Hálózati címfordítás

Számítógép-hálózatok

Dr. Lencse Gábor
egyetemi tanár
Széchenyi István Egyetem, Távközlési Tanszék
lencse@sze.hu

RÖVIDEN A HÁLÓZATI CÍMFORDÍTÁSRÓL

Network Address Translation – 1

- A TCP/IP protokollcsaládot eredetileg végponttól végpontig való kommunikációra tervezték
- Az alkalmazások arra számítanak, hogy a címek és portszámok a hálózati átvitel során változatlanok
- Az IPv4-címek szűkössége miatt elterjedt megoldás:
  - egy szervezet hálózatában privát IP-címeket használnak
  - a külső kommunikációhoz *címfordítás*t használnak
- A külső kommunikáció feladata lehet:
  1. A privát IP című gépeknek el kell érniük az Internetet
  2. Az Internet felől el kell érni valamely privát IP című gépet
- A feladatok megoldásához rendelkezésünkre áll egy router, amely rendelkezik publikus IP-címmel

Network Address Translation – 2

- Alapötlet az Internet eléréséhez:
  - A privát IP-címmel rendelkező kliens küldje el az IP datagramot a publikus IP-címmel rendelkező szerver felé
    - Forráscímként csak a saját privát IP-címét tudja használni
    - Privát IP-cím használata az Interneten NEM megengedett!
  - A kimenő router cserélje ki a forrás privát IP-címét a saját publikus IP-címére
  - A csomag megérkezik a címzetthez, és a válasz visszaér a routerhez.
  - A router továbbítsa a választ a forrásnak – DE HOGYAN?

Network Address Translation – 3

- Ahhoz, hogy a router a választ az eredeti feladónak vissza tudja küldeni, nyilván kell tartania, és fel kell ismernie, hogy ki volt az eredeti küldő.
  - Ennek érdekében az IP-címen túl mást is felhasznál. TCP és UDP esetén ezek a forrás portszámok
  - Nem elegendő ezeket megjegyezni, hiszen a forrás portszámok csak *gépenként egyediek*, a forrás IP-címet viszont a sajátjára cseréli
  - A forrás portszámokat kicseréli a *routeren egyedi portszámokra*
  - Az IP-címek és a célportszám mellett ezekkel már egyértelműen azonosítani tudja a kapcsolatokat
  - Kapcsolatonként nyilvántartja, hogy mit mire cserélt ki
  - A bejövő csomagoknál a cél IP-címen kívül a cél portszámot is vissza kell cserélnie ^(változott az irány)^

Network Address Translation – 4

- Az ismertetett megoldást hívjuk *Source NAT*-nak (SNAT) akkor, ha a router publikus IP-címe fix, és Masquerade-nek, ha DHCP-vel kapta az interfésze a címet
- Megjegyzések:
  - A terminológia nem egységes
    - Eredetileg a NAT csak az IP-címek cseréjét jelentette, ezt hívják ma *basic NAT*-nak, vagy *one-to-one NAT*-nak.
    - A fenti megoldás precíz neve a *NAPT* (Network Address and Port Translation). Nevezik *many-to-one NAT*-nak is.
  - Milyen esetben kell a forrás portszámot kicserélni?
    - Traditional NAPT: mindig
    - Extended NAPT: csak akkor, ha a nyilvántartásban ütközés lenne valamely másik kapcsolattal.

Network Address Translation – 5

- A másik irányú feladat az, hogy pusztán privát IP-címmel rendelkező gépeket elérhetővé tegyünk az Internet felől.
  - Erre a megoldás a *Destination NAT* (DNAT) vagy más néven *port forwarding*, ahol a router az adott portjára érkező datagramokat egy meghatározott privát IP című gépnek továbbítja úgy, hogy a célcímet kicseréli a csomagban.
    - Például a 80-as portra érkező datagramokat a 10.1.1.2 IP-című webszerver, a 25-ösre érkezőket pedig a 10.1.1.3 IP-című SMTP szerver felé továbbítja
- Mi helyzet az ICMP üzenetekkel?
  - ICMP esetén nincs portszám, de segíthet az, hogy egy ICMP hibaüzenetben benne van az azt kiváltó TCP vagy UDP adategység első 64 bitje a portszámokkal.
  - Amennyiben nem hibaüzenetről van szó, akkor is van megoldás: az ICMP üzenet valamilyen azonosító jellegű mezőjét használják fel.

Network Address Translation – 6

- Mindkét irányú megoldásnál gondot okozhat, ha az alkalmazások számítanak a címek és portok változatlanságára – ami részükről jogos elvárás.
  - Például egy FTP kliens aktív módban a vezérlő kapcsolaton keresztül megadja a szervernek, hogy mely portján várja, hogy a szerver felépítse az adatkapcsolatot.
  - Privát IP címmel várhatja – hacsak nem segít valaki: *protocol helper*
- Érdeklődőknek:
  - A NAT-ról bővebben az RFC 3022-ben olvashatunk, az IP, TCP, UDP, ICMP fejrészek mezőinek módosításával a 4.1. rész, az ellenőrző összeg hatékony újraszámításával a 4.2. rész foglalkozik.

Előzetes

- *Hálózati operációs rendszerek 1*:
  - NAT44 megvalósítása Linux alatt
- *IP alapú kommunikáció*:
  - NAT64 elmélet és gyakorlat is

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Lencse Gábor
egyetemi tanár
Széchenyi István Egyetem, Távközlési Tanszék
lencse@sze.hu