CURS 14

Propagarea rutelor spre clasele de adrese e specifică claselor de adrese IP reale.

Două categorii de clase IP:

- reale (routabile, publice)
- false (non routabile, private)

Clasele IP false:

- **10.0.0.0** / 255.0.0.0 (**/8**)
  - 1 clasă falsă A cu 2^{24} adrese IP
- **172.16.0.0** / 255.255.0.0 (**/16**)
  172.17.0.0 / 255.255.0.0
  …
  172.31.0.0 / 255.255.0.0
  - 16 clase false B cu 2^{16} adrese IP fiecare

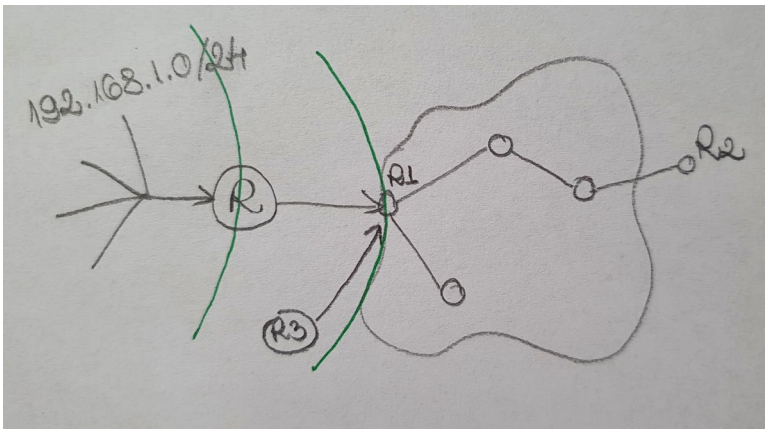
⇨ 172.16.0.0/12 (agregare)

- **192.168.0.0** / 255.255.255.0 (**/24**)
  192.168.1.0 / 255.255.255.0
  …
  192.168.255.0 / 255.255.255.0
  - 256 clase false C cu 2^8 adrese IP fiecare

⇨ 192.168.0.0/16 (agregare)

Router-ul nu o să spună niciodată router-ului vecin că el ține în spate clasa de adrese false. Informația despre clasa respectivă nu se propagă în Internet din două motive:

- router-ul nu anunță că ține în spate această clasă
- clasa mai e folosită și în alte colțuri din Internet



Clasa falsă, care inițial e vizibilă numai în rețeaua locală deservită de R. Dacă ar exista pe router-ul R1 o rută cum că spre clasa falsă se ajunge prin R, clasa s-ar propaga și ar fi vizibilă în toată rețeaua provider-ului respectiv.

Dacă 192.168.1.7 vrea să trimită un pachet în Internet, de exemplu la 80.81.82.83, va trimite pachetul cu IP sursă 192.168.1.7 și IP destinație 80.81.82.83 la router-ul de la provider (R1). El se uită în tabela de dirijare să vadă unde trebuie să trimită mai departe pachetul.

Când ajunge pachetul la 80.81.82.83, el trebuie să trimită un răspuns, așa că acum IP sursă devine 80.81.82.83, iar IP destinație devine 192.168.1.7. Router-ul nu va fi în stare să livreze pachetul, din două motive:

- ruta unde e localizat 192.168.1.7 nu e propagată în Internet
- orice router din Internet va fi dat peste cap, pentru că o astfel de clasă va fi folosită în foarte multe locuri

În mod normal, dacă R1 nu ar face *SNAT* (**S**ource **N**etwork **A**ddress **T**ranslation), pe calculatoarele din rețeaua locală deservită de R1 nu merge netul. Ele pot comunica ele între ele, dar nu cu exteriorul. Motivul nu este pentru că nu ar putea trimite pachete, ci pentru că destinația nu ar fi în stare să răspundă unor astfel de pachete.

Când un router din Internet primește un pachet care are ca și adresă IP sursă o adresă falsă, router-ul aruncă pachetul la gunoi.

(S)NAT

Întotdeauna când un pachet e expediat din rețeaua locală în exterior, adresa IP *sursă* a pachetului (adresă IP falsă) este înlocuită cu adresa IP publică pe care o are router-ul pe interfața externă (interfață de Internet/de WAN).

Mecanismul se află, în stiva TCP/IP, la nivel *Rețea*.

Legături PPP (**P**oint to **P**oint **P**rotocol) – folosită pentru conexiunile unde în spatele unui router este sigur 1 device; se pune netmask 255.255.255.255 (/32)

PPPoE (**PPP** **O**ver **E**thernet) – are loc un fel de VPN între router-ul de acasă și router-ul de la provider (e un fir virtual unde e doar calculatorul în spatele lui)

Router-ul păstrează o tabelă NAT în care ține minte toate conexiunile care tranzitează un anumit pachet. Atunci când vine un răspund din Internet la router, router-ul o să știe la care din device-urile din rețeaua locală trebuie să trimită răspunsul.

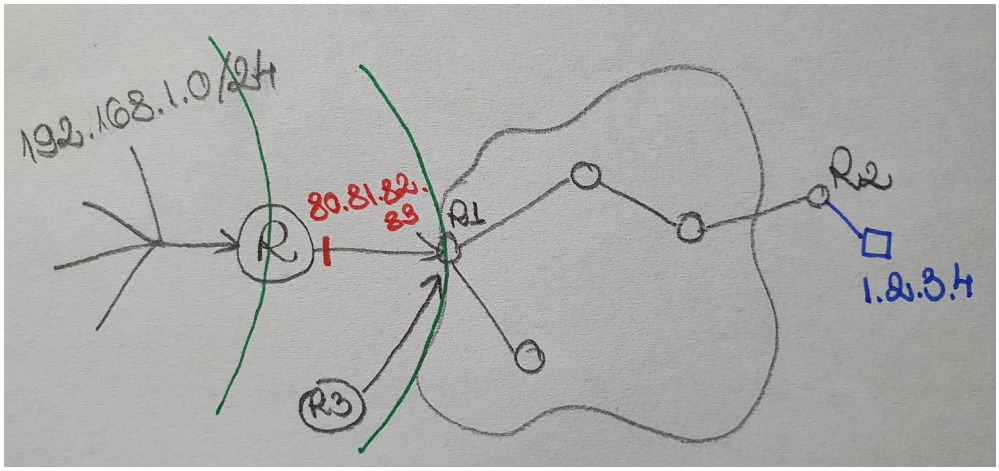


Tabela NAT

IP Sursă	IP extern router pt SNAT	IP Destinație
192.168.1.7:21322	80.81.82.83:21322	1.2.3.4:80
192.168.1.15:12323	80.81.82.83:12323	1.2.3.4:80

În momentul în care un router trebuie să translateze înapoi adresa IP destinație a pachetului, o să se folosească inclusiv de portul sursă și portul destinație.

Când un pachet merge de la o sursă spre o destinație, pachetul conexiunii are un port sursă (random printre cele libere). Serverul destinație nu o să știe că conexiunile sunt inițiate de două calculatoare diferite din rețeaua locală. El le vede venind de la aceeași adresă IP: 80.81.82.83. Dar pentru că porturile sunt diferite, nu îl încurcă cu nimic.

Pentru că device-urile sunt independente, cu sisteme de operare independente, se poate întâmpla ca, atunci când se creează conexiunile, ambele calculatoare să meargă pe port cu aceeași valoare.

IP Sursă	IP extern router pt SNAT	IP Destinație
192.168.1.7:**25000**	80.81.82.83:**25000**	1.2.3.4:80
192.168.1.15:**25000**	80.81.82.83:**25000**	1.2.3.4:80

Problema e că, dacă pachetele curg în exterior cu același port, nu se mai poate face diferențierea între ele, nici la nivelul server-ului care primește pachetele, nici la nivelul router-ului.

În momentul în care router-ul detectează că vine o conexiune nouă, care în momentul în care se face SNAT-ul, dacă conexiunea arată identic cu o altă conexiune pe care o are, trebuie să aibă loc o translatare de port sursă.

!!! Deci SNAT, în sine, nu e exclusiv la nivel Rețea. Când se face translatarea de port, se bagă și la nivel *Transport*

!!! E posibil să trebuiască să se facă translatare de port chiar dacă nu există o conexiune identică cu cea curentă. Asta se întâmplă când portul folosește același port când inițiază o conexiune client spre aceeași destinație.

DNAT (Destination Network Address Translation)

Toate pachetele care vin din exterior spre 80.81.82.83, router-ul înlocuiește adresa IP destinație și trimite pachetele respective în adresa locală căruia îi erau destinate.

Ex: Dacă din exterior vrem să accesăm un proces server care rulează în rețeaua locală pe un calculator cu adresă IP privată, trebuie spus router-ului, că orice vine din

exterior, specificând pe ce port și dacă e TCP/UDP, trebuie trimis înăuntru la calculatorul potrivit.

Tot așa, trebuie să se facă diferențierea pe porturi diferite.

Avantaje și dezavantaje ale claselor de adrese IP private:

Avantaje:

- permit economia de clase de adrese IP reale
- securitatea

Dezavantaje:

- e nevoie de SNAT ca să meargă internetul
- nu se pot rula servere pe ele care să fie accesibile din alte părți din Internet fără să se facă DNAT

În momentul în care un router face SNAT, se poate să nu facă cu o singură adresă IP reală pe care o are router-ul, ci poate cu un pool de adrese IP (de ex. de la 80.81.82.83 la 80.81.82.90). Această chestie e utilă când avem așa de multe calculatoare în rețeaua locală și se stabilesc așa de multe conexiuni, încât e nevoie să se facă translatare a porturilor sursă.

Acest pool nu trebuie neapărat să fie configurat pe interfața exterioară a router-ului. E important doar, ca pe următorul router să existe o rută cum că spre clasa din care fac parte IP-urile de la 83 la 90 se ajunge prin acel prim router.

!!! E o percepție greșită că NAT-ul înlocuiește adrese IP false cu adrese IP reale. Se poate înlocui și fals cu fals, real cu real etc.