Elemente de configurare rețea

Utilizarea Sistemelor de Operare

Paul Irofti

Universitatea din București
Facultatea de Matematică și Informatică
Department de Informatică
Email: paul.irofti@fmi.unibuc.ro

Rețele private

- adrese IP accesibile doar în rețeaua internă
- *host*-urile nu oferă servicii $\rightarrow$ nu comunică direct cu exteriorul
- exemplu: calculatoarele personale, stații de lucru
- rețelele private comunică cu exteriorul prin unul sau mai multe IP-uri publice
- de obicei aceste IP-uri publice aparțin unui server sau router
- server-ul are cel puțin două adrese IP: una privată și una publică

De la	Până la
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Tabela: IP-uri private

Mască rețea

- adresa IP este împărțită în două părți: rețeaua și *host*-ul
- cele două sunt separate cu ajutorul unei măști pe biți
- exemplu: IP `192.168.1.17` și masca `255.255.255.0`

IP	11000000	10101000	00000001	00010001
mască	11111111	11111111	11111111	00000000
rețea	11000000	10101000	00000001	00000000
	192	168	1	0

- biții setați indică partea de rețea – bloc contiguu
- biții zero indică partea de *host* – bloc contiguu
- notație CIDR (Classless Inter-Domain Routing): `IP`/*prefix*
- *prefix* – numărul de biți setați în mască
- exemplu: IP `192.168.1.17/24`, rețea `192.168.1.0/24`

Difuzare (Broadcast address)

- adresă de difuzare: date primite și distribuite în toată rețeaua
- 255.255.255.255 – broadcast către toate adresele IP
- broadcast în rețeaua locală → limited broadcast
- adresa: prefixul rețelei combinat + biții setați în partea de *host*
- exemplu: IP 192.168.1.17 și masca 255.255.255.0

rețea	11000000	10101000	00000001	00000000
mască	11111111	11111111	11111111	00000000
host	11111111	11111111	11111111	xxxxxxxx
broadcast	11000000	10101000	00000001	11111111
	192	168	1	255

- adresa broadcast în format CIDR: 192.168.1.255/24

Adresa MAC

- MAC = Media Access Control
- adresă unică de 48-biți stabilită de producătorul plăcii de rețea
- se mai numește adresă fizică sau adresă hardware
- reprezentare hexazecimal cu octeți separați prin `:` sau `-`
- exemplu: `ca:fe:de:ad:be:ef` sau `ca-fe-de-ad-be-ef`
- primii 3 octeți identifică producătorul
- adresare neierarhică $\rightarrow$ căutare grea în rețea
- adesea folosită drept un al doilea mod de identificare în rețea
- inițial adresa se schimba greu (aproape imposibil), acum este destul de facil

Dispozitive de transmisie

- placă de rețea
  - alias: network card, network adapter, NIC (Network Interface Controller)
  - primește și trimite pachete pentru un *host*
  - un *host* poate avea mai multe plăci de rețea
- switch
  - alias: hub, MAC bridge
  - conectează mai multe *host*-uri în rețeaua locală
  - transmite pachete bazându-se pe adresa MAC
  - nu are o adresă IP și nu participă altfel în rețea
- router
  - conectează mai multe calculatoare sau rețele
  - transmite pachete bazându-se pe adresa IP
  - conține tabele cu rute în rețea
  - citește destinația finală și folosește tabela cu rute pentru a trimite pachetul mai departe

Interfață de rețea

- alias: network interface
- de obicei e vorba despre o placă de rețea
- mai poate fi: un port hardware, un port în rețea, un socket
- in sistemul de operare configurăm interfața de rețea
- Linux: `eth0`, `eth1`, `eth2`, ... – *PlacăNumăr*
- Unix: `em0`, `iwm0`, `axe0` – *ProducătorNumăr*
- comandă: `ifconfig(8)` – setează IP, mască, MAC etc.

Transmisie (routing)

- transmisia este făcută prin tabela cu rute
- alias: routing table, routing information base (RIB)
- conține rute către anumite rețele
- ponderea fiecărei căi (metrics)
- rutele reprezintă (parte din) topologia rețelei
- rute dinamice și statice
- *host* transmite un pachet către o adresă IP fără să îi pese de destinație către *gateway*
- *gateway*-ul se ocupă să trimită pe calea corectă folosind tabela de rute
- comandă: `route(8)`
- afișare rute IPv4: `$ route show -inet`

Exemplu: rute IPv4

```
$ route -n show -inet
Routing tables

Internet:
Destination        Gateway                 Iface
default            192.168.1.1             iwm0
127/8              127.0.0.1               lo0
127.0.0.1          127.0.0.1               lo0
192.168.1/24       192.168.1.6             iwm0
192.168.1.1        10:c3:7b:54:4f:98       iwm0
192.168.1.6        dc:53:60:98:c9:9d       iwm0
192.168.1.255      192.168.1.6             iwm0
```

Exemplu: rute IPv4+DNS

```
$ route show -inet
Routing tables

Internet:
Destination         Gateway                 Iface
default             router.asus.com         iwm0
loopback            localhost               lo0
localhost           localhost               lo0
192.168.1/24        sci                     iwm0
router.asus.com     10:c3:7b:54:4f:98       iwm0
sci                 dc:53:60:98:c9:9d       iwm0
192.168.1.255       sci                     iwm0
```

Gateway

- rețeaua privată este conectată la alte rețele printr-un *gateway*
- direcționarea pachetelor este făcută prin *gateway*-ul *default* (implicit)
- *gateway*-ul este la bază un router
- conține cel puțin două interfețe de rețea: IP public și local
- în tabela de rute are informații despre interior și exterior
- de obicei nu trimite pachetul la destinația finală ci la următorul router (denumit și *hop*)
- următorul router trimite mai departe pachetul către următorul *hop* sau către destinația finală
- comandă: traceroute(8)

Exemplu: itinerariu pachete

```
$ traceroute fmi.unibuc.ro
traceroute to fmi.unibuc.ro (193.226.51.6), 64 hops max
 1  192.168.43.1 (192.168.43.1)
 2  * * *
 3  10.8.5.113 (10.8.5.113)
 4  10.8.5.129 (10.8.5.129)
 5  * * *
 6  static-10-220-128-98.rdsnet.ro (10.220.128.98)
 7  br01.bucuresti.rdsnet.ro (213.154.124.7)
 8  roedunet.bucuresti.rdsnet.ro (81.196.1.206)
 9  te-0-0-0-0.core1.nat.roedu.net (37.128.239.13)
10  37.128.232.30 (37.128.232.30)
11  37.128.230.74 (37.128.230.74)
12  fmi.unibuc.ro (193.226.51.6)
13  fmi.unibuc.ro (193.226.51.6)
14  fmi.unibuc.ro (193.226.51.6)
15  fmi.unibuc.ro (193.226.51.6)
16  ns1.fmi.unibuc.ro (193.226.51.1)
```

Network Address Translation (NAT)

- transformă o adresă din spațiul IP al unei rețele în spațiul altei rețele
- exemplu: $5.2.3.1/24 \leftrightarrow 192.168.1.1/24$
- util când se face legătura dintre o rețea privată și internet
- operație efectuată de router
- Fie o rețea privată unde *host*-urile au IP-uri private
  - un pachet pleacă de pe un *host* către un server din internet
  - ieșire: destinație IP global, sursă IP local
  - o dată trimis, așteaptă un răspuns
  - intrare destinație IP global, sursă IP global – cum ajunge pe *host*?

Configurarea unei mașini

Minim necesar pentru acces în rețea

- adresa IP a mașinii
- masca rețelei locale
- adresa IP gateway
- două adrese IP pentru servere DNS
- în situații limită se poate folosi `8.8.8.8` – DNS Google
- dacă aceste date sunt transmise static utilizatorului pot apărea probleme
  - la schimbarea IP-urilor rețelei `192.168.1.1/24` $\rightarrow$ `10.0.0.1/24`
  - la schimbarea serverelor DNS
  - eroare umană: același IP este dat la doi utilizatori
  - lipsă adrese disponibile pentru utilizatori noi
  - când știu că un IP nu mai este folosit?

Dynamic Host Configuration Protocol (DHCP)

- este suficient conectarea cablului de rețea sau selectarea rețelei wireless
- informațiile de configurare sunt luate automat de pe server-ul DHCP
- alocare IP-uri dintr-un interval – alocare dinamică
- alocare specifică pentru un host – bazat pe adresa MAC

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers 192.168.1.1;
  range 192.168.1.100 192.168.1.200;
  host sci {
    hardware ethernet dc:53:60:98:c9:9d;
    fixed-address 192.168.1.12;
    option host-name "sci";
  }
}
```

Filtrarea pachetelor

Firewall-ul Linux este configurat cu ajutorul tabelelor de intrare și ieșire setate de utilizator cu ajutorul `iptables(8)`

- tabele (*chains*): `INPUT`, `OUTPUT`, `FORWARD`
- `INPUT`: pachetele care intră în rețea
- `OUTPUT`: pachetele care ies din rețea
- `FORWARD`: pachetele care trebuie trimise mai departe, nu sunt pentru rețeaua router-ului
- când un pachet trece printr-o tabelă îi putem aplica reguli
- cele mai comune reguli: acceptare sau respingere a pachetului
- este aplicată tot timpul prima regulă care se potrivește
- exemplu:
  r1) permite trafic pe port 80
  r2) blochează tot traficul
  $\rightarrow$ traficul pe port 80 este permis, restul este blocat

iptables

Parametrii

- `-A` – specifică numele tabelei (ex. `-A OUTPUT`)
- `-p` – protocol (ex. `-p tcp`)
- `-dport` – port destinație (ex. `-dport 80`)
- `-j` – verdict, *jump chain* (ex. `-j DROP`)
- exemple:

```
sudo iptables -A INPUT -p tcp -dport ssh -j ACCEPT
sudo iptables -A INPUT -j DROP
```

- listă comenzi existente: `iptables -L`
- salvează reguli: `iptables-save > /etc/iptables.rules`

Configurarea unui router

- configurare a cel puțin două interfețe: rețeaua locală și externă
- rețeaua locală este cea controlată de router
- router-ul decide ce spațiu de adrese alege devenind *gateway*
- dacă rețeaua locală este privată trebuie să facă `NAT`
- trebuie configurat ce port-uri sunt vizibile și cum este redirecționat accesul în rețeaua locală
- opțional: serviciu DNS local $\rightarrow$ acces rapid
- opțional: serviciu `DHCP` pentru rețeaua locală