РАДИЈУС
ВЕКТОР

Carrier-grade NAT

Iskustva i problemi

Šta je Radijus Vektor?

- Kablovski operater, osnovan 1998. godine u Beogradu
- Danas pokriva 12 opština u Srbiji
- Vremenom je širio paletu usluga, sada pružajući i usluge pristupa internetu, digitalne televizije, web hostinga, server housinga, fiksne telefonije, itd.
- Preko 200 zaposlenih

РАДИЈУС ВЕКТОР

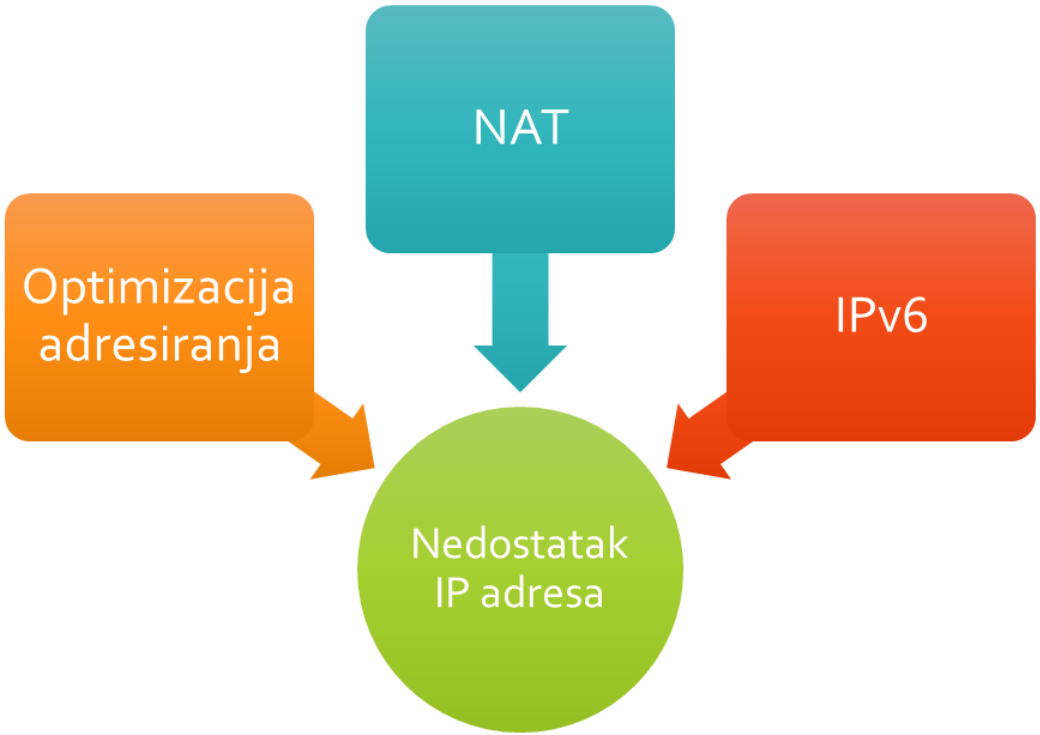
Ko sam ja?

- **Milan Anđelković**, sistem inženjer u Radijus Vektoru
- Zadužen primarno za razvoj i održavanje mreže
- Preko 10 godina iskustva u provajderskom okruženju
- Fokus na mreže, Linux servise i video striming

РАДИЈУС ВЕКТОР

Koji problem rešavamo?

- **Nedostatak IP adresa**
  - Optimizacija adresiranja donosi rezultate, ali je samo privremeno rešenje
  - NAT degradira servis i treba ga posmatrati kao privremeno ili srednjeročno rešenje
  - IPv6 je dugoročno rešenje, ali mu je primena još uvek ograničena



Šta je Carrier-grade NAT (CGN)?

- *Carrier-grade NAT* je *large-scale NAPT* (NAT+PAT) mehanizam.
- Ne čuva se informacija o destinaciji (destinaciona IP adresa i port).
- Obično se radi na namenskom uređaju unutar mreže ili na border ruteru (ruterima). U većim mrežama može biti smisleno da se radi i na access platformi.
- U slučaju više izlaznih tačaka iz mreže, namenski CGN uređaj je bolje rešenje.
- Na Cisco opremi, CGN se aktivira jednom komandom: "*ip nat settings mode cgn*".

CGN implementacija u Radijus Vektoru

- CGN koristimo na 2 lokacije
- Na obe se koristi potpuno redundantna Cisco ASR1006 šasija
- Zbog problema sa nekim internet servisima smo uključili *Paired-Address-Pooling*
- U proseku oko 100 translacija po korisniku

РАДИЈУС ВЕКТОР

CGN implementacija u Radijus Vektoru

- Logovanje NAT translacija se oslanja na:
  - *Netflow Event Logging*
  - *Nfacctd*
  - *Elastic search* (4 noda)
  - *Graylog* (2 noda) iza LB-a
- Trenutno se generiše oko 10-12GB logova dnevno, po lokaciji
- Uz kompresiju dobijamo ~9 puta manje zauzeće prostora
- Logove čuvamo godinu dana

РАДИЈУС ВЕКТОР

CGN implementacija u Radijus Vektoru

	Lokacija 1	Lokacija 2
ESP&RP	ESP100&RP2	ESP10&RP1
Broj korisnika	~9.000	~9.000
NAT pool	/23	/24
PAP limit	120	250
Iskorišćenost NAT pool-a	~50%	~30%
Broj NAT translacija	600k	800k
Max NAT translacija	12M	1M

РАДИЈУС ВЕКТОР

CGN implementacija u Radijus Vektoru

Lokacija 1

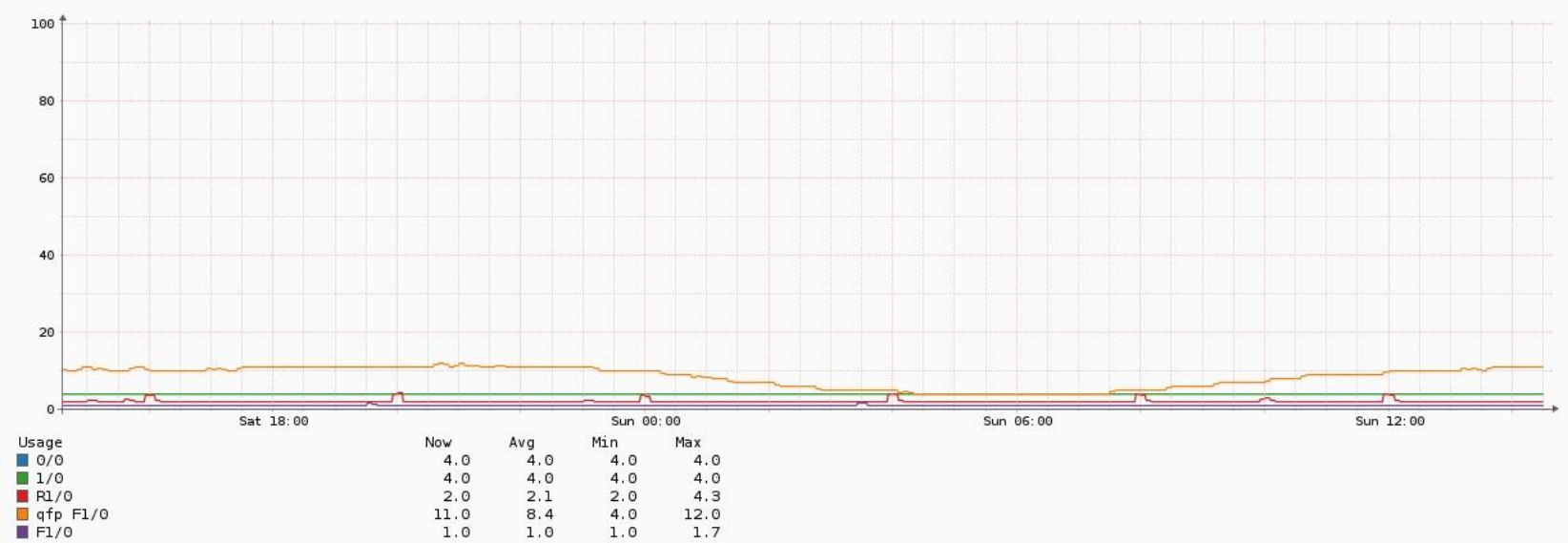
- Broj translacija u toku dana varira u skladu sa količinom saobraćaja, odnosno brojem aktivnih korisnika u tom trenutku

РАДИЈУС ВЕКТОР

CGN implementacija u Radijus Vektoru

Lokacija 1

- Opterećenje procesora takođe zavisi od aktivnosti korisnika



РАДИЈУС ВЕКТОР

Problemi uzrokovani korišćenjem CGN-a

- Potreba za logovanjem NAT translacija – potreban cluster koji može da izdrži opterećenje, kao i storage za dugoročno čuvanje podataka
- Neki internet servisi imaju problema sa CGN saobraćajem, npr. ebanking portali – treba koristiti *Paired-Address-Pooling (PAP)*
  - PAP omogućava konzistentno transliranje jedne privatne adrese u istu javnu adresu. Treba obratiti pažnju na PAP limit – prava vrednost zavisi od prirode saobraćaja
- Content caching (ggc, akamai) - GGC radi bez problema, dok AKAMAI mora biti eksterno pozicioniran u mreži jer ne prihvata saobraćaj sa privatnih adresa

Problemi uzrokovani korišćenjem CGN-a

- Bug-ovi u implementaciji – Cisco bug *CSCun06260* se odnosi na gatekeeper funkcionalnost kod Cisco ASR1000 serije. U slučaju da kroz interfejs koji radi NAT prolazi 1Gbps saobraćaja ili više, treba povećati gatekeeper cache: "*ip nat settings gatekeeper-size 64000*"
- Isključivanje korisnika iz NAT-a po zahtevu – mi koristimo CNR i njegov mehanizam po imenu *selection tag* za kontrolu dodeljivanja adresa iz javnog ili privatnog pool-a
- NAT444: preklapanje opsega usled duplog NAT-a – za CGN bi trebalo koristiti opseg iz *shared address space-a*: 100.64.0.0/10 (*RFC 6598*). Mi još uvek koristimo 10.0.0.0, ali planiramo da promenimo to.

Problemi uzrokovani korišćenjem CGN-a

- PfR - *Performance Routing* nije kompatibilian sa CGN-om. Mi smo razmatrali da ga koristimo pre implementacije CGN-a, ali nismo stigli da se bavimo time.
- Netflow analiza – potrebno je dobro osmisliti mehanizam pretrage podataka kada treba povezati javne adrese iz netflow podataka sa logovima NAT translacija, odnosno privatnim adresama korisnika.
- Abuse prijave – neophodno je da pored source adrese sadrže i source port (*RFC 6302*)
- Skalabilnost – šta kada broj korisnika prevaziđe kapacitet jednog CGN uređaja? Neophodno je izmeniti dizajn, što dodatno komplikuje setup.

Kraj

- Pitanja?

- Kontakt: *milan.andjelkovic@radijusvektor.rs*

РАДИЈУС ВЕКТОР