



ÓBUDAI EGYETEM
2011 TAVASZI FÉLÉV
10. LABORGYAKORLAT
PRÉM DÁNIEL

NAT/PAT

Számítógép hálózatok gyakorlata

Címkezelés problematikája

- Az Internetes hálózatokban ahhoz, hogy elérhetővé váljanak az egyes hálózatok egymás számára, globálisan érvényes címeket használunk.
- Hogy csökkentsük a felhasznált címek számát és növeljük a biztonságot, autonóm hálózatainkon (Intraneteinken) belül lokálisan érvényes címeket használunk. Ezek érvénytelenek az Interneten.
- Ezért autonóm rendszereink határán a lokális címeinket globális címre, vagy címekre fordítjuk. Ezt a megoldást hívjuk címfordításnak. (NAT/PAT)

Network Address Translation

A NAT egy címtranszformációs eljárás, melyben IP címeket képezünk le egy címzési övezetből egy másikba

Tulajdonságok:

- Transzparens címösszerendelés (nyilvántartás alapján)
- Transzparens forgalomirányítás biztosítása
- ICMP hibaüzenetek adatrészének transzformációja

Megvalósítása:

- Statikus összerendelés
- Dinamikus összerendelés

NAT előnyei és hátrányai

Előnyei:

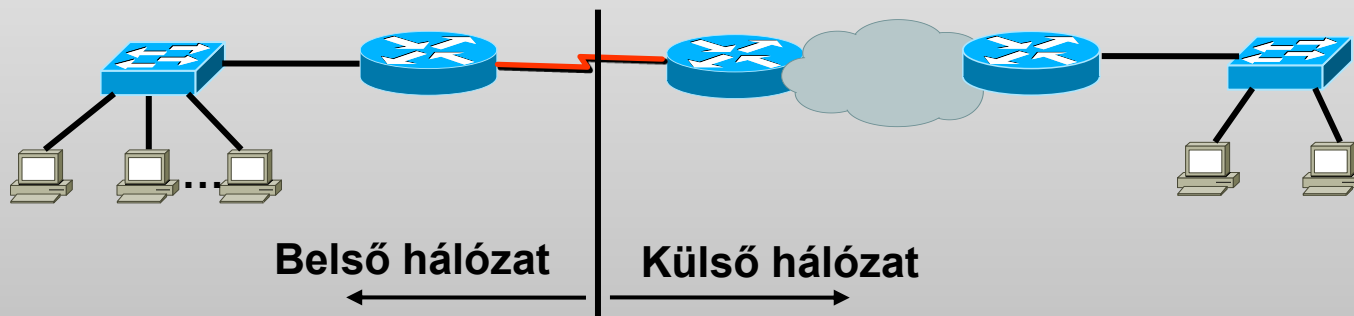
- Privát címek használata a belső hálózaton (címtakarékosság)
- Biztonság növelése
(a belső hálózat cím-struktúrája nem látható a külső hálózatról)

Hátrányai:

- A címfordítást végző eszközre jelentős terhelést ró
- Azon protokollok, amelyek a csomagok adatrészében cím információkat továbbítanak, csak akkor NAT tűrőek, ha a címfordítást végző eszköz képes az adatrészben továbbított tartalomban is elvégezni a szükséges címek cseréjét!
(Application Level Gateway – ALG funkció)

Fogalmak

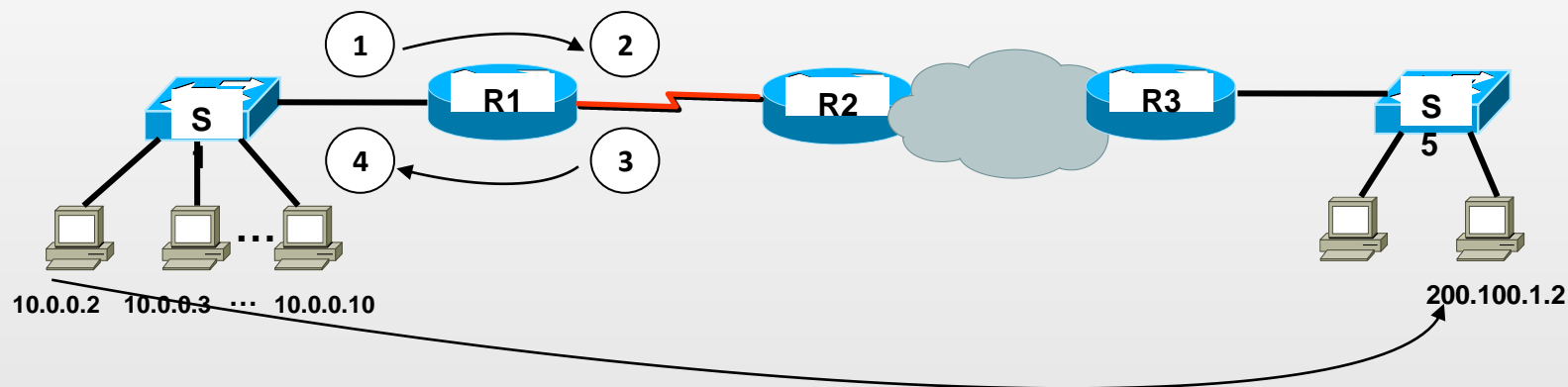
- **Címzési övezet (address realm):**
Az a hálózatrész, amelyben biztosítani kell az IP címek egyediségét
- **Külső hálózat (public/global/external network):**
Az IANA által kezelt címtartománnyal rendelkező címzési övezet
- **Belső hálózat (Private/Local Network):**
*Az intézmény saját (belső) címezéssel rendelkező címzési övezete.
Gyakran privát címtartomány: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16*



Fogalmak

- **Lokális cím:**
A belső hálózaton használt cím
- **Globális cím:**
A külső hálózaton használt cím
- **Belső lokális cím:**
Egy belső hálózati csomópont IP címe a belső hálózaton
- **Belső globális cím:**
Egy belső hálózati csomópont IP címe a külső hálózaton
- **Külső lokális cím:**
Egy külső hálózati csomópont IP címe a belső hálózaton
- **Külső globális cím:**
Egy külső hálózati csomópont IP címe a külső hálózaton

NAT Példa



Belső helyi címek: 10.0.0.1 – 10.0.0.10

Címfordításban résztvevő címek

Belső globális címek: 197.10.1.1 – 197.10.1.15

Címkészlet (pool)

Kimenő csomag:

Forrás IP

Cél IP

10.0.0.2

200.100.1.2

1

NAT fordítás

197.10.1.2

200.100.1.2

2

Bejövő csomag:

Forrás IP

Cél IP

200.100.1.2

197.10.1.2

3

NAT fordítás

200.100.1.2

10.0.0.2

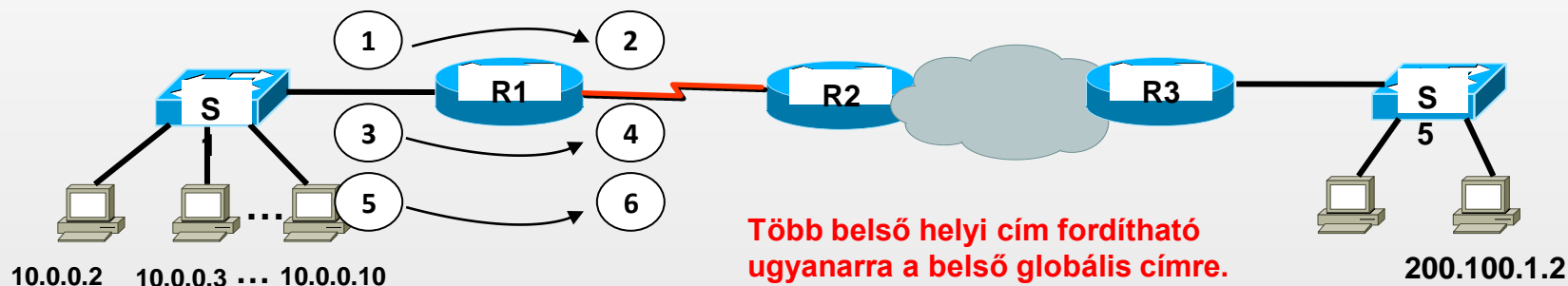
4

Port Address Translation

A NAT olyan megvalósítása, amikor lehetséges, hogy a címfordítás során a belső lokális és a belső globális címek között nem 1:1 típusú megfeleltetést alkalmazunk, hanem egy-egy globális IP-címnek több lokális címet is megfeleltetünk: N:1 típusú leképezés

A transzformációkat tartalmazó táblázatot ki kell egészíteni a Belső lokális és globális címeken túl:
a TCP/UDP port vagy az
ICMP saquece number értékével.

PAT Példa



Belső helyi címek: 10.0.0.1 – 10.0.0.10

Belső globális címek: 197.10.1.1 – 197.10.1.4

Címfordításban résztvevő címek

Címkészlet (pool)

Kimenő csomag:

<u>Forrás IP;port</u>	<u>Cél IP;port</u>
10.0.0.2; 1111	200.100.1.2: 80 (1)
↓ Címfordítás	
197.10.1.1; 1111	200.100.1.2: 80 (2)
10.0.0.3; 2222	200.100.1.2: 80 (3)
↓ Címfordítás	
197.10.1.1; 2222	200.100.1.2: 80 (4)

Kimenő csomag:

<u>Forrás IP;port</u>	<u>Cél IP;port</u>
10.0.0.4: 1111	200.100.1.2; 80 (5)
↓ Címfordítás ↓ Portfordítás	
197.10.1.1: 1112	200.100.1.2; 80 (6)

A TCP port címet is át kell írni!

Párosítások

Belső lokális cím	Belső Globális cím	Mód
1 db	1 db	NAT
Több	1 db	PAT
Több	Több (pool)	NAT/PAT
1db	Több (pool)	NAT

Dinamikus társítás:

A kommunikáció csak a belső hálózatról a külső hálózat irányába kezdődhet. Majd a dinamikusan létrejött bejegyzés útján a válaszcsoomagok visszaérkezhetnek. De a külső hálózat nem kezdeményezheti a kommunikációt!

Statikus társítás:

Adott eszközt mindig ugyan arra a címre képez le. Emiatt a külső hálózatról is kezdeményezhető a kommunikáció. PAT esetén Port Forward alkalmazható.

Dinamikus NAT pool konfiguráció

Több belső globális cím áll rendelkezésre a belső lokális címekkel rendelkező hálózat kiszolgálására. Viszont ha lokális több mint a pool, akkor a PAT is engedélyezhető az overload parancs használatával!

- **Pool létrehozása:**

```
Router(config)# ip nat pool PoolName 197.10.1.2 197.10.1.15 netmask 255.255.255.240
```

- **Címfordításban résztvevő gépek megadása:**

```
Router(config)# access-list 1 permit 10.0.0.0 0.0.0.255
```

- **Címhalmazok összekapcsolása:**

```
Router(config)# ip nat inside source list 1 pool PoolName [overload]
```

- **A címfordítás belső és külső interfészei:**

```
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit
```

```
Router(config)# interface Serial 2/0
```

```
Router(config-if)# ip nat outside
```

```
Router(config-if)# exit
```

Dinamikus PAT konfiguráció

Minden belső lokális cím az egyetlen belső globális címet használja ami nem más, mint a külső interfész címe is egyben!

- Címfordításban résztvevő gépek megadása:

```
Router(config)# access-list 1 permit 10.0.0.0 0.0.0.255
```

- A címfordítás interfészének megadása:

```
Router(config)# ip nat inside source list 1 interface Serial 2/0 overload
```

- A címfordítás belső és külső interfészei:

```
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit
```

```
Router(config)# interface Serial 2/0
```

```
Router(config-if)# ip nat outside
```

```
Router(config-if)# exit
```

Statikus NAT konfiguráció

A tipikus 1-1 kapcsolat megvalósítása

- Statikus címfordító bejegyzés:

```
Router(config)# ip nat inside source static 10.0.0.254 197.10.1.14
```

- A címfordítás belső és külső interfészei:

```
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit
```

```
Router(config)# interface Serial 2/0
```

```
Router(config-if)# ip nat outside
```

```
Router(config-if)# exit
```

Statikus PAT konfiguráció

A tipikus N-1 kapcsolat megvalósítása port továbbítással

- Statikus cím és port fordító bejegyzés:

```
Router(config)# ip nat inside source static tcp 10.0.0.254 80 197.10.1.14 80
```

```
Router(config)# ip nat inside source static tcp 10.0.0.253 22 197.10.1.14 22
```

- A címfordítás belső és külső interfészei:

```
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit
```

```
Router(config)# interface Serial 2/0
```

```
Router(config-if)# ip nat outside
```

```
Router(config-if)# exit
```