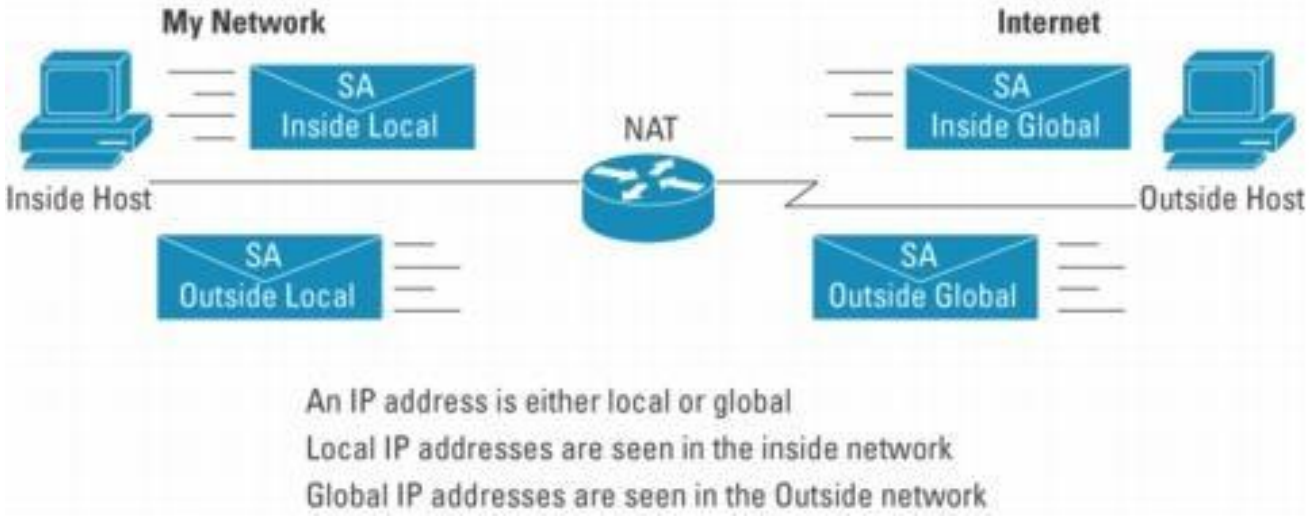
Fábián Zoltán – Hálózatok elmélet

NAT – Címfordítás
Routing – Útválasztás

Miért jött létre a NAT protokoll?

- Az IP címek megtakarításáért
- Segítségével válik lehetővé, hogy lokális IP hálózatokban szerepeljenek olyan hálózati eszközök, amelyek egymaguk több hálózati eszközt reprezentálnak a globális IP tartományokban
- A NAT protokoll használatához szükséges a routolás is – de ez majd később

Mikor használjuk?



- A belső hálózaton használt lokális címtartományból el akarjuk érni a külső globális címtartományt.
- A lokális IP címek csak a belső hálózaton láthatók
- A külső hálózatból indított kérések csak a NAT külső felének globális IP címét látják, tehát nem érik el kívülről a belső hálózat IP címeit

A NAT-ot végrehajtó eszköz leírása és szerepe

- Két hálózati csatoló van benne
  - Belső csatoló – lokális IP tartományból származik
  - Külső csatoló – globális IP tartományból származik
- A belső tartományból származó IP cím(ek) lokálisak és a globális IP tartományban csak egy IP címként látszanak.
- A külső tartományból származó globális IP címek a belső tartományban tökéletesen látszódnak

Címfordítások fajtái

- Egyszerű címfordítás: Egy IP címet fordítunk egy másikra.
- Port Address Translating (PAT): Portfordítás, amikor egy kapcsolatban lévő portot fordítunk egy másik portra
- Kiterjesztett címfordítás: Egy IP címet és port párost fordítunk másik párra
- Statikus címfordítás: Amikor egy-egy kapcsolatot fordítunk egy lokális és egy globális IP cím között
- Dinamikus címfordítás: Amikor a belső hálózat IP címeit lefordítom a globális IP tartomány egy tartományába.
  - Pl: 192.168.1.x <=> 80.81.22.x
  - A CISCO eszközök ennél cifrábbakat is tudnak!

Hogyan működik a címfordítás?

- A belső hálózat egy IP címéről egy porton keresztül el akarunk érni egy szolgáltatást,pl. 80.99.101.2:80
- A kliens gép 10.4.0.2:5000 portról küldi az IP csomagot
- A NAT a belső lábára érkező IP csomagban lecseréli a küldő IP címét a saját globális IP-jére.
- Feljegyzi a küldő IP-port párosát a memóriájában egy táblázatba
  - 10.4.0.2:5000 => 195.199.225.248:5000
- Az is előfordulhat, hogy nem csak az IP-t, hanem a portot is kicseréli másikra és a táblázatban feljegyzi a portot is
  - 10.4.0.2:5000 => 195.199.225.248:6801

A visszaérkezett válasz kezelése

- A külső IP címről a NAT külső lábára visszajövő válasz tartalmazza a küldő IP címét és portját, továbbá a cél IP címét és portját.
  - Forrás: 80.99.101.2:80
  - Címzett: 195.199.225.248:6801
- A NAT megnézi a táblázatot és kikeresi, hogy a címzett globális IP-port pároshoz milyen lokális IP port páros tartozik. A címzettet lecseréli az IP csomagban a korábban elmentett IP-port párosra:
  - 195.199.225.248:6801 => 10.4.0.2:5000

Mi történik, ha kívülről küldenek egy IP csomagot a hálóra?

- Leggyakrabban a NAT eszköz eldobja a kérést, mivel a táblázatában nem talál olyan IP-port párost, amely illene a bejövő forgalomhoz
- A NAT táblázatnak van lejárati ideje
- A kliens forráscíme véletlenszerű, kicsi az esélye annak, hogy egy csomag éppen arra a portra essen be, amelyik éppen kifelé küldött csomagot és várja a választ

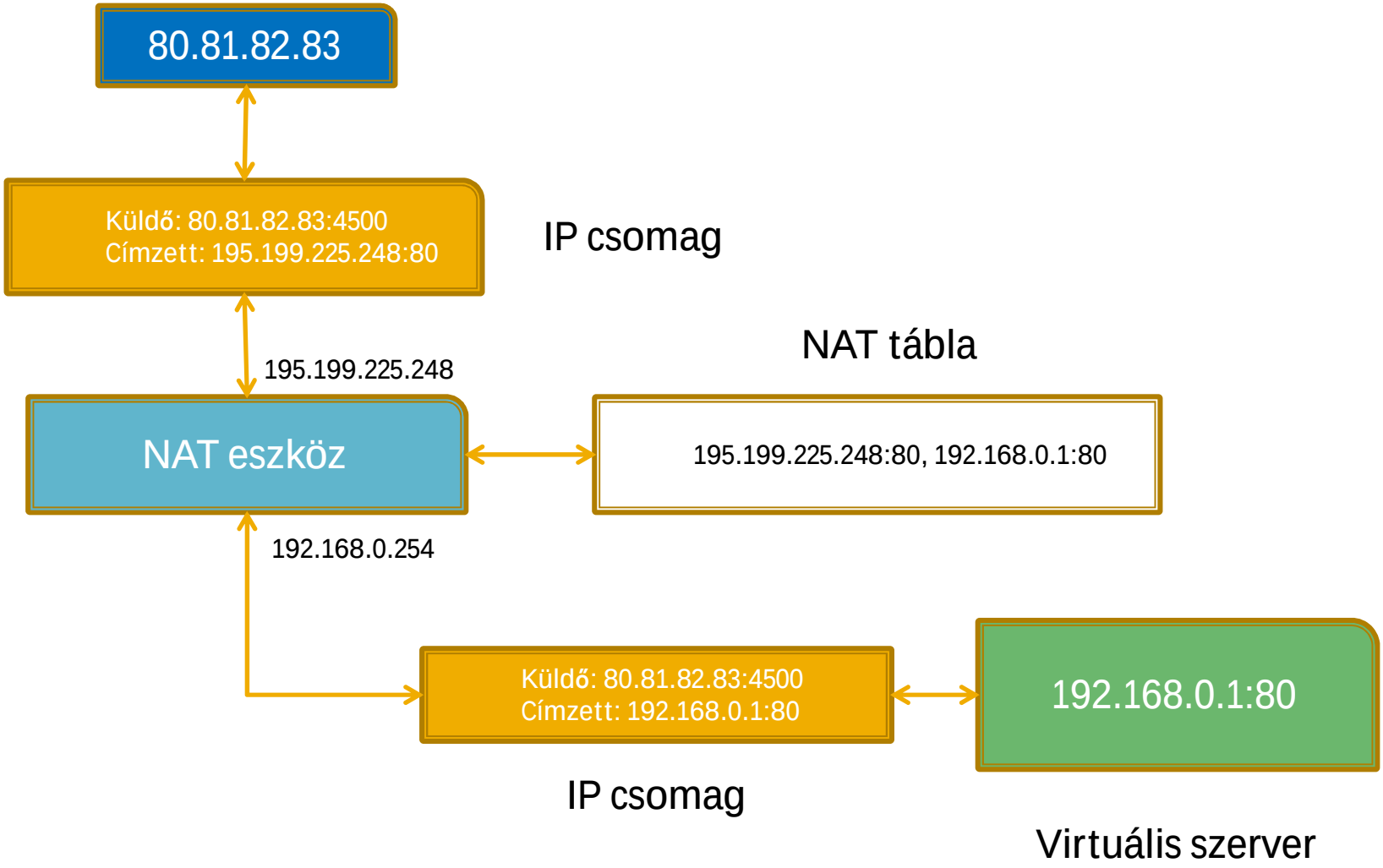
- Hogy ilyen ne legyen hozzáteszünk egy tűzfalat amely csak a válaszokat csak azokról az IP-krőI engedi be, amelyek a NAT-olás után címzettek lesznek a csomagban

- A belső gépek elérhetetlenek kívülről!

Hogyan tudunk NAT mögött szervert üzemeltetni?

- Ha egy lokális címen fut a szerver, pl.192.168.0.1:80 kívülről nem érhető el közvetlenül.
- Állítsunk be statikus NAT-olást. A NAT globális IP címét és egy portot fordítsuk le a lokális tartomány megadott IP-jére és portjára. Pl:
  - Küldő: 80.81.82.83:4500
  - Címzett: 195.199.225.248:80
- A folyamat ugyanaz. A kívülről jövő kérés címzettjét lecseréli a belső IP címre és lementi egy táblázatba a csomag paramétereit.
  - Küldő: 80.81.82.83:4500
  - Címzett: 192.168.0.1:80
- A benti szerver visszaküldi a választ a globális IP címre. Mivel a címzett globális IP cím, ezért az alapértelmezett átjáró kapja meg a csomagot. Ha a NAT eszköz belső IP címe és az alapértelmezett átjáró nem ugyanaz, akkor nem érkezik meg a válasz sem!
- A NAT eszköz visszacseréli a táblázatban letárolt értékek alapján a saját külső IP címére a Küldő IP címét és elküldi a csomagot.

A címfordítás vázlata



Linksys WRT 54G

- NAT
- PAT – Port Forward
- Port Range Forward

LINKSYS® by Cisco

Firmware Version: v7.00.8

Wireless-G Broadband Router WRT54G

Applications & Gaming

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Port Range Forward | Port Triggering | DMZ | QoS

Port Range Forward

Port Range					
Application	Start	End	Protocol	IP Address	Enable
HTTP	80 to	80	Both	192.168.0. 1	☑
FTP	20 to	21	Both	192.168.0. 1	☑
Radmin	5102 to	5102	TCP	192.168.0. 1	☑
Emule	4662 to	4662	Both	192.168.0. 1	☑
Emule2	4663 to	4663	Both	192.168.0. 1	☑
VNC	5900 to	5900	Both	192.168.0. 1	☐
Torrent	9388 to	9388	Both	192.168.0. 1	☑
Bitcomet	39999 to	39999	Both	192.168.0. 1	☑
https	443 to	443	Both	192.168.0. 1	☑
OpenVPN	1194 to	1194	Both	192.168.0. 1	☑

Port Range Forwarding: Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the **Enable** checkbox after you are finished.
More...

Save Settings | Cancel Changes

cisco

FTP szerver üzemeltetése NAT mögött

- FTP szerver üzemeltetése NAT-olva
  - Bejövő kérés a 21-en, válasz a 20-on megy ki.
  - A NAT tudni fogja-e hova küldje a választ?
- Válasz
  - Ha a NAT-nak megmondjuk, hogy egy adott PAT egy FTP protokollt fordít, akkor tudni fogja, hogy a válasz egy porttal lejjebb megy vissza.

A Gamerek hogyan játszhatnak NAT mögött?

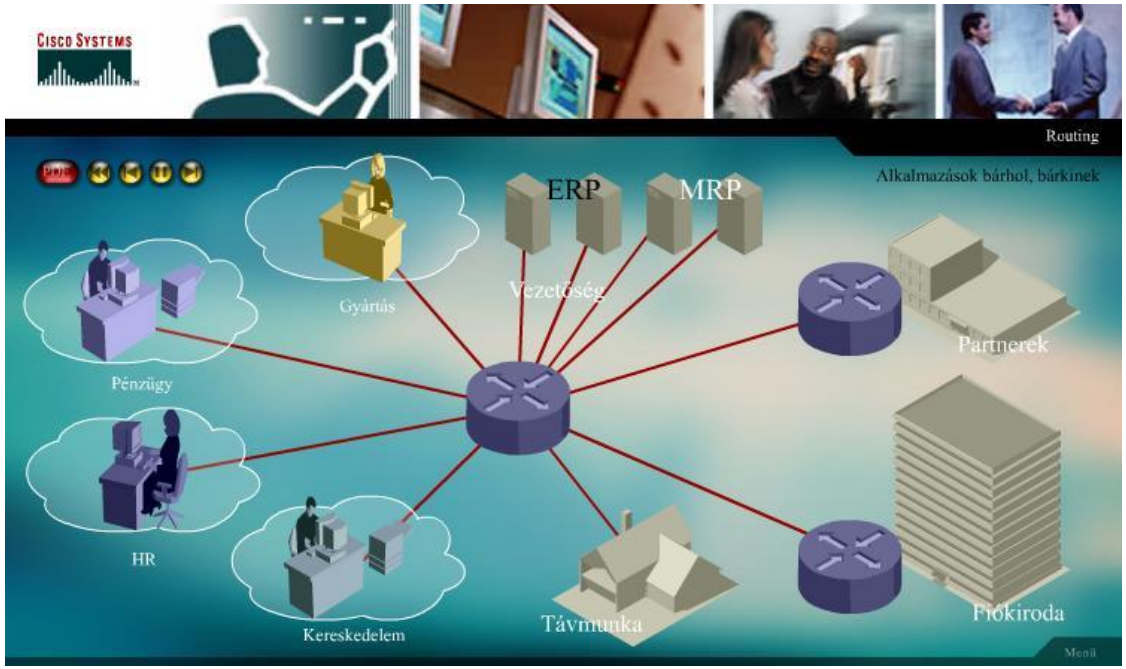
- Hogyan tud egy alkalmazás fogadni úgy kívülről jövő kéréseket, hogy nem állítunk be statikus NAT-ot?
- Válasz
  - Ha egy játéknak a NAT eszköz mögött kell egy nyilvános port, nosza nyisson egy szabályt, ami a megfelelő pillanatban beállítja a NAT-olás paramétereit automatikusan! Nem veszélyes ez? De az, de játszani kell!
  - Ha az alkalmazás leáll, akkor szűnjön meg a NAT szabály!

UPnP

- Olyan protokoll, amely segítségével a hálózati eszközök megnyithatnak automatikusan portokat tűzfalon, NAT eszközön, azokat a megfelelő portokra és saját belső IP címükre konfigurálhatják.
- Ha az eszköz lekapcsolódik a Nat-ról, akkor a port publikálása megszűnik.
- A protokollt a Microsoft kezdeményezte, mára az összes játékgyártó, illetve az intelligens hálózati eszközöket gyártó cégek csatlakoztak hozzá

Routing – Útválasztás, forgalomirányítás

- A cégek igényeiknek megfelelően sok hálózati alkalmazást használnak



A routolás működése - alapok

- Routing tábla – A szabályok táblázata, amelyek megmondják az eszköznek, hogy melyik IP csomagot melyik csatolóra továbbítsa

Célhálózat	Netmask	Kimentő interface	Következő host	Metrika

- Routolás: OSI modell 3. layer
- Routolható protokollok: IP, IPX
  - Mivel az IPX visszaszorult, ezért csak az IP-t tárgyaljuk

Autonóm rendszer, Metrika

- Autonóm rendszer
  - A hálózat forgalomirányítási szempontból egységes része
- Metrika
  - Egy routolás során előálló útvonal minőségének mérési módja
    - Távolság alapú
    - Költség alapú

A routolás működése

- A router a bemeneten érkező csomagot fogadja
- Várakozási sorba teszi
- A csomag célcímét illeszti a routing tábla soraira
- Ha nincs illeszkedő sor, akkor nem továbbítható a csomag – a router a csomagot eldobja és a feladónak visszaküld egy ICMP csomagot
- Ha van megfelelő szabály, akkor a megadott interfészen keresztül továbbítja a csomagot a szomszédhoz vagy a célállomáshoz

A statikus routolás protokoll

- A routing táblában található bejegyzéseket, a host a saját hálózati paramétereiből állítja elő
- A routing tábla kézzel is konfigurálható
  - Megjegyzés:
    - Kézzel beállított routolás újraindítás után is megmarad (Windows, Linux, hardver eszköz)
    - Open VPN esetén a csatlakozáskor a szerver kiküldhet route parancsokat, leváláskor, törlődnek a parancsok
- Előnye:
  - Egyszerű, megbízható, működik
- Hátránya
  - Nem alkalmazható változó hálózati környezetben
  - Nem optimális, nem terhelésfüggő

Dinamikus routing protokollok

- Változó hálózati környezet esetén használandók
  - Gyakori szakadás a hálózatban
  - Változó konfiguráció (WIFI eszközök)
  - Nagy forgalmú, több kapcsolattal rendelkező csomópont
- Adaptív forgalomirányítás – a változó környezet adatai alapján hoz döntéseket a router

Adaptív routing

- Elszigetelt adaptív routing – Az eszköz csak a saját kimeneteinek ismeretében hoz döntéseket (torlódás, forgalomméret)
- Elosztott adaptív forgalomirányítás – Az eszközök információt cserélnek és így hoznak routolási döntéseket
- Központosított forgalomirányítás – az egyes helyi routerek egy v. több központi routernek küldik el a forgalmi adatokat, amely ez alapján állít fel szabályokat

A routerek információt cserélnek

- A kimeneteik állapotát (sebesség, várakozási idő, stb)
- A szomszéd routerektől kapott információkat
  - Az elküldött és továbbküldött információknak élettartamuk van
  - Minden továbbküldéskor eggyel csökken az élettartam
  - Ha az élettartam nulla, akkor a router nem küldi tovább az információt

A routolás komplex feladatai

- A legrövidebb út megkeresése
- A „legrövidebb” ebben az esetben az alábbi paramétereket jelentheti
  - Távolság
  - Átviteli sebesség – sávszélesség
  - Átlagos forgalom
  - Pillanatnyi forgalom
  - Kommunikációs költség
- Torlódás – A bejövő IP csomagok várakozási sorba kerülnek => a szerver pufferei idővel megtelnek
- Befulladás (lock up) – Az adatok feldolgozása annyira lelassul, hogy a host timeout-ra fut.

A torlódás szélsőséges esete - Holtpont

- A szomszédos routerek tájékoztatják egymást a forgalmi információkról
- Csak akkor küldik tovább a csomagot, ha a szomszédos router erőforrásai felszabadultak
- Két router egymásnak akar továbbküldeni csomagot
- Kialakul a holtpont
- Az informatikában általános fogalom – az év folyamán később megnézzük az általános esetét

Távolságvektor alapú protokoll

- A router nyilvántartja, hogy a hálózatban melyik irányban milyen távolsággal érhető el a cél
- Az adatokat a routerek időnként kicserélik
- Az új információk birtokában a routerek ellenőrzik a változtatás szükségességét

Routing Information Protocol - RIP

- Távolságalapú protokoll
- Metrika: 16 ugrás = végtelen távolság
- Max. 15 router távolságban használják
- 30 sec a routing információ frissítése
- RIP táblázat adatai
  - A cél IP-je
  - A célhoz vezető optimális útvonal hossza
  - A következő routerhez vezető interface azonosítója
  - Időzítési info
  - Flag-ek

Enhanced Interior Gateway Routing Protocol – EIGRP

- CISCO távolságalapú protokollja
- 90 másodpercenként frissít
- Sokcélú, flexibilis
- A metrika összetett, összetevői
  - Sávszélesség mértéke
  - Késleltetés ideje
  - Load (a pufferek telítettsége)
  - MTU – a legnagyobb átvihető adatcsomag mérete
  - Megbízhatóság (reliability)

Link állapotú forgalomirányítás

- Szomszédok felfedezése
- Szomszédokhoz vezető út költségének mérése
- Csomag készítés a mérési eredményekből
- A csomagok elküldése a hálózat összes routerének
- Minden router ismeri a hálózat topológiáját és ki tudja számítani a legrövidebb utat (Dijkstra algoritmus = http://hu.wikipedia.org/wiki/Dijkstra-algoritmus)

Open Shortest Path First – OSPF

- Link állapotú protokoll
- 90’-es évektől alkalmazzák
- Kisebb hálózati egység esetén használják
- Routerek osztályozása
  - A területen belüli
  - Területhatáron működő
  - Gerinchálózaton működő (backbone)
- Egyenlő költségű több utas irányítás lehetősége
- IP fejléc „szolgáltatás típusa” mező használata

Konkrét Routing példák - Windows

- ROUTE PRINT – routing tábla kiíratása
  - Az routing tábla oszlopainak jelentése
    - Network cél
    - Hálózati maszk
    - Átjáró
    - Kapcsolat
    - Metrika
  - Ugyanaz, mint a NETSTAT –r
- Dzsóker használata
  - ROUTE PRINT 10.1.*

Routing tábla módosítása

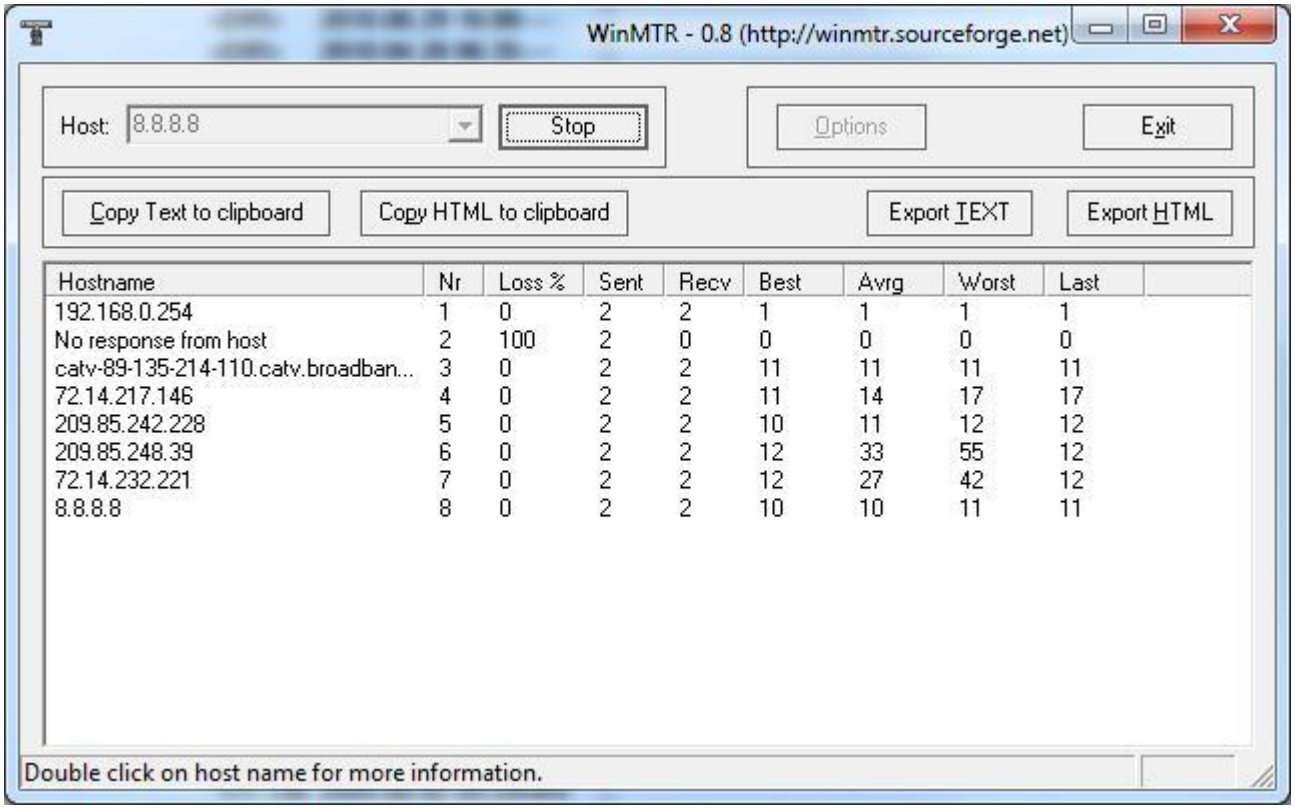
- ROUTE ADD 10.64.0.0 MASK 255.255.0.0 10.8.0.87 METRIC 10
  - Célhálózat – 10.64.0.0
  - Alhálózati maszk – 255.255.0.0
  - Saját hálózati csatoló címe – 10.8.0.87
  - Metrika – mindig a legkisebb érték felé továbbítja a csomagokat - 10
- ROUTE DELETE 10.64.0.0
- ROUTE DELETE 10.64.*

Routing adatok tárolása a Registry-ben

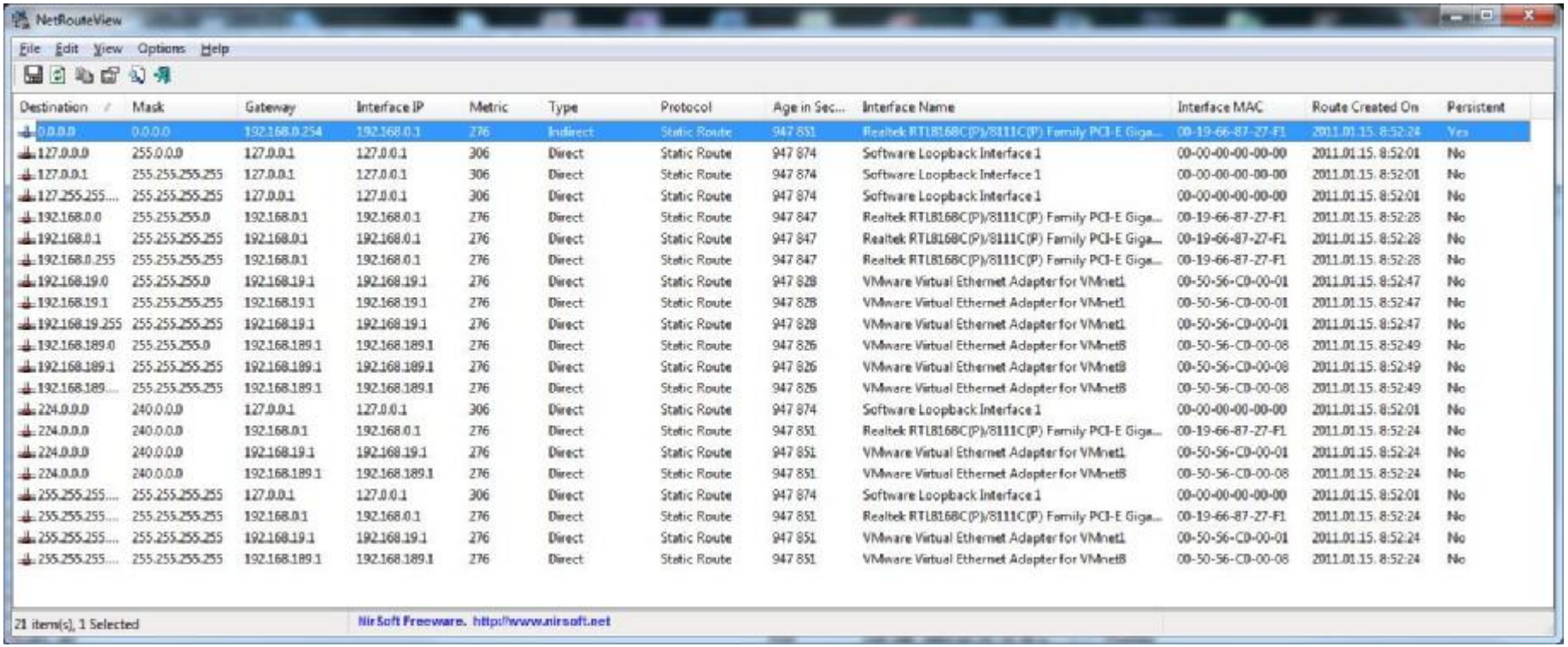
- A regisztrációs adatbázisban tárolt adat újraindítás után is megmarad
- Helye
  - HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters\ PersistentRoutes
- ROUTE –p ADD 10.64.0.0 MASK 255.255.0.0 10.8.0.88
- Töröléskor a registry-ből is törlődik

Routing szabály működésének ellenőrzése

- TRACERT parancs
- WINMTR – ingyenes



NetRouteView



További hálózati segédprogramok

- PINGINFO – Több eszköz párhuzamos pingelése
- AdapterWatch – Több hálózati eszköz adatainak kinyerése
- CPORTS – Nyitott TCP/IP és UDP portok felderítése
- SocketSniff – Windows socketek és processzek működésének felderítése
- SmartSniff – Háózati csomagok vizsgálata
  - Szükséges: NETCAP.EXE
- SniffPass – Hálózati jelszavak felderítése
- WhoisTD – Domain adatok felderítése (NSLOOKUP helyett)