Tavasz 2017

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software

Számítógép-hálózatok 11. gyakorlat
Network Address Translation

Bordé Sándor

Szegedi Tudományegyetem

Tartalomjegyzék

Bevezetés

A korábbi fejezetekben előkerült már többször, hogy IPv4 címekből nincs annyi, hogy a világ összes, hálózatra csatlakozó eszközét ellássuk vele. Erre már viszonylag korán, a 80-as évek végén, 90-es évek elején rájöttek, ezért elkezdtek gondolkodni megoldási módokon.

Az ideális megoldás az lenne, ha olyan címzést használnánk, ami egyfelől hierarchikus, másfelől egyedi címet biztosít minden eszköznek. Az IPv6 protokoll teljesíti ezeket a követelményeket, viszont amíg megtörténik a teljes átállás, addig is szükség volt valamilyen áthidaló megoldásra. Ezt a célt szolgálták az olyan megoldások, mint a CIDR (**C**lassless **I**nter-**D**omain **R**outing), a DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol), címtartományok alhálózatokra bontása, privát címtartományok használata, illetve a NAT.

IP masquerading

Ha a világon csak egymástól független helyi hálózataink lennének, akkor a címzésük megoldható lenne privát címtartományok használatával. Azonban ezek a címek nem léphetnek nyilvános hálózatokra, ezért szükségünk van globális címekre, hogy mindegyik eszköz egyértelműen azonosítható legyen. Ehhez viszont nincs elegendő címünk.

Viszont általában nincs szükség arra, hogy mindenkinek folyamatosan legyen saját nyilvános IP címe. Pl. egy céges hálózatban a forgalomnak csak egy része hagyja el a belső hálózatot, a fennmaradó része viszont tartományon belül marad. Felmerül a kérdés, hogy ilyenkor miért foglaljon le egy eszköz egy IP címet akkor is, amikor épp nincs rá szüksége? Nem lehetne, hogy egy eszköz csak akkor kapjon nyilvános címet, amikor szüksége van rá?

Az IP masquerading technika lehetővé teszi, hogy privát címek (vagy akár privát címtartományok) a nyilvános hálózaton csak egy közös címet használjanak. Ekkor a külvilág számára mindegyik privát cím ugyanannak a nyilvános címnek fog látszani. Ezt a cserét a hálózatunk forgalomirányítója fogja végrehajtani a NAT protokoll segítségével. A protokoll ismertsége és népszerűsége miatt erre az egész folyamatra gyakran NAT-ként hivatkoznak, a későbbiekben mi is ez a megnevezést használjuk.

Network Address Translation

Az integrált router az internetszolgáltatótól kap (többnyire) egy nyilvános IP címet, ami lehetővé teszi csomagok küldését és fogadását az Interneten. Erre a címre fognak leképződni a belső, privát címek kifele irányuló kommunikáció esetén, illetve ezeket fordítja vissza a router befele jövő csomagoknál.

A folyamatot, ami átalakítja a magáncímeket az Interneten irányítható címekké, hálózati címfordításnak, **NAT**-nak hívják (**N**etwork **A**ddress **T**ranslation). A **NAT** segítségével a magán (helyi) forrás IP-címeket nyilvános (globális) címekké alakítjuk. A folyamat megfordul a bejövő csomagoknál. A NAT-ot használva a router képes több belső IP címet is ugyanarra a nyilvános címre fordítani.

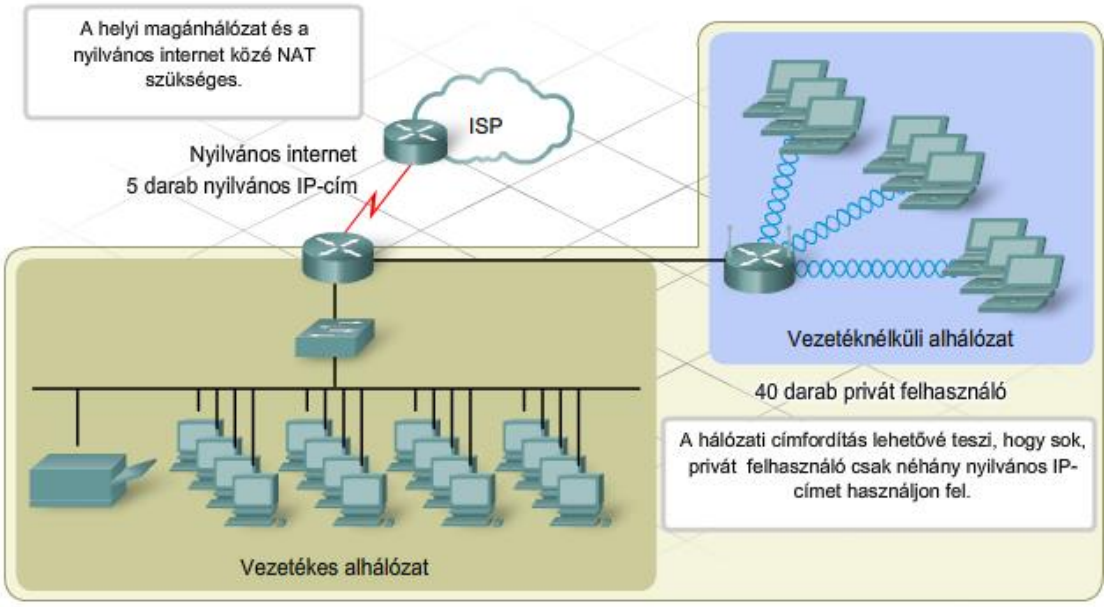
A helyi hálózaton belül egymásnak küldött csomagokat továbbra is címezhetjük privát címekkel, csak a más hálózatoknak szóló csomagokat kell fordítani. Amikor ezek a csomagok elérik az átjárót (default gateway), az integrált forgalomirányító lecseréli a forrásállomás magán IP címét a saját nyilvános IP címére és így továbbítja a külvilág felé.

Osztály	Privát IP cím	Alapértelmezett maszk	Hálózatok száma	Hosztok száma hálózatonként	Hosztok száma összesen
A	10.0.0.0 – 10.255.255.255	255.0.0.0	1	16777214	16777214
B	172.16.0.0 – 172.31.255.255	255.255.0.0	16	65534	1048544
C	192.168.0.0 – 192.168.255.255	255.255.255.0	256	254	65024

1. táblázat Privát címtartományok

A hálózati címfordítás alapjai

A címfordítás hasonlít a vállalati telefonrendszer működéséhez. Ahogy a cég folyamatosan veszi fel az embereket, egy ponton túl nem vezetnek minden dolgozó asztalához külön külső telefonvonalat. Ehelyett olyan rendszert használnak, amely lehetővé teszi, hogy a vállalat minden dolgozójához egy melléket rendeljen. A dolgozók egymást hívhatják csak a mellék tárcsázásával, kívülről pedig egy központi számot hívnak, ahol kapcsolják a kívánt melléket. A cég ezt gond nélkül megteheti, mert az összes dolgozó egyidejűleg nem akar telefonálni. A belső hívószámok használatával a cégnek kevesebb külső vonalat kell vásárolnia a telefontársaságtól. A NAT is hasonlóképpen működik.



1. ábra A NAT alapelemei

Előnyök, hátrányok

A NAT elsődleges előnye az, hogy IP címeket takaríthatunk meg azáltal, hogy több, helyi hálózaton lévő host számára képes kiosztani ugyanazt a globális IP címet. Ez feltűnés nélkül (transzparensen) működik, azaz kívülről úgy látszik,

mintha a hálózati csomag a globális címről jött volna, a privát cím rejtve marad a külvilág számára. Ezáltal egyfajta védelmet is biztosít: nyilvános hálózatból nem lehet elérni a belső eszközöket, csak a belső gép által küldött üzenetekre kapott válaszok jutnak be.

Ennek a védelemnek hátránya is van. Bizonyos esetekben (pl. távoli elérés, peer-to-peer kapcsolat) hasznos lenne, ha az arra jogosult felhasználók elérhetnék a belső eszközöket, de ez csak bizonyos beállítások után lehetséges. A NAT másik hátránya, hogy romolhat a szolgáltatás minősége. A címfordítás időt és erőforrást igényel, ami miatt bizonyos mértékben lassul a hálózat forgalma és nő a routerek terheltsége.

Előnyök	Hátrányok
• Nyilvános IP címek megosztása • Transzparens a felhasználók számára • Javított biztonság • LAN bővíthetősége, skálázhatósága • Helyi vezérlés ISP kapcsolattal	• Összeférhetetlen bizonyos alkalmazásokkal • Elrejti a távoli hozzáférést jogos esetben is • A teljesítmény csökkenhet a megnövekedett terhelés miatt

2. táblázat NAT előnyei - hátrányai

IP NAT alapfogalmak

A forgalomirányító IP-címfordítás opciójának beállításakor van néhány alapfogalom, amelyre szükségünk lesz, hogy megértsük a konfiguráció lépéseit.

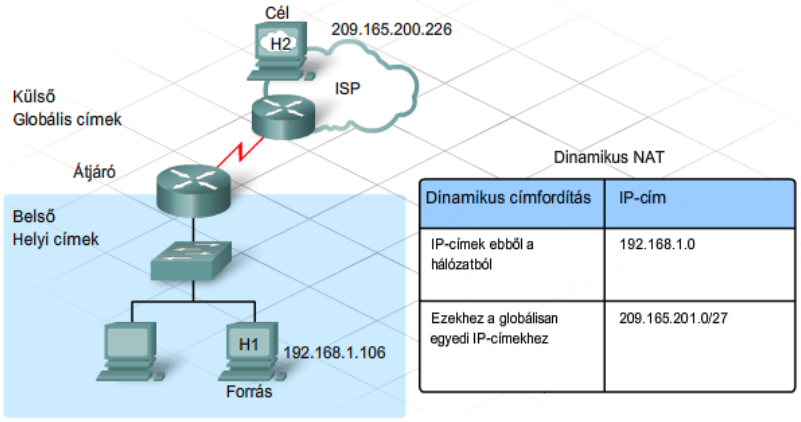
- **Belső (helyi) hálózat**: bármilyen, a forgalomirányítóhoz csatlakozó hálózat, amely a privát címzést használó helyi hálózat (LAN) része. A belső hálózaton levő állomások IP-címe fordításon megy át, mielőtt külső célpontokhoz továbbítják.
- **Külső (globális) hálózat**: minden olyan hálózat, amely a helyi hálózaton kívül van, és nem ismeri fel a helyi hálózat állomásaihoz hozzárendelt privát címeket.
- **Belső helyi cím**: a belső hálózat egy állomásán beállított magánhálózati cím, privát IP-cím. A cím csak úgy kerülhet ki a helyi hálózati címzési struktúrából, ha előtte lefordítjuk.
- **Belső globális cím**: a belső hálózat állomásának címe a külső hálózatok felé. Ez a lefordított cím.
- **Külső helyi cím**: a helyi hálózaton tartózkodó adatcsomag célpontjának címe. Ez a cím rendszerint ugyanaz, mint a külső globális cím (mivel mi sem látjuk annak a privát címeit)
- **Külső globális cím**: egy külső állomás nyilvános IP-címe. A cím egy globálisan továbbítható címből, vagy hálózati tartományból van származtatva.

Statikus és dinamikus NAT

A NAT-nak kétféle módja van: statikus és dinamikus. Mindkettőnek megvan az előnye és a hátránya. Szükség esetén ez a két módszer egyidejűleg is használható.

Dinamikus NAT

Ha egy belső, privát címmel rendelkező host szeretne külső hálózat felé kommunikálni, akkor a csomagot először elküldi az alapértelmezett átjárónak (ahogy azt már láttuk korábban). Mivel a forgalomirányító látja, hogy ez a csomag külső hálózatba tart, kijelöl a küldő gép számára egy globális címet, ami egy címtárból (*pool*) kerül ki. Ez a címtár tartalmazhat egy vagy több címet, vagy akár címtartományokat is. Továbbítás előtt a kimenő csomagban átírja a küldő IP címet erre a globális címre és megjegyzi a párosítást. Amíg a kapcsolat él (tehát még várunk a címzett válaszára), a forgalomirányító érvényesnek tekinti a globális címet és a nyugtákat küld a kezdeményező eszköznek. Amint a kapcsolat véget ér (azaz megérkezett a válasz a címzettől), a forgalomirányító megszűnteti a párosítást és visszajuttatja a belső globális címet a címtárba.



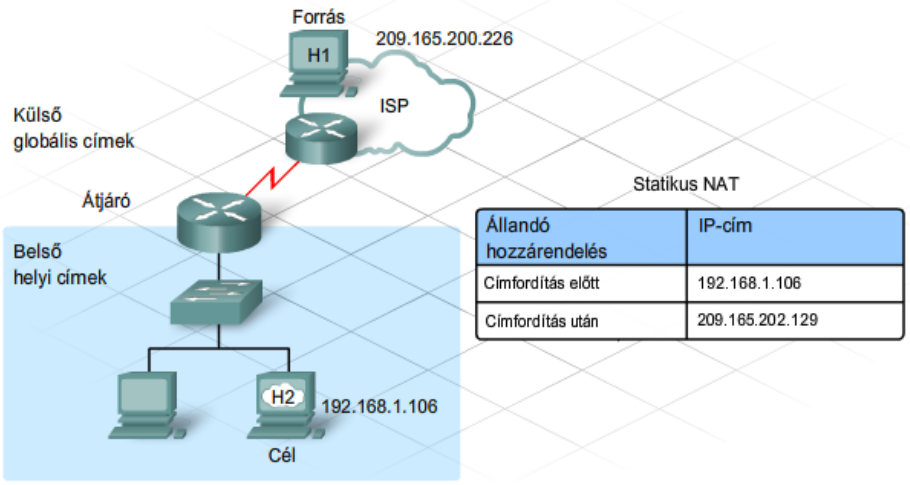
2. ábra Dinamikus NAT

Láthatjuk, hogy egy globális címre küldött csomagot csak akkor továbbít a belső hálózat felé a router, ha van hozzá érvényes párosítás, egyébként eldobja. Természetesen ez sem tökéletes védelem, de egyfajta biztonságot nyújt a belső eszközök számára.

Statikus NAT

A dinamikus NAT egyik előnye, hogy az egyes hostok nem érhetők el közvetlenül a külső hálózatból. De mi a helyzet akkor, ha egy belső hálózaton található állomáson/szerveren olyan szolgáltatások futnak, amelyeknek az Internet felől is elérhetőnek kell lenniük?

Egy belső eszközt kívülről is elérhetővé tehetünk úgy, hogy a NAT-ot végző routernek előírjuk, hogy ezt a privát címet mindig ugyanarra a globális címre fordítsa le. A rögzített címre fordítás biztosítja, hogy ez a globális cím mindig ugyanahhoz az eszközhöz fog tartozni és más állomás garantáltan nem használja. Így már lehetséges, hogy a nyilvános hálózaton levő állomások egy magánhálózaton levő kiválasztott állomásokhoz csatlakozzanak.



3. ábra Statikus NAT

Konfigurálás

Statikus vagy dinamikus NAT konfigurálása során:

- Vegyük számba azokat a kiszolgálókat, amelyek állandó külső címet igényelnek!
- Határozzuk meg mely belső állomások igényelnek címfordítást!
- Határozzuk meg, mely interfészekre érkezik a külvilág felé irányuló belső forgalom! Ezek lesznek a belső interfészek.
- Határozzuk meg, melyik interfész továbbítja a forgalmat az internet felé! Ez lesz a külső interfész.
- Határozzuk meg a felhasználható nyilvános címtartományt!

Statikus NAT konfigurálása

1. Határozzuk meg azt a nyilvános IP-címet, amelyet a külső felhasználók használhatnak a belső eszköz vagy kiszolgáló eléréséhez!
   - Erre a célra leggyakrabban a címtartomány első vagy utolsó címeit használják.
2. Végezzük el a belső (privát) címek nyilvános címekhez rendelését!
3. Állítsuk be a belső és külső interfészeket!

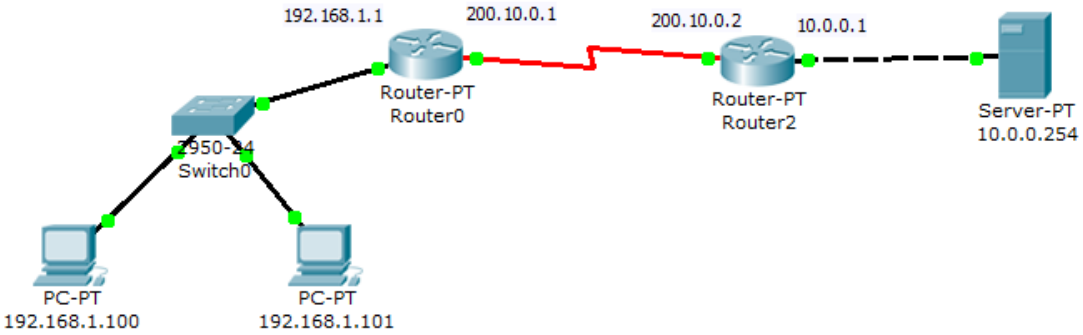
Dinamikus NAT konfigurálása

1. Határozzuk meg a felhasználható nyilvános IP-címkészletet!
2. Hozzunk létre hozzáférési listát (ACL) a címfordítást igénylő állomások meghatározásához.
3. Állítsuk be a belső és a külső interfészeket.
4. Rendeljük hozzá a címkészlethez a hozzáférési listát!

A dinamikus NAT konfigurálásának fontos lépése a hozzáférési listák alkalmazása. A hozzáférési lista engedélyező- és tiltó utasításokkal határozza meg azokat az állomásokat, amelyek címfordítást igényelnek. A hozzáférési lista vonatkozhat egy egész hálózatra, egy alhálózatra vagy csak egy adott állomásra.

Terjedelmét tekintve állhat egyetlen sorból vagy számos engedélyező és tiltó parancsból.

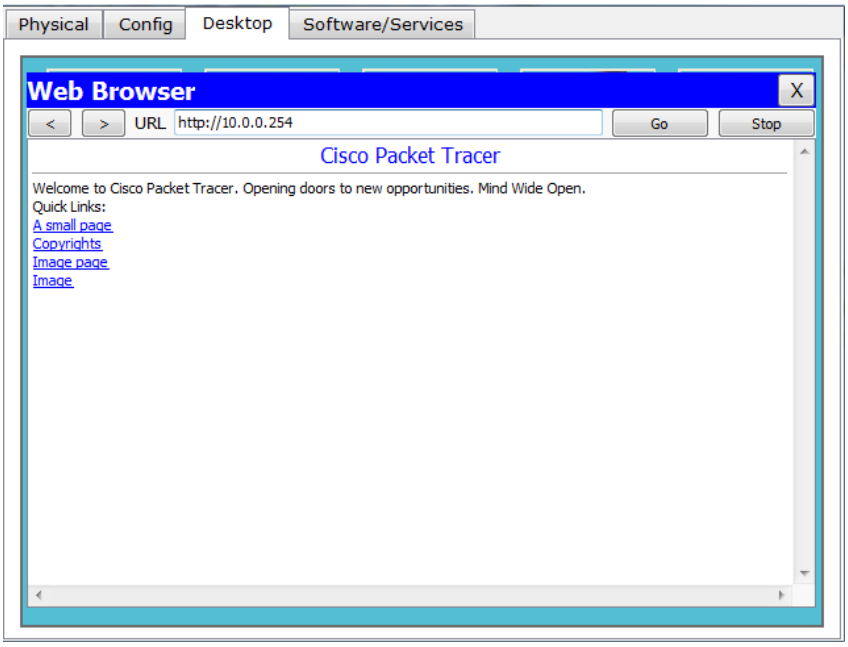
1. Példa



A Router0-t és a Router2-t serial porton keresztül kötjük össze, méghozzá úgy, hogy az egyik órajelet biztosítson. Ezt a Serial DCE nevű vezetékkel érjük el.

A `clock rate` (vagy `clockrate`) interfészkonfigurációs parancs beállítja a soros interfészeken keresztüli hardverkapcsolatok, például a hálózati interfész-modulok (NIM) és az interfészprocesszorok órajelét egy elfogadható bitsebességre.

Ha a hálózat felépítésével készen vagyunk (**TIPP**: routinghoz használhatjuk az előző gyakorlaton tanult RIP-et), nyissuk meg az egyik kiválasztott PC-ről a *Web Browser* alkalmazást, majd az URL-hez gépeljük be a szerver címét: 10.0.0.254. A web szerverre sikeresen felléptünk, ha a hálózatunkat jól konfiguráltuk be.



4. ábra Web szerverrel való kapcsolat

A probléma az, hogy a 10.0.0.254 egy privát cím, így nem használható nyilvános hálózaton, emiatt egy publikus címet kell hozzárendelni. Tegyük is meg ezt statikusan.

Válasszuk ki a Router2-öt és lépjünk be parancssori interfészbe, majd gépeljük be a következőt:

```
Router>enable
Router#configure terminal
Router(config)#ip nat inside source static 10.0.0.254 200.10.0.2
Router(config)#interface serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface fastethernet0/0
Router(config-if)#ip nat inside
```

Az utasítások:

- A belső interfész azonosítása az **ip nat inside** paranccsal
- A külső interfész azonosítása az **ip nat outside** paranccsal
- A statikus címfordítás megadása az **ip nat inside source static** paranccsal

Ebben a példában, a kiszolgáló belső címe (10.0.0.254) mindig átfordításra kerül a külső címre (200.10.0.2).

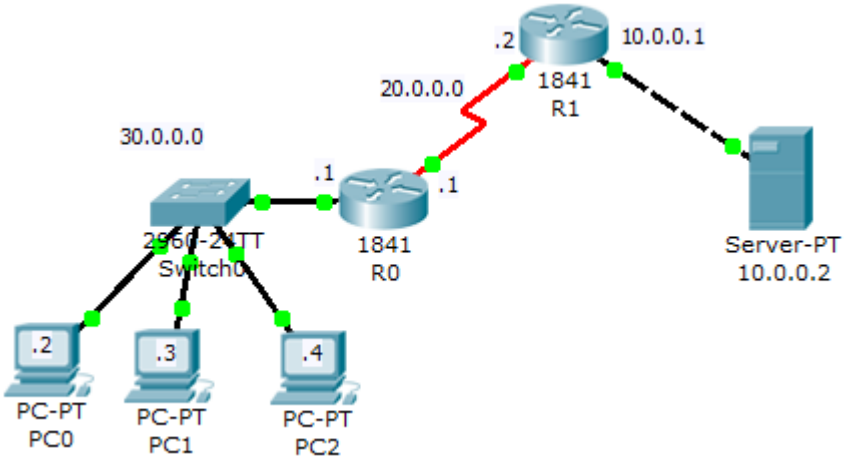
Ha most ismét megnyitjuk a Web browsert, a 10.0.0.254-el már nem tud kommunikálni, helyette a 200.10.0.2 címet kell használnunk. (*Valójában, ha a RIP miatt bekerült a hálózatba az eredeti cím, akkor továbbra is működik. A pontosság kedvéért a router ne hirdesse tovább a 10.0.0.0 hálózatot!)* Ha megpingeljük a gépet, látható, hogy a válasz a már átfordított címről fog érkezni.

```
Pinging 10.0.0.254 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=44ms TTL=126
Reply from 200.10.0.2: bytes=32 time=30ms TTL=126
Reply from 200.10.0.2: bytes=32 time=20ms TTL=126
Reply from 200.10.0.2: bytes=32 time=29ms TTL=126
```

A szerver privát címe átalakul publikus címmé, és a szerver címe rejtve marad a router mögött.

2. Példa



Miután felépítettük a topológiát és beállítottuk a címeket a következő NAT és routing beállításokat adjuk meg:

```
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.1
R1(config)#ip nat inside source static 10.0.0.2 50.0.0.1
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#

R0(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2
```

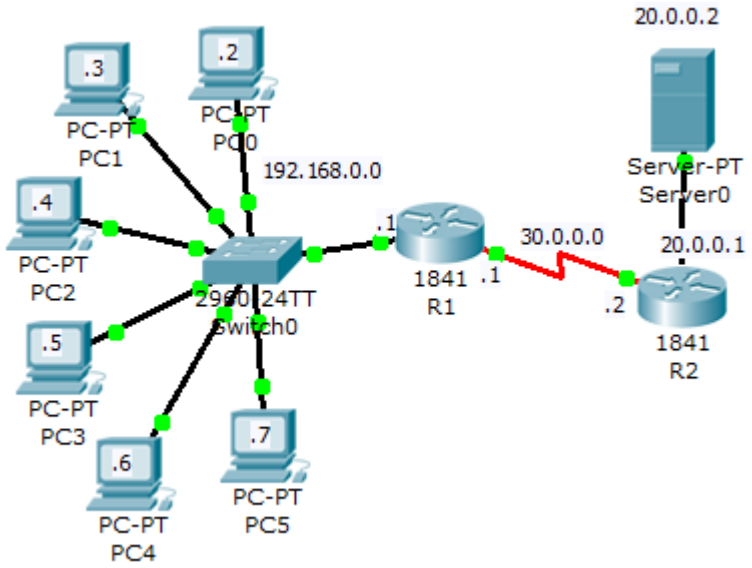
Ezzel a következőt érjük el: a webszerver a router mögött rejtve marad, de mégis el tudjuk érni. Ha megpróbáljuk pingelni az 50.0.0.1-es IP címet, akkor érkezi fog válasz, de 10.0.0.2 esetén már nem.

A következő példában, a sok routing helyett használjuk a következőt:

`R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0.`

az alapértelmezett útvonal beállítására, így csak azt kell megadnunk, melyik portra menjen tovább a csomag.

3. Példa



A hostok (PC0 – PC5) privát címekkel vannak ellátva, és mi azt szeretnénk, hogy a 50.0.0.1–50.0.0.5 tartományban található publikus címeket használják a nyilvános hálózaton. Ennek eléréséhez dinamikus NAT-ot használunk. Miután minden mást beállítottunk, adjuk ki az alábbi parancsokat:

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)#ip nat pool test 50.0.0.1 50.0.0.5 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool test
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#exit
```

Az utasítások:

- A címfordítást igénylő állomások meghatározása az **access-list [azonosító] permit** paranccsal
- A felhasználható nyilvános IP-címkészlet meghatározása **az ip nat pool [name]** paranccsal
- A címkészlethez a hozzáférési lista hozzárendelése az **ip nat inside source list [azonosító] pool [name]** paranccsal

Ugyanúgy, mint az előző két hálózatnál, meg kell adnunk a külső és a belső interfészt, majd össze kell párosítani a nyilvános címeket a belső interfész rejtett címeivel.

Ellenőrzés és hibaelhárítás

A NAT működés ellenőrzéséhez és hibaelhárításához számos CLI parancs áll rendelkezésre.

Az előző hálózatban (példa3) adjuk ki a következő utasítást: **debug ip nat**, és figyeljük meg a címfordításokat csomagküldés közben.

Az egyik leghasznosabb parancs a **show ip nat translations**, amely a NAT hozzárendelések részleteit jeleníti meg. A parancs megjelenít minden beállított statikus és a forgalom által generált dinamikus fordítást. Minden címfordításnál szerepel a protokoll, valamint a belső és külső lokális, illetve globális cím.

A **show ip nat statistics** parancs megjeleníti az aktív címfordítások teljes számát, a NAT konfiguráció paramétereit, valamint a címkészlet kioszthető és kiosztott elemeinek számát.

A fentieken túl a **show run** parancs segítségével is megtekinthetők a NAT beállítások.

```
R1# show ip nat translations
Pro     Inside global         Inside local       Outside local      Outside global
---     209.165.202.130       172.31.232.14      ------
icmp    209.165.202.131:512   172.31.232.1:512   209.165.200.1:512  209.165.200.1:512
udp     209.165.202.131:1067  172.31.232.2:1067  209.165.200.2:53   209.165.200.2:53
Tcp     209.165.202.131:1028  172.31.232.2:1028  209.165.200.3:80   209.165.200.3:80

R1# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial 0/0/0
Inside interfaces:
  FastEthernet 0/0
Hits: 47  Misses: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pub-addr refcount 4
 pool pub-addr: netmask 255.255.255.0
        start 209.165.202.131 end 209.165.202.140
        type generic, total addresses 10, allocated 2 (20%), misses 0
Queued Packets: 0
```

Beugró kérdések

1. Mi a NAT feladata?
2. Melyek a NAT előnyei? (Több válasz is lehetséges.)
3. Melyek a NAT hátrányai? (Több válasz is lehetséges)
4. Mi az a külső globális hálózat?
5. Mi az a belső globális cím?
6. A statikus NAT konfigurálása során… (Több válasz is lehetséges)
7. Mi az, amit a statikus és dinamikus NAT konfigurálás esetén is be kell állítanunk?
8. Melyik utasítás szolgál a statikus NAT megadására?
9. Mely utasítások szükségesek a dinamikus NAT konfiguráláshoz? (Több válasz is lehetséges)
10. Melyik utasítással NEM tudjuk elvégezni a konfigurálás ellenőrzését, illetve a hibák elhárítását?

Források

[1] http://computernetworkingnotes.com

[2] CISCO CCNA második és harmadik szemeszterének tananyaga