tot nucleul acționează în consecință.



Ping (Tip 8 în header)

- Un pachet ICMP cu tipul 8 informează dispozitivul de destinație că dorește să capete un răspuns de la acesta (Echo request).

```
root@student:~# ping 127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.040 ms
```

- În momentul în care pachetul ICMP ajunge la destinație, dispozitivul (dacă nu e configurat să nu răspundă la ping) va trimite către dispozitivul inițial un alt pachet ICMP care va conține în header tipul 0 (Echo reply).

```
root@student:~# ping 216.58.205.228

PING 216.58.205.228 (216.58.205.228) 56(84) bytes of data.
64 bytes from 216.58.205.228: icmp_seq=1 ttl=55 time=15.4 ms
64 bytes from 216.58.205.228: icmp_seq=2 ttl=55 time=15.4 ms
```

- Orice pachet IP are în header o informație numită TTL (Time To Live) care asigură faptul că pachetele nu se for plimba la nesfârșit pe rețea. Fiecare router prin care trece pachetul respectiv va scădea valoarea TTL, când aceasta ajunge la 0 pachetul este ignorat de routerul respectiv.

- Valoarea TTL-ului arată numărul de routere prin care a trecut pachetul trimis de către dispozitivul de la distanță pe drumul către dispozitivul de la care a fost executată comanda ping.

Ping

Diferite dispozitive aleg valori diferite ale TTL-ului inițial când crează un pachet ICMP. În majoritatea cazurilor TTL-ul este configurabil.

Windows 95/98	32
Windows (altele)	128
Free BSD	64 / 255
Linux / Alte versiuni de UNIX	64

Ping of death

Un pachet ICMP are de obicei 56 octeți. În același timp, un pachet IPv4 poate avea dimensiuni până la 65.536 octeți. Multe sisteme de operare nu puteau procesa pachete ICMP de dimensiuni mari și, când primeau unul, nucleul se oprea cu o eroare de tip buffer overflow, oprind computerul.

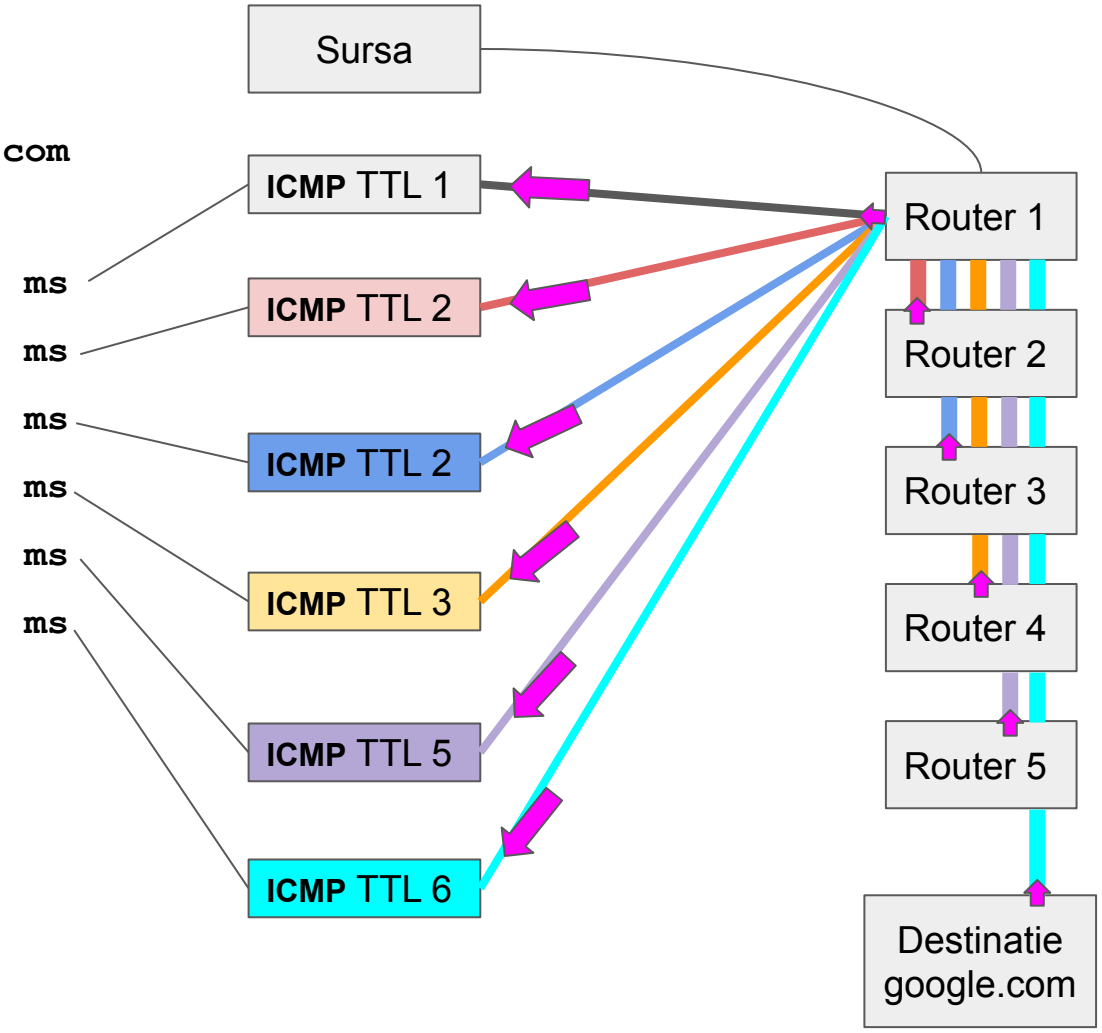
ICMP flood attack

Pachetele ICMP trimise pe comanda ping solicită serverului destinație trimiterea unui pachet răspuns. Dacă se trimit extrem de multe, serverul destinație se poate bloca în crearea unei cantități prea mari de pachete de răspuns.

Traceroute

Traceroute este un program care folosește în mod inteligent TTL-ul pachetelor IP pentru a descoperi routerele prin care trec pachetele de la sursă la destinație.

```
traceroute -I -n google.com

 1   80.211.136.2   12.479 ms
 2   62.149.185.99   0.731 ms
 3   62.149.191.50   7.286 ms
 4   217.29.66.96    7.776 ms
 5   216.239.42.19   7.748 ms
 6   216.58.205.110  7.624 ms
```



Rutare

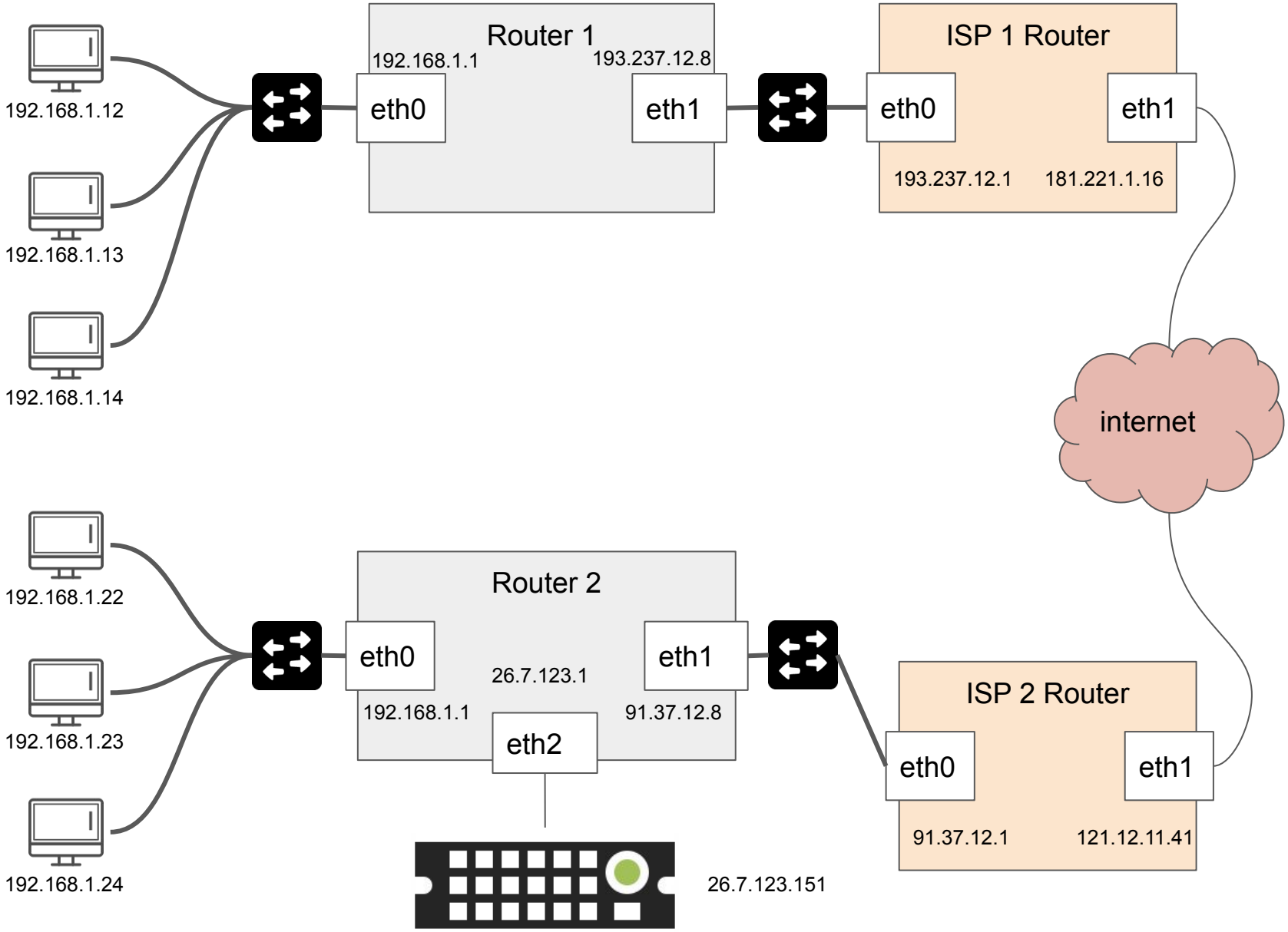
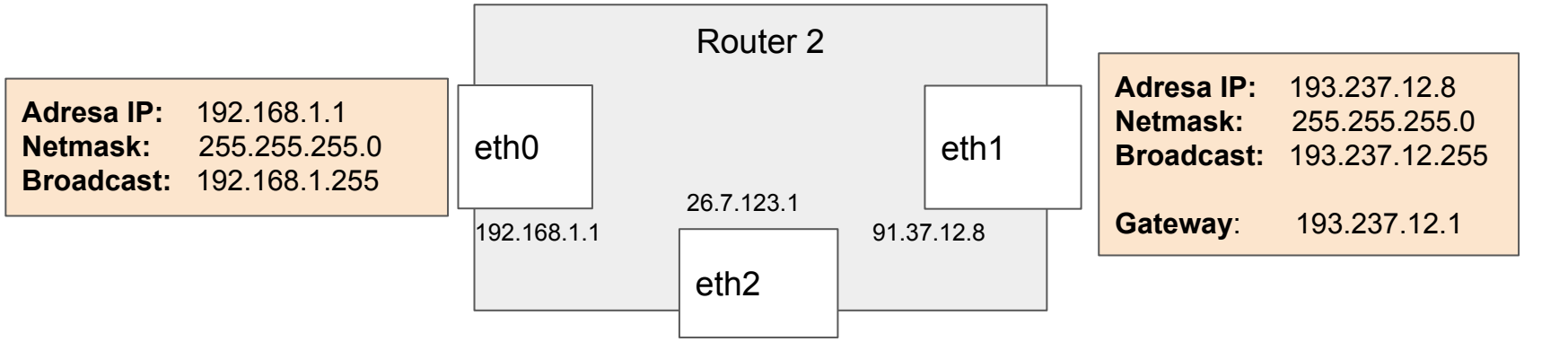

Router 1
192.168.1.1
193.237.12.8
eth0
eth1
ISP 1 Router
eth0
eth1
193.237.12.1
181.221.1.16
192.168.1.12
192.168.1.13
192.168.1.14
internet
192.168.1.22
192.168.1.23
192.168.1.24
Router 2
eth0
26.7.123.1
192.168.1.1
eth1
91.37.12.8
eth2
ISP 2 Router
eth0
eth1
91.37.12.1
121.12.11.41
26.7.123.151

Tabela de routare



Adresa IP: 192.168.1.1
Netmask: 255.255.255.0
Broadcast: 192.168.1.255

Adresa IP: 193.237.12.8
Netmask: 255.255.255.0
Broadcast: 193.237.12.255

Gateway: 193.237.12.1

Adresa IP: 26.7.123.1
Netmask: 255.255.255.0
Broadcast: 26.7.123.255

Configurare a retelei

```
NETWORKING=yes
GATEWAY=193.237.12.1
GATEWAYDEV=eth1
```

Configurare a nucleului

```
net.ipv4.ip_forward = 1
```

```
root@fireles:~# route -n

Kernel IP routing table
Destination  Gateway      Genmask          Flags Metric Ref  Use Iface
0.0.0.0      193.237.12.1 0.0.0.0          UG       0    0        0 eth1
193.237.12.0 0.0.0.0      255.255.255.0    U        0    0        0 eth1
127.0.0.0    0.0.0.0      255.0.0.0        U        0    0        0 lo
26.7.123.1   0.0.0.0      255.255.255.0    U        0    0        0 eth2
192.168.1.0  0.0.0.0      255.255.255.0    U        0    0        0 eth0
```

Configurarea interfețelor de rețea

192.168.1.12

Adresa IP:	192.168.1.12
Netmask:	255.255.255.0
Broadcast:	192.168.1.255
Gateway:	192.168.1.1

192.168.1.13

Adresa IP:	192.168.1.13
Netmask:	255.255.255.0
Broadcast:	192.168.1.255
Gateway:	192.168.1.1

Adresa IP:	192.168.1.1
Netmask:	255.255.255.0
Broadcast:	192.168.1.255

Router 1

eth0 — 192.168.1.1

eth1 — 193.237.12.8

Adresa IP:	193.237.12.8
Netmask:	255.255.255.0
Broadcast:	193.237.12.255
Gateway:	193.237.12.1

Configurare a retelei

```
NETWORKING=yes
GATEWAY=193.237.12.1
GATEWAYDEV=eth1
```

Configurare a nucleului

```
net.ipv4.ip_forward = 1
```

Configurare a nucleului

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Configurarea interfețelor de rețea

192.168.1.12

Adresa IP: 192.168.1.12
Netmask: 255.255.255.0
Broadcast: 192.168.1.255

Gateway: 192.168.1.1

Adresa IP: 192.168.1.1
Netmask: 255.255.255.0
Broadcast: 192.168.1.255

Router 1

eth0 — 192.168.1.1

eth1 — 193.237.12.8

Adresa IP: 193.237.12.8
Netmask: 255.255.255.0
Broadcast: 193.237.12.255

Gateway: 193.237.12.1

192.168.1.13

Adresa IP: 192.168.1.13
Netmask: 255.255.255.0
Broadcast: 192.168.1.255

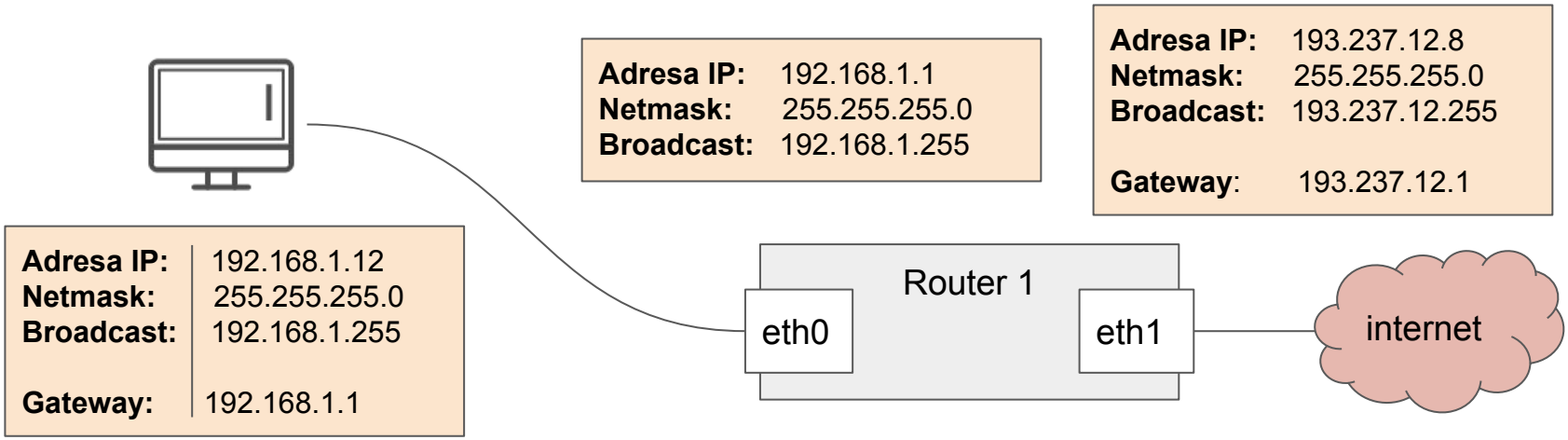
Gateway: 192.168.1.1

```
root@router:~# route -n

Kernel IP routing table

Destination  Gateway      Genmask         Flags Metric Ref    Use Iface
0.0.0.0      193.237.12.1 0.0.0.0          UG    0      0        0 eth1
193.237.12.8 0.0.0.0      255.255.254.0    U     0      0        0 eth1
127.0.0.0    0.0.0.0      255.0.0.0        U     0      0        0 lo
192.168.1.0  0.0.0.0      255.255.255.0    U     0      0        0 eth0
```

Gateway 0.0.0.0
inseamna nespecificat

Flags:
U = UP
G = Gateway
H = host

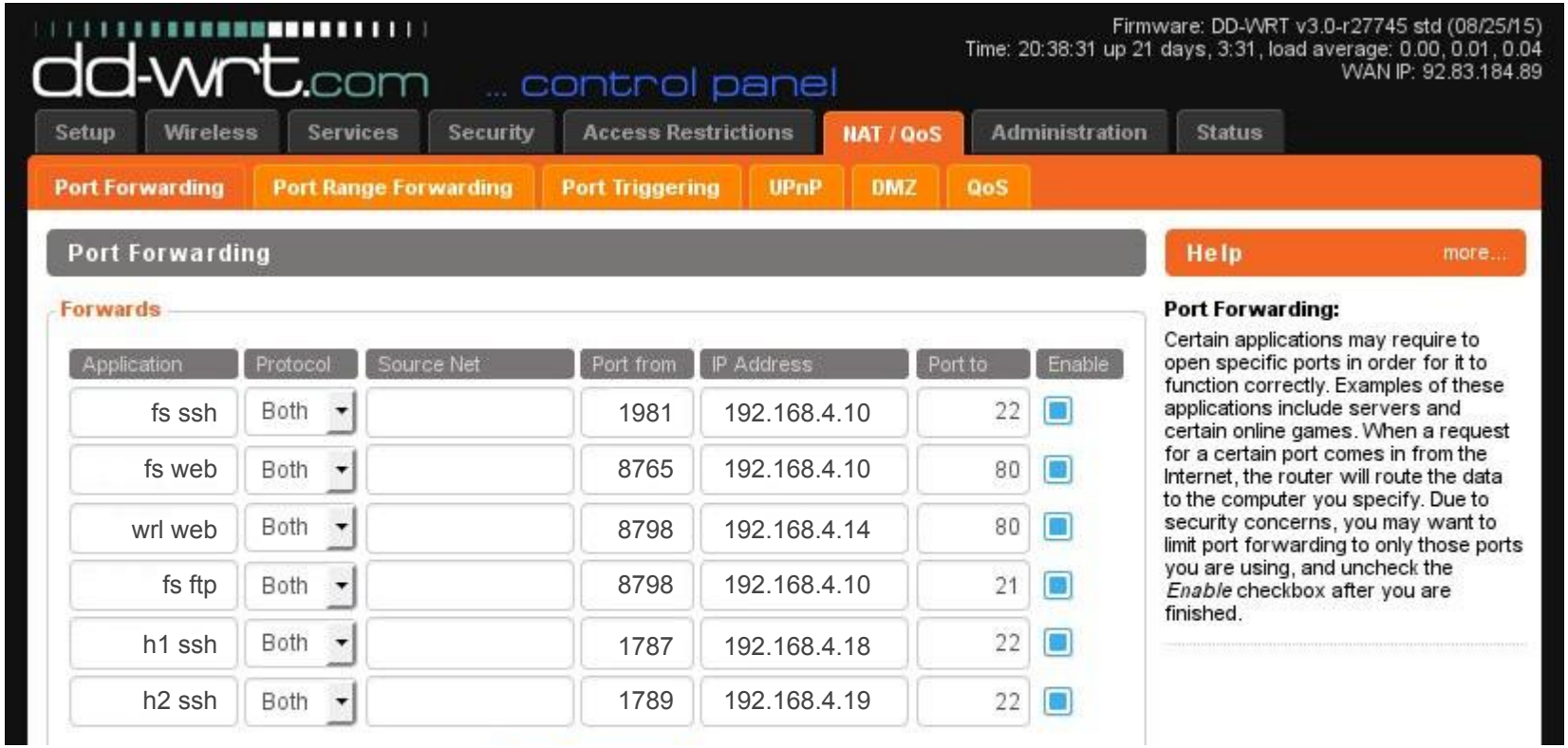
Network Address Translation




```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- Un pachet pleacă de la stația de lucru cu IP-ul sursă 192.168.1.12 și ip-ul destinație 172.217.18.78 Serverul îl primește pe placa de rețea eth0 și ar putea să-l trimită mai departe dar, dacă sursa pachetului rămâne nerutabila (192.168.1.12), pachetul nu va trece de următorul router.
- Network Address Translation este un sistem implementat în nucleul sistemului de operare care rescrie adresa sursă a pachetelor, înlocuind-o cu adresa publica a lui (a interfeței eth1), înainte de trimiterea lor către internet.
- Astfel, pentru toate celelalte routere din internet, pachetele provenite de la stația de lucru par a proveni de pe router, au IP de proveniență rutabil și pot fi trimise mai departe. Routerul menține un tabel cu toate aceste rescrieri de adrese pentru a putea recunoaște pachetele răspuns, a le înlocui adresa destinație cu cea a stației de proveniență (192.168.1.12) și a le trimite spre interfața eth0

Port forwarding



iptables -A PREROUTING -t nat -p tcp -d 92.86.21.12 --dport 1981 -j DNAT --to 192.168.4.10:22

- Port forwarding este un anumit fel de Network Address Translation care trimite toate comunicările destinate unui port oarecare pe router către un alt port deschis pe un computer cu adresă nerutabilă aflat în spatele routerului.
- Folosind port forwarding se pot expune către internet servicii deschise pe computerele cu adrese nerutabile și/sau se pot ascunde (nu cu foarte mare succes) anumite servicii din spatele routerelor.