15_LAŽIRANJE IP ADRESA

IP adresa je jedinstvena brojevna oznaka računara na mreži. IP adresa je u osnovi binarni broj, koji je u slučaju trenutno važeće verzije IP protokola, IPv4, binarni broj 32 bita dug. Često se radi lakšeg pamćenja IP adrese zapisuju u dekadskoj notaciji, gde se 32-bitni broj podeli na četiri 8-bitna broja, koji se zatim prikazuju kao četiri decimalna broja odvojena tačkom. Svaki od tih brojeva je u rasponu 0-255, što je upravo raspon brojeva koje je moguće prikazati u jednom 8-bitnom binarnom prikazu. IPv6 verzija protokola predviđa 128-bitne adrese, pa se u tom slučaju može koristiti i heksadecimalni zapis, radi kraćeg oblika i jednostavnosti. Primjer IP adrese je 172.16.254.1.

Svaki računar koji je povezan na mrežu mora imati jednoznačno dodeljenu IP adresu. Ove adrese su nužne da bi se paketi upućeni sa izvora mogli preusmeriti do odredišta. Taj postupak preusmeravanja vrše računari specifične namene koje nazivamo *gateway*. Trenutni standard za IP adresiranje na Internetu je IPv4.

Kako je nužno da IP adrese budu jednoznačno određene, postoje međunarodne organizacije koje se brinu o raspodeli IP adresnog prostora. Takva je organizacija The Internet Assigned Numbers Authority (IANA). IANA zatim za određen raspon adresa delegira regionalne Internet registre, pa je za područje Evrope zadužen RIPE Network Coordination Centre. Ono što bi se moglo da se nazove IPv5 je postojalo samo kao eksperimentalni ne-IP protokol u realnom vremenu (nazvan ST2 i opisan u RFC 1819). Ovaj protokol je napušten u korist RSVPa.

IP adrese se dele na javne i privatne. Javne IP adrese su jedinstvene, globalne i standardizovane. Razvojem Interneta počinje da nedostaje sve više i više slobodnih IP adresa. Rešenje tog problema su bile privatne IP adrese. Privatne adrese mogu biti višestruke, uz uslov da se ne nalaze u istoj lokalnoj mreži. Prilikom izlaska korisnika iz lokalne mreže na Internet, privatna adresa IP adresa se pretvara u javnu IP adresu pomoću metoda NAT (Network Address Translation) i PAT (Port Address Translation).

U IPv6, novom (ali ne još uvek široko korišćenom) standardnom internet protokolu su adrese duge 128 bita i to bi, čak i sa velikim dodelama netblokova, trebalo da zadovolji blisku budućnost. Teoretski, postojalo bi tačno 2128, ili 3.403×1038 unikatnih adresa. (Kada bi zemlja bila sačinjena kompletno od zrna pijeska od 1cm³, onda bi se mogla dodeliti jedinstvena adresa svakom zrnu u 300 miliona planeta veličine zemlje.) Veliki prostor za adrese će biti retko popunjen, što omogućava ponovno kodiranje više informacija. Globalne adrese koje se šalju ka jednom odredištu sastoje se iz dva dela: 64-bitni dio za rutiranje i 64-bitni identifikator domaćina. Netblokovi se određuju kao moderne alternative IPv4: broj mreže, koga prati kosa crta i broj značajnih bitova (u decimalnom zapisu). Primjer je 12AB::CD30:0:0:0:0/60 uključuje sve adrese koje počinju s 12AB00000000CD3. IPv6 ima dosta poboljšanja u odnosu na IPv4, pored samo većeg prostora za adrese, uključujući i samostalno ponovno odbrojavanje i obveznu upotrebu IPsec-a.

Nečiju IP adresu (jedinstveni broj) moguće je saznati na više načina. Šta se dobija ako se zna nečiji IP? Sa nečijom IP adresom moguće je saznati iz kojeg se grada/države, i preko kojeg se internet provajdera klijent spaja na internet. Ovo nije dovoljno informacija da se sazna I kućna adresa klienta, ali ipak ako je neko uporan u nameri da vas maltretira na internet, moguće je e-mailom kontaktirati službu njegovog internet providera koju može da se sazna tako što se uradi pretraga po IP adresi napadača.

Lažiranje IP adresa (čest je engleski izraz *IP spoofing*) je pojam vezan za računarske mreže, odnosno to je naziv za tehniku kojom se IP paketima menja adresa izvora.

Uz pretpostavku da postoji uređaj s IP adresom koja se lažira, odgovor na pakete kojima je postavljena lažna adresa izvora neće nikad doći do računara s koga su poslani, već će doći do računara čija se IP adresa lažira. Zato je najčešća svrha lažiranja IP adresa tzv. *Denial of service* (*dDoS*) napad, čiji je cilj da se zaguši računar čija se adresa lažira, tj. Da se onemogući usluga ili u krajnjem slučaju da se izbaci iz operativnog stanja. Odbrana od ovakvih napada je otežana, jer paketi dolaze s raznih adresa (sa svih onih kojima su poslani početni paketi sa lažiranom IP adresom izvora), i njihovo trajno filtriranje nema smisla.