

Mrežni protokol IPv6

- **IP** - nespojna usluga izvedena datagramski (komutacija paketa)
- Svaki datagram se usmjerava odvojeno - sadrži potpune informacije o izvoru i odredistu
- **Moguci problemi:** - gubitci paketa (zbog pogreske ili zagusenja), pogresan redosljed dostave paketa, vece kasnjenje u slucaju retransmisije s kraja na kraj mreze, nema povratne info
- **Funkcionalnosti IP-a:**
 - **Definira shemu adresiranja** - jedinstveni adresni prostor, svako mrežno sučelje po 1 IP, routing, broadcast/multicast/loopback
 - **Fragmentacija** - datagram mora stati u ethernet okvir, sastavlja se na odredistu
- **Ipv4 - 32bit adresa:**
 - **A klasa** - [0][7bit NetID][24bit HostID]
 - **B klasa** - [10][14bit NetID][16bit HostID]
 - **C klasa** - [110][21bit NetID][8bit HostID]
 - **D klasa** - [1110][28bit HostID] - **multicast**
 - **E klasa** - [1111][28bit HostID] - **rezervirano**
- **Loopback** - 127.0.0.0/8
- **Broadcast** - 255.255.255.255
- **NetID** - prva adresa u rasponu 10.0.0.0/8
- **Prefiksni prikaz** - oznacava duljinu mreznog dijela - 10.0.0.0/8 => 8 bitova NetID-a
- **CIDR - classless inter-domain routing** - routing baziran na varijabilnoj maski, a ne klasama
- **Format IP datagrama:**
 - **Version** - verzija internet protokola (Ipv4)
 - **IHL** - duljina zaglavlja, broj 32-bitnih rijeci (od 5 do 15)
 - **duljina** - broj okteta u paketu, ukljucujuci zaglavlje
 - **identifikacija** - jedinstveni broj datagrama, isti za sve fragmente
 - **zastavice** - 3 bita za oznake kod fragmentiranja
 - **mjesto fragmenta (offset)** - oznaka za izracunavanje mjesta u datagramu
 - **TTL** - najveći broj skokova kroz routere (kada dodje do 0, paket se odbaci)
 - **protokol** - oznaka protokola u payloadu (TCP, UDP, ...)
 - **checksum zaglavlja** - zastitna suma za otkrivanje gresaka u zaglavlju
 - **source i destination IP**
 - **opcije** - posebne mogucnosti
 - **punjenje** - nule za 32-bit align

- **Fragmentacija** - rade je routeri, sastavlja se na odredistu - nepoželjna jer gubitak fragmenta zahtjeva retransmisiju cijelog datagrama, prenosi se više kontrolnih informacija (zaglavlja) za istu količinu korisnih
- **Routing postupak:** dodje paket -> provjeri se checksum (ako ne valja discarda se paket, salje se ICMP poruka) -> smanji se TTL, ako je 0 provjeri se je li mreza direktno spojena, ako nije odbacuje se, ako jest dostavlja se -> ako nije onda se gledaju prvo specificne pa defaultna ruta -> ako ne postoji ni jedno, odbacuje se i salje se ICMP poruka
- **ICMP** - definira dvije vrste kontrolnih poruka: poruke o greskama i zahtjeve za informacijama
- **IPv6** - nadogradnja na IPv4. Ograničenja IPv4: **broj raspoloživih adresa, prevelike routing tablice, problemi upravljanja mrežom, nedovoljni sigurnosni mehanizmi, nedovoljni mehanizmi pokretljivosti, nedovoljna podrška za prijenos u stvarnom vremenu (QoS)**
 - 128-bitno adresiranje
 - Pojednostavljen format zaglavlja (manje polja, fiksna duljina)
 - Unaprijeđen routing
 - Mogućnost označavanja tokova
 - Podrška za QoS
 - Provjera autentičnosti, integriteta i privatnost
 - Podrška za pokretljivost
- **Zaglavlje:**
 - **Verzija** - verzija IP protokola (IPv6)
 - **Prometna klasa (class)** - određuje rukovanje paketom ovisno o zagusenju
 - promet upravljan zagusenjem - izvoriste provodi kontrolu zagusenje i daje prioritet upravljackom prometu, pa interaktivnom, pa prometu koji prenosi veliku količinu podataka.
 - promet neupravljan zagusenjem - koristi se za real-time promet (video, audio, etc)
 - **Oznaka toka (flow label)** - određuje sve pakete koji pripadaju istom toku (idu od istog izvorista, istom odredistu i istoj aplikaciji), a zahtjevaju posebno rukovanje na usmjeriteljima
- **Dodatna zaglavlja** - dolaze nakon osnovnog
 - **Hop-by-hop header** - informacija namjenjena svakom cvoru na putu, sadrži informaciju o akciji koju svaki cvor poduzima (prijenos vrlo velikih paketa, ne fragmentati i sl.)
 - **Destination header (1,2)** - informacija namjenjena prvom sljedećem cvoru i svima u *Routing header (1)* ili samo za krajnje odrediste (2) - primjer: Mobile IPv6

- **Routing header** - sadrzi popis usmjeritelja kojima datagram mora proci na putu do odredista, primjer: Mobile IPv6, odabir ISP-a
- **Fragment header** - zaglavlje koje opisuje fragmente u slucaju fragmentiranja, **fragmentira se samo na izvoristu** (za razliku od IPv4). Ukoliko dodje do potrebe za daljnjim fragmentiranjem, odbacuje se paket i salje ICMP poruka
- **Authentication header (AH)** - jamci autenticnost izvora IP datagrama i da datagram nije mijenjan
- **Encapsulating security payload header (ESP)** - jamci povjerljivost i integritet
 - transporni nacin - zastita samo TCP/UDP paketa
 - tunelski nacin - zastita cijelog datagrama
- **IPv6 adrese su 128 bitne** - zapisuju se kao 16bitne adrese odvojene dvotočkama
 - niz nula se moze zamijeniti s :: - **samo jednom**
 - **stare adrese ce se pretvarati dodavanjem nula, pa je zapis ::10.1.1.1 moguc**
 - moguca prefiksna notacija kao i kod IPv4
- **Vrste IPv6 adresa:**
 - **Unicast** - jednodredisna, identificira jedno sucelje, globalne i lokalne
 - Globalne - koriste se na javnom Internetu
 - Lokalne na razini organizacije (site-local)
 - Lokalne na razini poveznice (link-local) - izvode se iz MAC-a
 - Posebne
 - **Multicast** - odredjuje skup sucelja, dostavlja se svima
 - **Anycast** - isto kao multicast samo se dostavlja najblizem sucelju
- **Globalne unicast adrese:**
 - [001][TLA ID 13bit][RES 8bit][NLA ID 24bit][SLA ID 16bit][Interface ID 64bit]
 - 001 - format prefiks
 - TLA ID - identifikator davatelja usluge najvise razine (Tier 1)
 - Res - rezervirano za buduće potrebe
 - NLA ID - Tier 2 identifikator
 - SLA ID - Tier 3 identifikator
 - Interface ID - identifikator sucelja u IEEE EUI-64 standardu
- **Lokalne unicast adrese**
 - **FE80::/64**

- automatski se konfiguriraju i koriste za komunikaciju u subnetu
 - ne prosljedjuje ih usmeritelj
 - potrebne za autokonfiguraciju i otkrivanje susjeda (NDP)
- **FC00::/48**
 - analogne privatnim adresama (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
 - ne konfiguriraju se automatski
- **Multicast adrese** - paketi poslani na tu adresu dostavljaju se svima u toj grupi
 - **[1111 1111][F 4bit][S 4bit][Group ID 112bit]**
 - **F (flag)** - definirana samo T zastavica koja koristi krajnji desni bit
 - 0001 - privremeno dodjeljena adresa
 - 0000 - trajno dodjeljena adresa
 - **S (scope)** - naznacuje doseg adrese
 - 0001 - node local
 - 0010 - link local
 - 0101 - site local
 - 1000 - organization local
 - 1110 - global
 - **Group ID** - jedinstvena adresa grupe unutar dosega
- **Anycast adresa** - dodijeljuje se vecem broju sucelja, paketi se prosljedjuju do najblizeg (metrikom)
 - iste kao Unicast adrese
 - Posebna jedino **Subnet-router** adresa koja se dodjeljuje routerima. Zapravo je oznaka mreze.
- **Posebne adrese:**
 - **nespecificirane adrese** - npr ::, koristi se kao i 0.0.0.0 kod IPv4
 - **Loopback adresa** - ::1 - isto kao i 127.0.0.1
 - **IPv4 kompatibilne** - ::10.1.1.1
 - **IPv4 preslikane** - ::ffff:10.1.1.1 - ne koriste se kao izvoriste ili odrediste
 - **6to4 adrese** - 2002::/16 - za tuneliranje IPv6 prometa kroz IPv4 mrezu
- **Kontrolni protokoli:**
 - **ICMPv6** - služi da dojavu pogresaka i dijagnostiku
 - nije kompatibilan s ICMPv4
 - sadrzi podrsku za multicasting
 - poruke o pogreskama, ping, pripadnost grupi, podrška za NDP
 - **NDP (Neighbour discovery protocol)** - zamjenjuje ARP i proširuje funkcionalnost, sastavni dio ICMPv6

- Otkrivanje routera, prefiksa, parametara (MTU i sl.), autokonfiguracija adrese
- zamjenjuje ARP, otkrivanje sljedećeg skoka, provjera dostupnosti, provjera dvostruke adrese
- **redirect funkcija** - usmjeritelj informira računalo o boljem putu
- **MLD (Multicast listener directory)** - zamjenjuje IGMP i proširuje, ICMPv6
- **DHCPv6** - dinamičke IPv6 adrese i druge konfiguracijske informacije
 - zasniva se na: **lokalnoj adresi (link-local)** koja se **autokonfigurira i viseodređeno adresira** DHCPv6 servera i relayeva
 - **Poruke:**
 - DHCP Solicit - multicast poruka kojom se traži server ili relay
 - DHCP Advertise - oglašava se poslužitelj
 - DHCP Request - odabire se poslužitelj i zahtjevaju parametri
 - DHCP Replay - dostavljaju se parametri
 - DHCP Release - otpustavljaju parametara
 - DHCP Reconfigure - rekonfiguracija nekih parametara.

Pokretljivost u IP mreži / Uvodjenje IPv6-a

- Kod klasičnog IPv4 interneta IP adresa globalno i jednoznačno određuje računalo. U slučaju promjene točke priključka u drugi subnet potrebno je promijeniti IP adresu.
- **Zahtjevi za pokretljivost u Internetu su:**
 - pokretan čvor mora moći komunicirati s drugima nakon promjene točke priključka
 - mora moći komunicirati sa svojom stalnom IP adresom, bez obzira na točku priključka
 - mora moći komunicirati s ne-pokretnim čvorovima
 - ne smije biti izložen dodatnim sigurnosnim rizicima
- **Mobile IPv4/IPv6 implementirani na mrežnom sloju** - transparentno za TCP/UDP/ i fizički sloj
- **Mobile IP adrese:**
 - **domaća adresa (home address)** - stalna adresa dodijeljena čvoru, ne mijenja se promjenom točke priključka
 - **trenutna adresa (care-of address)** - adresa dodijeljena čvoru kada je priključen preko neke točke. Mijenja se promjenom priključne točke, destinacijska je kada se nešto šalje čvoru.

- **Mobile IP funkcijski entiteti:**
 - **Mobile node, MN (pokretni cvor)** - cvor koji mijenja točku priključka
 - **Home agent, HA (domaći agent)** - router sa sučeljem na domaćem linku. Pokretni cvor ga obavještava o promjeni care-of adrese, omogućava usmjeravanje prema stalnoj IP cvora, tunelira promet prema care-of adresi
 - **Foreign agent, FA (strani agent)** - router na stranom linku, obavještava home agent o trenutnoj adresi, usmjerava datagrama ka/od MN-a.
- **Trenutne adrese:**
 - **posredstvom stranog agenta** - IP adresa stranog agenta. Mrežni prefiks ove vrste ne mora biti jednak mrežnom prefiksu stranog linka. Vise MN-ova može koristiti ovakvu adresu istovremeno
 - **mjesna trenutna adresa** - IP adresa dodjeljena sučelju pokretnog cvora. Mrežni prefiks mora odgovarati, može je koristiti samo jedan agent. Ne treba postojati strani agent.
- **Otkrivanje agenta - ICMP poruke**
 - **Oglasavanje agenta (AA - agent advertisement)** - svaki agent periodički šalje ove poruke na poveznice gdje služi kao HA ili FA (broadcast ili multicast). Prosirena poruka Router Advertisement. Dodana polja Lifetime - govori koliko često se šalje AA poruka (u pravilu puno češće nego Lifetime vrijednost zbog gubitaka) i Care-of address - trenutna adresa stranog agenta koju će cvoru služiti za registraciju s domaćim
 - **Traženje agenta (AS - agent solicitation)** - MN šalje kako bi potaknuo HA ili FA da pošalje AA. Poruka slična ICMP Router solicitation, TTL postavljen na 1.
- **Utvrđivanje promjene poveznice:**
 - Ako ne primi AA od FA u Lifetime vremenu
 - Ako u AA poruci detektira promjenu mrežnog prefiksa ili router adrese
- **Problemi s otkrivanjem agenta** - ne primi AA ni nakon slanja nekoliko AS
 - 1. pretpostavka - nalazi se u domaćoj mreži, a ne radi HA. Pokušava komunicirati s default gateway-em
 - 2. pretpostavka - nalazi se u stranoj mreži. Pokušava dobiti adresu DHCPom ili je ručno konfigurira.
- **Postupak registracije:**
 - **Obavlja se putem Registration request/reply poruka (UDP).**
 - Prijavljuje se preko FA, a ukoliko isti ne postoji dobiva se adresa od DHCP-a i direktno se šalje Registration Request HA-u, koji potvrđuje s Reply-em. Ukoliko nakon nekoliko pokušaja ne dobijemo Reply registracija je nuspješna.

- **Postupak deregistracije:**
 - **koriste se iste poruke**
 - Provodi se kada se MN vrati u domacu mrežu
- **Autenticnost i integritet poruka** - koristi se MD5 hash i PKI infrastruktura. Kreira se fiksni dio Request poruke i Mobile Home Authentication prosirenje. Sve se hashira i potpisuje privatnim kljucem. HA desifrira javnim kljucem i provjerava hash. Zamjenjene uloge kod Reply-a.
- **Usmjeravanje datagrama:**
 - Prema pokretnom cvoru se diže tunel do FA. FA vadi datagrame iz tuneliranih i isporučuje MN-u.
 - Od pokretnog cvora ide routingom preko FA ili nekog drugog routera navedenog u AA poruci.
 - **Problem trokutastog usmjeravanja** - izražen kada je MN blizu sugovornika, a oboje su daleko od HA. Puno efikasnije rjesenje bilo bi direktan tunel. **Rijesno u Mobile IPv6.**
- **Mobile IPv6:**
 - **isto kao i Mobile IPv4:** MN, HA, domaca poveznica, strana poveznica
 - **drugacije:** adresiranje (domace i care-of adrese), nema FA - koristi se IPv6 router.
 - **ново:** anycast adresiranje HA, optimizacija puta je dio specifikacije (problem trokutastog routinga), zastita (IPSec)
- **Entiteti - MN, HA, CN (Corresponding node, sugovornik)**
- **Nacin rada:** MN otkriva promjenu tocke prikljucka, autokonfigurira adresu i registrira je kod HA, HA tunelira sav promet prema novoj adresi, ako CN nema podršku za Mobile IPv6 kreira se dvosmjerni tunel, a ako ima onda se optimizira routing. Komunikacija MN i HA zasticena IPSec-om.
- **Za otkrivanje routera koristi se NDP (Router Advertisement i Router Solicitation).**
- **Router advertisement se salju multicastom** - ako unutar nekog vremena ne primi RA od default routera, znaci da je promijenio poveznicu i prelazi na autokonfiguraciju (to radi i kad se promjeni default gateway). Prefiks trenutne adrese odgovora prefiksu mreže.
- **Registracija - Binding - sustinski ista kao MIPv4.** Koriste se poruke koje **se prenose dodatnim MIPv6 zaglavljem - Mobility header:**
 - **Binding Update** - MN obavjestava HA o trenutnoj adresi
 - **Binding Acknowledgment** - HA potvrđuje Binding Update
 - **Binding Refresh Request** - CN cvor zahtjeva da mu HA posalje Binding Update poruku s trenutnom adresom MN
 - **Home Address** - poruka koju salje MN kao obavijest o svojoj domacoj adresi

- **Dodatne podatkovne strukture:**
 - **Binding cache** - spremnik pridruženih adresa (u IPv6 routeru)
 - pri primitku svake Binding Update poruke, adresa se pohranjuje u spremnik. Kod slanja paketa provjerava se cache i ako postoji adresa usmjerava se direktno na trenutnu adresu koristeći dodatno zaglavlje
 - **Binding update list** - svaki MN čuva popis svih Binding update poruka koje je poslao HA ili CN, a kojima nije istakao Lifetime
 - **Home Agents List** - svaki MN čuva listu HA-ova sastavljenih na temelju RA
- **Optimizacija usmjeravanja:**
 - MN šalje CN-u dvije poruke, jednu s svoje home address (Home Test Init - HoTI) i jednu s svoje care-of adrese (Care-of Test Init - CoTI). CN potvrđuje s Home Test - HoT i Care-of Test - CoT. Poruke HoT i HoTI idu preko HA. Nakon toga MN šalje Binding Update CN-u. Tu poruku cachiraju svi IPv6 usmjeritelji na putu. Kada CN pošalje poruku prema MN-u, provjerava se cache i ako postoji adresa **koristi se dodatno routing zaglavlje** da bi se paket dostavio direktno, a ne kroz tunel. U tom zaglavlju definira se put kojim treba usmjeravati pakete, a ima 2 hop-a. Prvi hop je trenutna adresa, a drugi je "povratna petlja" unutar samog cvora, a sadrži adresu HA.
- **Zastita:** koristi se AH zaglavlje za autentikaciju (integritet) i ESP zaglavlje za privatnost (kriptiranje)
- **Uvodjenje IPv6 u mrežu** - za komunikaciju IPv6 cvorova preko IPv4 mreže potrebni su posebni mehanizmi
 - **Dual-stack implementacija**
 - **Tuneliranje (ručno, automatsko, konfigurirano)**
 - **Prevodjenje protokola**
- **Tuneliranje** - enkapsulira se IPv6 paket unutar IPv4 paketa i takav putuje kroz IPv4 mrežu. Kada dođe do dijela gdje je podržan IPv6, odbacuje se IPv4 zaglavlje, po potrebi obnavlja IPv6 zaglavlje i tako dalje putuje.
 - **Router-to-router - konfigurirano tuneliranje** - kreiraju tunel između sebe
 - **Host-to-router - konfigurirano tuneliranje**
 - **Router-to-host - automatsko tuneliranje**
 - **Host-to-host - automatsko tuneliranje**

Protokoli usmjeravanja

- **Usmjeravanje** - postupak pronalazenja puta i prosljedjivanja paketa od izvorista do odredista. Datagrami mogu putovati razlicitim putevima.
- **Odredjivanje puta temelji se na odredisnoj IP adresi**
- **Usmjeritelj** - sustav s najmanje dva sucelja u dvije razlicite mreze. Sadrzi tablicu usmjeravanja
- **Protokole usmjeravanja dijelimo s obzirom na podrucje djelovanja:**
 - **Unutar autonomnog sustava - AS-a** (Interior gateway protocol)
 - **Izmedju AS-ova** (Exterior gateway protocol)
- **Algoritam usmjeravanja moze biti:**
 - **staticki** - neadaptivan
 - **dinamicki** - adaptivan
- **Na osnovu routing tablica** nalazi se optimalan put kroz mrezu
- **Osnovne upravljacke informacije:**
 - **Odredisna adresa**
 - **Izvorisna adresa**
 - **TTL**
- **CIDR** - routing bez klasa
 - prednosti su efikasnije iskoristavanje IP prostora, manje routing tablice
 - nedostatak je slozenost
- **Protokoli usmjeravanja** - izvedeni su u usmjeriteljima, a ukljucuju strategiju usmjeravanja i algoritme usmjeravanja
- **Proces usmjeravanja:** prikuplja znanje o topologiji, azurira podatke i sprema ih u tablicu usmjeravanja i na osnovu tih podataka bira put za svaki datagram.
- **IGP protokoli:**
 - **RIPv2** - temelji se na algoritmu vektora udaljenosti
 - **OSPFv2** - temelji se na algoritmu stanja poveznice
- **EGP protokoli:**
 - **BGPv4** - temelji se na algoritmu vektora puta
- **Algoritam usmjeravanja:**
 - **Azurira tablicu usmjeravanja**
 - **Zahtjevi** - korektnost, robusnost, jednostavnost, stabilnost, optimalnost, pravednost
 - **Kriterij optimalnosti puta** - kasnjenje, udaljenost, cijena, sigurnost
 - **Staticki** - putevi se postavljaju prilikom inicijalizacije i ne mijenjaju se (usmjeravanje najkracim putem, preplavlivanje)

- **Dinamicki** - putevi se dinamički mijenjaju s promjenama u mreži (usmjeravanje prema vektoru udaljenosti, usmjeravanje prema stanju poveznice)
- **RIPv2** - classless routing, ruta sljedećeg skoka, autentifikacija, multicast usmjeravanje, koristi UDP, distance-vector
- **Timing:**
 - Prilikom pokretanja šalje broadcast gdje zahtjeva routing tablice
 - U aktivnom načinu svakih 30sec šalje svoju tablicu
 - Svaka promjena se broadcasta
 - Ako u 6 ciklusa (180sec) ne dobije tablicu od susjeda, postavlja metriku na 16, a nakon sljedećih 60sec je brise.
- **Ogranicenja:**
 - Ne uzima u obzir stanje linka, samo broj hopova
 - Maksimalno 16 hopova, neprikladno za veće mreže
 - Spora konvergencija
 - Brojanje do beskonačno
- **Rjesenja za brojanje do beskonačno:**
 - **Split horizon** - nikada ne oglasavati rutu na interface na koji je naučena
 - **Split horizon with poison reverse** - oglasavati takvu rutu s metrikom 16
 - **Postaviti hold-down timer (60-120sec) nakon detekcije ispada** - zanemariti bilo kakve informacije o ruti u tom vremenu
- **Rjesenje za sporu konvergenciju:**
 - **Triggered update** - slati update čim se detektira promjena
- **OSPF - open shortest path first protocol**
 - Brza konvergencija
 - CIDR
 - manji promet između routera
 - Složeniji od RIPv2
- **Osnovne operacije:**
 - Otkrivanje susjeda
 - Izbor nadležnog usmjeritelja (DR) i pomoćnog nadležnog (backup)
 - Sinkronizacija tablice usmjeravanja
 - Kreiranje/održavanje tablica
 - Oglasavanje stanja poveznica (LSA - link state advertisement)
- **Hijerarhijsko usmjeravanje** - grupiranje u područja (areas), gdje svako područje ima svoj DR i backup DR. Kategorizira se: internal, border, backbone
- **Multipath routing** - više linkova s istim costom - load balancing
- **Identične informacije u svim routerima**

- Router posjeduje potpunu sliku mreze - svaki router salje informacije o stanju poveznica DR-u i backup DR-u
- DR i backup DR primljene informacije salju svim ostalim routerima u areai
- Uzima u obzir stanje linka pri racunanju costa
- Salju se samo promjene u tablici, ne cijele tablice
- Podrzava autentifikaciju
- Svaki usmjeritelj odrzava LSDB (link-state database) - informacije o svim routerima s kojima nisu direktno vezani
- Tipovi poruka
 - Hello - otkrivanje i odrzavanje susjednih odnosa kod usmjeritelja - salje se svakih 10 sec, nakon 40sec bez Hello paketa zakljucuje prekid veze
 - Database Description - opisuje bazu podataka, poruke se razmjenjuju tijekom inicijalne sinkronizacije
 - Link State Request - poruka kojom se zahtjeva stanje linka
 - Link State Update - poruke kojima se opisuju ili osvjezavaju stanja linkova
 - Link State Acknowledgment - poruke kojima se potvrđuje osvjezeno stanje linka
- Inicijalna sinkronizacija:
 - Razmjena baza podataka
 - Salju se zaglavlja svih LSA-ova (serijom paketa Database Description)
 - Salju se zahtjevi svih LSA-ova kojih nema (Link State Request) i odgovori (Link State Update)
- Kontinuirana sinkronizacija:
 - Pojavom novih LSA-ova
 - Preplavljanjem
 - Pocinje kada usmjeritelj zeli osvjeziti neki od svojih LSAova

Obavezno pogledati RIP i OSPF crteze u skripti