Slovenská technická univerzita
Katedra informatiky a výpočtovej techniky, Fakulta elektrotechniky a informatiky
Ilkovičova 3, 812 19 Bratislava

NAT

Autor: **Pavol Lupták**
Názov: **Network Address Translators**

Študijný odbor: Informatika
Ročník: 4
Predmet: Počítačové siete II.
Školský rok: 2000/2001

Obsah

1 Úvod

- Od internet providera sme dostali pridelenú jednu (vonkajšiu) internet IP adresu (prideľovanými IANA - Internet Assigned Numbers Authority). Ako zabezpečiť plný internetový prístup veľkého množstva počítačov z našej privátnej siete na internet? (prípad PPP modemového pripojenia, kedy dostaneme od nášho ISP dynamicky pridelenú len jednu IP)
- Máme vysoko zaťažený server s konkrétnou IP. Ako zabezpečíme rovnomerné rozloženie záťaže (jednoduchý load-sharing) na viacero skrytých serverov v našej privátnej sieti?
- Ako zabezpečíme, aby všetky web prístupy z našej vnútornej siete na okolité webservery prechádzali cez našu nakonfigurovanú proxy bez toho, aby sme obťažovali používateľov nastaviť vo svojich browseroch použitie proxy servera?

Odpoveď na všetky 3 otázky je NAT alebo tiež Network Address Translators, čo v skratke vystihuje samotnú podstatu funkčnosti. V prvom prípade ide o SNAT (source NAT), implementácia pod OS Linuxom sa nazýva maškaráda (masquerading), v druhom o prípade ide o DNAT (destination NAT), tretí prípad nazývame transparentné proxy.

2 Špecifikácia NAT

2.1 RFC špecifikácia

RFC-2663 IP Network Address Translator (NAT) Terminology and Considerations
RFC-2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC-3022 Traditional IP Network Address Translator (Traditional NAT)
RFC-3027 Protocol Complications with the IP Network Address Translator

2.2 Čo je NAT?

Network Address Translation je metóda pomocou ktorej sú IP adresy mapované s jednej podsiete do druhej zabezpečujúca transparentné smerovanie až k cieľovým hostom. Existuje veľa spôsobov prekladu adries v závislosti od rôznych aplikácií. Všetky vlastnosti NAT zariadení by mali ale zodpovedať nasledujúcej charakteristike :

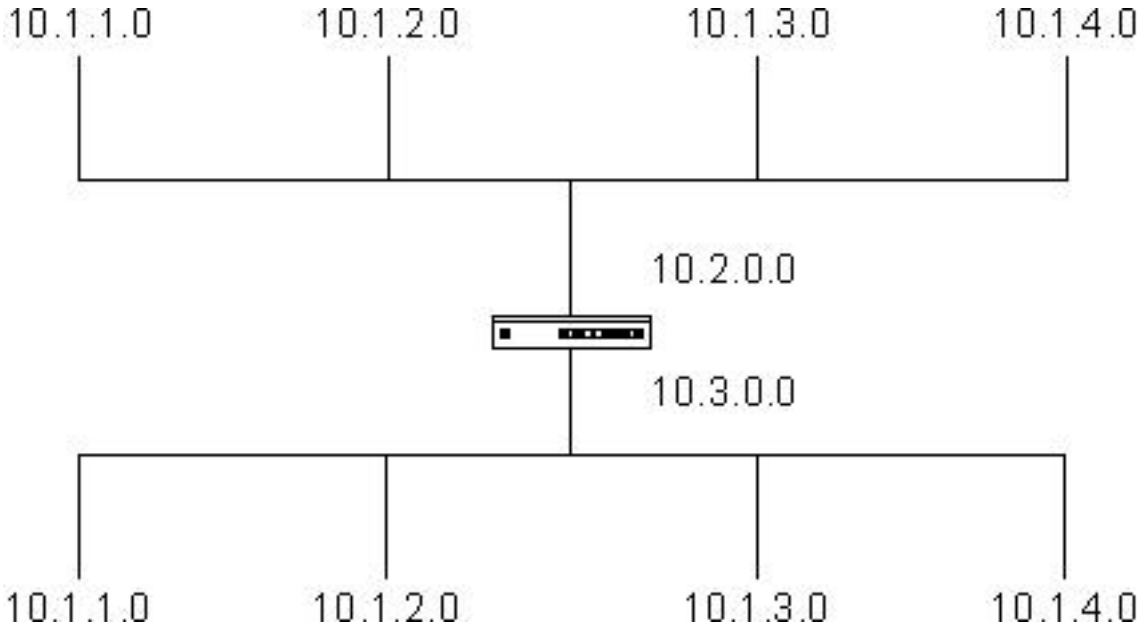
1. Transparentné mapovanie adries
2. Transparentné smerovanie po preklade adries (smerovanie v tomto prípade znamená smerovanie paketov, nie výmenu smerovacej informácie)
3. Preklad ICMP paketov potrebných na detekciu chýb

2.3 Transparentné mapovanie adries

NAT viaže adresy v privátnej sieti na adresy v globálnej (vonkajšej) sieti a naopak na to, aby bolo zabezpečené transparentné smerovanie datagramov putujúcich medzi podsieťami. Viazanie sa môže v niektorých prípadoch aplikovať na identifikátory na úrovni transportnej vrstvy (napríklad TCP/UDP porty).

2.3.1 Statické mapovanie adries

V tomto prípade ide o "jeden-na-jeden" adresné mapovanie pre hosty medzi privátnou sieťovou adresou a vonkajšou sieťovou adresou trvajúce čas typický pre NAT operáciu. Statické mapovanie adries zaisťuje, že NAT nemusí mať na starosti riadenie toku spojenia (session flows).



Obrázok 1: Preklad staticky mapovaných adries

2.3.2 Dynamické mapovanie adries

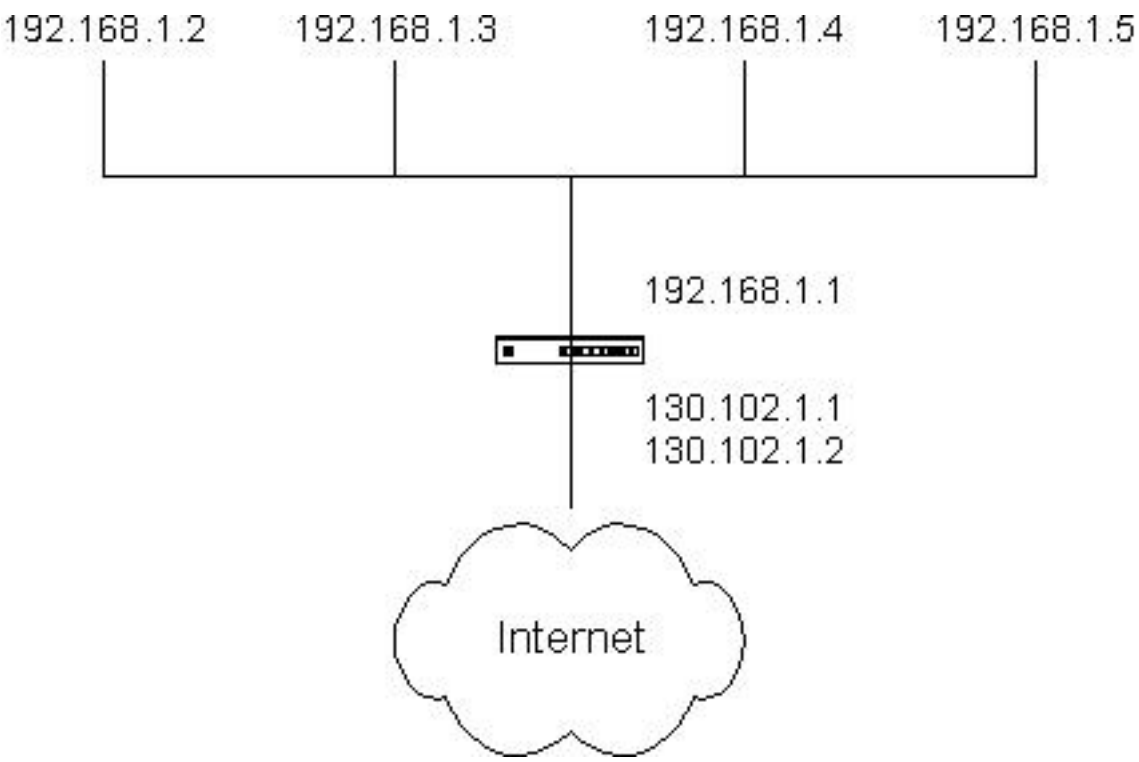
V tomto prípade sú vonkajšie adresy mapované do privátnej siete a naopak, dynamicky v závislosti od používateľských odporúčaní a toku spojenia (session flow) determinovaného heuristicky cez NAT.

2.4 Transparentné smerovanie

NAT smerovač je umiestnený medzi dvomi sieťami a prekladá adresy v IP hlavičkách tak, že keď paket odchádza z jednej siete a vstupuje do druhej, je smerovaný úplne správne. Vzhľadom k tomu, že NAT zariadenia majú pripojenie do viacerých sietí, musia zabezpečiť, aby sa medzi sieťami nešírili nesprávne informácie. Rozlišujeme tri fázy adresového prekladu. Dokopy majú tieto fázy na starosti vytvorenie, udržiavanie a ukončenie spojení (sessions) prechádzajúcich cez NAT zariadenia.

2.4.1 Viazanie adries

Viazanie adries je fáza, kedy lokálna IP adresa je asociovaná s vonkajšou adresou a naopak (potrebné pre preklad). Viazanie adries je nemenné pri statickom mapovaní adries a dynamické pri dynamickom mapovaní adries. V okamihu vytvorenia väzby medzi dvomi adresami, všetky nasledujúce spojenia z toho a do toho istého hostu budú používať rovnaké viazanie spojenia. Nove viazanie adries je vytvorené na začiatku novej sessiony, v



Obrázok 2: Preklad dynamicky mapovaných adries

prípade, že také viazanie adries doteraz ešte neexistuje. Ak je raz lokálna adresa naviazaná na vonkajšiu adresu, všetky nasledujúce spojenia smerované z rovnakej lokálnej adresy alebo smerované rovnakej lokálnej adrese budú používať rovnaké viazanie. Z toho istého hostu môže byť vytvorených simultánne viacero spojení používajúcich jedno viazenie adries.

2.4.2 Prezeranie adries a preklad

Po vytvorení spojenia, všetky pakety patriace spojení musíme prezrieť a preložiť. Rozlišujeme *address lookup*, kedy sú modifikované len hlavičky IP paketov a *transport lookup*, kedy je nutné modifikovať aj prenášanú informáciu (prit DNS, FTP, .. protokoloch). Preklad adresových (hlavičky IP paketov) ako aj transportných identifikátorov datagramu bude mať za následok, že datagram smerovaný z originálnej adresy jednej siete k cieľovej adrese druhej siete bude príslušne modifikovaný.

2.4.3 Zrušenie naviazania adries

Zrušenie naviazania adries je fáza, kedy privátna adresa už nie je dlhšiu dobu asociovanú s globálnou adresou (potrebné pre preklad). NAT prevádza rušenie naviazania adries v domnení, že posledné spojenie používajúce viazanie adries bolo už ukončené.

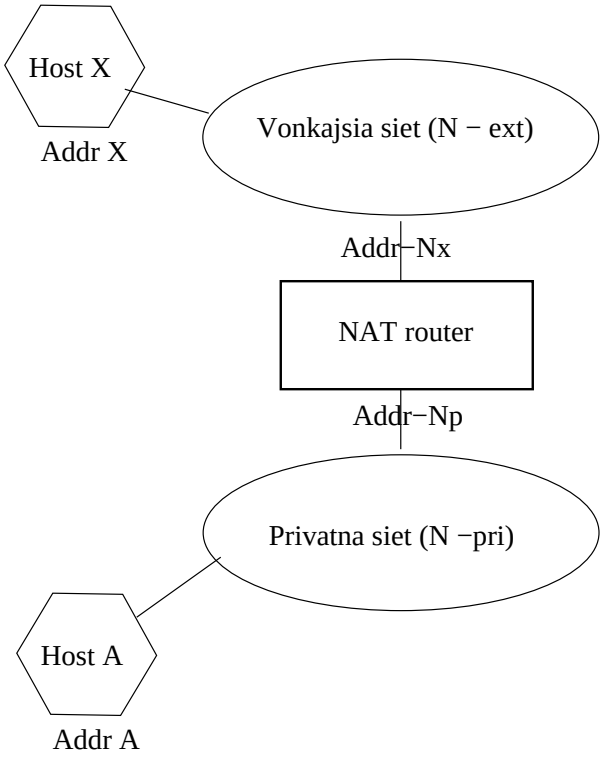
2.5 Preklad ICMP paketov potrebných na detekciu chýb

Všetky ICMP chybové správy (s výnimkou typu Redirect Message) musia byť modifikované pri prechode NAT. ICMP chybové správy na ktoré sa vzťahuje NAT modifikácia sú *Destination-Unreachable, Source-Quench, Time-Exceeded* a *Parameter-Problem*. NAT

by sa nemal snažiť prekladať správu typu Redirect. Zmeny v ICMP chybových správach zahrňujú zmeny v originál IP pakete na ktorý sa vzťahuje ICMP chybová správa. Na zabezpečenie kompletnej transparentnosti až k cieľovým hostom, IP adresy IP hlavičky vložených v správe ICMP pakete musia byť modifikované, kontrolný súčet IP hlavičky musí byť poprípade tiež modifikovaný. Tým pádom kontrolný súčet ICMP hlavičky musí byť tiež modifikovaný (vzhľadom na zmeny v IP a transportných hlavičkách), navyše normálna IP hlavička musí byť tiež modifikovaná.

2.6 Rôzne vlastnosti NAT

Nasledujúci diagram použijeme ako základný model na ilustráciu NAT vlastností. Host A s adresou Addr-A je umiestnený v privátnej sieti (N-Pri). N-Pri je izolovaná od vonkajšej sieti pomocou NAT smerovača. Host X s adresou Addr-X je umiestnený na vonkajšej sieti (N-Ext). NAT smerovač s dvomi interfejsami (každým pripojeným do jednej sieti) zabezpečuje transparentné smerovanie medzi dvomi sieťami. Interfejs pre vonkajšiu sieť má priradenú adresu Addr-Nx a interfejs pre privátnu sieť má priradenú adresu Addr-Np. Pochopiteľne, adresy Addr-A a Addr-Np korešpondujú s N-Pri sieťou a adresy Addr-X a Addr-Nx s N-Ext sieťou.



Obrázok 3: Základný model na ilustráciu NAT termínov

2.6.1 Tradičná (outbound) NAT

Tradičná NAT dovoľuje hostom v privátnej sieti transparentne pristupovať k hostom vo vonkajšej sieti. V tradičnej NAT, spojenia sú jednosmerné inicializované z vnútornej siete. To je v kontraste s obojsmernou NAT, ktorá dovoľuje obojsmerné spojenia (2.6.4). Nasleduje popis vlastností sietí podporovaných tradičnou NAT. IP adresy hostov v externej sieti sú unikátne a platné ako vo vonkajšej, tak aj v privátnej sieti. Adresy hostov

v privátnej sieti sú ale unikátne len v rámci privátnej siete a nemusia byť platné v externej sieti. Povedané inými slovami, NAT nesprístupňuje privátnu sieť vonkajšiej sieti. Ale siete vonkajšieho sveta sú sprístupnené v rámci privátnej sieti. Adresy použité v privátnej sieti sa nemôžu prekrývať s vonkajšími adresami. Daná adresa musí byť zaraditeľná - buď do privátnej siete, alebo vonkajšej, nie do oboch. Klasický NAT smerovač na obrázku 2.6 povolí hostu A inicializovať spojenie na Host X, ale nie naopak. Tiež, N-Ext je smerovateľná zo siete N-Pri, kdežto N-Pri nie je smerovateľná zo siete N-Next. Tradičná NAT sa používa hlavne v sieťach používajúcich privátne adresy, ktoré si želajú vytvárať spojenia z ich strany. Existujú dve varianty tradičnej NAT, jednoduchá NAT (Basic NAT) a NAPT (Network Address Port Translation).

2.6.2 Jednoduchá NAT

V jednoduchej NAT sa na preklad privátnych adries používa block externých adries. Pre odchádzajúce pakety z privátnej siete, sa prekladá zdrojová IP adresa ako aj príslušné položky (IP, TCP, UDP a ICMP kontrolné súčty hlavičiek). Pre prichádzajúce pakety sa prekladá cieľová IP adresa a hore uvedené kontrolné súčty. Jednoduchý NAT smerovač môže byť nakonfigurovaný aby prekladal sieť N-Pri na blok vonkajších adries, povedzme Addr-i až Addr-n patriacich do externej siete N-Ext.

2.6.3 Network Address Port Translation (NAPT)

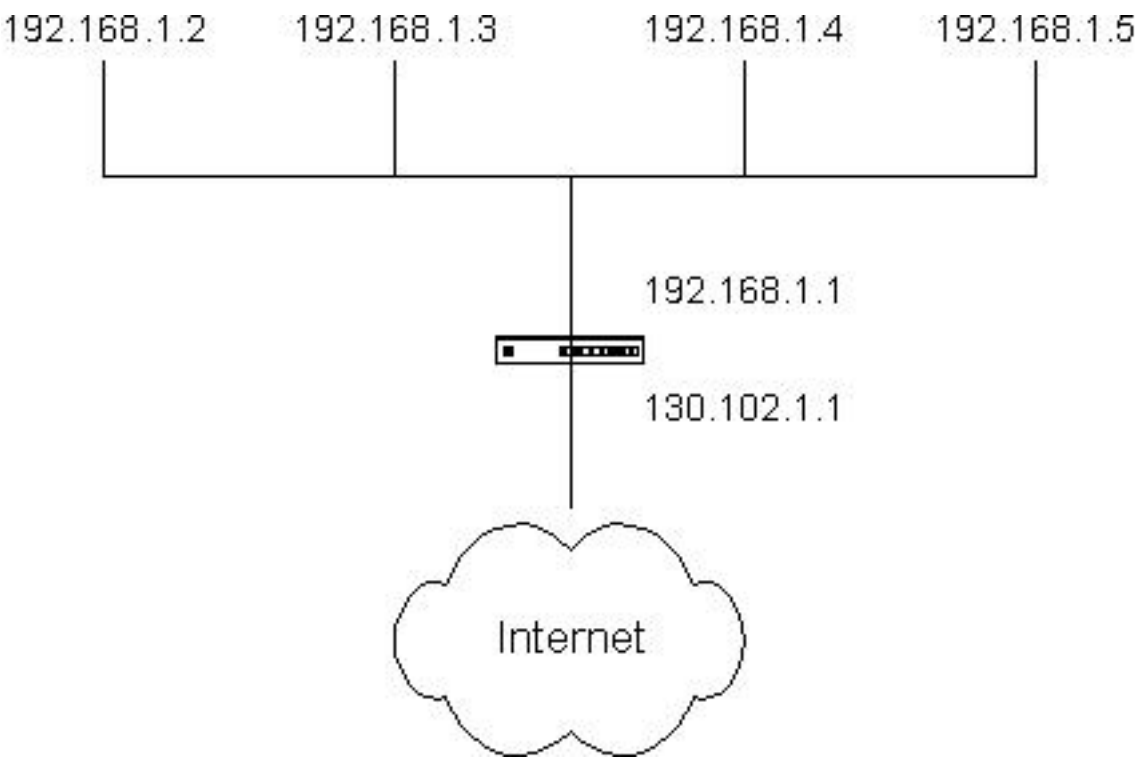
NAPT rozširuje jednokrokový preklad tiež o preklad transportných identifikátorov (TCP, UDP čísla portov, ICMP query identifikátory). Toto umožňuje transportným identifikátorom množstva privátnych hostov byť multiplexovaných do transportných identifikátorov jednej externej adresy. Pre odchádzajúce pakety z privátnej siete, NAPT prekladá zdrojové IP adresy, zdrojové transportné identifikátory a iné vzťahujúce sa položky ako IP, TCP, UDP a ICMP kontrolné súčty hlavičiek. Transportný identifikátor môže byť TCP/UDP port alebo ICMP query ID. Pre prichádzajúce pakety sa prekladá cieľová IP adresa, cieľový transportný identifikátor a IP a transportné kontrolné súčty hlavičiek. NAPT smerovač môže byť nakonfigurovaný aby prekladal sieť N-Pri do jednej vonkajšej adresy, povedzme Addr-i. Veľmi často sa ako táto adresa používa vonkajšia adresa interfejsu Addr-Nx NAPT smerovača.

2.6.4 Obojsmerná NAT

S obojsmernou NAT, spojenia môžu byť inicializované z hostov z vonkajšej siete rovnako dobre, ako z privátnej siete. Privátné sieťové adresy sú naviazané na jedinečné globálne adresy (staticky alebo dynamicky) ako spojenia vytvorené v každom smere. Pri obojsmernej NAT musí byť použitá technika DNS-ALG na správne mapovanie mien na adresy. DNS-ALG musí zabezpečovať preklad privátnych adries v DNS queries ako aj odpovediach do vonkajších adries a naopak počas putovania DNS paketov medzi privátnou a vonkajšou sieťou. Obojsmerný NAT smerovač povolí hostu A inicializovať spojenia na host X a hostu X povolí inicializovať spojenia na host A. Rovnako ako pri tradičnej NAT, sieť N-Ext je smerovateľná zo siete N-Pri, ale N-Pri nie je smerovateľná zo siete N-Ext.

2.6.5 Dvojitá (twice) NAT

Dvojitá NAT je varianta NAT, kedy zdrojová a súčasne aj cieľová adresa je modifikovaná NAT smerovačom v okamihu prenosu datagramu medzi sieťami. V prípade tradičnej



Obrázok 4: Network Address Port Translation (NAPT)

NAT ako aj obojsmernej NAT sa totiž prekladá vždy buď zdrojová alebo cieľová adresa. Dvojitá NAT je potrebná v prípade, že privátna a externá sieť majú adresné kolízie. Najčastejšie sa to stáva, keď má privátna sieť nesprávne očíslovaná svoje vnútorné uzly pomocou verejných adries, ktoré v skutočnosti patria inej organizácii. Problém nastáva, keď adresa hostu vo vonkajšej sieti je rovnaká ako adresa hostu v privátnej sieti. Ak nastane tento prípad, paket je forwardovaný do vnútorneho uzla namiesto toho, aby bol poslaný na NAT smerovač na vonkajšiu sieť. Dvojité NAT smerovače sa snažia riešiť tento problém prekladom zdrojovej aj cieľovej adresy IP paketu. Dvojitý NAT smerovač povolí hostu A inicializovať spojenie na host X, hostu X inicializovať spojenie na host A. Napriek tomu, N-Ext (alebo podsieť N-Ext) nebude smerovateľná z hostu N-Pri a sieť N-Pri nebude smerovateľná z N-Ext. Typické použitie dvojitej NAT je v prípade, keď privátna sieť používa adresný priestor 200.200.200.0/24, ktorý je oficiálne pridelený inej sieti na verejnom internete. Host A (200.200.200.1) v privátnej sieti sa rozhodne pripojiť na Host X (200.200.200.100) vo verejnej sieti. Na to, aby sme vytvorili správne spojenie, adresa hostu X namapujeme na inú adresu pre host A naopak.

2.6.6 Viacnásobna (multihomed) NAT

Existujú pár obmedzení v prípade použitia NAT. Napríklad, žiadosti ako aj odpovede v jednom spojení musia byť smerované cez rovnaký NAT smerovač, vzhľadom k tomu, že NAT smerovač má na starosti stavovú informáciu pre vytvorené spojenie. Všetky IP pakety odosielané ako aj prijaté z/do danej sieťovej domény idú cez jeden unikátny NAT smerovač, čo nie je bezpečné riešenie, nakoľko smerovač predstavuje jediný bod možného výpadku. Na to, aby sme zabezpečili pre privátne siete konektivitu s vonkajšími sieťami, v prípade, že jeden NAT smerovač vypadne, použijeme viacnásobne (multihomed) NAT smerovanie (cez viacero NAT smerovačov). Napríklad privátna sieť je pripojená cez dvoch

odlišných providerov a spojenia z privátnych hostov sú smerované na NAT smerovač s lepšou metrikou pre daný cieľ. V prípade, že jeden z NAT smerovačov vypadne, druhý dokáže smerovať traffic pre všetky spojenia. Viacnásobne NAT zariadenia so zdieľanou rovnakou NAT konfiguráciu môžu sami seba nahradzovať pri výpadku niektorého z nich.

2.7 NAT prevádzkové charakteristiky

NAT zariadenia sú aplikačne nezávisle, kedy je preklad limitovaný len na IP/TCP/UDP-ICMP hlavičky a ICMP chybové správy. NAT zariadenia nemenia transportnú časť prenášanú paketmi (špecifickú pre danú aplikáciu). NAT zariadenia (až na výnimku ALG techník) nepreverujú a nemodifikujú transportnú časť. Z tohto dôvodu NAT zariadenia sú vo väčšine prípadoch pre aplikácie transparentné. Existujú dve oblasti, kedy NAT zariadenia zapríčiňujú ťažkosti:

1. keď transportná prenášaná časť obsahuje IP adresu
2. keď je potrebné end-to-end zabezpečenie

Bezpečnostné techniky na aplikačnej úrovni, ktoré nezávisia od IP adries pracujú korektne aj pri NAT (napr. TLS, SSL a ssh). Naopak, bezpečnostné techniky na transportnej úrovni ako IPsec alebo TCP MD5 nepobežia. NAT zariadenia taktiež zapríčinujú ťažkosti pri distribúcii verejných kľúčov v protokoloch ako Secure DNS (RFC 2535 Ref 18) a X.509 certifikátoch s označenými verejnými klúčmi.
Za zmienku stojí, že IKE (Session key negotiaton protocol) založený na UDP nie je chránený bezpečnosťou siete IPsec. Tým pádom, IKE spojenia pobežia cez NAT, dovtedy, dokým prenášená dáta IKE nebudú obsahovať adresy alebo transportné identifikátory špecifické len pre jednu sieť a nie pre druhú.

2.7.1 Podpora FTP

Jeden z najpopulárnejších internetových protokolov FTP nepobeží s našim uvedeným popisom NAT. FTP ALG je spôsob, ako zabezpečiť bezproblémovy spôsob ftp prenosu a je podporovaný väčšinou NAT zariadení.
"PORT" command a "PASV" odpoveď v riadiacom ftp spojení identifikuje IP adresu a TCP port, ktorá musí byť použitá na spätné dátove spojenie. Argumenty PORT commandu a PASV odpoveď sú IP adresy a TCP port uvedené v ASCII. FTP ALG musí monitorovať a aktualizovať FTP riadiace spojenie, tak aby informácia obsiahnutá v prenášanej časti bola relevantná vzhľadom na koncové uzly. ALG musí tiež aktualizovať NAT s príslušnými parametrami dátového spojenia a jeho smeru, tak aby NAT mohol nastaviť stavovú informáciu pre FTP dátové spojenia. Pretože adresa TCP portu je kódovaná pomocou ASCII, môže to mať za následok zmenu veľkosti paketu. V prípade, že nová veľkosť paketu je rovnaká ako predošlá, stačí vypočítať len nový TCP kontrolný súčet. Ak nová veľkosť paketu je menšia alebo väčšia ako predošlá, musia byť zmenené TCP sekvenčné čísla (vzhľadom na zmenu dĺžky ftp riadiaceho spojenia). Na opravu TCP sekvenčných čísel a ACK čísel môže ALG používať špeciálnu tabuľku. Samozrejme, že opravy TCP sekvenčných a ACK čísel musia byť potom aplikovateľné na všetky ďalšie prichádzajúce pakety v spojení.

2.8 Obmedzenia NAT

2.8.1 Aplikácie s obsahom IP adries

Nie všetky aplikácie pobežie po preklade NAT zariadeniami. Špeciálne aplikácie, ktoré prenášajú IP adresu (a TCP/UDP port v prípade NAPT) vo vnorenom protokole. ALG (Application Level Gateways) by mali byť použité na preklad v prípade týchto aplikácií. ALG môžu dodatočné pozmeniť adresu (a port) označenia vytvoreného NAT a realizovať preklad špecifický pre danú aplikáciu. Kombinácia NAT a ALGs nezabezpečí end-to-end bezpečnosť zaisťovanú IPsecom. Napriek tomu, môžeme zapnúť tunelovací mód IPsec s NAT smerovačom ako cieľovým bodom tunelu. SNMP je jedna z tých aplikácií, obsahujúca vnorenú IP adresu. NAT smerovače neprekladajú IP adresy v SNMP paketoch. Je dosť nezvyčajné pre SNMP špecifikovať ALG, ktorý by zabezpečil SNMP MIB preklad správne pre danú privátnu sieť.

2.8.2 Aplikácie so spojenými nezávislými riadiacimi a dátovými spojeniami

NAT zariadenia pracujú v domnení, že každé spojenie je nezávislé. Charakteristiky spojenia, ako smer spojenia, zdrojová a cieľová IP adresa, protokol spojenia, zdrojové a cieľové transportné identifikátory sú determinované nezávisle na začiatku každého nového spojenia. Existujú ale aplikácie ako napríklad H.323, ktoré používajú jednu alebo viacero riadiacich spojení na nastavenie týchto charakteristík a podľa nich neskôr smerujú ďalší spôsob spojenia. Tieto aplikácie vyžadujú použitie aplikačne špecifických ALG, ktoré dokážu interpretovať a správne preložiť prenášanú časť, v prípade, že je to potrebné.

2.9 Zabezpečenie

Množstvu ľudí pripadá tradičný NAT smerovač ako jednosmerný traffic filter, blokujúci spojenia z vonkajších hostov na vnútorné počítače. V prípade, že priraďovanie adries v NAT smerovači je realizované dynamicky, je pre útočníka ťažšie detekovať špecifický host v rámci NAT domény. NAT smerovače môžu byť použité v kombinácii s firewallmi na odfiltrovanie nechceného trafficu. NAT zariadenia kombinované s ALG, môžu zaistiť, že datagramy posielané na Internet nebudú mať privátne adresy v hlavičkách alebo tele paketu. Aplikácie, ktoré nespĺňajú dané ALG by mali byť rušené použitím firewallovacích filtrov. NAT brány môžu byť použité ako koncové body tunelov na vytvorenie bezpečných VPN prenosov paketov cez vonkajšiu sieťovú doménu. Bezpečnostné riziká týkajúce sa NAT smerovačov:

1. UDP datagramy nie sú bezpečné, odpoveď na datagram môže prísť z adresy, ktorá je odlišná ako cieľová adresa použitá odosielateľom. Prichádzajúci UDP paket môže zapadnúť do outbound spojenia (inicializovaného zvnútra) (cieľová adresa a UDP port paketu sa zhoduje, ale zdrojová adresa a číslo portu sa nezhoduje). V tomto prípade, existuje potenciálny bezpečnostný kompromis pre NAT zariadenie, ktoré povolí prichádzajúce pakety s čiastočnou zhodou.

2. Multikastové spojenie (založené na UDP) môže byť zdrojom ďalšej bezpečnostnej slabiny pre tradičné NAT smerovače. Host v privátnej sieti inicializuje multikastové spojenie. Datagram poslaný z privátneho hostu môže zapnúť odpovede v reverznom smere od viacerých vonkajších hostov. Tradičná implementácia NAT,

ktorá používa jeden stav na záznam multikastového spojenia nemôže naisto determinovať, či prichádzajúci UDP paket je odpoveď na existujúceho multikastového spojenie alebo začiatok nového UDP spojenia inicializovaného útočníkom.

3. NAT zariadenia môžu byť cieľom pre útoky NAT zariadenia sú hosty na Internete, ktoré môžu byť cieľom viacerých odlišných útokov, ako SYN flood, ping flood útoky. Na NAT zariadenia by sa mali aplikovať rovnaké bezpečnostné ochrany ako na iné servery umiestnené na Internete.

3 Implementácia NAT

Budeme sa zaoberať implementáciou NAT v linuxovom kerneli 2.4.x, ktorá zahrňuje väčšinu zašpecifikovaných vlastností NATu.

3.1 Prečo použiť NAT?

Podrobnejšie si rozoberieme otázky položené v úvode.

- Modemové spojenia na Internet
  Väčšina ISP (Internet service providers) nám pridelí po dovolaní k nim len jednu IP adresu. Môžeme poslať von pakety s ľubovoľnou zdrojovou adresou, odpoveď dostaneme ale len na pakety, ktoré majú ako zdrojovú adresu túto pridelenú IP adresu. Ak chceme použiť viacero odlišných počítačov na pripojenie k Internetu cez jednu prípojku, musíme použiť NAT. Ide o SNAT (source NAT), nakoľko meníme len zdrojové adresy odosielaných paketov.

- Prístup k viacerým serverom
  Niekedy si želáme zmeniť smerovanie paketov v prípade, že prídu do našej siete. Stáva sa to často v prípade, že máme len jednu IP adresu, ale chceme umožniť vonkajší prístup k počítačom umiestnenými za touto jednou "reálnou" IP adresou. Dosiahneme to prepísaním cieľovej adresy prichádzajúcich paketov. Jeden z prípadov je "load-sharing" rovnomerné zaťažovanie, kedy ako cieľovu adresu mapujeme jednu z možných vnútorných IP. Tento typ NAT sa nazýval tiež port-forwarding v predošlých verziách Linuxu.

- Transparentné proxy
  Niekedy potrebujeme zaistiť, aby každý paket, ktorý prejde linuxovým smerovačom bol určený pre ďalšie programové spracovanie (squid). Toto je použité pri vytvárení transparentných proxy, proxy je program, ktorý zabezpečuje web komunikáciu medzi vnútornou a vonkajšou sieťou. Transparentné to nazývame preto, lebo naša sieť netuší, že komunikuje s proxy, samozrejme pokým proxy nevypadne.

3.2 2 typy NAT

- Source NAT
  V tomto prípade modifikujeme zdrojovú adresu prvého paketu (zmeníme smer odkiaľ prichádza spojenie). Source NAT sa vykonáva vždy po smerovaní (post-routing) predtým ako samotný paket odošleme. Maškaráda (Masquerading) je špeciálny prípad SNAT.

- Destination NAT
  V tomto prípade modifikujeme cieľovú adresu prvého paketu (zmeníme smer cieľového spojenia). Destination NAT sa vykonáva vždy pred smerovaním (pre-routing) v okamihu ako prijmeme paket. Port forwarding, load sharing a transparentné proxy sú prípady DNAT.

3.3 Implementácia jednoduchej PPP maškarády

Ak máme dynamicky alokovanú IP PPP pripojením, chceme aby náš linux zariadil, aby všetky pakety prichádzajúce z našej vnútornej siete vyzerali ako keby prichádzali z IP PPP pripojenia, rovnako chceme, aby na pripojenia s našej vnútornej siete aj správne odpovedal, teda po prijatí odpoveďe na PPP host poslal paket vnútornému hostu.

```
# -A pripojíme pravidlo do NAT tabuľky (-t NAT) po smerovaní (POSTROUTING)
# pre všetky pakety smerované na ppp0 (-o ppp0) a nastavíme maškarádovanie
# -j MASQUERADE
iptables -A POSTROUTING -t nat -o ppp0 -j MASQUERADE

# zapneme IP forwardovanie
echo 1 >/proc/sys/net/ipv4/ip_forward
```

3.4 Port forwarding

Linux 2.2 :

```
# forwarduje TCP pakety posielané na port 8080 na 1.2.3.4
# na adresu 192.168.1.1 port 80
ipmasqadm portfw -a -P tcp -L 1.2.3.4 8080 -R 192.168.1.1 80
```

Linux 2.4 :

```
iptables -A PREROUTING -t nat -p tcp -d 1.2.3.4 --dport 8080 -j DNAT \
         --to 192.168.1.1:80
```

Ak chceme, aby sa uvedené pravidlo vzťahovalo aj na lokálne spojenia (na samotnom NAT boxe, pri pokuse telnetu na 1.2.3.4 port 8080 sa dostaneme na 192.168.1.1 port 80), môžeme rovnaké pravidlo vložiť do OUTPUT reťaze (čo je pre lokálne poslané pakety).

```
# Linux 2.4
iptables -A OUTPUT -t nat -p tcp -d 1.2.3.4 --dport 8080 -j DNAT \
         --to 192.168.1.1:80
```

3.5 Riadenie NAT

Vytvoríme si NAT pravidlá, ktoré povedia kernelu, ktoré spojenia má pozmeniť a akým spôsobom to má urobiť. Na to aby sme to realizovali, použijeme veľmi univerzálny prostriedok **iptables**, ktorému žiadosť o zmenu NAT tabuľky povieme špecifikovaním prepínača '-t'.
Tabuľka NAT pravidiel obsahuje 3 zoznamy nazývane "reťaze" (chains). Tieto tri reťaze sa nazývaju PREROUTING (pre DNAT, v okamihu, keď prídu pakety), POSTROUTING (pre SNAT, v okamihu, keď pakety odchádzajú) a OUTPUT (pre DNAT a lokálne

generované pakety). V prípade nového spojenia, pozrieme sa do korešpondujúcej "reťaze" v NAT tabuľke na to, aby sme zistili, čo máme ďalej robiť. Túto odpoveď potom aplikujeme na všetky ďalšie budúce pakety v tomto spojení.

3.5.1 Prepínače iptables

Jeden z najdôležitejších prepínačov je '-t'. Pre všetky NAT operácie s NAT tabuľkou musíme použiť '-t nat'. Druhý najdôležitejší prepínač je '-A', ktorý pripojí nové pravidlo na koniec reťaze (napr. '-A POSTROUTING'), alebo '-I' prepínač, ktorý pravidlo vloží na začiatok. Môžeme špecifikovať zdroj ('-s') alebo cieľ ('-d') paketov, na ktoré chceme aplikovať NAT. Zdroj alebo cieľ je uvádzaný buď ako jednoduchá IP adresa (192.168.1.1), meno hostu (hq.alert.sk) alebo adresa siete (192.168.1.0/24 alebo 192.168.1.0/255.255.255.0). Môžeme špecifikovať prichádzajúci (incoming) '-i' alebo odchádzajúci (outgoing) '-o' interfejs, ktorý sa musí zhodovať pre NAT. Pravidlo patriace do reťaze PREROUTING môžeme aplikovať len na prichádzajúci interfejs, do reťaze POSTROUTING len na odchádzajúci interfejs. V prípade, že vynecháme prepínač na zdrojovú adresu, tak pravidlu bude vyhovovať ľubovoľná zdrojová adresa, ak vynecháme prepínač na cieľovu adresu, tak pravidlu bude vyhovavať ľubovoľná cieľová adresa. Použitý protokol môžeme špecifikovať prepínačom '-p', napr.TCP alebo UDP, kedy sa budú brať do úvahy len pakety so zvoleným protokolom. Po zašpecifikovaný protokolu TCP alebo UDP, môžeme použiť tiež na prepínač '-sport' alebo '–dport' na prípadnú zhodu zdrojového, alebo cieľového portu. (užitočné pre redirektovanie web requestov, TCP port 80).

3.6 Ako modifikovať pakety

Chceme vedieť, akým spôsobom vybrať pakety, ktoré chceme modifikovať (preklad IP hlavičky).

3.6.1 Zdrojové NAT

Ide nám o Source NAT, zmenu zdrojovej adresy spojenia na nejakú inú. Realizujeme to v POSTROUTING reťazi, tesne predtým, ako samotný paket vyšleme. Je to dôležité si uvedomiť, nakoľko všetko ostatné bežiace na linuxe (smerovanie, paket filtering) nám paket už nezmenia. Tiež to znamená, že v tomto prípade môžeme použiť '-o' outgoing interfejs. Source NAT je špecifikovaný použitím '-j SNAT' a prepínačom '–to-source' obsahujúcim IP adresu, resp. rozsah IP adries, prípadne port, rozsah portov (len pre UDP, TCP protokoly).

```
# Zmeníme zdrojové adresy na 1.2.3.4
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

# Zmeníme zdrojové adresy na 1.2.3.4, 1.2.3.5 a 1.2.3.6
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4-1.2.3.6

# Zmeníme zdrojové adresy na 1.2.3.4 porty 1-1023
iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4:1-1023
```

3.6.2 Maškaráda

Ide o špeciálny prípad Source NAT. Maškaráda by mala byť použitá len pre dynamicky prideľovaných IP adresách ako sú štandartné dialupy (pre statické IP adresy sa odporúča použiť hore uvedený SNAT). V prípade maškarády nemusíme explicitne uvádzať novú zdrojovú adresu, použije sa zdrojová adresa interfejsu, z ktorého paket príde.

```
# Maškaráduj všetko odchádzajúce z ppp0
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

3.6.3 Cieľové NAT

Realizujeme v PREROUTING reťazi, v okamihu, keď príde paket. Znamená to, že všetko ostatné bežiace na linuxe (smerovanie, paket filtering) sa aplikuje na paket s "novým" reálnym cieľom. Tiež to znamená, že v tomto prípade môžeme použiť '-i' incoming interfejs. Na zmenu cieľa lokálne generovaných paketov musíme použiť reťaz OUTPUT (čo nie je obvyklý prípad). Destination NAT je špecifikovaný použitím '-j DNAT' a prepínačom '–to-destination' obsahujúcim IP adresu, resp. rozsah IP adries, pripadne port, rozsah portov (len pre UDP a TCP protokoly).

```
# Zmeníme cieľové adresy na 5.6.7.8
iptables -t nat -A PREROUTING -i eth1 -j DNAT --to 5.6.7.8

# Zmeníme cieľové adresy na 5.6.7.8, 5.6.7.9 a 5.6.7.10
iptables -t nat -A PREROUTING -i eth1 -j DNAT --to 5.6.7.8-5.6.7.10

# Zmeníme cieľové adresy web trafficu na 5.6.7.8 port 8080
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth1 -j DNAT \
        --to 5.6.7.8:8080

# presmerujeme lokálne pakety na 1.2.3.4 na loopback
iptables -t nat -A OUTPUT -d 1.2.3.4 -j DNAT --to 127.0.0.1
```

3.6.4 Transparentné proxy

Ide o špeciálny prípad DNAT nazývaného transparentné proxy.

```
# Pošle prichádzajúci web traffic nášmu squid (transparentnému) proxy
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT \
         --to-port 3128
```