NAT – hálózati címfordítás

Az IP-címek szűkös erőforrások. Az IP-címek kifogyásának kérdése nem elvi probléma, ami talán valamikor a távoli jövőben fog előfordulni. Ez itt és most történik. A hosszú távú megoldás az ha az egész internet átáll az IPv6-ra, ami 128 bites címeket használ. A átállás lassan meg is kezdődik, de még évek telnek el addig amíg befejeződik. Ezért gondolták néhányan azt, hogy gyors javításra van szükség. Ez a gyors javítás a **NAT (Network Address Translation; hálózati címfordítás)** képében jött el. A NAT-ot az RFC 3022 írja le.

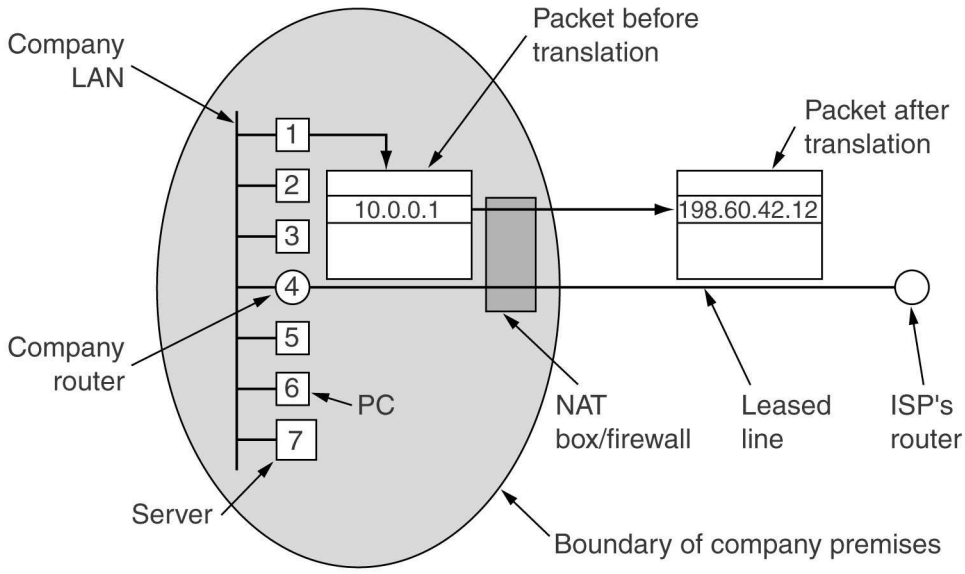
A NAT alapötlete az, hogy az internet forgalom számára mindencégnek egy (vagy legalábbis kevés számú) IP-címet osztanak ki. Egy vállalaton belül minden számítógép egyede IP-címet kap, amit a házon belüli forgalom irányításához használnak. Amikor viszont egy csomag elhagyja a vállalatot, és kimegy az internetszolgáltató felé, akkor címfordításra kerül sor. Mindezt az teszi lehetővé, hogy három IP-címtartományt jelöltek ki privát használatra. A vállalatok saját berkeiken belül úgy használják fel ezeket, ahogy akakrják.Az egyetlen kikötés az, hogy magán az interneten nem jelenhet meg olyan csomag amely ezeket a címeket tartalmazza. A három fenntartott címtírtomány:

10.0.0.0 - 10.255.255.255/8 (16 777 214 hoszt)

172.16.0.0 - 172.31.255.255/12 (1 048 574 hoszt)

192.168.0.0 - 192.168.255.255/16 (65 534 hoszt)

A NAT működését az alábbi ábra mutatja be:



A vállalat határain belül minden gépnek egyedi címe van, 10.x.y.z alakban. Ha azonban egy csomag elhagyja a vállalat területét, akkor áthalad egy NAT-dobozon (NAT box), ami átalakítja a belső IP-forrás csomópont címét, vagyis az ábrán a 10.0.0.1-et, a vállalat tényleges IP-címére, ami példánkban 198.60.42.12. A NAT-dobozt akár a vállalati routterrel is egybe építhetjük.

Eddig átsiklottunk egy apró részlet felett. Amikor a válasz visszaérkezik, természetesen a 198.60.42.12címre küldik. Honnan fogja ekkor a NAT-doboz tudni, hogy melyik címre cserélje azt ki? Ebben rejlik a NAT problémája. Ha lenne még egy maradék mező az IP fejrészben, azt felhasználhatnánk arra, hogy nyomon kövessük, ki volt az eredeti feladó; de már csak 1 bit maradt kihasználatlanul.

A NAT tervezői megfigyelték, hogy a legtöbb IP-csomag TCP- vagy UDP-tartalmat hordoz. Mindkettőjük fejrésze tartalmaz egy forrás port és cél port mezőt. A portok 16 bites egészek, melyek azonosítják, hogy hol kezdődik, és hol végződik egy TCP(UDP) kapcsolat. Ezek a portok lesznek tehát, azok a mezők, amelyekre a NAT működéséhez szükség van.

A *Forrás port* mező használatával megoldhatjuk a leképezési problémánkat. Amikor egy kilépő csomag eléri a NAT-dobozt, a 10.x.y.z forráscímet lecseréljük a vállalat igazi IP-címére. Ezenkívül, a TCP *Forrás port* mezőt lecseréljük egy mutatóra, ami a NAT-doboz 65 536 bejegyzésből álló fordítási táblázatára mutat. A mutatott bejegyzés tartalmazza az eredeti IP-címet és az eredeti forrás portot. Végül az IP- és a TCP-fejrészek ellenörző összegeit is újra számolják, és az eredményt beírják a csomagba. Azért kell kicserélni a *Forrás port* mezőt, mert a 10.0.0.1 és a 10.0.0.2 gépekről induló összeköttetések is használhatják például véletlenül az 5000-es portot, vagyis a *Forrás port* önmagában nem elég a feladó folyamat azonosítására.

Amikor egy csomag megérkezik a NAT-dobozhoz az internet szolgáltatótól, a TCP-fejrészben található *Forrás port* mezőt kiveszik, és indexként használják a NAT-doboz leképezési táblázatában. Az így talált bejegyzésből kiveszik a belső IP-címet és az eredeti TCP *Forrás port* mezőt, és belerakják azokat a csomagba. Ezután újraszámolják mind az IP-, mind a TCP-ellenörzőösszegeket, és azokat is beleírják a csomagba. A csomagot átadják hagyományos továbbításra a vállalati routernek a 10.x.y.z cím használatával.

Jóllehet ez a séma megoldja a problémát, az IP-közösségben mégis sokan ellenzik. Röviden összefoglaljuk az ellenérveket.

1. A NAT megsérti az IP felépítési modelljét, mely szerint minden IP-cím globálisan egyértelmű módon egyetlen gépet azonosít .AZ Internet teljes szoftver strukturája erre a tényre épül. A NAT révén azonban gépek ezrei használhatják (és használják is) a magánhálózati IP-címeket.

2. A NAT az összeköttetés nélküli Internetből egyfajta összeköttetés alapú hálózatot csinál. A gondot itt az okozza, hogy a NAT-doboznak minden rajta keresztülmenő kapcsolatról információt kell tárolnia. A kapcsolatállapot ilyen jellegű számontartása az összeköttetés alapú hálózatok sajátossága. Ha a NAT-doboz összeomlik és a leképezési táblázat elvész, akkor a doboz összes TCP-kapcsolata megszűnik. Ha nincs NAT a routerek összeomlása nincs hatással a TCP-re. Ilyenkor az történik,hogy a feladó folyamat időzítője lejár, mire minden nyugtázatlan csomagot újra ad. A NAT használatával az Internet olyan sebezhető lesz mint egy vonalkapcsolt hálózat.

3. A NAT megsérti a protokoll rétegelés legfontosabb alapelvét: a *k.* réteg nem tehet semmilyen feltételezést arról, hogy a *k+1.* réteg mit tett az adatmezejébe. Az alapelv az, hogy a rétegeket függetlennek kell tartani. Ha a TCP-t egyszer tovább fejlesztik TCP-2-re, és megváltozik a fejlécformátum, akkor a NAT megbukik. A rétegzett protokollok lényege pont az, hogy biztosítják, hogy az egyik rétegben bekövetkezet változások nem követelik meg a többi réteg megváltoztatását. A NAT megszünteti ezt a függetlenséget.

4. A folyamatok az Interneten nem feltétlenül használnak TCP-t vagy UDP-t. Ha az *A* gépen egy felhasználó úgy dönt, hogy egy új szálítási protokoll segítségével fog beszélni *B* gép egy felhasználójával, akkor a NAT-doboz bevezetésével az alkalmazás már nem fog működni, mert a NAT-doboz nem fog megfelelő TCP *Forrás port*ot találni.

5. Néhány alkalmazás a szöveg törzsébe illeszti az IP-címeket. A vevő azután innen veszi ki és használja tovább azokat. Mivel a NAT semmit sem tud ezekről a címekről, kicserélni sem tudja azokat, így a másik oldalon a címek használatára tett bármilyen kísérlet kudarcot fog vallani. A szabványos **FTP** is így működik, ezért a NAT jelenlétében nem fog működni, hacsak nem teszünk különleges intézkedéseket. Nem túl jó ötlet, hogy a NAT-doboz szoftverét mindenegyes alkalommal, amikor új alkalmazás megjelenik, újra ki kell javítani.
6. Mivel a TCP *Forrás port* 16 bites, legfeljebb 65 536 folyamatot lehet egy IP-címhez rendelni. A tényleges érték enné kicsit kevesebb, mert az első 4096 portot speciális célokra tartják fenn. Persze, ha több IP-cím áll rendelkezésünkre, akkor mindegyikkel lekezelhetünk legfeljebb 61 440 folyamatot.

Általában véve a NAT ellenzői azt mondják, hogy a túl kevés IP-cím problémájának egy ilyen ideiglenes és csúnya bütyköléssel való megoldása csak csökkenti az igazi megoldásra, vagyis az IPv6-ra való átállásra ösztönző nyomást, ez pedig nem jó dolog.