Virtualizacija v omrežjih

Univerza v Ljubljani
Fakulteta za elektrotehniko
Laboratorij za telekomunikacije

Ljubljana, maj 2011

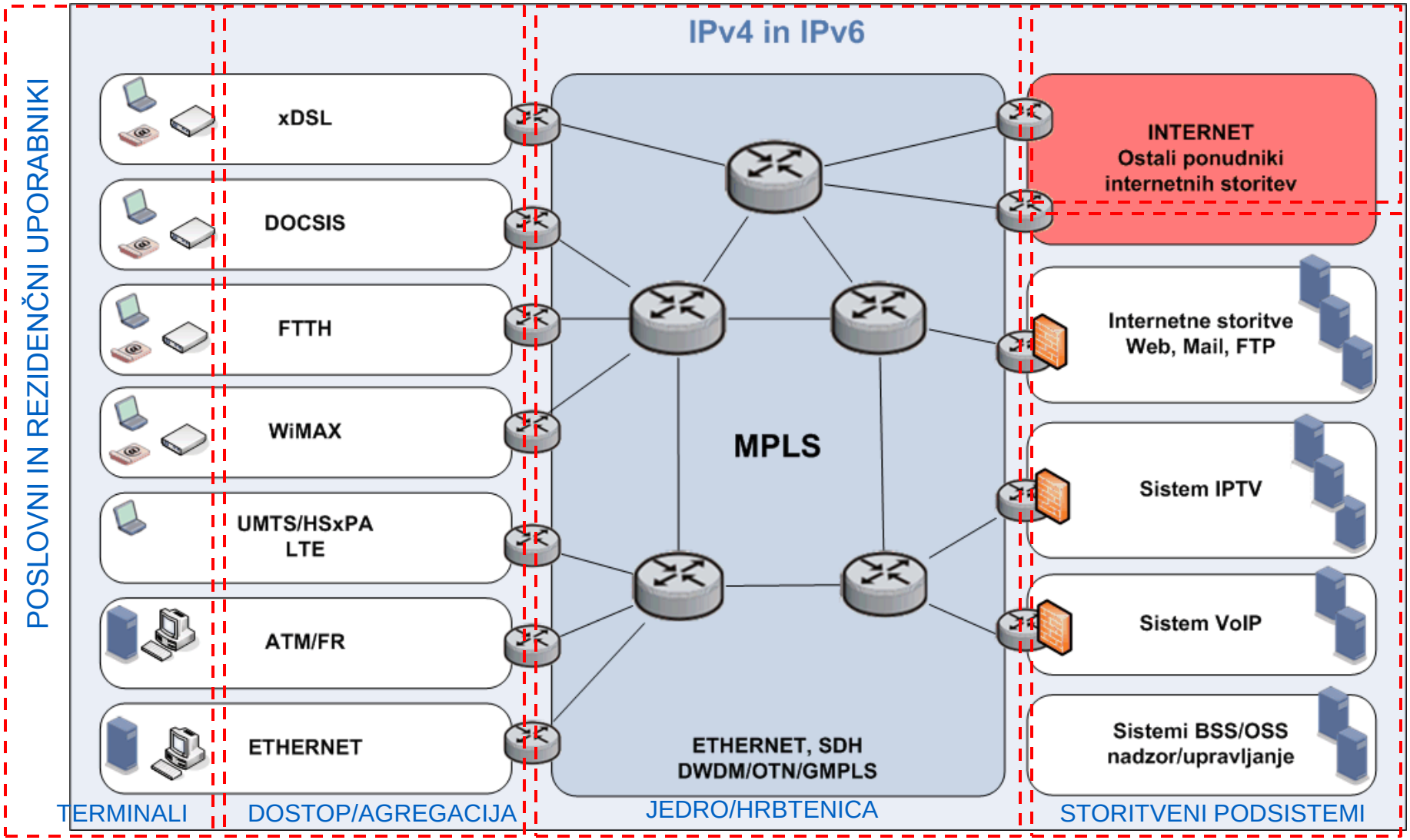
Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

Koncepti virtualizacije v omrežjih

- Virtualizacija vmesnikov
  - kreiranje logičnih vmesnikov
  - npr. VLAN ID
- Tunelski mehanizmi
  - prenos PDU znotraj drugega PDU
  - npr. IP prek IPSec
- Virtualizacija omrežnih naprav
  - kreiranje več logičnih instanc stikala Ethernet, usmerjevalnika IP, požarne pregrade na eni fizični napravi
- Storitev navideznega zasebnega omrežja
  - skupina geografsko razpršenih lokacij/omrežij, ki na varen način komunicira prek skupne omrežne infrastrukture

Transportni sloj sodobnih omrežij



Omrežne storitve 1/2

	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Podatkovna raven	Globalno naslavljanje	Unicast naslavljanje		-	✓	✓	-
		Multicast naslavljanje		-	✓	✓	-
		Anycast naslavljanje		-	✓	✓	-
	Lokalno naslavljanje	Unicast naslavljanje		✓	✓	✓	✓
		Multicast naslavljanje		✓	✓	✓	✓
		Anycast naslavljanje		-	✓	✓	-
		Broadcast		✓	✓	-	-
	Prenos	Nepovezavni	Unicast posredovanje	✓	✓	✓	-
			Multicast posredovanje	✓	✓	✓	-
			Anycast posredovanje	-	✓	✓	-
			Broadcast posredovanje	✓	✓	-	-
		Povezavni	Točka-točka (Unicast)	-	-	-	✓
			Točka-več točk (Multicast)	-	-	-	✓
	Avtomatska nastavitev omrežnih parametrov			Privzeta nastavitev	DHCP	SLAAC in DHCPv6	Signalizacija LDP in RSVP-TE
	Globalno usmerjanje	Unicast usmerjanje IGP		-	OSPF, ISIS, RIP	OSPFv3, ISIS,RIPng	-
		Unicast usmerjanje EGP		-	BGP	BGP	-
		Multicast usmerjanje IGP		-	PIM-SM, PIM-DM	PIM-SM, PIM-SSM	-
		Multicast usmerjanje IGP		-	BGP	BGP, PIM-SSM	-
	Prometni inženiring			MSTP	OSPF-TE ISIS-TE	OSPF-TE ISIS-TE	MPLS-TE (RSVP-TE)
	Zaščitni mehanizmi	Zaščita povezave		STP, RSTP, MSTP, LinkAgregation	OSPF, ISIS, RIP	OSPFv3, ISIS, RIPng	Sekundarna pot, FRR
		Zaščita naprave		STP, RSTP, MSTP, LinkAgregation	OSPF, ISIS, RIP	OSPFv3, ISIS, RIPng	Sekundarna pot, FRR
		Zaščita poti		STP, RSTP, MSTP, LinkAgregation	OSPF, ISIS, RIP	OSPFv3, ISIS, RIPng	Sekundarna pot
		Zaščita omrežja		-	BGP	BGP	-
	Kakovost storitev	Krmiljenje dostopa		-	IntServ	IntServ	MPLS-TE
		Klasifikacija prometa		802.1p	DiffServ	DiffServ	MPLS QoS
		Označevanje prometa		802.1p	DiffServ	DiffServ	MPLS QoS
		Krmiljenje in glajenje		802.1p	DiffServ	DiffServ	MPLS QoS
		Signalizacija zamašitev ECN		-	ECN	ECN	-
	Mobilnost			-	Mobile IP, PMIP	DSMIPv6, PMIPv6	-

Omrežne storitve 2/2

	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Kontrolna in upravljavska raven	Varnostne storitve	Zaščita podatkovne ravnine	Avtentikacija	-	IPSec, SSL,HMAC	IPSec, SSL, HMAC	-
			Nadzor dostopa	filtri ACL	IPSec, SSL, filtri ACL, Relay,	IPSec, SSL, filtri ACL, Relay,	filtri ACL
			Zasebnost/enkripcija	-	IPSec, SSL	IPSec, SSL	-
			Celovitost	-	IPSec, SSL	IPSec, SSL	-
			Zaščita pred DoS	-	IPSec	IPSec	-
		Zaščita kontrolne ravnine	Avtentikacija	-	IKE, MD5 (BGP, OSPF, ISIS),	IKE, MD5 (BGP), IPSec (RIPng, OSPFv3)	-
			Nadzor dostopa	BPDU guard, DHCP snooping, ARP inspection, RA guard	IKE, IGMP Proxy/snooping	IKE, MLD Proxy/snooping	-
			Zasebnost/enkripcija	-	IKE	IKE	-
			Celovitost	-	IKE	IKE	-
			Zaščita pred DoS	-	IGMP Proxy	MLD Proxy, Filtri VRF	-
		Zaščita upravljavske ravnine	Avtentikacija	-	SNMPv3, SSH	SNMPv3, SSH	-
			Nadzor dostopa	-	Filtri ACL, SSH	Filtri ACL, SSH	-
			Zasebnost/enkripcija	-	SNMPv3, SSH	SNMPv3, SSH	-
			Celovitost	-	SNMPv3, SSH	SNMPv3, SSH	-
			Zaščita pred DoS	-	-	-	-
	AAA	Avtentikacija		802.1X	Radius, Diameter, TACACS	Radius, Diameter, TACACS	-
		Avtorizacija		802.1X	Radius, Diameter, TACACS	Radius, Diameter, TACACS	-
		Beleženje		-	Radius, Diameter, SNMP, SYSLOG	Radius, Diameter, SNMP, SYSLOG	-
Virtualizacija	Navidezna zasebna omrežja	Prenos bitov		-	L2TPv3	L2TPv3	VPWS
		Prenos L2 PDU		VLAN, QinQ, VLANinVLAN	L2TPv3	L2TPv3	VPLS, VPWS, IPLS
		Prenos L3 PDU		-	IPSec, GRE, SSL VPN, L2TPv3	IPSec, GRE, SSL VPN, L2TPv3	BGP/MPLS

Vsebina

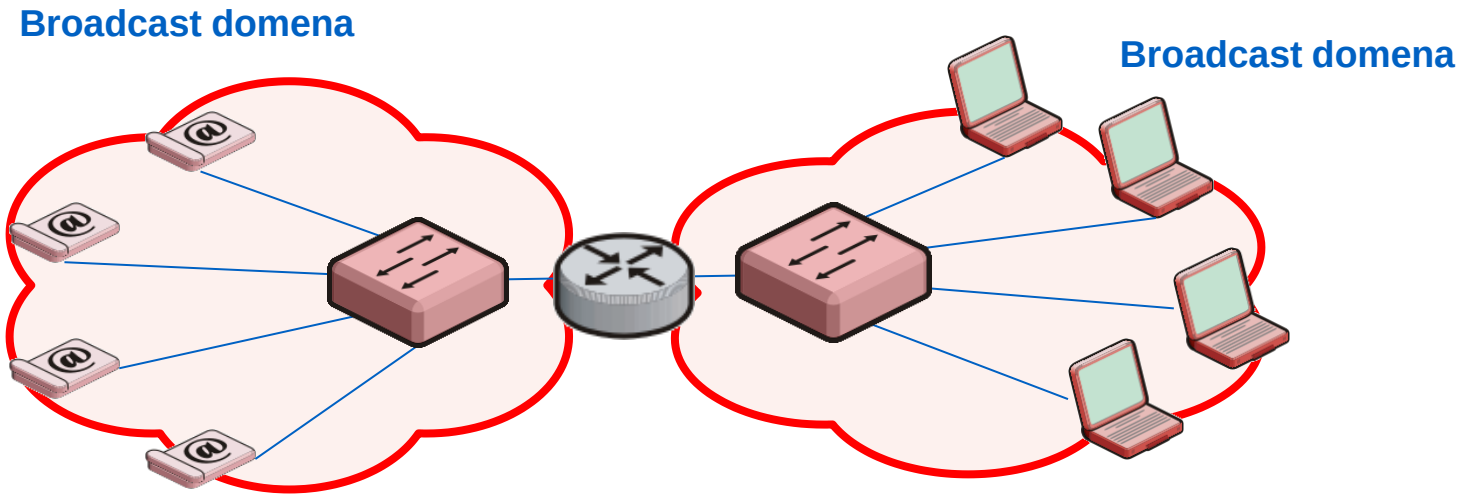
- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

Ethernet

- Tehnologija v osnovi razvita za okolja LAN
  - deluje po princip ´´Plug and Play´´
  - nič ni potrebno nastaviti, vse se zgodi avtomatsko
- Tehnologija Ethernet
  - fizični vmesniki Ethernet
    - prenosne hitrosti 10/100/1000/10000/40000 Mbit/s
    - prenos prek optičnih vodnikov in bakrenih vodnikov
    - brezžični Ethernet – WiFi/WLAN
  - omrežna oprema Ethernet
    - angl. hub, bridge, switch
  - podporni mehanizmi Ethernet
    - VLAN (angl. Virtual LAN) – mehanizem za virtualizacijo omrežja
    - STP (angl. Spanning Tree Protocol) – mehanizem za preprečevanje zank
      - zagotavljanje velike razpoložljivosti in redundantnih povezav
    - PoE (angl. Power over Ethernet) – napajanje naprav prek Ethernet
    - Link aggregation – združevanje fizičnih vmesnikov

Komponente omrežja Ethernet

- **Končne naprave Ethernet**
  - osebni računalniki, delovne postaje, strežniki, IP telefoni
  - usmerjevalniki, požarni zidovi
- **Omrežna oprema Ethernet**
  - stikalo Ethernet (angl. switch) – aktivno vozlišče



Okvir Ethernet in uporabniška vsebina

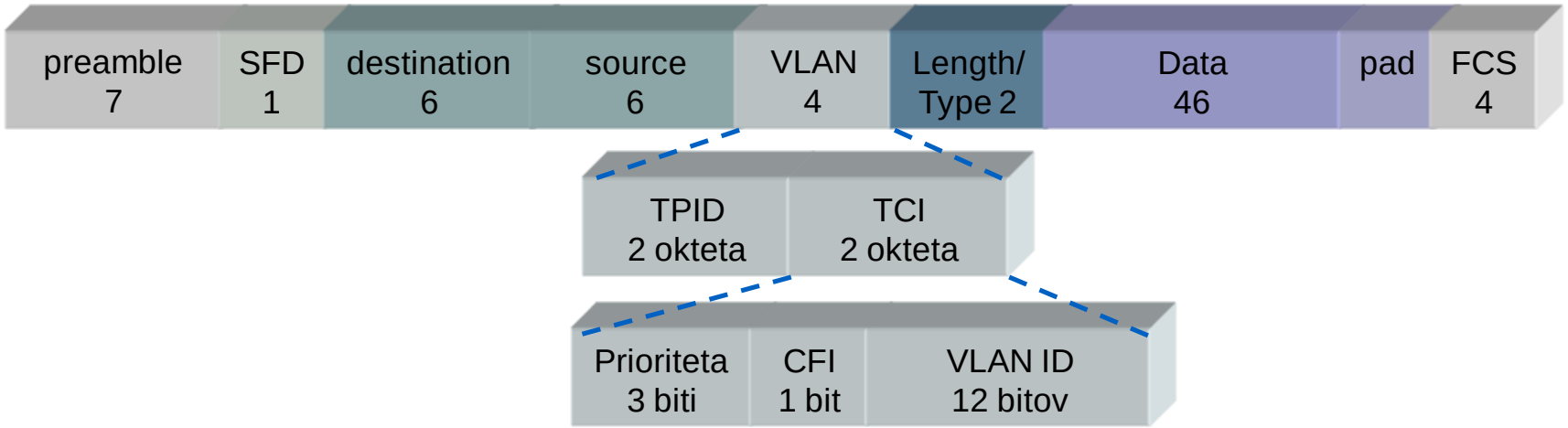
- Uporabniška vsebina se prenaša v okvirjih Ethernet
  - uporabniška vsebina – paketi IPv4, IPv6, ARP, MPLS
- Naloga okvirja Ethernet
  - prenos “bitov – uporabniške vsebine” prek fizičnega medija
  - naslavljanje Ethernet naprav, odkrivanje napak pri prenosu
- Vsebina in velikost okvirja Ethernet je za vse verzije Ethernet-a enaka
  - omogoča združljivost “novih različic” Ethernet-a za obstoječimi
  - dokler se uporabniška vsebina prenaša prek Ethernet omrežja, se okvir ne spreminja
- Značilnosti okvirja Ethernet
  - velikost okvirja je 1518 oktetov
  - velikost “glava + rep” je 18 oktetov
  - velikost koristne vsebine je 1500 oktetov (npr. paketa IPv4)

Tehnologija VLAN

- Standard IEEE 802.1Q
- VLAN – tehnologija za virtualizacijo omrežij Ethernet
  - omogoča logično ločitev uporabnikov (terminalov), neodvisno od fizične lokacije
  - logična topologija omrežja je tako neodvisna od fizične topologije
  - omejuje nam ˝broadcast˝ in ˝multicast˝ domene
- Večina implemetacij stikal Ethernet podpira tehnologijo VLAN
  - logična topologija postane neodvisna od fizične topologije
- Vsako omrežje VLAN je identificirano s svojo številko VLAN ID
  - vrednosti VLAN ID so od 1 do 4094 (privzeta vrednost je 1)
  - terminali, ki so v istem omrežju VLAN (enak VLAN ID) komunicirajo, kot da so del istega fizičnega omrežja (ista ˝broadcast˝ domena)
  - terminal, ki so v različnih omrežjih VLAN (čeprav so priklopljeni na isto fizično infrastrukturo), lahko komunicirajo le prek usmerjevalnika oziroma sorodne naprave
- Nadgradnja mehanizmiv VLAN
  - 802.1ad – VLANvVLAN (QinQ)
  - 802.1ah – MACinMAC

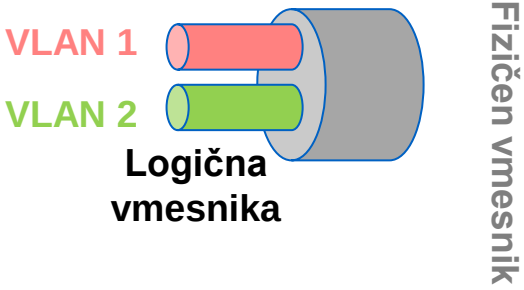
Tehnologija VLAN

- **Razširitev okvirja Ethernet**
- **Polja dodana klasičnemu okvirju Ethernet (4 okteti)**
  - **TPID (Tag Protocol IDentifier) – indikator okvirja VLAN (2 okteta)**
  - **TCI (Tag Control Information) – kontrolna informacija (2 okteta)**
    - **polje prioriteta – 3 biti za določitev prioritete okvirja (standard 802.1p)**
    - **CFI (Canonical Format Identicator) – zastavica, ki identificira tip okvirja: vrednost 0 (Ethernet), vrednost 1 (Token Ring)**
    - **VLAN ID – identifikator omrežja VLAN, možnih je 4094 VLAN ID (vrednosti 0 in FFF sta rezervirani)**

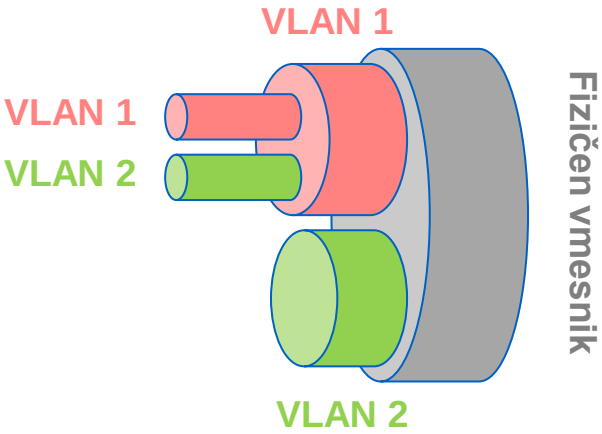


VLAN virtualizacijski mehanizmi 1/3

- **Logični vmesniki**
  - **VLAN ID**
- **Tunelski mehanizem**
  - **Transport Ethernet okvirja prek VLAN**
  - **Transport Ethernet VLAN znotraj VLAN (QinQ)**
  - **Transport Ethernet okvirja in VLAN znotraj drugega Ethernet okvirja (MAcinMAC)**



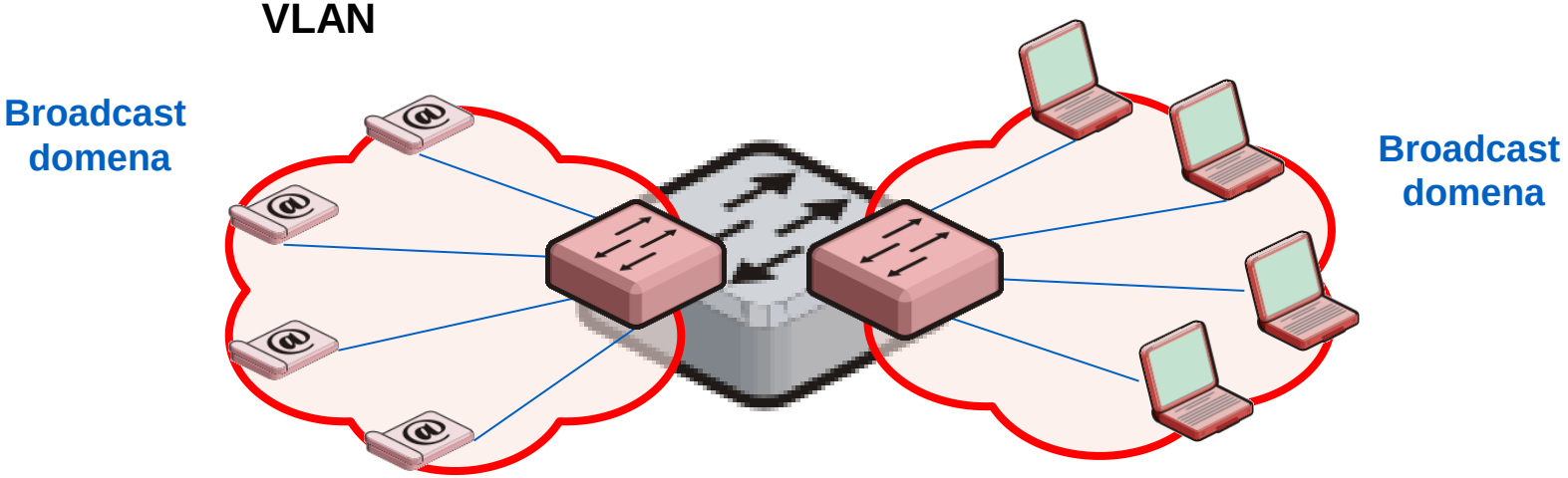
Koncept VLAN



Koncept QinQ

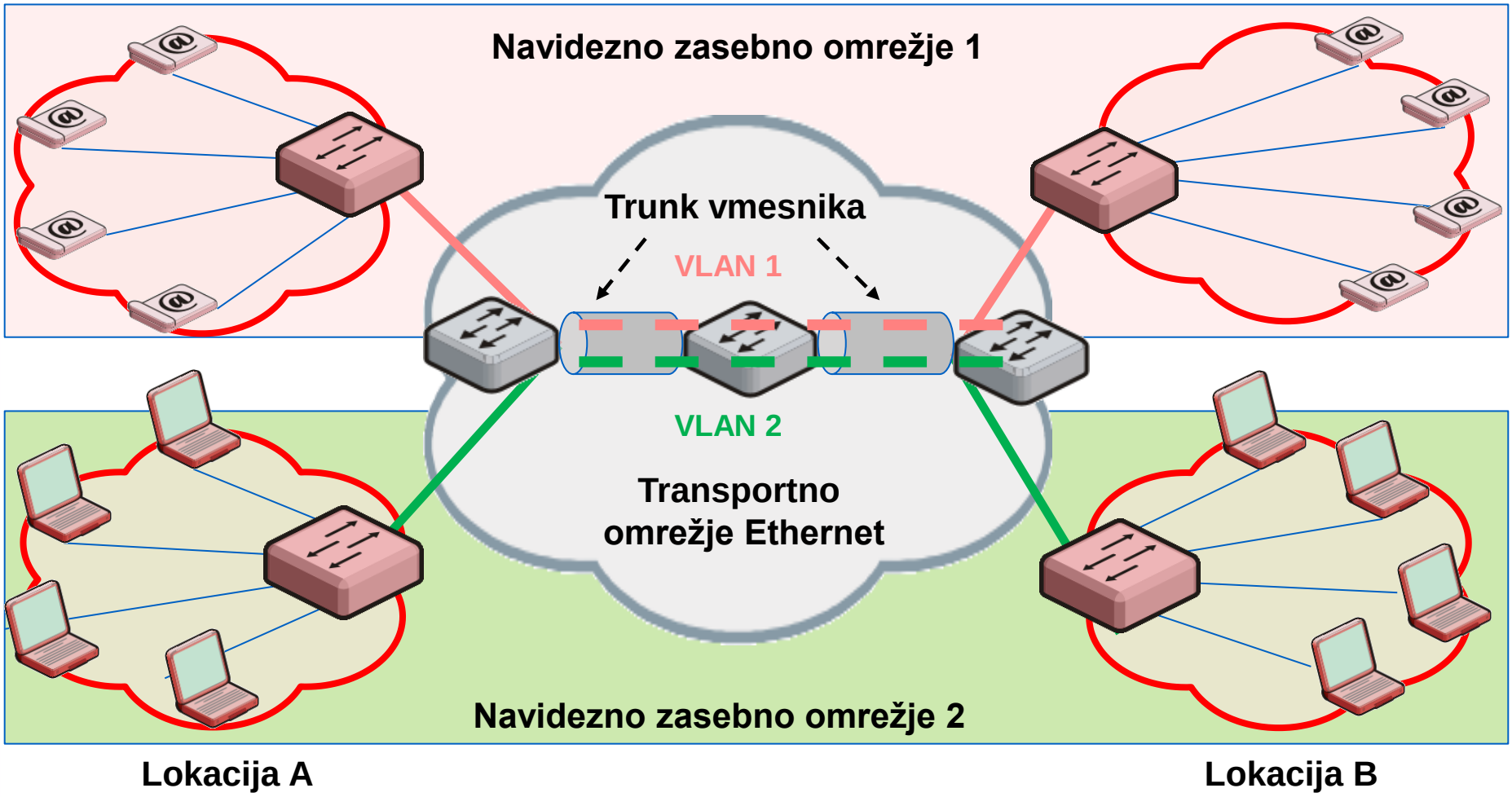
VLAN virtualizacijski mehanizmi 2/3

- Virtualizacija Ethernet stikala
  - emulacija fizičnega stikala na programskem in/ali strojnem nivoju
    - na eni fizični napravi/stikalu se nahaja več logičnih stikal
  - VLAN emulira funkcionalnosti fizičnega stikala
    - dinamično učenje naslovo MAC znotraj omrežja VLAN
    - ločene tabele MAC
  - logično stikalo je povezano s fizičnimi in/ali logičnimi vmesniki "Trunk VLAN"
    - uporaba fizičnega vmesnika za priklop končnih naprav
    - uporaba "trunk vmesnika" za povezovanje na druga stikala s podporo VLAN



VLAN virtualizacijski mehanizmi 3/3

- **Storitev navideznega zasebnega omrežja**

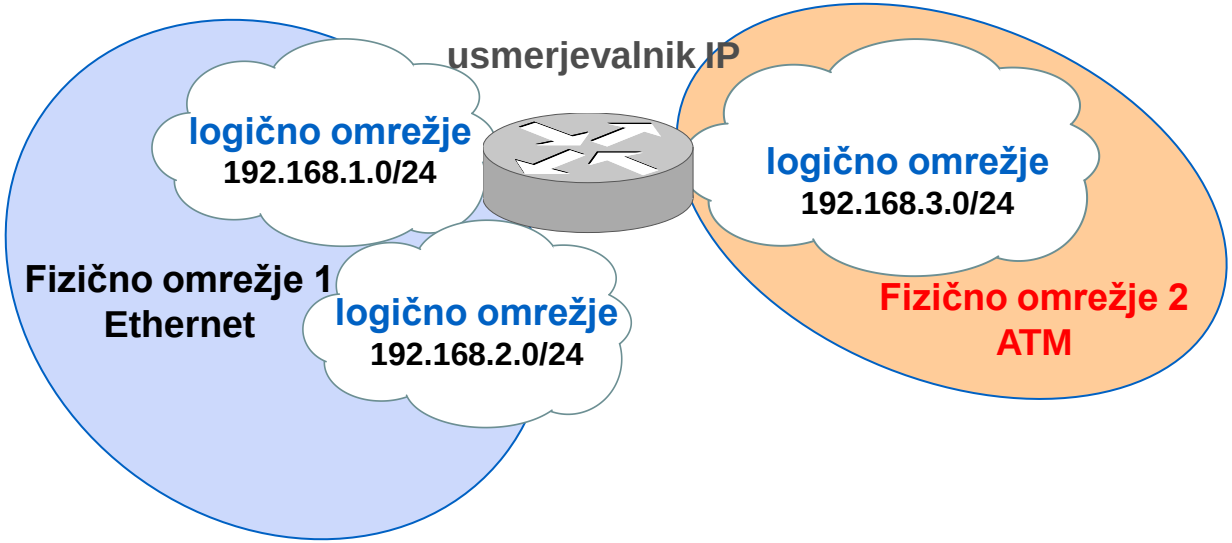


Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

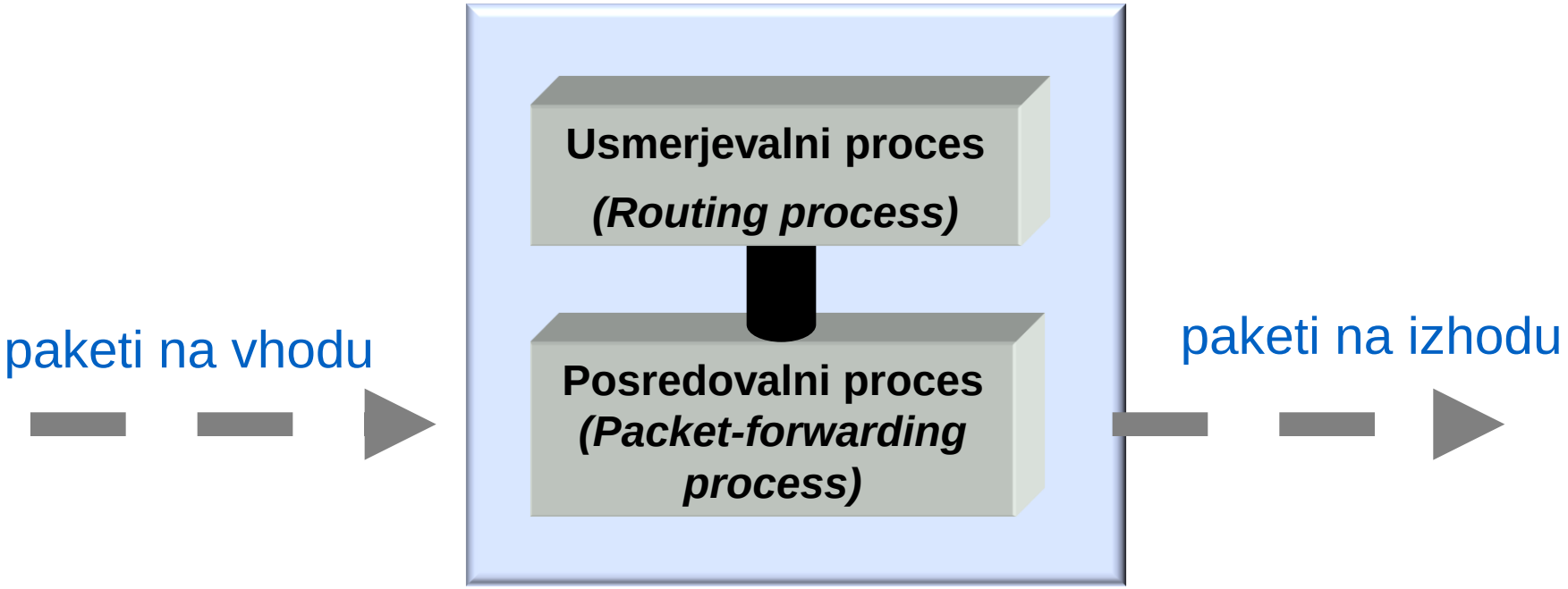
Naloge protokola IP

- Prenos podatkov prek omrežja
- Posredovanje datagramov med mrežnimi povezavami
- Ustvari logično omrežje
  - logično naslavljanje mrežnih povezav



Zgradba usmerjevalnega sistema

- **Usmerjevalni proces**
  - **določitev optimalne poti**
  - **izvaja se lahko v nerealnem času**
- **Posredovalni proces (packet switching)**
  - **posredovanje paketov na izhodni vmesnik**
  - **izvajati se mora v realnem času**

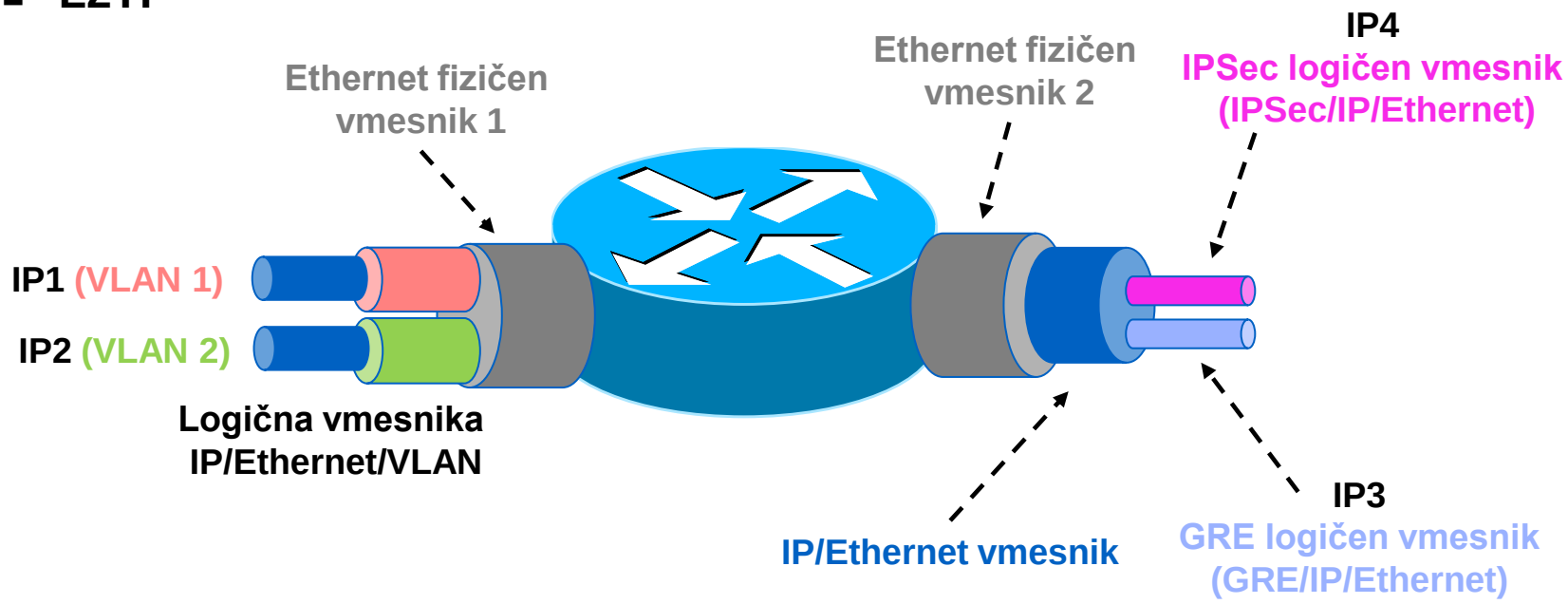


Usmerjanje in posredovanje

- **Usmerjevalni proces**
  - odločanje o tem, kam datagram poslati, imenujemo usmerjanje (routing)
  - poganja usmerjevalne protokole
    - izmenjava usmerjevalnih informacij
    - izgradnja usmerjevalne tabele (posredovalne tabele)
- **Posredovalni proces**
  - odločitev na osnovi usmerjevalne tabele, ki vsebuje zapis, prek katerega izhodnega fizičnega vmesnika mora usmerjevalnik posredovati paket za določen ciljni naslov IP
  - posredovalna funkcija je sestavljena iz
    - sprejema paketa na vhodnem vmesniku
    - dekapsulacije datagrama IP (odstranitev okvirja L2)
    - vpogleda v posredovalno tabelo
    - inkapsulacije datagrama IP (dodajanje ustrezne glave in repa L2)
    - prenosa paketa na ustrezen izhodni vmesnik, ki ga določa usmerjevalna tabela

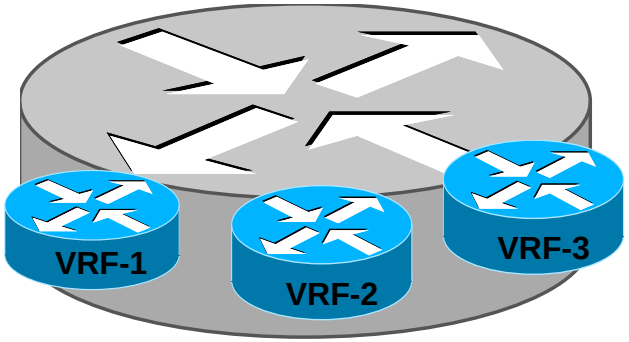
IP virtualizacijski mehanizmi 1/3

- **Logični vmesniki na usmerjevalniku**
  - **povezovanje z IP logičnimi vmesniki (npr. IPSec, GRE, L2TP)**
  - **povezovanje z logičnimi vmesniki L2 (npr. VLAN ID)**
- **Tunelski mehanizmi**
  - **IPSec**
  - **GRE**
  - **L2TP**



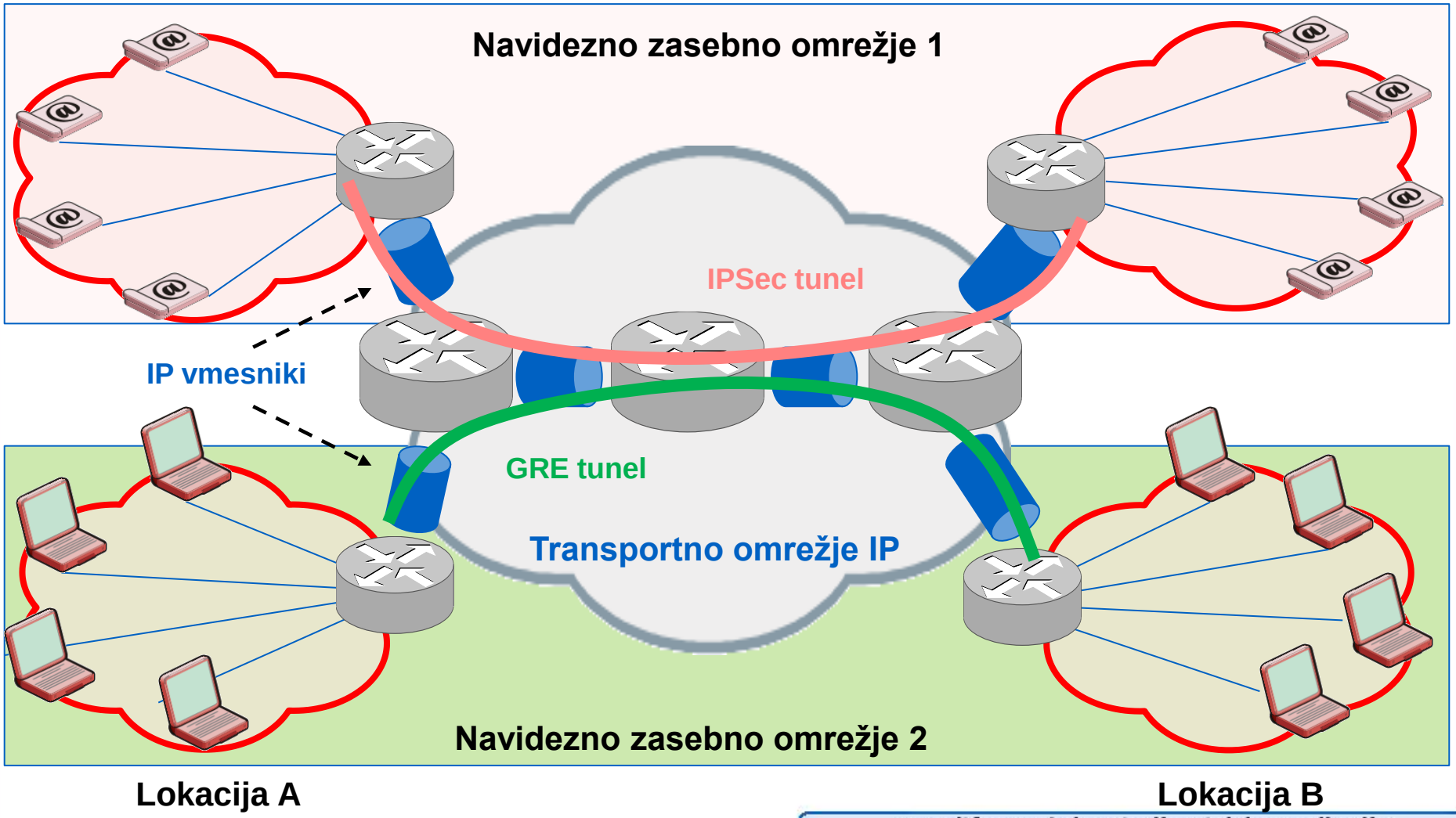
IP virtualizacijski mehanizmi 2/3

- Virtualizacija usmerjevalnika
  - mehanizem VRF – VPN Routing and Forwarding
  - Emulacija fizičnega usmerjevalnika na programskem in/ali strojnem nivoju
    - na eni fizični napravi/usmerjevalniku se lahko nahaja več logičnih usmerjevalnikov
  - VRF emulira vse funkcionalnosti fizičnega usmerjevalnika
    - ločene usmerjevalne/posredovalne tabele
    - vsak usmerjevalnik VRF poganja svojo instanco usmerjevalnega protokola (BGP, RIP, OSPF, IS-IS)
  - logičen usmerjevalnik je povezan s fizičnim in/ali logičnim vmesnikom



IP virtualizacijski mehanizmi 3/3

- Storitev navideznega zasebnega omrežja



Vsebina

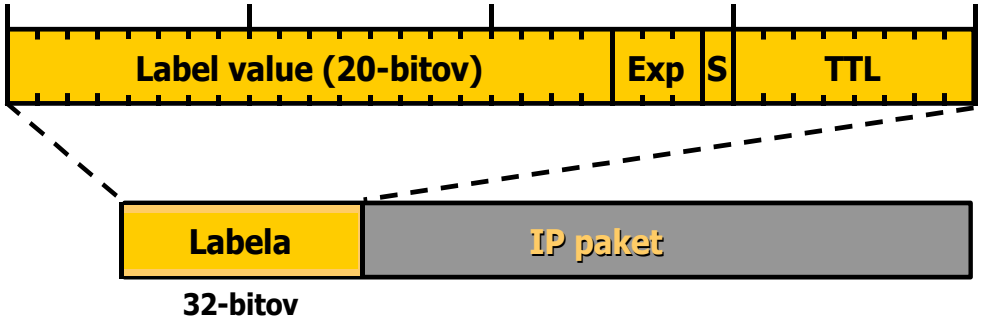
- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

Osnovni koncepti MPLS

- **Glava MPLS**
  - kratek identifikator fiksne dolžine
  - doda se pred prenašani PDU (npr. datagram IP)
- **Usmerjevalnik LSR (angl. Label Switched Router)**
  - izvaja posredovanje paketov MPLS
- **Labela**
  - polje v glavi MPLS
  - uporablja se za posredovanje paketov
- **Pot LSP (angl. Label-Switched Path)**
  - enosmeren (angl. simplex) tunel skozi omrežje MPLS
- **Razred FEC (angl. Forwarding Equivalence Class)**
  - predstavlja skupino paketov (npr. datagrami IP), ki so na usmerjevalniku LSR obravnavani na enak način
  - Razred FEC se mapira v ustrezno pot LSP

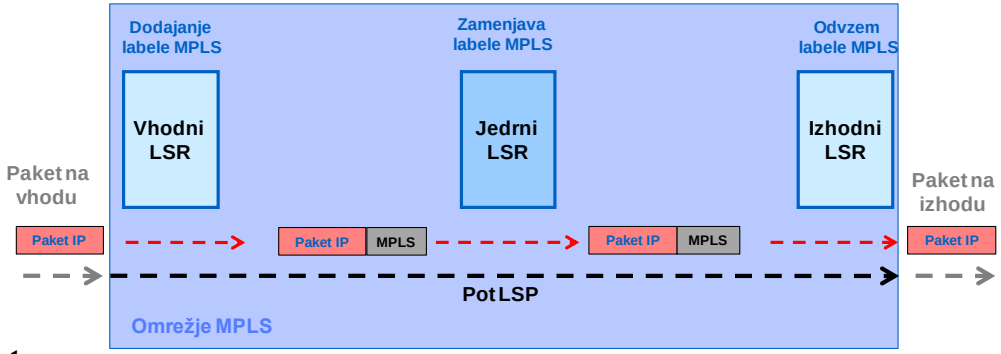
Osnovni koncepti – glava MPLS

- Glava MPLS – kratek identifikator fiksne dolžine (4 oktete)
  - vrine se pred prenašani PDU (npr. IP)
- Polja v glavi MPLS
  - polje “vrednost labele” (angl. Label value)
    - uporablja se za posredovanje paketov
  - eksperimentalno polje (angl. Exp/CoS)
    - uporablja se za zagotavljanje QoS
  - življenjski čas (angl. TTL)
    - uporablja se za preprečevanje zank v omrežju MPLS
  - polje s (angl. end of stack)
    - indikator zadnje labele v skladu

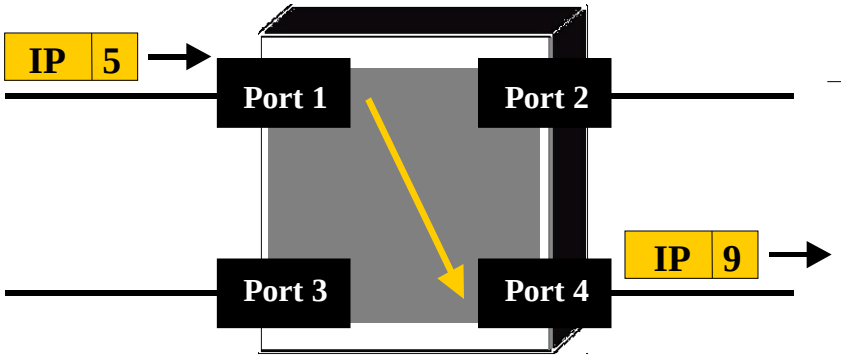


Osnovni koncepti – usmerjevalnik LSR

- **Angl. LSR – Label Switched Router**
  - glede na lokacijo v omrežju: vhodni, tranzitni, izhodni
  - izvaja tri osnovne operacije
    - dodajanje labele MPLS
    - zamenjava labele MPLS
    - odvzem labele MPLS



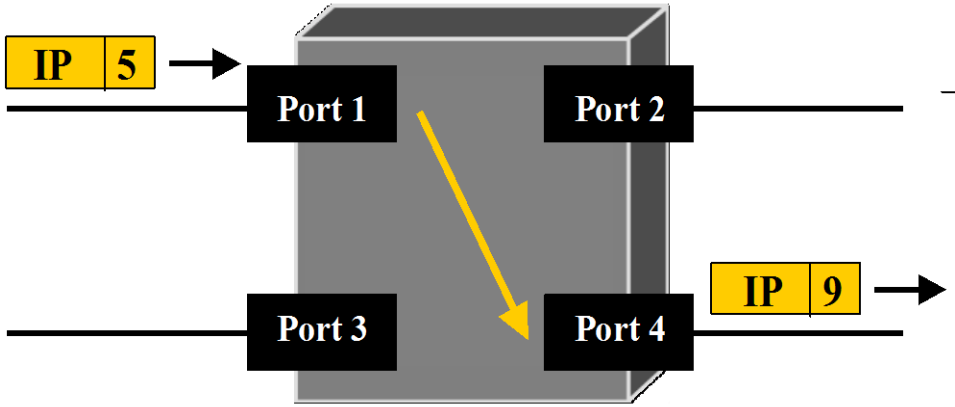
- **Zamenjava glave MPLS**
  - vhodni vmesnik in labela določata
    - operacijo: dodaj, zamenjaj, odstrani
    - izhodni vmesnik in izhodno labelo
  - podoben posredovalni mehanizem je bil uporabljen v ATM in FR



Vhod (port,labela)	Izhod (port,labela)	Labela Operacija
(1, 2)	(2, 7)	Zamenjava
(1, 4)	(3, 7)	Zamenjava
(1, 5)	(4, 9)	Zamenjava
(2, 3)	(3, 2)	Zamenjava

Osnovni koncepti – labela

- **Labela**
  - ima lokalen pomen
    - med dvema usmerjevalnikoma (LSR – Label Switch Router)
  - omogočen je sklad label
    - predstavlja osnovo za aplikacije MPLS
    - storitve VPN, TE in QoS
- **Pot LSP**
  - angl. Label-Switched Path
  - pot LSP predstavlja enosmeren (simplex) tunel skozi omrežje MPLS
  - predstavljamo si ga lahko kot zaporedje enega ali več hopov z zamenjavo label – analogija ATM in FR navideznim potem/kanalom



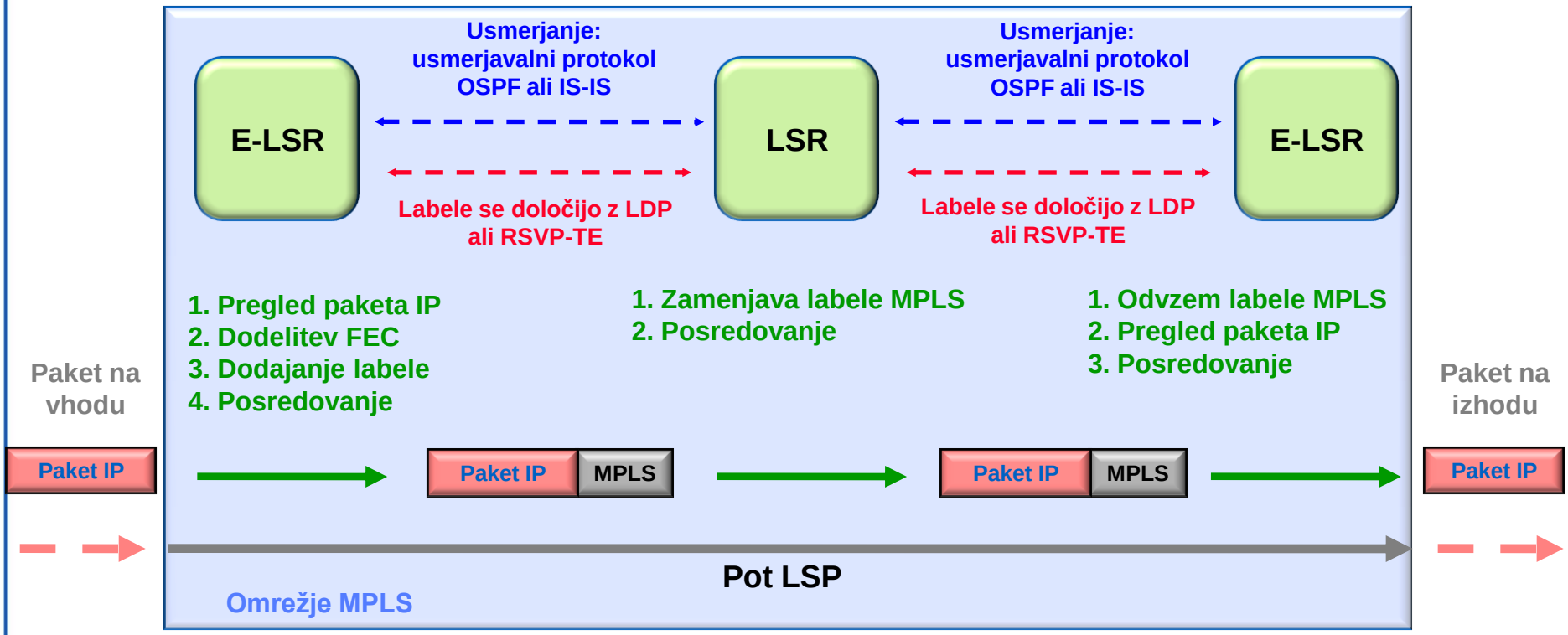
Vhod (port, labela)	Izhod (port, labela)	Labela Operacija
(1, 2)	(2, 7)	Zamenjava
(1, 4)	(3, 7)	Zamenjava
(1, 5)	(4, 9)	Zamenjava
(2, 3)	(3, 2)	Zamenjava

Osnovni koncepti – razred FEC

- Ekvivalentni posredovalni razred
  - FEC – Forwarding Equivalence Class
- Predstavlja pretok paketov (npr. IP), ki so s strani omrežja obravnavani na enak način
  - posredovani so po isti poti
  - povezani so na isto labelo
  - imajo zagotovljene enake razmere QoS
- Mehanizem za mapiranje FEC/labela
  - fleksibilno, odvisno od uporabljene signalizacije in storitev
  - izvorni/ciljni naslov IPv4/IPv6
  - izvorno omrežje, ciljno omrežje IPv4/IPv6
  - polje ToS/DSCP
  - logičen vmesnik

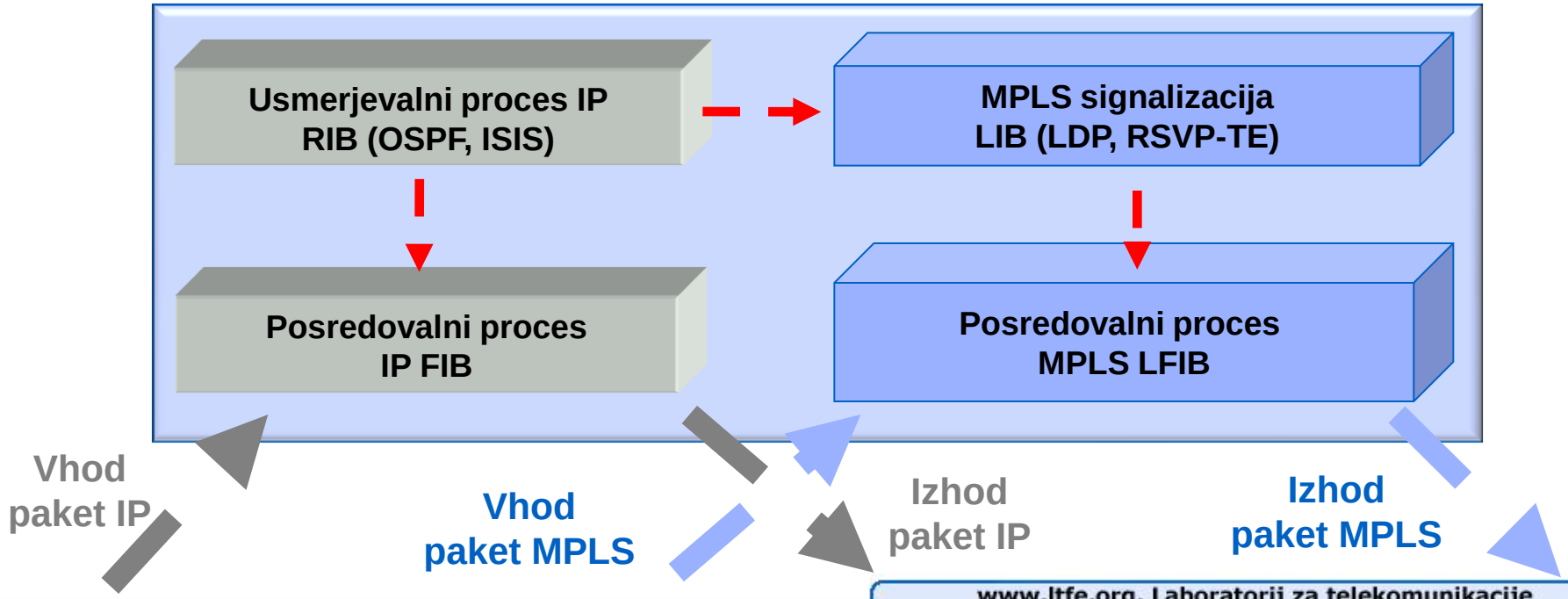
Delovanje MPLS

- **Komponente**
  - glava MPLS (labela)
  - usmerjevalniki LSR
    - robni, jedrni
  - pot LSP in razred FEC
- **Omrežje MPLS**
  - vpelje povezavno usmerjen (CO) princip v nepovezavno usmerjeno (CL) omrežje IP
  - poti LSP in signalizacija



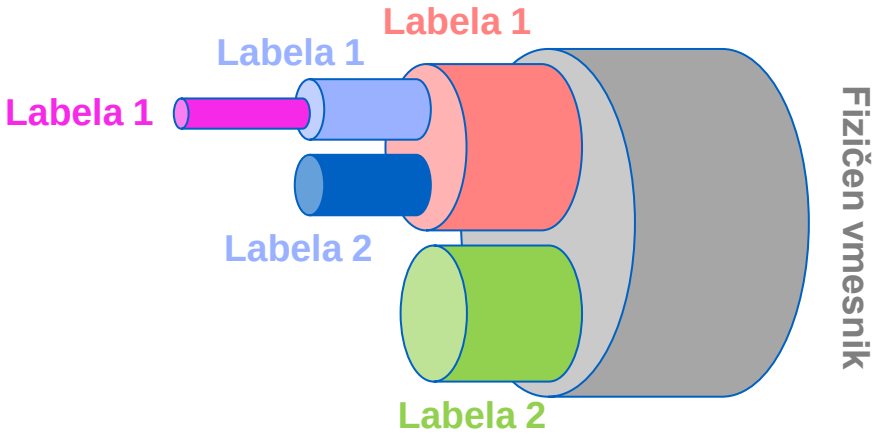
MPLS na usmerjevalniku IP

- **Ločitev kontrolne in podatkovne ravnine usmerjevalnika IP**
  - **kontrolna ravnina IP in MPLS**
    - **RIB – Routing Information Base (OSPF, ISIS)**
    - **LIB – Label Information Base (LDP, RSVP-TE)**
  - **podatkovna ravnina IP in MPLS**
    - **FIB – Forwarding Information Base (izvaja “longest-prefix match”)**
    - **LFIB – Label Forwarding Information Base (izvaja “exact match”)**



MPLS virtualizacijski mehanizmi 1/2

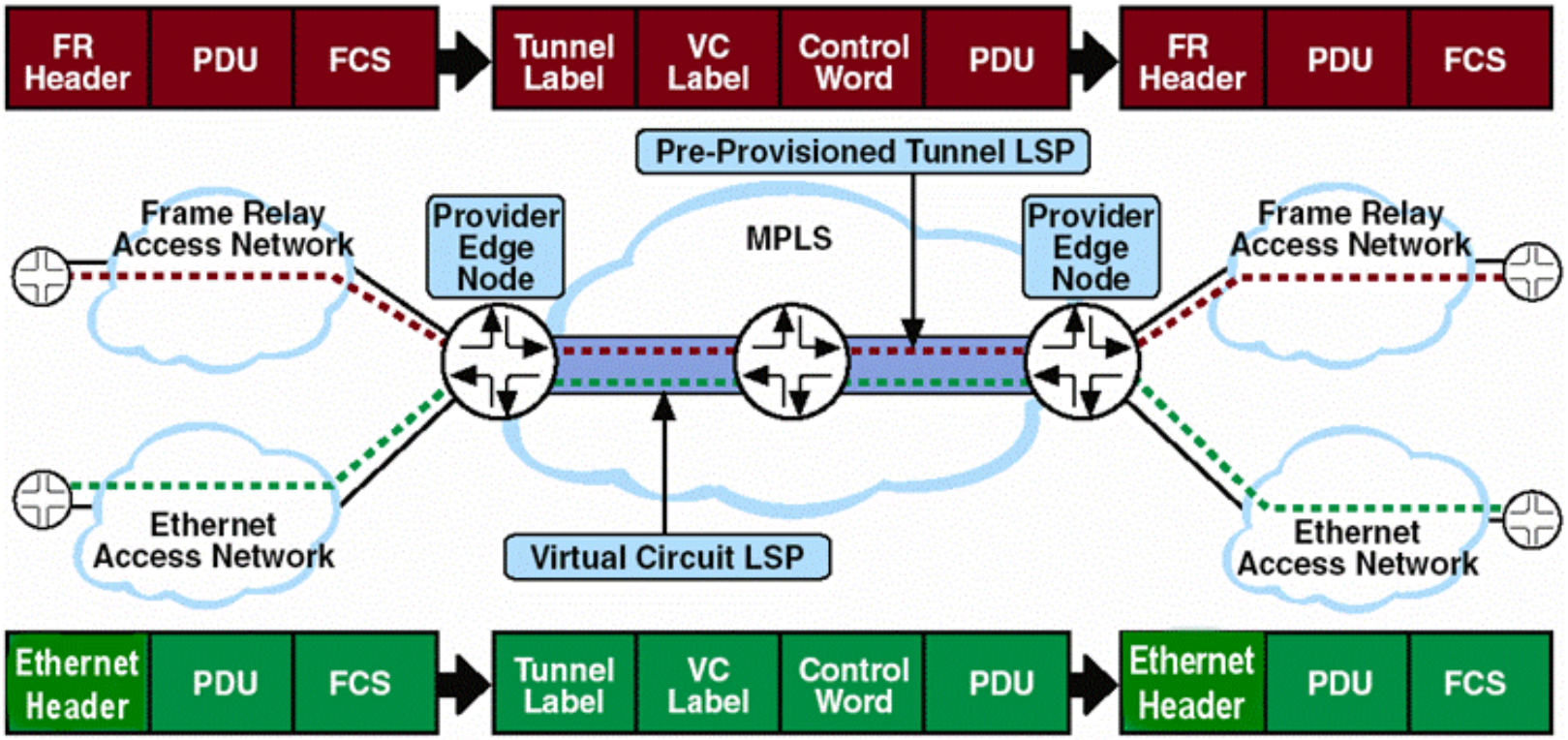
- **Logični vmesniki na usmerjevalniku IP/MPLS**
  - **povezovanje z logičnimi vmesniki - labela MPLS**
- **Tunelski mehanizmi**
  - **MPLS LSP**
- **Virtualizacija usmerjevalnika**
  - **mehanizem VRF – VPN Routing and Forwarding**



Sklad label MPLS

MPLS virtualizacijski mehanizmi 2/2

- Storitev navideznega zasebnega omrežja



Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- **Navidezna zasebna omrežja**
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

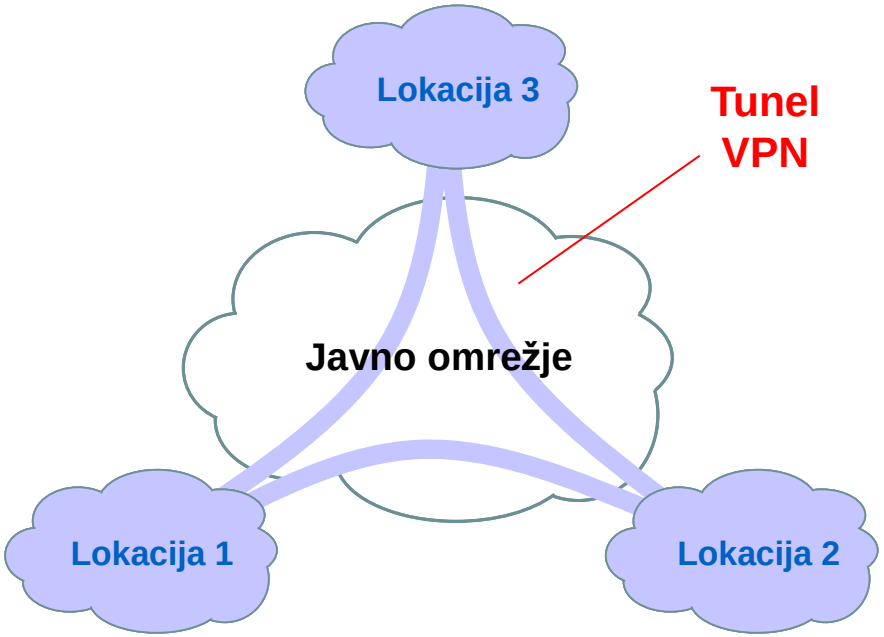
VPN – Virtual Private Network

- **Skupina geografsko razpršenih lokacij/omrežij, ki na varen način komunicira prek skupne (javne, operaterske) omrežne infrastrukture**
  - **Internet, omrežje MPLS, omrežje SDH, omrežje DWDM**

- **Primeri storitev VPN**
  - **L0 VPN – storitev transporta valovne dolžine (WDM)**
  - **L1 VPN – storitev transporta bitov (SDH)**
    - **za prenos FastEthernet prek SDH 125 Mbit/s**
  - **L2 VPN – storitev transporta uporabniških L2 PDU**
    - **Ethernet okvir, ATM celica, FR paket**
  - **L3 VPN – storitev transporta uporabniških L3 PDU, zagotavljanje usmerjanja**
    - **IP datagram (BGP/MPLS, IPSec, GRE)**
    - **prenos usmerjevalnih informacij (BGP/MPLS VPN)**

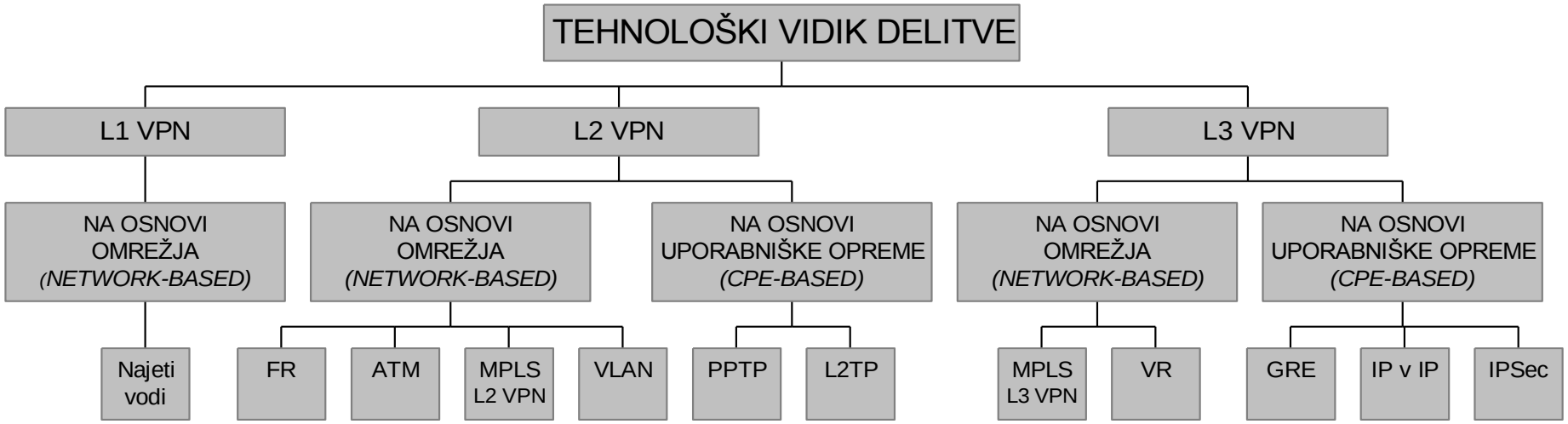
Osnovni koncepti VPN

- **Tunelski mehanizem**
  - zagotavlja neodvisen format paketov znotraj tunela od mehanizmov za prenos skozi javni del omrežja
- **Transparentnost**
  - uporaba lastne naslovne sheme, prenos različnih tipov PDU
- **Varnost**
  - onemogočeno prestrezanje, branje, spreminjanje in potvarjanje podatkov
- **Podpora QoS**
  - zagotavljena pasovna širina, predvidljive zakasnitve, variacija zakasnitve, razpoložljivost
- **Preprosta razširljivost**
  - preprosto dodajanje novih lokacij, povečevanje pasovne širine



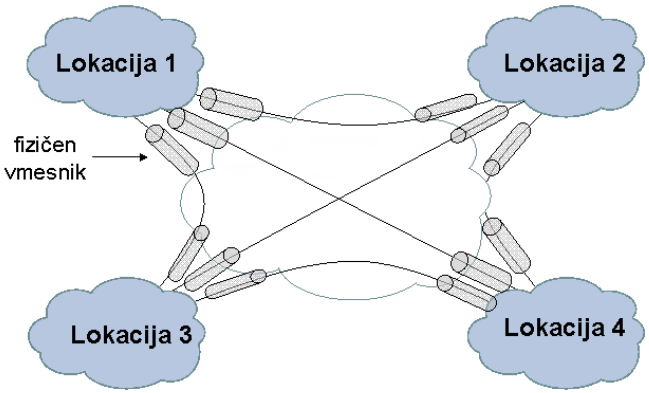
Delitev rešitev VPN

- **Funkcionalni vidik**
  - **rešitve za oddaljen dostop**
  - **rešitve za povezovanje lokalnih omrežij (intranet, ekstranet)**
- **Tehnološki vidik**
  - **storitve VPN se lahko zagotavljajo na slojih L1, L2, L3, L4 in L7 referenčnega modela OSI**

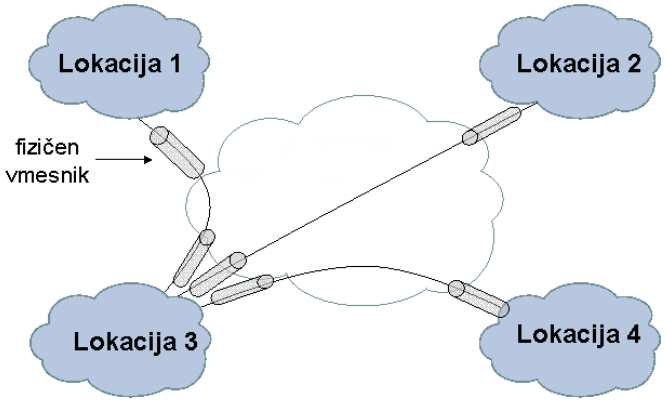


Tradicionalne rešitve VPN

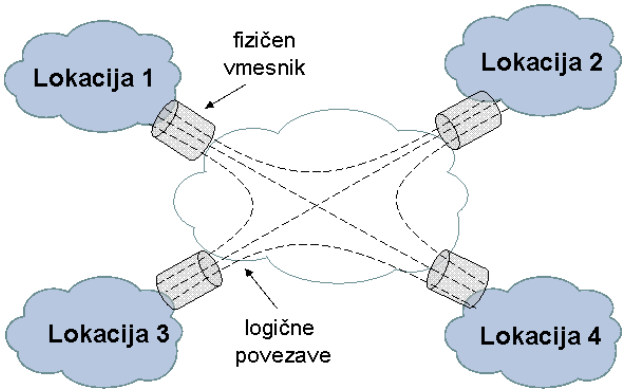
- **Najeti vodi (SDH, LL)**
  - **popolna mreža povezav**



  - **topologija zvezda**

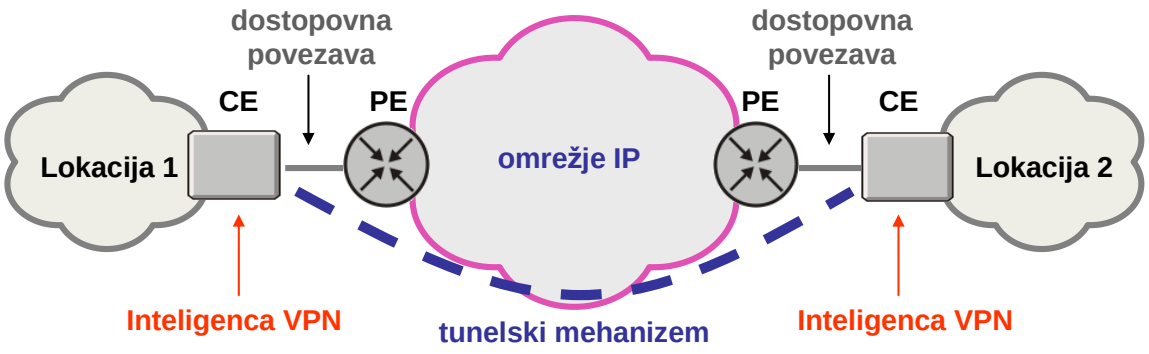


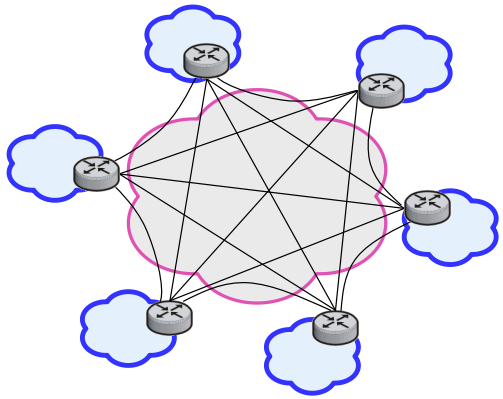
- **Povezave L2 (ATM, FR)**
  - **popolna mreža povezav**



Rešitve na osnovi uporabniške opreme

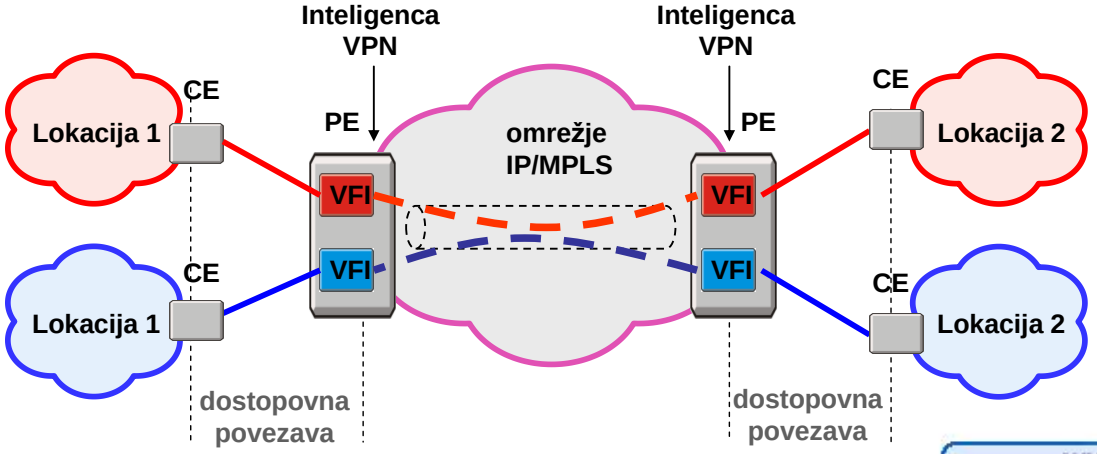
- CPE – Customer Premises Equpment
- Vse potrebne informacije o omrežju VPN so vsebovane v napravah CPE
- Uporabnik sam poskrbi za gradnjo tunelov prek javnega omrežja
  - za optimalno usmerjanje je potrebna popolna mreža povezav (N^2 problem)
- Funkcionalnosti VPN so vgrajene v omrežne naprave, kot so požarni zidovi, robni usmerjevalniki in specializirane terminalne naprave VPN

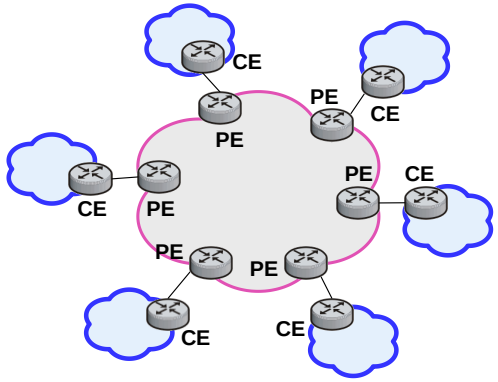




Omrežne rešitve (network-based)

- Vse potrebne informacije o omrežju VPN so vsebovane v omrežnih napravah ponudnika storitev
- Za načrtovanje omrežja in usmerjanje poskrbi ponudnik storitev
- Uporabnik najame storitev VPN pri ponudniku storitev
  - stroški načrtovanja, opreme, izgradnje, vzdrževanja, upravljanja in podpore se porazdelijo med več uporabnikov
  - uporabnik je lahko manj izobražen, kar pa pomeni več dela in več odgovornosti za ponudnika storitev
  - ponudnik prodaja storitev z večjo dodano vrednostjo





Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

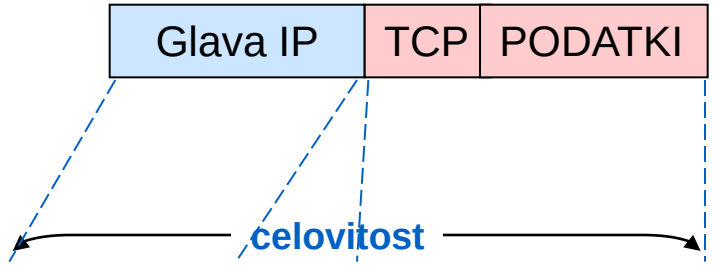
Varnostne storitve protokola IPSec

- Avtentikacija izvora podatkov
  - zajamči točnost izvora podatkov
- Zaupnost podatkov
  - preprečuje prebiranje in kopiranje podatkov, ko se prenašajo prek javnega omrežja
- Nepovezavna celovitost podatkov
  - zagotavlja, da podatki v času prenosa skozi omrežje niso bili spremenjeni
- Nadzor dostopa
- Delno prekrivanje prometnega pretoka
- Zaščita pred podvajanjem datagramov IP
- Dodatna storitev: stiskanje (kompresija) podatkov

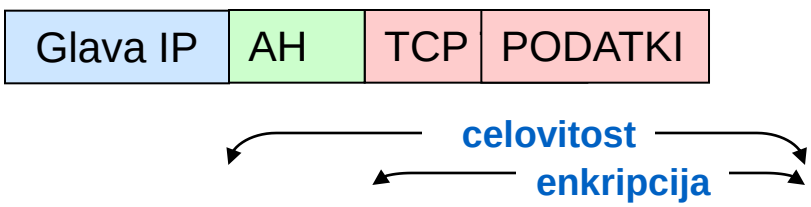
Prenosna načina IPSec

- **Transportni način**

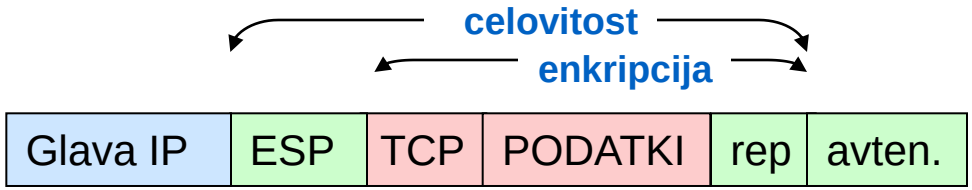
Originalni paket IP



Protokol AH



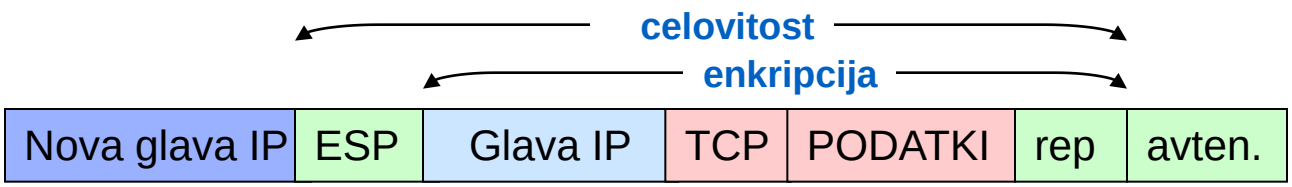
Protokol ESP



- **Tunelski način**

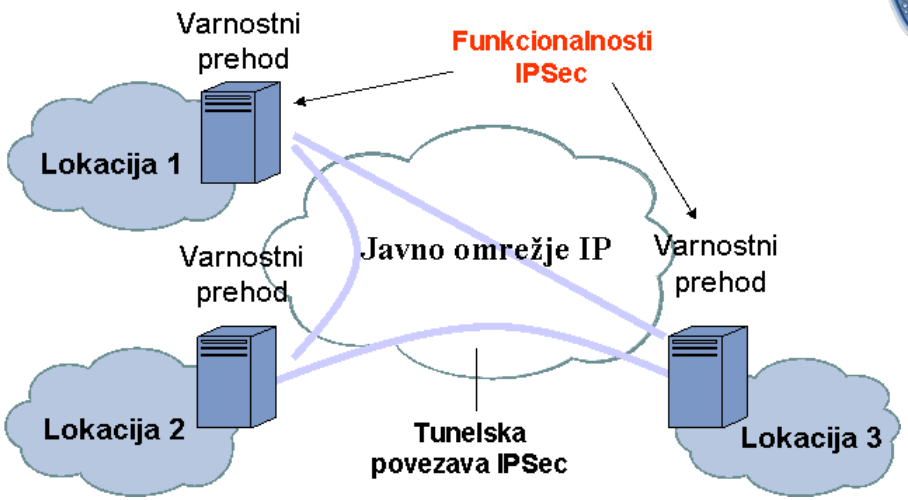
Protokol AH

Protokol ESP

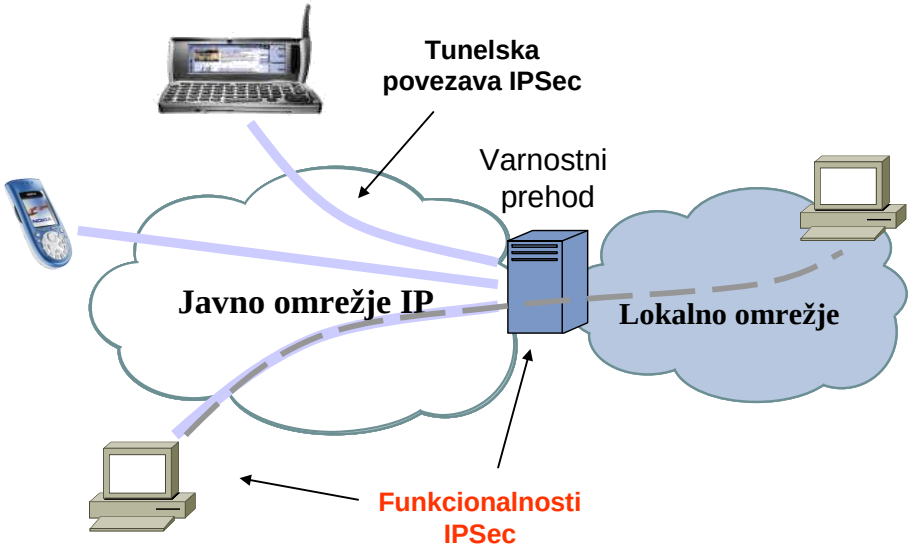


IPSec v omrežjih VPN 1/2

- **Rešitve VPN na osnovi IPSec tipično uporabljajo protokol ESP v tunelskem načinu prenosa**
  - omogoča uporabo privatnega naslovnega prostora
  - prekrivanje izvora podatkov
  - multipleksiranje
- **Primer omrežja VPN**



Povezovanje lokalnih omrežij



Oddaljen dostop

IPSec v omrežjih VPN 2/2

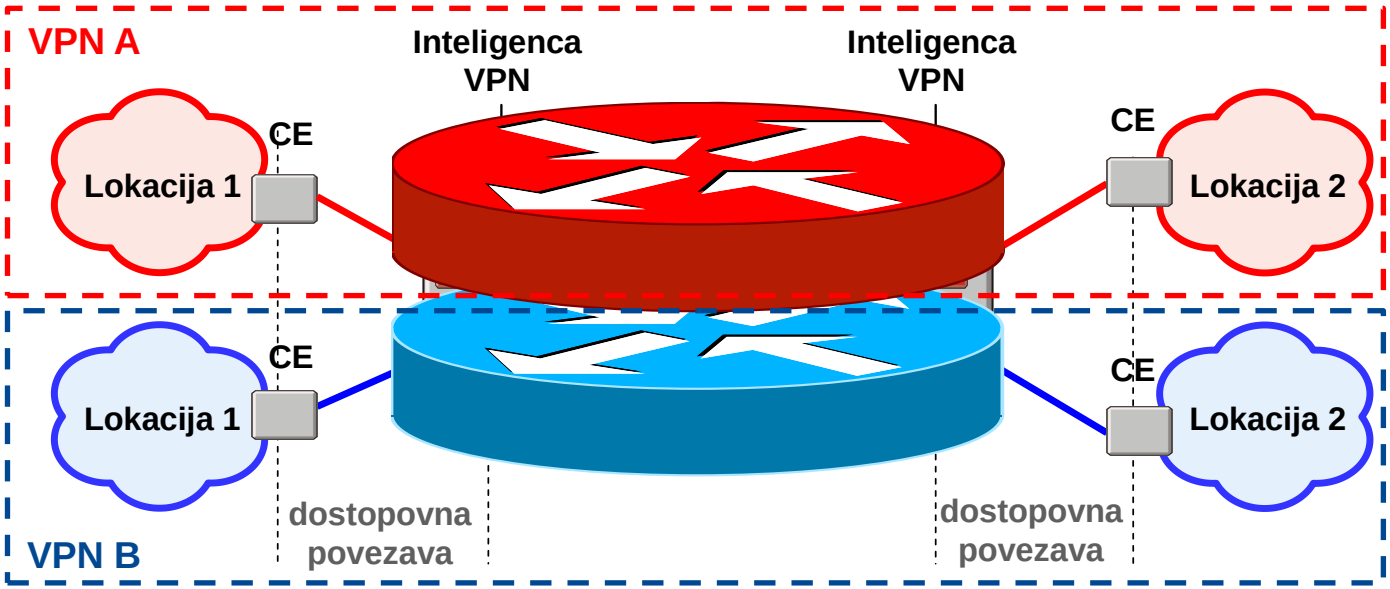
- **Prednosti**
  - celovit varnostni mehanizem
  - implementacija je možna prek katerega koli omrežja IP
    - mobilna omrežja
    - brezžična omrežja
    - fiksna omrežja
  - omogoča globalno pokrivanje
- **Slabosti**
  - problem vzdrževanja velikega števila tunelov
    - N^2 - problem

Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

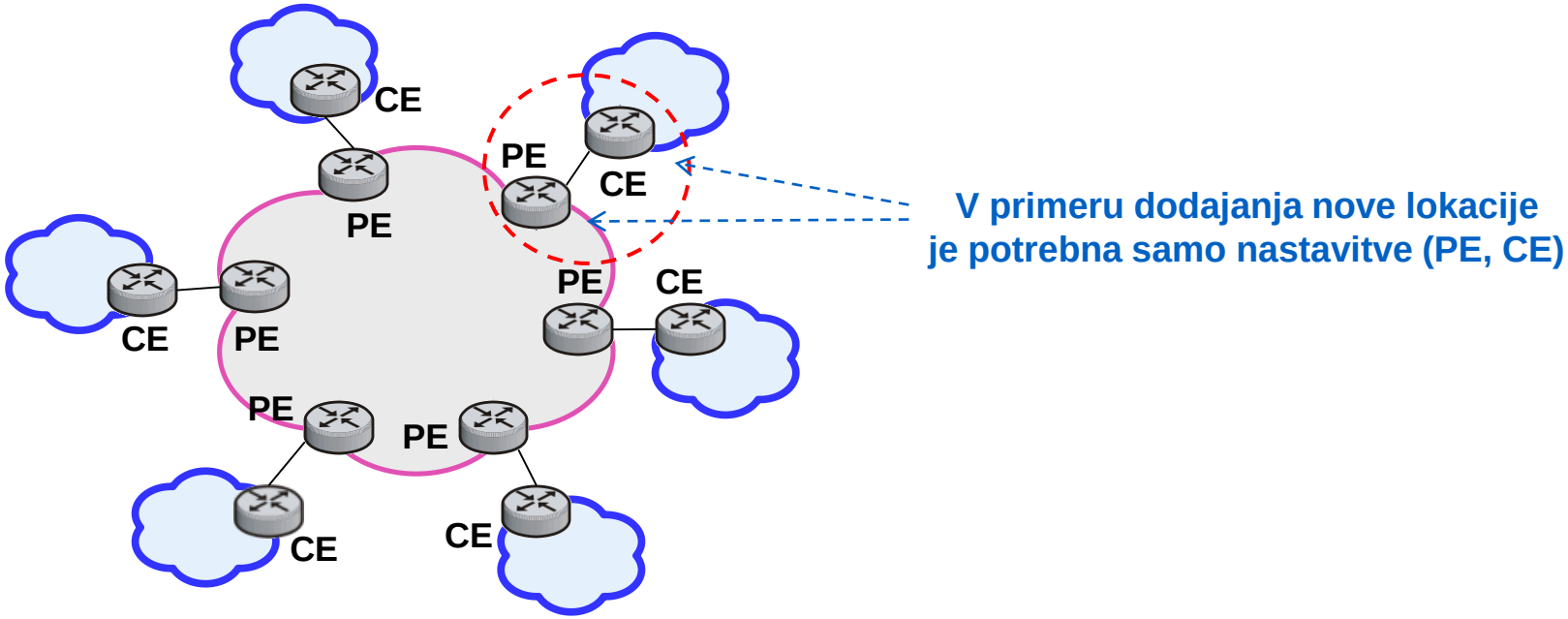
Povezavni model BGP/MPLS VPN

- S stališča uporabnikov VPN deluje omrežje ponudnika storitev kot en usmerjevalnik
  - Omrežje BGP/MPLS VPN poskrbi za prenos uporabniških PDU (paketi IPv4, IPv6) med lokacijami VPN
  - Omrežje BGP/MPLS VPN poskrbi za prenos usmerjevalnih informacij med lokacijami VPN



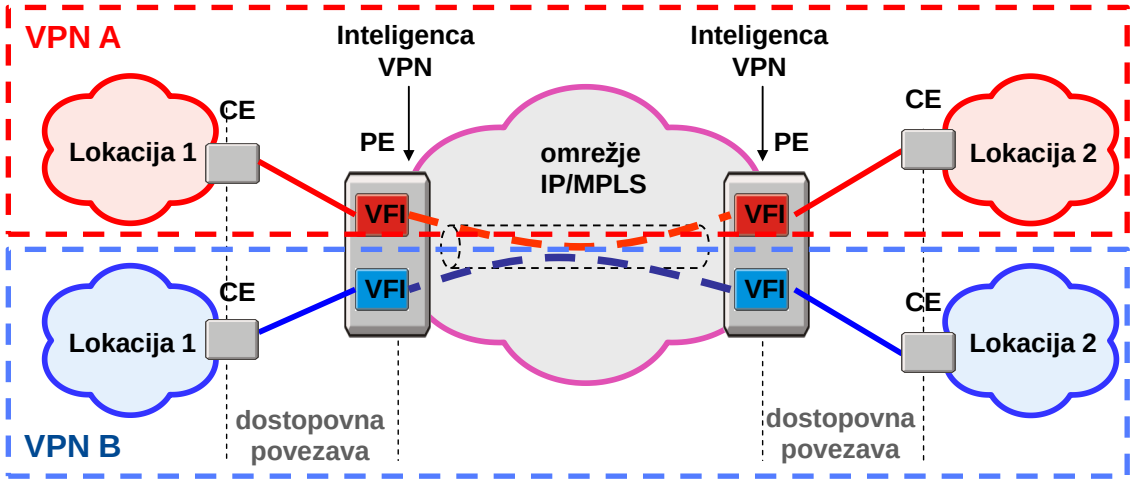
Povezavni model BGP/MPLS VPN

- **Za dodajanje nove lokacije v omrežje VPN je potrebno nastaviti samo robni napravi PE in CE**
  - **Za signalizacijo in distribucijo VPN informacij poskrbijo mehanizmi BGP/MPLS VPN – signalizacij s protokolom MP-BGP**



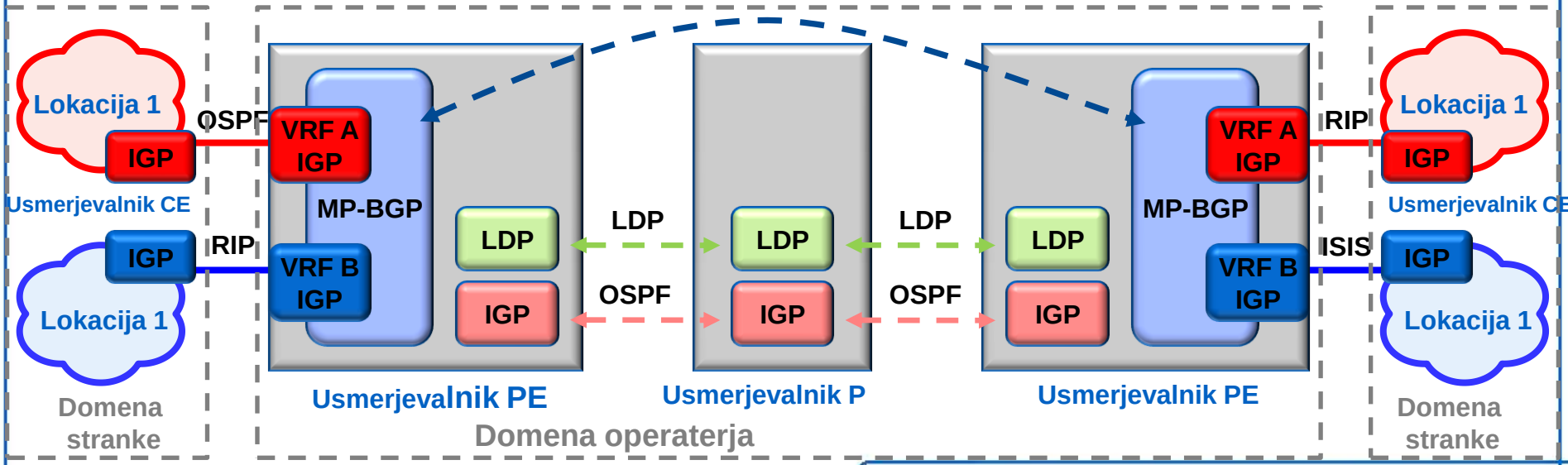
Arhitektura MPLS VPN

- Robna naprava uporabnika (CE – Customer Edge device)
  - usmerjevalnik ali terminalna oprema, ki se nahaja na robu omrežja uporabnika
- Robni usmerjevalnik ponudnika (PE – Provider Edge router)
  - usmerjevalnik, ki se nahaja na robu omrežja ponudnika storitev
- Hrbtenični usmerjevalnik (P – Provider router)
  - usmerjevalnik, ki se nahaja v jedru ponudnikovega omrežja
- Dostopovne povezave (Attachment circuit)
  - naprave CE in PE so lahko medseboj povezane s povezavami Ethernet, ADSL, PPP, ATM, FR, IPSec, L2TP, GTP



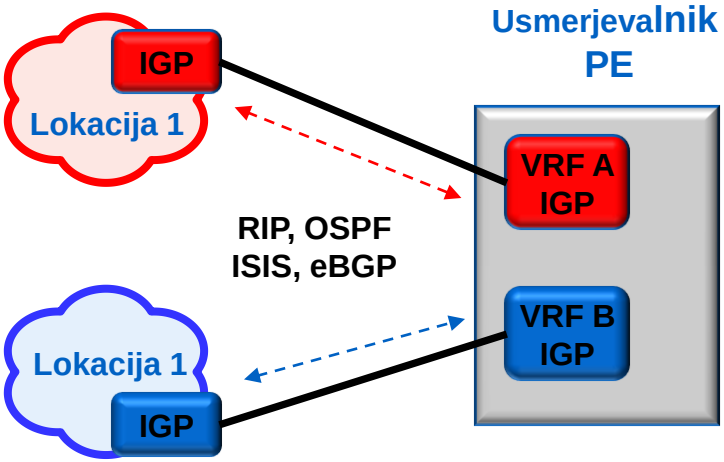
Komponente BGP/MPLS VPN 1/3

- **Kontrolna ravnina**
  - **med napravami PE in CE – standardni usmerjevalni protokoli (IGP)**
  - **na napravi PE – usmerjevalna in posredovalna tabela VPN (VRF)**
    - **omogoča razlikovanje med različnimi omrežji VPN**
  - **med napravami PE – razširjena verzija protokola BGP (MP-BGP)**
    - **nova naslovna shema VPN-IPv4, prenos label**
  - **med napravami v jedru omrežja – usmerjevalni protokoli IGP (OSPF, ISIS) in signalizacija MPLS (LDP, RSVP-TE)**



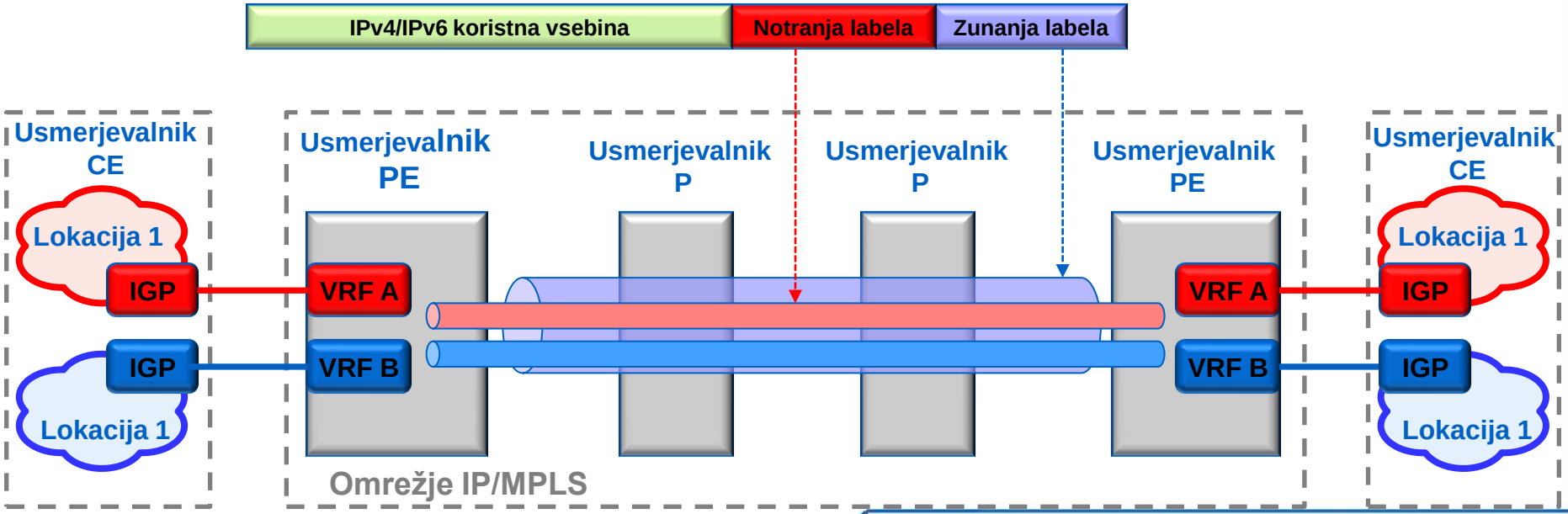
Komponente BGP/MPLS VPN 2/3

- Povezljivost med napravami CE in PE
  - med usmerjevalniki CE in PE je potrebna “IP povezljivost”
    - dostopovne povezave so lahko izvedene na osnovi Ethernet/VLAN, xDSL, PPP, ATM, FR, IPSec, L2TP, GTP
  - vsaka dostopovna povezava (fizična, logična, tunel) je povezana s svojo tabelo VRF
  - usmerjevalniki PE vzdržujejo ločene tabele VRF za vsak VPN
    - zagotavljajo ločevanje med različnimi omrežiji VPN
    - omogočajo prekrivno naslovno shemo med različnimi omrežji VPN
  - izmenjava usmerjevalnih informacij VRF-VPN poteka na osnovi klasičnih usmerjevalnih protokolov
    - statično, RIP, OSPF, IS-IS, eBGP



Komponente BGP/MPLS VPN 3/3

- **Podatkovna ravnina – sklad label zagotavlja transparenten prenos IPv4/IPv6 prek hrbteničnega omrežja IP/MPLS**
  - **zunanja labela zagotavlja povezljivost LSP med napravami PE (popolna mreža tunelov MPLS med napravami PE)**
    - **distribucija label (zunanjih) poteka na osnovi protokola LDP, RSVP-TE**
    - **kot tunelski mehanizem se lahko uporabi tudi IPSec, IPvIP ali GRE**
  - **notranja labela določa omrežje VPN**
    - **distribucija label (notranjih) poteka na osnovi protokola MP-BGP**

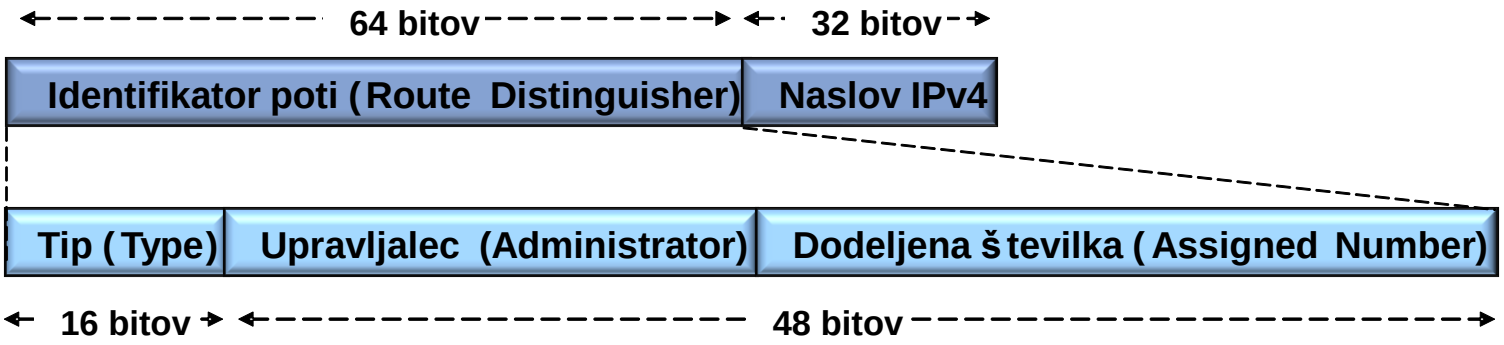


Protokol MP-BGP

- Usmerjevalniki PE si izmenjujejo usmerjevalne informacije VPN na osnovi protokola MP-BGP
  - med usmerjevalniki PE mora biti vzpostavljena popolna mreža sej
  - opcijsko se lahko uporabijo reflektorji poti (RR – Route Reflector)
    - zagotavlja razširljivost
- Tipično se oglašujejo sledeči parametri
  - oglaševana pot VPN-IPv4
    - RD – Route Distinguisher
  - naslov naslednjega hopa (BGP next hop)
    - določa izvorni usmerjevalnik PE
  - identifikator oglaševane poti (RT – Route Target)
    - določa skupino lokacij kateri se lahko oglašuje izbrana pot
  - pripadajoča labela MPLS
    - določa lahko izhodno dostopovno povezavo ali tabelo VRF

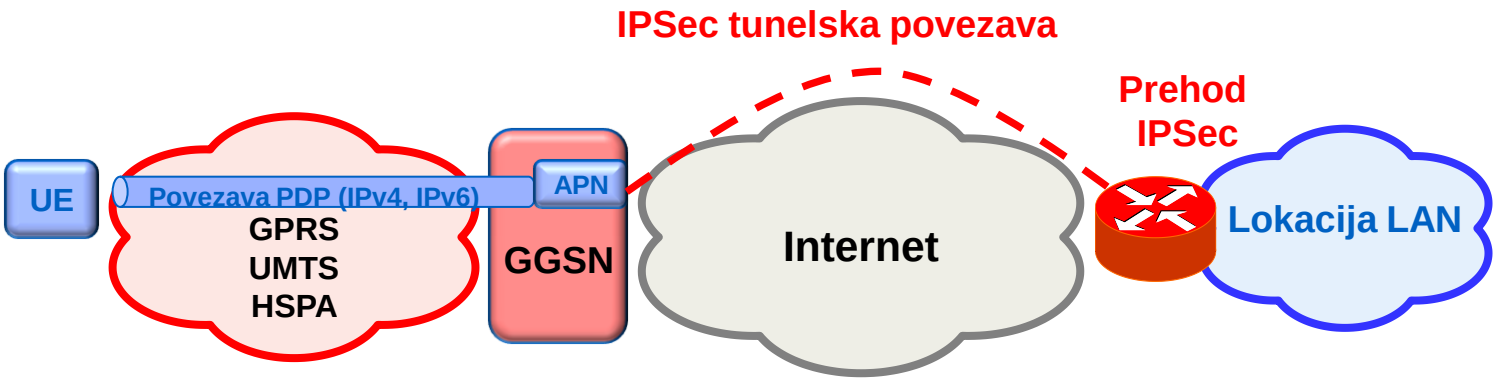
Naslovna shema VPN-IPv4

- Naslov VPN-IPv4 je globalno unikaten naslov, ki je sestavljen iz dveh delov
  - identifikatorja poti (RD – Route Distinguisher)
    - omogoča globalno unikatnost privatnih naslovov IPv4
    - dodeljen je vsaki tabeli VRF
  - naslova IPv4
    - naslovi, ki so uporabljeni znotraj omrežja VPN
- Format identifikatorja RD
  - polje Tip določa interpretacijo polja Upravljalec in Dodeljena številka
  - trenutno so definirani trije tipi identifikatorjev RD (Tip 0, Tip 1, Tip 2)

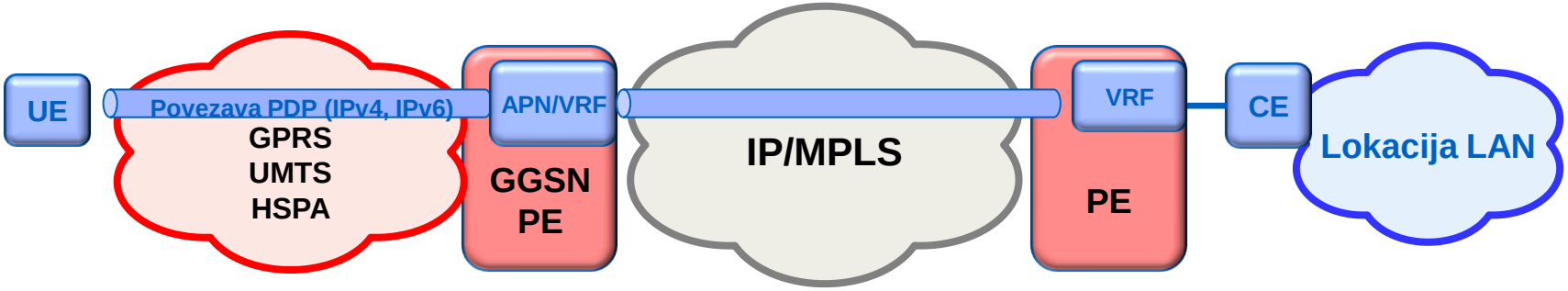


Primer uporabe MPLS in APN VPN

- **Storitev L3 VPN – storitev zagotavlja mobilni operater**
  - **QoS ni zagotovljen**



- **Storitev L3 VPN (BGP/MPLS VPN)**
  - **storitev zagotavljata mobilni in fiksni operater**
  - **Ustrezne razmere QoS se lahko zagotovi na celotni prenosni poti**



BGP/MPLS VPN v praksi

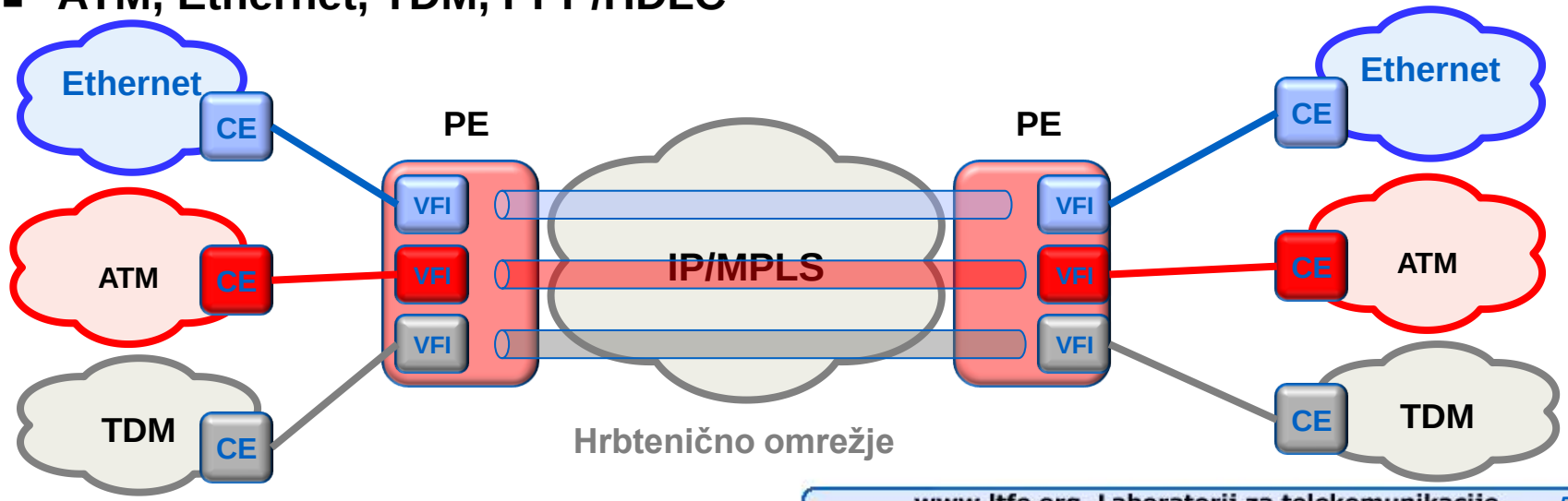
- V segmentu storitev IP VPN prevladujejo BGP/MPLS VPN rešitve
  - največkrat uporabljani topologiji sta “full mesh” in “hub and spoke”
- Uporabnik mora popolnoma zaupati ponudniku storitev
  - ponudnik storitev poskrbi za načrtovanje omrežja, usmerjanje, vzdrževanje in upravljanje
  - ponudnik mora prevzeti večjo odgovornost kot pri klasičnih L2 VPN
- Da se na Ethernet povezavah ne izvaja fragmentacija paketov, je potrebno na vmesniku povečati MTU
  - v primeru BGP/MPLS VPN je to vsaj 8 oktetov (2 × glava MPLS)

Vsebina

- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

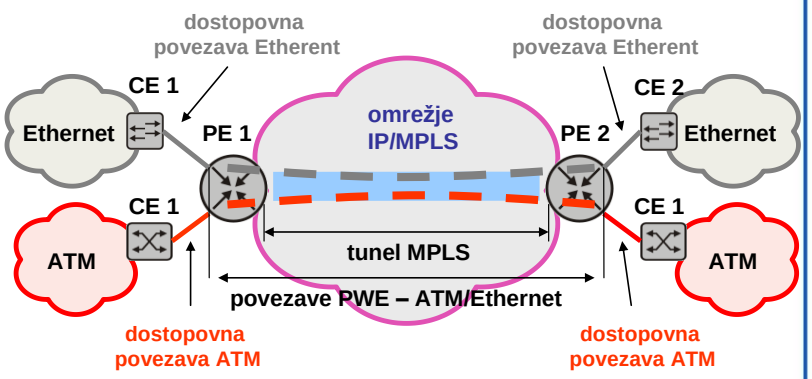
L2 MPLS VPN

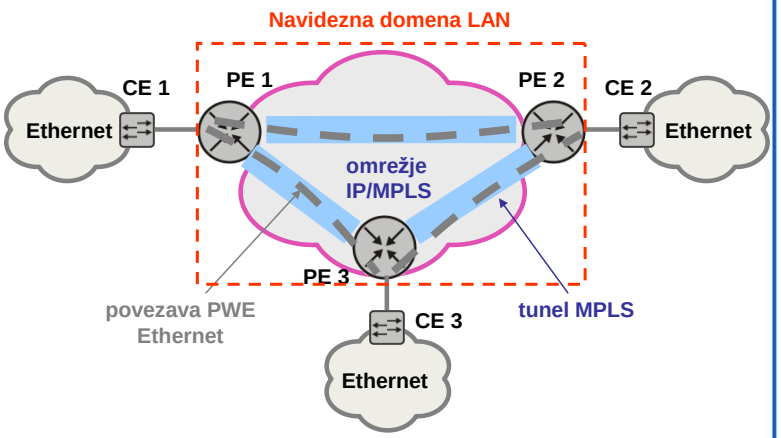
- **Motivacija**
  - ena transportna infrastruktura (MPLS) za vse vrste prometa
- **Možnost prenosa "katerega koli" tipa prometa**
  - ATM celice, ATM AAL5, FR, Ethernet, Ethernet VLAN, PPP/HDLC, Sonet/SDH, TDM
  - velika teorija poenotenja (še ena)
- **Ponudnik storitev ne sodeluje pri usmerjanju prometa**
  - zagotavlja le povezljivost L2
- **Uporabniki ohranijo obstoječo dostopovno tehnologijo**
  - ATM, Ethernet, TDM, PPP/HDLC



Trije tipi storitev L2 MPLS VPN

- **Storitev VPWS (Virtual Private Wire Service)**
  - emulacija linka “point-to-point” (PWE)
  - podobno kot storitve ATM in FR
  - prenos prometa Ethernet, ATM, FR, TDM, SDH, PPP/HDLC
- **Storitev VPLS (Virtual Private Lan Service)**
  - “multipoint”
  - transparentna storitev LAN (LAN emulacija)
  - omrežje ponudnika emulira stikalo L2 oziroma bridge
- **Storitev IPLS (IP-only LAN Service)**
  - “multipoint”
  - prenos prometa IP na osnovi informacij L2
  - naprave na strani uporabnika morajo biti L3 (usmerjevalnik, terminalna oprema IP)





Storitev navideznega zasebnega voda

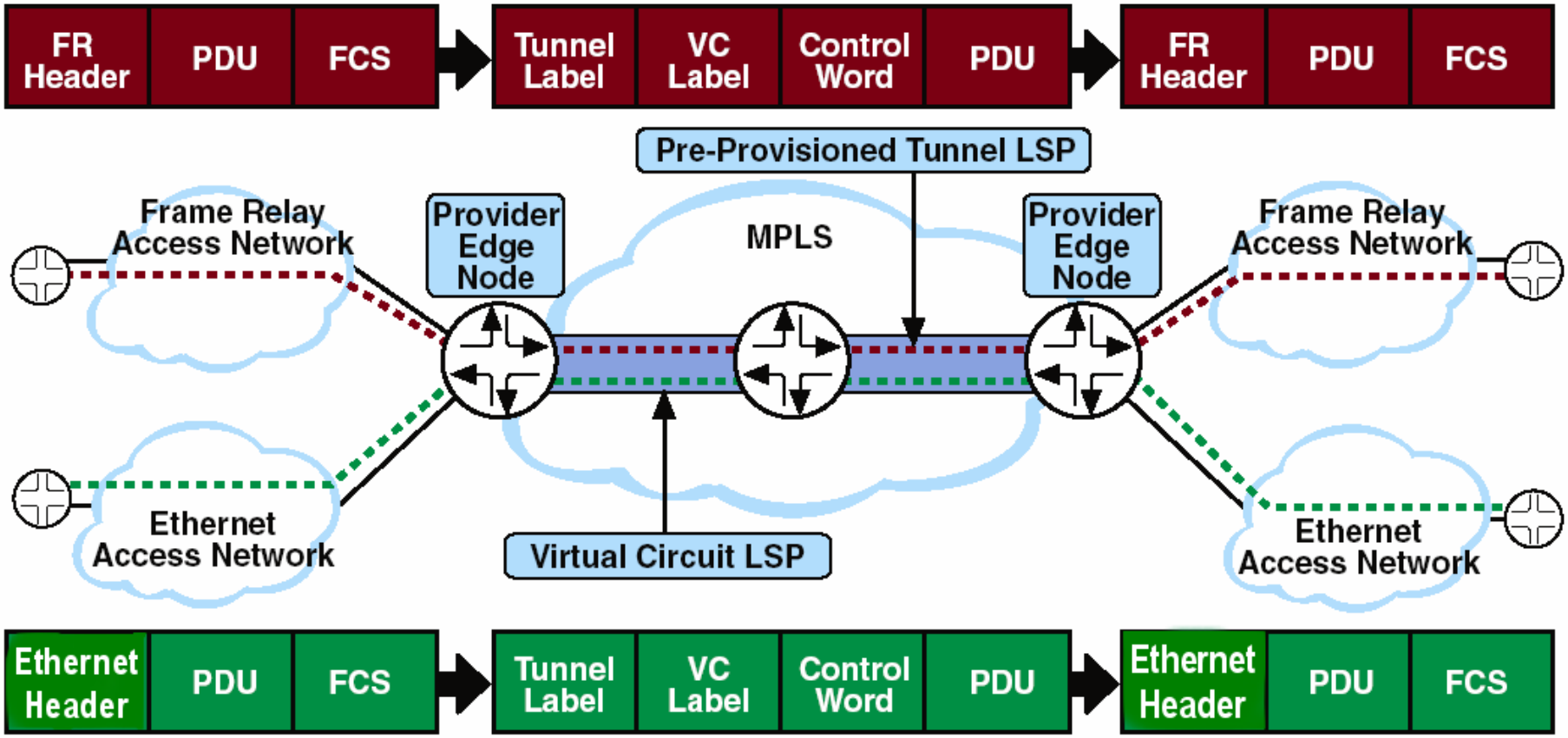
VPWS

Storitev VPWS

- Emulacija povezav “točka-točka”
  - PWE – Pseudo Wire Emulation
- Uporabniki ohranijo obstoječo dostopovno tehnologijo
  - FR, ATM, Ethernet, PPP/HDLC
- Sklad label omogoča transparenten prenos L2 okvirjev/celic prek hrbteničnega omrežja
  - zunanja labela (Tunnel Header) določa pot skozi hrbtenično omrežje
  - notranja labela (Demux Field) določa omrežje L2 VPN oziroma izhodno povezavo
- Signalizacija med robnimi usmerjevalniki PE
  - LDP kontrolna ravnina (Draft-Martini)
    - signalizacija temelji na protokolu LDP
    - LDP deluje v načinu “point-to-point”
    - vzpostavitev PW se signalizira samo tistemu PE, ki sodeluje pri PWE
  - BGP kontrolna ravnina (Draft-Kompella)
    - signalizacija temelji na protokolu MP-BGP (podobno kot BGP/MPLS)
    - BGP deluje v načinu “point-to-multipoint”
    - vzpostavitev PWE se signalizira vsem robnim PE

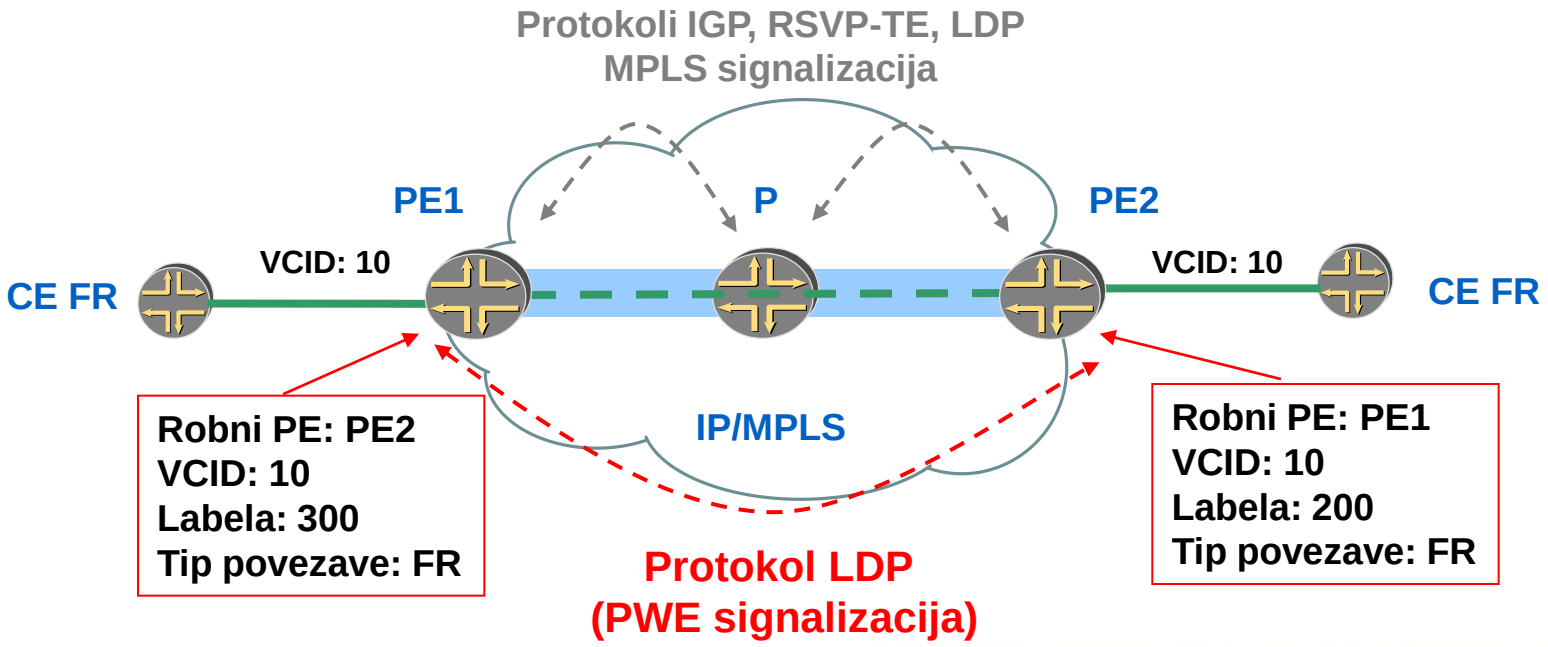
Povezavni model VPWS

- Primer inkapsulacije FR in Ethernet prek IP/MPLS



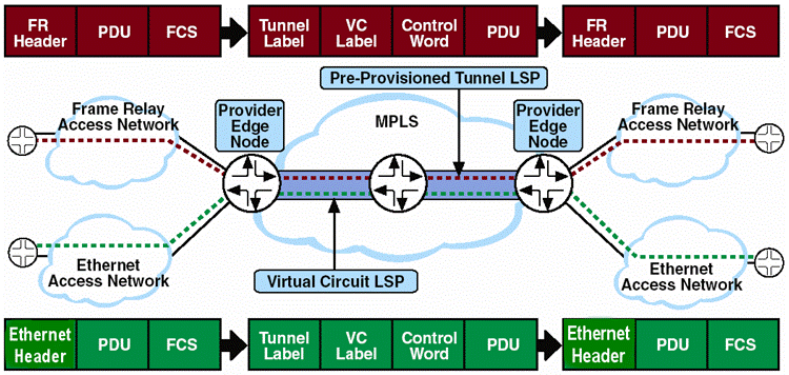
Signalizacija VPWS

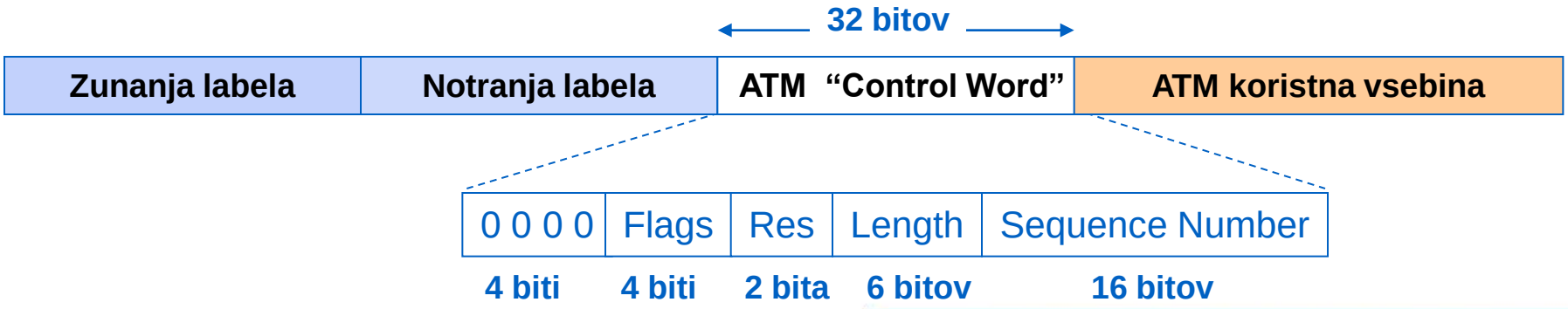
- V hrbteničnem omrežju MPLS (IP/MPLS signalizacija)
  - protokoli RIP, OSPF, IS-IS, BGP (IGP)
  - protokoli LDP, RSVP-TE (distribucija label)
- Med robnimi napravami PE (PWE signalizacija)
  - protokol MP-BGP
  - protokol LDP
- Primer: LDP



Tunelski mehanizem

- **Zunanja labela**
  - **določa LSP med dvema PE**
- **Notranja labela**
  - **določa povezavo PWE**
- **ATM "Control Word" (2 tipa)**
  - **zgradba polja CW za N:1 celični način ter ALL5 SDU način**
    - **prvi 4 biti so rezervirani (0000)**
    - **Flags: prenos parametrov iz glave ATM (EFCI, CLP ...)**
    - **Length: če je paket manjši od 64 oktetov (doda se mu "padding") določa velikost paketa, drugače je polje zapolnjeno z ničlami**
    - **Sequence Number: za zagotavljanje pravilnega vrstnega reda prispelih paketov**





Emulacija povezave ATM – načini delovanja

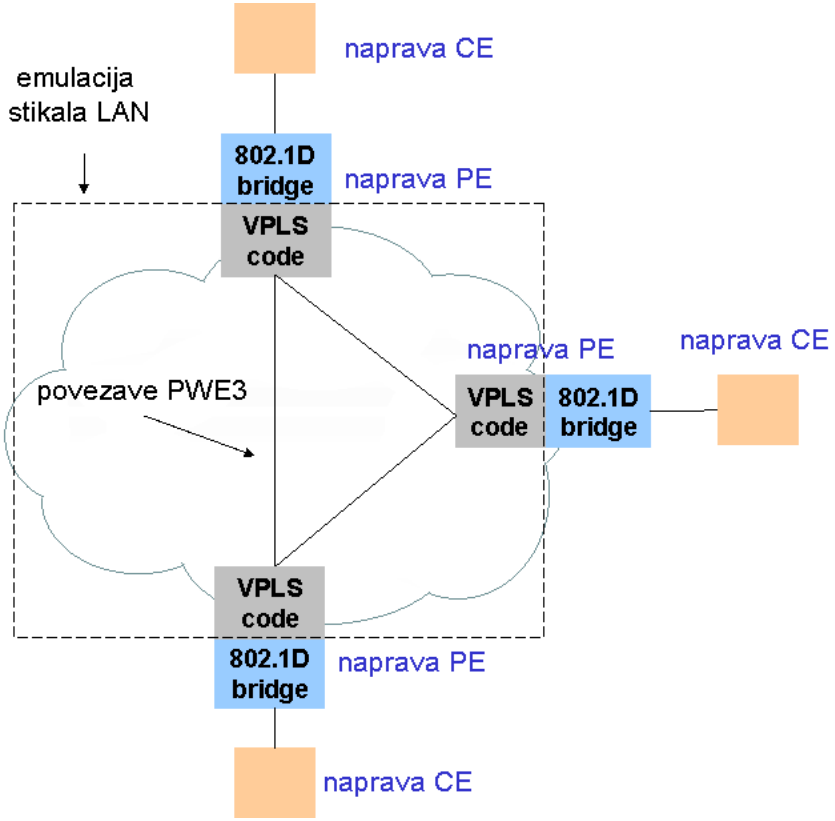
- Prenos ATM celic – “ATM cell mode”
  - “1:1 celični način”:
    - vsak VPC (Virtual Path Connection) oziroma VCC (Virtual Channel Connection) se prenaša v svoji povezavi PWE
    - boljši izkoristek pasovne širine
    - ni potrebno prenašati VPI/VCI v primeru VCC ter VCI v primeru VPC
  - “N:1 celični način”
    - več VPC/VCC se lahko prenaša v eni povezavi PWE
  - omogočata prenos vseh AAL tipov
  - boljši izkoristek pasovne širine se lahko doseže s postopkom “Cell Concatenation” – prenos večih celic znotraj enega transportnega PDU
- Prenos ATM AAL5 – “ATM AAL5 mode”
  - AAL5 PDU način
    - transparenten za ATM OAM
  - AAL5 SDU način
    - ni transparenten za ATM OAM
    - SDU je PDU zmanjšan za AAL5 trailer (8 oktetov)

Storitev navideznega zasebnega omrežja LAN

VPLS

Emulacija segmenta LAN (VPLS)

- Emulacija segmenta LAN prek hrbteničnega omrežja IP/MPLS
- Topologije VPLS
  - point-to-point
  - point-to-multipoint
  - any-to-any
- Naprava PE zagotavlja
  - funkcinalnost Ethernet bridge
    - IEEE 802.1D
    - tabela CAM
  - funkcionalnost VPLS
    - posredovalni mehanizem
    - signalizacijski mehanizem



- STP/RSTP BPDU se filtrirajo na vhodu v PWE
  - za preprečevanje zank se uporablja mehanizem “split-horizon”

Standardizacija VPLS v IETF

- Signalizacija zagotavlja dve ločeni funkciji
  - iskanje naprav PE, ki sodelujejo v izbranem VPLS
  - izmenjava parametrov za vzpostavitev povezav PWE
- Draft Kompella
  - draft-ietf-l2vpn-vpls-bgp-03.txt
  - signalizacija temelji na protokolu MP-BGP
    - koncept BGP/MPLS VPN
    - omogoča “avtomatsko” vzpostavitev povezav
- Draft Lasserre-V.Kompella
  - draft-ietf-l2vpn-vpls-ldp-05.txt
  - signalizacija temelji na protokolu LDP
- Radius
  - draft-ietf-l2vpn-radius-pe-discovery-00.txt
  - draft-ietf-l2vpn-l2tp-radius-vpls-00.txt
  - dobro poznan protokol med operaterji
  - omogoča avtentikacijo in avtorizacijo