

MEĐUSOBNO POVEZIVANJE PRIVATNIH MREŽA

NAT, VPN

Uvod

- ◆ Današnji Internet može da se posmatra kao arhitektura u 2 nivoa:
- ◆ (a) svaka organizacija ima svoj privatni internet, a
- ◆ (b) svetski Internet ih međusobno povezuje.
- ◆ Za ove potrebe uvedene su dve nove tehnologije:
- ◆ (a) prva rešava problem ograničenog adresnog prostora
- ◆ (b) druga obezbeđuje privatnost sprečavanjem pristupa privatnim podacima.

Privatne i hibridne mreže

- ◆ Jedan od osnovnih nedostataka do sada razmatranog modela Interneta je nedostatak privatnosti.
- ◆ Ako neka organizacija obuhvata više lokaliteta, sadržaji datagrama koji se prenose između lokaliteta su dostupni i organizacijama preko čijih mreža se oni prenose.
- ◆ Arhitektura sa dva nivoa deli datagrame na unutrašnje i spoljne (datagrami koji se razmenjuju između različitih organizacija).
- ◆ Cilj je da unutrašnji datagrami budu privatni, a da se pri tome ne spreči komunikacija sa drugim organizacijama.

Privatni internet (privatna mreža)

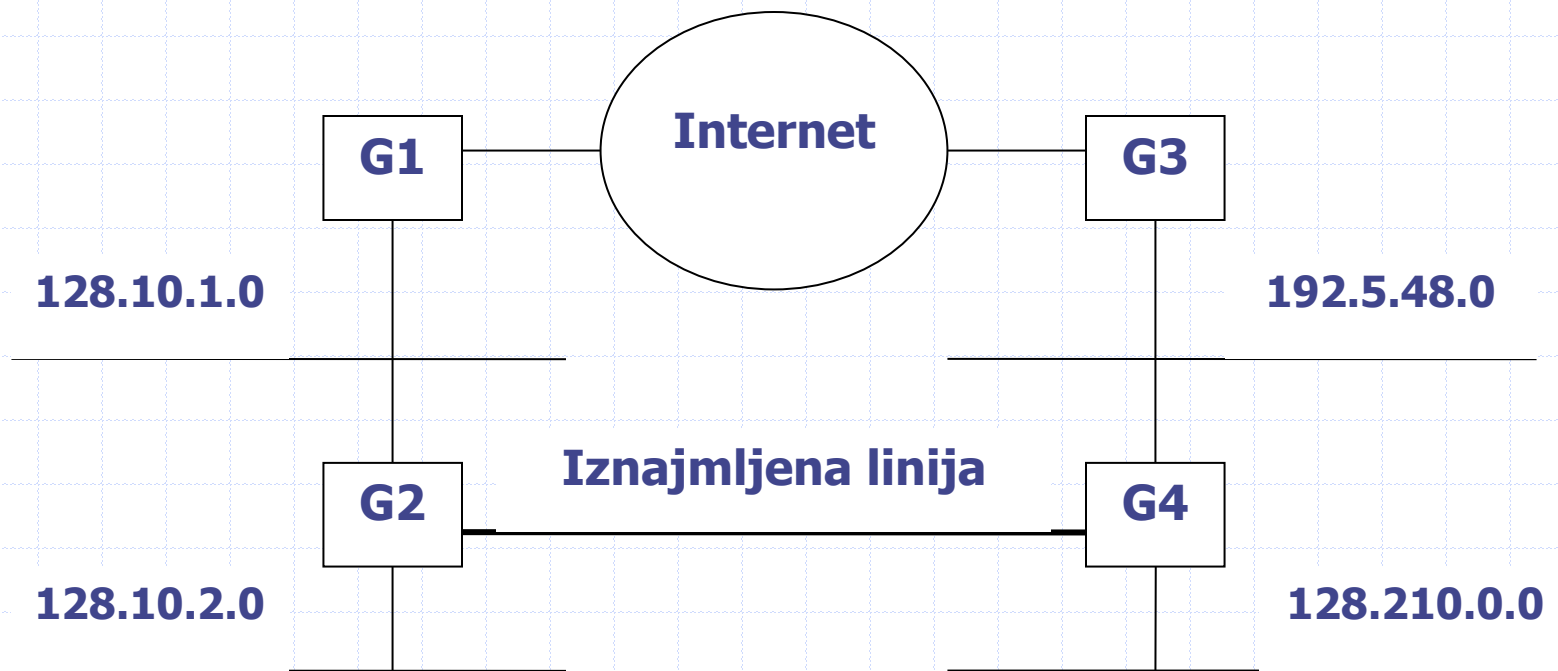
- ◆ Najlakši način da se obezbedi privatnost je da se izgradi privatni internet, potpuno mimo javnog Interneta.
- ◆ Za međusobno povezivanje lokaliteta koriste se iznajmljene digitalne linije.
- ◆ Prednosti ovog pristupa su:
 - ◆ (a) svi podaci su privatni, i
 - ◆ (b) mogu se koristiti proizvoljne IP adrese.

Hibridna mreža

- ◆ Organizacija koja ne želi potpunu izolaciju može da se opredeli za tzv. *hibridnu* mrežu.
- ◆ Ona nudi prednost privatnog umrežavanja zajedno sa prednošću povezivanja sa javnim Internetom.
- ◆ Za povezivanje lokaliteta se koriste javne IP adrese.
- ◆ Računari u organizaciji po potrebi mogu pristupati javnom Internetu, a sva unutrašnja komunikacija je privatna.
- ◆ Unutrašnja komunikacija je privatna pošto se odvija preko iznajmljenih linija.

Primer hibridne mreže

(Sav privatan saobraćaj se odvija preko iznajmljenih veza.)



Virtuelna privatna mreža (VPN)

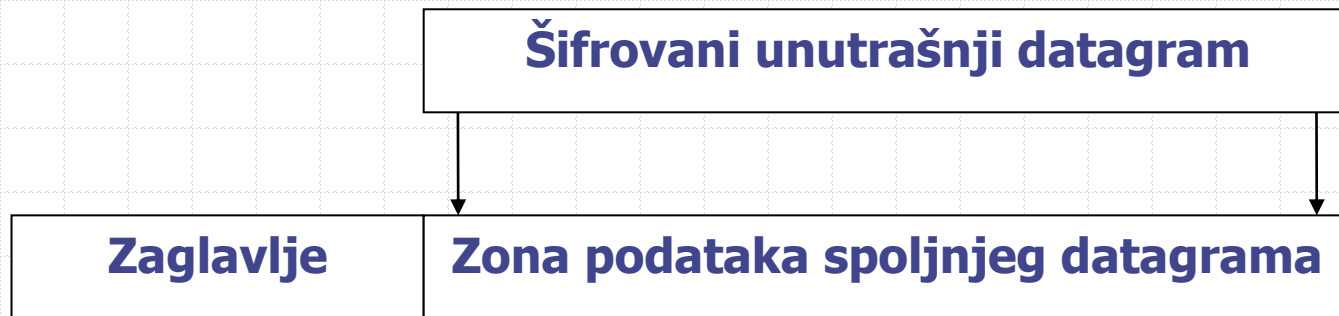
- ◆ Osnovni nedostatak privatne, kao i hibridne, mreže su veliki troškovi iznajmljenih digitalnih linija (E1 i sl.).
- ◆ Trošak se može smanjiti primenom drugih tehnologija, kao što su FR (Frame Relay) i ATM PVC (Permanent Virtual Circuit).
- ◆ Drugi način je upotreba manjeg broja linija.
- ◆ Najmanji trošak se postiže ukoliko se sav saobraćaj prenosi preko javnog Interneta.
- ◆ Ali, postavlja se pitanje kako obezbediti privatnost saobraćaja preko javnog Interneta?
- ◆ Odgovor je, primenom VPN tehnologije.

VPN tehnologija

- ◆ Čine je dve osnovne tehnike:
 - ◆ (a) Tunelovanje
 - ◆ (b) Šifrovanje
- ◆ Tunelovanje se zasniva na postavljanju tunela između konvertora na dva različita lokaliteta i slanju IP datagrama unutar IP datagrama (IP-u-IP enkapsulacija)
- ◆ Svaki IP datagram se šifruje pre nego što se upiše u polje podataka IP datagram kojim se prenosi do odredišta.
- ◆ Dakle, virtuelna privatna mreža šalje podatke preko javnog Interneta, ali ih šifruje radi obezbeđenja privatnosti.

Ilustracija IP-u-IP enkapsulacije

(Unutrašnji datagram se pre slanja šifruje.)

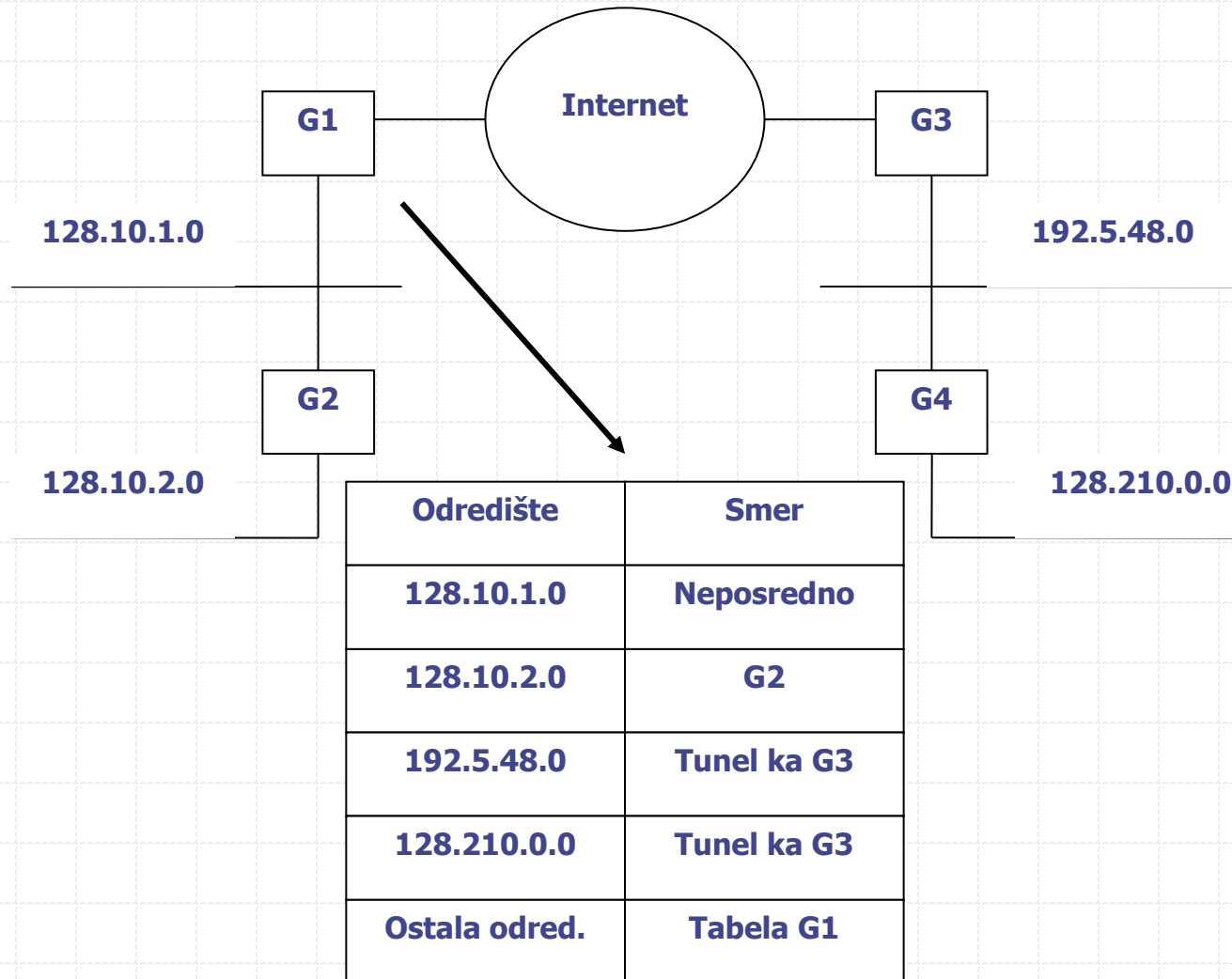


Adresiranje i usmeravanje u VPN

- ◆ Logički, VPN tunel zamenjuje iznajmljenu vezu privatne mreže.
- ◆ U tabelama usmeravanja postoje eksplicitni smerovi za odredišta unutar organizacije.
- ◆ Umesto da bude usmeren ka iznajmljenim linijama, unutrašnji saobraćaj se usmerava prema VPN tunelima.
- ◆ Radi ilustracije ovog koncepta posmatra se tabela usmeravanja konvertora protokola G1 (iz prethodnog primera).
- ◆ Npr. saobraćaj iz mreže 128.10.2.0 za 128.210.0.0 se usmerava od G2, preko G1, kroz tunel do G3, i dalje do G4, koji obavlja neposrednu isporuku.

Tabela usmeravanja u G1

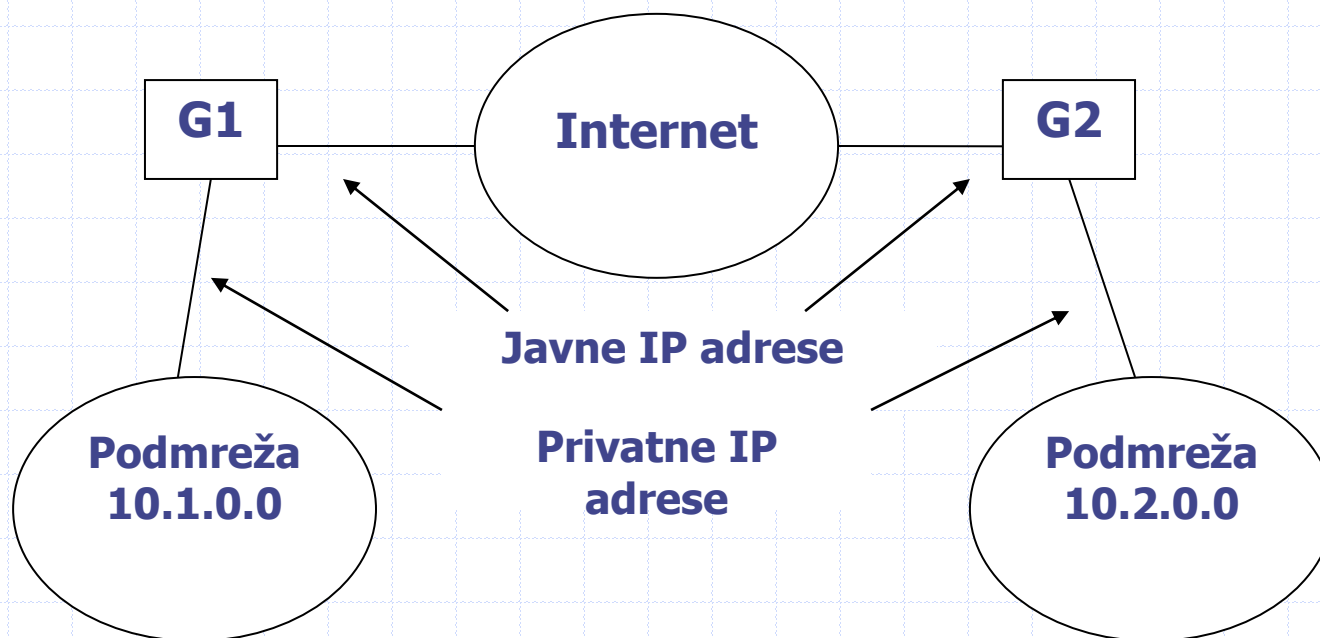
(Tunel G1-G3 se konfigurira kao iznajmljena linija.)



VPN sa privatnim adresama

- ◆ VPN nudi iste opcije adresiranja kao i privatna mreža.
- ◆ Ako ne postoji potreba za povezivanje računara na javni Internet, mogu se koristiti proizvoljne IP adrese.
- ◆ Ukoliko postoji potreba za pristup javnom Internetu, koristi se hibridna adresna šema.
- ◆ Za potrebe tunelovanja mora se obezbediti po jedna javna IP adresa sa svake strane tunela.
- ◆ U narednom primeru organizacija poseduje dva lokaliteta (podmreže 10.1.0.0 i 10.2.0.0).
- ◆ U posmatranom primeru G1 i G2 koriste javne IP adrese za pristup javnom Internetu.

Primer adresiranja u VPN sa 2 lokaliteta



- ◆ Računari na oba lokaliteta koriste privatne adrese.
- ◆ G1 i G2 za pristup Internetu koriste javne IP adrese.

Primene VPN

◆ Danas se najčešće sreću dva slučaja:

- Rad od kuće ili sa druge udaljene lokacije i pristup resursima i uslugama mreže preduzeća
- Sakrivanje lokacije korisnika da bi se zaobišla ograničenja koja nameću pojedine usluge a koja su vezana za lokaciju korisnika

Kako obezbediti pristup javnom Internetu svakom računaru, a da mu se ne dodeli javna IP adresa?

- ◆ Postoje sledeća dva rešenja:
- ◆ (1) pomoću aplikativnog mrežnog konvertora protokola
- ◆ (2) prevođenjem mrežnih adresa.
- ◆ Aplikativni mrežni konvertor protokola obezbeđuje usluge Interneta bez pristupa na IP nivou.
- ◆ On se izvršava na računaru koji je povezan i na javni Internet i na unutrašnju mrežu.
- ◆ Na zahtev računara iz unutrašnje mreže, aplikativni mrežni konvertor pristupa poslužiocu u Internetu, i nakon toga prosleđuje informaciju nazad kroz unutrašnju mrežu (npr. e-mail usluga).

Prednosti i nedostaci ovog pristupa

- ◆ Prednost: mogućnost da se radi bez izmena u infrastrukturi i adresiranju.
- ◆ Nedostatak: rešenje nije univerzalno, zato što jedan konvertor obezbeđuje samo jednu jedinu uslugu.
- ◆ Ovaj nedostatak je otklonjen uvođenjem tehnologije prevođenja mrežnih adresa (NAT, Network Address Translation).

Prevođenje mrežnih adresa (NAT)

- ◆ Dovoljno je da lokalitet ima jednu vezu sa javnim Internetom i bar jednu javnu IP adresu, J.
- ◆ Ova adresa je dodeljena tzv. NAT kutiji (računar koji povezuje lokalitet sa javnim Internetom, i na kom se izvršava NAT programska podrška).
- ◆ NAT prevodi adrese tako što:
 - ◆ (a) u odlaznim paketima zamenjuje adresu pošiljaoca javnom IP adresom J, i
 - ◆ (b) u dolaznim paketima zamenjuje javnu IP adresu privatnom adresom stvarnog odredišta.
- ◆ Nakon zamene adrese, mora se preračunati kontrolna suma zaglavlja.

Prednosti NAT

- ◆ (1) Univerzalnost: NAT omogućava svim unutrašnjim računarima pristup svim uslugama Interneta.
- ◆ (2) Transparentnost: NAT omogućava unutrašnjim računarima da koriste usluge javnog Interneta putem privatne (neusmerene) adrese.

Tabela za prevođenje adresa

- ◆ Svaka vrsta tabele ima dve kolone:
- ◆ (1) javna IP adresa računara na Internetu, i
- ◆ (2) unutrašnja IP adresa računara.
- ◆ Kako i kad se ova tabela popunjava?
- ◆ Postoje 3 načina:
- ◆ (1) Ručno popunjavanje. Ovo radi administrator.
- ◆ (2) Na osnovu odlaznih datagrama. NAT otvara novu vrstu i beleži adresu računara i adresu odredišta.
- ◆ (3) Na osnovu dolaznog DNS zahteva. Nova vrsta tabele se otvara na osnovu DNS zahteva računara iz Interneta za određivanje IP adrese unutrašnjeg računara.

Prednosti i nedostaci raznih načina popunjavanja tabele prevođenja adresa

- ◆ Ručnim popunjavanjem se dobija trajna tabela, koja omogućava prijem i slanje datagrama u bilo kom trenutku.
- ◆ Korišćenje odlaznih datagrama omogućava automatsko popunjavanje tabele, ali ne dozvoljava da komunikacija počne spolja.
- ◆ Korišćenje dolaznih DNS zahteva modifikaciju DNS programa, omogućava da komunikacija počne spolja, ali je moguća samo ako njoj prethodi DNS zahtev.

Popunjavanje na osnovu odlaznih paketa

- ◆ Najčešće se koristi popunjavanje na osnovu odlaznih datagrama (posebno kod posrednika za Internet, ISP).
- ◆ Radi ilustracije posmatra se primer malog Internet posrednika, koji pruža usluge Interneta preko komutiranih telefonskih linija.
- ◆ NAT omogućava Internet posredniku da dodeljuje privatne adrese (npr. 10.0.0.1 prvom, 10.0.0.2 drugom, itd.).
- ◆ Kad korisnik pošalje datagram ka odredištu na Internetu, NAT otvara novu vrstu u tabeli za prevođenje adresa.

Višeadresni NAT

- ◆ Do sada je opisan 1-na-1 model prevođenja adresa.
- ◆ On ne dopušta da više unutrašnjih računara istovremeno komunicira sa istom javnom IP adresom.
- ◆ Da bi se ovaj problem rešio, uvedena je šema pod nazivom *višeadresni NAT*: NAT kutiji se dodeli K javnih IP adresa.
- ◆ NAT dinamički, redom, dodeljuje javne adrese unutrašnjim računarima.
- ◆ Time je omogućeno da do K unutrašnjih računara istovremeno pristupa istom odredištu na Internetu.

NAT sa preslikavanjem prolaza (eng. port)

- ◆ Naredno proširenje NAT, omogućava i prevođenje brojeva prolaza UDP i TCP protokola.
- ◆ Ova šema se označava skraćenicom NAPT (Network Address Port Translation).
- ◆ Odgovarajuća tabela prevođenja ima dve dodatne kolone, u koje se unose brojevi prolaza protokola izvorišta i odredišta.
- ◆ Radi ilustracije, posmatra se primer kad 4 unutrašnja računara pristupa odredištima na Internetu.
- ◆ Svi koriste TCP, koji svaku vezu identifikuje četvorkom, koju čine IP adrese i prolazi izvora i odredišta.

Primer tabele sa preslikavanjem prolaza

(Dva unutrašnja računara, 10.0.0.5 i 10.0.0.1, pristupaju Web serveru, prolaz 80, na računaru 128.10.19.20.)

Privatna adresa	Privatni prolaz	Javna adresa	Javni prolaz	NAT prolaz	Protokol
10.0.0.5	21023	128.10.19.20	80	14003	TCP
10.0.0.1	386	128.10.19.20	80	14010	TCP
10.0.2.6	26600	207.200.75.200	21	14012	TCP
10.0.0.3	1274	128.210.1.5	80	14007	TCP

Prednosti i nedostaci NAT-a

- ◆ Prednost: univerzalnost koja se postiže jednom javnom adresom.
- ◆ Nedostatak: ograničava se na UDP i TCP.

Međudejstvo NAT i ICMP

- ◆ NAT ne može biti transparentan za ICMP poruke.
- ◆ Na primer ICMP poruka za preusmeravanje (redirect) mora da se obradi lokalno u NAT kutiji, ažuriranjem tabele usmeravanja.
- ◆ Generalno, pre prosleđivanja ICMP poruke, NAT mora:
 - ◆ (1) da utvrdi da li poruku treba lokalno obraditi, i
 - ◆ (2) mora da prevede ICMP poruku.
- ◆ Npr. prevođenje ICMP poruke “odredište nedostupno” zahteva zamenu javne adrese privatnom adresom P, i određivanje kontrolnih suma za P, ICMP zaglavlje, i zaglavlje spoljašnjeg datagrama.

Međudejstvo NAT i aplikacija

- ◆ Aplikativni protokoli, pored ICMP, dodatno usložnjavaju realizaciju NAT.
- ◆ Osim u slučaju nekoliko standardnih aplikacija, kao što je FTP, aplikativni protokoli koji prenose IP adrese, ili brojeve prolaza UDP i TCP protokola, kao podatke ne mogu da rade kroz NAT.
- ◆ Menjanje toka podataka usložnjava NAT na 2 načina:
 - ◆ (1) NAT mora da poznaje detalje aplikacije
 - ◆ (2) ako su brojevi dati u ASCII (kao kod FTP), menjanje vrednosti može da promeni broj okteta u toku podataka i tada NAT mora da menja i redne brojeve segmenata.

Konceptualni adresni domeni

- ◆ NAT može, u stvari, da poveže bilo koja 2 adresna domena (npr. 2 privatne mreže, koje obe koriste adresu 10.0.0.0).
- ◆ Dalje, NAT može da se koristi na više nivoa.
- ◆ Npr. na 2 nivoa: između privatnog adresnog domena korisnika i privatnog adresnog domena ISP-a, kao i adresnog domena ISP-a i javnog Interneta.
- ◆ NAT može i da se kombinuje sa VPN u hibridnoj arhitekturi, gde se privatne adrese koriste unutar organizacije, a putem NAT se povezuju lokaliteti između sebe i sa javnim Internetom.

Slirp i Masquerade

- ◆ Su dve popularne realizacije NAT.
- ◆ Slirp je program iz BSD UNIX sistema 4.4, koji podržava pristup preko komutiranih telefonskih linija.
- ◆ Slirp povezuje PPP i NAT u jedan program.
- ◆ Izvršava se na računaru sa javnom IP adresom, stalnom vezom ka Internetu i jednim ili više modema.
- ◆ Računar sa privatnom adresom poziva sistem preko modema i pokreće *slirp*, komutirana linija prelazi sa ASCII komandi na PPP, čime računar dobija pristup Internetu (npr. Web serveru).

Masquerade (NAPT za OS Linux)

- ◆ Za razliku od slirp-a ne zahteva da se računari povezuju preko telefonske linije, i nije potrebno da se korisnik prijavi na UNIX da bi se program pokrenuo.
- ◆ Umesto toga *masquerade* pruža različite mogućnosti, kao što je usmeravanje između dve mreže, korišćenje više IP adresa, i slično.

