Prevođenje mrežnih adresa

Potreba

Usled pojave sve većeg broja računara na Internetu dolazi do problema manjka slobodnih IP adresa. Dugoročno rešenje može da predstavlja IPv6 sa 128-bitnim adresama, međutim za ovakvo rešenje su potrebne godine. Brzo rešenje se pojavilo u obliku sistema za **prevođenje mrežnih adresa** (*Network Address Translation, NAT*).

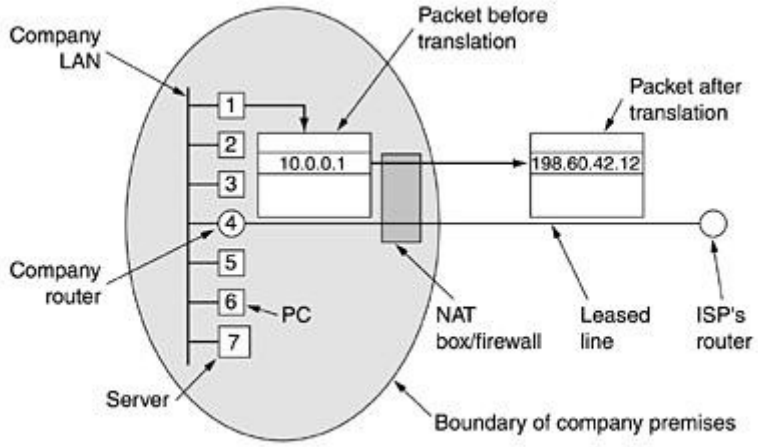
Ideja

Sistem NAT dodeljuje svakoj kompaniji (manjoj mreži) samo jednu IP adresu za saobraćaj na Internetu. Unutar te mreže, svaki računar dobija jedinstvenu IP adresu koja služi za interni saobraćaj. Kada paket napušta kompaniju i odlazi ka davaocu Internet usluga, njegova adresa se prevodi. Ovakav sistem može da radi zahvaljujući IP adresama rezervisanim za privatne potrebe. Tri rezervisana opsega su:

10.0.0.0 - 10.255.255.255/8(16.777.216 računara)
172.16.0.0 - 172.31.255.255/12 (1.048.567 računara)
192.168.0.0 - 192.168.255.255/16 (65.536 računara)

Rad

Unutar kompanije, svaki računar ima jedinstvenu adresu oblika 10.*x.y.z.* NAT sistem pretpostavlja da se komunikacija odvija preko TCP ili UDP protokola. Zaglavlja okvira ovih protokola sadrže **izvorišni** (*source port*) i **odredišni** (*destination port*) priključak. Ti priključci su 16-bitni celi brojevi koji ukazuju gde veza počinje, a gde se završava. Kada paket napušta kompaniju on prolazi kroz **NAT kutiju** (*NAT box*), koja internu IP adresu izvorišta (na slici 10.0.0.1) pretvara u pravu IP adresu kompanije (na slici 192.60.42.12). Tada se *Izvorišna adresa* zamenjuje sa ineksom u tabeli za prevođenje sa 65.356 odrednica u NAT kutiji. Ta odrednica sadrži originalnu IP adresu i originalni priključak izvorišta



Slika 1: Postavljanje i rad NAT kutije

Kada stigne odgovor (npr sa Web servera), on je adresiran na adresu kompanije(na slici 192.60.42.12). Tad se vadi *Izvorišni priključak* iz zaglavlja okvira i koristi kao indeks u tabeli za prevđenje NAT kutije. Iz pronađene odrednice čitaju se interna IP adresa i originalni *Izvorišni priključak* zaglavlja, i umeću se u paket. Paket se potom prosleđuje usmerivaču radi uobičajne isporuke.

Mane

Iako opisani sistem na izvestan način rešava problem malog broja IP adresa, on ima svoje nedostatke.

Prvo, NAT narušava arhitekturu IP modela u kome svaka IP adresa jedinstveno identifikuje samo jedan računar na čitavom svetu. Softverska struktura Interneta u celini je izgrađena na toj pretpostavci. Sa NAT sistemom hiljade računara može da koristi istu adresu.

Drugo, NAT pretvara Internet u mrežu sa izvesnim uspostavljanjem direktne veze. NAT kutija održava informacije za svaku vezu koja prolazi kroz nju. Kada mreža održava informacije o stanju veze, tada ona liči na mrežu sa uspostavljanjem direktne veze (iako to nije).

Treće, NAT narašava osnovno pravilo raspoređivanja protokola po slojevima. Sloj *k* ne sme da pravi nikakve pretpostavke o tome šta je sloj *k+1* smestio u polje za korisničke podatke. Takva ideja protokola svodi se na obezbeđivanje nezavisnosti između slojeva. NAT tu nezavisnost ruši.

Četvrto, od procesa na Internetu se ne zahteva da koriste TCP ili UDP protokole. U slučaju nekog drugog protokola NAT kutija će osujetiti aplikaciju jer neće biti u stanju da ispravno locira *izvorišni priključak*.

Peto, neke aplikacije umeću IP adrese u sam tekst. NAT ništa ne zna o tim adresama, te ih ne može zameniti. Tada će propasti pokušaji da se one iskoriste na udaljenom kraju veze.

Šesto, pošto TCP polje *Izvorišni priključak* ima 16 bitova, najviše 61.440 (jer se prvih 4096 priključaka čuva za posebne namene) računara može biti preslikano u jednu IP adresu. Međutim, da je na raspolaganju više IP adresa, svaka bi zadovoljila 61.440 računara.

Protokoli za upravljanje porukama na Internetu

Rad Interneta nadziru usmerivači. Kada se dogodi nešto neočekivano, o događaju se izveštava **protokol za upravljanje porukama na Internetu** (*Internet Control Message Protocol, ICMP*). Definisano je više od deset vrsta ICMP poruka. ICMP poruka bilo koje vrste kapsulira se u IP paket.

Vrsta poruke	**Opis**
Destination unreachable (Odresšte nedostupno)	Paket se ne može isporučiti
Time exceeded (Isteklo vreme)	Vrednost polja *životni vek* dostigla je nulu
Parametar problem (Greška u parametrima)	Neispravno polje u zaglvlju
Source quench (Prigušavanje izvorišta)	Prigušni paket
Redirect (Preusmeravanje)	Poučavanje usmerivača o topologiji
Echo (Eho)	Proveravanje aktivnosti računara
Echo reply (Odgovor na eho)	Potvrda aktivnosti računara
Timestamp request (Zahtev s vremenskom oznakom)	Isto kao Eho, s vremenskom oznakom
Timestamp reply (Odgovor na ahtev s vremenskom oznakom)	Isto kao Odgovor na eho, s vremenskom oznkom

Tabela 1: Osnovne vrste ICMP protokola

Poruka ODREDIŠTE NEDOSTUPNO koristi se kada podmreža ili usmerivač ne mogu da lociraju odredište ili kada paket s postavljenim bitom NF ne može da se isporuči jer mu je na putu mreža oja ograničava veličinu paketa.

Poruka VREME ISTEKLO šalje se kada se paket odbaci jer mu je životni vek istekao. Ovaj događaj ukazuje na to da paketi kruže u petlji , da postoji izuzetno zagušenje ili da je rok tajmera suviše kratak.

Poruka GREŠKA U PARAMETRIMA ukazuje na to da je u nekom polju zaglavlja otkrivena nedozvoljena vrednost. Poruka signalizira na grešku u IP softveru pošiljaoca ili možda na greške u softveru usputnih usmerivača.

Poruka PRIGUŠENJE IZVORIŠTA prvobitno je korišćena za opominjanje računara koji prebrzo šalju poruke. Danas se retko koristi. Upravljanje zagušenjem na Internetu danas se uglavnom obavlja u transportnom sloju.

Poruku PREUSMERAVANJE šalje usmerivač koji smatra da je paket pogrešno usmeren. On time pošiljaoca obaveštava o problemu.

Poruke EHO i ODGOVOR NA EHO koriste se pri utvrđivanju da li je određeno odredište dostupno i aktivno. Kada primi poruku EHO, odredište treba da vrati poruku ODGOVOR NA EHO. Slične su i poruke ZAHTEV S VREENSKOM OZNAKOM i ODGOVOR NA ZAHTEV S VREENSKOM OZNAKOM, s tim što se u odgovoru beleže vremena stizanja zahteva i slanja odgovora.

ARP - Protokol za razrešavanje adresa

Iako svaki računar na Internetu ima jedinstvenu IP adresu , one se u stvari ne mogu koristi za slanje paketa jer hardver sloja veze ne razume Internet adrese. Danas su računari u većini kompanija i univerziteta povezani u lokalne mreže preko mrežne kartice koje razumeju samo lokalne adrese.

Postavlja se pitanje kao se IP adrese preslikavaju u adrese sloja veze podataka? Jedno od rešenja je **protokol za razrešavanje adresa** (*Address Resolution Protocol, ARP*). Izvršava ga skoro svaki računar na Internetu. Prednost protokola ARP nad konfiguracijskim datotekma jeste jednostavnost njegovog korišćenja. Administrator sistema treba samo da svakom računaru dodeli IP adresu i da odluči o maskama podmreže. Sve ostalo radi ARP.

Računar *R1* difuzno emituje paket na Ethernet mreži pitajući: Ko ima adresu, npr 192.31.65.0? Pitanje će stići do svakog korisnika na toj mreži, pri čemu će samo jedan računar *R2* da ogovori sa svojom Ethernet adresom (*E*). Na taj način računar *R1* saznaje da IP adresa 192.31.65.0 pripada računaru sa Ethernet adresom *E*. Tada IP softver na računaru *R1* pravi Ethernet okvir adresiran na *E*, smešta IP paket u polje za podatke, i šalje ga na Ethernet. Ethernet kartica računara *R2* otkriva ovaj okvir, preuzima ga i izaziva prekid.