Univerzitet u Beogradu, Elektrotehnički fakultet
Računarske osnove Interneta – IR4RM2, SI3RM2

VPN, MPLS, L2TP, IPsec

dr Pavle Vuletić

Virtuelne privatne mreže - VPN

- Virtuelna privatna mreža je mreža jedne institucije ili grupe korisnika realizovana preko javne ili deljene infrastrukture (Internet, provajderske mreže)
- VPN tehnologije:
  - Frame Relay
  - ATM
  - IP VPN tehnologije:
    - MPLS
    - IPsec
    - SSL
    - L2TP
    - GRE
    - Q-in-Q
    - …

2

http://www.ciscopress.com/content/images/1587051796/samplechapter/1587051796content.pdf

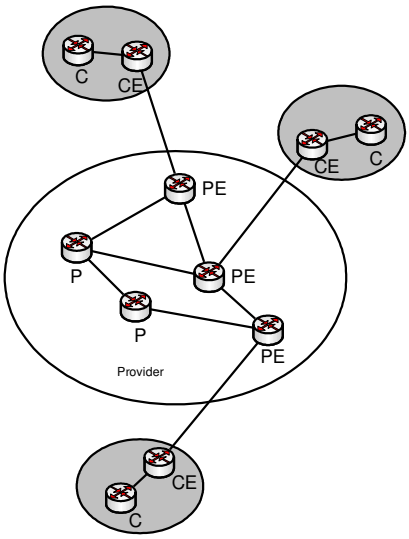
Razlozi za uvođenje VPN

- Potreba za novim aplikacijama
  - e-commerce, e-business
  - Bandwidth on demand
  - Voice/Video over IP
  - mobilnost
- Sigurnosni problemi
- Bolja organizacija saobraćaja, rutiranja
- Nedostatak podrške za QoS
- Problem broja IP adresa i migracija na IPv6

3

Vrste VPN uređaja

- Podela prema tome kome pripadaju uređaji i gde su u VPN:
  - C – customer
  - CE – customer edge
  - PE – provider edge
  - P – provider



4

Podele VPN

- Po tome ko ih realizuje:
  - Provider provisioned
  - Customer enabled
- Po vrsti servisa:
  - Site-to-site (LAN-to-LAN)
    - Intranet (lokacije jedne institucije)
    - Extranet (povezivanje različitih institucija)
  - Remote Access
    - Compulsory (access server inicira VPN vezu)
    - Voluntary (klijent inicira VPN vezu)
- Po sloju rada: L1, L2, L3
- Po poverljivosti podataka
  - Trusted VPN
  - Secure VPN

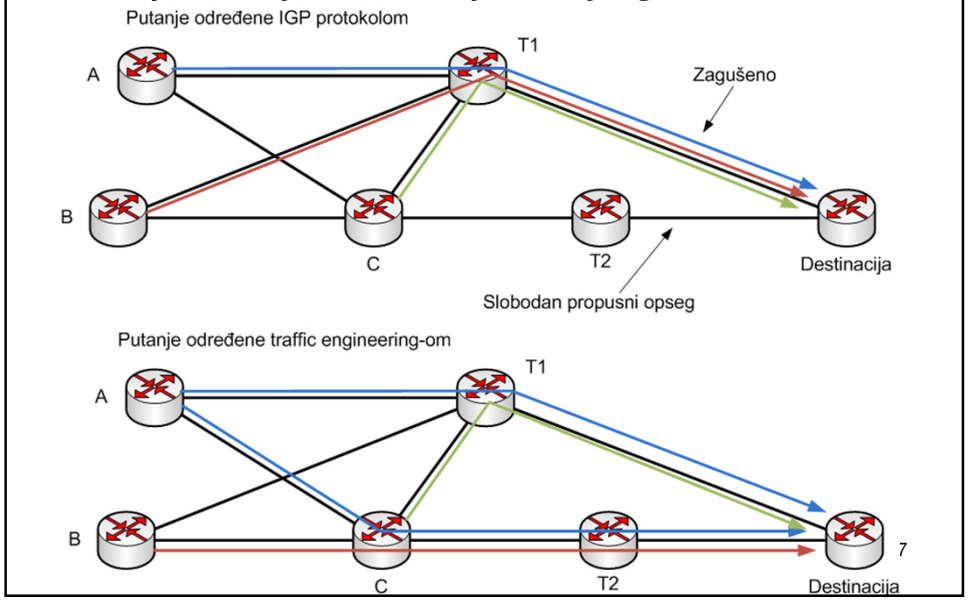
5

MPLS tehnologija

- Klasičan IP ne može da pruži neke servise koji su vremenom postali značajni za ozbiljne primene u oblasti pružanja telekomunikacionih servisa (QoS, traffic engineering, VPN,...)
- ATM je zamišljen kao tehnologija koja bi rešavala navedene probleme, ali ATM nije uspeo da se nametne kao dominantna tehnologija
- 1996. formirana MPLS grupa u okviru IETF. Prvi RFC 1999

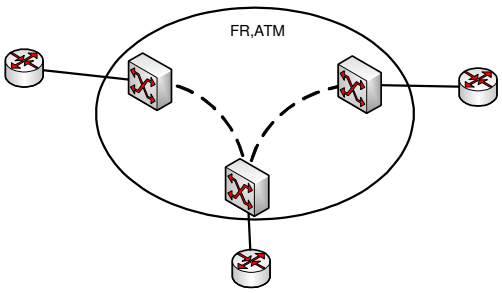
6

IP problem – saobraćaj se rutira po putanjama najmanjeg cost-a



Problem odnosa L2 i L3 tehnologija

- L2 tehnologije (FR, ATM) mogu da pruže neke od zahtevanih servisa
- L2 tehnologije ne mogu da vrše prosleđivanje na osnovu IP adresa
- Neoptimalno rutiranje
- Statičko postavljanje L2 logičkih veza
- Neskalabilnost
- Teška procena potrebnog propusnog opsega



8

Problem – IP rutiranje je relativno sporo

- Klasično IP rutiranje – svaki paket se nezavisno procesira i za svaki paket se donosi nezavisna odluka
- Moguće je da se izbegne rutiranje na osnovu destinacije – Policy based routing, ali ono je sporo i procesorski zahtevno
- Takođe, IP zaglavlje ima više informacija nego što je potrebno za prosleđivanje paketa, pa je njegovo procesiranje sporije

9

Procesiranje paketa

- Kada paket dodje u ruter obavljaju se sledece aktivnosti:
  - Proverava se L2 checksum
  - Proverava se IP header Checksum
- Kada se paket prosledjuje:
  - Menjaju se source i dest MAC adrese
  - Dekrementira se TTL
  - Racuna se novi IP header Checksum
  - Racuna se novi L2 checksum

10

Vrste prosleđivanja paketa

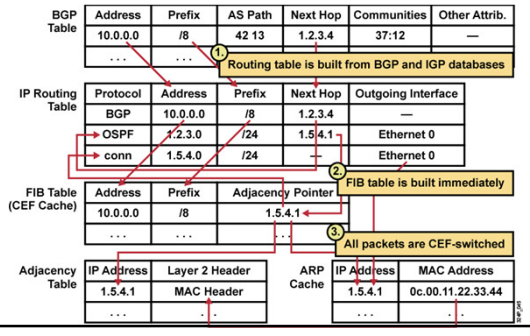
- Process/interrupt switching
  - Prosleđivanje u softveru
  - Svaki paket se nezavisno prosleđuje
- Fast switching (cache)
  - Prvi paket namenjen nekoj destinaciji se prosleđuje po process switching metodi, pravi se ulaz u switching kešu
  - Svičing keš sadrži IP adresu destinacije, next hop, L2 rewrite info
  - Ostali paketi iz istog toka se prosleđuju brže, na osnovu zapisa u switching kešu
- Hardversko prosleđivanje
  - Razdvojen control plane i data plane
  - Forwarding tabela se puni na osnovu routing tabele

11

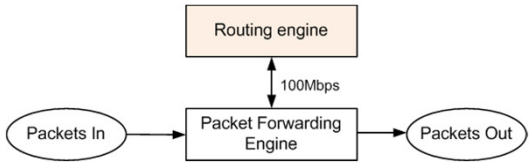
http://www.cisco.com/application/pdf/paws/13706/20.pdf

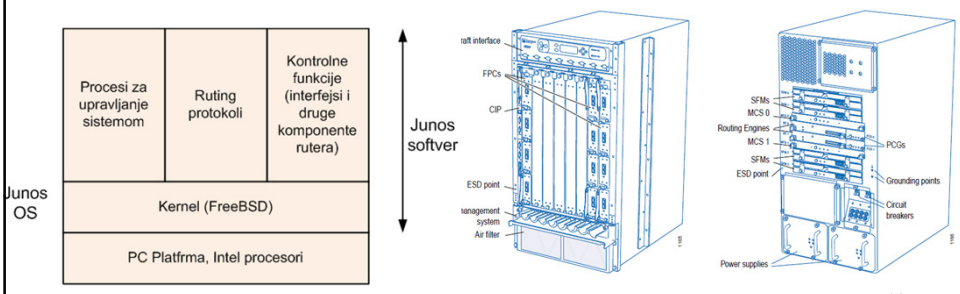
Cisco express forwarding (CEF)

- FIB (Forwarding Information Base) tabela i Adjacency tabela (na posebnim ASIC čipovima)
- FIB se puni iz ruting tabele
- Adjacency tabela – L2 informacije koje je potrebno upisati u odlazni paket
- Postoji centralizovani CEF (FIB i Adjacency tabele na centralnom Route procesoru) i distribuirani (FIB i Adjacency tabele na svakoj interfejs kartici)



Juniper arhitektura (M5, M10, M40, M160)





13

http://www.juniper.net/techpubs/grc/m160-grc.pdf

Juniper PFE

- Razlicite platforme imaju različite arhitekture:
  - Forwarding Engine Board (FEB) (M5/M10 ruteri),
  - System and Switch Board (SSB) (M20 ruteri),
  - Switching and Forwarding Module (SFM) (M40e i M160 ruteri)
- Zasnovane na ASIC čipovima
- M40e/M160 SFM (usmerava, filtrira i prosleđuje do 40Mpps):
  - Forwarding tabela u sinhronom SRAM (Internet Processor II ASIC)
  - Upravljanje deljenom memorijom (baferima) za FPC (koncentratori kartica sa interfejsima) radi se na Distributed buffer management ASIC (DBM) – dolazni paketi se smestaju u bafere
  - Drugi DBM prosleđuje pakete do izlaznog FPC gde se paket sprema za slanje
  - Internet Processor II ASIC šalje informacije o greškama i kontrolne pakete procesoru na SFM, koji ih prosleđuje Route engine-u

14

http://www.juniper.net/techpubs/hardware/m-series/fru-m40e-m160-sfm.pdf

MPLS (RFC 3031)

- MPLS – mehanizam za brzo prosleđivanje paketa, ne nužno na osnovu destanacione adrese, sa mogućnošću pružanja različitih servisa
- Ideja: saobraćaj razvrstati u FEC klase i za svaku FEC klasu odrediti NextHop
- FEC – Forwarding Equvalence Class
- Paketi se označavaju prema FEC klasi na ulasku u mrežu (PE uređaj)
- Oznaka se zove labela

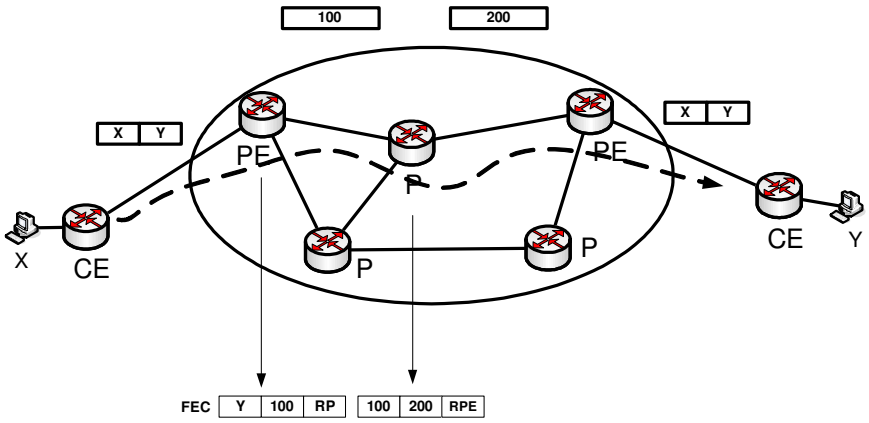
15

MPLS (RFC 3031)

- Nakon ulaska u mrežu paketi se na P uređajima prosleđuju na osnovu labele
- Svi PE i P uređaji poseduju tabele parova (labela, next_hop) i prosleđuju pakete ka MPLS mreži na osnovu labela
- Labele nisu jedinstvene za neku FEC u celoj mreži, već se na svakom uređaju menjaju
- Razlike u odnosu na WAN tehnologije
  - Labele se dodeljuju na osnovu IP adresa
  - Može da postoji niz labela

16

Put paketa kroz MPLS mrežu



LSP – Label Switched Path

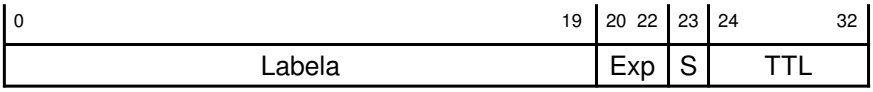
17

MPLS prosleđivanje

- Labele se najčešće dodeljuju na osnovu destinacione IP adrese paketa, ali nisu kodovane u labelu.
- Labele mogu da se dodeljuju i na osnovu drugih parametara, poput interfejsa preko kog je stigao paket, na osnovu rutera,...
- Na taj način se menja osnovna paradigma IP rutiranja koje je isključivo zasnovano na destinacionoj adresi
- U MPLS različite putanje ka istoj destinaciji mogu da imaju paketi koji su u mrežu ušli preko npr. različitih rutera ili različitih interfejsa jednog rutera
- MPLS source routing – predefinisana putanja za neku FEC

18

Format labele (RFC 3032)

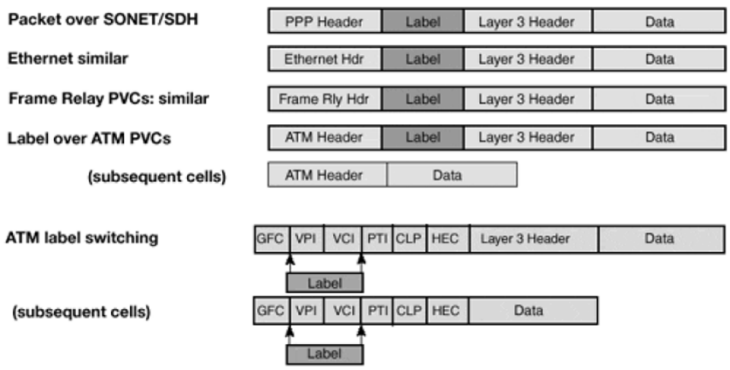


- Exp – Experimental – za organizaciju redova za čekanje
- S – Bottom of Stack bit – 0 ako iza date labele postoji još jedna labela, 1 ako nema više labela
- Labele od 0 do 15 su rezervisane
- U Labeli ne postoji polje za protokol 3. sloja enkapsuliran labelom, pa ruteri implicitno prilikom dodeljivanja labela moraju da vode računa o tome da je za određene labele enkapsuliran određeni protokol 3. sloja

19

Zašto Multiprotocol?

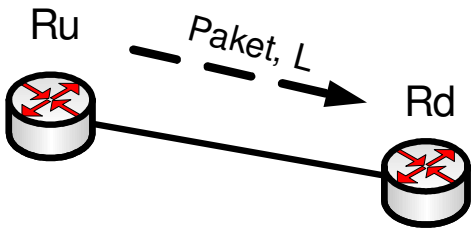
- Labela se smešta između protokola 2. i 3. sloja



20

MPLS terminologija

- LSR – Label Switching Router
- Ru – Upstream ruter
- Rd – Downstream ruter
- Labela L je outgoing za Ru, a incoming za Rd
- Ru i Rd moraju da se slože da određena L odgovara nekoj FEC kako bi znali način na koji će da izvrše label switching



21

Dodeljivanje labela

- Labelu nekoj FEC dodeljuje ruter bliži destinaciji (downstream)
- Labele nakon toga propagiraju ka upstream ruterima
- Labele su “downstream asigned”
- Labele mogu da imaju pridružene i atribute
- Ruteri informišu jedan drugog o načinu povezivanja FEC i labele putem različitih protokola:
  - LDP
  - MPBGP
  - RSVP

22

Label Distribution Protocol – LDP (RFC 3036)

- LDP koristi TCP protokol po portu 646
- Uspostavljaju se susedski odnosi putem Hello paketa
- Vrši se razmena labela i prefiksa
- Režimi rada LDP:
  - Unsolicited vs. On demand
  - Independent vs. Ordered control
  - Liberal retention vs. Conservative retention
- Dozvoljene su različite kombinacije režima rada

23

Unsolicited vs. On demand

- *Unsolicited* – ruter šalje svoje parove (FEC (prefiks),labela) svim susednim ruterima, bez pitanja. Ruter poredi next hop rute u svojoj ruting tabeli sa ruterom od kog je dobio par. Ukoliko je par dobijen od next hop rutera za dati prefiks (a to je downstream ruter), labela se prihvata
- *On demand* – ruter šalje svoje parove (FEC (prefiks),labela) po zahtevu susednog rutera

24

Independent vs. Ordered control

- *Independent control* - ruter dodeljuje labele prefiksima u svojoj ruting tabeli i šalje ih bez obzira na to da li je ruter dobio mapiranje u labelu za za tu rutu od downstream rutera
- *Ordered control* – Ruter šalje svoje (FEC,labela) parove samo za one FEC za koje ima mapiranje dobijeno od downstream rutera

25

Liberal retention vs. Conservative retention

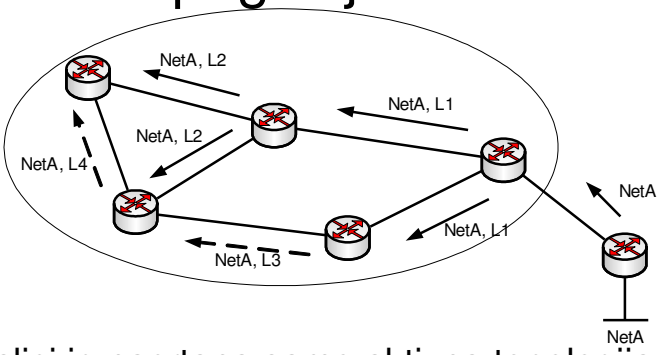
- *Liberal retention* – ruter čuva sve parove (FEC, Labela) dobijene od svih suseda, a prosleđuje pakete na osnovu labela dobijenih od nizvodnog rutera
- *Conservative retention* - ruter čuva samo one parove (FEC, Labela) dobijene od downstream suseda za dati FEC (od Next Hop)
- *Liberal* – više memorije, brza konvergencija
- *Conservative* – manje memorije, sporija konvergencija

26

Frame-mode MPLS

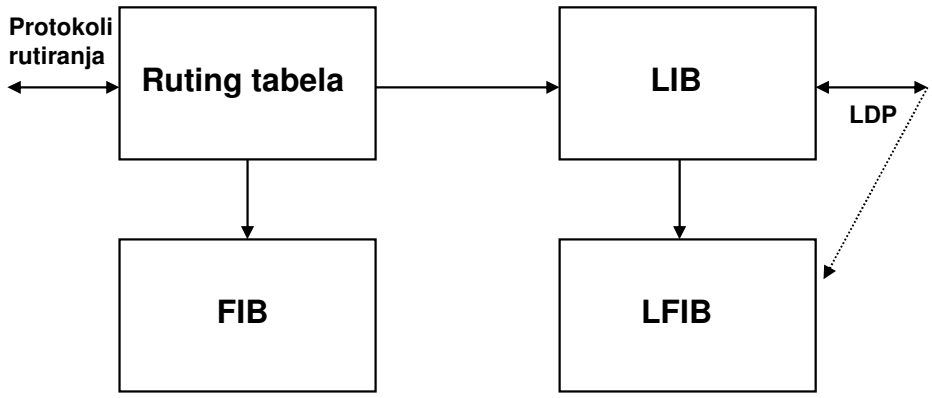
- Režim kada se MPLS koristi kao zamena za klasično destination based rutiranje
- MPLS se čvrsto oslanja na IP rutiranje i interni protokol rutiranja i labele se dodeljuju na osnovu ruta u riting tabeli
- LDP mehanizam rada je najčešće: *independent control with unsolicited downstream and liberal retention*

Propagacija labela



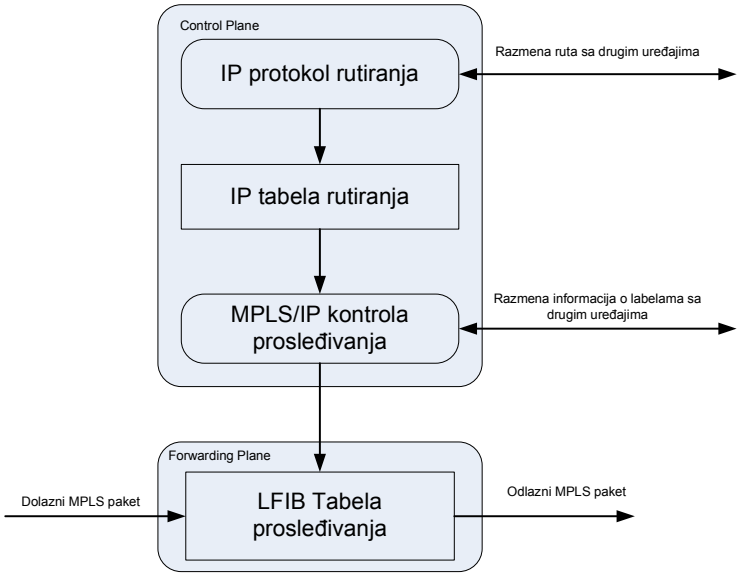
- Na slici je nacrtana samo aktivna topologija
- U stvarnosti, labele propagiraju ka svim susednim ruterima

Tabele u MPLS uređajima



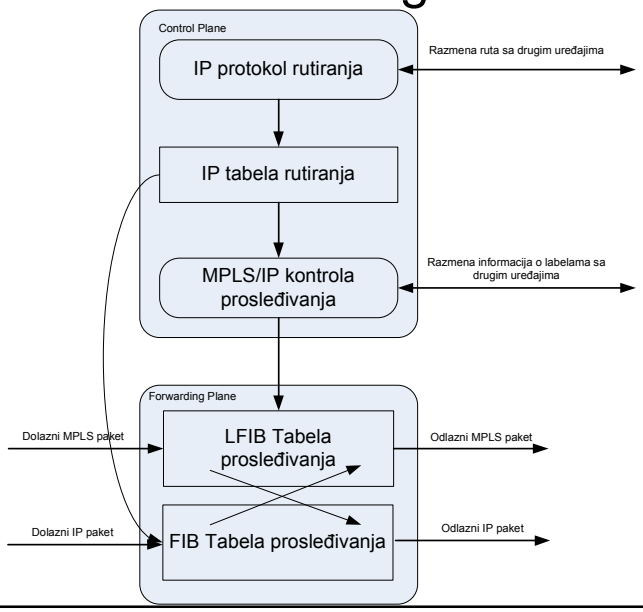
29

Arhitektura MPLS LSR rutera



30

Arhitektura MPLS Edge LSR rutera



31

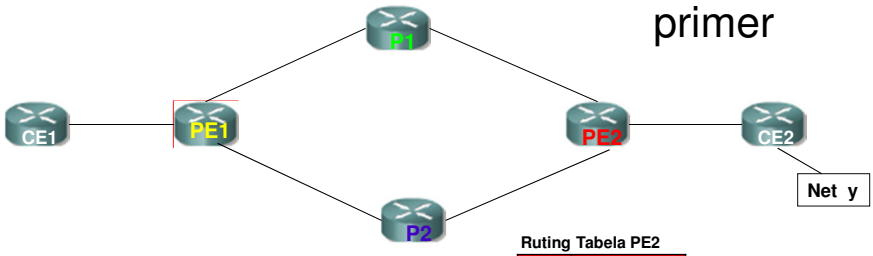
Propagacija labela - detaljan primer

Ruting Tabela PE1

Dest	Next Hop
y	P1

Ruting Tabela P1

Dest	Next Hop
y	PE2



Ruting Tabela PE2

Dest	Next Hop
y	CE2

Ruting Tabela P2

Dest	Next Hop
y	PE2

32

Ruting Tabela PE1

Dest	Next Hop
y	P1

LIB Tabela PE1

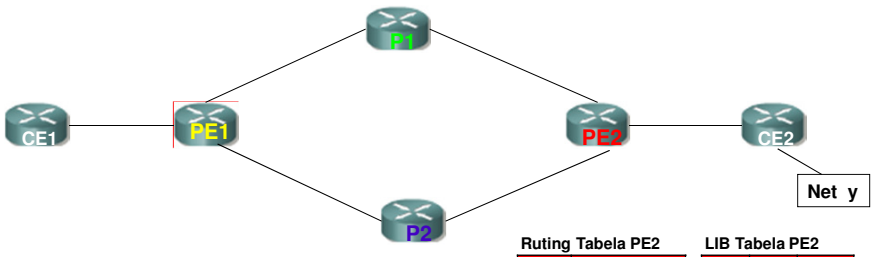
Dest	Label	LSR
y	100	Local

Ruting Tabela P1

Dest	Next Hop
y	PE2

LIB Tabela P1

Dest	Label	LSR
y	37	Local



Ruting Tabela P2

Dest	Next Hop
y	PE2

LIB Tabela P2

Dest	Label	LSR
y	56	Local

Ruting Tabela PE2

Dest	Next Hop
y	CE2

LIB Tabela PE2

Dest	Label	LSR
y	141	Local

33

Ruting Tabela PE1

Dest	Next Hop
y	P1

LIB Tabela PE1

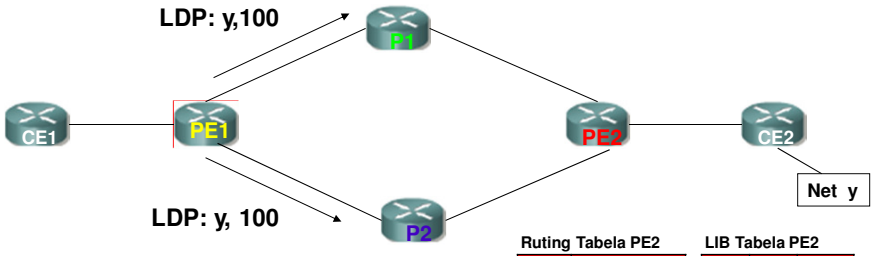
Dest	Label	LSR
y	100	Local

Ruting Tabela P1

Dest	Next Hop
y	PE2

LIB Tabela P1

Dest	Label	LSR
y	37	Local
	100	PE1



Ruting Tabela P2

Dest	Next Hop
y	PE2

LIB Tabela P2

Dest	Label	LSR
y	56	Local
	100	PE1

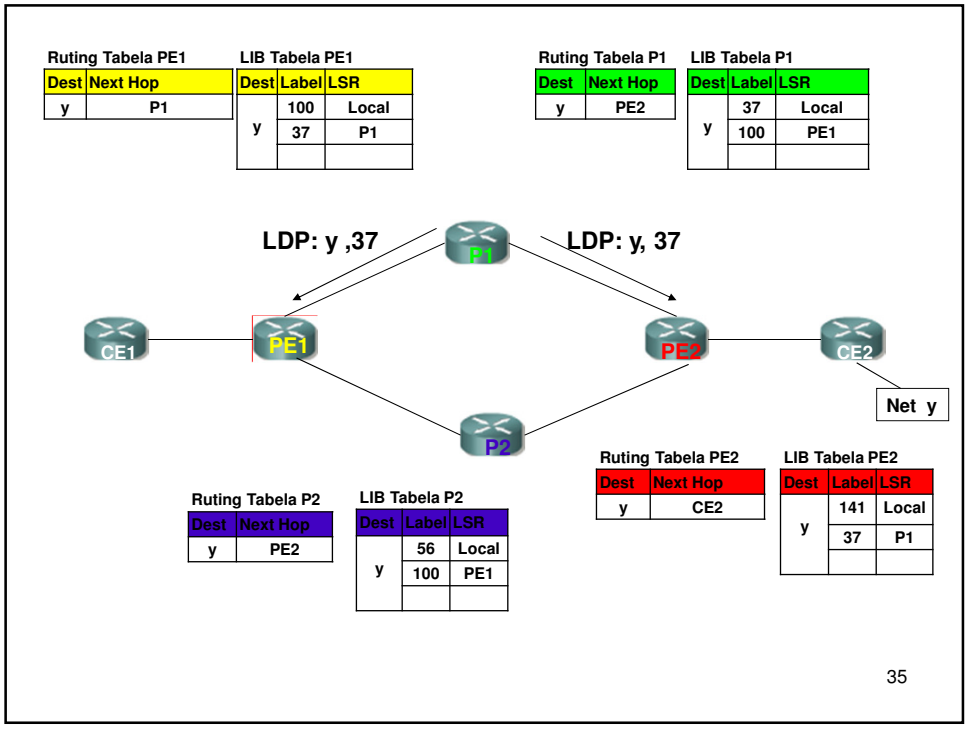
Ruting Tabela PE2

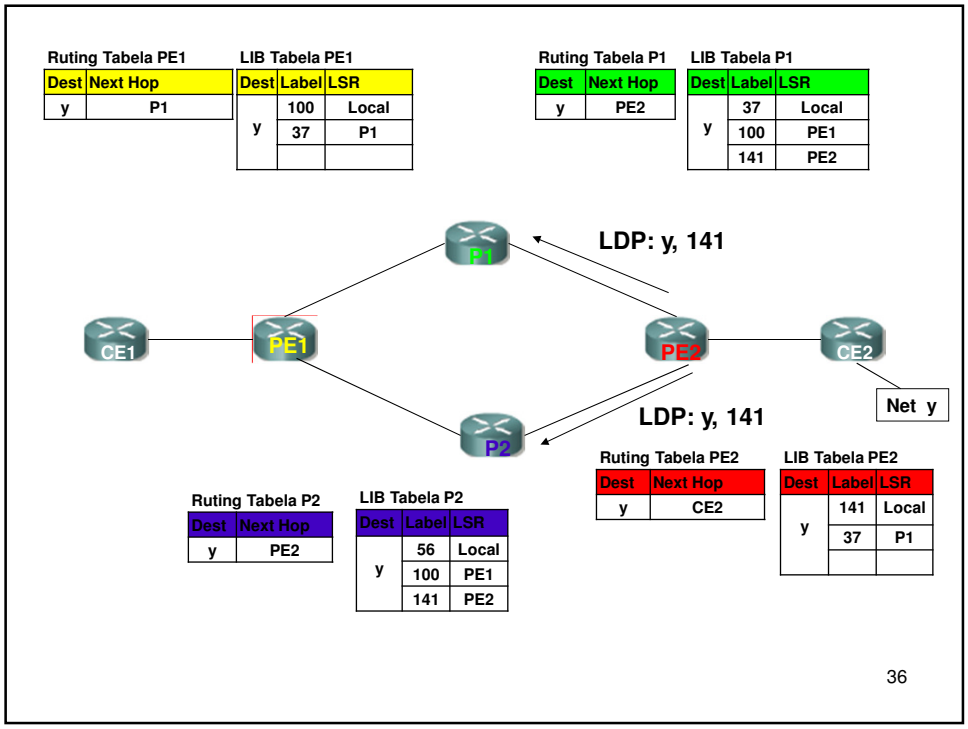
Dest	Next Hop
y	CE2

LIB Tabela PE2

Dest	Label	LSR
y	141	Local

34


Ruting Tabela PE1
Dest Next Hop
y P1
LIB Tabela PE1
Dest Label LSR
y 100 Local
37 P1
Ruting Tabela P1
Dest Next Hop
y PE2
LIB Tabela P1
Dest Label LSR
y 37 Local
100 PE1
LDP: y ,37
LDP: y, 37
P1
CE1
PE1
PE2
CE2
Net y
P2
Ruting Tabela PE2
Dest Next Hop
y CE2
LIB Tabela PE2
Dest Label LSR
y 141 Local
37 P1
Ruting Tabela P2
Dest Next Hop
y PE2
LIB Tabela P2
Dest Label LSR
y 56 Local
100 PE1
35


Ruting Tabela PE1
Dest Next Hop
y P1
LIB Tabela PE1
Dest Label LSR
y 100 Local
37 P1
Ruting Tabela P1
Dest Next Hop
y PE2
LIB Tabela P1
Dest Label LSR
y 37 Local
100 PE1
141 PE2
P1
LDP: y, 141
CE1
PE1
PE2
CE2
Net y
LDP: y, 141
P2
Ruting Tabela PE2
Dest Next Hop
y CE2
LIB Tabela PE2
Dest Label LSR
y 141 Local
37 P1
Ruting Tabela P2
Dest Next Hop
y PE2
LIB Tabela P2
Dest Label LSR
y 56 Local
100 PE1
141 PE2
36

Ruting Tabela PE1

Dest	Next Hop
y	P1

LIB Tabela PE1

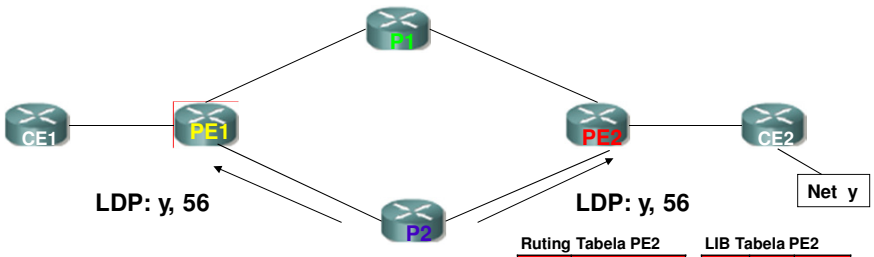
Dest	Label	LSR
y	100	Local
	37	P1
	56	P2

Ruting Tabela P1

Dest	Next Hop
y	PE2

LIB Tabela P1

Dest	Label	LSR
y	37	Local
	100	PE1
	141	PE2



Ruting Tabela P2

Dest	Next Hop
y	PE2

LIB Tabela P2

Dest	Label	LSR
y	56	Local
	100	PE1
	141	PE2

Ruting Tabela PE2

Dest	Next Hop
y	CE2

LIB Tabela PE2

Dest	Label	LSR
y	141	Local
	37	P1
	56	P2

37

Ruting Tabela PE1

Dest	Next Hop
y	P1

LIB Tabela PE1

Dest	Label	LSR
y	100	Local
	37	P1
	56	P2

Ruting Tabela P1

Dest	Next Hop
y	PE2

LIB Tabela P1

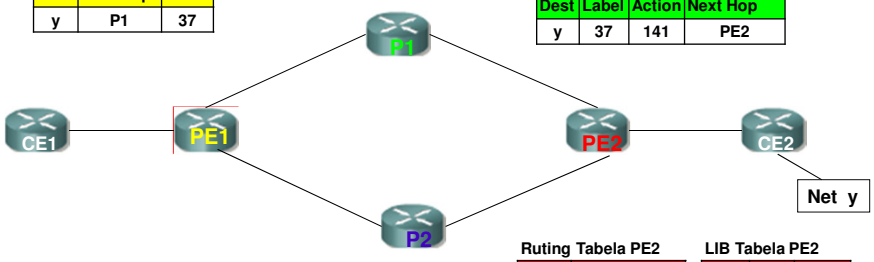
Dest	Label	LSR
y	37	Local
	100	PE1
	141	PE2

FIB Tabela Pe1

Dest	Next Hop	Label
y	P1	37

LFIB Tabela P1

Dest	Label	Action	Next Hop
y	37	141	PE2



Ruting Tabela P2

Dest	Next Hop
y	PE2

LIB Tabela P2

Dest	Label	LSR
y	56	Local
	100	PE1
	141	PE2

Ruting Tabela PE2

Dest	Next Hop
y	CE2

LIB Tabela PE2

Dest	Label	LSR
y	141	Local
	37	P1
	56	P2

LFIB Tabela PE2

Dest	Label	Action	Next Hop
y	141	POP	CE2

LFIB Tabela P2

Dest	Label	Action	Next Hop
y	56	141	PE2

38

Petlje u MPLS mreži

- *Unsolicited downstream* metod narušava *split horizon* pravilo.
- MPLS Frame mode se oslanja na protokole rutiranja koji obezbeđuju da nema petlji
- LDP poseduje mehanizam zaštite od petlji koji može da se uključi u zavisnosti od režima rada LDP
- Detekcija petlji se vrši po principu sličnom onom u BGP – uz parove (labela,prefiks) u LDP porukama mogu da se šalju *Path vector* atributi u kojima je lista svih rutera koji su oglasili dati par

39

Konvergencija MPLS mreže

- Promena ruting tabele povlači promenu u labelama (nove labele ili labele koje nestaju)
- Vreme konvergencije = vreme konvergencije IGP + vreme konvergencije LDP
- *independent control with unsolicited downstream with liberal retention* režim rada je izabran jer pruža najbržu konvergenciju

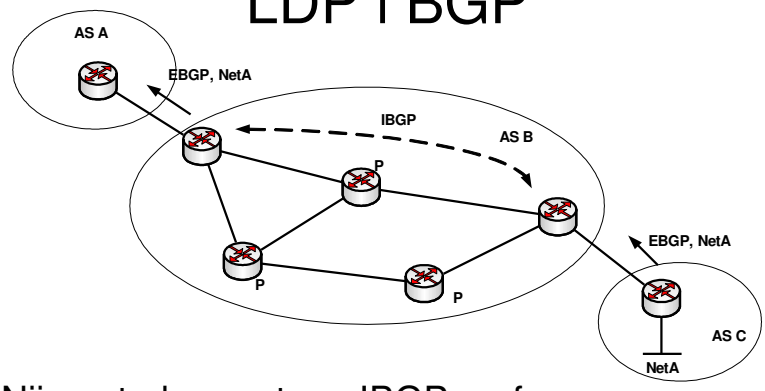
40

LDP i BGP

- **Sve rute dobijene BGP protokolom imaju istu labelu kao njihov Next hop!!!**
- BGP prefiksi nemaju svoje labele!
- P ruteri ne moraju da razmenjuju BGP rute, već je dovoljno da imaju rutu (labelu) ka Next Hop mreži

41

LDP i BGP



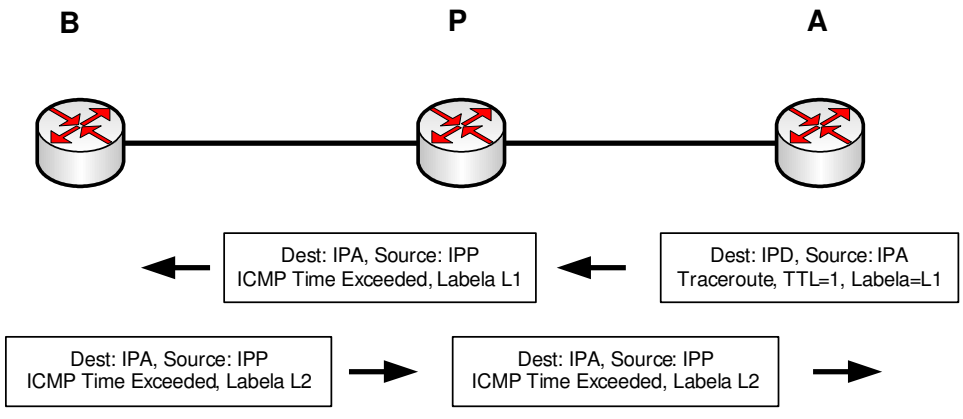
- Nije potreban potpun IBGP graf
- P ruteri ne moraju uopšte da pokreću BGP proces
- U slučaju punih Internet ruting tabela – značajna ušteda resursa

Traceroute kod MPLS

- Da bi funkcionisao traceroute mehanizam, ruteri na kome se paketi odbacuju moraju da u ruting tabeli imaju rutu kao source adresi
- Šta ako paket treba da odbaci P ruter koji nema punu ruting tabelu?
- TTL iz IP paketa mora da se preslika u TTL u labeli

43

MPLS traceroute



44

PHP

- Poslednji (*egress*) ruter MPLS mreže treba da uradi sledeće:
  - da primi paket sa određenom labelom,
  - da proveri u tabeli labela šta sa tim paketom
  - da skine labelu i da ga prosledi van mreže klasičnim IP rutiranjem (da pogleda IP ruting tabelu)
- Dvostruko gledanje u tabele – neoptimalno
- Zato je dobro da se labela skida na pretposlednjem ruteru (*Penultimate Hop Popping*), pa da se paket od pretposlednjeg do poslednjeg rutera prosledi klasičnim IP
- Poslednji ruter pretposlednjem šalje “implicit null” labelu

45

L3 VPN modeli

- Overlay
  - Provajder kreira virtuelna iznajmljena kola korisniku
  - Jasno razdvajanje PE i CE
- Peer to peer
  - PE i CE razmenjuju informacije o rutama

46

Prednosti Peer to peer modela

- Jednostavnije rutiranje (iz perspektive korisnika) – samo razmena ruta CE-PE
- Optimalno rutiranje između CE uređaja
- Jednostavnije pružanje garantovanih propusnih opsega
- Jednostavnije dodavanje nove lokacije – skalabilnost

47

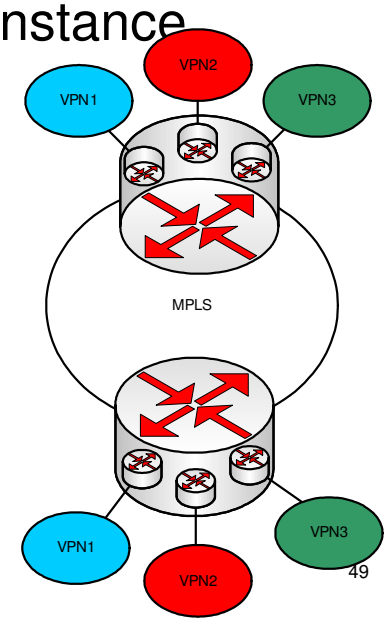
MPLS/VPN

- Kreiranje privatnih mreža preko MPLS infrastrukture
- Zahtevi:
  - Svaka privatna mreža može da ima proizvoljan skup adresa
  - Svaka privatna mreža može da ima nezavisno interno rutiranje (slanje informacija o rutama unutar jedne od lokacija)

48

VRF - VPN Routing and Forwarding instance

- VRF čuva adrese i rute iz date VPN i razmenjuje ih sa drugim VRF instancama date VPN
- Omogućavaju rad sa proizvoljnim adresnim prostorima
- Postoje na PE ruterima
- Na jednom PE ruteru može da postoji više VRF
- Interfejs PE rutera može da pripada samo jednoj VRF, odnosno, interfejs se dodeljuje određenoj VRF
- Jedna VPN može da ima jednu ili više VRF na jednom PE ruteru
- Da li VRF mogu da koriste nezavisne protokole rutiranja?



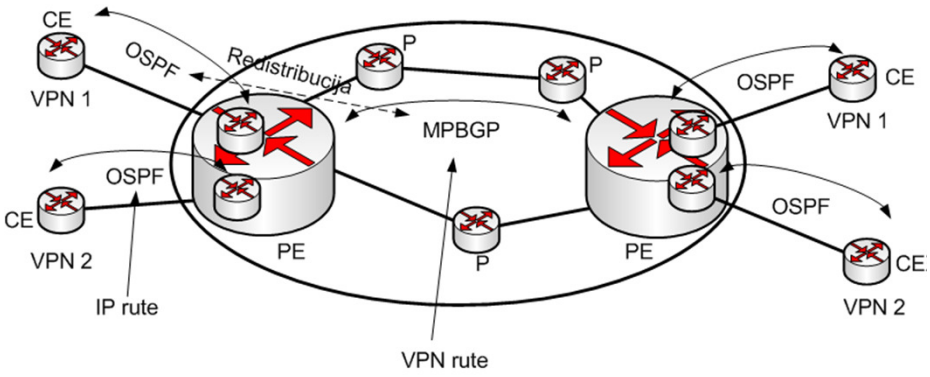
49

Route distinguisher

- PE ruteri razmenjuju korisničke rute obeležene “route distingusher”-om
- Svakom interfejsu koji je u nekoj VRF instanci se dodeljuje jedan RD
- Route distingusher je oznaka kojom se obeležavaju rute koje pripadaju pojedinoj VRF instanci ≈ VPN identifikator (jedna VPN može da ima i više RD)
- RD je 64-bitna vrednost; najčešći način označavanja ASN provajdera: broj
- RD + IP prefiks = VPN prefiks
- Korisničke rute se razmenjuju između PE rutera putem MP-BGP – najskalabilnije rešenje

50

Propagacija ruta kroz MPLS VPN

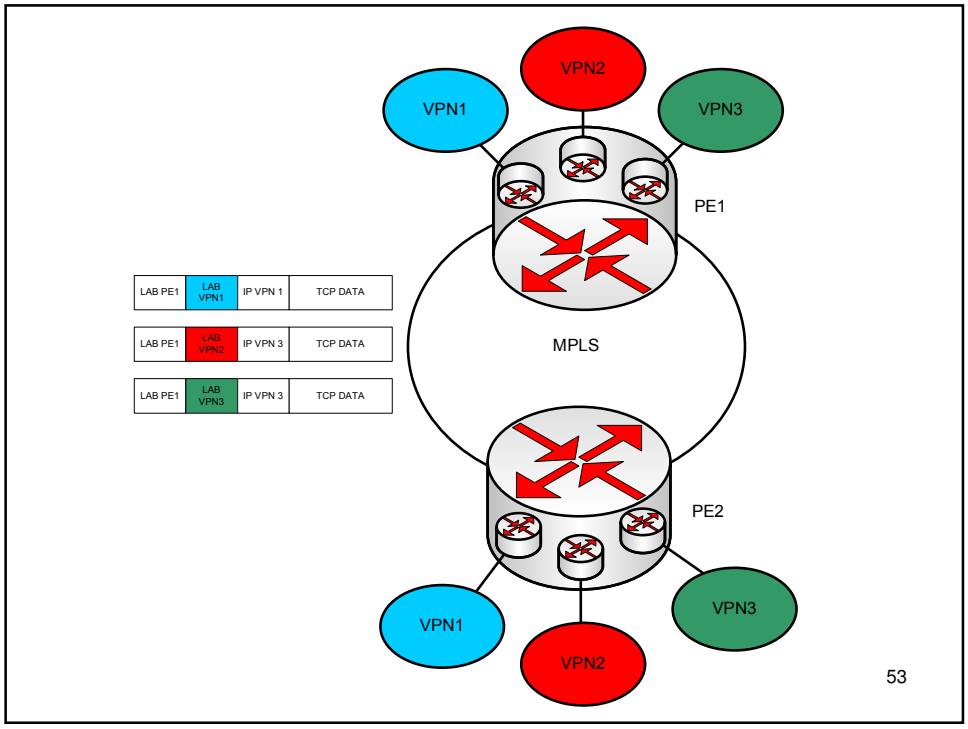


51

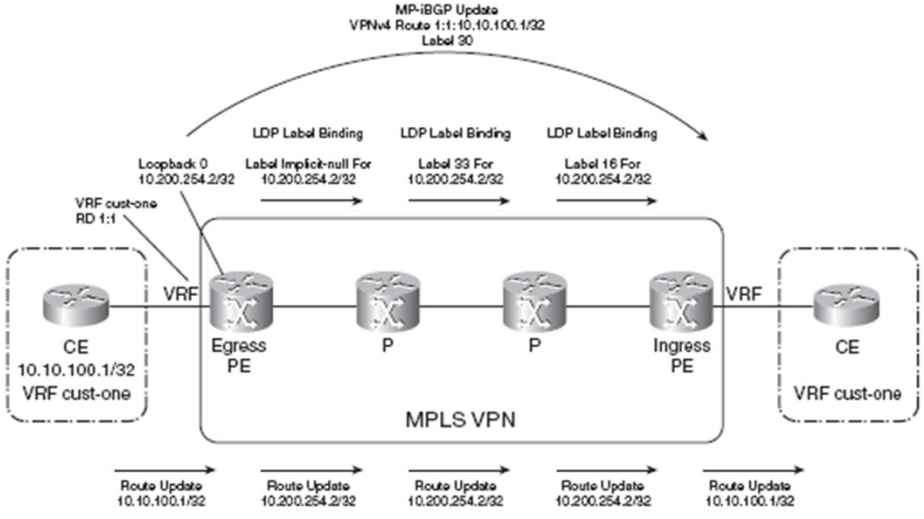
Prosleđivanje paketa

- Da bi se razlikovao saobraćaj između različitih VPN, paketi moraju da budu na neki način obeleženi
- Obeležavanje se vrši drugim setom labela, koje su enkapsulirane u labele za prenos paketa po MPLS mreži

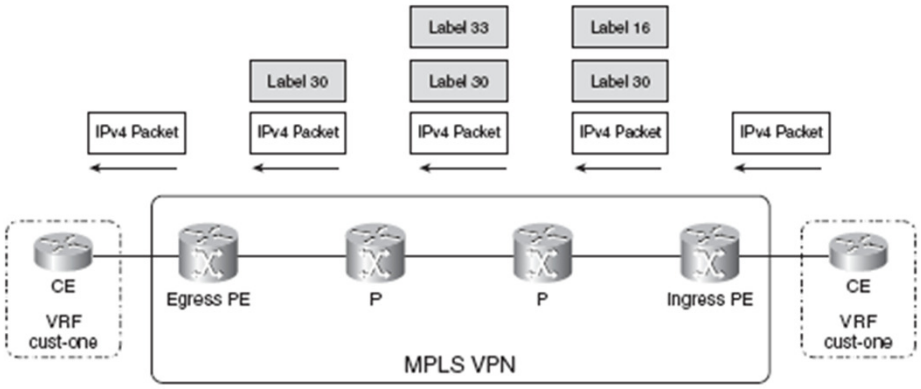
52



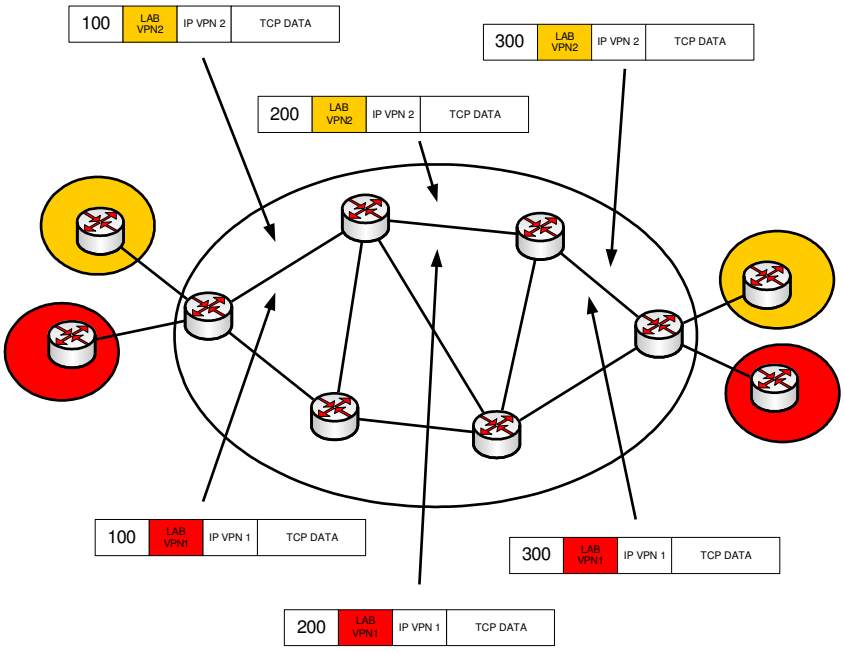
Prosleđivanje paketa – detaljno



Prosleđivanje paketa – detaljno

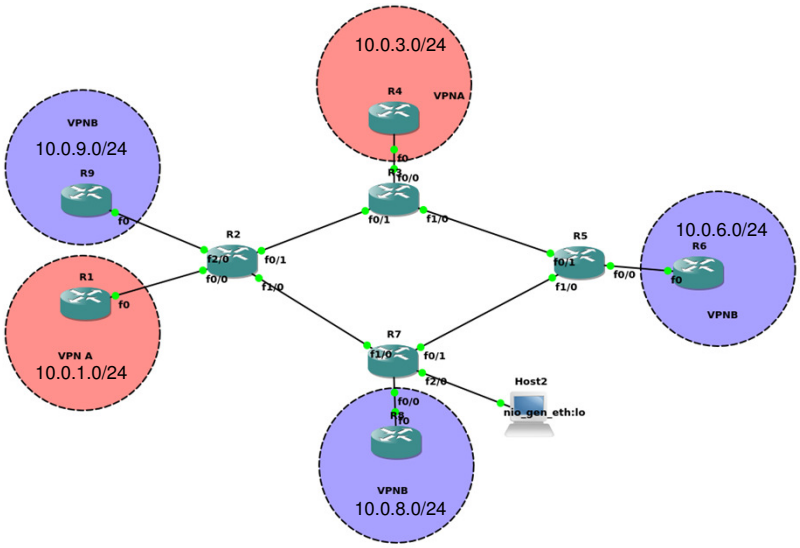


55



56

MPLS VPN primer



Konfiguracija klijentskih rutera
R9 - VPNB

```
R9#sh run
!
hostname R9
!
interface Loopback0
 ip address 10.0.9.1 255.255.255.0
!
interface FastEthernet0
 ip address 192.168.29.92 255.255.255.0
 speed auto
!
router ospf 100
 log-adjacency-changes
 network 10.0.9.0 0.0.0.255 area 0
 network 192.168.29.0 0.0.0.255 area 0
!
end
```

Ruting tabela klijentskih rutera - VPNB

```
R9#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.29.0/24 is directly connected, FastEthernet0
O IA 192.168.78.0/24 [110/2] via 192.168.29.29, 00:10:53, FastEthernet0
O IA 192.168.56.0/24 [110/2] via 192.168.29.29, 00:10:53, FastEthernet0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.9.0/24 is directly connected, Loopback0
O IA    10.0.8.1/32 [110/12] via 192.168.29.29, 00:10:53, FastEthernet0
O IA    10.0.6.1/32 [110/12] via 192.168.29.29, 00:10:53, FastEthernet0
```

Ruting tabela klijentskih rutera - VPNA

```
R1>sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, FastEthernet0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O IA    10.0.3.1/32 [110/12] via 192.168.12.21, 00:09:13, FastEthernet0
C       10.0.1.0/24 is directly connected, Loopback0
O IA 192.168.34.0/24 [110/2] via 192.168.12.21, 00:09:13, FastEthernet0
```

Konfiguracija PE rutera – R2 (1)

```
R2#sh run
hostname R2
!
!
ip vrf VPNA
 rd 65000:110
 route-target export 65000:1100
 route-target import 65000:1100
!
ip vrf VPNB
 rd 65000:120
 route-target export 65000:1200
 route-target import 65000:1200
!
interface Loopback0
 ip address 172.16.2.1 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding VPNA
 ip address 192.168.12.21 255.255.255.0
 speed auto
 full-duplex
!
interface FastEthernet0/1
 ip address 192.168.23.23 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet1/0
 ip address 192.168.27.27 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet2/0
 ip vrf forwarding VPNB
 ip address 192.168.29.29 255.255.255.0
```

Konfiguracija PE rutera – R2 (2)

```
router ospf 100 vrf VPNA
 log-adjacency-changes
 redistribute bgp 65000 subnets
 network 192.168.12.21 0.0.0.0 area 0
!
router ospf 101 vrf VPNB
 log-adjacency-changes
 redistribute bgp 65000 subnets
 network 192.168.29.29 0.0.0.0 area 0
!
router ospf 1
 log-adjacency-changes
 network 172.16.2.1 0.0.0.0 area 0
 network 192.168.23.23 0.0.0.0 area 0
 network 192.168.27.27 0.0.0.0 area 0
!
```

Konfiguracija PE rutera – R2 (3)

```
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 redistribute connected
 neighbor iBGP peer-group
 neighbor iBGP remote-as 65000
 neighbor iBGP password iBGP_Password
 neighbor iBGP update-source Loopback0
 neighbor iBGP next-hop-self
 neighbor iBGP send-community
 neighbor iBGP soft-reconfiguration inbound
 neighbor 172.16.3.1 peer-group iBGP
 neighbor 172.16.5.1 peer-group iBGP
 neighbor 172.16.7.1 peer-group iBGP
 no auto-summary
 !
 address-family vpnv4
  neighbor iBGP send-community extended
  neighbor 172.16.3.1 activate
  neighbor 172.16.5.1 activate
  neighbor 172.16.7.1 activate
 exit-address-family
```

```
 address-family ipv4 vrf VPNB
  redistribute ospf 101 vrf VPNB
  neighbor 172.16.3.1 remote-as 65000
  neighbor 172.16.3.1 update-source Loopback
  neighbor 172.16.3.1 activate
  neighbor 172.16.3.1 send-community extende
  neighbor 172.16.3.1 next-hop-self
  neighbor 172.16.5.1 remote-as 65000
  neighbor 172.16.5.1 update-source Loopback
  neighbor 172.16.5.1 activate
  neighbor 172.16.5.1 send-community extende
  neighbor 172.16.5.1 next-hop-self
  neighbor 172.16.7.1 remote-as 65000
  neighbor 172.16.7.1 update-source Loopback
  neighbor 172.16.7.1 activate
  neighbor 172.16.7.1 send-community extende
  neighbor 172.16.7.1 next-hop-self
  no synchronization
 exit-address-family
 !
```

PE ruter – ruting tabele – VPNA

```
R2#sh ip ro vrf VPNA

Routing Table: VPNA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/32 is subnetted, 2 subnets
B       10.0.3.1 [200/11] via 172.16.3.1, 00:03:05
O       10.0.1.1 [110/11] via 192.168.12.12, 00:04:06, FastEthernet0/0
B    192.168.34.0/24 [200/0] via 172.16.3.1, 00:03:06
```

PE ruter – ruting tabele - VPNB

```
R2#sh ip ro vrf VPNB

Routing Table: VPNB
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.29.0/24 is directly connected, FastEthernet2/0
B    192.168.78.0/24 [200/0] via 172.16.7.1, 00:03:24
B    192.168.56.0/24 [200/0] via 172.16.5.1, 00:03:24
     10.0.0.0/32 is subnetted, 3 subnets
O       10.0.9.1 [110/2] via 192.168.29.92, 00:04:25, FastEthernet2/0
B       10.0.8.1 [200/11] via 172.16.7.1, 00:03:24
B       10.0.6.1 [200/11] via 172.16.5.1, 00:03:24
```

PE ruter – ruting tabele

```
R2#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.27.0/24 is directly connected, FastEthernet1/0
O    192.168.57.0/24 [110/11] via 192.168.27.72, 00:04:27, FastEthernet1/0
     172.16.0.0/32 is subnetted, 4 subnets
O       172.16.5.1 [110/12] via 192.168.27.72, 00:04:27, FastEthernet1/0
                   [110/12] via 192.168.23.32, 00:04:27, FastEthernet0/1
O       172.16.7.1 [110/2] via 192.168.27.72, 00:04:27, FastEthernet1/0
O       172.16.3.1 [110/11] via 192.168.23.32, 00:04:27, FastEthernet0/1
C       172.16.2.1 is directly connected, Loopback0
C    192.168.23.0/24 is directly connected, FastEthernet0/1
O    192.168.35.0/24 [110/11] via 192.168.23.32, 00:04:28, FastEthernet0/1
O    192.168.87.0/24 [110/2] via 192.168.27.72, 00:04:28, FastEthernet1/0
```

VPN labele

```
R2#sh ip bgp vpnv4 all labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 65000:110 (VPNA)
...
Route Distinguisher: 65000:120 (VPNB)
   10.0.6.1/32      172.16.5.1      nolabel/22
   10.0.8.1/32      172.16.7.1      nolabel/21
   10.0.9.1/32      192.168.29.92   24/nolabel
   192.168.29.0     0.0.0.0         25/aggregate(VPNB)
   192.168.56.0     172.16.5.1      nolabel/23
   192.168.78.0     172.16.7.1      nolabel/22

R2#sh mpls forw
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     192.168.35.0/24  0          Fa0/1       192.168.23.32
17     Pop tag     192.168.57.0/24  0          Fa1/0       192.168.27.72
18     Pop tag     172.16.3.1/32    2344       Fa0/1       192.168.23.32
19     20          172.16.5.1/32    0          Fa1/0       192.168.27.72
       16          172.16.5.1/32    0          Fa0/1       192.168.23.32
20     Pop tag     172.16.7.1/32    0          Fa1/0       192.168.27.72
...
```

Izgled paketa ping od 10.0.9.1 ka 10.0.6.1

```
▸ Frame 18: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
▸ Ethernet II, Src: c4:02:3e:fc:00:01 (c4:02:3e:fc:00:01), Dst: c4:03:50:48:00:01 (c4:03:50:48:00:01)
▾ MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 0, TTL: 254
    0000 0000 0000 0001 0000 .... .... .... = MPLS Label: 16
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
▾ MultiProtocol Label Switching Header, Label: 22, Exp: 0, S: 1, TTL: 254
    0000 0000 0000 0001 0110 .... .... .... = MPLS Label: 22
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
▸ Internet Protocol Version 4, Src: 10.0.9.1, Dst: 10.0.6.1
▸ Internet Control Message Protocol
```

MPLS TE – RFC 2702

- Traffic Engineering – skup metoda kojima se optimalno iskorišćavaju resursi mreže
- Osnovna ideja: omogućiti da se prosleđivanje paketa vrši na osnovu
  - topologije mreže,
  - skupa ograničenja
  - raspoloživih resursa
- MPLS TE – niz mehanizama kojima se automatizuje kreiranje TE LSP

69

Atributi (ograničenja) na osnovu kojih se određuje optimalni LSP

- Destinacija
- Propusni opseg
- Afinitet (svaki link po 32 “boje”, po kašnjenju, nekoj karakteristici linka...)
- Preče pravo (Preemption)
- Optimizovana metrika
- Zaštita pomoću Fast Reroute mehanizma

70

Preče pravo (preemption)

- LSP većeg prioriteta u slučaju nedovoljnih resursa ima pravo da raskine LSP nižeg prioriteta
- Primer:
  - Ukupni propusni opseg potreban za LSP T1, T2,T3, T4 je veći od raspoloživog
  - T1 ima veći prioritet od T2, T3, T4
  - LSP sa najnižim prioritetom će biti raskinut

71

Šta ako ni jedan TE-LSP ne zadovoljava postavljene uslove?

- Može da se kreira Fallback sekvenca različitih uslova za dati TE LSP
- Poslednji tip TE LSP u ovoj sekvenci može da bude kreiranje putanje po IGP putanji
- Prilikom reoptimizacije headend ruter će ponovo pokušati da uspostavi TE LSP počev od prvog skupa uslova.

72

Optimizovana metrika

- “druga” metrika – RFC 3785
- Jedna metrika – klasična IGP metrika
- Druga metrika – metrika za CBR
- Za jedan LSP se putanja određuje na osnovu jedne od ove dve metrike
- Pronalaženje optimalne putanje po obe metrike istovremeno je NP-potpun problem

73

Određivanje TE LSP

- Offline
  - LSP se izračunava van rutera i implementira na njima
  - Optimalne putanje
- Online
  - Sami ruteri izračunavaju najbolje LSP (CSPF)
  - Neoptimalne putanje
  - Otporno na promene u mreži
  - Skalabilnije

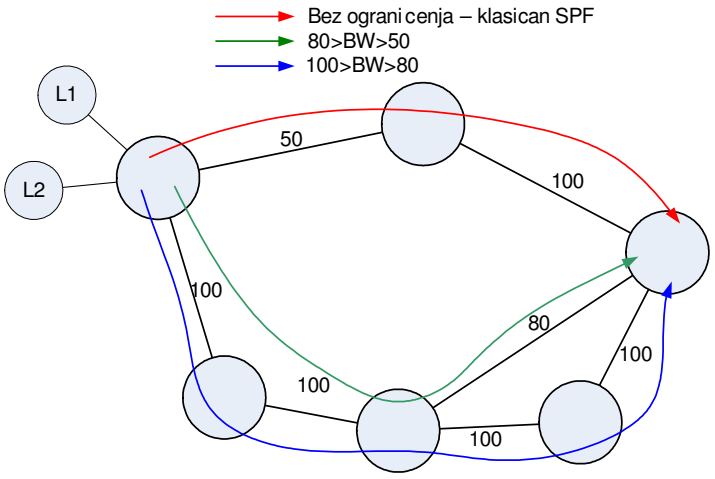
74

CSPF, CBR

- CBR – Constrained Based Routing
- CSPF - Constrained Shortest Path First
- Ne postoji definisan standard
- Postoje ekstenzije za OSPF i ISIS
- Princip:
  - Dijkstra algoritam se primenjuje na osnovni graf iz kog su izbačene grane koje ne zadovoljavaju neki kriterijum
  - Između ostalih grana se bira ona sa najmanjim cost-om
  - Ako postoji više putanja bira se ona sa najvećim minimalnim propusnim opsegom
  - Ako to ne razreši, bira se ona sa najmanjim brojem hopova
  - Ako to ne razreši, bira se nasumično

75

CSPF



76

TE ekstenzije ruting protokola

- Na svim linkovima administratori konfigurišu koliko propusnog opsega može da se zauzme LSP-ovima
- Svaki novi LSP sa određenim zahtevom za propusnim opsegom izaziva promenu slobodnog propusnog opsega na nekom linku => LSA se generiše => novo Dijkstra izračunavanje
- Zato postoji mehanizam kojim se ne reaguje na male promene slobodnog propusnog opsega
- “Headend” ruter može da ima netačnu sliku o zauzeću propusnog opsega u mreži

77

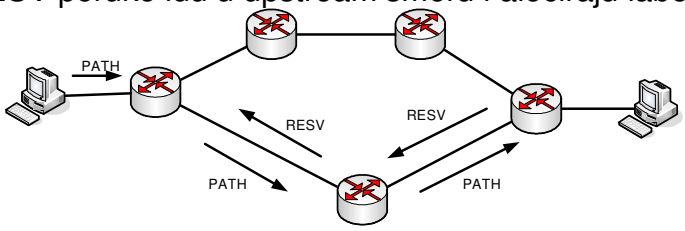
OSPF-TE

- RFC 3630
- Nova vrsta LSA – Tip 10, koja se razmenjuje unutar jedne oblasti
- LSA tip 10 nosi nove atribute za svaki link:
  - 1 - Link type (1 octet)
  - 2 - Link ID (4 octets)
  - 3 - Local interface IP address (4 octets)
  - 4 - Remote interface IP address (4 octets)
  - **5 - Traffic engineering metric (4 octets) – TE metrika**
  - **6 - Maximum bandwidth (4 octets) – BW linka**
  - **7 - Maximum reservable bandwidth [bps] (4 octets) – adm konfiguriše**
  - **8 - Unreserved bandwidth (32 octets) – 8 vrednosti za 8 preempt prioriteta**
  - **9 - Administrative group (4 octets) – afinitet, boja**

78

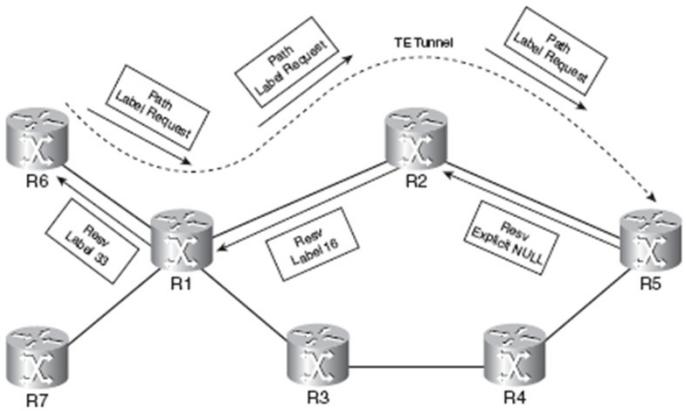
Uspostavljanje TE-LSP

- RSVP – Resource reSerVation Protocol – IntServ QoS arhitektura
- Koristi se ekstenzija RSVP protokola – RSVP-TE
- PATH poruke idu u downstream smeru, sa posebnim poljem LABEL_REQUEST u kojem su opisani parametri (ograničenja) zahtevanog LSP
- RESV poruke idu u upstream smeru i alociraju labele



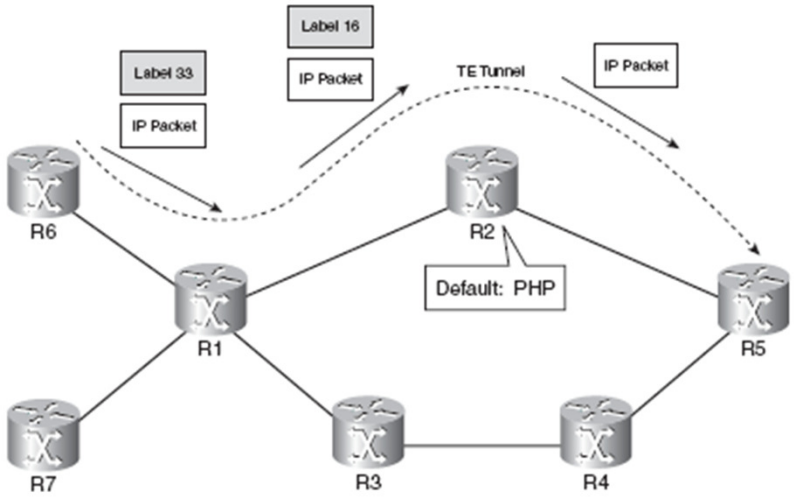
79

Uspostavljanje TE-LSP



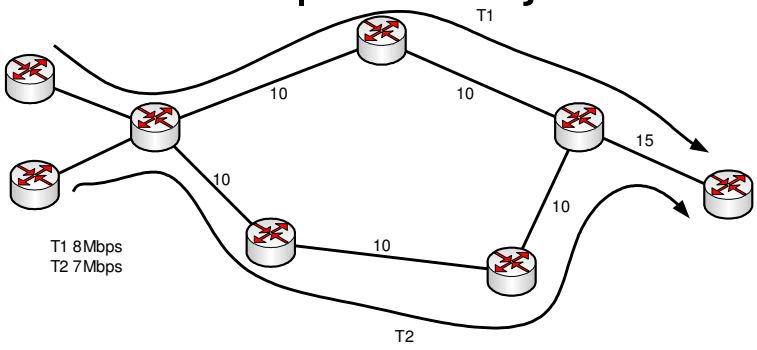
80

Prosleđivanje Paketa



81

Reoptimizacija



- Ako nestane T1, T2 će preći na kraću putanju
- MPLS TE ima "*make-before-brake*" optimizaciju
- Postoji mehanizam koji sprečava "*double booking*"
- Reoptimizacija može da se pokrene ručno, po isteku nekog tajmera, nakon nekog događaja

82

Fast reroute

- Mehanizam kojim se omogućava brzo pronalaženje alternativne putanje (LSP)
- Alternativni LSP se formira prilikom formiranja primarnog LSP
- Vreme prebacivanja – nekoliko desetina ms

83

L2TP

- Layer 2 Tunneling Protocol
- Nastao iz L2F i PPTP protokola
- Najnovija verzija L2TPv3 (RFC 3931)
- Služi za prenos različitih L2 tehnologija preko IP mreža
  - Ethernet
  - 802.1q
  - Frame Relay
  - HDLC
  - PPP

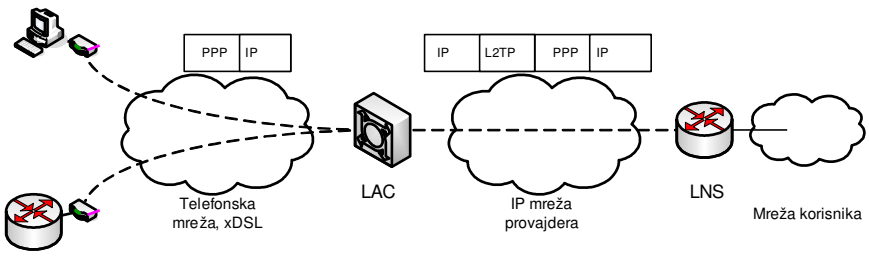
84

L2TP primena “compulsory remote access VPN”

- Može da služi za pružanje ADSL ili dial-VPN usluge
- PPP sesija se od pojedinačnog korisnika produžuje do destinacione mreže kako bi se obezbedila autentifikacija i drugi servisi koje pruža PPP
- Uređaji koji učestvuju u stvaranju tunela:
  - LAC - L2TP Access Concentrator
  - LNS – L2TP Network Server

85

Osnovni mehanizam funkcionisanja compulsory remote access VPN



86

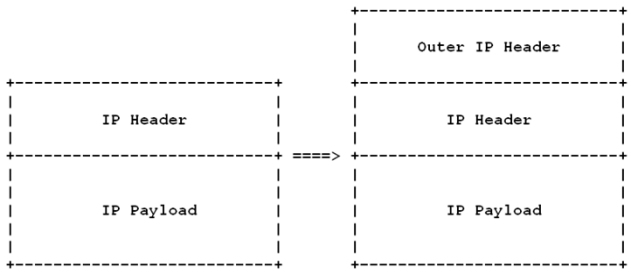
L2TPv3

- Sa omogućavanjem prenosa različitih L2 tehnologija omogućeno je i stvaranje site-to-site L2 VPN preko IP mreža – L2TPv3 pseudowire
- L2TPv3 pseudowire može da prenosi ne-IP saobraćaj (AppleTalk, IPX)
- L2TPv3 pseudowire može da se koristi kao mehanizam za tranziciju na IPv6

87

IP in IP – RFC 2003

- Namenjen za korišćenje u Mobile IP



88

Mobile IP

- Home address: adresa iz matične mreže
- Care-of address: adresa u novoj mreži
  - Foreign Agent CoA (svi mobilni čvorovi u stranoj mreži imaju istu CoA)
  - Collocated CoA (mobilni čvorovi u stranoj mreži imaju različite adrese)
- Home agent: ruter u matičnoj mreži
  - Mobility binding table: parovi (home,care-of)
- Foreign agent: ruter u novoj mreži
  - Visitor table: parovi(home address, home agent)

89

Pronalaženje agenata

- Mobilni agenti oglašavaju svoje prisustvo periodičnim broadcast-om Agent Advertisement poruka. Agent Advertisement poruke sadrže jednu ili više care-of adresa.
- Mobilni uređaj koji prima Agent Advertisement može da otkrije da li je u pitanju home ili foreign agent tj da li je u svojoj ili stranoj mreži.
- Ako mobilni uređaj ne želi da čeka na periodične Agent Advertisment poruke, može da pošalje svoje Agent Solicitation poruke, kako bi inicirao slanje poruka od strane agenata.

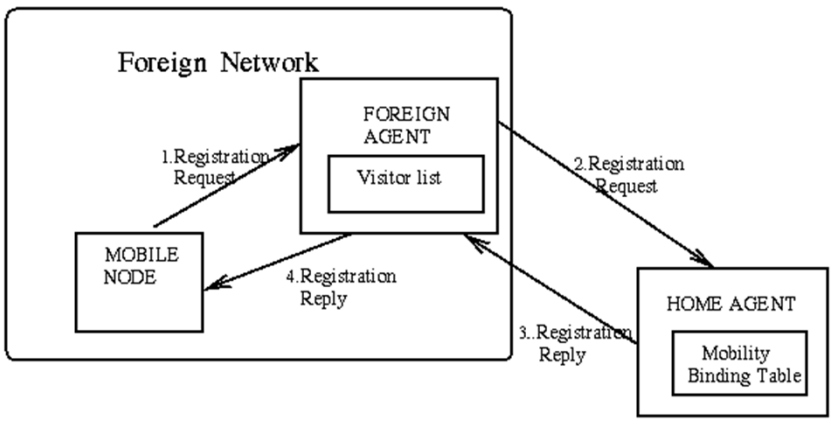
90

Registracija

- Ako je mobilni uređaj na svojoj mreži, nastaviće da komunicira bez korišćenja IP mobility mehanizma.
- Ako je mobilni uređaj na stranoj mreži, registruje svoje prisustvo kod stranog agenta slanjem Registration Request poruka u kojima je home adresa mobilnog uređaja i IP adresa njegovog home agenta.
- Foreign agent prosleđuje registracione poruke ka home agentu mobilnog uređaja i u te poruke dopisuje Care-of adresu koja se koristi u komunikaciji sa mobilnim uređajem
- Home agent kada primi registracionu poruku upisuje uz IP adresu mobilnog uređaja novu Care-of adresu za njega.
- Home agent šalje acknowledgement foreign agentu i počinje da prosleđuje pakete ka mobilnom uređaju.
- Foreign agent prosleđuje odgovor mobilnom uređaju.

91

Proces registracije



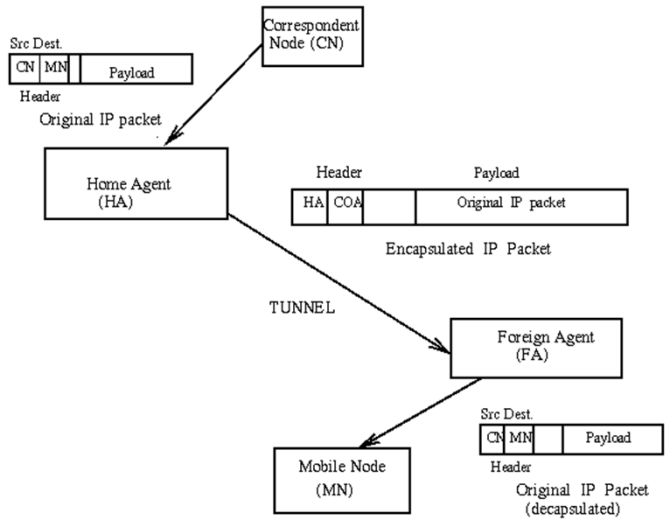
92

Tok komunikacije

- Računari šalju pakete na home adresu.
- Home agent presreće pakete i u mobility binding tabeli proverava da li je mobilni uređaj u svojoj mreži ili nije.
- Kada mobilni uređaj nije u svojoj matičnoj mreži, home agent vrši IP in IP tunelovanje i u spoljašnje zaglavlje kao source adresu stavlja svoju adresu, a kao destinacionu care-of adresu.
- Kada enkapsulirani paket dođe do care-of adrese (agent ili sam uređaj), dekapsulira se i prosleđuje do mobilnog uređaja.
- U suprotnom smeru paketi mogu da se šalju direktno ka uređaju sa kojim se komunicira, a mogu i da se vrate kroz tunel do home agenta.

93

Tok komunikacije



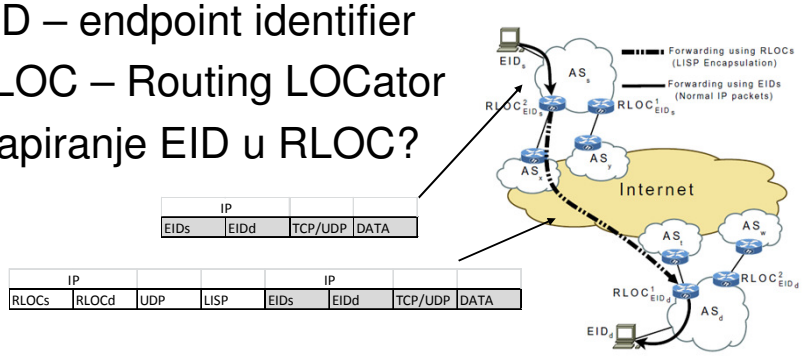
94

(LISP)

- Locator/ID Separation Protocol (RFC 6830 – januar 2013)
- „*dirty slate*“ pristup promeni arhitekture Interneta (za krajnjeg korisnika nema nikakvih izmena)
- Namenjen da reši:
  - problem broja ruta na Internetu
  - multihoming
  - mobilnost

(LISP)

- EID – endpoint identifier
- RLOC – Routing LOCator
- Mapiranje EID u RLOC?

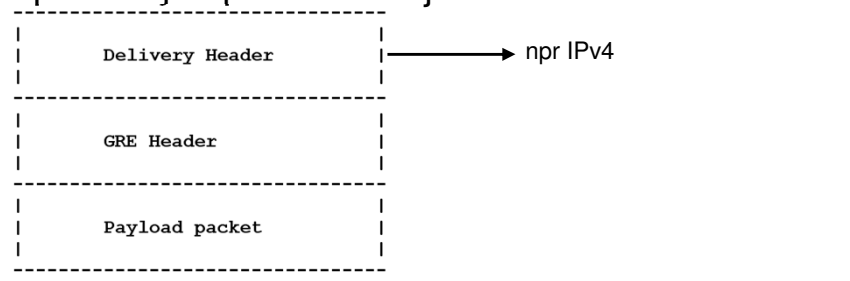


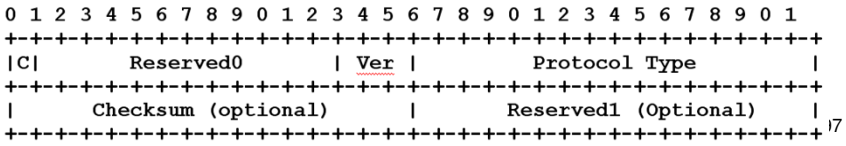
- Internet ruting tabela – tabela RLOC

Slika preuzeta iz: Iannone, L., Saucez, D., & Bonaventure, O. (2010). Implementing the Locator/ID Separation Protocol: Design and experience. *Computer Networks*, *55*(4), 948–958. doi:10.1016/j.comnet.2010.12.017

GRE – RFC 2784

- GRE – Generic routing encapsulation
- Proizvoljni paketi 3. sloja se enkapsuliraju u proizvoljne pakete 3 sloja





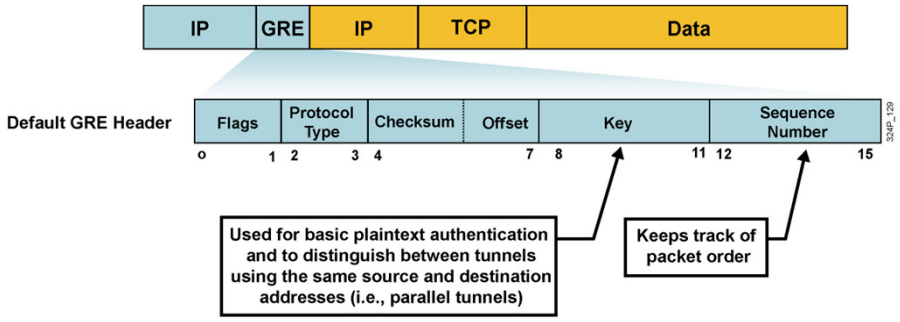
[7]

Osnovno GRE zaglavlje
GRE flag-ovi

- GRE flagovi i polja:
  - –Checksum Present (bit 0)
  - –Key Present (bit 2)
  - –Sequence Number Present (bit 3)
  - –Version Number (bits 13–15): 0 najčešće, 1 za PPTP
  - –Protocol Type

98

Opcione GRE ekstenzije



- GRE keepalive – za proveru rada tunela

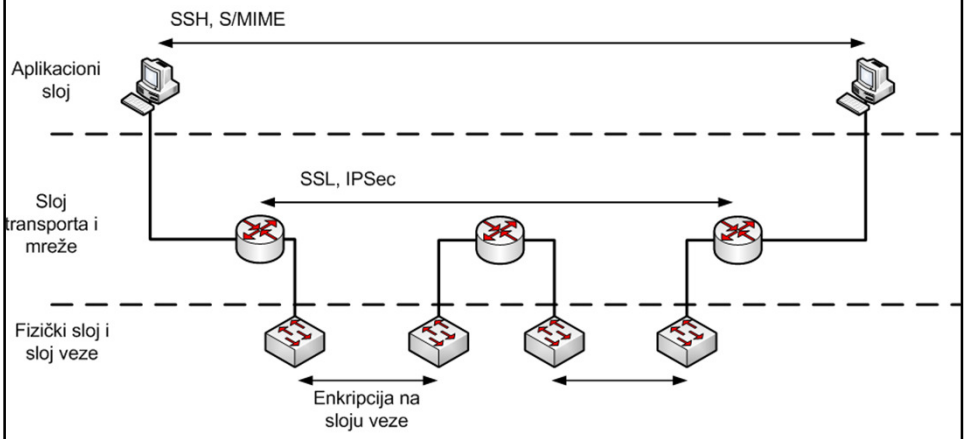
99

Secure VPN funkcije

- **Secure VPN ima sledeće funkcije:**
  - **Poverljivost** – Poverljivost podataka se dobija kriptovanjem sadržaja paketa.
  - **Integritet podataka** – Integritet podataka se čuva nekim mehanizmom koji potvrđuje da podaci u paketu nisu menjani tokom njegovog prolaza kroz Internet
  - **Autentikacija porekla** – Destinacija vrši autentikaciju pošiljaoca kako bi se osigurala da pakete dobija od odgovarajućeg izvora.

100

Zaštita saobraćaja na različitim OSI slojevima



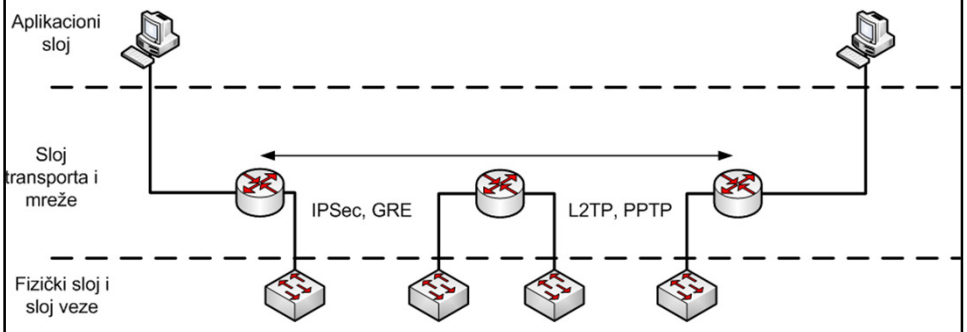
101

Zaštita saobraćaja na različitim OSI slojevima

- Data link sloj: zaštita postoji samo na jednom mrežnom segmentu, ali je zaštićen svaki paket na tom segmentu
- Aplikacioni sloj: Zaštićen je dati protokol aplikacionog sloja s kraja na kraj
- Mrežni sloj: Zaštićen je sav saobraćaj s kraja na kraj

102

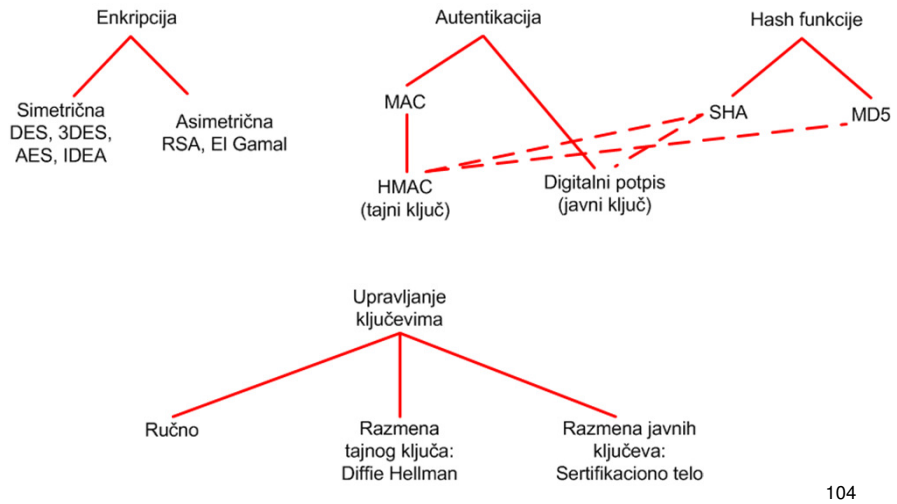
Protokoli za tunelovanje na OSI L3



VPN Protocols	Description	Standard
L2TP	Layer 2 Tunneling Protocol	RFC 2661
GRE	Generic Routing Encapsulation	RFC 1701 and 2784
IPSec	Internet Protocol Security	RFC 2401

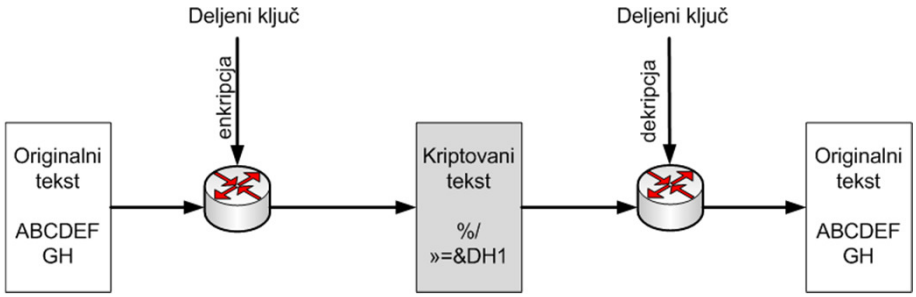
103

Kripto-mehanizmi pregled



104

Simetrična enkripcija



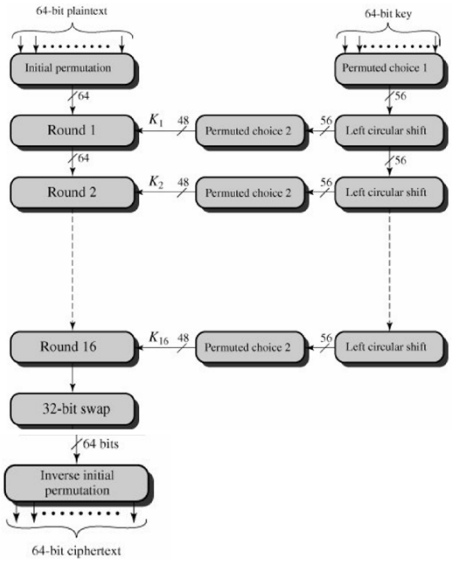
105

Algoritmi simetrične enkripcije

- DES vrši enkripciju 64-bitnih blokova.
- Sa današnjim računarima moguće je razbijanje DES enkripcije za nekoliko dana
- 3DES koristi dvostruku dužinu ključa (112 bita) i izvodi tri DES operacije za redom
- Advanced Encryption Standard (AES) je trenutno aktuelan standard za simetrično kriptovanje ključevima različite veličine 128, 192 ili 256 bita kojima se kriptuju blokovi dužine 128, 192 ili 256 bits (moguće su sve kombinacije dužine ključa i veličine blokova)
- Drugi simetrični algoritmi: IDEA,

106

DES



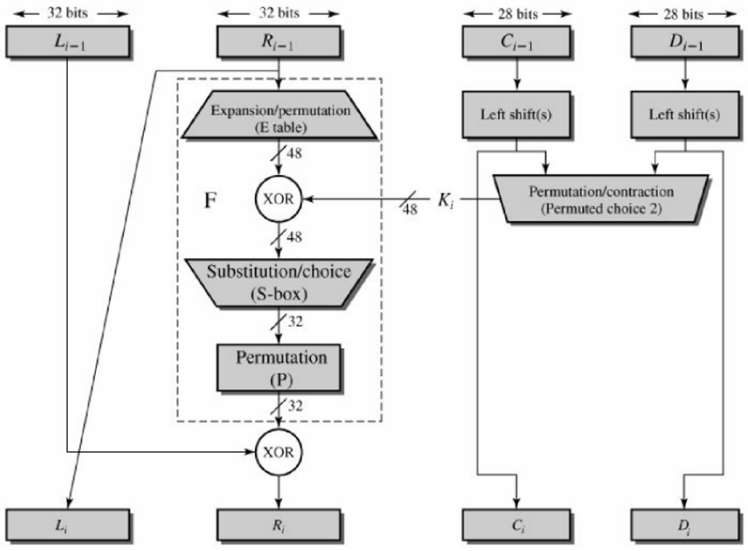
107

DES inicijalna permutacija

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

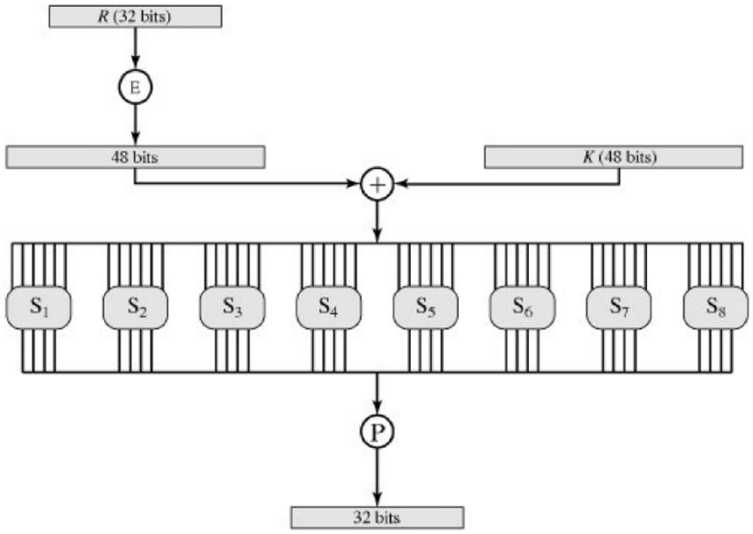
108

Jedan krug DES algoritma



109

DES F(R,K)



110

DES S-BOX

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

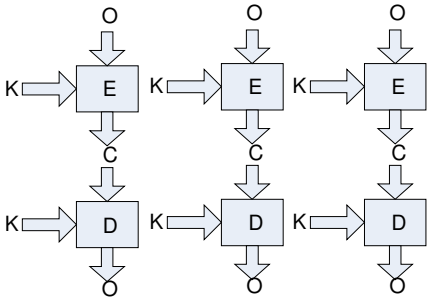
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

111

DES načini rada

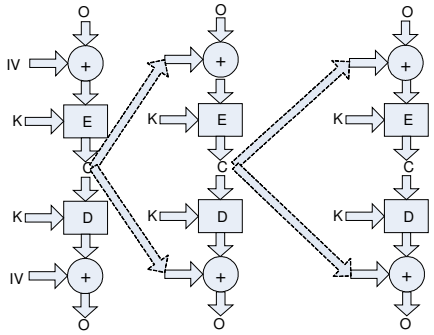
- Electronic Codebook Mode (ECB)
- Svaki blok se nezavisno enkriptuje/dekriptuje
- Relativno nesiguran način za duže poruke/pakete
- Isti originalni blok – isti kriptovani blok



112

DES načini rada

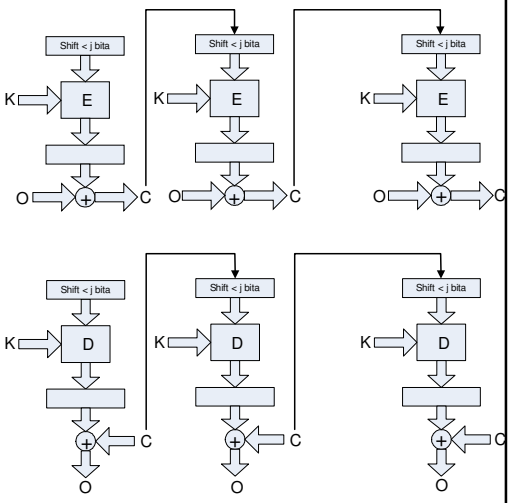
- Cipher Block Chaining (CBC)
- Isti blok originalnog teksta ne proizvodi isti kriptovani tekst
- IV mora bezbedno da se razmeni, kao ključ



113

DES načini rada

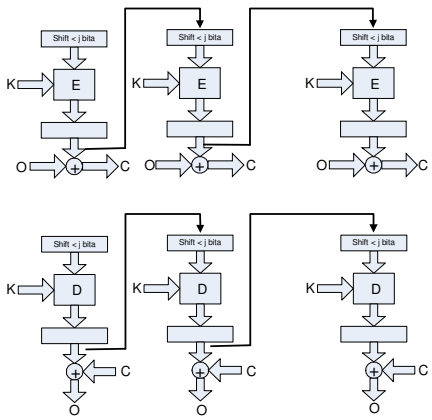
- Cipher Feedback (CFB)
- J – jedinica prenosa – obično 8 bita
- Stream režim rada (nema paddinga) – ista dužina originalnog i kriptovanog teksta
- Registri na početku imaju IV



114

DES načini rada

- Output Feedback (OFB)
- Slično kao CFB
- Stream algoritam



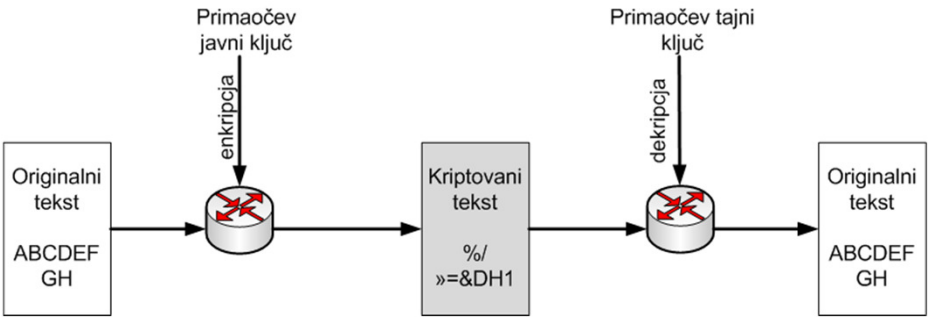
115

3DES

- 2DES se ne primenjuje zbog Meet-in-the-middle napada:
  - $C=E_{K1}(E_{K2}(O))$ – ukupna dužina ključa 2xn – 2^{2n} broj pokušaja
  - Ako napadač poznaje C i O, može da proba da napravi $E_{Kn}(O)$ i $D_{Kn}(C)$ sa sve kn i da ih upari – 2^{n+1} pokušaja
- Varijante 3DES:
  - EEE $C=E_{k3}(E_{k2}(E_{k1}(O)))$ – 168 bita
  - EDE $C=E_{k3}(D_{k2}(E_{k1}(O)))$
  - EDE – 2DES - $C=E_{k1}(D_{k2}(E_{k1}(O)))$ – 112 bita

116

Asimetrična ekripcija



Najpoznatiji algoritmi asimetrične enkripcije su RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) i El Gamal algoritam.

117

RSA

- Izaberu se dva velika prosta broja *p* i *q*
- *n=pq*
- Totient*: phi=(p-1)(q-1)*
- Pronađe se ceo broj *e* takav da je *1<e<phi* i *e* i *phi* su uzajamno prosti
- ***e* je javni ključ**
- Izračuna se *d* takvo da je *de=1mod(phi)*
- ***d* je privatni ključ**

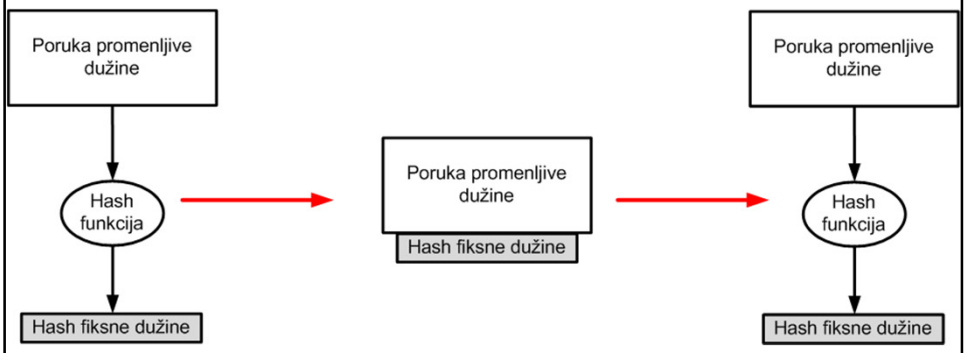
118

RSA kriptovanje i dekriptovanje

- Kriptovanje:
  - $c=m^e \bmod n$
- Dekriptovanje
  - $m=c^d \bmod n$
- Primer
  - p=61, q=53 => n=3233, phi=3120
  - e=17 => d=2753
  - c=123 => $c=123^{17} \bmod 3233 = 855 = m$
  - $m=855^{2753} \bmod 3233 = 123$
- Realni RSA ključevi 1024 bita i više

119

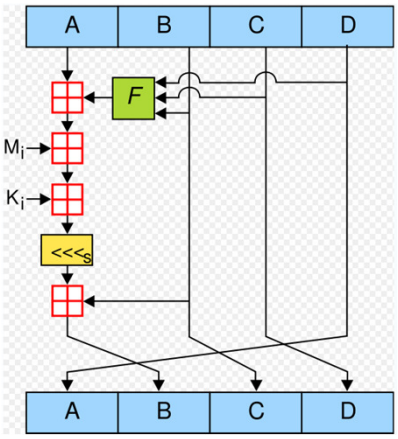
Hash funkcije primena



120

MD5 – RFC1321

- Poruka mora da bude nx512 bita
- 128 bit hash
- A,B,C,D – 32 bita
- <<< Left shift
- + - sabiranje po modulu 2^{32}
- F – F,G,H,I – 4 runde za svaki blok od 128



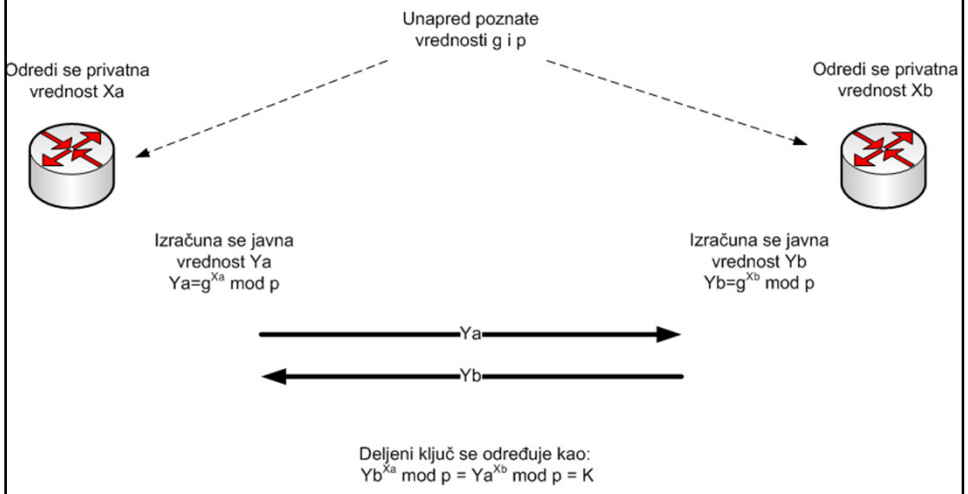
$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

Hashing algoritmi

- Dva najrasprostranjenija hash algoritma: MD5 i SHA
- HMAC verzije – sa ključem:
  - **HMAC-MD5** – Koristi 128-bit ključ. Izlaz je 128-bit hash.
  - **HMAC-SHA-1** – Koristi 160-bit ključ. Izlaz je 160-bit hash.

122

Razmena ključeva – Diffie-Hellman



123

Razmena ključeva – Diffie-Hellman

p i g su prosti brojevi, g je obično 2, a p je veliki (pseudo)prost broj.

Primer: p=11, g=2, Xa = 9, Xb = 4.

$Ya = 2^9 \pmod{11}$

$Ya = 6$

$K=Yb^{Xa} \pmod{11}$

$K=5^9 \pmod{11} = 1953125 \pmod{11}$

$K=9$

$Yb=2^4 \pmod{11}$

$Yb=5$

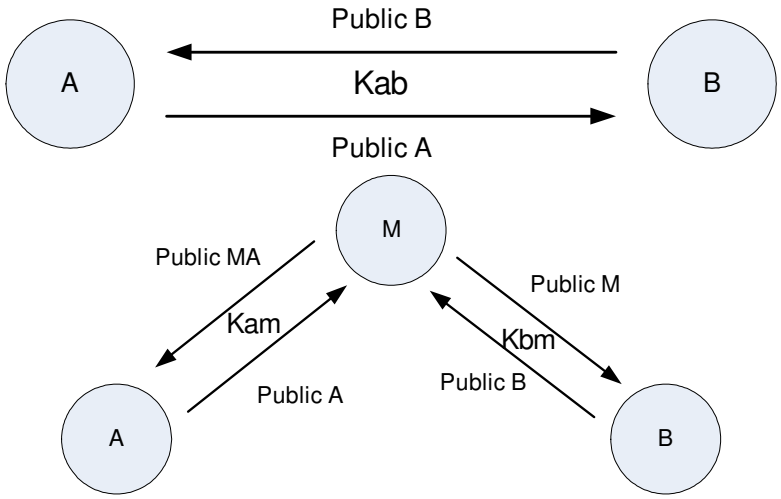
$K=Ya^{Xb} \pmod{11}$

$K=6^4 \pmod{11} = 1296 \pmod{11}$

$K=9$

124

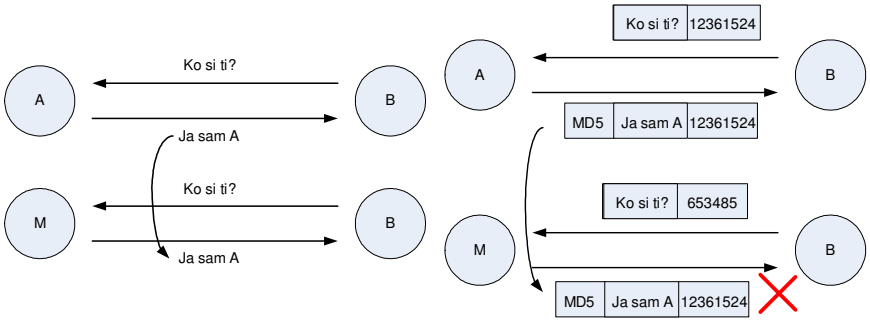
DH problem: Man-in-the-middle



Odbrana: jaka autentikacija A i B, enkripcija materijala simetričnim ili privatnim ključem,...

125

Replay napad



Odbrana: postojanje pseudo-slučajnih “session token”-a ili “nonce”-a

126

Gde se koriste algoritmi za kriptovanje

- Ključevi asimetričnih algoritama su mnogo duži od ključeva simetričnih i njihovo izvršavanje je za više redova veličine sporije.
- Približno: simetričnom algoritmu sa ključem dužine 64 bita odgovara asimetrični algoritam sa ključem dužine 768 bita (za zaštitu ekvivalentne kriptografske snage)
- Asimetrični algoritmi se koriste za razmenu kriptografskog materijala
- Simetrični algoritmi se koriste za zaštitu saobraćaja

127

Preporuka za dužinu ključa

- Računa se na osnovu broja operacija potrebnih za razbijanje algoritma isprobavanjem ključeva u nekom vremenskom periodu (npr 20 god)
- RFC preporuka: 1996. – 90 bita
- Broj bita povećati za 2/3 svake godine ako se računa da se brzina računara povećava po Murovom zakonu.

128

Preporučene veličine ključeva

- *n* - broj operacija za simetrični algoritam nad jednim blokom
- *k* - broj bita u ključu simetričnog algoritma
- Broj operacija za razbijanje = $n2^k$

$$n2^k = 0.02e^{(1.92\sqrt[3]{\ln(kp)\cdot(\ln(\ln(kp))^2)})}$$

- *kp* - broj bita u ključu asimetričnog algoritma

129

Preporučene veličine ključeva

- Pretpostavke:
  - Računari se razvijaju tempom kao do sada
  - Nema napretka u relevantnim oblastima matematike

System requirement for attack resistance (bits)	Symmetric key size (bits)	RSA or DH modulus size (bits)	DSA subgroup size (bits)
70	70	947	129
80	80	1228	148
90	90	1553	167
100	100	1926	186
150	150	4575	284
200	200	8719	383
250	250	14596	482

130

IPsec

- Skup protokola i metoda opisanim u RFC: 2401 (4301) i brojnim drugim RFC dokumentima
- Sastavni deo IPv6
- Osnovne komponente:
  - Authentication Header
  - Encapsulating Security Payload
  - IKE/ISAKMP
- Dva režima prenosa paketa
  - Tunel
  - Transport

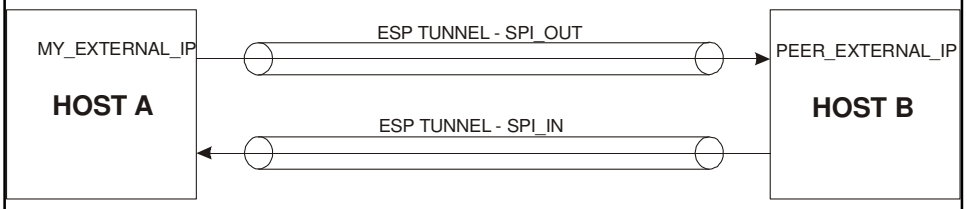
131

Sigurnosna asocijacija - SA

- SA je skup pravila i metoda koje će IPsec strane u komunikaciji koristiti za zaštitu saobraćaja između njih.
- SA sadrži sve sigurnosne parametre potrebne za siguran transport paketa kroz mrežu korišćenjem IPsec
- Uspostavljanje SA je preduslov za IPSec zaštitu saobraćaja.
- SA su uvek unidirekcione. Za zaštitu saobraćaja u oba smera, potrebno je da postoje dve paralelne SA.
- SA se čuvaju u SA database (SADB)
- Skup pravila se čuva u Security policy DB SPDB

132

SA



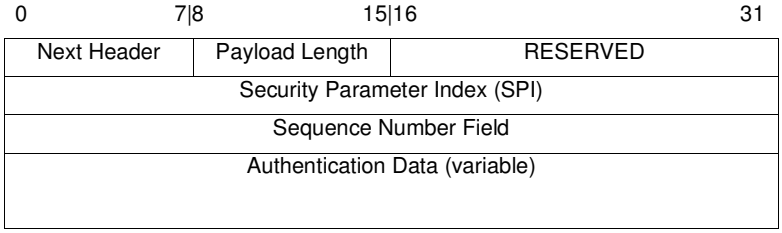
133

SA

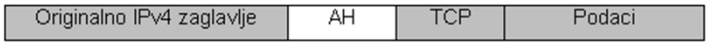
- Za svaki poseban protokol koji se koristi postoji posebna SA
- Parametri koji postoje u SA:
  - Algoritam za autentikaciju/enkripciju, dužina ključa, trajanje ključa
  - Ključevi koji služe za autentikaciju (HMAC) i enkripciju
  - Specifikaciju saobraćaja koji će biti podvrgnut datoj SA
  - IPSec protokol za enkapsulaciju (AH or ESP) i režim rada (tunel ili transport)

134

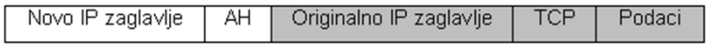
Authentication header - AH



Slika 4.6 Izgled paketa pre primene AH



Slika 4.7 Izgled paketa posle primene AH u transport modu



Slika 4.8 Izgled paketa posle primene AH u tunel modu

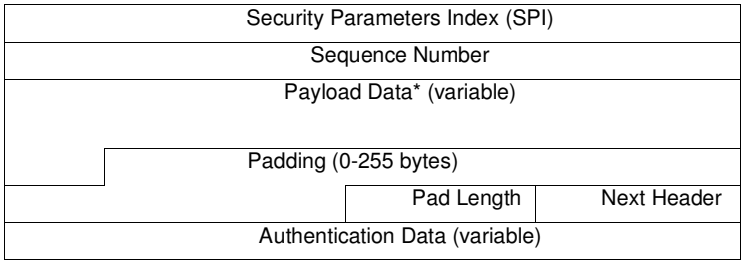
135

AH

- IP Authentication Header (AH) se koristi za
  - Obezbeđivanje integriteta bez ostvarivanja konekcije
  - Autentikacije porekla IP paketa
  - Zaštitu od napada ponavljanjem
- Delovi IP zaglavlja koji se menjaju tokom prolaska kroz mrežu ne mogu da budu zaštićeni (TTL, Flags, Fragment offset, TOS)

136

Encapsulation Security Payload - ESP



Slika 4.10 Originalan izgled paketa

Slika 4.11 Izgled paketa posle primene ESP u transport modu

Slika 4.12 Izgled paketa posle primene ESP u tunel modu

137

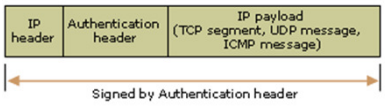
ESP

- ESP pruža sledeće servise:
  - Poverljivost
  - Autentikaciju porekla
  - Obezbeđivanje integriteta bez ostvarivanja konekcije
  - Anti-replay servis
  - Ograničenu zaštitu od analize tokova u mreži (kada se koristi tunel mod)

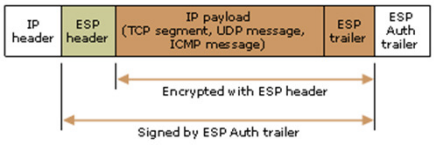
138

ESP i AH u transportnom modu

- AH autentifikuje ceo originalni IP paket



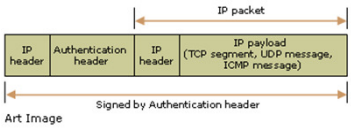
- ESP autentifikuje samo “data” deo originalnog paketa



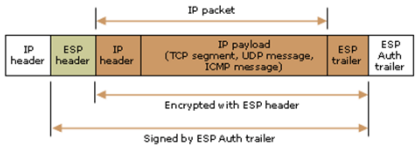
139

ESP i AH u tunel modu

- AH autentifikuje ceo originalni IP paket i spoljašnje zaglavlje

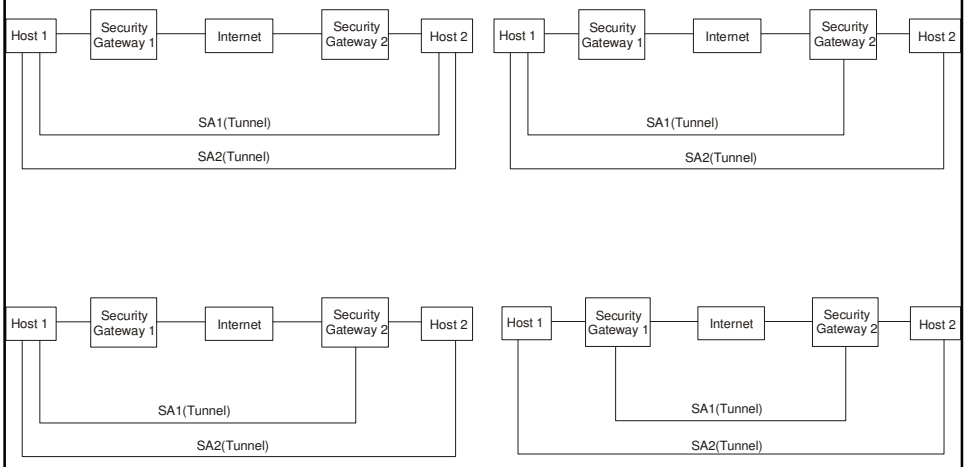


- ESP autentifikuje originalni paket i ESP zaglavlje

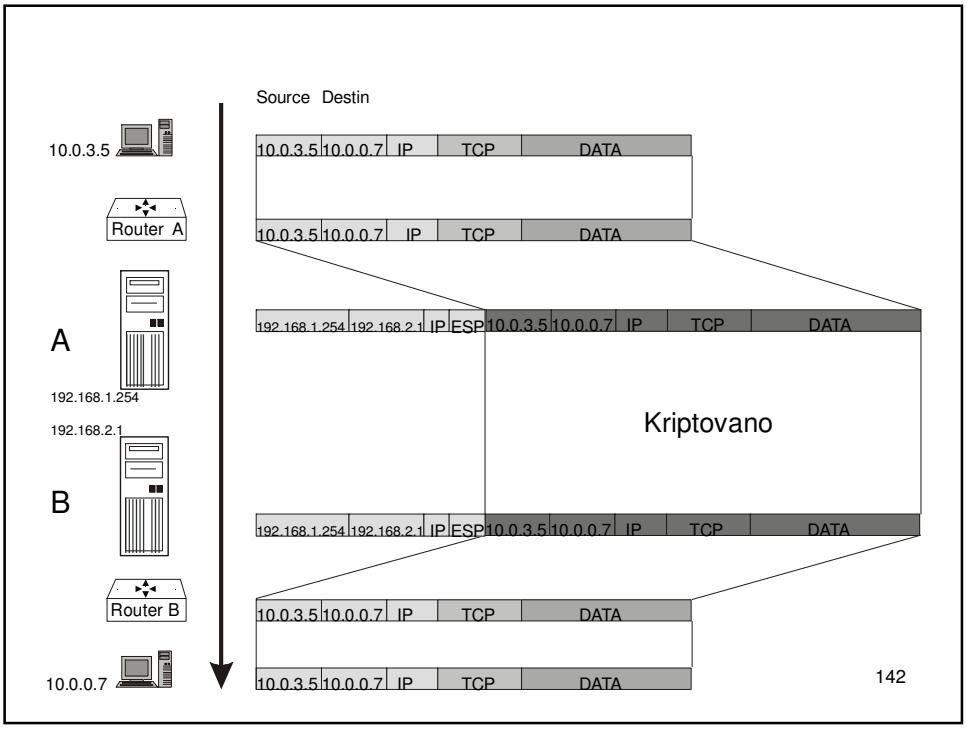


140

Kombinacije dve SA



141



142

IKE/ISAKMP

- IKEv1 – RFC 2409
- ISAKMP – RFC 2407, 2408
- IKEv2 – RFC 4306 (obsoletes 2407, 2408, 2409)
- IKE je hibridni protokol koji je nastao iz Oakley i Skeme mehanizma za razmenu ključeva i koristi Internet Security Association and Key Management Protocol (ISAKMP) okvir kao mehanizam za razmenu poruka
- Oakley i Skeme mehanizmi su zasnovani na DH razmeni ključeva

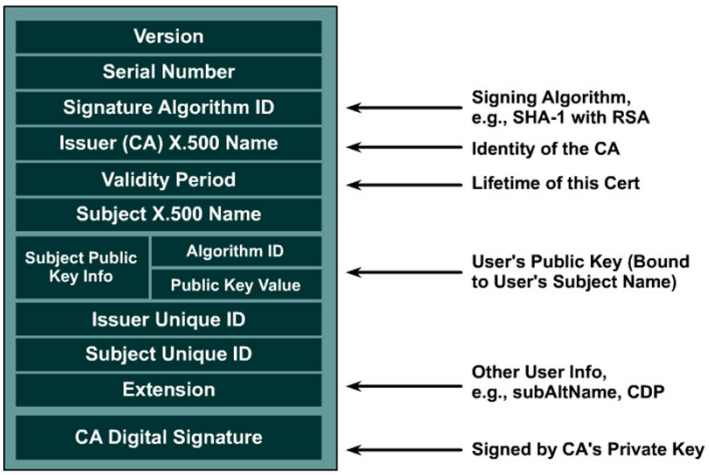
143

IKE

- Osnovni Diffie-Hellman mehanizam ne pruža autentikaciju učesnika u razmeni ključeva.
- Nedostatak autentikacije omogućava Man-in-the-middle napade.
- Autentikacija se ostvaruje na različite načine:
  - unapred razmenjenim ključevima
  - digitalnim potpisima
  - Sertifikatima
- U IKE protokol su uključene i druge zaštite od replay,... Napada
- PFS – Perfect Forward Secrecy

144

X.509 v3 digitalni sertifikat



145

IKE mehanizam

- IKE razmena ključa se sastoji od dve faze:
  - Main mode
  - Quick mode
- U Main mode fazi se dobija ključ koji služi za zaštitu IKE saobraćaja (ISAKMP SA)
- U Quick mode fazi se dobija ključ koji služi za zaštitu korisničkog saobraćaja (IPsec SA)

146

IKEv1 sa unapred razmenjenim ključevima

- Main mode

(1) HDR,SA	=>	
(2)	<=	HDR,SA
(3) HDR,KE,Ni	=>	
(4)	<=	HDR,KE,Nr
(5) HDR*,IDii,HASH_I	=>	
(6)	<=	HDR*,IDir,HASH_R

- Quick mode

```
HDR, SA, KE, Ni, IDii -->
                      <--    HDR, SA, KE, Nr, IDir, HASH_R
HDR, HASH_I           -->
```

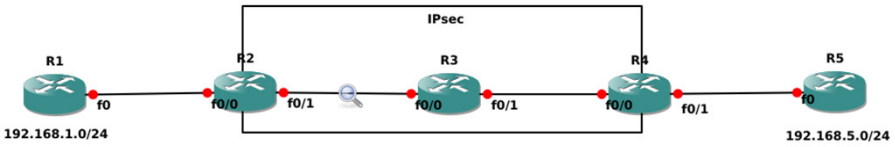
147

IKEv2 – RFC 4306

- Jednostavniji
  - Samo jedna vrsta razmene ključeva
  - Manje kriptografskih algoritama
- Stabilniji
- Bolja zaštita od DoS napada
- Malo realizovanih implementacija

148

IPsec Site-to-Site VPN



Konfiguracija klijentskih strana

R1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
 speed auto
!
ip route 0.0.0.0 0.0.0.0 192.168.12.2
!
```

R5

```
interface Loopback0
 ip address 192.168.5.1 255.255.255.0
!
interface FastEthernet0
 ip address 192.168.45.5 255.255.255.0
 speed auto
!
ip route 0.0.0.0 0.0.0.0 192.168.45.4
!
```

IPsec konfiguracija

R2

```
!Konfiguracija ISAKMP SA
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key vpnuser address 192.168.34.4
!
!Konfiguracija IPsec SA
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.34.4
 set transform-set myset
 match address 100
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255
!
interface FastEthernet0/1
 ip address 192.168.23.2 255.255.255.0
 duplex auto
 speed auto
 crypto map mymap
```

Pokretanje IPsec

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.5.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/75/92 ms
```

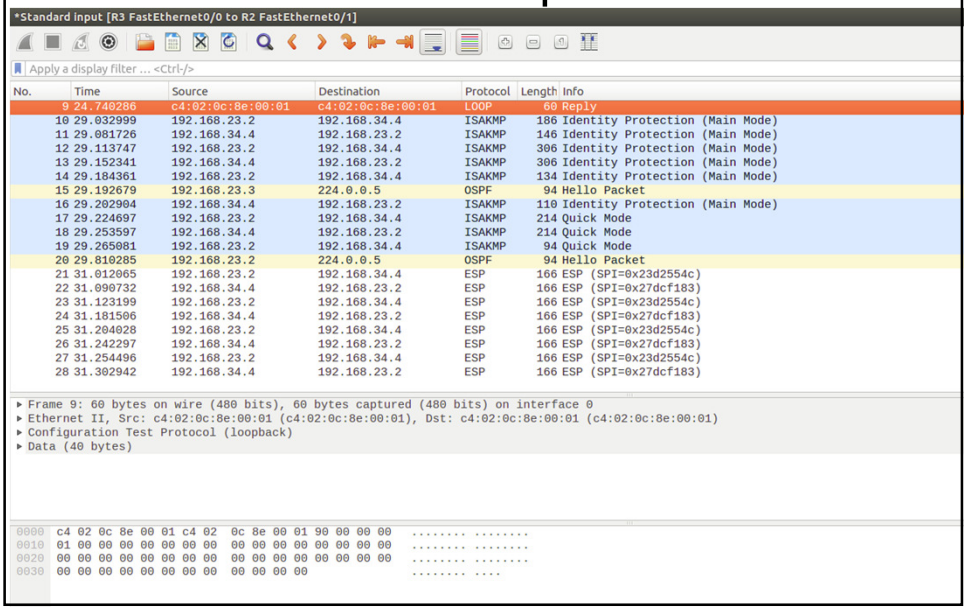
Nadgledanje IPsec (1)

```
R2#sh crypto isakmp sa
dst             src             state          conn-id slot status
192.168.34.4    192.168.23.2    QM_IDLE              2    0 ACTIVE

R2#sh crypto ips sa

interface: FastEthernet0/1
    Crypto map tag: mymap, local addr 192.168.23.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   current_peer 192.168.34.4 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.23.2, remote crypto endpt.:
192.168.34.4
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x23D2554C(600986956)

… nastavak na sledećem slajdu
```

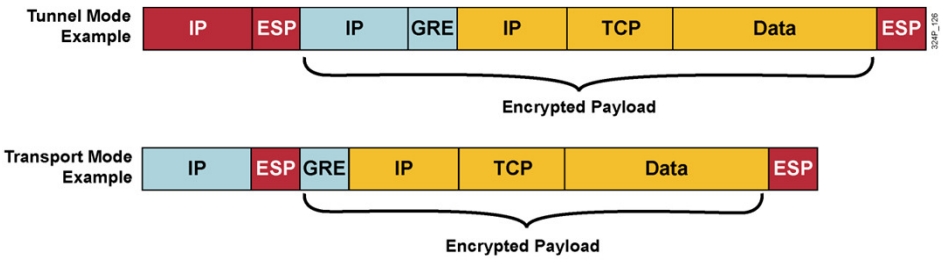
Nadgledanje IPsec (2)

```
… nastavak sa prethodnog slajda
     inbound esp sas:
      spi: 0x27DCF183(668791171)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: mymap
        sa timing: remaining key lifetime (k/sec):
(4524281/2843)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x23D2554C(600986956)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec):
(4524281/2842)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Packet capture



Rutiranje preko IPsec



- IPsec ne prenosi multicast?
- GRE – za prenos paketa protkola rutiranja

156

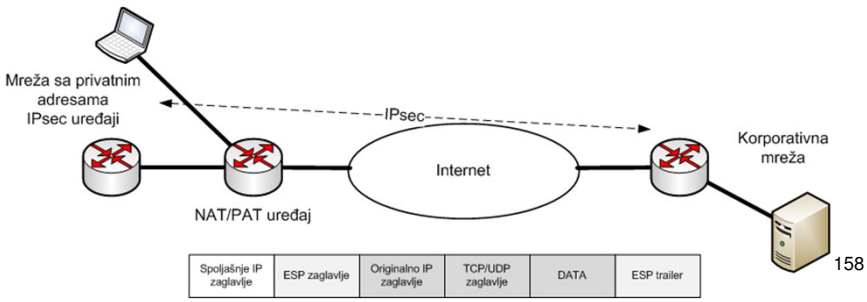
IKE dodaci

- Faza 1.5
  - Xauth
  - Mode konfiguracija
- NAT Traversal
- IKE DPD (dead peer detection)
  - DPD šalje keepalive pakete kada nema saobraćaja kroz SA
  - DPD mehanizam može da bude periodičan ili po pozivu

157

NAT Traversal

- Problem kada se između IPsec uređaja vrši PAT ili NAT overload (brojevi portova u zaglavlju transportnog sloja se ne vide)
- NAT-T detekcija
- NAT-T akcija



158

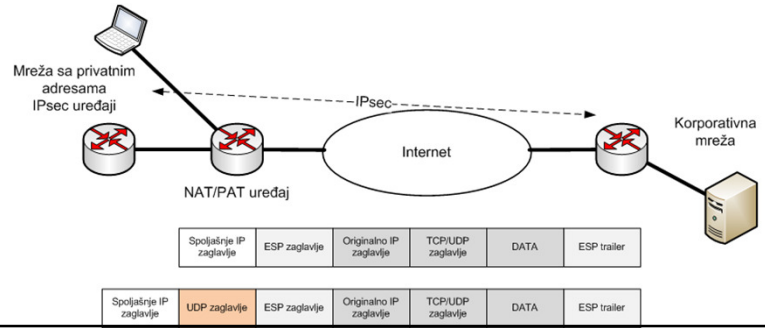
NAT-T detekcija

- Za vreme IKE faze 1 uređaji detektuju dva događaja:
  - Podršku za NAT-T
  - Postojanje NAT duž putanje
- Za detekciju podrške za NAT-T razmenjuje se vendor ID string u okviru IKE poruka
- Postojanje NAT se detektuje tako što se pošalje hash(IP adrese, portovi) u okviru NAT discovery (NAT-D) delova IKE poruke.
- Ako je hash koji je izračunat na destinaciji jednak poslatom hash-u – nema NAT-a

159

NAT-T akcija i enkapsulacija

- NAT-T akcija: Tokom IKE faze 2 se odlučuje da li će da se primeni NAT-T
- UDP enkapsulacija IPsec paketa: Ako se koristi NAT-T dodatno UDP zaglavlje se umeće između spoljašnjeg IP zaglavlja i IPsec zaglavlja
- UDP checksum: Novo UDP zaglavlje ima checksum vrednost 0, kako se ne bi proveravala ova vrednost



160

Kreiranje IPsec SA

- IPsec SA može da se kreira:
  - Po potrebi, kada naiđe paket koji pripada datoj SA
    - Manje zauzeće resursa
    - Inicijalno kašnjenje veliko
    - Potencijalno veći broj rekey-a
  - Da bude permanentna, bez obzira na saobraćaj

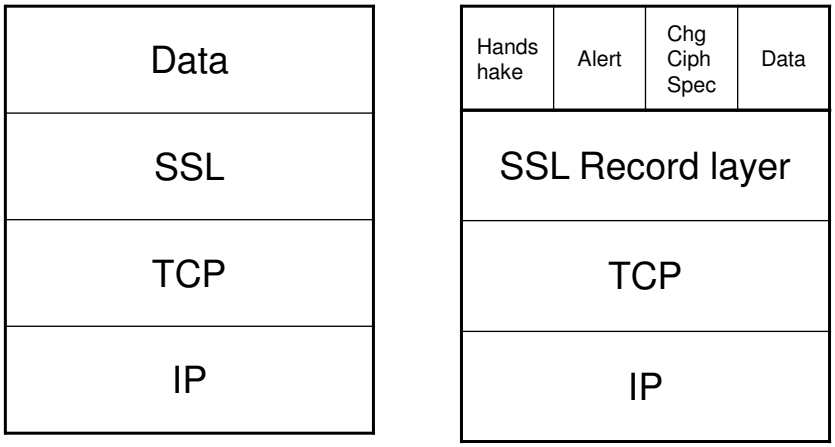
161

SSL – Secure Sockets Layer

- SSL v1,v2,v3. Verzije v1 i v2 se smatraju za nesigurne
- Transport Layer Security – TLS (RFC 2246), v1.1(RFC 4346), v1.2 (RFC 5246)
- SSL služi za zaštitu TCP protokola
- SSL se koristi kod HTTPS, FTPS, POP3S, SMTPS
- Može da se koristi za zaštitu pojedinačnih protokola ili celokupnog saobraćaja

162

SSL slojevi



163

SSL Record Layer

- Fragmentacija
- Kompresija
- Message Authentication Code
- Enkripcija/dekripcija

164

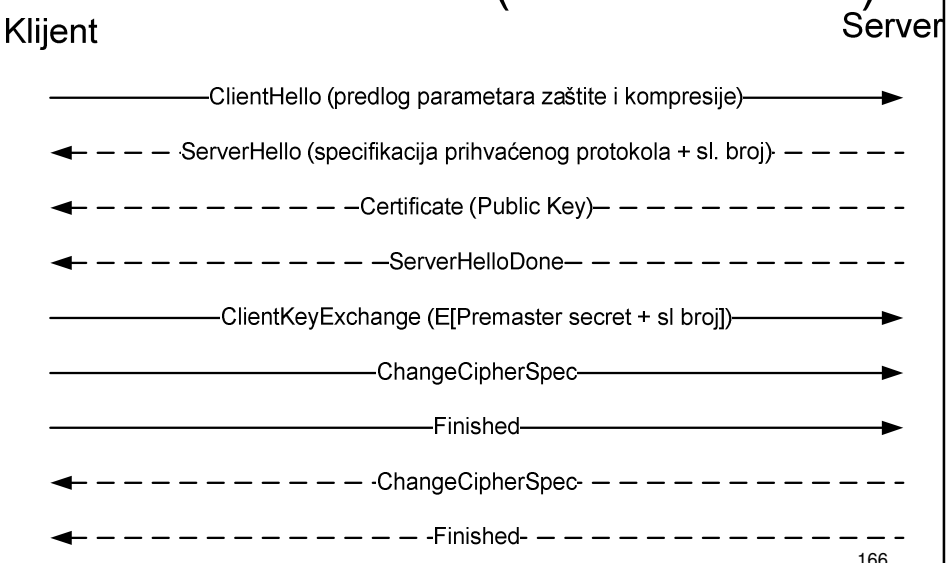
SSL Protokoli

Handshake – za uspostavljanje SSL sesija

- Alert – Signalizacija gresaka
- Change Cipher Specification – signalizacija da su naredne SSL poruke kriptovane
- Application data protocol (HTTP, FTP, POP3, IMAP, SMTP)

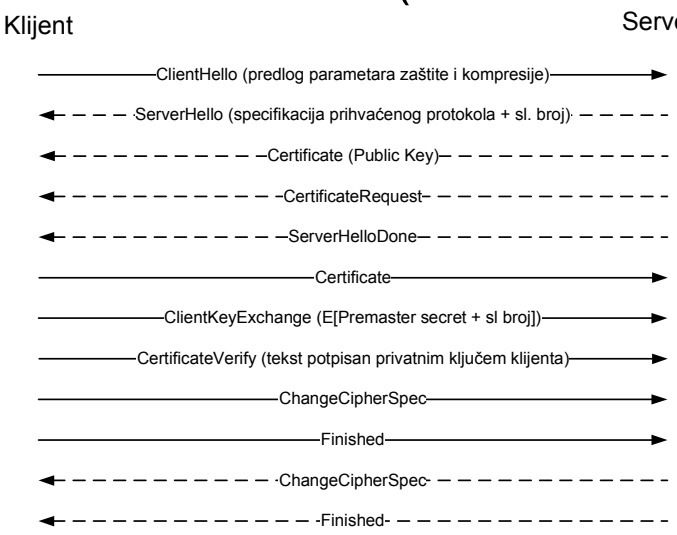
165

SSL Handshake (no client auth)



166

SSL Handshake (w client auth)



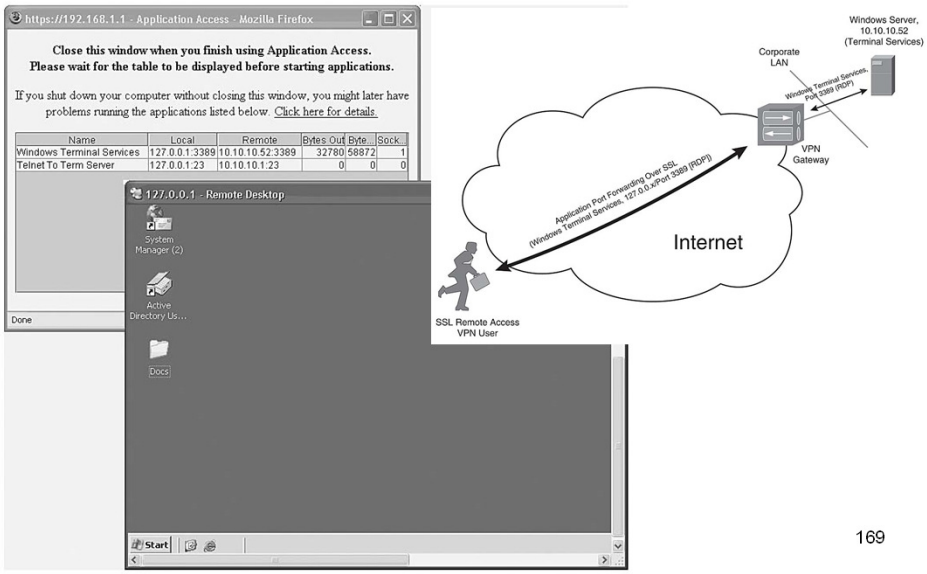
167

Načini rada SSL VPN

- Svaka aplikacija zasebna zaštita
- Pristup preko weba (clientless) – port forwarding konfigurisan na centralnoj lokaciji
- Pristup kroz web, pa download klijenta koji je validan za vreme trajanja jedne SSL VPN sesije
- Unapred instaliran klijent

168

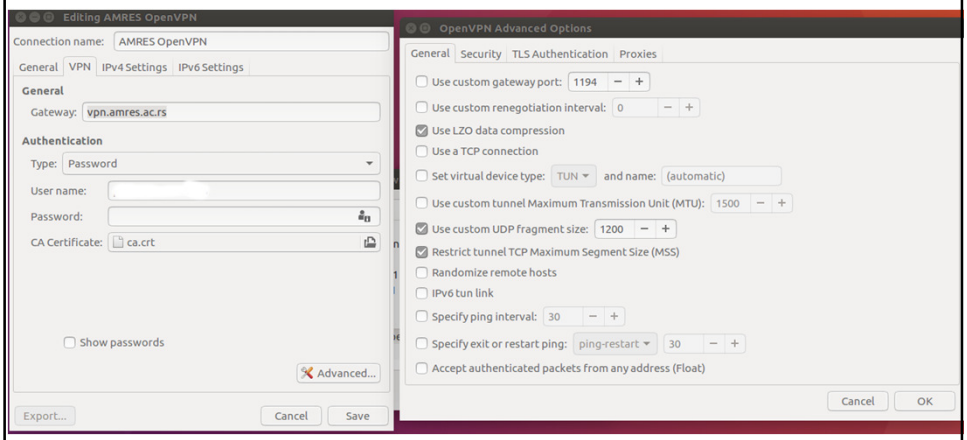
Clientless (port forwarding)



169

SSL VPN rute

```
pavle@pavle-ThinkPad-T420:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    600    0        0 wlp3s0
link-local      *               255.255.0.0     U     1000   0        0 wlp3s0
192.168.1.0     *               255.255.255.0   U     600    0        0 wlp3s0
pavle@pavle-ThinkPad-T420:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    600    0        0 wlp3s0
10.8.0.0        *               255.255.0.0     U     50     0        0 tun0
91.187.128.0    10.8.0.1        255.255.224.0   UG    50     0        0 tun0
147.91.0.0      10.8.0.1        255.255.0.0     UG    50     0        0 tun0
vpn.amres.ac.rs 192.168.1.1     255.255.255.255 UGH   600    0        0 wlp3s0
160.99.0.0      10.8.0.1        255.255.0.0     UG    50     0        0 tun0
link-local      *               255.255.0.0     U     1000   0        0 wlp3s0
192.168.1.0     *               255.255.255.0   U     600    0        0 wlp3s0
```



SSL literatura

- http://www.networkworld.com/subnets/cisco/072507-ch10-deploying-vpns.html?page=1

172