# Fejezet 11: IPv4 hálózati címfordítás (NAT) 11.0.1.1 Bevezetés

# Bevezetés

## Bevezetés

Az interneten használt valamennyi nyilvános IPv4-címet be kell jegyezni egy regionális internetes regisztrációs hivatalnál (Regional Internet Registry, RIR). A szervezetek bérelhetnek nyilvános címeket egy szolgáltatótól, de egy nyilvános internetes címnek csak a regisztrált tulajdonosa rendelheti hozzá azt a címet egy hálózati eszközhöz. A maximum 4,3 milliárd elméletileg lehetséges címével az IPv4-címtér azonban erősen korlátozott. Amikor Bob Kahn és Vint Cerf először kifejlesztette a TCP/IP-protokollcsomagot, beleértve az IPv4-et is 1981-ben, nem is képzelhették, hogy mivé válik az internet. Abban az időben a személyi számítógép leginkább az amatőrök kíváncsiságát keltette fel, és a World Wide Web még több mint egy évtizednyi távolságban volt.

A személyi számítógépek elterjedésével és a World Wide Web beköszöntével hamar nyilvánvalóvá vált, hogy 4,3 milliárd IPv4-cím nem lesz elég. A hosszútávú megoldás az IPv6 volt, de sokkal gyorsabb megoldásokra volt szükség ahhoz, hogy a címek elfogyását elkerüljük. Rövidtávon több megoldást is alkalmazott az IETF, beleértve a hálózati címfordítást (Network Address Translation, NAT) és az RFC 1918 szerinti privát IPv4-címek bevezetését. A fejezet azt tárgyalja, hogy a NAT - a magán címtartománnyal kombinálva - hogyan használható az IPv4-címek megőrzésére és hatékonyabb kihasználására, hogy tetszőleges méretű hálózatnak biztosíthassa a hozzáférést az internethez. A fejezet főbb témakörei:

* A NAT jellemzői, terminológiája és általános működése.
* A NAT különböző típusai, beleértve a statikus, a dinamikus és a túlterheléses NAT-ot.
* A NAT előnyei és hátrányai.
* A statikus, a dinamikus és a túlterheléses NAT konfigurálása, ellenőrzése és elemzése.
* Hogyan használható a porttovábbítás az internet felől egy belső eszközökhöz való hozzáférésre.
* A NAT hibaelhárítása a **show** és **debug** parancsokkal.
* Hogyan használható az IPv6 NAT az IPv6- és IPv4-címek közötti fordításra.

# Bevezetés

## Bevezetés

**A NAT fogalmai**

**Esetleírás**

Tegyük fel, hogy egy nagy egyetemen vagy iskolai rendszerben alkalmaznak bennünket.

Mivel hálózati rendszergazdaként dolgozunk, sok tanár, adminisztratív dolgozó és a többi hálózati rendszergazda igényli napi rendszerességgel segítségünket a hálózaton végzett munkájukhoz. A munkanap teljes ideje alatt hívogatnak, és a sok telefonhívás miatt nem tudjuk befejezni a szokásos rendszergazdai feladatainkat.

Meg kell találnunk a módot annak korlátozására, hogy mikor és kitől fogadunk hívásokat. Ezen felül el kell rejteni a telefonszámunkat, hogy amikor hívunk valakit, egy másik szám jelenjen meg a hívott félnél.

Ez az esetleírás egy nagyon gyakori problémát fogalmaz meg a legtöbb kis- és közepes méretű vállalkozásnál. További információkért látogassunk el a "How Network Address Translation Works" c. oldalra a <http://computer.howstuffworks.com/nat.htm/printable> címen, ahol láthatjuk, hogy a digitális világ hogyan kezeli a munkanapok ilyen típusú megszakítását.

Használjuk a feladathoz mellékelt PDF állományt annak továbbgondolásához, hogy a NAT-ként ismert folyamat hogyan ad választ az esetleírásban megfogalmazott kihívásra!

[Csoportos feladat - Conceptual NAT Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/11.0.1.2%20Conceptual%20NAT%20Instructions.pdf)

# A NAT működése

## A NAT jellemzői

Nincs elegendő nyilvános IPv4-cím ahhoz, hogy az internethez csatlakozó minden eszközhöz egyedi címet tudjunk rendelni. A hálózatokat gyakran valósítják meg privát (vagy magán) IPv4-címekkel, amiket az RFC 1918 határoz meg. Az 1. ábra mutatja az RFC 1918-ban foglalt címtartományokat. Nagyon valószínű, hogy a kurzus megtekintéséhez használt számítógéphez is egy privát címet rendeltek.

Ezeket a privát címeket használják egy szervezeten vagy telephelyen belül, hogy az eszközök helyben tudjanak kommunikálni. Mivel azonban ezek a címek nem azonosítanak egyértelműen egyetlen vállalatot vagy szervezetet, privát IPv4-címeket nem lehet forgalomirányításra használni az interneten. Ahhoz, hogy egy privát IPv4-című készülék a helyi hálózaton kívüli eszközökhöz és erőforrásokhoz is hozzáférhessen, a privát címet először egy publikus (vagy nyilvános) címre kell lefordítani.

Ahogy a 2. ábrán látható, a NAT biztosítja a privát címek publikus címre történő fordítását. Ez teszi lehetővé egy privát IPv4-című eszköz számára az olyan magánhálózaton kívüli erőforrásokhoz való hozzáférést, mint amilyenek például az interneten találhatók. A NAT privát IPv4-címekkel való kombinálása bizonyítottan hasznos módszer a nyilvános IPv4-címekkel való takarékoskodásra. Egyetlen nyilvános IPv4-címet meg lehet osztani több száz vagy akár több ezer eszköz között, amelyeken egyedi privát IPv4-címet állítottak be.

A NAT nélkül az IPv4 címtartomány kimerülése még jóval a 2000-es év előtt bekövetkezett volna. A NAT-nak azonban vannak bizonyos korlátai, amelyeket később fogunk megvizsgálni ebben a fejezetben. Az IPv4-címtartomány kimerülésére és a NAT korlátozásaira a megoldás a végleges átállás az IPv6-ra.

# A NAT működése

## A NAT jellemzői

A NAT sokféleképpen használható, de az elsődleges célja a nyilvános IPv4-címekkel való takarékoskodás. Teszi ezt azáltal, hogy a hálózatokon belül megengedi a privát IPv4-címek használatát, és publikus címre való fordítást csak akkor biztosít, ha arra szükség van. A NAT rendelkezik egy további előnnyel: hozzáad egy bizonyos fokú titkosságot és biztonságot a hálózathoz, mert elrejti a belső IPv4-címeket a külső hálózatok elől.

A NAT-képes forgalomirányítók egy vagy több érvényes nyilvános IPv4-címmel is konfigurálhatók. Ezeket a nyilvános címeket NAT-címkészlet néven ismerjük. Amikor egy belső eszköz forgalmat küld ki a hálózatból, a NAT-képes forgalomirányító lefordítja a készülék belső IPv4-címét egy a NAT-címkészletből származó nyilvános címre. A külső eszközök szemszögéből úgy tűnik, mintha mind a be-, mind a kilépő forgalom egy a címkészletből származó nyilvános IPv4-címmel rendelkezne.

A NAT-képes forgalomirányítók általában egy véghálózat határán végzik munkájukat. Egy véghálózat (stub network) olyan hálózat, amelynek egyetlen kapcsolata van a szomszédos hálózattal, egy út vezet be és ki a hálózatból. Az ábrán lévő példában az R2 egy határ-forgalomirányító. Az ISP irányából nézve az R2 egy véghálózatot képez.

Ha egy véghálózat egyik állomása egy külső állomással szeretne kommunikálni, akkor csomagjait a határ-forgalomirányító felé küldi. A határ-forgalomirányító lefuttatja a NAT-folyamatot, amelynek során az állomás belső privát címét egy külső, irányítható címre cseréli.

**MEGJEGYZÉS**: Az internetszolgáltató felé vezető kapcsolat is használhat privát címet vagy olyan publikus címet, amin osztoznak az előfizetők. Ennek a fejezetnek a céljaihoz egy publikus cím kerül bemutatásra.

# A NAT működése

## A NAT jellemzői

A NAT terminológiájában a belső hálózat azoknak a hálózatoknak az összessége, amelyek a fordítás tárgyát képezik. A külső hálózat kifejezés minden más hálózatra vonatkozik.

Amikor a NAT-ot használjuk, az IPv4-címeket különböző elnevezésekkel illetjük az alapján, hogy azok a belső hálózaton, vagy a nyilvános hálózaton (interneten) vannak, és hogy a forgalom bejövő vagy kimenő.

A NAT a címek négy típusát használja:

* belső helyi cím
* belső globális cím
* külső helyi cím
* külső globális cím

Amikor meghatározzuk, hogy milyen típusú címet használunk, fontos megjegyezni, hogy a NAT terminológiát mindig a lefordított címmel rendelkező készülék szempontjából alkalmazzuk:

* **Belső cím** - Annak az eszköznek a címe, amelyet lefordít a NAT.
* **Külső cím** - A céleszköz címe.

A NAT ezen felül a helyi (lokális) vagy a globális fogalmát is használja a címek tekintetében:

* **Helyi (lokális) cím** - A helyi cím bármely olyan cím, amely a hálózat belső részén jelenik meg.
* **Globális cím** - A globális cím olyan cím, amely a hálózat külső részén jelenik meg.

Az ábrán a PC1-nek egy belső helyi címe van, a 192.168.10.10. A PC1 szemszögéből nézve a webszervernek külső címe van, ez a 209.165.201.1. Ha csomagokat küldünk a PC1-ről a webszerver globális címére, a PC1 belső helyi címe a 209.165.200.226-ra (belső globális cím) fordítódik le. A külső eszköz címe általában nem kerül fordításra, mert az általában egy nyilvános IPv4-cím.

Figyeljük meg, hogy a PC1 különböző lokális és globális címmel rendelkezik, míg a webszervernek ugyanaz a nyilvános IPv4-címe van mindkét célra! A webszerver szemszögéből nézve a PC1-től induló forgalom úgy tűnik, hogy a 209.165.200.226 címről, a belső globális címről származik.

A ábrán R2-vel jelölt NAT-forgalomirányító a demarkációs pont a belső és külső hálózatok között, valamint a helyi és a globális címek között.

# A NAT működése

## A NAT jellemzői

A "külső" és "belső" kifejezéseket kombináljuk a "helyi" és "globális" kifejezésekkel, hogy egy adott címre utaljunk. Az ábrán az R2 forgalomirányítót lett a NAT-ra beállítva. Nyilvános címekből álló címkészlete van, amit hozzá lehet rendelni a belső állomásokhoz.

* **Belső helyi cím** - A forrás címe, ahogy az a belső hálózatról látható. Az ábrán a 192.168.10.10 IPv4-címet rendelték a PC1-hez. Ez a PC1 belső helyi címe.
* **Belső globális cím** - A forrás címe, ahogy az a külső hálózatról látszik. Az ábrán, amikor forgalom indul a PC1-ről a webszerver 209.165.201.1 címére, az R2 lefordítja a belső helyi címet egy belső globális címre. Ebben az esetben az R2 megváltoztatja az IPv4-forráscímet a 192.168.10.10-ről a 209.165.200.226-ra. A NAT terminológia szerint a 192.168.10.10 belső helyi címet lefordították a 209.165.200.226 belső globális címre.
* **Külső globális cím** - A rendeltetési hely címe, ahogy az a külső hálózatból látható. Ez egy globálisan irányítható IPv4-cím, amit egy állomáshoz rendeltek az interneten. A webszerver például a 209.165.201.1 IPv4-címen érhető el. A legtöbb esetben a külső helyi és a külső globális cím ugyanaz.
* **Külső helyi cím** - A cél címe, ahogy az a belső hálózatról látszik. Ebben a példában a PC1 forgalmat küld a webszerver 209.165.201.1 IPv4-címére. Bár ritka, de ez a cím lehet más is, mint a rendeltetési hely globálisan irányítható címe.

Az ábra azt mutatja, hogy egy belső PC-ről egy külső webszerverre küldött forgalom címzése hogyan történik a NAT-képes forgalomirányítón áthaladva. Azt is mutatja, hogy a visszatérő forgalom címzése és átfordítása miként történik.

**MEGJEGYZÉS**: a külső helyi cím használata kívül esik a kurzus keretein.

# A NAT működése

## A NAT jellemzői

Ebben a példában a 192.168.10.10 privát címmel rendelkező PC1 kommunikálni akar egy külső webszerverrel, aminek publikus címe 209.165.201.1.

Kattintsunk a lejátszás gombra az animáció elindításához!

A PC1 elküld egy a webszervernek címzett csomagot. A csomagot az R1 továbbítja az R2-nek.

Amikor a csomag megérkezik az R2-höz, a hálózat NAT-képes forgalomirányítójához, az R2 kiolvassa a csomagból a cél IPv4-címét annak meghatározására, hogy a csomag megfelel-e a meghatározott kritériumoknak a fordításhoz.

Ebben az esetben a forrás IPv4-cím megfelel a feltételeknek, és lefordítódik a 192.168.10.10-ről (belső helyi cím) a 209.165.200.226-ra (belső globális cím). Az R2 hozzáadja ezt a helyi és globális címek közötti leképezést a címfordítási táblához.

Az R2 a lefordított forráscímmel küldi el a csomagot a cél felé.

A webszerver egy a PC1 belső globális címére (209.165.200.226) címzett csomaggal válaszol.

Az R2 a csomagot a 209.165.200.226 célcímmel kapja meg. A forgalomirányító ellenőrzi a címfordítási tábláját, és talál egy bejegyzést ehhez a leképezéshez. Az R2 ezeket az információkat felhasználva lefordítja a belső globális címet (209.165.200.226) a belső helyi címre (192.168.10.10), majd a csomagot továbbítja a PC1 felé.

# A NAT működése

## A NAT típusai

A NAT-nak három típusa van:

* **Statikus címfordítás (statikus NAT)** - Egy-az-egyhez típusú hozzárendelés a helyi és a globális címek között.
* **Dinamikus címfordítás (dinamikus NAT)** - Több-a-többhöz típusú hozzárendelés a helyi és a globális címek között.
* **Port címfordítás (Port Address Translation, PAT)** - Több-az-egyhez típusú megfeleltetés a helyi és a globális címek között. Ezt a módszert túlterhelésként (NAT overloading) is ismerjük.

**Statikus NAT**

A statikus NAT egy-az-egyhez típusú összerendelést használ a helyi és globális címek között. Ezeket a leképezéseket a hálózati rendszergazda állítja be, és állandóak maradnak.

Az ábrán az R2 van beállítva az Svr1, a PC2 és a PC3 belső helyi címének statikus leképezésre. Amikor ezek az eszközök forgalmat küldenek az internetre, a belső helyi címeiket átfordítja a beállított belső globális címekre. A külső hálózatok felé ezek az eszközök publikus IPv4-címekkel rendelkeznek.

A statikus NAT különösen hasznos olyan webszerverek és egyéb eszközök számára, amelyeknek egy állandó, interneten keresztül is elérhető cím kell. Ilyen például egy vállalati webszerver. Szintén hasznos olyan eszközök esetében, amelyeknek az arra jogosult, de telephelyen kívül tartózkodó személyzet számára hozzáférhetőnek kell lenniük, de az internetes nagyközönség számára nem. A hálózati rendszergazda például a PC4-ről beléphet SSH-val a Svr1-re annak belső globális címén (209.165.200.226). Az R2 lefordítja ezt a belső globális címet a belső helyi címre, majd a rendszergazda munkamenetét csatlakoztatja az Svr1-re.

A statikus NAT megköveteli, hogy az összes egyidejű felhasználói munkamenethez elegendő nyilvános cím álljon rendelkezésre.

# A NAT működése

## A NAT típusai

A dinamikus NAT nyilvános címekből álló készletet (pool) használ, és érkezési sorrendben rendeli hozzá őket. Ha egy belső eszköz hozzáférést kér egy külső hálózathoz, akkor a dinamikus NAT hozzárendel egy rendelkezésre álló nyilvános IPv4-címet a készletből.

Az ábrán a PC3 elérheti az internetet az első szabad címmel a dinamikus NAT címkészletéből. A többi cím továbbra is rendelkezésre áll. A statikus NAT-hoz hasonlóan a dinamikus NAT is azt igényli, hogy legyen elég rendelkezésre álló publikus cím, ami kielégíti az összes egyidejű felhasználói munkamenet igényeit.

# A NAT működése

## A NAT típusai

A port címfordítás (PAT), más néven a túlterheléses NAT, több privát IPv4-címet képez le egyetlen vagy néhány nyilvános IPv4-címre. Ez az, amit a legtöbb otthoni forgalomirányító csinál. A szolgáltató egy címet rendel a forgalomirányítóhoz, a háztartás több tagja mégis egyszerre képes elérni az internetet. Ez a NAT leggyakoribb formája.

A PAT esetében több címet is le lehet képezni egyetlen vagy néhány címre, mivel minden privát címet a port száma alapján is nyomon követnek. Amikor egy eszköz egy TCP/IP munkamenetet kezdeményez, akkor létrehoz egy TCP vagy UDP forrásport értéket is a munkamenet egyedi azonosítására. Amikor a NAT-ot végző forgalomirányító csomagot kap a klienstől, felhasználja a forrásport számát az adott címfordítás egyedi azonosításához.

A PAT gondoskodik arról, hogy az eszközök minden munkamenethez különböző TCP-portszámot használjanak, amikor egy interneten található szerverrel kommunikálnak. Ha válasz érkezik vissza a szervertől, akkor a forrásport száma - ami a cél portszám lesz a visszaúton - határozza meg, hogy melyik eszközhöz továbbítsa a forgalomirányító a csomagokat. A PAT-folyamat azt is ellenőrzi, hogy a bejövő csomagokat valóban igényelték-e, így hozzáad egy bizonyos fokú biztonságot is a munkamenethez.

Az animáció a lejátszás és szünet gombokkal vezérelhető.

Az animáció a PAT-folyamatot szemlélteti. A PAT egyedi forrás portszámokat ad a belső globális címhez, hogy meg tudja különböztetni a fordításokat.

Ahogy az R2 minden egyes csomagot feldolgoz, egy portszámot használ (a fenti példában 1331 és 1555), hogy azonosítsa a készüléket, amelytől a csomag származik. A forráscím (SA) a belső helyi cím, kiegészítve a hozzárendelt TCP/IP-portszámmal. A célcím (DA) a külső helyi cím a szolgáltatást azonosító portszámmal együtt. Ebben a példában a szolgáltatás portja a 80-as: HTTP.

A forráscím esetében az R2 lefordítja a belső helyi címet belső globális címre, hozzáadva a port számát. A célcím nem változik, de mostantól külső globális címnek nevezzük. Amikor a webszerver válaszol, az útvonal megfordul.

# A NAT működése

## A NAT típusai

Az előző példában a kliens portszámok, az 1331 és 1555, nem változtak a NAT-képes forgalomirányítónál. Ez nem túl valószínű forgatókönyv, mert jó esély van arra, hogy ezek a portszámok már más aktív munkamenetekhez tartoznak.

A PAT megpróbálja megőrizni az eredeti forrásportot. Ha azonban az eredeti forrásport már használatban van, akkor a PAT az első szabad portszámot rendeli hozzá a megfelelő portcsoport (0-511, 512-1023 vagy 1024-65535) elejéről. Ha nincs több használható portszám, de egynél több külső IP-cím áll rendelkezésre, akkor PAT a következő IP-címre lép tovább, és újfent megpróbálja kiosztani az eredeti forrásportot. A folyamat mindaddig folytatódik, míg a portok és a külső IP-címek egyaránt el nem fogynak.

A PAT működésének megtekintéséhez kattintsunk a lejátszás gombra!

Az animáción az állomások ugyanazt az 1444-es portszámot választották. Ez elfogadható a belső címek esetében, mert az állomásoknak egyedi privát IP-címe van. Ugyanakkor a NAT-ot végző forgalomirányítónál a port számát meg kell változtatni, ellenkező esetben a két különböző állomásról érkező csomagok azonos forráscímmel lépnének ki az R2-ből. Ebben a példában a PAT a következő elérhető portot (1445) rendeli hozzá a második gép címéhez.

# A NAT működése

## A NAT típusai

A NAT és a PAT közti különbségek összegzése segít mindkettő megértésében.

Amint az ábra mutatja, a NAT egy-az-egyben végzi az IPv4-címek fordítását a magán és a nyilvános IPv4-címek között. A PAT viszont mind a címet, mind pedig a portszámot módosítja.

A NAT a belső célállomásra bejövő csomagokat úgy továbbítja, hogy megnézi a bejövő IPv4-forráscímet, amit a nyilvános hálózaton lévő állomás ad meg. A PAT esetében általában csak egy vagy nagyon kevés nyilvános IPv4-cím van. A nyilvános hálózatról bejövő csomagokat a magánhálózaton egy a NAT-ot végző forgalomirányítón lévő táblázat alapján irányítják a célhoz. Ez a táblázat követi nyomon a publikus és privát portpárokat. Ezt hívják kapcsolat-nyomkövetésnek.

**4. rétegbeli szegmens nélküli csomagok**

Mi a helyzet azonban azokkal az IPv4-es csomagokkal, amelyek nem TCP- vagy UDP-szegmenst tartalmazó adatot szállítanak? Ezek a csomagok ugyanis nem tartalmaznak 4. rétegbeli portszámot. A PAT lefordítja azokat a legáltalánosabb IPv4 által szállított protokollokat is, amelyek sem a TCP-t, sem az UDP-t nem használják szállítási rétegprotokollként. A leggyakoribb ezek közül az ICMPv4. A PAT minden ilyen típusú protokollt eltérően kezel. Az ICMPv4 lekérdező, visszhangkérés és visszhangválasz üzenetek például tartalmaznak egy lekérdezési azonosítót (Query ID). Az ICMPv4 a lekérdezési azonosítót használja a visszhangkérés és a megfelelő válasz azonosításához. A lekérdezési azonosító növekszik minden kiküldött visszhangkérés esetén. A PAT ezt használja a 4. rétegbeli portszám helyett.

**MEGJEGYZÉS**: Egyéb ICMPv4-üzenetek nem használják a lekérdezési azonosítót. Ezek az üzenetek és más protokollok, amelyek nem használnak TCP vagy UDP portszámokat, különbözőek és túlmutatnak a jelen tananyag keretein.

# A NAT működése

## A NAT előnyei

A NAT-nak számos előnye van, többek között:

* A NAT segít megtartani a hivatalosan regisztrált címzési rendszert az intranetek priváttá tételével. A NAT címeket takarít meg az alkalmazások port-szintű multilexelésével. A NAT túlterhelés esetében a belső állomások egyetlen nyilvános IPv4-címen osztoznak minden külső kommunikációhoz. Az ilyen rendszereknél nagyon kevés külső címmel nagyon sok belső állomás hozzáférése valósítható meg, vagyis takarékoskodni lehet az IP-címekkel.
* A NAT növeli a nyilvános hálózat felé vezető kapcsolatok rugalmasságát. Több címkészlet, tartalék és terheléselosztó készletek segítségével megbízható kapcsolat teremthető a nyilvános hálózatok felé.
* A NAT egységességet biztosít a belső hálózati címzési rendszer számára. Azon a hálózaton, amely nem használ privát IPv4-címeket és NAT-ot, a nyilvános IPv4-címzési rendszer megváltozása megköveteli az összes gép újracímzését. Az állomások újracímzésének költsége sokszor számottevő is lehet. A NAT lehetővé teszi, hogy a meglévő belső címzési séma megmaradjon, ugyanakkor könnyű átállást is biztosít egy új publikus címzési rendszerre. Ez azt jelenti, hogy egy szervezet megváltoztathatja az internetszolgáltatóját, de nem kell megváltoztatnia semmit a saját belső kliensein.
* A NAT biztonságot ad a hálózatnak. Mivel a privát hálózatok nem hirdetik címeiket és belső topológiájukat, a NAT használatával ellenőrzött módon biztosítható a külvilág elérésének lehetősége, így ezek a hálózatok magas fokú védelmet élveznek. Azonban a NAT nem helyettesíti a tűzfalakat.

# A NAT működése

## A NAT előnyei

A NAT-nak néhány hátránya is van. Az a tény, hogy az internetes állomások számára úgy tűnik, hogy közvetlenül a NAT-képes eszközzel, nem pedig a tényleges magánhálózaton belüli állomással kommunikálnak, számos kérdést vet fel.

A NAT egyik hátránya összefügg a hálózati teljesítménnyel, különösen a valós idejű protokolloknál, mint a VoIP. A NAT növeli a kapcsolási késleltetést, mivel a csomag fejlécében lévő minden egyes IPv4-cím lefordítása időt vesz igénybe. Az első csomag folyamat-kapcsolt, ez mindig a lassabb útvonalon megy keresztül. A forgalomirányítónak meg kell néznie minden csomagot, hogy eldönthesse, szükség van-e fordításra. Ezen felül meg kell változtatnia az IPv4-fejlécet, sőt esetleg még a TCP- vagy UDP-fejlécet is. Az IPv4-fejléc ellenőrző összegét, valamint a TCP vagy UDP ellenőrző összeget újra kell számolnia minden egyes alkalommal, amikor fordítás történik. A többi csomag a gyorskapcsolású útvonalon halad, feltéve, hogy létezik megfelelő gyorsítótár-bejegyzés, egyébként ezek is késleltetést szenvednek.

A másik hátrány az, hogy NAT használatával a végponttól végpontig terjedő címzés megszűnik. Számos internetes protokoll és alkalmazás függ a végponttól végpontig terjedő címzéstől, a forrástól egészen a célig. Egyes alkalmazások nem működnek a NAT-tal. Egyes biztonsági alkalmazások, mint például a digitális aláírás, nem működnek, mivel a forrás IPv4-címe megváltozik, mielőtt elérné a célját. Azok az alkalmazások, amelyek minősített tartománynevek helyett fizikai címeket használnak, nem fogják elérni a NAT-forgalomirányító által címfordított célállomásokat. Az ilyen problémák egyes esetekben statikus NAT-hozzárendelésekkel elháríthatók.

Az IPv4 végponttól végpontig tartó követhetősége szintén megszűnik. Egy csomagot sokkal nehezebb követni, ha több NAT-ugráson áthaladva nagy számú címváltozáson esik át, ezáltal a hibaelhárítás is nagyobb kihívás.

A NAT bonyolítja az alagutazó (tunneling) protokollokat is, mint például az IPSec, mert a módosítja a fejlécek értékeit, ami megzavarja az IPsec és más alagutazó protokollok által végzett integritás-ellenőrzést.

A TCP-kapcsolatok külső hálózatból való kezdeményezését igénylő szolgáltatásokban, vagy az olyan kapcsolat nélküli protokollokban, mint például az UDP, zavar keletkezhet. Amíg a NAT-forgalomirányítót be nem állítják úgy, hogy támogassa az ilyen protokollokat, a bejövő csomagok nem tudják elérni a céljukat. Egyes protokollok képesek a NAT egyetlen példányának kezelésére a résztvevő állomások között (ilyen például a passzív módú FTP), de nem működnek, ha mindkét rendszert NAT-tal választják el az internettől.

# A NAT konfigurálása

## A statikus NAT konfigurálása

A statikus NAT egy-az-egyhez típusú leképezés egy belső és egy külső cím között. A statikus NAT lehetővé teszi a külső eszközök számára, hogy kapcsolatot kezdeményezzenek a belső eszközök felé, a statikusan hozzárendelt publikus címet használva. Egy belső webszerverhez például hozzá lehet rendelni egy konkrét belső globális címet úgy, hogy külső hálózatokból is hozzáférhető legyen.

Az 1. ábra egy belső hálózatot mutat, amelyben egy webszerver található privát IPv4-címmel. Az R2 forgalomirányító statikus NAT használatára van beállítva, hogy a külső hálózaton (interneten) lévő eszközök hozzáférhessenek a webszerverhez. A külső hálózaton lévő kliens a webszervert egy nyilvános IPv4-címen éri el. A statikus NAT lefordítja a nyilvános IPv4-címet a privát IPv4-címre.

Két alapvető feladat van a statikus NAT címfordítások beállításakor.

**1. lépés:** Az első feladat az, hogy létrehozzunk egy leképezést a belső helyi cím és a belső globális cím között. Az 1. ábrán például a 192.168.10.254 belső helyi címet és a 209.165.201.5 belső globális címet állították be a statikus NAT-fordításhoz.

**2. lépés:** Miután a leképezést beállítottuk, a fordításban részt vevő interfészeket konfiguráljuk mint belső vagy külső interfészt, a NAT-hoz viszonyítva. A példában a Serial 0/0/0 interfész az R2-n belső, a Serial 0/1/0 pedig külső interfész.

Az R2 a belső interfészén (Serial 0/0/0) érkező csomagokat a beállított belső helyi IPv4-címről (192.168.10.254) lefordítja, majd továbbítja a külső hálózat felé. Az R2 a külső interfészére (Serial 0/1/0) érkező csomagokat, amelyeket a beállított belső globális IPv4-címre (209.165.201.5) címeztek, lefordítja a belső helyi címre (192.168.10.254), majd továbbítja a belső hálózatra.

A 2. ábra vázolja a statikus NAT konfigurálásához szükséges parancsokat.

A 3. ábra mutatja az R2-n szükséges parancsokat, amelyek a példaként szereplő topológiában a webszerver statikus NAT leképezéséhez szükségesek. A bemutatott konfigurációban az R2 fordítja a webszerver címéről (192.168.10.254) érkező csomagokat a nyilvános 209.165.201.5 IPv4-címre. Az internetes kliensek a webes kéréseiket a nyilvános 209.165.201.5 címre küldik. Az R2 továbbítja ezt a forgalmat a webszerverhez a 192.168.10.254 címen.

Használjuk a parancsszimulátort a 4. ábrán, hogy beállíthassunk egy további statikus NAT-bejegyzést az R2-n!

# A NAT konfigurálása

## A statikus NAT konfigurálása

A korábbi beállításokat felhasználva, az ábra bemutatja a statikus NAT fordítási folyamatát a kliens és a webszerver között. A statikus fordítások általában akkor használhatók, ha a klienseknek a külső hálózatról (internet) kell elérniük a belső hálózaton lévő szervereket.

1. A kliens kapcsolatot kíván létesíteni a webszerverrel. Kiküld egy csomagot a webszerver felé a 209.165.201.5 nyilvános IPv4-célcímet használva. Ez a webszerver belső globális címe.

2. Az első csomagnál, amit megkap a klienstől a külső NAT-interfészén, az R2 ellenőrzi a címfordítási táblát. A cél IPv4-cím megtalálható a címfordítási táblában, és lefordítandó.

3. Az R2 lecseréli a 209.165.201.5 belső globális címet a 192.168.10.254 belső helyi címre. Az R2 ezután továbbítja a csomagot a webszerver felé.

4. A webszerver fogadja a csomagot, és válaszol a kliensnek a belső helyi címéről (192.168.10.254).

5a. Az R2 megkapja a webszervertől érkező csomagot a belső NAT interfészén, a webszerver belső helyi címével (192.168.10.254) mint forráscímmel.

5b. Az R2 ellenőrzi a címfordítási táblázatot a belső helyi cím fordításához. A cím megtalálható a címfordítási táblázatban. Az R2 lefordítja a forráscímet a 209.165.201.5 belső globális címre, majd kiküldi a csomagot a Serial 0/1/0 interfészen a kliens felé.

6. A kliens megkapja a csomagot, és folytatja a párbeszédet. A NAT-forgalomirányító minden egyes csomagon végrehajtja a 2. és 5b. közti lépéseket. (A 6. lépés nem látható az ábrán.)

# A NAT konfigurálása

## A statikus NAT konfigurálása

Egy hasznos parancs a NAT működésének ellenőrzéséhez a **show ip nat translations** parancs. Ez a parancs megjeleníti az aktív NAT-fordításokat. A statikus címfordítások, ellentétben a dinamikus fordításokkal, mindig benne vannak a címfordítási táblában. Az 1. ábra az előző konfigurációs példát felhasználó parancs kimenetét mutatja. Mivel ez egy statikus NAT-konfiguráció példája, ezért a kommunikációktól függetlenül a fordítás mindig benne van a címfordítási táblázatban. Ha a parancsot egy aktív munkamenet során adjuk ki, a kimenet a külső készülék címét is jelzi, az 1. ábrán látható módon.

Egy másik hasznos parancs a **show ip nat statistics** parancs. Ahogy a 2. ábrán látható, a **show ip nat statistics** parancs információkat jelenít meg az összes aktív fordításról, NAT konfigurációs paraméterről, a készletben lévő címek számáról és a lefoglalt címek számáról.

A NAT működésének ellenőrzésére a legjobb megoldás, ha töröljük bármely korábbi fordítás statisztikáit a **clear ip nat statistics** paranccsal a tesztelés előtt.

A webszerverrel való bármilyen kommunikációt megelőzően a **show ip nat statistics** parancs nem mutat aktuális találatokat. Miután az ügyfél kapcsolatot létesített a webszerverrel, a **show ip nat statistics** parancs már öt találatot mutat. Ez igazolja, hogy a statikus NAT lezajlott az R2-n.

# A NAT konfigurálása

## A dinamikus NAT konfigurálása

Míg a statikus NAT állandó leképezést biztosít a belső helyi cím és egy belső globális cím között, addig a dinamikus NAT lehetővé teszi az automatikus leképezést a belső helyi címek és a belső globális címek között. Ezek a belső globális címek jellemzően nyilvános IPv4-címek. A dinamikus NAT egy nyilvános IPv4-címekből álló címcsoportot vagy készletet használ a fordításhoz.

A dinamikus NAT a statikushoz hasonlóan a NAT-ban részt vevő külső és belső interfészek beállítását igényli. Azonban míg a statikus NAT állandó leképezést hoz létre egyetlen címre, addig a dinamikus NAT egy címkészletet használ.

**MEGJEGYZÉS**: A publikus és privát IPv4-címek közötti fordítás messze a leggyakoribb NAT használati mód. Címfordítás azonban bármilyen két között is történhet.

Az ábrán látható példa szerinti topológiában van egy belső hálózat, amelynek címei az RFC 1918 privát címtartományból származnak. Az R1 forgalomirányítóhoz két LAN kapcsolódik, a 192.168.10.0/24 és a 192.168.11.0/24. Az R2 határ-forgalomirányító dinamikus NAT-ra van beállítva, a 209.165.200.226-tól a 209.165.200.240-ig terjedő nyilvános IPv4-címekből álló készletet használva.

A nyilvános IPv4-címekből álló készlet (belső globális címkészlet) rendelkezésre áll a belső hálózat bármely eszköze számára, beérkezési sorrend alapján. A dinamikus NAT esetében egy belső cím kerül fordításra egyetlen külső címre. Az ilyen típusú fordításnál elegendő címnek kell lenni a készletben ahhoz, hogy kielégíthesse az összes belső eszközt, amelyek ugyanabban az időben igénylik a hozzáférést a külső hálózathoz. Ha a készlet minden címe használatban van, az eszköznek várnia kell egy szabad címre, mielőtt elérné a külső hálózatot.

# A NAT konfigurálása

## A dinamikus NAT konfigurálása

Az 1. ábra mutatja a dinamikus NAT lépéseit és a konfigurálásához szükséges parancsokat.

**1. lépés:** Határozzuk meg a fordításhoz használandó címkészletet az **ip nat pool** paranccsal. Ez a címkészlet jellemzően nyilvános címek egy csoportja. A címek meghatározása a készlet kezdő IP-címe és az utolsó IP-cím megadásával történik. A **netmask** vagy **prefix-length** kulcsszó jelzi, hogy mely címbitek tartoznak a hálózathoz és mely bitek tartoznak az állomáshoz a címtartományban.

**2. lépés:** Állítsunk be egy normál ACL-t kizárólag a lefordítandó címek azonosítására (engedélyezésére). Egy túl engedékeny ACL kiszámíthatatlan eredményekhez vezethet. Ne feledjük, hogy egy implicit **deny all** utasítás van minden ACL végén!

**3. lépés:** Rendeljük hozzá az ACL-t a címkészlettel. Az **ip nat inside source list** *hozzáférési-lista-száma* **pool** *pool-neve* paranccsal rendeljük hozzá az ACL-t a címkészlethez. Ezt a konfigurációt használja a forgalomirányító annak megállapítására, hogy melyik eszköz (**list**) melyik címet (**pool**) kapja meg.

**4. lépés:** Határozzuk meg, melyek a belső interfészek a NAT viszonylatában, azaz minden olyan interfészt, amely a belső hálózathoz kapcsolódik.

**5. lépés:** Határozzuk meg, melyek a külső interfészek a NAT viszonylatában, azaz minden olyan interfészt, amely összeköt a külső hálózattal.

A 2. ábra egy példaként szolgáló topológiát és konfigurációt mutat be. Ez a konfiguráció lehetővé teszi a fordítást az összes gép számára a 192.168.0.0/16 hálózaton - amely magában foglalja a 192.168.10.0 és a 192.168.11.0 LAN-t is -, amikor az S0/0/0-án belépő és az S0/1/0-án kilépő forgalmat generálnak. Ezek a állomások egy szabad címre lesznek lefordítva a 209.165.200.226 és 209.165.200.240 közé eső tartományból.

A 3. ábra a parancsszimulátor konfigurálásához használt topológiát mutatja. Használjuk a parancsszimulátort a 4. ábrán, hogy beállíthassuk a dinamikus NAT-ot az R2-n!

# A NAT konfigurálása

## A dinamikus NAT konfigurálása

A korábbi beállításokat felhasználva, az ábrák a dinamikus NAT fordítási folyamatát szemléltetik két kliens és a webszerver között:

Az 1. ábrán a belülről kifelé haladó forgalom látható:

1. Az állomások a 192.168.10.10 (PC1) és a 192.168.11.10 (PC2) IPv4-forráscímekkel kapcsolatkérési csomagokat küldenek a szerverhez annak nyilvános IPv4-címére (209.165.200.254).

2. Az R2 megkapja az első csomagot a 192.168.10.10 állomástól. Mivel ez a csomag egy belsőnek konfigurált NAT-interfészen érkezett, az R2 ellenőrzi a NAT-konfigurációt annak meghatározása céljából, hogy a csomagot le kell-e fordítani. Az ACL engedélyezi ezt a csomagot, így az R2 le fogja fordítani azt. Az R2 ellenőrzi a címfordítási tábláját. Mivel nincs fordítási bejegyzés ehhez az IP-címhez, az R2 azt állapítja meg, hogy a 192.168.10.10 forráscímet dinamikusan kell fordítani. Az R2 kiválaszt egy szabad globális címet a dinamikus címkészletből, és létrehoz egy fordítási bejegyzést a 209.165.200.226-nak. A címfordítási táblában az eredeti IPv4-forráscím (192.168.10.10) a belső helyi cím, a lefordított cím pedig a belső globális cím (209.165.200.226).

A második állomás, a 192.168.11.10 esetében az R2 megismétli az eljárást, kiválasztja a következő rendelkezésre álló globális címet a dinamikus címkészletből, és létrehoz egy második fordítási bejegyzést a 209.165.200.227 címhez.

3. Az R2 helyettesíti a PC1 belső helyi forráscímét, a 192.168.10.10-et a lefordított belső globális címmel (209.165.200.226), és továbbítja a csomagot. Ugyanez a folyamat megy végbe a PC2-től érkező csomagon, a PC2 számára lefordított címmel (209.165.200.227).

A 2. ábrán a kívülről befelé haladó forgalom jelenik meg:

4. A szerver megkapja a csomagot a PC1-től, és válaszol a 209.165.200.226 célcímet felhasználva. Amikor a szerver a második csomagot kapja meg, a 209.165.200.227 célcím segítségével válaszol a PC2-nek.

5a. Amikor az R2 megkapja a csomagot a 209.165.200.226 IPv4-célcímmel, keresést hajt végre a címfordítási táblában. A táblából származó leképezést felhasználva az R2 visszafordítja a címet a belső helyi címre (192.168.10.10), és továbbítja a csomagot PC1 felé.

5b. Amikor R2 megkapja a csomagot a 209.165.200.227 cél IPv4-címmel, ismét elvégzi a NAT táblában való keresést. A táblából származó leképezést felhasználva az R2 visszafordítja a címet a belső helyi címre (192.168.11.10) és továbbítja a csomagot PC2 felé.

6. A PC1 a 192.168.10.10 címen, a PC2 pedig a 192.168.11.10 címen kapja meg a csomagokat és folytatja a párbeszédet. A NAT-forgalomirányító végrehajtja a 2-5. lépéseket minden egyes csomagon. (A 6. lépés nem látható az ábrákon).

# A NAT konfigurálása

## A dinamikus NAT konfigurálása

A **show ip nat translations** parancsból származó kimenet az 1. ábrán látható, és megjeleníti a két korábbi NAT-feladat részleteit. A parancs megjelenít minden beállított statikus, illetve forgalom által generált dinamikus fordítást.

Ha hozzáadjuk a **verbose** kulcsszót, további információt jelenít meg minden egyes fordításról, beleértve, hogy milyen régen hozták létre és használják a bejegyzést.

Alapértelmezésben a fordítási bejegyzések elévülnek 24 óra elteltével, kivéve, ha az időzítőket újrakonfigurálták az **ip nat translation timeout** *elévülési-idő-másodpercben* paranccsal globális konfigurációs módban.

A dinamikus bejegyzések elévülés előtti törléséhez használjuk a **clear ip nat translation** globális konfigurációs parancsot (2. ábra). Hasznos lehet, ha töröljük a dinamikus bejegyzéseket a NAT-konfiguráció vizsgálatakor. Amint a táblázatban látható, ez a parancs kulcsszavakkal és változókkal is használható, amelyekkel szabályozhatjuk, hogy melyik bejegyzés törlődjön. Adott bejegyzések törölhetők, hogy elkerüljük az aktív munkamenetek megzavarását. Használjuk a **clear ip nat translation \*** globális konfigurációs parancsot az összes fordítás törlésére a táblából.

**MEGJEGYZÉS**: Csak a dinamikus fordítások tűnnek el. A statikus címfordítások nem törölhetők a címfordítási táblából.

A 3. ábrán a **show ip nat statistics** parancs megjeleníti az aktív címfordítások teljes számát, a NAT-konfiguráció paramétereit, valamint azt, hogy hány cím van a készletben és mennyi foglalt már ezekből.

Másik megoldásként használjuk a **show running-config** parancsot, és keressük meg a NAT, ACL, interface vagy pool parancsokat a kívánt értékekkel. Vizsgáljuk meg ezeket gondosan, és javítsuk a felfedezett hibákat!

# A NAT konfigurálása

## A port címfordítás (Port Address Translation, PAT) konfigurálása

A PAT (más néven NAT túlterhelés) azáltal tud takarékoskodni a belső globális címkészletből származó címekkel, hogy a forgalomirányító egyik belső globális címét használja sok belső helyi címhez. Más szóval, egyetlen nyilvános IPv4-címet fel lehet használni több száz, sőt több ezer belső privát IPv4-címhez. Az ilyen fordítási típus esetében a forgalomirányító elegendő információt tart karban a magasabb szintű protokollokról, például TCP- vagy UDP-portszámokat, hogy a belső globális címet visszafordíthassa a megfelelő belső helyi címre. Amikor több belső helyi címet képezünk le egy belső globális címre, a TCP- vagy UDP-portszámok tesznek különbséget az egyes belső helyi állomáscímek között.

**MEGJEGYZÉS**: Egy-egy külső IP-címre elméletileg legfeljebb 65536 belső cím fordítható le. A gyakorlatban az egy IP-címhez hozzárendelhető belső címek száma 4000 körül van.

A PAT kétféle módon állítható be, attól függően, hogy a szolgáltató miként osztotta ki az IPv4-címeket. Az első esetben az internetszolgáltató több nyilvános IPv4-címet oszt ki a szervezetnek, a másikban csak egy nyilvános IPv4-címet, amely a szervezet szolgáltatóhoz történő csatlakozásához szükséges.

**A PAT konfigurálása nyilvános IP-címekből álló címkészlet esetében**

Ha egy telephelynek több, mint egy nyilvános IPv4-címet osztottak ki, ezek a címek részei lehetnek a PAT által használt címkészletnek. Ez hasonló a dinamikus NAT-hoz, kivéve, hogy nincs elég nyilvános cím a belső és a külső címek egy-az-egyben történő leképezéséhez. A kisebb címkészlet nagyobb számú eszköz között oszlik meg.

Az 1. ábra bemutatja azokat a lépéseket, amelyekkel a PAT a címkészlet használatára állítható be. Az elsődleges különbség ezen konfiguráció és a dinamikus, egy-az-egyhez típusú NAT-konfiguráció között az **overload** kulcsszó használata. Az **overload** kulcsszóval engedélyezhető a PAT használata.

A 2. ábrán látható példakonfiguráció túlterheléses címfordítást hoz létre a NAT-POOL2 nevű címkészlethez. A NAT-POOL2 a 209.165.200.226-tól a 209.165.200.240-ig tartalmaz címeket. A 192.168.0.0/16 hálózatbeli állomások képezik a fordítás tárgyát. Az S0/0/0 interfészt belső, a S0/1/0 interfészt pedig külső interfészként azonosítjuk.

Használjuk a parancsszimulátort a 3. ábrán, hogy beállítsuk a PAT címkészlettel történő használatát az R2-n!

# A NAT konfigurálása

## A port címfordítás (Port Address Translation, PAT) konfigurálása

**A PAT konfigurálása egyetlen publikus IPv4-cím esetén**

Az 1. ábra topológiája egy olyan PAT-megvalósítást mutat, ahol egyetlen nyilvános IPv4-címet használunk a címfordításhoz. A példában az összes 192.168.0.0/16 hálózaton lévő (az ACL 1-re illeszkedő) gép, amely a forgalmat az R2 forgalomirányítón keresztül küldi az internetre, lefordításra kerül a 209.165.200.225 címre (az S0/1/0 interfész IPv4-címére). Az adatfolyamokat a címfordítási táblában a portszámok fogják azonosítani, mivel az **overload** kulcsszót használták.

A 2. ábra mutatja a követendő lépéseket a PAT egyetlen IPv4-címmel való konfigurálásához. Ha csak egyetlen nyilvános IPv4-cím áll rendelkezésre, a túlterheléses konfiguráció a publikus címet általában a külső interfészhez rendeli hozzá, amely összeköttetést biztosít a szolgáltatóval. Minden belső cím erre az egyetlen IPv4-círe lesz lefordítva, ahogy kilép a külső interfészen.

**1. lépés:** Adjunk meg egy ACL-t, hogy engedélyezzük a lefordítandó forgalmat.

**2. lépés:** Konfiguráljuk a forrás címfordítást az **interface** és **overload** kulcsszavakkal. Az **interface** kulcsszó azonosítja, hogy melyik interfész IP-címét használjuk, amikor lefordítjuk a belső címeket. Az **overload** kulcsszó utasítja a forgalomirányítót, hogy kövesse nyomon a portszámokat minden egyes címfordítási bejegyzésnél.

**3. lépés:** Határozzuk meg, melyek a belső interfészek a NAT viszonylatában. Ez minden olyan interfész, amely a belső hálózathoz csatlakozik.

**4. lépés:** Határozzuk meg, melyik a külső interfész a NAT viszonylatában. Ez ugyanaz az interfész, mint amit a 2. lépésben a forrás címfordítási utasításnál azonosítottunk.

A konfiguráció hasonló a dinamikus NAT-hoz, kivéve, hogy egy készlet neve helyett az **interface** kulcsszót használjuk a külső IPv4-cím azonosítására. Ezért nincs NAT-címkészlet definiálva.

Használjuk a parancsszimulátort a 3. ábrán, hogy beállíthassuk a PAT egyetlen címmel történő használatát az R2-n!

# A NAT konfigurálása

## A port címfordítás (Port Address Translation, PAT) konfigurálása

A NAT túlterhelés folyamata ugyanaz, akár készletbeli címeket, akár egyetlen címet használunk. Folytatva a korábbi PAT-példát, a PC1 kommunikálni akar az Svr1 webszerverrel egy nyilvános IPv4-címet használva. Ugyanabban az időpontban egy másik kliens, a PC2 hasonló munkamenetet kíván létrehozni az Svr2 webszerverrel. Mind a PC1, mind a PC2 privát IPv4-címmel van beállítva, az R2-n pedig engedélyezve van a PAT.

**A PC-től a szerverig tartó folyamat**

1. Az 1. ábra mutatja mind a PC1-et, mind a PC2-t, amint csomagokat küldenek az Svr1 és az Svr2 felé. A PC1 IPv4-forráscíme 192.168.10.10, a TCP forrásportja pedig 1444. A PC2 IPv4-forráscíme 192.168.10.11, és véletlenül ugyanazt a forrásportot, az 1444-et használja.

2. Először a PC1 csomagja éri el az R2-t. A PAT használatakor az R2 az IPv4-forráscímet 209.165.200.225-re (belső globális cím) módosítja. Nincs más eszköz a címfordítási táblában, ami az 1444-es portot használná, így a PAT megtartja ugyanazt a portszámot. A csomag ezután továbbítódik a 209.165.201.1 címen található Svr1 felé.

3. Ezután a PC2 csomagja éri el az R2-t. A PAT úgy van beállítva, hogy a 209.165.200.225 belső globális IPv4-címet használja minden fordításhoz. Hasonlóan a PC1 fordítási folyamatához, a PAT megváltoztatja a PC2 IPv4-forráscímét a 209.165.200.225 belső globális címre. Azonban a PC2 ugyanazzal a forrásporttal rendelkezik, mint egy jelenlegi PAT-bejegyzés a PC1 fordításához. A PAT addig növeli a forrásport számát, amíg az egyedi érték nem lesz a táblázatban. Ebben az esetben a címfordítási táblában lévő forrásport-bejegyzés és a PC2-höz tartozó csomag is az 1445-öt kapja.

Bár a PC1 és a PC2 ugyanazt a lefordított címet használja (a 209.165.200.225 belső globális címet), és ugyanaz a forrásport száma is (1444), de a PC2 címfordítási táblán belül módosított portszáma (1445) mégis minden bejegyzést egyedivé tesz. Ez nyilvánvalóvá válik azoknál a csomagoknál, amelyeket a szerver visszaküld az klienseknek.

**A szervertől a PC-ig tartó folyamat**

4. Amint a 2. ábrán látható, egy tipikus kliens-szerver adatcsere esetén a Svr1 és az Svr2 reagál a PC1-től és a PC2-től kapott kérésekre. A szerverek a kapott csomagban lévő forrásportot használják célportként, a forráscímet pedig a célállomás címeként a visszatérő forgalomban. A szerverek számára úgy tűnik, mintha ugyanazzal a géppel, a 209.165.200.225-tel kommunikálnának; azonban nem ez a helyzet.

5. Ahogy a csomagok megérkeznek, az R2 megkeresi az egyedi bejegyzéseket a címfordítási táblában, felhasználva a célcímet és a célportot minden csomag esetében. Az Svr1-től érkező csomag esetében a 209.165.200.225 IPv4-célcím többször is be van jegyezve, de csak az egyiknél 1444 a célport értéke. A táblázatban lévő bejegyzés segítségével az R2 megváltoztatja a csomag IPv4-célcímét 192.168.10.10-re, így nincs szükség a célport megváltoztatására. A csomagot ezután továbbítja a PC1 felé.

6. Amikor az Svr2 csomagja érkezik meg, az R2 hasonló fordítást végez. A 209.165.200.225 IPv4-célcím ismét több bejegyzésben megtalálható. Viszont az 1445-ös célporttal az R2 képes egyedileg azonosítani a fordítási bejegyzést. Az IPv4-célcím 192.168.10.11-re változik. Ebben az esetben a célportot is módosítani kell, vissza az eredeti 1444-es értékre, amely a címfordítási táblában szerepel. A csomagot ezután továbbítja a PC2 felé.

# A NAT konfigurálása

## A port címfordítás (Port Address Translation, PAT) konfigurálása

Az R2 forgalomirányítót úgy állították be, hogy PAT szolgáltatást biztosítson a 192.168.0.0/16 klienseknek. Amikor a belső állomások az R2-n keresztül kijutnak az internetre, a címük fordítása egy PAT-címkészletből származó IPv4-címre történik, egyedi forrás portszámmal.

Ahogy az 1. ábrán is látható, ugyanazokat a parancsokat használjuk a PAT, mint a statikus és a dinamikus NAT ellenőrzésére. A **show ip nat translations** parancs két különböző állomásról jeleníti meg a fordításokat különböző webszerverekhez. Figyeljük meg, hogy két különböző belső állomás ugyanazt a 209.165.200.226-os IPv4-címet (belső globális cím) kapja meg! A forrás portszámok tesznek különbséget a címfordítási táblában a két eset között.

Amint a 2. ábrán látható, a **show ip nat statistics** parancs ellenőrzi, hogy a NAT-POOL2-ből jutott-e cím mindkét fordításhoz. A kimenet megjeleníti az aktív címfordítások teljes számát, a NAT-konfiguráció paramétereit, valamint a címkészlet már kiosztott és a még kiosztható elemeinek számát.

# A NAT konfigurálása

## Port továbbítás

A port továbbítás (port forwarding, néha alagutazás) az a tevékenység, amelynek során egy hálózati portot továbbítunk egyik hálózati csomópontról a másikra. Ez a technika lehetővé teszi egy külső felhasználó számára, hogy kívülről érhessen el egy privát IPv4-címen (belső LAN-on) lévő portot, egy NAT-képes forgalomirányítón keresztül.

A P2P fájlmegosztó programok és olyan műveletek, mint például a webszolgáltatás, valamint a kimenő FTP, általában megkövetelik, hogy a forgalomirányító portjait továbbítsuk vagy megnyissuk ezen alkalmazások működése érdekében, ahogy az 1. ábra mutatja. Mivel a NAT elrejti a belső címeket, a P2P csak ott működik belülről kifelé, ahol a NAT le tudja képezni a kimenő kérésekre beérkező válaszokat.

A probléma az, hogy a NAT nem teszi lehetővé kérések kívülről jövő kezdeményezését. Ezt a helyzetet kézi beavatkozással lehet megoldani. A port továbbítást be lehet úgy állítani, hogy meghatározzuk azokat az adott portokat, amelyek továbbíthatók a belső állomások felé.

Emlékezzünk vissza, hogy az internetes szoftveralkalmazások felhasználói portokkal kommunikálnak. A portoknak nyitva vagy elérhetőnek kell lenniük ezen alkalmazások számára. A különböző alkalmazások különböző portokat használnak. Ez kiszámíthatóvá teszi az alkalmazások és a forgalomirányítók számára a hálózati szolgáltatások azonosítását. A HTTP például a jól ismert 80-as porton keresztül működik. Ha valaki beírja a **http://cisco.com** címet, a böngésző megjeleníti a Cisco Systems Inc. honlapját. Figyeljük meg, hogy nem kell megadni a HTTP portszámát a lap lekéréséhez, mert az alkalmazás feltételezi, hogy az a 80-as port!

Amennyiben egy másik portszámot kellene megadni, akkor azt kettősponttal (:) elválasztva csatolni kell az URL-hez. Ha a webszerver például a 8080-as porton figyel, akkor a felhasználónak a következőt kell begépelni: **http://www.example.com:8080**.

A port továbbítás lehetővé teszi az interneten lévő felhasználók számára, hogy hozzáférjenek a belső szerverekhez a forgalomirányító WAN-portcíme és a megfelelő külső portszám segítségével. A belső szervereket általában az RFC 1918 privát IPv4-címekkel konfigurálják. Amikor egy kérés érkezik a WAN-port IPv4-címére az interneten keresztül, a forgalomirányító továbbítja a kérést a megfelelő szerverhez a LAN-on. Biztonsági okokból a szélessávú forgalomirányítók alapértelmezés szerint nem engedélyezik külső hálózati kérések továbbítását a belső állomásokhoz.

A 2. ábra egy kis üzlet tulajdonosát mutatja egy értékesítési (Point of Sale, POS) szerverrel, hogy a boltban nyomon kövesse az értékesítést és a készletet. A szerver elérhető a bolton belül, viszont mivel privát IPv4-címe van, nyilvánosan nem érhető el az interneten. A port továbbítás engedélyezése a helyi forgalomirányítón lehetővé teszi, hogy a tulajdonos bárhonnan az internetről elérje az értékesítési szervert. A port továbbítást a forgalomirányítón a célport számának és az értékesítési szerver privát IPv4-címének felhasználásával állítjuk be. A szerverhez való hozzáféréskor a kliens-oldali szoftver a forgalomirányító nyilvános IPv4-címét és a szerver portszámát használja.

# A NAT konfigurálása

## Port továbbítás

Az ábrán egy Linksys EA6500 SOHO forgalomirányító Single Port Forwarding (egyszerű port továbbítás) konfigurációs ablaka látható. Alapértelmezésben a port továbbítás nincs engedélyezve az eszközön.

A port továbbítást engedélyezni lehet az alkalmazások számára a belső helyi cím megadásával, ahova a kérelmeket el kell küldeni. Az ábrán a Linksys forgalomirányítóra beérkező, HTTP-szolgáltatás iránti kéréseket továbbítják a webszerver 192.168.1.254 belső helyi címére. Ha az otthoni/kisirodai forgalomirányító WAN-interfészének külső IPv4-címe 209.165.200.225, a külső felhasználó megadhatja a **http://www.example.com** címet, és a Linksys eszköz átirányítja a HTTP-kérést a a 192.168.1.254 címen található belső webszerverhez, az alapértelmezett 80-as portszámot használva.

Az alapértelmezett 80-astól eltérő port is megadható. A külső felhasználónak ugyanakkor tudnia kell, hogy ezt az adott portszámot használja. Egy másik port megadásához a külső port (External Port) értékét kell a Single Port Forwarding ablakban módosítani.

A megközelítés, ahogy a port továbbítást konfigurálni kell, függ a szélessávú forgalomirányító márkájától és a modelltől. Mindazonáltal néhány általános lépést kell követni. Ha a szolgáltató által biztosított vagy a forgalomirányítóhoz mellékelt utasítások nem adnak megfelelő iránymutatást, a [http://www.portforward.com](http://www.portforward.com/) oldal több szélessávú eszközhöz kínál útmutatókat. Kövessük a portok hozzáadására vagy törlésére vonatkozó utasításokat, hogy az megfeleljen minden engedélyezni vagy tiltani kívánt alkalmazás igényeinek.

# A NAT konfigurálása

## Port továbbítás

A port továbbítás IOS parancsokkal történő megvalósítása hasonló, mint a statikus NAT beállításához használt parancsok. A port továbbítás lényegében egy statikus NAT, adott TCP- vagy UDP-portszámmal.

Az 1. ábra a statikus NAT azon parancsát mutatja be, amelyet a port továbbítás konfigurálásához használunk az IOS segítségével.

A 2. ábra a port továbbítás IOS parancsokkal történő beállítására mutat egy példát az R2 forgalomirányítón. A 192.168.10.254 a webszerver belső helyi IPv4-címe, amely a 80-as porton figyel. A felhasználók a belső webszerver eléréséhez a 209.165.200.225 globális IP-címet, vagyis egy globálisan egyedi nyilvános IPv4-címet használnak. Jelen esetben ez az R2 forgalomirányító Serial 0/1/0 interfészének címe. A globális port 8080-as értékre lett beállítva. Ez a célport, a globális 209.165.200.225 IPv4-címmel együtt biztosítja a belső webszerver elérését. Figyeljük meg a NAT-konfigurációnál használt parancs következő paramétereit:

* *helyi-ip* = 192.168.10.254
* *helyi-port* = 80
* *globális-ip* = 209.165.200.225
* *globális-port* = 8080

Ha nem egy jól ismert portszám használatáról van szó, a kliensnek meg kell adnia az alkalmazáshoz használt a portszámot.

Csakúgy, mint a NAT egyéb típusainál, a port továbbítás is igényli mind a külső, mind a belső NAT-interfészek beállítását.

A statikus NAT-hoz hasonlóan, a **show ip nat translations** parancs használható a port továbbítás ellenőrzésére, amint az a 3. ábrán is látható.

A példában, amikor a forgalomirányító megkapja a csomagot a 209.165.200.225 belső globális IPv4-címmel és a 8080-as TCP-célporttal, a címfordítási táblában való kereséshez az IPv4-célcímet és -célportot használja. A forgalomirányító ezután lefordítja a címet az állomás 192.168.10.254 belső helyi címére és a 80-as célportra. Az R2 végül továbbítja a csomagot a webszervernek. A webszervertől a kliens felé visszajövő csomagoknál ez a folyamat megfordul.

# A NAT konfigurálása

## A NAT és az IPv6 konfigurálása

Az 1990-es évek elejétől kezdve az IETF prioritásai között szerepelt az IPv4-címtartomány kimerülése miatti aggodalom. Az RFC 1918 szerinti magán IPv4-címek és a NAT kombinálása alapvető szerepet játszott ennek a folyamatnak a lassításában. A NAT jelentős hátrányokkal is bír, és 2011. januárjában az IANA kiosztotta az utolsó IPv4-címeket a RIR-ek számára.

Az IPv4 NAT egyik akaratlan előnye, hogy elrejti a privát hálózatot az internet felől. A NAT-nak megvan az az előnye, hogy a biztonság egy érzékelhető szintjét biztosítja a belső gépekhez való hozzáférés megtiltásával a nyilvános interneten lévő számítógépekről. Viszont nem tekinthető a megfelelő hálózati biztonság - mint amilyet a tűzfal biztosít - helyettesítésének.

Az RFC 5902-be az IAB (Internet Architecture Board) többek között az alábbi idézetet rakta az IPv6 hálózati címfordításra vonatkozóan:

"Általában érzékelhető, hogy a NAT-eszköz biztosít egy bizonyos védelmi szintet nyújt, mivel a külső állomások közvetlenül nem kezdeményezhetnek kommunikációt a NAT mögötti állomásokkal. Ugyanakkor a NAT-eszközöket nem szabad összetéveszteni a tűzfalakkal. Amint azt az [RFC4864] 2.2-es fejezete tárgyalja, a címfordítás önmagában nem nyújt biztonságot is. Az állapottartó szűrési funkció azonos szintű védelmet biztosít a fordítási funkció igénye nélkül."

Az IPv6 a 128-bites címtartománnyal 340 szextillió címet biztosít. Ezért a címtartomány mérete nem probléma. Az IPv6-ot azzal a szándékkal fejlesztették, hogy szükségtelenné tegye az NAT nyilvános és privát IPv4-címek közötti fordítási funkcióját. Ugyanakkor az IPv6 a NAT egy bizonyos formáját is megvalósítja. Az IPv6 tartalmaz saját, privát IPv6-címtartományt és NAT-ot is, amelyet azonban másképpen valósít meg, mint az IPv4.

# A NAT konfigurálása

## A NAT és az IPv6 konfigurálása

Az IPv6 egyedi lokális címek (Unique Local Addresses, ULA) mutatnak némi hasonlóságot az IPv4 RFC 1918 privát címeivel, de van néhány lényeges különbség is közöttük. Az ULA mögötti szándék az, hogy IPv6-címtartományt biztosítson egy helyi telephelyen belüli kommunikációhoz. Ez nem azt jelenti, hogy további IPv6-címtartományt biztosítana, és az sem célja, hogy a biztonság szintjét növelje.

Amint az ábrán látható, az ULA előtagja FC00::/7, ami az első hextett FC00-tól FDFF-ig terjedő tartományát jelenti. A következő bit értéke 1-es, ha az előtagot helyileg rendelték hozzá. A 0 beállítást valószínűleg a jövőben fogják meghatározni. A következő 40 bit egy globális azonosító, amit egy 16-bites alhálózati azonosító követ. Ez az első 64 bit összességében adja ki az ULA előtagját. Ez meghagyja a fennmaradó 64 bitet az interfészazonosító, vagy az IPv4 esetében az állomásazonosító rész számára.

Az egyedi lokális címeket az RFC 4193 határozza meg. Az ULA-kat lokális IPv6-címként is ismerik (nem tévesztendő össze az IPv6 link-local címekkel) és számos jellemzőjük van, többek között:

* Lehetővé teszi a telephelyek összevonását vagy magánjellegű összekapcsolását anélkül, hogy bármilyen címütközést okozna, esetleg azon interfészek újracímzését igényelné, amelyek használják ezeket az előtagokat.
* Nem függ egyetlen szolgáltatótól sem, és felhasználható a kommunikációhoz bármilyen internetkapcsolat nélküli telephelyen belül.
* Nem irányítható az interneten keresztül, azonban, ha véletlenül kiszivárog a forgalomirányítás vagy a DNS miatt, akkor nincs ütközés más címekkel.

Az ULA nem annyira egyértelmű, mint az RFC 1918 címek. Ellentétben a privát IPv4-címekkel, az IETF-nek nem volt szándéka, hogy egyfajta NAT-ot használjunk az egyedi lokális címek és az IPv6 globális egyedi címek közötti fordításhoz.

Az IPv6 egyedi lokális címek megvalósítását és lehetséges felhasználását továbbra is vizsgálja az internetes közösség. Az IETF például azt fontolgatja, hogy lehetővé teszi az ULA-előtag helyileg való létrehozásának lehetőségét FC00::/8 értékkel, illetve annak egy harmadik fél által történő automatikus kiosztását az FD00::/8-tól kezdődően.

**MEGJEGYZÉS**: Az eredeti IPv6-specifikáció lefoglalt egy címtartományt a telephelyen belüli (site-local) címeknek, az RFC 3513 szerint. A telephelyen belüli címek azóta elavultak az IETF RFC 3879 szerint, mert a "telephely" fogalma kétértelmű. A telephelyen belüli címek a FEC0::/10 előtag-tartománnyal rendelkeztek, és még mindig megtalálhatók néhány régebbi IPv6-dokumentációban.

# A NAT konfigurálása

## A NAT és az IPv6 konfigurálása

Az IPv6 NAT használata egészen más viszonylatban történik, mint az IPv4 NAT esetében. Az IPv6 NAT módozatait transzparens elérésre használják csak IPv6- illetve csak IPv4-képes hálózatok között. Nem használatos egyfajta privát IPv6-ról globális IPv6-ra történő fordításhoz.

Ideális esetben az IPv6-ot natív módon kell futtatni, ahol csak lehetséges. Ez azt jelenti, hogy az IPv6-eszközök tisztán IPv6-hálózatokon keresztül kommunikálnak egymással. Azért, hogy segítse az áttérést az IPv4-ről az IPv6-ra, az IETF számos átmeneti technikát fejlesztett ki a különböző IPv4-ről IPv6-ra való átállási forgatókönyvek befogadására, beleértve a dual-stack, valamint az alagutazási és címfordítási technikákat.

A dual-stack (kettős protokollkészlet) eszközök egyszerre futtatják az IPv4-re és az IPv6-ra épülő protokollokat is. Az IPv6-alagutazás az a folyamat, amikor egy IPv6-csomagot egy IPv4-csomag belsejébe ágyazunk. Ez lehetővé teszi az IPv6-csomag továbbítását a tisztán IPv4-hálózaton.

Az IPv6 NAT nem használható hosszú távú stratégiaként, csak mint ideiglenes mechanizmus, hogy segítséget nyújtson az IPv4-IPv6 migrációban. Az évek során már több típusú NAT létezett az IPv6-hoz, beleértve a Hálózati Címfordítás - Protokollfordítás (Network Address Translation-Protocol Translation, NAT-PT) technikát. A NAT-PT elavulásáról az IETF döntött, a cseréjének szánt NAT64 javára. A NAT64 túlmutat ezen tananyag keretein.

# A NAT hibaelhárítása

## A NAT hibaelhárítása

Az 1. ábra az R2 forgalomirányítót mutatja, amelyen engedélyezték a PAT-ot a 209.165.200.226 - 209.165.200.240 címtartományt felhasználva.

Ha egy NAT-ot alkalmazó környezetben problémák jelentkeznek az IPv4-alapú kapcsolatok működésében, akkor általában elég nehéz felderíteni a hiba okát. A probléma megoldásában az első lépés az, hogy kizárjuk a NAT-ot, mint hibaokot. Kövessük az alábbi lépéseket annak ellenőrzésére, hogy a NAT a várakozásoknak megfelelően működik-e:

**1. lépés:** A konfiguráció alapján pontosan, tisztán definiáljuk, hogy mit várunk a NAT-tól. Ez felfedi, ha probléma van a konfigurációval.

**2. lépés:** Ellenőrizzük, hogy helyes fordítások találhatók-e a címfordítási táblában a **show ip nat translations** paranccsal.

**3. lépés:** Használjuk a **clear** és **debug** parancsokat a NAT elvárt működésének ellenőrzéséhez. Ellenőrizzük, hogy a dinamikus bejegyzések létrejönnek-e újra, miután töröljük őket.

**4. lépés:** Részletesen vizsgáljuk meg, hogy mi történik a csomagokkal, és ellenőrizzük, hogy a forgalomirányítók rendelkeznek-e a csomagok helyes továbbításához szükséges irányítási információkkal.

A 2. ábra mutatja a **show ip nat statistics** és **show ip nat translations** parancsok kimenetét. Mielőtt használnánk a **show** parancsokat, töröljük a NAT statisztikáit és bejegyzéseit a címfordítási táblából a **clear ip nat statistics** és **clear ip nat translation \*** parancsokkal. Miután a 192.168.10.10 című állomás a Telnet használatával csatlakozik a 209.165.201.1 című szerverhez, jelenítsük meg a NAT-statisztikákat és a címfordítási táblát, hogy ellenőrizzük a NAT elvárt működését.

Egy egyszerű hálózati környezetben érdemes nyomon követni a NAT-statisztikákat a **show ip nat statistics** paranccsal. A **show ip nat statistics** parancs információkat jelenít meg az összes aktív fordításról, NAT-konfigurációs paraméterről, a készletben lévő címek és a lefoglalt címek számáról. Egy összetettebb NAT-környezetben azonban, ahol több fordítás is zajlik, ez a parancs nem azonosítja egyértelműen a problémát. Szükség lehet a **debug** parancs futtatására a forgalomirányítón.

# A NAT hibaelhárítása

## A NAT hibaelhárítása

Használjuk a **debug ip nat** parancsot, hogy ellenőrizzük a NAT-funkció működését minden, a forgalomirányító által lefordított csomagról szóló információ megjelenítésével. A **debug ip nat detailed** parancs leírást ad minden fordításra kerülő csomagról. A parancs bizonyos hibákról és kivételes helyzetekről is információkat ad, ilyen például a globális cím hozzárendelésének sikertelensége. A **debug ip nat detailed** parancs többletterhet jelent a **debug ip nat** parancshoz képest, de ez biztosítja azt a részletességet, amire szükség lehet a NAT-probléma elhárításánál. Mindig kapcsoljuk ki a hibakeresést, ha végeztünk!

Az 1. ábra egy mintát mutat a **debug ip nat** kimenetére. Azt mutatja, hogy a forgalmat a belső állomás (192.168.10.10) kezdeményezte a külső állomás felé (209.165.201.1), és a forráscímet lefordították a 209.165.200.226-ra.

A debug kimenetének értelmezésekor vegyük figyelembe, hogy mit jelentenek a következő szimbólumok és értékek:

* **\* (Csillag)** - A NAT szó mellett látható csillag arra utal, hogy a fordítás a gyorskapcsolású útvonalon történik. Az első csomag a párbeszéden belül mindig folyamatkapcsolású, ami lassabb. A további csomagok a gyorskapcsolású útvonalon haladnak, feltéve, hogy létezik megfelelő gyorsítótár-bejegyzés.
* **s=** - Ez a szimbólum a IP-forráscímet jelzi.
* **a.b.c.d**--->**w.x.y.z** - Ez az érték mutatja, hogy az a.b.c.d forráscímet fordítjuk le w.x.y.z-re.
* **d=** - Ez a szimbólum a IP-célcímet mutatja.
* **[xxxx]** A szögletes zárójelek között látható érték az IP-azonosító. Az információ hasznos lehet a hibakereséskor, mivel a segítségével kapott kimenet összevethető az egyéb protokollelemzők által végzett csomagkövetések eredményeivel.

**MEGJEGYZÉS**: Ellenőrizzük, hogy a NAT parancsban lévő ACL-hivatkozás engedélyezi-e az összes szükséges hálózatot. A 2. ábrán csak a 192.168.0.0/16 címek jogosultak a címfordításra. A belső hálózatról az internetre szánt csomagokat, amelyek forráscímeit nem engedélyezi kifejezetten az 1-es ACL, nem fordítja le az R2.

# A NAT hibaelhárítása

## A NAT hibaelhárítása

**1. esettanulmány**

Az 1. ábra azt mutatja, hogy a 192.168.0.0/16 LAN-on lévő állomásokról, a PC1-ről és a PC2-ről nem lehet pingelni a külső hálózatbeli szervereket, az Svr1-et és az Svr2-t.

A probléma hibakereséséhez használjuk a **show ip nat translations** parancsot, hogy lássuk, van-e jelenleg fordítás a címfordítási táblában. Az 1. ábra kimenete azt mutatja, hogy nincs.

A **show ip nat statistics** parancs segítségével meghatározhatjuk, hogy sor került-e fordításra. Azokat az interfészeket is azonosítja, amelyekk között a fordításnak be kellene következnie. Amint azt a 2. ábra kimenete mutatja, a NAT-számlálók értéke 0-n áll, ami azt jelenti, hogy nem történt fordítás. Ha összehasonlítjuk a kimenetet az 1. ábrán látható topológiával, észrevehetjük, hogy a forgalomirányítón a NAT belső illetve külső interfészeit helytelenül adták meg. A helytelen konfiguráció ezen kívül ellenőrizhető a **show running-config** paranccsal is.

A jelenlegi NAT interfész-konfigurációt törölni kell az interfészekről a helyes konfiguráció alkalmazása előtt.

Miután helyesen határoztuk meg a NAT külső és belső interfészeit, a következő ping a PC1-ről az Svr1 felé sikertelen. Használjuk a **show ip nat translations** és **show ip nat statistics** parancsokat, hogy lássuk, a fordítások még mindig nem jönnek létre.

Ahogy a 3. ábrán is látható, a **show access-lists** parancs segítségével meghatározhatjuk, hogy a NAT parancsban hivatkozott ACL engedélyezi-e az összes szükséges hálózatot. A kimenetet vizsgálva kiderül, hogy nem megfelelő helyettesítő bitmaszkot használtak az ACL-ben, amely meghatározza a fordítandó címeket. A helyettesítő maszk csak a 192.168.0.0/24 alhálózatot engedélyezi. A hozzáférési listát először el kell távolítani, majd újrakonfigurálni a megfelelő helyettesítő maszkkal.

Miután a konfigurációt kijavítottuk, egy PC1-ről az Svr1-re indított ping már sikeres. Ahogy a 4. ábrán is látszik, a **show ip nat translations** és **show ip nat statistics** parancsokkal ellenőrizhető, hogy a NAT-fordítás megtörténik.

# Összefoglalás

## Összefoglalás

**A NAT ellenőrzése**

**Esetleírás**

A hálózati címfordítás jelenleg nem része a vállalati hálózat kialakításának. Az a döntés született, hogy bizonyos eszközöket NAT-szolgáltatások használatára állítunk be a levelező szerverhez való csatlakozáshoz.

Mielőtt telepítenénk a NAT-ot a hálózaton, prototípust készítünk egy hálózati szimulációs program használatával.

A mellékelt PDF dokumentumban találhatók a feladathoz tartozó további utasítások.

[Csoportos feladat - NAT Check Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/11.4.1.1%20NAT%20Check%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

Ez a fejezet felvázolta, hogy a NAT miként használható arra, hogy segítsen enyhíteni az IPv4-címtartomány kimerülésének problémáját. Az IPv4 NAT segítségével a hálózati rendszergazdák használhatják az RFC 1918 magánhálózati címeket, miközben kapcsolatot biztosítanak az internethez egyetlen vagy korlátozott számú nyilvános címmel.

A NAT takarékoskodik a publikus címtérrel és jelentős adminisztratív terhektől szabadít meg a bejegyzések, mozgatások és változások felügyelete során. A NAT és a PAT megvalósításával megőrizhető a publikus címtartomány, valamint saját, biztonságos intranet építhető anélkül, hogy az befolyásolná a szolgáltatói kapcsolatot. Azonban a NAT hátrányait tekintve negatív hatással van a készülék teljesítményére, a biztonságra, a mobilitásra, valamint a végpontok közötti kapcsolatokra, és csak rövid távú megoldásként lehet figyelembe venni a címek kimerülése ellen, míg a hosszú távú megoldás az IPv6 lesz.

Ez a fejezet az IPv4 NAT-ot tárgyalta, többek között:

* a NAT jellemzőit, terminológiáját és általános működését
* a NAT különböző típusait, beleértve a statikus, a dinamikus és a túlterheléses NAT-ot
* a NAT előnyeit és hátrányait
* a statikus, a dinamikus és a túlterheléses NAT konfigurálását, ellenőrzését és elemzését
* hogyan használható a port továbbítás a belső eszközökhöz való hozzáféréshez az internetről
* a NAT hibaelhárítását a **show** és **debug** parancsokkal.

