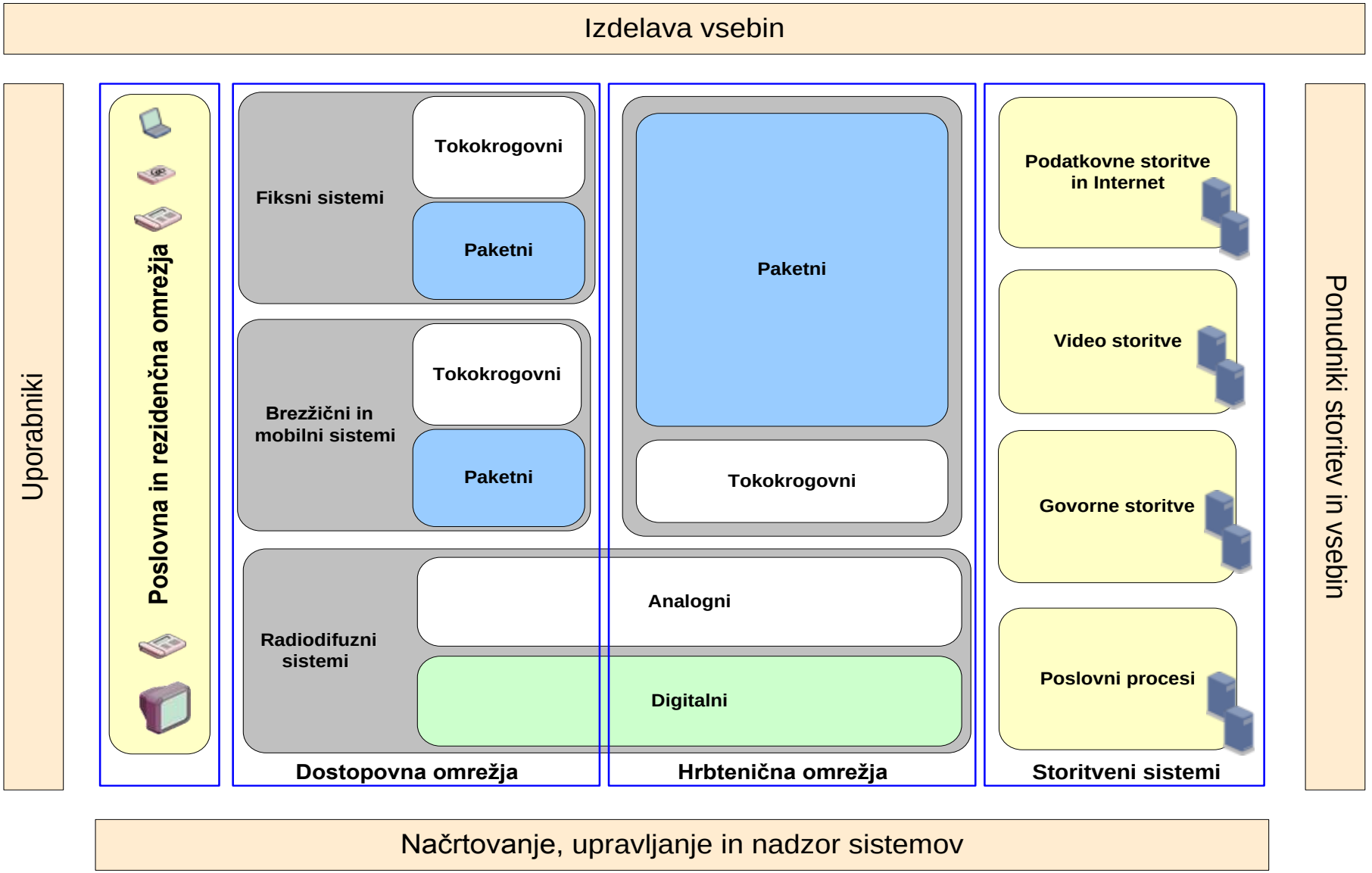
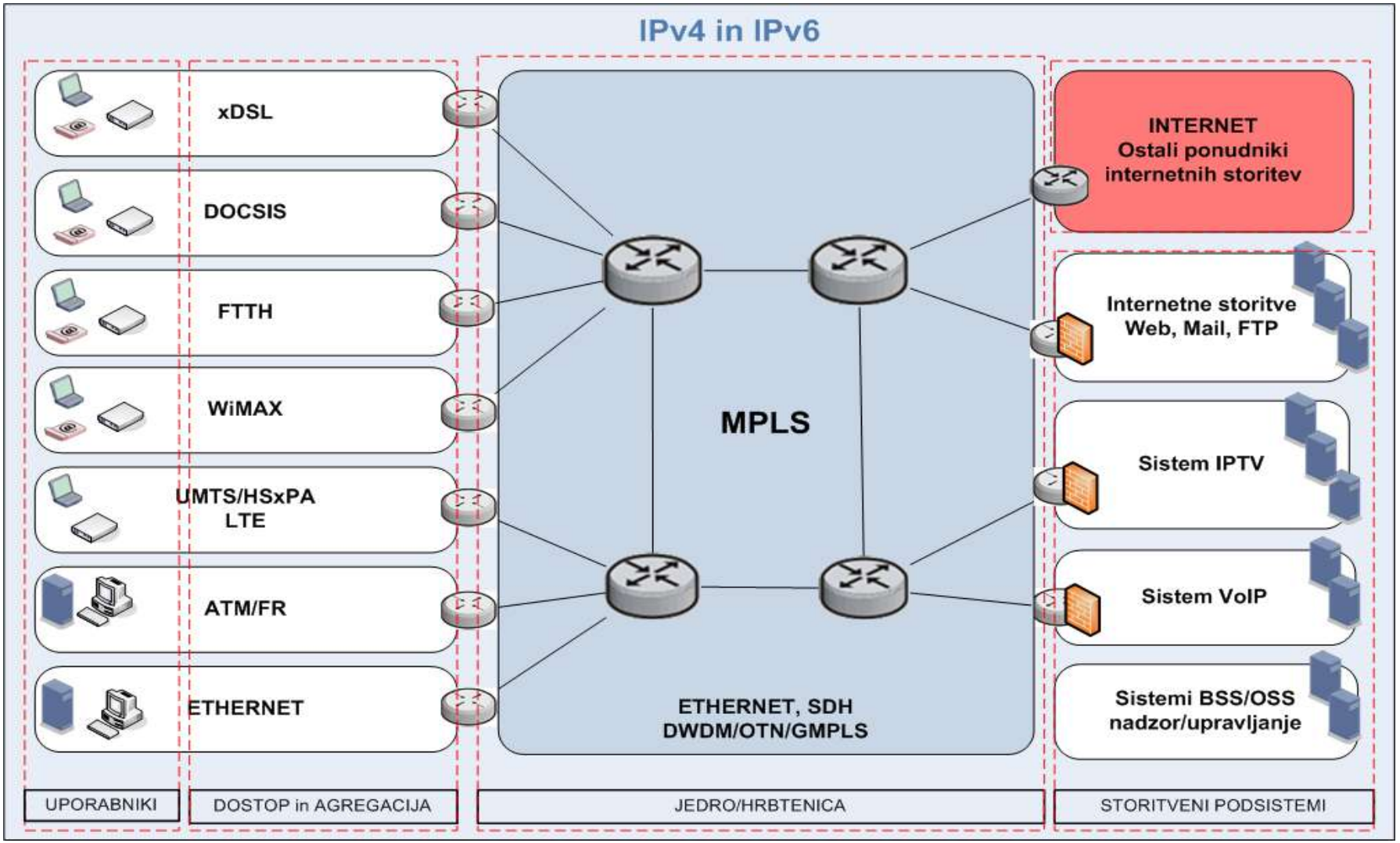
Ethernet

Sodobni komunikacijski sistemi



Operatersko omrežje – Internet

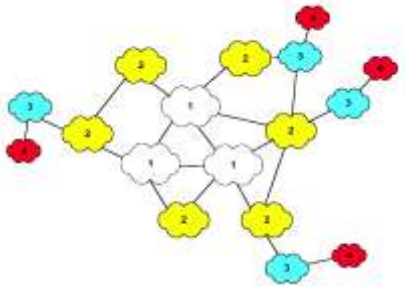


Internet

- **Zelo veliko število končnih odjemalcev**
  - osebni računalniki, delovne postaje, prenosniki, strežniki, dlančniki, pametni mobilni telefoni

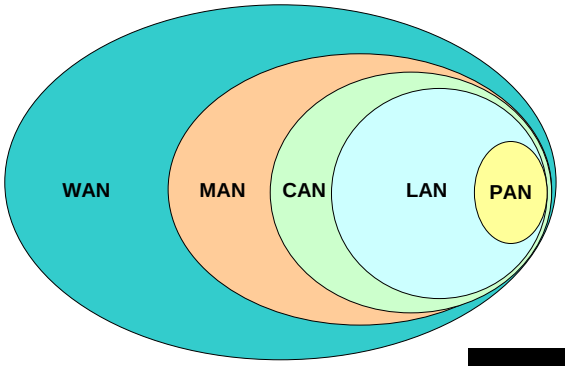
- **Različne komunikacijske povezave**
  - optika, baker, brezžični in mobilni, sateliti

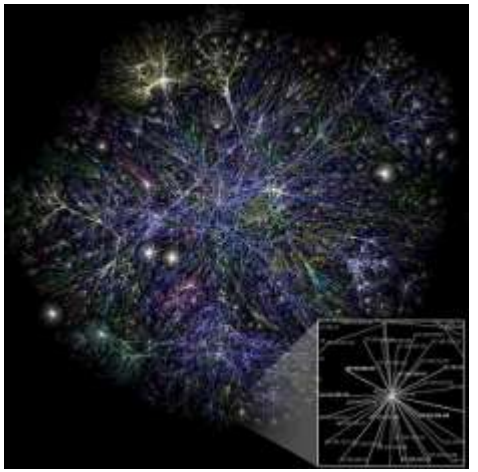
- **Usmerjevalniki**
  - usmerjajo in posredujejo pakete
- **Internet je "omrežje omrežij"**
  - omrežja, ki so med seboj povezana



Klasifikacija omrežij IP

- Glede na doseg pokrivanja
  - osebno omrežje
    - PAN – Personal Area Network
  - lokalno omrežje
    - LAN – Local Area Network
  - omrežje v kampusu
    - CAN – Campus Area Network
  - mestno omrežje
    - MAN – Metropolitan Area Network
  - prostrano omrežje
    - WAN – Wide Area Network



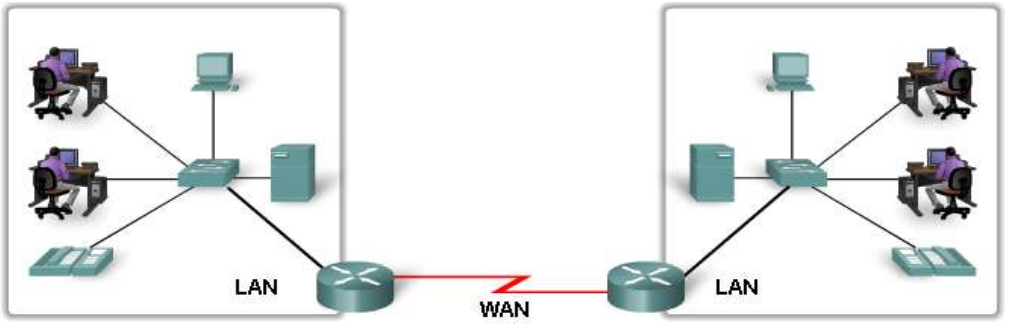


Vir: http://en.wikipedia.org/wiki/Internet

- Omrežji PAN in LAN – domača omrežja
- Omrežja PAN, LAN, CAN – omrežja v poslovnih okoljih
- Omrežji MAN in WAN – operaterska omrežja

Lokalna omrežja – LAN

- Osnovni elementi omrežja
  - terminalna oprema
    - osebni računalniki delovne postaje
  - strežniki, omrežni tiskalniki
  - omrežna oprema
    - stikala, usmerjevalniki, požarni zidovi, brezžične dostopovne točke



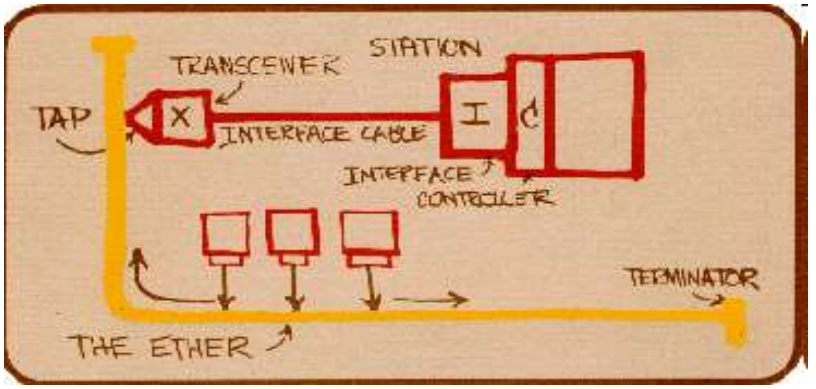
- Komunikacijske povezave med elementi omrežja
  - optične, bakrene, brezžične
  - "de-facto" standard predstavlja tehnologiji Ethernet

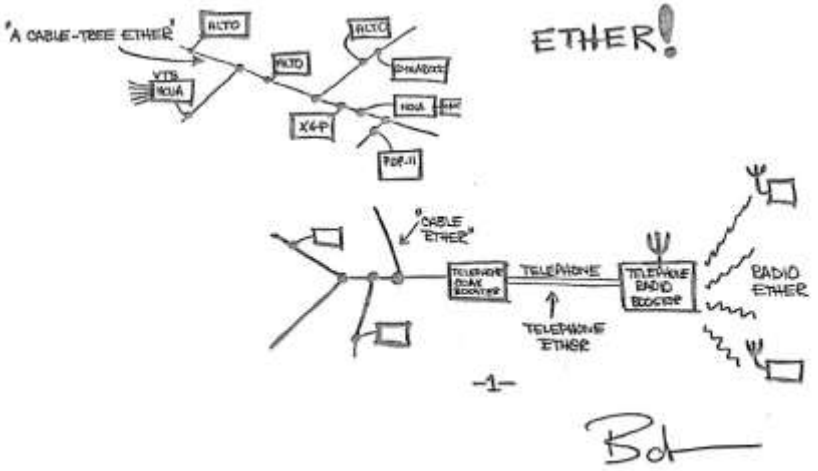
- Namen omrežja – zagotavljanje omrežnih storitev
  - prenos datotek – protokol FTP (angl. File Transfer Protocol)
  - prenos elektronske pošte – SMTP (angl. Simple Mail Transfer Protocol)
  - spletne storitve – HTTP (angl. HyperText Transfer Protocol)
  - upravljanje naprav – SNMP (angl. Simple Network Manage Protocol)

Tehnologija Ethernet

Začetki Ethernet

- Ethernet = Ether + Net
  - 1973!
- Xerox PARC
  - Robert Metcalfe
- Izhodišča pri razvoju
  - deluje po principu “plug and play”
  - poceni in preprosto povezovanje računalnikov v omrežjih LAN
  - skupen prenosni medij – koaksialni kabel
    - osnova za prenos – protokol CSMA/CD



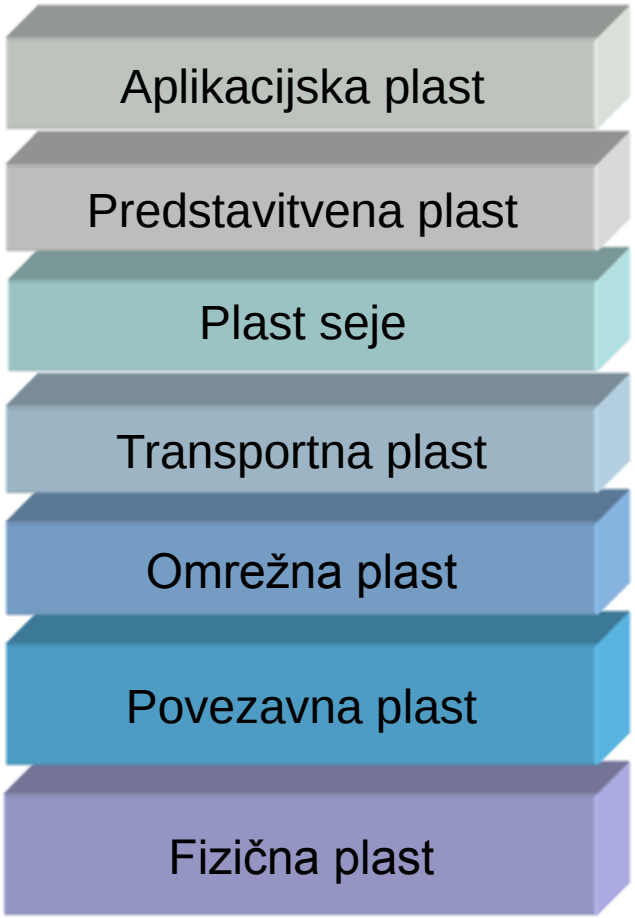


Razvoj Ethernet-a

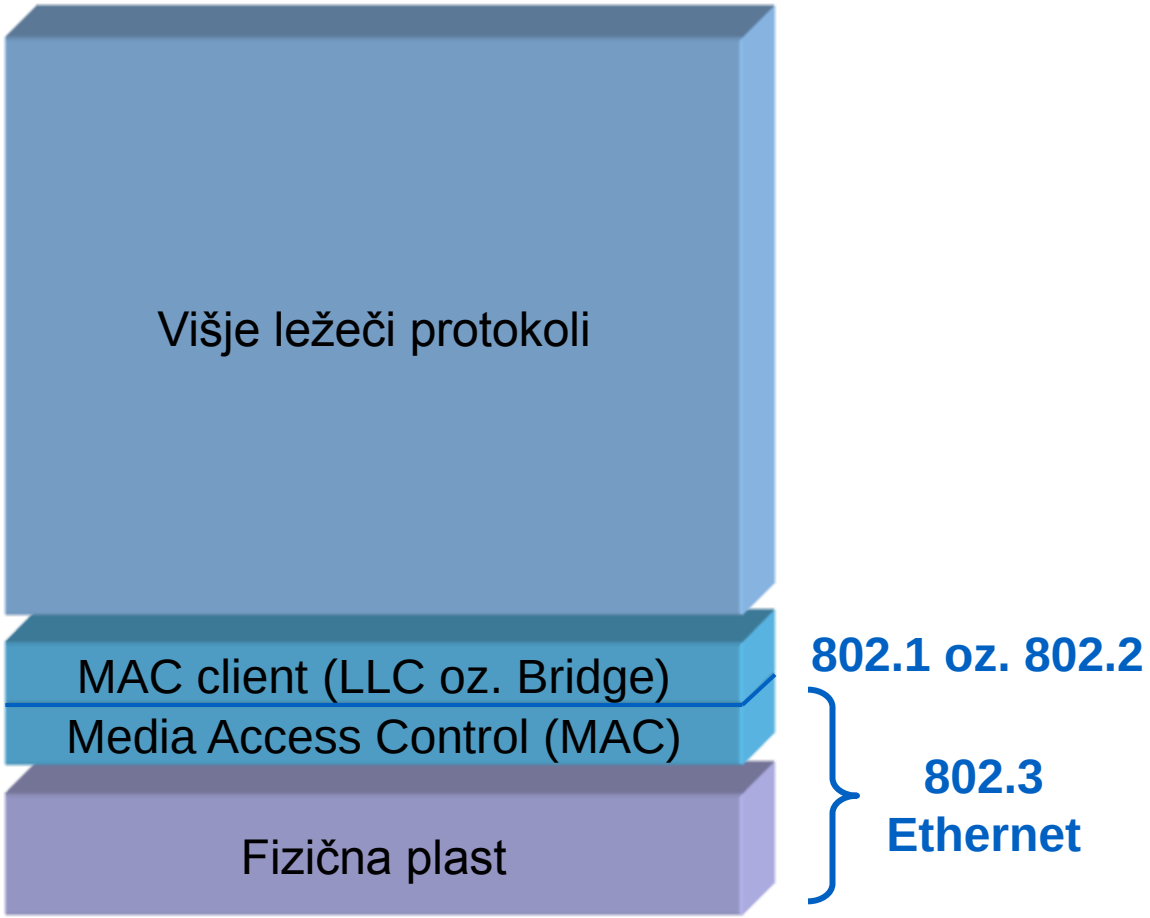
- 1970 – Aloha – University of Hawaii
- 1973 – Xerox – 3 Mbit/s Ethernet
- 1980 – standard DIX (Digital, Intel in Xerox) v1.0 – Ethernet
- 1982 – standard DIX v2.0 – Ethernet II
- 1983 – IEEE 802.3 – 10Base5 (thick)
- 1985 – IEEE 802.3a – 10Base2 (thin)
- 1990 – IEEE 802.3i – 10Base-T
- 1995 – IEEE 802.3u – 100base-T
  - 100base-TX, 100base-T4, 100base-FX (optika)
- 1997 – IEEE 802.3x – standard za full-duplex
- 1998 – IEEE 802.3z – 1000base-X (Gigabit Ethernet)
- 1998 – IEEE 802.3ac – VLAN
- 2003 – IEEE 802.3ae (optika)
- 2006 – 802.3an – 10G (UTP)

Ethernet in referenčni model OSI

Referenčni model OSI



Referenčni model Ethernet (IEEE 802.3)



Značilnosti tehnologije Ethernet

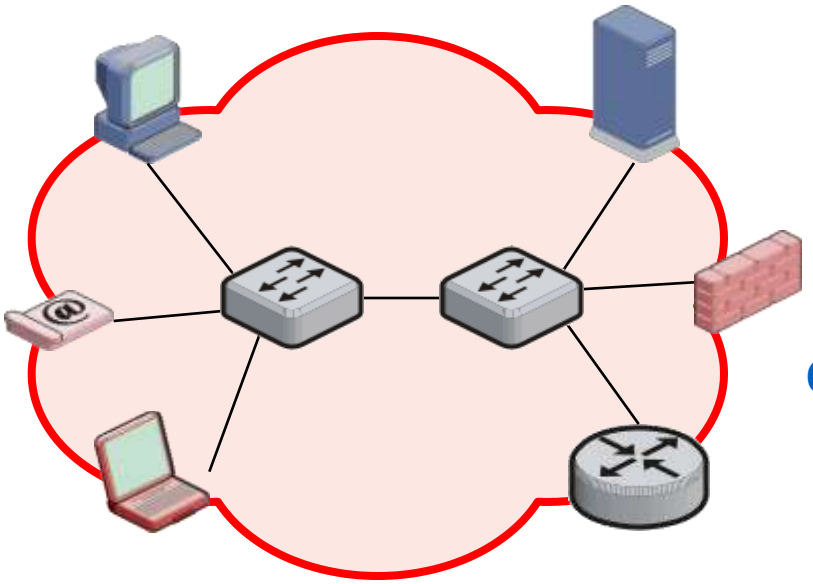
- Tehnologija v osnovi razvita za okolja LAN
  - deluje po princip ˝Plug and Play˝
  - nič ni potrebno nastaviti, vse se zgodi avtomatsko

- 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 z
      - 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
  - obnavljalnik/vozel Ethernet (angl. hub) – pasivno vozlišče

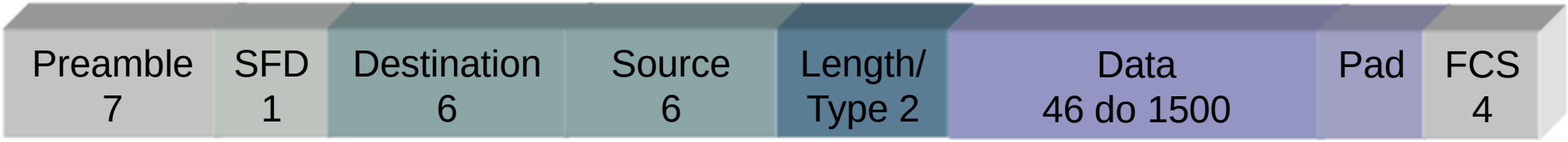


Omrežje Ethernet

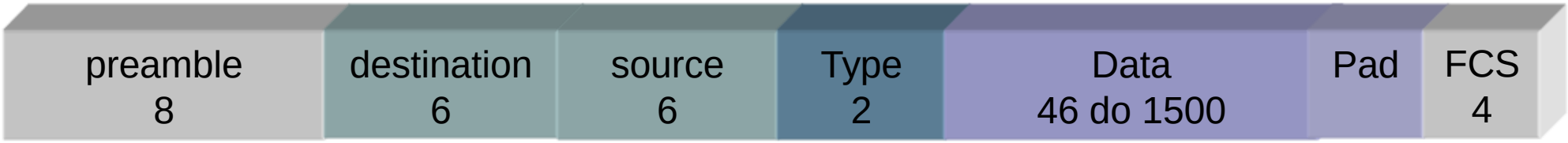
Struktura okvirja Ethernet

- **Preamble – niz potreben za sinhronizacijo (1010 ...)**
  - **združljivost za nazaj – 10 Mbit Ethernet (asinhron)**
  - **SFD (Start Frame Delimiter) – konec sinhronizacije (niz 10101011)**
- **Destination/source**
  - **ciljni/izvorni naslov MAC**
- **Length/Type**
  - **vrednost manjša od 600 HEX (=1536 dec) – polje Length**
  - **vrednost enaka ali večja od 600 HEX - polje Type**
  - **0800HEX = IPv4, 806HEX=ARP**
- **PAD – polnilni biti**
- **FCS – polje za zapis izračunane vrednosti CRC**

Okvir IEEE 802.3



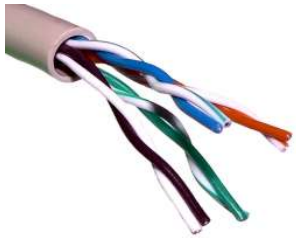
Okvir Ethernet II – DIX v2



Vmesniki Ethernet

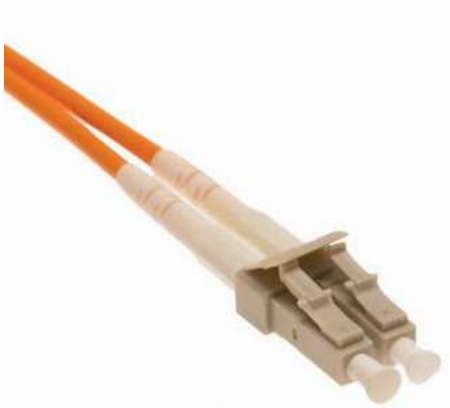
Ethernet vmesniki

- **Ethernet fizični vmesniki – trenutne hitrosti vmesnikov**
  - 10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s, (40 Gbit/s, 100 Gbit/s)
- **Mehanizem za avtomatsko prilagajanje hitrosti in način delovanja**
  - half duplex, full duplex
  - npr. vmesnik 1000BASE-T lahko deluje z različnimi hitrostmi: 1000 Mbit/s, 100 Mbit/s, 10 Mbit/s
    - odvisno od hitrosti vmesnika na napravi (stikalo) na katero je priključen
- **Prenos v osnovnem pasu (base band)**
  - omogoča neposreden prenos prek različnih medijev
    - bakreni vodniki (npr. vodnik UTP, konektor RJ45)
    - optični vodniki (npr. večrodovno vlakno MM, konektor LC)



Kabel UTP

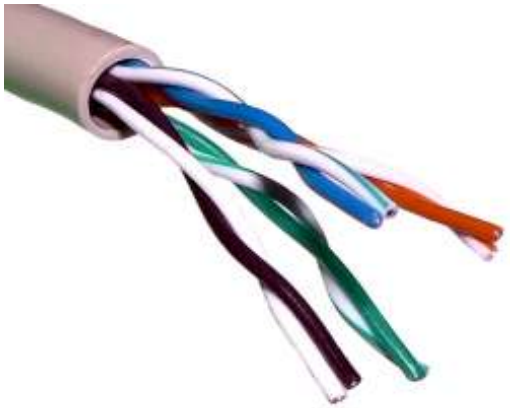
Konektor RJ45



Večrodovno optično vlakno s konektorjem LC

Ethernet – ožičenje UTP

- Kabel UTP – 8 žilni kabel (4 pari)
  - oranžna, oranžno-bela
  - zelena, zeleno-bela
  - modro, modro-bela
  - rjava, rjavo-bela



- Konektor RJ45
  - moški del
  - ženski del

- Klasičen kabel UTP “straight through
  - povezovanje sponk konektorjev

Ethernet omrežne naprave

Ethernet omrežne naprave

- **Obnavljalnik (angl. regenerator)**
  - dvo portna naprava, ki zgolj slepo prenaša okvirje iz enega omrežja v drugo omrežje (deluje na sloju L1)
- **Vozel (angl. hub)**
  - obnavljalnik z več vrati (porti)
- **Premoščevalnik (angl. bridge)**
  - naprava, ki prenaša okvirje iz enega omrežja v drugo omrežje glede na naslov MAC (deluje na sloju L2)
  - gradi si tabelo, v katero si zapisuje, s kakšnimi naslovi prihajajo okvirji prek določenih vrat. Okvir pošlje samo na tista vrata, katerih naslov ustreza ciljnemu naslovu zapisanem v glavi okvirja Ethernet.
- **Stikalo (angl. switch)**
  - premoščevalnik z več vrati (porti)
- **Usmerjevalnik (angl. router)**
  - naprava, ki prenaša pakete IP iz enega omrežja v drugo omrežje glede na naslov omrežnega nivo (deluje na sloju L3)

Omrežne naprave – umestitev v OSI

L5 - L7

L4

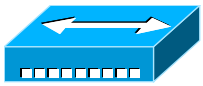
usmerjevalnik

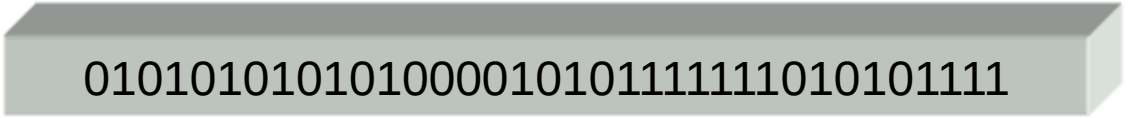
L3

premoščevalnik, stikalo

L2

obnavljalnik, vozel (hub)

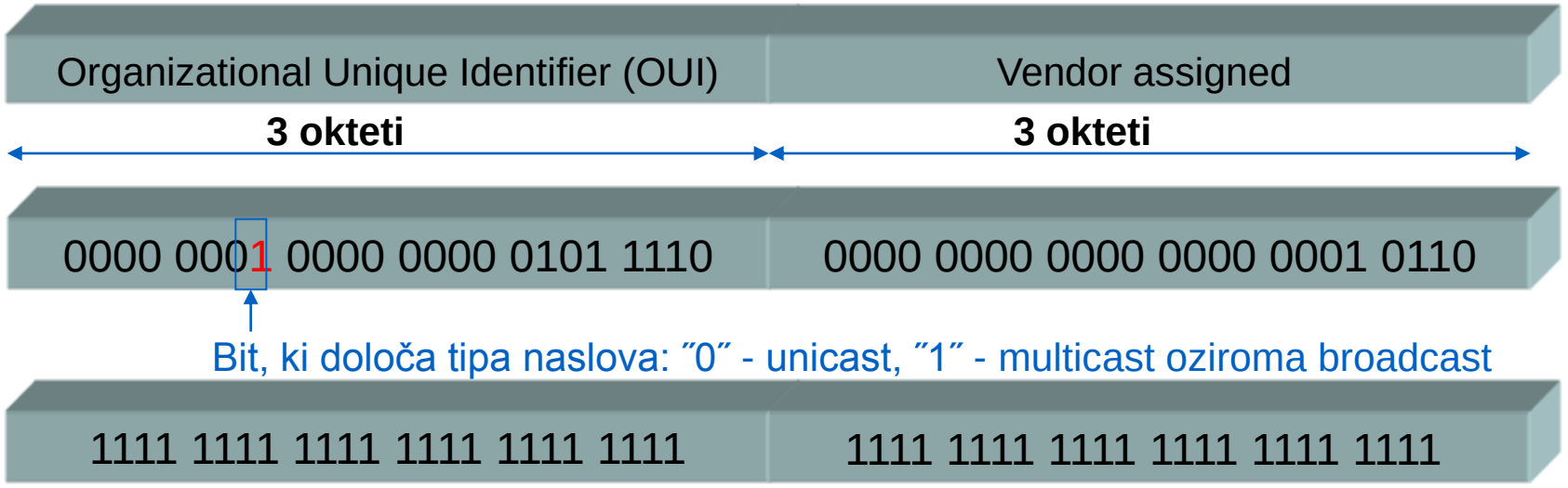




L1

Ethernet naslavljanje

- 48 bitni naslov MAC zapisan v formatu HEX
  - sestavljen iz dveh delov: OUI in vendor assigned
  - primeri naslovov OUI
    - Cisco (00-60-2F-xx-xx-xx)
    - IANA multicast (01-00-5E-xx-xx-xx)
- Tipi naslovov MAC
  - unicast, multicast, broadcast (FF-FF-FF-FF-FF-FF)



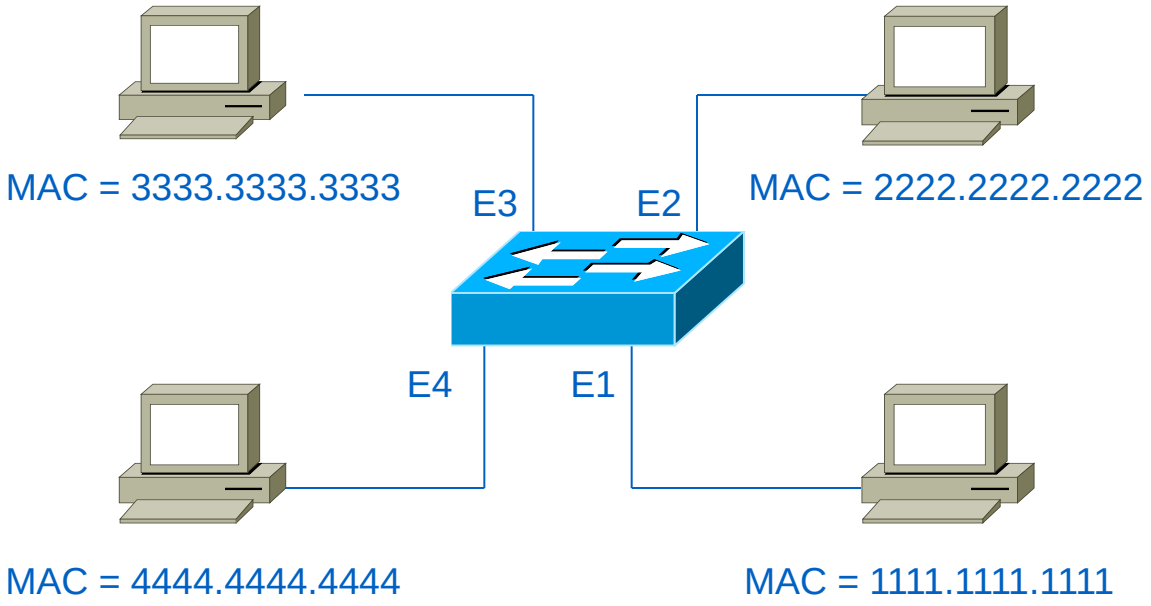
Ethernet stikalo

- Standard ANSI/IEEE 802.1D
  - transparent bridge
  - spanning tree
- Vzdržuje tabelo (tabela MAC, CAM, Filtering Database), v kateri so vnosi, ki zagotavljajo mapiranje med naslovi MAC in posameznimi fizičnimi vmesniki
  - statični vnosi
  - dinamični vnosi – posamezen vnos se odstrani po izteku časovnika (Ageing Time = 300 s)
- Princip delovanja
  - okvir (unicast) se posreduje samo na tista izhodna vrata, katerih naslov MAC ustreza ciljnemu naslovu zapisanem v glavi okvirja
  - če v tabeli MAC ni vnosa za posamezen ciljni naslov MAC se okvir (unicast) posreduje na vse izhodne vmesnike
  - okvirji, ki vsebujejo multicast in broadcast naslov se posredujejo na vse oktivne izhodne vmesnike

Princip delovanja stikala Ethernet

Tabela MAC

Ciljni naslov MAC	Izhodni vmesnik
1111.1111.1111	E1
2222.2222.2222	E2
3333.3333.3333	E3
4444.4444.4444	E4



Ethernet – omrežne storitve

Značilnosti

- Tehnologija v osnovi razvita za LAN okolja
- Nepovezavno usmerjena tehnologija
- Deluje po princip “plug and play”
  - nič ni potrebno nastaviti, vse se zgodi avtomatsko ☺
- Podatkovna in kontrolna ravnina združeni
  - Ethernet stikalo zgradi tabelo MAC na osnovi posredovalne funkcije
- Ethernet okvir je za vse verzije enak
  - razlika med IEEE 802.3 in Ethernet II je majhna
  - omrežne kartice (NIC) tipično oddajajo in sprejemajo oba tipa okvirjev
- Dokler ostane sporočilo na Ethernet omrežju se okvir ne spreminja
  - omogoča veliko razširljivost
- Velike hitrosti delovanja
  - 10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s, 40Gbit/s, (100Gbit/s)
- Raznolikost prenosnih medijev
- Standardizacija v IEEE
  - standardi 802.3 – Ethernet vmesniki 10/100/1000/10000 Mbit/s
  - standardi 802.1 – Ethernet komutacija, zaščitni mehanizmi, OAM

Standardizacija Ethernet – IEEE

- 802.1D – (MAC) Ethernet bridge
  - zaščita pred zankami (STP) konvergenca ~30 s do 50 s
- 802.1w – Rapid Spanning Tree Protocol (RSPT)
  - hitra zaščita pred zankami
  - kovergenca ~1 s
- 802.1s – Multiple Spanning Trees (MSTP)
  - preprečevanje zank znotraj omrežij VLAN
- 802.1Q/802.1p – Virtual LAN, QoS
  - logična segmentacija omrežja
  - prioritizacija prometa
- 802.1X – Port Based Network Access Control
  - nadzor dostopa na nivoju fizičnega vmesnika
- 802.3ad – Link Aggregation
  - združevanje vmesnikov v logične vmesnike konvergenca ~ 500 ms
- 802.3af – DTE Power via MDI
  - napajanje terminalne opreme prek vmesnikov Ethernet
- 802.3 – standardi za fizične vmesnike
  - standardizirani so vmesniki hitrosti 10/100/1000/10000 Mbit/s
- 802.11 – standardi za brezžične vmesnike (WiFi)
  - vmesniki s hitrostmi 11 – 54 Mbit/s
- 802.16 – standardi za brezžične/mobilne vmesnike (WiMAX)
  - vmesniki s hitrostmi do ~70 Mbit/s

Ethernet okvir

- Preamble – niz potreben za sinhronizacijo (1010 ...)
  - združljivost za nazaj – 10 Mbit Ethernet (asinhron)
  - SFD (Start Frame Delimiter) – konec sinhronizacije (niz 10101011)
- Destination/source
  - ciljni/izvorni naslov MAC
- Length/Type
  - vrednost manjša od 600 HEX (=1536 dec) – polje Length
  - vrednost enaka ali večja od 600 HEX – polje Type
  - 0800HEX = IPv4, 806HEX=ARP
- PAD – polnilni biti
- FCS – polje za zapis izračunane vrednosti CRC

Okvir IEEE 802.3

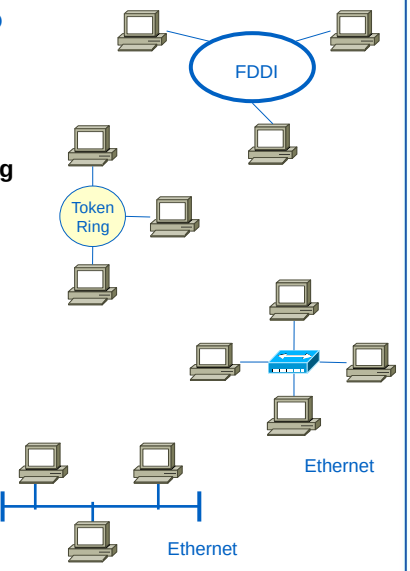
Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data 46 do 1500	Pad	FCS 4

Okvir Ethernet II – DIX v2

Preamble 8	Destination 6	Source 6	Type 2	Data 46 do 1500	Pad	FCS 4

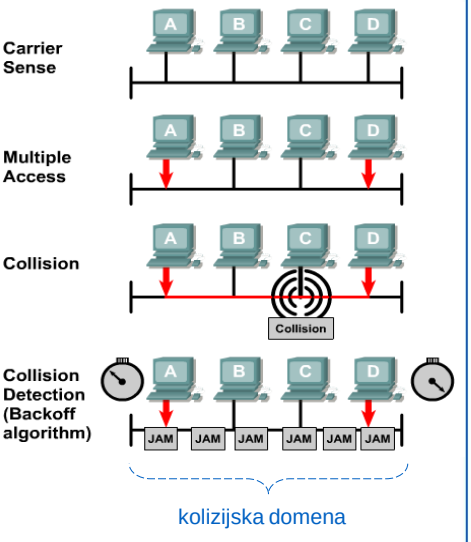
Media Access Control (MAC)

- Pod sloj, ki določa način sodostopa do skupinskega medija
  - kolizijske domene ˝collision domain˝
- MAC – tipi
  - deterministični – ne prihaja do kolozij (taking turns)
    - FDDI
      - fizično – topologija dvojnega obroča
      - logično – topologija obroča
    - Token Ring
      - fizično – topologija zvezde
      - logično – topologija obroča
  - nedeterministični – lahko prihaja do kolozij (first come, first served)
    - CSMA/CD – Carrier Sense Multiple Access/Collision Detection
      - fizično – topologija zvezde ali vodila
      - logični – topologija vodila



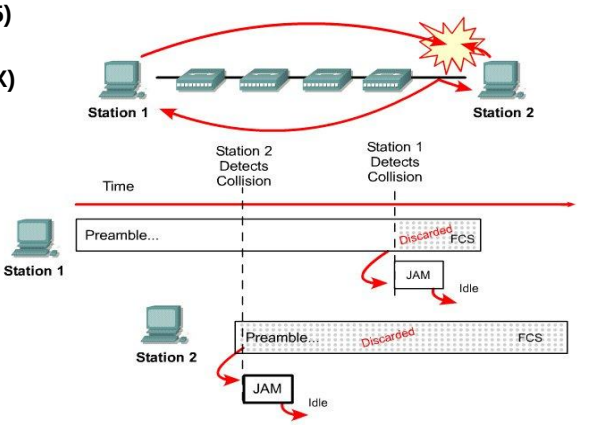
Delovanje CSMA/CD

- Carrier Sense
  - pred oddajo paketa preveri če je medij prost
- Multiple Access
  - sočasno lahko prične oddajati več naprav
- Collision Detection
  - ko začne oddajati hkrati tudi posluša če je prišlo do trka (če zazna trk ustavi oddajanje in sproži časovno kontrolo)
- Naloga protokola CSMA/CD
  - oddaja in sprejem paketov
  - dekodiranje sprejetih paketov, detekcija napak, preverjanje naslovov
  - detekcija kolozij pri prenosu



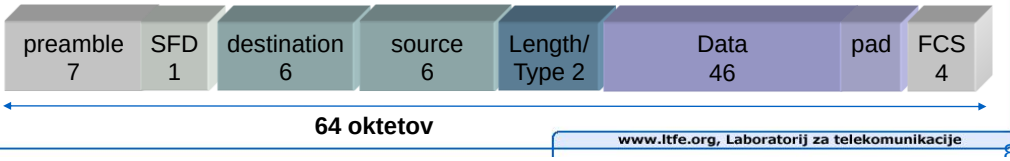
Kolizije

- Delno oddano sporočilo (okvir), pri katerem je prišlo do kolizije, imenujemo ˝collision fragment˝ oz. ˝runt˝
- Zaznavanje kolozij
  - COAX (10BASE2, 10BASE5)
    - dvig napetosti na mediju
  - UTP (10base-T, 100base-TX)
    - NIC sprejeme signal na RX-paru sočasno ko oddaja na TX-paru



Tipi kolizij

- Večina kolizij se zgodi pred pričetkom oddaje polja SFD
- Tipi kolizij
  - lokalna (local)
    - okvir je manjši od 64 oktetov
    - dvig napetosti na mediju oz. sočasen sprejem na paru TX in RX
  - oddaljena (remote)
    - okvir je manjši od 64 oktetov
    - FCS je napačen
    - v kolizijski domeni se nahaja regenerator (repeater)
  - pozna (late)
    - okvir je večji od 64 oktetov
    - kolizije, ki se zgodijo zaradi napačnega delovanja NIC (ilegalna kolizija)
    - za ponovno oddajo sporočila morajo poskrbeti višje ležeči protokoli



Viri napak

- Kolizije
  - lokalne, oddaljene in pozne
- Jabber, long frame, range error
  - oddajni čas signala je daljši od dovoljenega
- Kratek okvir, ˝collision frame or runt˝
  - oddajni čas signala je krajši od dovoljenega (FCS je pravilen)
- Napake FCS/ Alignment error
  - napaka pri prenosu okvirja
- Range error
  - število sprejetih bit-ov in polje ˝length˝ se ne ujemata
- Gost ali jabber
  - predolga sekvenca ˝preambule˝

Časovni parametri

- Bit time
  - čas enega bita
- Slot time
  - čas, ki je potreben za prenos signala med dvema najbolj oddaljenima postajama v kolizijski domeni (v obe smeri)
  - oddajna postaja mora ugotoviti, da je prišlo do kolizje še preden konča z oddajo najmanjšega možnega okvirja
  - čas prenosa okvirja ne sme biti manjši od ˝slot time˝ (zato je padding)
  - ˝slot time˝ je pomemben le pri ˝half-duplex˝ prenosu
- Interframe spacing
  - ˝prazen˝ čas med dvema oddanima okvirjema

HITROST	BIT TIME
10 Mbit/s	100 ns
100 Mbit/s	10 ns
1 Gbit/s	1 ns
10 Gbit/s	0,1 ns

HITROST	SLOT TIME	ČASOVNI INTERVAL
10 Mbit/s	512 *bit time	51,2µs
100 Mbit/s	512 *bit time	5,12µs
1 Gbit/s	4096 *bit time	4,096µs
10 Gbit/s	-	-

HITROST	INTERFRAME SPACING	ČASOVNI INTERVAL
10 Mbit/s	96 *bit time	9,6µs
100 Mbit/s	96 *bit time	0,96µs
1 Gbit/s	96 *bit time	0,096µs
10 Gbit/s	96 *bit time	0,0096 µs

Ethernet stikalo

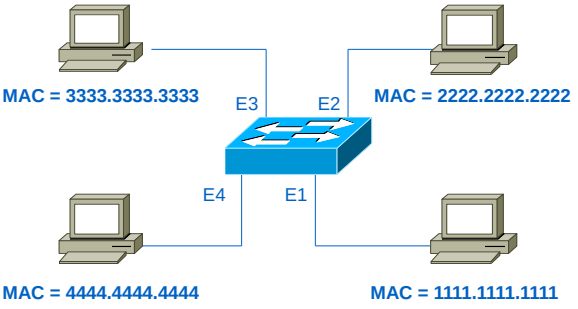
Ethernet stikalo

- Standard ANSI/IEEE 802.1D
  - Transparent Bridge
  - Spanning Tree
- Vzdržuje tabelo (tabela MAC, CAM, Filtering Database), v kateri so vnosi, ki zagotavljajo mapiranje med naslovi MAC in posameznimi fizičnimi vmesniki
  - statični vnosi
  - dinamični vnosi – posamezen vnos se odstrani po izteku časovnika (Ageing Time = 300 s)
- Princip delovanja
  - okvir (unicast) se posreduje samo na tista izhodna vrata, katerih naslov MAC ustreza ciljnemu naslovu zapisanem v glavi okvirja
  - če v tabeli MAC ni vnosa za posamezen ciljni naslov MAC, se okvir (unicast) posreduje na vse izhodne vmesnike
  - okvirji, ki vsebujejo multicast in broadcast naslov, se posredujejo na vse izhodne vmesnike
    - izjema je vmesnik, prek katerega je bil okvir sprejet

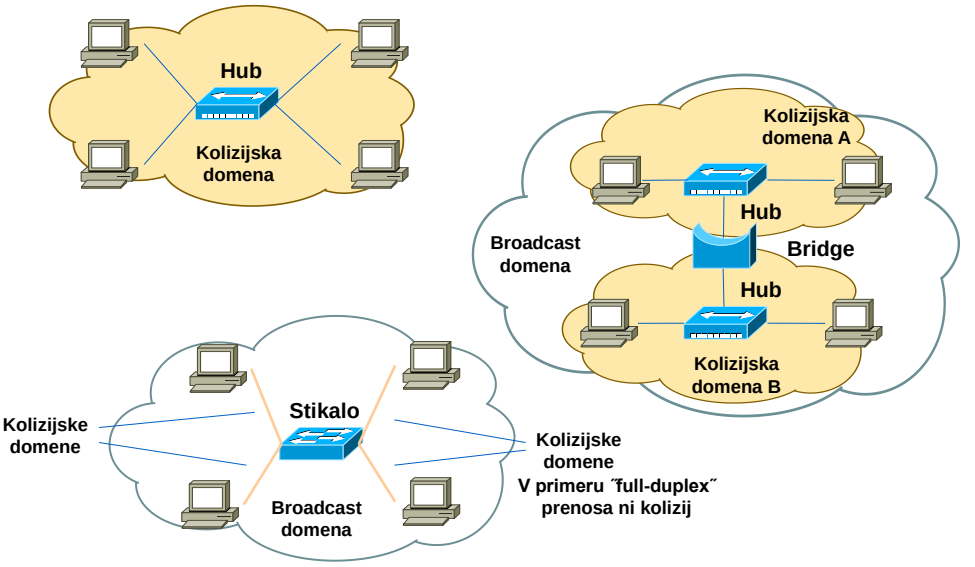
Princip delovanja stikala Ethernet

Tabela MAC

Ciljni naslov MAC	Izhodni vmesnik
1111.1111.1111	E1
2222.2222.2222	E2
3333.3333.3333	E3
4444.4444.4444	E4

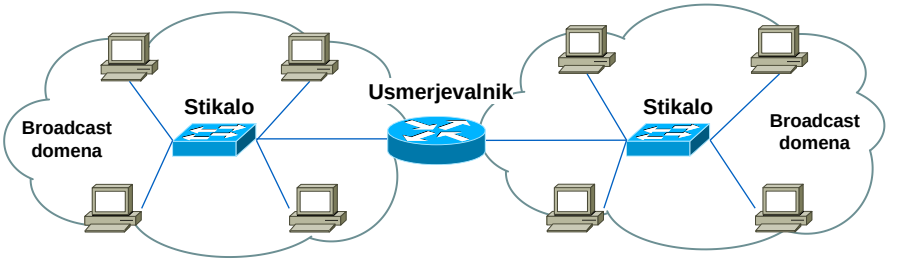


Omrežne naprave – L1 in L2



Omrežne naprave L1 in L2 in L3

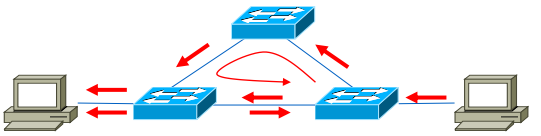
- Naprave L1 podaljšujejo/povečujejo kolizijske domene
- Kolizijske domene lahko omejimo z
  - premoščevalnikom (bridge)
  - stikalom (switch)
  - usmerjevalnikom (router)
- ˝Broadcast˝ domene lahko omejimo z
  - usmerjevalnikom
  - VLAN



Spanning Tree Protocol – STP

Spanning Tree Protocol – STP

- Standard IEEE 802.1D
- Namen
  - mehanizem za preprečevanje zank v Ethernet omrežjih
    - ˝broadcast storm˝
  - mehanizem za zagotavljanje redundance v Ethernet omrežjih
- Omogoča izmenjavo informacij med Ethernet stikali
  - sporočila BPDU (Bridge Protocol Data Unit)
- Algoritem STP določa kateri vmesniki lahko posredujejo Ethernet okvirje
  - zgradi optimalno drevo omrežja (Spanning Tree)
  - vsak fizičen vmesnik se postavi v enega izmed dveh končnih stanj
    - posreduj
    - blokiraj



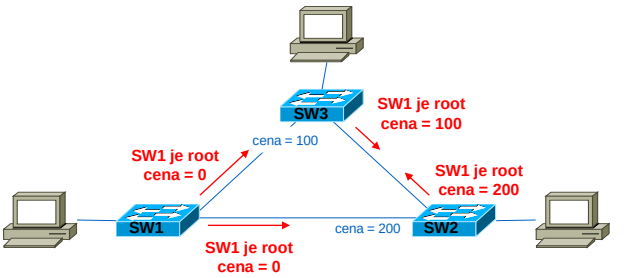
broadcast storm

Princip delovanja STP

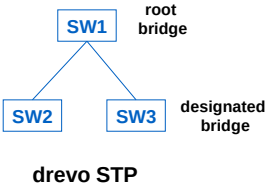
- Eno izmed stikal je izbrano za ˝root˝ bridge
  - stikalo z najmanjšim BID (Bridge ID)
  - vsi njegovi vmesniki se postavijo v stanje posreduj
- ˝Root˝ bridge oglašuje sporočila ˝hello˝ BPDU
- Ostala stikala le sprejmejo ˝hello˝ BPDU
  - neposredno od ˝root˝ bridge
  - posredno od ostalih stikal (stikala posredujejo ˝hello˝ BPDU naprej)
  - stikalo lahko sprejme ˝hello˝ BPDU na večih vmesnikih
    - vmesnik prek katerega je bil sprejet ˝hello˝ BPDU z najmanjšo ceno poti se postavi v stanje posreduj in se označi kot ˝root port˝
- Za vse preostale segmente LAN se izbere ˝designated bridge˝ katerega vmesik se postavi v stanje posreduj
  - vmesnik, ki oglašuje ˝hello˝ BPDU z najnižjo ceno - ˝designated port˝
- Vsi preostali vmesniki se postavijo v stanje blokiraj
- Če stikalo ne sprejema več ˝hello˝ BPDU ponovno steče proces izračuna optimalnega drevesa STP

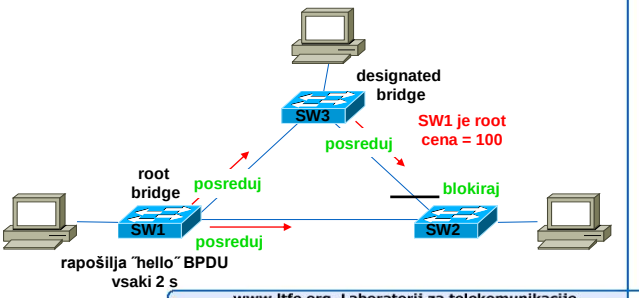
Proces gradnje drevesa STP

- Gradnja drevesa STP



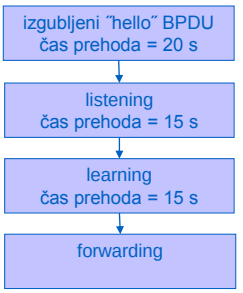
- Stanje konvergence





Stanje konvergence

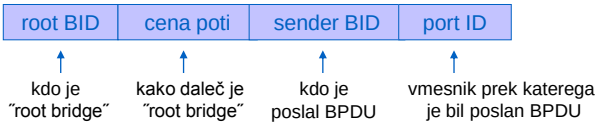
- ″Root″ bridge periodično razpošilja sporočila ″hello″ BPDU
  - privzeta nastavitev je vsaki 2 sekundi (Hello Time)
- Ostala stikala posredujejo sprejeta sporočila naprej
  - v sporočilu ″hello″ BPDU popravijo ceno za posamezno povezavo
- Če stikalo ne sprejme ″hello″ BPDU v ustreznem času (MaxAge), prične s postopkom ponovnega izračuna drevesa STP



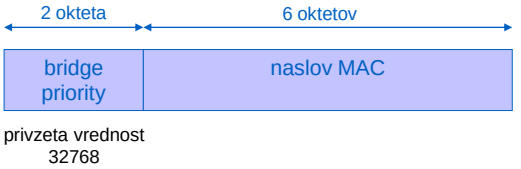
Stanje vmesnika	Posreduje okvirje	učenje naslovov	stanje	čas prehoda
blocking	ne	ne	stabilno	20 s (MaxAge)
listening	ne	ne	prehodno	15 s
learning	ne	da	prehodno	15 s
forwarding	da	da	stabilno	

Sporočilo BPDU

- **Polja v sporočilu ˝hello˝ BPDU**



- **Identifikator stikala (Bridge ID – BID)**



VLAN

Navidezna lokalna omrežja – VLAN

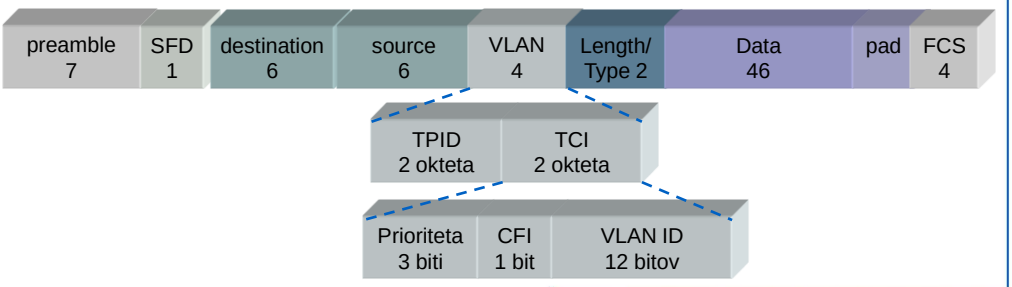
- Standard IEEE 802.1Q
- VLAN je komutirano omrežje, ki omogoča logično segmentacijo uporabnikov (terminalov), ne glede na njihovo fizično lokacijo
  - logična topologija omrežja je tako neodvisna od fizične topologije
  - omejuje nam “broadcast” domene
  - omejuje nam “multicast” domene
- Večina implemetacij 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, kjer je mogoče določiti ustrezno politiko
- Stikala VLAN tipično lahko delujejo na sloju L2 in L3
  - komutacija na osnovi naslovov MAC (L2 switching)
  - komutacija na osnovi naslovov IP (L3 switching)

Koncept delovanja VLAN

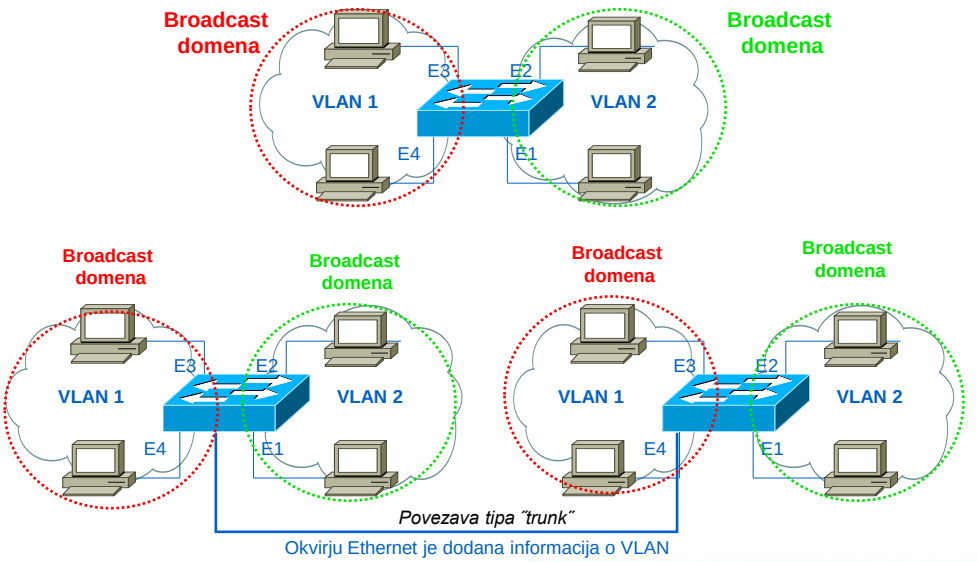
- Način dodeljevanja vmesnikov v VLAN
  - statično
    - administrator ročno določi kateremu omrežju VLAN bo pripadal posamezen fizičen vmesnik
    - privzeta vrednost VLAN ID = 1
  - dinamično
    - potreben je dodaten protokol (GVRP – GARP VLAN Registration Protocol)
      - GARP – Generic Attribute Registration Protocol (IEEE Std 802.1D)
- Načini delovanja fizičnih vmesnikov
  - vmesnik pripada enemu omrežju VLAN
  - vmesnik pripada večim omrežjem VLAN
  - vmesnik deluje v načinu "trunk" (IEEE 802.1Q, ATM, ISL)
    - klasičnemu okvirju Ethernet se doda informacija o pripadnosti VLAN
    - za povezovanje stikala z ostalimi stikali VLAN
    - za povezavo stikala z usmerjevalnikom

Format okvirja 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)



Primer omrežja VLAN



Okvirju Ethernet je dodana informacija o VLAN

Omejitve Etherneta

Omejitve Ethernet-a v MAN/WAN

- Omejen mehanizem za zagotavljanje kakovosti storitev
  - ne omogoča komunikacije z zagotovljeno QoS
- "Počasna" konvergenca zaščitnih mehanizmov
  - ~30 sekund s protokolom STP
  - ~1 sekunda s protokolom RSTP
- Ni definiranega vmesnika za OAM (Operations Administration and Maintenance)
- Ne omogoča logične delitve fizičnega prenosnega kanala
- Omejeno število omrežij VLAN
  - max VLAN ID = 4094 (x2 v standardizaciji)
- Varnostni vidiki
  - MAC snooping
  - poplavljanje z MAC
  - poplavljanje z ARP
  - napadi na protokol STP

Prihodnost Etherneta

Prihodnost Etherneta

- Tehnologija za omrežja LAN, MAN in WAN
- Na voljo so vmesniki za 40 GBbit/s Ethernet
- Razvoj standardov za 100 Gbit/s
- Metro oziroma carrier Ethernet
- Prenosni mediji
  - baker
    - hitrosti do 10000 Mbit/s
  - optična vlakna
    - trenutno smo še daleč od teoretične meje (prenosne hitrosti omejujejo oddajniki/sprejemniki)
    - tehnologije WDW, DWDM

Cenovna učinkovitost tehnologije

	Equipment price per Mbit/s	BW mgmt & provisioning	Annual maint. upgrades	BW on demand
IP/ATM/SONET	$ 8 - 40	$ 5,000	$ 750 - 3,750	Hard
IP/SONET	$ 6 - 35	$ 5,000	$ 750 - 3,750	Hard
IP/Ethernet	$ 1 - 3	$ 1,000	$ 150 - 450	Easy
Gbit Ethernet advantage	8:1 - 13:1	5:1	5:1 - 8:1	Easy

Source: Yipes, Dell 'Oro, Yankee Group, Extreme Networks, Juniper Networks
Assumes a regional network with five hubs and 10 rings, Costs in US$

Telekomunikacije in informacijske tehnologije
Laboratorij za telekomunikacije
Fakulteta za elektrotehniko

IPv6

Univerza v Ljubljani

Fakulteta za elektrotehniko

Laboratorij za telekomunikacije

Ljubljana, april 2011

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Omrežne storitve 1/2

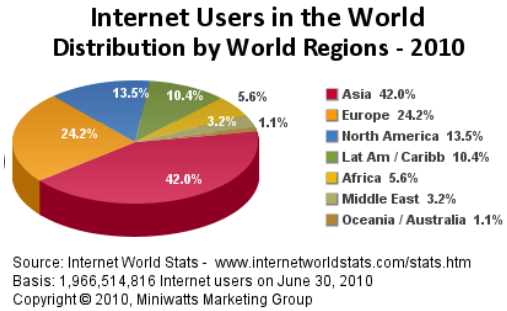
	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Podatkovna raven	Globalno naslavljanje	Unicast naslavljanje		-	✓	✓	-
		Multicast naslavljanje		-	✓	✓	-
		Anycast naslavljanje		-	✓	✓	-
	Lokalno naslavljanje	Unicast naslavljanje		✓	✓	✓	✓
		Multicast naslavljanje		✓	✓	✓	✓
		Anycast naslavljanje		-	✓	✓	-
		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

Penetracija interneta

- Trenutna penetracija interneta v svetovnem merilu je 28.7 %
- Gonilo razvoja IPv6
  - mobilni internet:
    - mobilni telefoni ~ 5 milijard
    - ″ad-hoc″ mobilna omrežja ~ 1 milijarda avtomobilov
  - ″always-on″ (xDSL, Cable, EFM, Wireless)
  - VoIP, Skype, IPTV, ″peer-to-peer″
  - UMTS/HSxPA, FMC, IMS



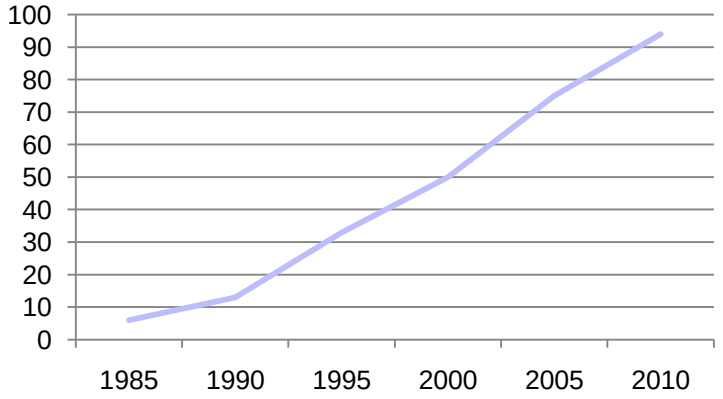
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 1,966,514,816 Internet users on June 30, 2010
Copyright © 2010, Miniwatts Marketing Group

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

Vir: www.internetworldstats.com (junij 2010)

Razlogi za prehod iz IPv4 v IPv6

- **Naslov IPv4 je 32 biten = 4 milijarde naslovov (teoretično)**
  - praktična omejitev ~ 250 milijonov naslovov (RFC 3194)
- **Izraba /8 naslovnega prostora organizacije IANA**
  - 1981 izdan standard IPv4
  - 1985 ~ 6 % naslovnega prostora
  - 1990 ~ 13 % naslovnega prostora
  - 1995 ~ 33 % naslovnega prostora
  - 2000 ~ 50 % naslovnega prostora
  - 2005 ~ 75 % naslovnega prostora
  - 2010 ~ 94 % naslovnega prostora
  - 2011 ~ 100% naslovnega prostora



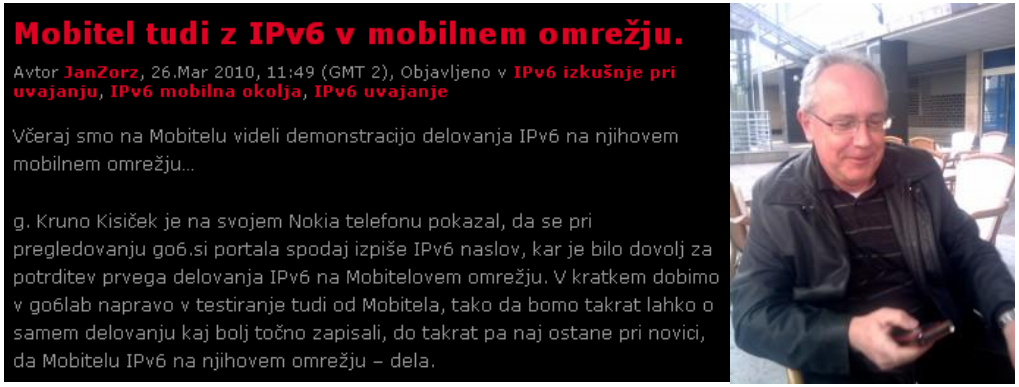
- **Mehanizmi za podaljševanje IPv4**
  - 1993 – CIDR (Classless InterDomain Routing)
  - 1993 – VLSM (Variable Length Subnet Mask)
  - 1993 – DHCP (Dynamic Host Configuration Protocol)
  - 1994 – NAT (Network Address translation)
  - 1996 – zasebni naslovni prostor (RFC 1918)

Pripravljenost infrastrukture na IPv6

- OECD (7. april 2010)
  - www.oecd.org/STI/ICT/IPv6
- Omrežja
  - 5 % omrežij v internetu
- Končne naprave
  - 90 % obstoječih naprav podpira IPv6
  - 25 % naprav podpira IPv6 pod privzetimi nastavitvami (Windows, Mac)
- Podpora IPv6 pri ponudnikih vsebin
  - 1,45 % od 1000 najbolj obiskanih strani
  - 0,15 % od 1000000 najbolj obiskanih strani

Stanje IPv6 v Sloveniji

- **ISP**
  - **Arnes – Geant/Dante**
  - **Volja**
  - **Amis**
  - **Telekom Slovenije**
  - **Mobitel**
  - **T-2**
  - **Tušmobil**



- **Nekatere raziskovalne ustanove**
  - **Metulj – 10 G hrbtenica UNI LJ**
  - **FRI, FE …**

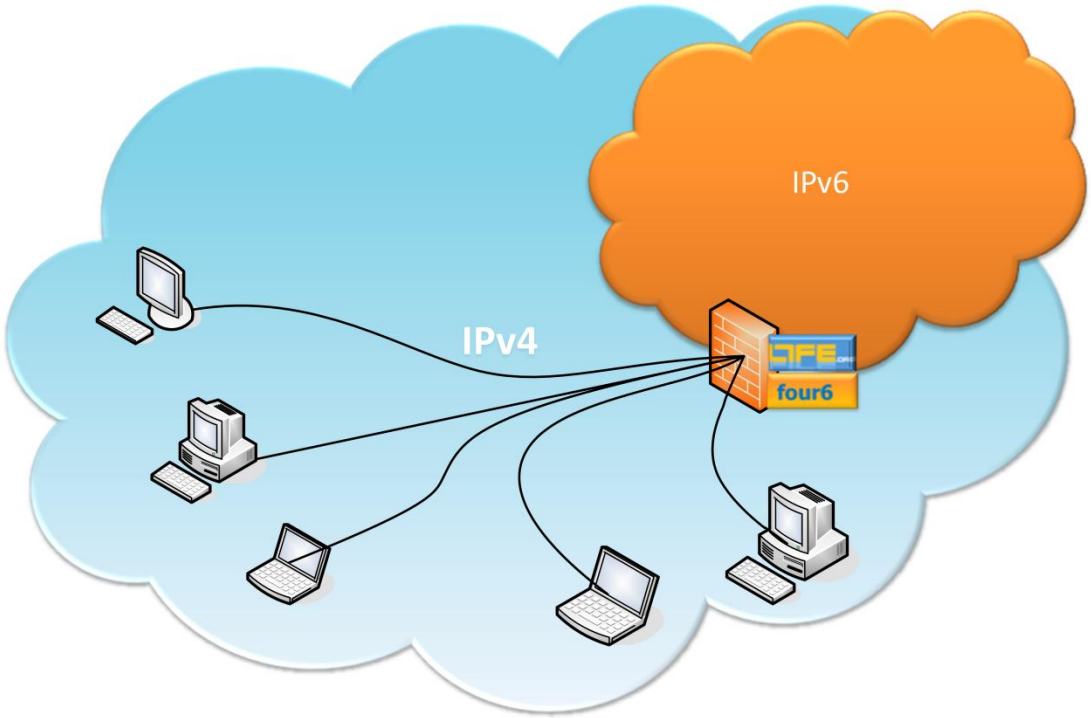
Vir: http://www.dante.net/server/show/conWebDoc.870

Slovenska iniciativa za prehod na IPv6

- go6.si
  - http://go6.si/
  - neprofitna slovenska organizacija in iniciativa za prehod na IPv6
  - ozaveščanje, izobraževanje, svetovanje in pomoč pri uvajanju IPv6 internetnega protokola na področju Slovenije in širše
  - organizacija srečanj in delavnic na temo uvajanja IPv6

LTFEfour6 tunel – www.ltfe.org

- Namenjen predvsem študentom UNI-LJ
- SSL VPN tehnologija
  - operacijski sistemi
    - Windows XP, Vista, 7
    - Linux
    - Mac OS



IPv6 v praksi

Podpora IPv6 pri proizvajalcih opreme

- Juniper – Junos, Netscreen
  - podpora v programski in strojni opremi
  - http://www.juniper.net
- Cisco – IOS
  - podpora v programski in strojni opremi
  - www.cisco.com/go/ipv6
- Microsoft Windows XP (SP1, SP2, SP3), Windows 2003 & 2008 Server, CE .NET (Pocket PC 4.1), Windows Vista & 7
  - http://www.microsoft.com/ipv6
- Linux – RedHat, Mandrake, SuSE, Debian, Ubuntu
- Mac OS
- FreeBSD
- Oracle (Sun) – Solaris
- IBM – z/OS Rel. 1.4, AIX 4.3, OS/390 V2R6 eNCS

Evolucijski pristop pri vpeljavi IPv6 1/2

- 1. Hrbtenica interneta (ISP)
  - usmerjevalniki nove generacije že imajo strojno podporo za posredovanje/usmerjanje IPv6
    - nadgradnja jedra in robnih naprav – dvojni protokolni sklad
      - usmerjanje IPv4 in IPv6 (OSPF ali ISIS)
    - nadgradnja samo robnih naprav (BRAS, N-PE)
      - IPv6 prek MPLS, GRE
      - usmerjanje v hrbtenici ostane IPv4
      - robne naprave – dvojni protokolni sklad
      - Dual stack VRF – IPv6 prek BGP
- 2. Dostopovna omrežja
  - xDSL (DSLAM), metro Ethernet stikala, WiMAX, DOCSIS, WiFi
    - DHCP relay, MLD snooping, MLD Proxy
    - PPPv6 IA?
- 3. Enterprise usmerjevalniki, L2/L3 stikala, požarni zidovi, sistemi IDS/IPS, proxy naprave
  - DHCP relay, DHCP proxy, SEND, MLD snooping, MLD Proxy
  - varnostne funkcije NDP, DHCP, MLD ”inspection”

Evolucijski pristop pri vpeljavi IPv6 2/2

- 4. Privzeta podpora na delovnih postajah, končnih odjemalcih
  - vsi operacijski sistemi podpirajo IPv6
  - privzeta podpora v OS
    - Windows Vista, 7 in Server 2008
    - Linux
    - Mac OS
    - FreeBSD
- 5. Podpora v aplikacijah
  - IE, Safari, Mozzila, Firefox, Google Chrome, Safari, Torrent, Ping6, traceroute6 …
- 6. Sčasoma bo vsak kos strojne in programske opreme privzeto podpiral IPv6

Vsebina

- *Uvod*
- ***Osnove***
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Zgodovina IPv6

- Začetki segajo v zgodnja 90. leta
  - velika poraba naslovnega prostora IPv4
  - študije so predvidevale popolno izrabo naslovnega prostora do leta 2005
- Možna sta bila dva pristopa
  - protokol IPv4 ostane enak, poveča se le naslovni prostor
  - razvoj popolnoma novega protokola
- Začetno delovno ime IP Next Generation (IPng)
- Prva specifikacija protokola (RFC 1883) je bila izdana leta 1995
  - ime protokola preimenovano v IPv6

Naslovni prostor IPv6

- **Naslovni prostor IPv6 je 128 biten**
  - 2^128 = 2^32 × 2^96
  - 340,282,366,920,938,463,463,374,607,431,768,211,456
  - 3.4 × 10^38
  - 655,570,793,348,866,943,898,599 (6.5 × 10^23) naslovov na kvadratni meter Zemeljske površine
  - 5.2 × 10^28 naslovov na zemljana (2006)
- **Slavni citati**
  - Thomas Watson, IBM, 1943
    - "I think there is a world market for maybe five computers"
  - Bill Gates, 1981
    - "640 K should be enough for anybody"
  - Vint Cerf, 1977
    - "32 bits ought to be enough address space"

Ključne novosti IPv6

- Povečan naslovni prostor (128 bitov) = 3.4 × 10^38 naslovov
- Naslavljanje unicast, multicast, anycast
  - nič več "broadcast" naslavljanja
- Poenostavljen format glave
  - fiksna dolžina glave (40 oktetov)
  - zmanjšano število polj
  - polja, ki niso nujna se nahajajo v opcijskih glavah
- Mehanizem za določitev MTU
  - IPv6 ne podpira fragmentacije paketov
- Nov protokol za poizvedbe med sosedi
  - protokol Neighbor Discovery
  - nadomešča protokol ARP
- Varnostni mehanizmi integrirani – obvezen IPSec
- Izboljšan mehanizem QoS
  - dodatno polje "Flow label", ki označuje prometni pretok
- Mehanizem za avtomatsko dodeljevanje naslovov
- Izboljšana mobilnost

Primerjava IPv4 in IPv6 1/2

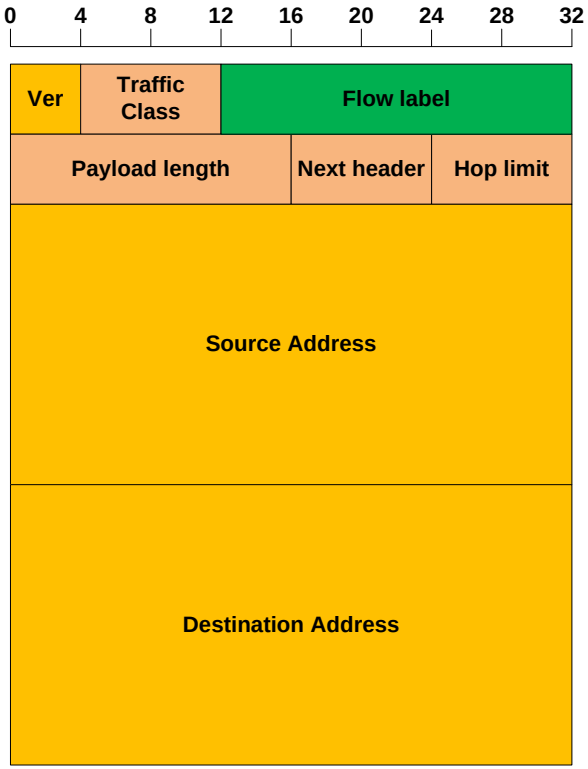
IPv4	IPv6
Naslovi so 32 bitni (4 okteti)	Naslovi so 128 bitni (16 oktetov)
Podpora za IPsec je opcijska	Podpora za IPsec je obvezna
IPv4 glava ne vsebuje ekvivalentnega polja	IPv6 glava vsebuje dodatno polje (flow label), ki omogoča identifikacijo različnih prometnih tokov
Izvorne naprave in usmerjevalniki lahko izvajajo fragmentacijo datagramov	Fragmentacijo datagramov lahko izvajajo le izvorne naprave
V glavi IP je vsebovana kontrolna vsota	Glava IP ne vsebuje polja za izračun kontrolne vsote
V osnovno glavo so vključena tudi opcijska polja	Opcijska polja se prenašajo v dodatnih glavah
Protokol ARP se uporablja za mapiranje med naslovi MAC (Ethernet) in IP	Funkcije protokola ARP izvaja protokol ICMPv6 – sporočila "Neighbor Solicitation"

Primerjava IPv4 in IPv6 2/2

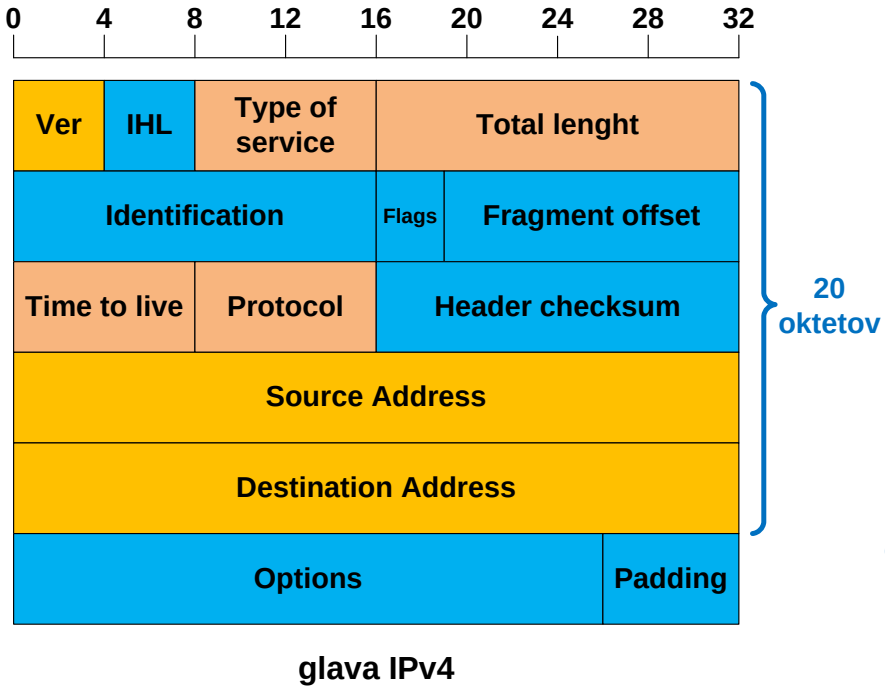
IPv4	IPv6
Za interakcijo med multicast odjemalci in robnimi usmerjevalniki se uporablja protokol IGMP	Za interakcijo med multicast odjemalci in robnimi usmerjevalniki se uporablja protokol MLD (ICMPv6)
Za naslavljanje vseh odjemalcev v podomrežju se uporablja broadcast naslov	IPv6 ne podpira broadcast naslovov. Za naslavljanje odjemalcev v podomrežju se uporabljajo multicast naslovi
Nastavitev parametrov IPv4: DHCP, ročno	Nastavitev parametrov IPv6: avtomatsko, DHCPv6, ročno
Za povezavo domenskih imen z naslovi IPv4 se uporablja "A source record"	Za povezavo domenskih imen z naslovi IPv6 se uporablja "AAAA source record"
Za povezavo naslovov IPv4 z domenskimi imeni se uporablja IN-ADDR.ARPA	Za povezavo naslovov IPv6 z domenskimi imeni se uporablja IP6.ARPA
Minimalen MTU je 576 oktetov	Minimalen MTU je 1280 oktetov

Glava datagrama IPv6

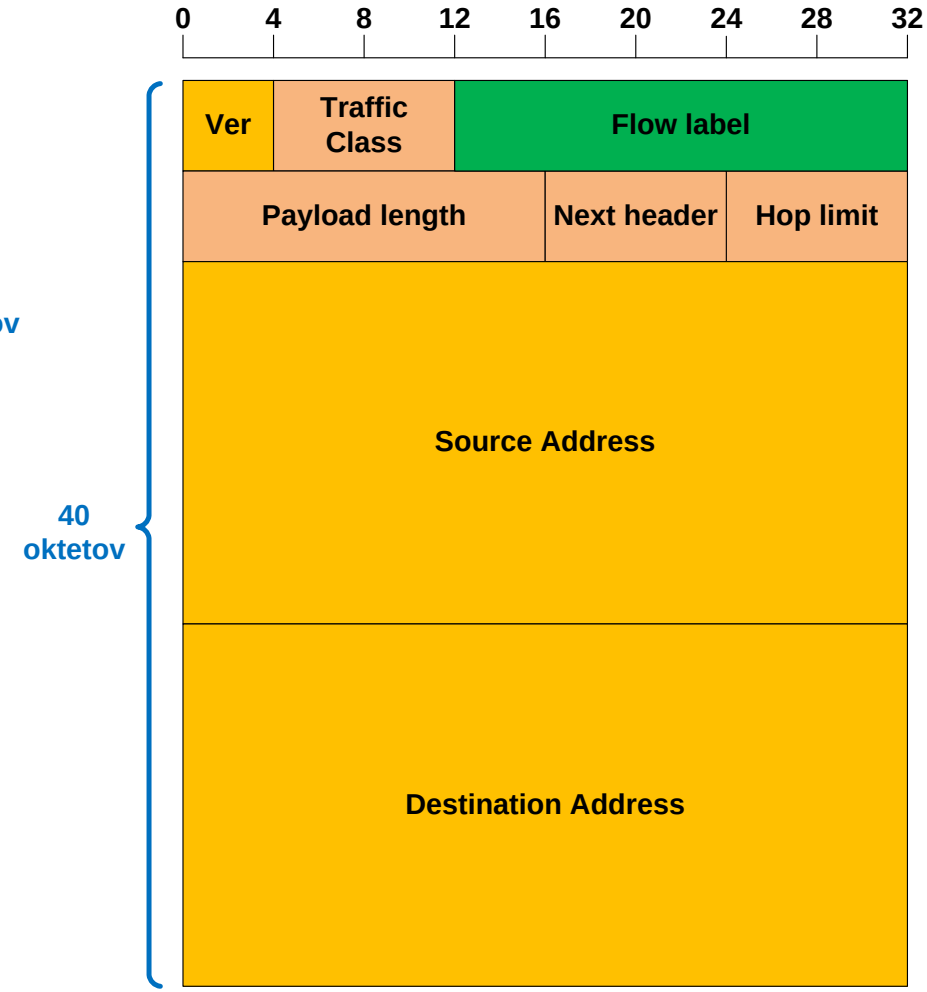
- Glava IPv6 je fiksne dolžine 40 oktetov
- Nepotrebna oziroma redko uporabljana polja se prenašajo v opcijskih glavah
  - kljub 4-krat večjemu naslovnemu prostoru je glava datagrama IPv6 (40 oktetov) le 2-krat večja od glave datagrama IPv4 (20 oktetov)



Primerjava glave IPv4 in IPv6



glava IPv4



glava IPv6

- Imena polj ostanejo enaka
- Ime in pozicija polja je spremenjena
- Odstranjena polja
- Novo polje

Polja v glavi IPv6

- **Version (4 biti)**
  - verzija protokola IP – vrednost polja je 6
- **Traffic Class (8 bitov)**
  - identifikator razreda oz. prioritete kateremu pripada datagram
- **Flow Label (20 bitov)**
  - identifikator prometnega pretoka med dvema odjemalcema
  - vrednost določi izvorna naprava
  - uporaba polja je določena v RFC 3697
- **Payload Length (16 bitov)**
  - dolžina koristne vsebine datagrama IPv6 vključno z opcijskimi glavami
- **Next Header (8 bitov)**
  - določa tip opcijske glave ali uporabljenega transportnega protokola (TCP, UDP, SCTP, ICMP)
- **Hop Limit (8 bitov)**
  - maksimalno število prehodov IP, ki jih lahko prečka datagram
  - določa "življenski čas" datagrama
- **Source Address (128 biten)**
  - določa izvorni naslov omrežne naprave
- **Destination Address (128 biten)**
  - določa ponorni naslov omrežne naprave

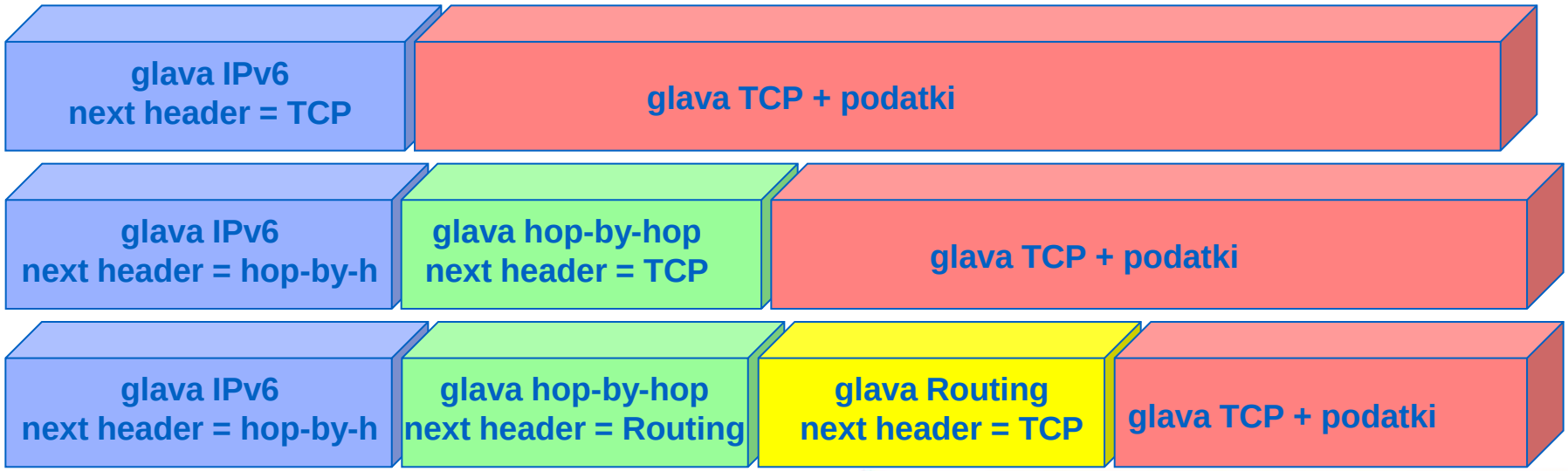
Primerjava polj IPv4 in IPv6

Glava IPv4	Glava IPv6
Version	Isto polje, spremenjena vrednost
Internet Header Length	Odstranjeno iz IPv6. Glava IPv6 je fiksne dolžine
Type of Service	Zamenjan s poljem "*Traffic Class*".
Total Length	Zamenjan s poljem "*Payload Length*"
Identification, Fragmentation Flags, Fragment Offset	Odstranjeno iz IPv6. V primeru izvajanja fragmentacije se potrebne informacije prenašajo v opcijskih glavah *"Fragment Header"*
Time to Live	Zamenjan s poljem "*Total Length*".
Protocol	Zamenjan s poljem "*Next Header*".
Header Checksum	Odstranjeno iz IPv6. Detekcija napak se izvaja na nižjih ali višjih slojih
Source Address	Isto polje, dolžina se poveča na 128 bitov
Destination Address	Isto polje, dolžina se poveča na 128 bitov
Options	Odstranjeno iz IPv6. Opcijska polja se prenašajo v opcijskih glavah.

Opcijske glave v IPv6

- Glavi IPv6 sledijo opcijske glave v sledečem zaporedju
  - hop-by-hop
  - destination option
  - routing
  - fragment
  - authentication header
  - encapsulating security payload
  - upper-layer (TCP, UDP, ICMP)

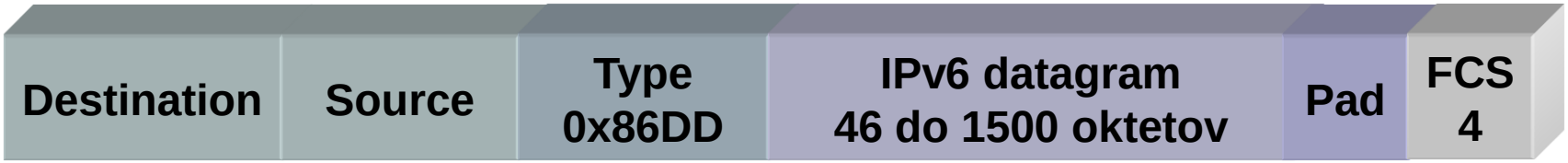
Vrednost polja (desetiško)	Pomen
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
46	Resource ReSerVation Protocol
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No next header
60	Destination Options Header



Prenos IPv6 prek Ethernet – RFC 1972

- V omrežjih LAN je najbolj razširjen Ethernet okvir verzije Ethernet II – DIXv2
- V primeru prenosa IPv6 v okvirju Ethernet II se v polje “Type” zapiše vrednost 86DD (hex)
  - minimalna velikost paketa IPv6 je 46 oktetov
  - maksimalna velikost paketa IPv6 je 1500 oktetov
- V primeru prenosa datagrama IPv4 se v polju “Type” nahaja vrednost 0800 (hex)

Okvir Ethernet II – DIXv2



TCP in UDP prek IPv6

- **Kontrolna vsota v glavi TCP in UDP je odvisna tudi od polj v glavi IPv4 in IPv6 (RFC 2460)**
  - **izvorni naslov IPv6**
  - **ponorni naslov IPv6**
  - **dolžina koristne vsebine, vključno z glavo TCP oziroma UDP**
  - **polja "next header"**

Vsebina

- *Uvod*
- *Osnove*
- ***Naslavljanje***
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Naslavljanje v IPv6

- Naslovni prostor je 128 bit-en (RFC 3513)
  - naslavljanje temelji na principu CIDR
    - naslov omrežja/maska
    - 2001:1470:FFFE:1::/64
  - naslov IPv6 je zapisan v skupinah po 16 bit-ov v formatu HEX, posamezne skupine so ločene z dvopičjem
    - 2002:c14d:4f42:1:50e6:3a11:10bd:fab8 (colon-hexadecimal)
  - vodilne ničle niso obvezne, zaporedne ničle se lahko zapišejo kot "::" (double-colon)
    - 0:0:0:0:0:0:0:1 ⇔ ::1
  - primer krajšave zapisa naslova FF02:3000:0:0:0:0:0:2
    - FF02:3::2 – ni pravilno!
    - FF02:3000::2 – pravilno!
- Primer zapisa naslova IPv6
  - binarno
    - 0000000000000000 1111111111111111 1000100010001000 1111111111111111
0000000000000000 1111111111111111 1000100010001000 1111111111111111
  - hex
    - 0000:FFFF:8888:FFFF:0000:FFFF:8888:FFFF

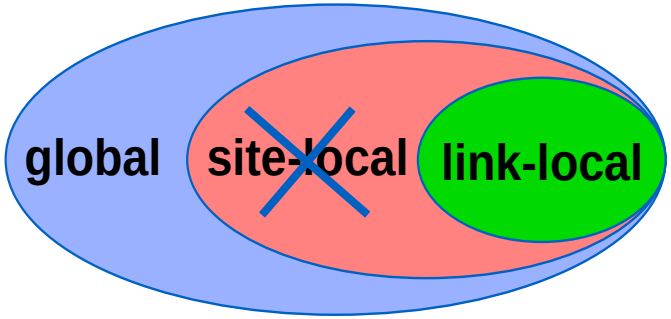
Tipi naslovov IPv6

- **Unicast naslov**
  - identificira posamezno napravo oziroma vmesnik
- **Anycast naslov**
  - identificira skupino naprav
  - dostava se izvede najbližji naprav (s stališča usmerjanja)
  - "one–to–one-of-many"
- **Multicast naslov**
  - naslavljanje skupine naprav
- **Ni broadcast naslovov!**
  - nalogo broadcast naslavljanja so prevzeli multicast naslovi
- **IPv4 kompatibilni naslovi (10.14.1.11 ➔ ::0A0E:010B)**

Unicast naslovi

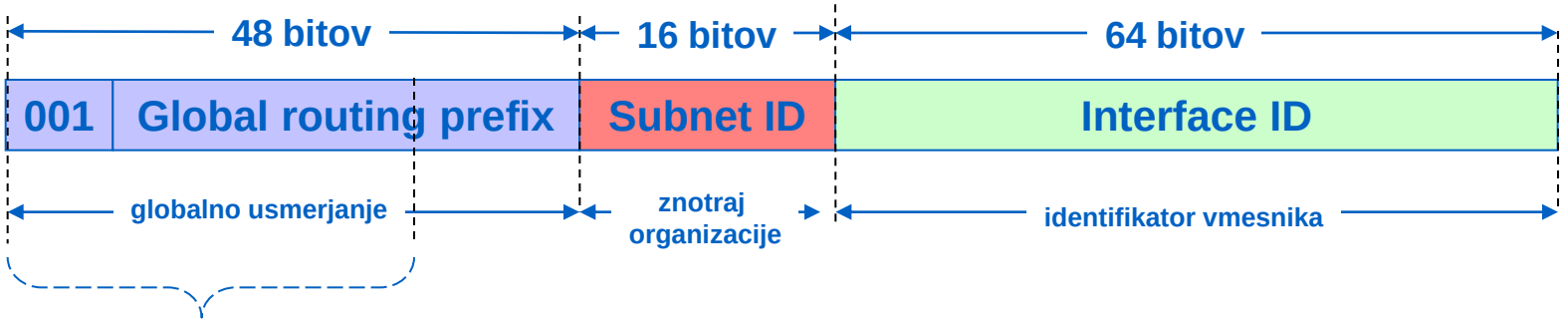
Delitev unicast naslovov

- Globalni naslovi – RFC 3587
  - ekvivalent javnim naslovom IPv4
  - imajo globalen doseg
- "Link-local" naslovi
  - ekvivalent avtomatskim naslovom IPv4
  - doseg znotraj posameznega subnet-a
  - vedno se začnejo z 1111 1110 10 (FE80::/10)
- "Site-local" naslovi – se ne uporabljajo več (RFC 3879)!
  - ekvivalent privatnim naslovom IPv4 (RFC 1918)
  - vedno se začnejo z 1111 1110 11 (FEC0::/10)
  - še vedno podprti v večini trenutnih implementacij IPv6
- "Unique local" naslovi
  - globalno unikaten naslov, zamenjava za "Site-local" naslove
- Rezervirani
  - 0:0:0:0:0:0:0:0 (::) – nedoločen naslov (privzeta pot)
  - 0:0:0:0:0:0:0:1 (::1) – "loopback" naslov



Globalni naslovi 1/2

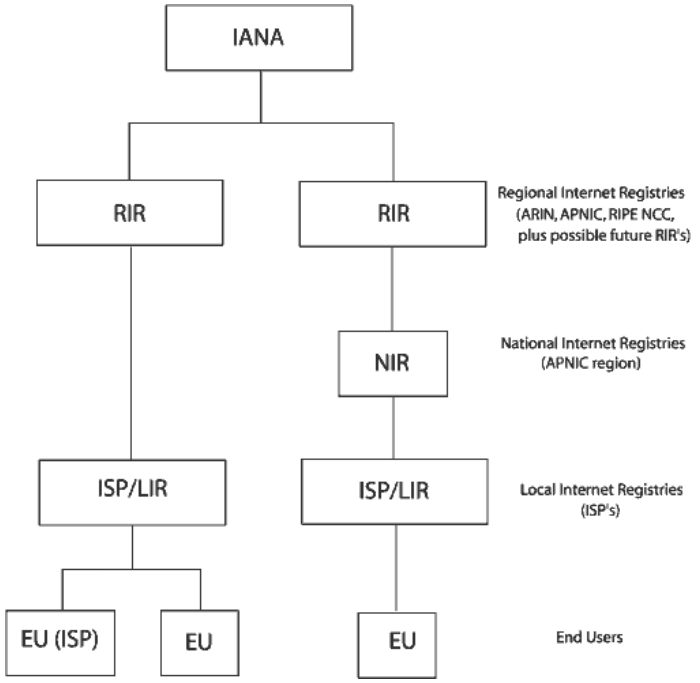
- Naslavljanje in usmerjanje IPv6 je hierarhično
  - "Global routing prefix"
    - predpona, ki identificira posamezno organizacijo
    - uporablja se za globalno usmerjanje
  - "Subnet ID"
    - predpona, ki identificira posamezno omrežje znotraj organizacije
    - uporablja se za usmerjanje znotraj organizacije
  - "Interface ID"
    - identifikator vmesnika
- Vsi trenutno dodeljeni globalni naslovi se začnejo z 001
  - RFC 3587

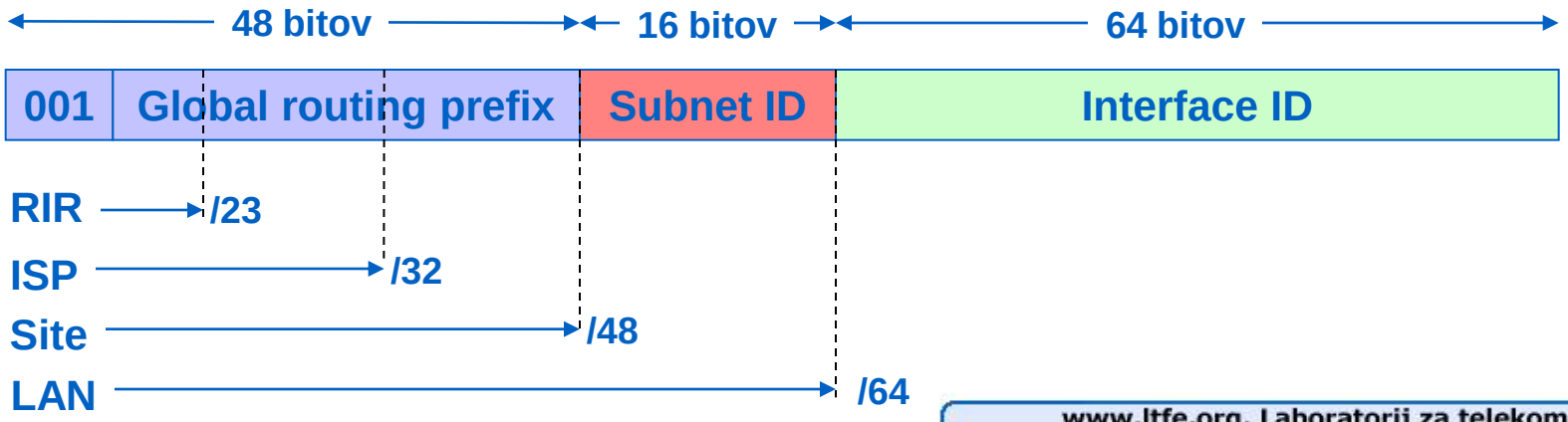


Vnosi v BGP usmerjevalni tabeli /32

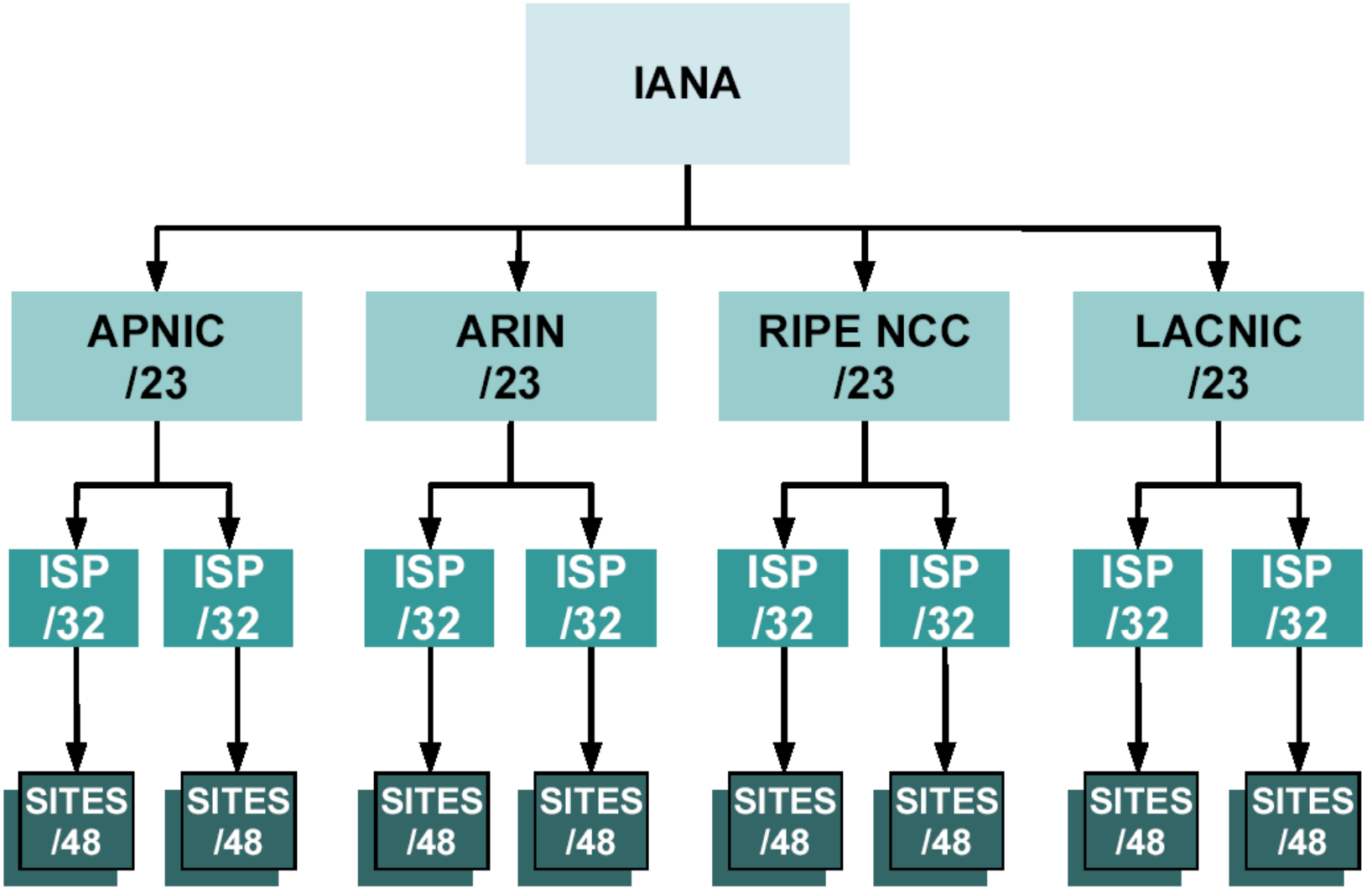
Globalni naslovi 2/2

- Dodeljuje ga IANA
- Obstoječi RIR
  - RIPE NCC
    - 2001:0600::/23, 2001:0800::/23
  - APNIC
    - 2001:0200::/23 in 2001:0C00::/23
  - ARIN
    - 2001:0400::/23
- 6Bone 3FFE::/16
- Tuneli 6to4 2002::/16



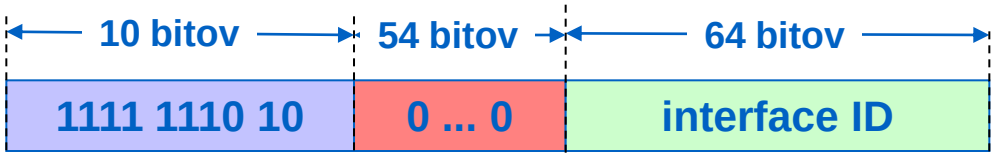


Dodeljevanja globalnih naslovov



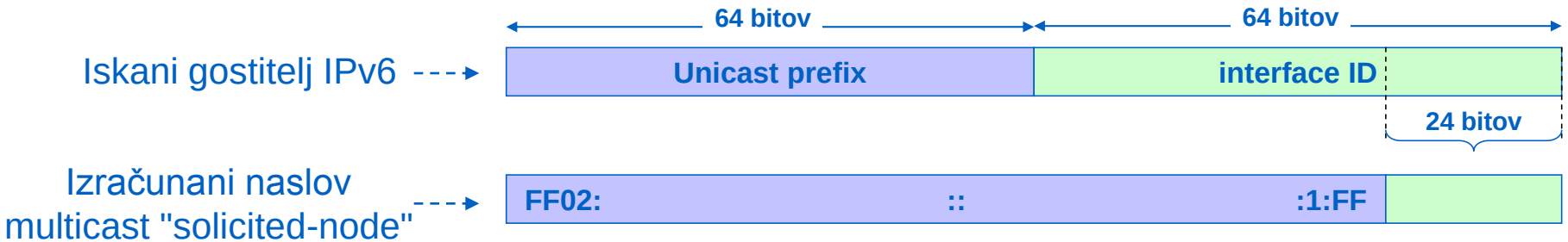
Naslovi “link-local”

- Ekvivalenten avtomatskim naslovom IPv4
  - doseg znotraj posameznega subnet-a
  - paket z naslovom “link-local” se nikoli ne posreduje zunaj lokalnega omrežja
  - generira in nastavi se avtomatsko, tudi v primeru ko v omrežju ni usmerjevalnika
  - uporablja se v procesu “Neighbor discovery”
  - vedno se začnejo z 1111 1110 10 (FE80::/10)
- Primer izračuna naslova “link-local”
  - prvih 10 bitov je fiksnih (1111 1110 10)
  - sledi jim 54 ničel
  - interface ID se generira iz naslova MAC



Naslov "Solicited-Node"

- Multicast naslov, ki se uporablja v procesu iskanja sosedov
  - mapiranje IPv6 naslovov v naslove MAC
- Iskanje sosedov v IPv4
  - pošlje se zahteva ARP tipa broadcast
  - vse naprave v Ethernet domeni procesirajo zahteve ARP
- Iskanje sosedov v IPv6
  - pošlje se sporočilo ICMP "Neighbor discovery"
  - kot ciljni naslov se uporabi "solicited-node address"
  - samo napravi, ki ji pripada iskani naslov IPv6, se dostavi sporočilo
- Primer izračuna naslova "solicited-node"



Vsebina

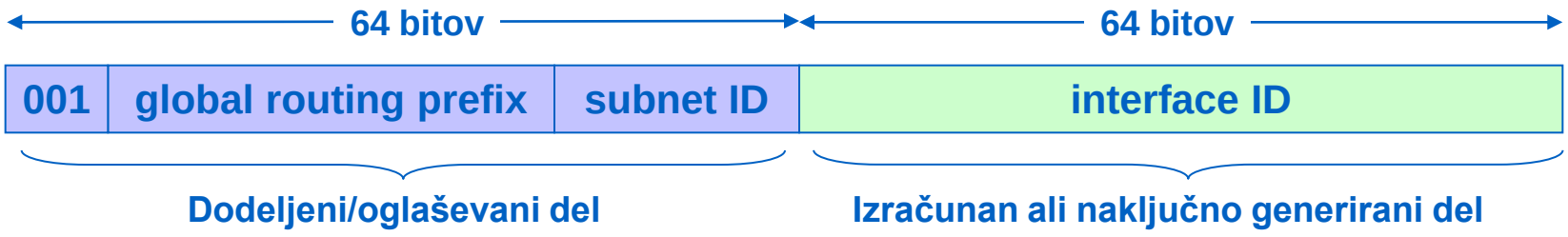
- *Uvod*
- *Osnove*
- *Naslavljanje*
- ***Mehanizmi za dodeljevanje naslovov***
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Naslovi IPv6 na odjemalcih

- Pripadajoči naslovi IPv6 na odjemalcu
  - lokalen naslov (link-local), izračunan iz naslova Ethernet MAC
  - globalen unicast naslov (lahko jih je več)
    - opcijsko je lahko dodeljen tudi "site-local" naslov (se ne uporabljajo več)
  - naslov vmesnika loopback ::1
- Pripadajoči naslovi IPv6 na usmerjevalniku – vsak vmesnik
  - globalen unicast naslov (lahko jih je več) s pripadajočo masko
    - opcijsko je lahko dodeljen tudi "site-local" naslov (se ne uporabljajo več)
  - lokalen naslov (link-local), izračunan iz naslova Ethernet MAC
  - anycast naslov za vsako podomrežje
  - naslov vmesnika loopback ::

Mehanizmi za dodeljevanje naslovov

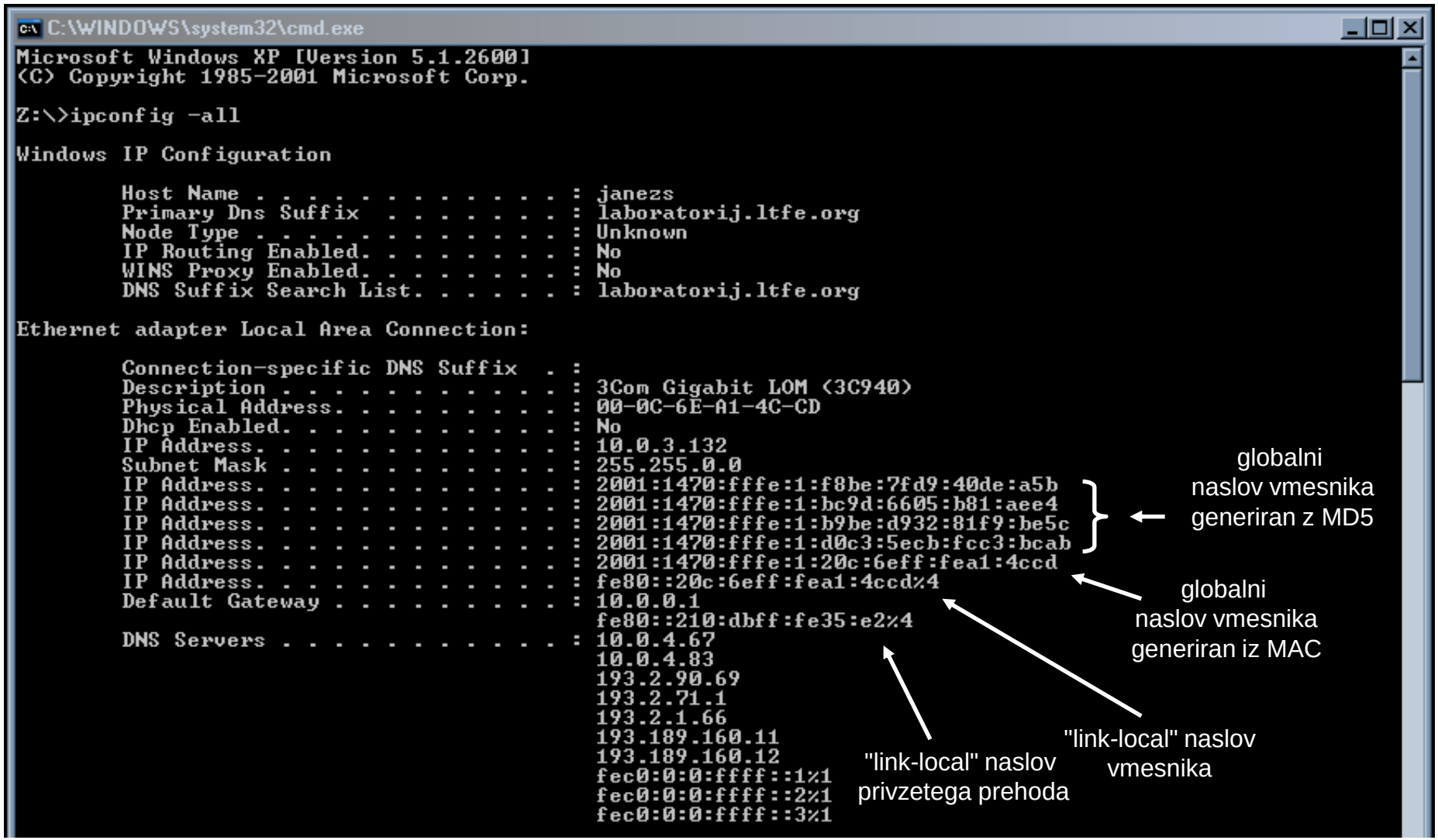
- Naslov nastavljen ročno
- Naslov dodeljen na osnovi protokola DHCPv6 " stateful"
- Terminal izračuna svoj naslov (interface ID) "stateless"
  - na osnovi identifikatorja IEEE EUI-64 ali na osnovi razširjenega naslova Ethernet MAC
  - usmerjevalniki oglašujejo omrežje v katerem se naprava nahaja
    - sporočila ICMPv6
      - router solicitation/ router advertisements
      - neighbor solicitation/ neighbor advertisements
- Terminal generira naključen "interface ID" (RFC 3041)
  - na osnovi zgoščevalne funkcije MD5
  - omejen čas trajanja (za zagotavljanje anonimnosti)



DHCPv6

- Predstavlja razširitev protokola DHCP iz IPv4
  - "statefull" DHCP (RFC 3315)
    - malo praktično delujočih implementacij
  - "stateless" DHCP (RFC 3736)
    - omejen nabor opcij iz osnovnega standarda
    - konfiguracijski parametri
- Podpira nov način naslavljanja IPv6
- Uporablja se lahko za avtomatsko registracijo domenskih imen
- Princip delovanja je "podoben" kot v primeru IPv4
  - naprava preveri, če je v omrežju prisoten usmerjevalnik
  - v sporočilu "router advertisements" preveri če lahko uporabi storitev DHCP
  - naprava pošlje zahtevo DHCP "Solicit message" na multicast naslov FF02::1:2 (vsi DHCP agenti)
    - kot izvoren naslov IPv6 uporabi svoj "link-local" naslov

Naslovi IPv6 – Windows XP

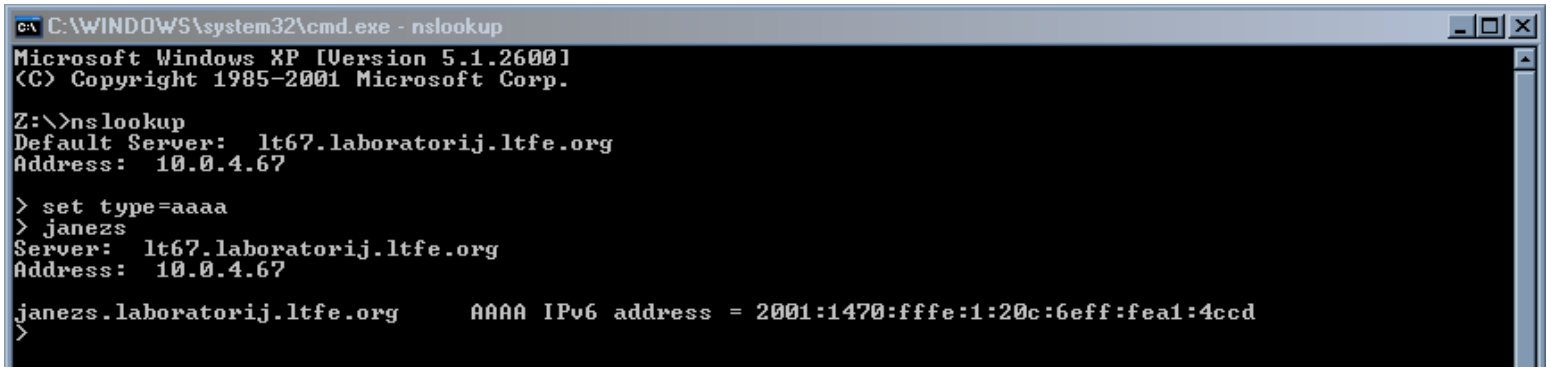


Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- ***DNS in IPv6***
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

DNS in IPv6

- Za povezovanje domenskih imen z naslovi IPv6 se uporablja DNS sporočilo "host address resource record" tipa AAAA (RFC 1886, RFC 3152)
  - janezs.laboratorij.ltfe.org; AAAA 2001:1470:fffe:1:20c:6eff:fea1:4ccd
- Za povratno poizvedbo se uporablja domena IP6.ARPA
  - d.c.c.4.1.a.e.f.f.f.e.6.c.0.2.0.1.0.0.0.e.f.f.f.0.7.4.1.1.0.0.2.IP6.ARPA
- Praktične implementacije IPv6 v operacijskih sistemih omogočajo poizvedovanje tipa A ali AAAA prek IPv6 DNS poizvedb ali prek IPv4 DNS poizvedb
- Korenski strežniki DNS podpirajo IPv6 od julija 2004



Primer IPv6 DNS poizvedbe prek IPv4

- **DNS poizvedba tipa AAAA (IPv6)**

```
⊞ Frame 62 (72 bytes on wire, 72 bytes captured)
⊞ Ethernet II, Src: AsustekC_a1:4c:cd (00:0c:6e:a1:4c:cd), Dst: 3com_0f:3a:57 (00:01:02:0f:3a:57)
⊞ Internet Protocol, Src: 10.0.3.132 (10.0.3.132), Dst: 10.0.4.83 (10.0.4.83)
⊞ User Datagram Protocol, Src Port: 1026 (1026), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x2513
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.6net.org: type AAAA, class IN
        Name: www.6net.org
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

- **DNS odgovor tipa AAAA (IPv6)**

```
⊞ Frame 63 (485 bytes on wire, 485 bytes captured)
⊞ Ethernet II, Src: 3com_0f:3a:57 (00:01:02:0f:3a:57), Dst: AsustekC_a1:4c:cd (00:0c:6e:a1:4c:cd)
⊞ Internet Protocol, Src: 10.0.4.83 (10.0.4.83), Dst: 10.0.3.132 (10.0.3.132)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 1026 (1026)
⊟ Domain Name System (response)
    Transaction ID: 0x2513
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 6
    Additional RRs: 10
  ⊞ Queries
  ⊟ Answers
    ⊟ www.6net.org: type AAAA, class IN, addr 2001:610:148:dead:210:18ff:fe02:e38
        Name: www.6net.org
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
        Time to live: 4 minutes, 32 seconds
        Data length: 16
        Addr: 2001:610:148:dead:210:18ff:fe02:e38
  ⊞ Authoritative nameservers
  ⊞ Additional records
```

Primerjava naslavljanja IPv4 in IPv6

IPv4	IPv6
Multicast naslovi (224.0.0.0/4)	Multicast naslovi (FF00::/8)
Broadcast naslovi	Ne obstaja ekvivalenten naslov PIV
Nedoločen naslov 0.0.0.0	Nedoločen naslov ::
"Loopback" naslov 127.0.0.1	"Loopback" naslov ::1
Javni naslovi IP	Globalni "unicast" naslovi
Privatni naslovi IP (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)	Naslovi "Site-local" (se ne uporabljajo več) Naslovi "Unique-local"
Avtomatsko dodeljeni (169.254.0.0/16)	Naslovi "Link-local" (FE80::/64)
Pretvorba imen DNS: IPv4 host address (A) resource record	Pretvorba imen DNS: IPv6 host address (AAAA) resource record
Inverzna poizvedba imen DNS: domena IN-ADDR.ARPA	Inverzna poizvedba imen DNS: domena IP6.ARPA

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- ***ICMPv6***
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Protokol ICMPv6

- Predstavlja razširitev funkcij protokola ICMP iz IPv4
- Izvaja nekaj ključnih nalog v okviru IPv6
  - obveščanje o napakah pri prenosu in dostavi datagramov
    - "Destination Unreachable"
    - "Packet Too Big"
    - "Time Exceeded"
    - "Parameter Problem"
  - funkcije OAM
    - ping
    - traceroute
  - podpora interakciji med multicast odjemalci in robnimi usmerjevalniki
    - transport sporočil MLD (Multicast Listeners Discovery)
    - zamenjava protokola IGMP
  - podpora neposredni komunikaciji med odjemalci IPv6
    - transport sporočil ND (Neighbor Discovery)
    - zamenjava protokolov ARP, ICMP Router Discovery, ICMP Redirect

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- ***Usmerjanje***
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Usmerjanje IPv6

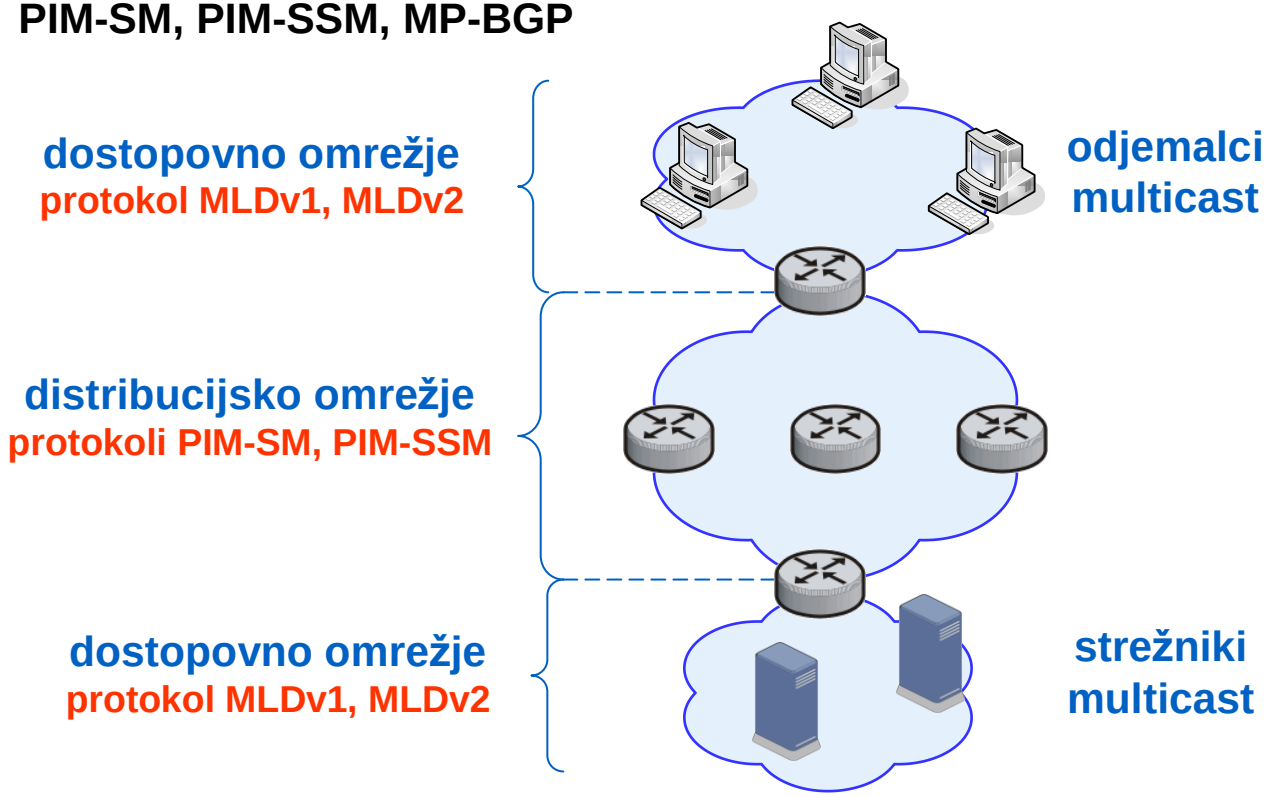
- Enaki principi kot v primeru usmerjanja v IPv4
- Usmerjevalnik poišče za vsak sprejeti paket IPv6 optimalno pot (izhoden vmesnik) v usmerjevalni tabeli
  - iskanje "longest-prefix match"
- Dve družini usmerjevalnih protokolov
  - IGP
    - RIPng (RFC 2080)
    - Integrated ISISv6 (draft-ietf-isis-ipv6-02)
    - OSPFv3 (RFC 2740)
  - EGP
    - MP-BGPv4 (RFC 2858, RFC 2545)
  - potrebna je nadgradnja protokolov
- Statične poti
  - za naslov naslednjega hopa (usmerjevalnika) se naj uporabi njegov "link-local" naslov – omogoča dinamične preusmeritve
    - sporočila "ICMPv6 redirect"

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- ***Multicast***
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

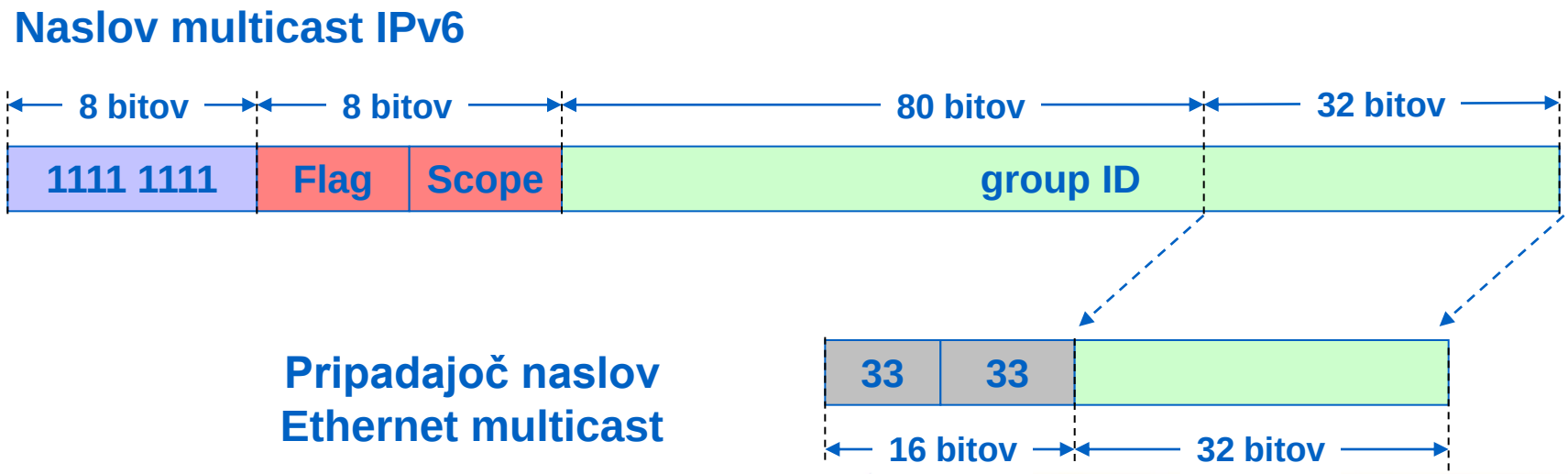
Arhitekturni gradniki

- Enak koncept delovanja kot v primeru IPv4 multicast
  - komunikacija med robnimi usmerjevalniki in odjemalci multicast
    - protokol MLDv1, MLDv2
  - komunikacija med jedrnimi usmerjevalniki
    - PIM-SM, PIM-SSM, MP-BGP



MLD snooping

- MLD snooping – ekvivalent IGMP snooping
  - klasična Ethernet stikala obravnavajo multicast promet na enak način kot broadcast promet
- Ethernet multicast naslov, ki predstavlja ekvivalent IPv6 mulicast naslovu je sestavljen iz dveh delov (RFC 3513)
  - fiksni del, dolžine 16 bitov – 33 33 (hex)
  - variabilni del – zadnjih 32 bitov naslova multicast IPv6 (group ID) se preslika v Ethernet multicast naslov



Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- ***Orodja***
- *Aplikacije*
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Ping verzija 6

- Najbolj uporabljano orodje IP OAM
  - uporablja se za preverjanje dosegljivosti naprav v omrežju
- Opravlja enake funkcije kot v primeru protokola IPv4
- Za delovanje uporablja sporočila protokola ICMPv6
  - Echo Request
  - Echo Reply
- Program pošlje zahtevo ICMP in izpisuje informacije o prejetih odgovorih
  - meri čas posredovanja paketa od izvora do ponora ter nazaj
    - indikacija, kako “daleč v omrežju” je določena naprava
  - število izgubljenih paketov
  - velikost paketa

Primer uporabe orodja Ping

- Windows OS

```
Z:\>ping6 -?

Usage: ping6 [-t] [-a] [-n count] [-l size] [-w timeout] [-s srcaddr] [-r] dest

Options:
-t              Ping the specifed host until interrupted.
-a              Resolve addresses to hostnames.
-n count        Number of echo requests to send.
-l size         Send buffer size.
-w timeout      Timeout in milliseconds to wait for each reply.
-s srcaddr      Source address to use.
-r              Use routing header to test reverse route also.

Z:\>ping6 2001:1470:fffe:1::1

Pinging 2001:1470:fffe:1::1
from 2001:1470:fffe:1:88eb:7a97:aaa5:4a4a with 32 bytes of data:

Reply from 2001:1470:fffe:1::1: bytes=32 time=1ms
Reply from 2001:1470:fffe:1::1: bytes=32 time=1ms
Reply from 2001:1470:fffe:1::1: bytes=32 time=1ms
Reply from 2001:1470:fffe:1::1: bytes=32 time=1ms

Ping statistics for 2001:1470:fffe:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

Z:\>
```

Traceroute verzija 6

- Traceroute je aplikacija, ki izpiše pot, po kateri potuje paket od izvorne do ponorne naprave
- Opravlja enake funkcije kot v primeru protokola IPv4
- Za delovanje uporablja sporočila protokola ICMPv6
  - Echo Request
  - Time Exceeded
- Izpiše
  - pot paketa in zakasnitev na vsakem vozlišču
  - napake v omrežju
  - točko prekinitve komunikacije
- Ni garancije, da bosta dva zaporedna paketa res šla po isti poti
- Ni garancije, da je pot nazaj enaka poti od izvorne do ponorne naprave

Primer uporabe orodja Traceroute

- Windows OS

```
Z:\>tracert6 www.6net.org

Tracing route to www.6net.org [2001:610:148:dead:210:18ff:fe02:e38]
from 2001:1470:fffe:1:88eb:7a97:aaa5:4a4a over a maximum of 30 hops:

  1       <1 ms    <1 ms    <1 ms  2001:1470:fffe:1::1
  2        3 ms     3 ms     3 ms  2001:1470:fffe::1
  3        8 ms     9 ms     8 ms  rarnes2-v6-T1.arnes.si [2001:1470:fe:1000:0:1:0:1]
  4        7 ms     8 ms     8 ms  larnes6-v6-V603.arnes.si [2001:1470:0:10ff:0:1:0:1]
  5        8 ms    18 ms     8 ms  rarnesGEANT-v6-V600.arnes.si [2001:1470:0:ff00::1]
  6        8 ms     8 ms     8 ms  arnes.si1.si.geant.net [2001:798:2026:10aa::5]
  7       15 ms    16 ms    16 ms  si.at1.at.geant.net [2001:798:20cc:1001:2601::1]
  8       23 ms    23 ms    23 ms  at.hu1.hu.geant.net [2001:798:20cc:1001:1801::6]
  9       26 ms    49 ms    26 ms  hu.sk1.sk.geant.net [2001:798:20cc:1801:2701::2]
 10       30 ms    31 ms    31 ms  sk.cz1.cz.geant.net [2001:798:20cc:1301:2701::1]
 11       62 ms    39 ms    38 ms  so-6-3-0.rt1.fra.de.geant2.net [2001:798:cc:1301:1401::2]
 12       60 ms    46 ms    46 ms  so-5-0-0.rt1.ams.nl.geant2.net [2001:798:cc:1401:2201::2]
 13       45 ms    45 ms    46 ms  2001:798:22:10aa::e
 14        *        *        *     Request timed out.
 15       46 ms    46 ms    62 ms  TERENA-router.Customer.surf.net [2001:610:ff:5::2]
 16       47 ms    46 ms    46 ms  TERENA-router.Customer.surf.net [2001:610:ff:5::2]
 17       45 ms    46 ms    46 ms  www.6net.org [2001:610:148:dead:210:18ff:fe02:e38]

Trace complete.

Z:\>
```

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- ***Aplikacije***
- *Tranzicijski mehanizmi*
- *IPv6 na končnih napravah*

Aplikacije IPv6 1/2

- V aplikacijah mora biti zagotovljena ustrezna podpora za delovanje prek IPv6
  - novi naslovni prostor!

Aplikacije IPv6 2/2

- Primeri aplikacij, ki imajo podporo za IPv6
  - 6DISS (nadaljevanje projekta 6net)
  - http://www.6diss.org/

Aplikacija	Uporaba
Apple iTunes	Audio/video klient
Apple QuickTime	Audio/video klient
VideoLAN/VLC	Audio/video klient
Quake 3	Igra
Mozilla Firefox	HTTP klient/brskalnik
Opera	HTTP klient/brskalnik
Mozilla Thunderbird	Mail klient
BitTorrent	P2P klient
RealVNC	Klient za oddaljeni dostop
Wireshark	Analizator omrežnega prometa
Putty	Telnet klient
Smart FTP	FTP klient
BEA WebLogic SIP Server	SIP strežnik

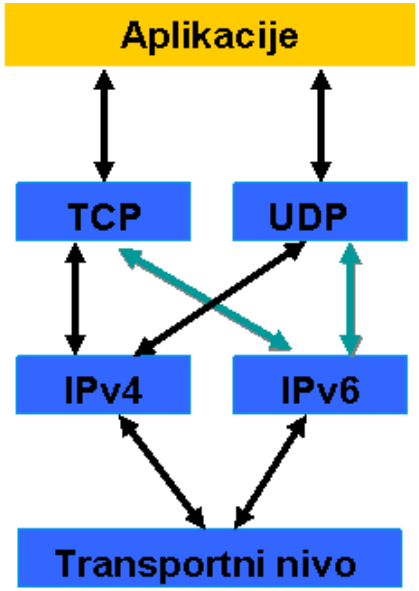
Vir: www.ipv6-to-standard.org

Vsebina

- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- ***Tranzicijski mehanizmi***
- *IPv6 na končnih napravah*

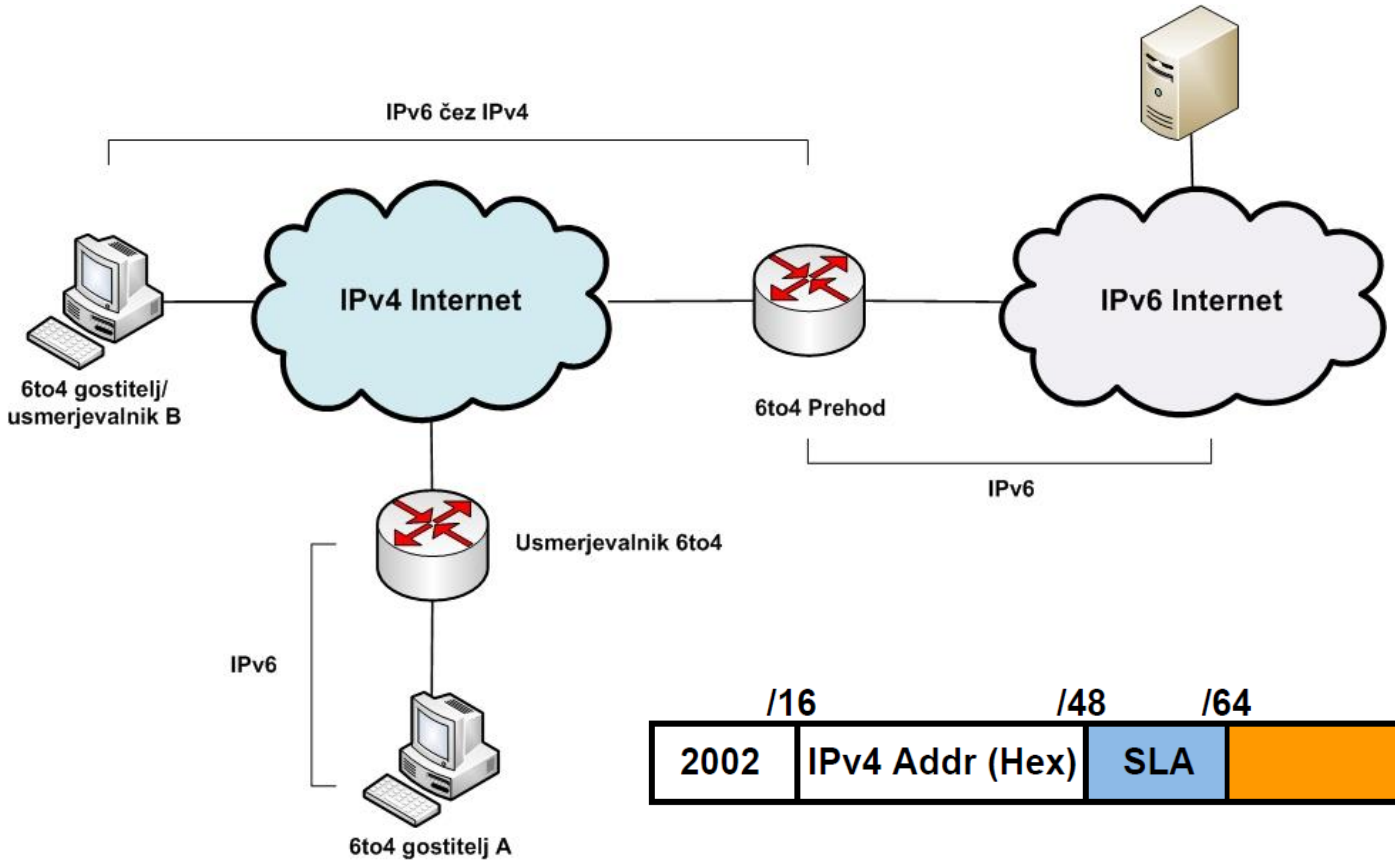
Prehod iz IPv4 v IPv6

- Zvezen, sočasen obstoj obeh verzij
- dvojni protokolni sklad "dual stack"
  - naprave s protokolnim skladom IPv4 in IPv6
- Tuneliranje
  - IPv6 prek IPv4 (RFC 2893)
  - IPv6 prek GRE (RFC 2473)
  - IPv4 kompatibilni naslovi (RFC 2893)
    - iz naslova IPv4 se izračuna IPv6 (::192.168.100.1)
  - 6to4 (RFC 3056)
    - iz naslova IPv4 izračunamo IPv6 (2002:192.168.100.1::/48)
    - javni "6to4 anycast relay" – 2002:c058:6301:: (RFC3068)
  - ISATAP
  - Teredo (prehajanje naprav NAT)
- Prevajanje naslovov IPv4 ⇔ IPv6 (NAT-PT)
  - komunikacija med napravami, ki imajo samo IPv4 ali samo IPv6 protokolni sklad (RFC 2766)



Tuneliranje 6to4

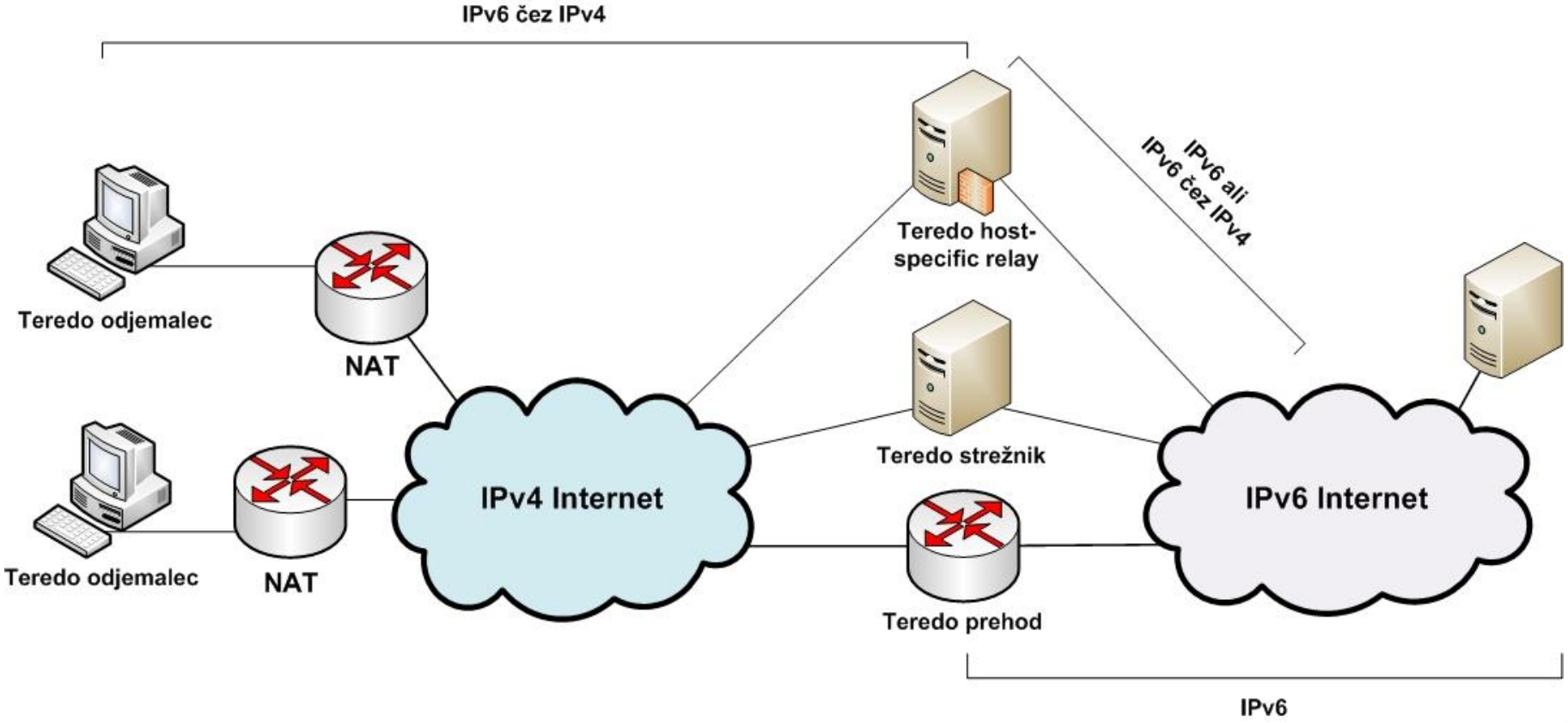
- **Komponente**
  - gostitelji
  - usmerjevalniki
  - prehodi (relay)



Tuneliranje Teredo

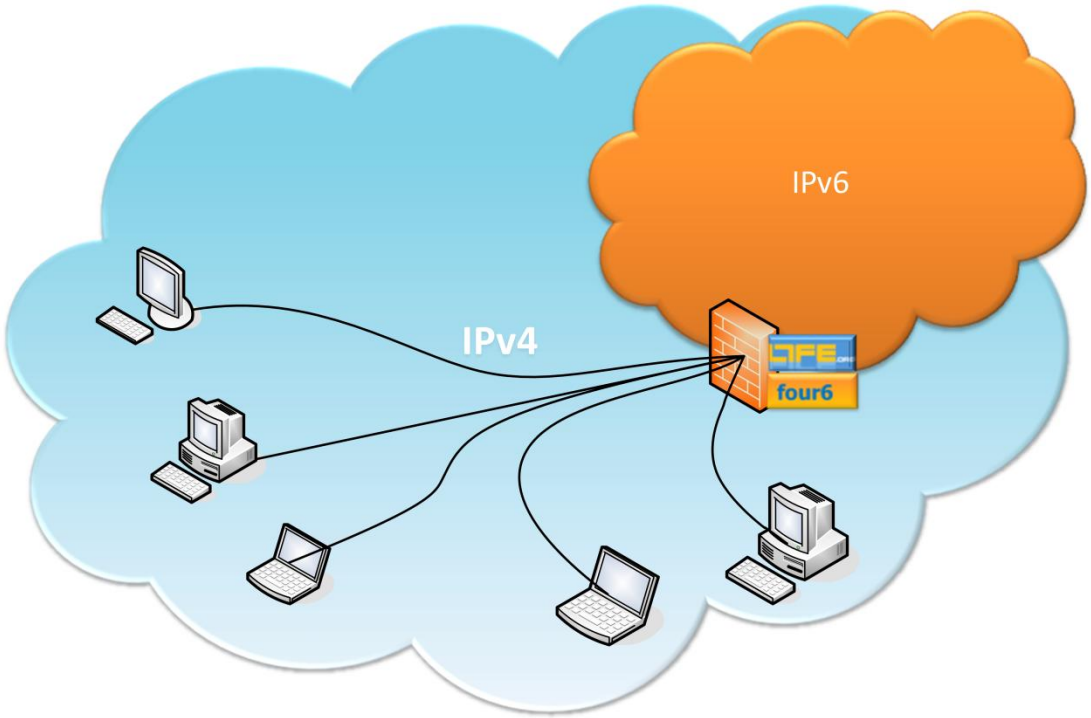
- **Komponente**
  - gostitelji/strežniki
  - prehodi (relay)
  - ‘’host-specific relay’’

Teredo predpona 2001:0000	Naslov IPv4 Teredo strežnika	Zastavice	Zunanji UDP port	Zunanji naslov IPv4



LTFEfour6 tunel – www.ltfe.org

- Namenjen študentom UNI-LJ
- SSL VPN tehnologija
  - Operacijski sistemi
    - Windows XP, Vista, 7
    - Linux
    - Mac OS

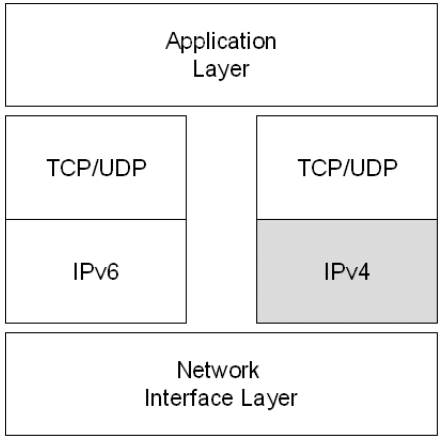


Vsebina

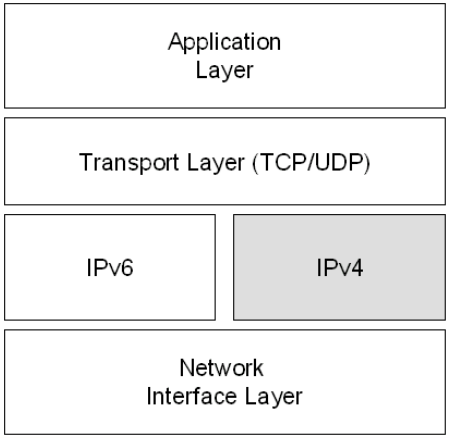
- *Uvod*
- *Osnove*
- *Naslavljanje*
- *Mehanizmi za dodeljevanje naslovov*
- *DNS in IPv6*
- *ICMPv6*
- *Usmerjanje*
- *Multicast*
- *Orodja*
- *Aplikacije*
- *Tranzicijski mehanizmi*
- ***IPv6 na končnih napravah***

IPv6 & Microsoft 1/2

- "Microsoft loves IPv6" ☺
- Windows XP & Server 2003
  - opcijsko
  - *ipv6 install*
  - ločen protokolni sklad L3 in L4
  - pod privzetimi nastavitvami uporablja IPv4
  - DNS
    - najprej zahteva AAAA (IPv6), nato A (IPv4)



- Windows Vista, 7 & Server 2008
  - privzeto nameščen in omogočen IPv6
  - ločen protokolni sklad na L3 in enoten na L4
  - DNS
    - optimizacija glede na Windows XP – težave ☺
  - MLDv2
  - IPv6/PPP
  - DHCPv6

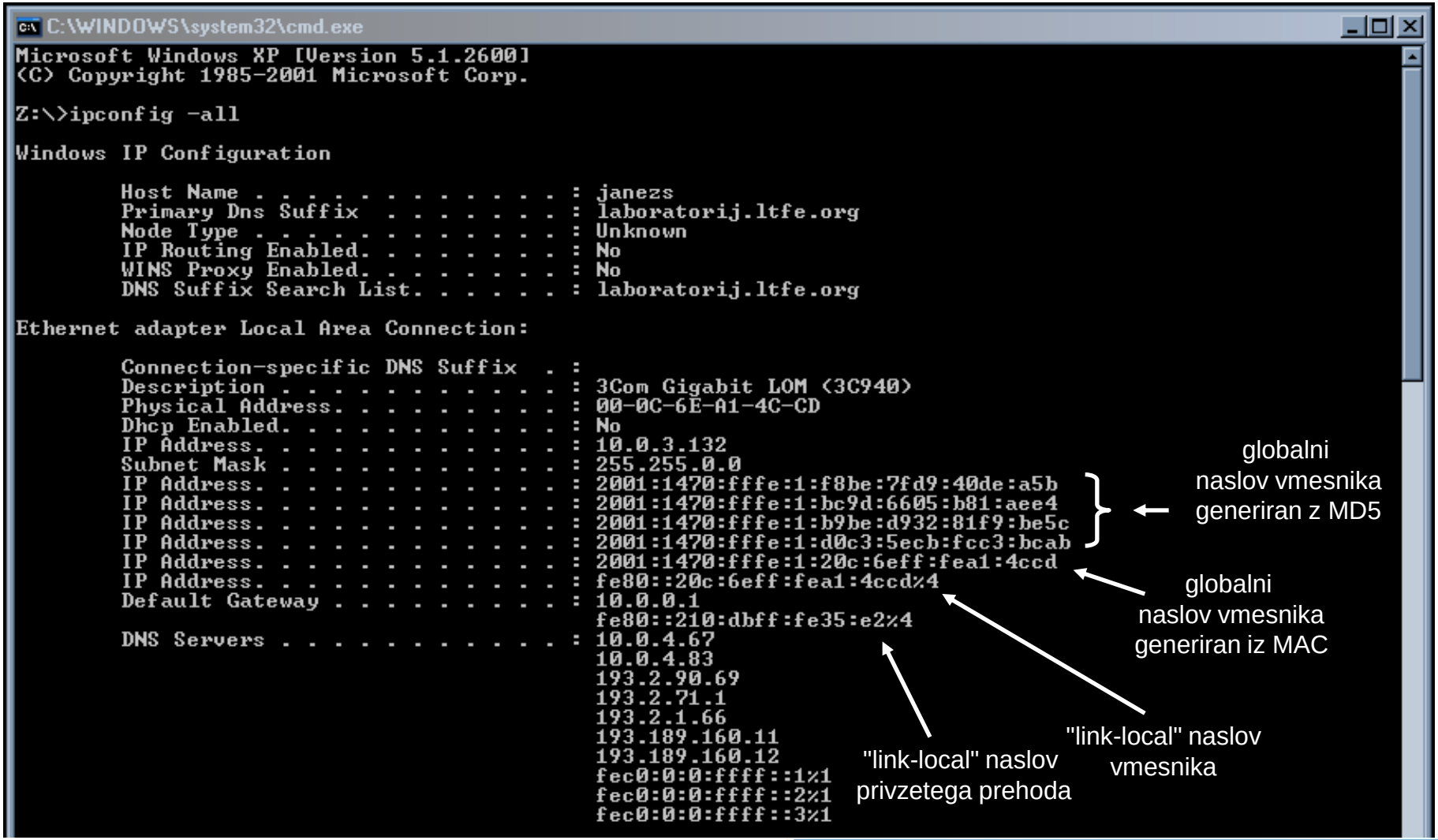


IPv6 & Microsoft 2/2

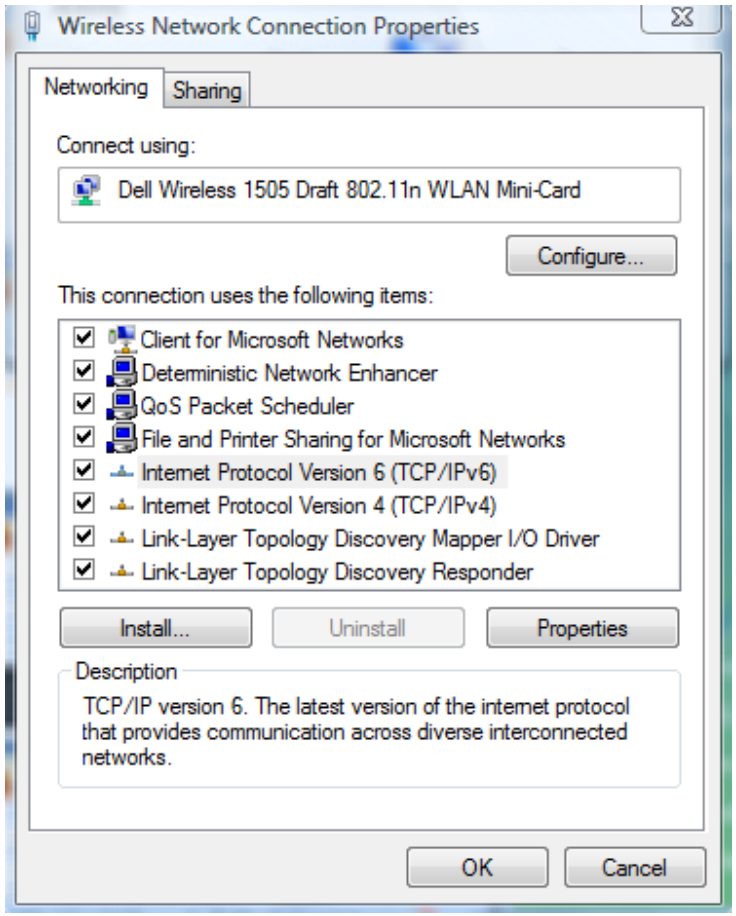
- Postopek konfiguracije IP v Vista, 7 & Server 2008
  - IPv6
    - neighbor discovery
    - DHCPv6 (stateful autoconfiguration)
    - router advertisement (stateless autoconfiguration)
    - ISATAP
    - Teredo
    - preostali možni tuneli (opcijsko)
  - IPv4
- Nadgradnja
  - grafični vmesnik
    - XP, Server 2003 ➔ netsh interface …
  - LLMNR, LLTD
  - interface ID (link-local, global) generiran naključno (drugače kot XP!)
    - preprečuje skeniranje naslovov (poznamo proizvajalce mrežne opreme!)
    - algoritem MD5
  - povsem nov požarni zid

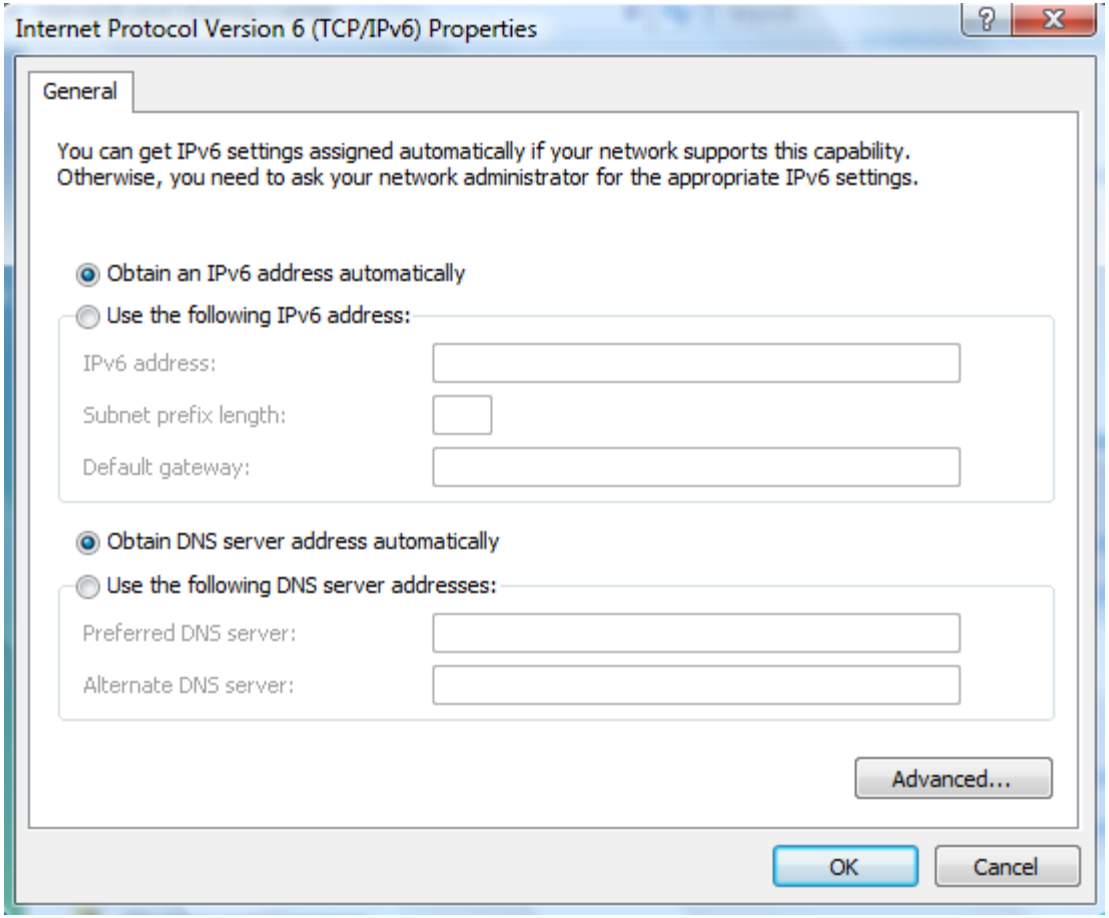
Preverjanje nastavitev IPv6 – WinXP

- ipconfig -all



Nastavitve IPv6 – Vista & 7



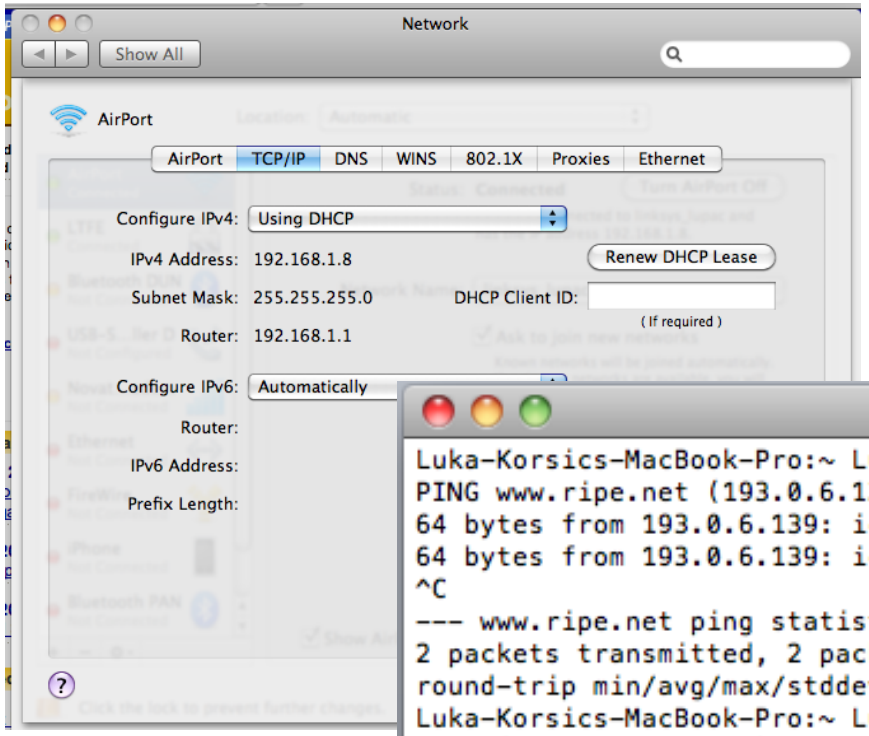


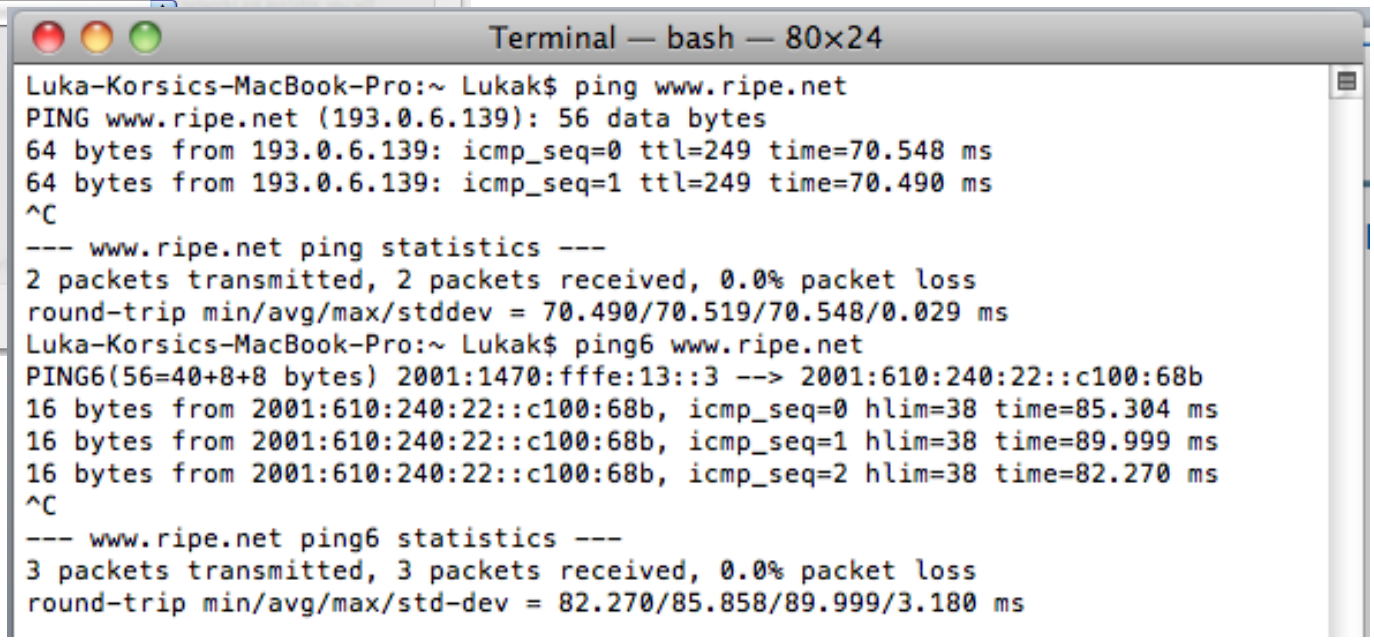
IPv6 & Linux

- Podporo omogoča večina različic
  - Red Hat
  - SUSE
  - Fedora
  - Ubuntu
- Primer nastavitev pri Ubuntu
  - autokonfiguracija omogočena pod privzetimi nastavitvami
  - /etc/network/interfaces
    - auto eth0
    - iface eth0 inet dhcp
    - iface eth0 inet6 (stateless autoconfiguration)
  - ali
    - iface eth0 inet 6 static
    - address 2001:6b0:e:2018::226
    - netmask 64
    - gateway 2001:6b0:e:2018::1

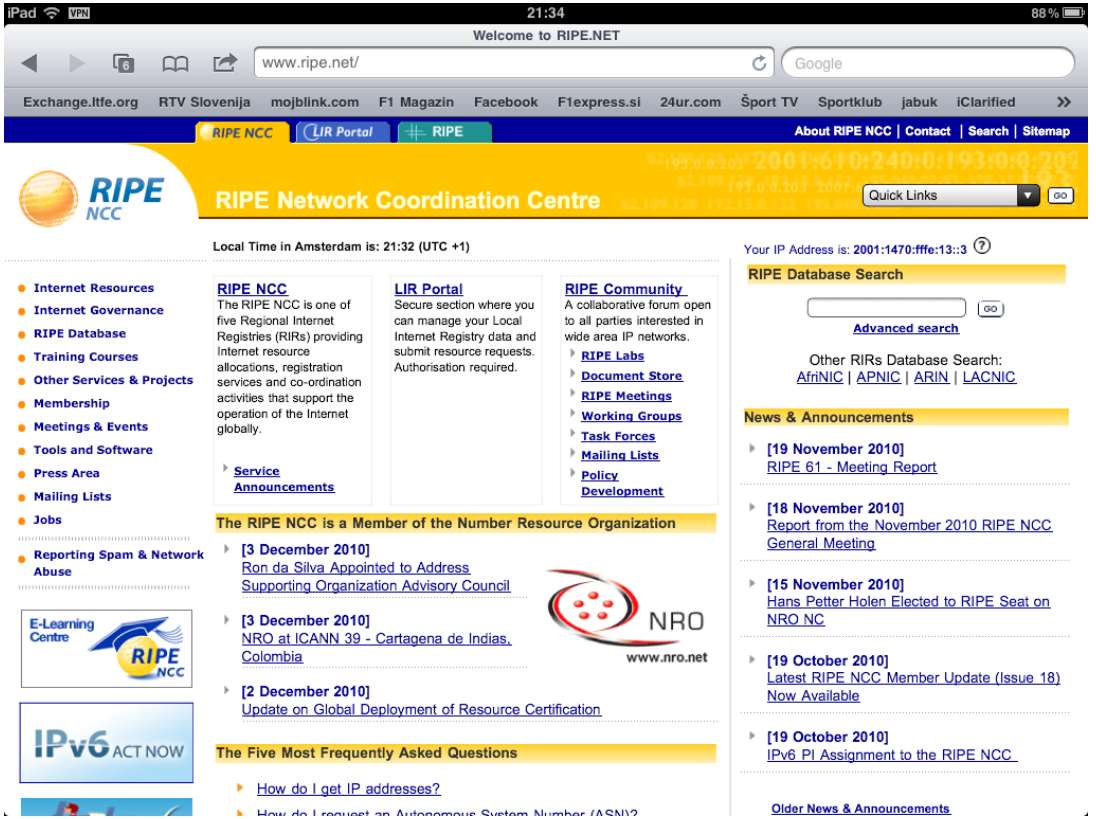
IPv6 & Mac OS

- Nameščen in omogočen IPv6 pod privzetimi nastavitvami





IPv6 na mobilnih napravah



Viri

- IETF
  - http://www.rfc-editor.org/rfc/rfc2460.txt
- 6DISS Tutorials
  - http://www.6diss.org/tutorials/index.html
- 6NET IPv6 deployment guide
  - http://www.6net.org/book/deployment-guide.pdf
- Microsoft tutorials
  - http://technet.microsoft.com/en-us/network/bb530961.aspx
- Cisco tutorials
  - www.cisco.com/go/ipv6
- Juniper tutorials
  - http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/Concepts13.html
- go6.si
  - http://ipv6.go6.si/2-slo-ipv6-summit/

Multicast

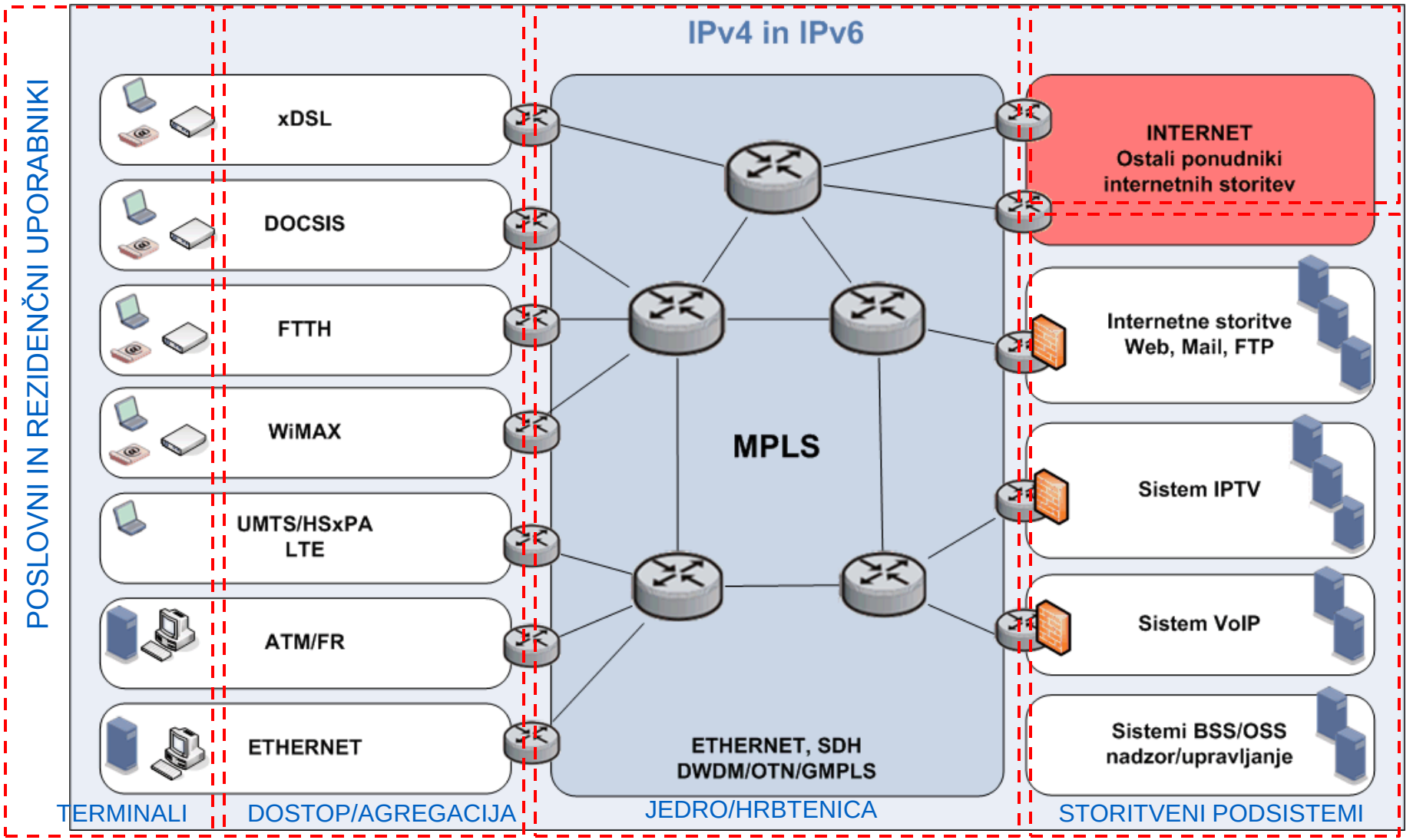
Univerza v Ljubljani
Fakulteta za elektrotehniko
Laboratorij za telekomunikacije

Ljubljana, april 2011

Vsebina

- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

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

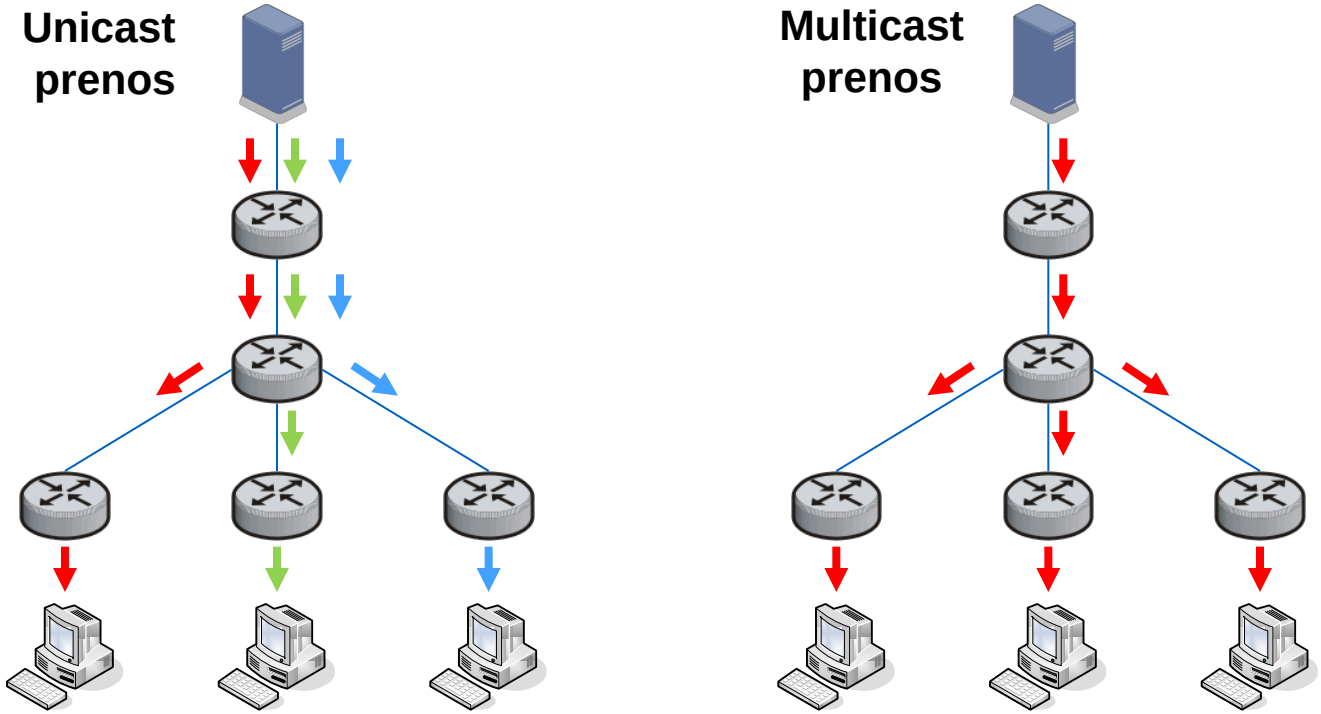
	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Kontrolna in upravljavska raven	Varnostne storitve	Zaščita podatkovne ravnine	Avtentikacija	-	IPSec, SSL,HMAC	IPSec, SSL, HMAC	-
			Nadzor dostopa	filtri ACL	IPSec, SSL, filtri ACL, Relay,	IPSec, SSL, filtri ACL, Relay,	filtri ACL
			Zasebnost/enkripcija	-	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

Uvod v multicast

- 1989
  - IGMPv1
- 1995
  - ustanovljen MBONE (Multicast backBONE)
  - veliko interesa za multicast s strani industrije in podjetij
- 1997 – 2000
  - ˝hype got ahead of technology˝
- 2000 – 2007
  - postavljeni realni temelji za multicast prek interneta
  - standardiziran PIM-SM
  - uveljavljati se je pričel Multicast BGP peering
  - multicast storitveni model se je razdelil
    - ASM – multipoint-to-multipoint
    - SSM – point-to-multipoint
  - ˝Killer app˝ za multicast
    - distribucija borznih informacij (NASDAQ, NYSE, NIKKEI, FTSE)
    - Triple Play – video (multicast), govor, podatki

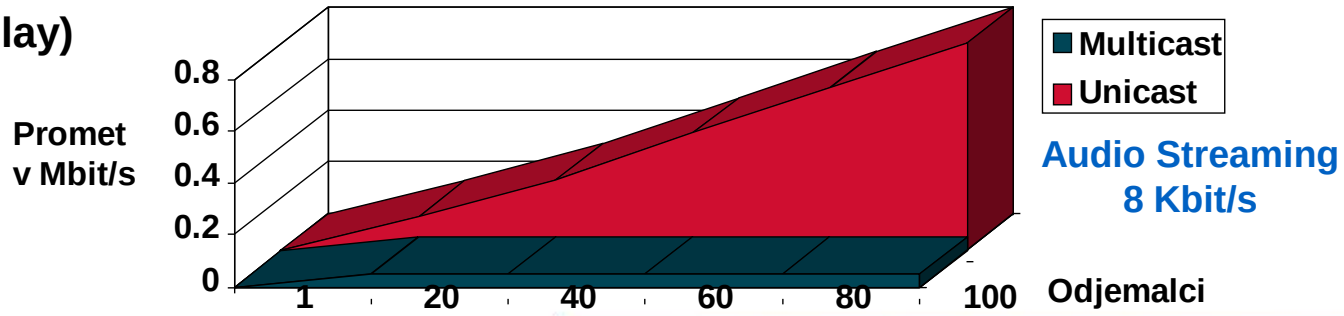
Primerjava unicast in multicast

- **Unicast prenosni način**
  - prenos enega podatkovnega toka enemu končnem odjemalcu
- **Multicast prenosni način**
  - simultan prenos enega podatkovnega toka skupini odjemalcev



Prednosti multicast

- **Zmanjša količino prometa**
  - zmanjšajo se obremenitve strežnikov
  - zmanjšajo se obremenitve omrežnih naprav
    - Unicast – število sej je ekvivalentno številu končnih uporabnikov
    - Multicast – število sej je ekvivalentno številu programov / storitev / aplikacij
- **Omogoča ˝multipoint˝ aplikacije**
  - prenos videa v živo (IPTV), prenos zvoka v živo (internetni radio)
    - BBC Radio, BBC Television
  - distribcija borznih informacij
    - NASDAQ, NYSE, NIKKEI, FTSE
    - IPTV (3Play)



Vsebina

- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

Osnovni koncepti IP

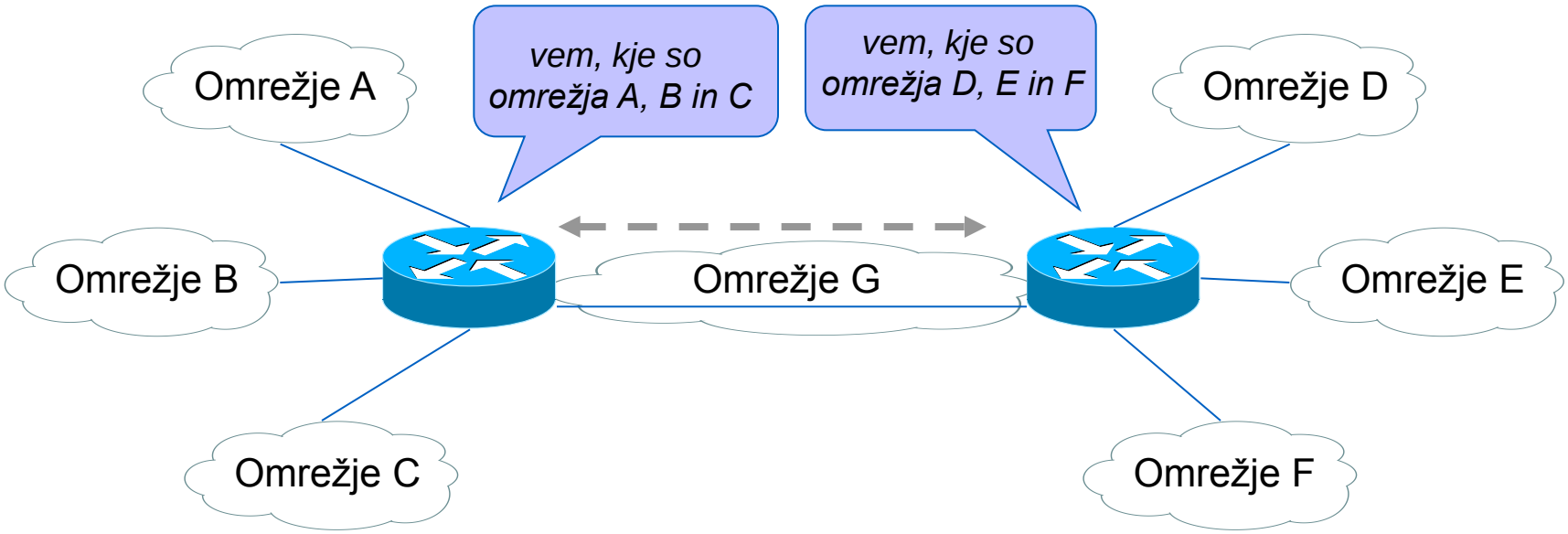
- Protokol IP
  - odprt storitveni model
    - vsak lahko komunicira z vsakim
    - za vse uporabnike se predvideva, da so legitimni
    - ni avtentikacije oddajnika in sprejemnika
      - brez preverjanja izvornih in ponornih naslovov
    - ni enkripcije prenosnega kanala
- Protokol UDP
  - nepovezavno usmerjen protokol
  - enak princip delovanja kot IP
- Protokol TCP
  - povezavno usmerjen protokol
  - vzpostavitev zveze

Lastnosti protokola IP

- Nepovezavno usmerjena tehnologija omrežnega (L3) sloja
  - vsak paket v glavi nosi izvorni in ciljni naslov IP
- Vročitve naslovniku ne zagotavlja
  - to prepušča višjim slojem (npr. TCP)
- Usmerjanje / posredovanje se za vsak paket izvrši v vsakem vozlišču posebej
  - neodvisno od ostalih paketov istega podatkovnega toka
- Usmerjevalni podatki so shranjeni v usmerjevalni tabeli
- Usmerjevalna tabela se lahko zgradi
  - statično – "na roke"
  - dinamično – na osnovi usmerjevalnih protokolov
    - unicast – RIP, OSPF, IS-IS, MP-BGP
    - multicast – PIM (SM/SSM), MP-BGP

Kaj je usmerjanje?

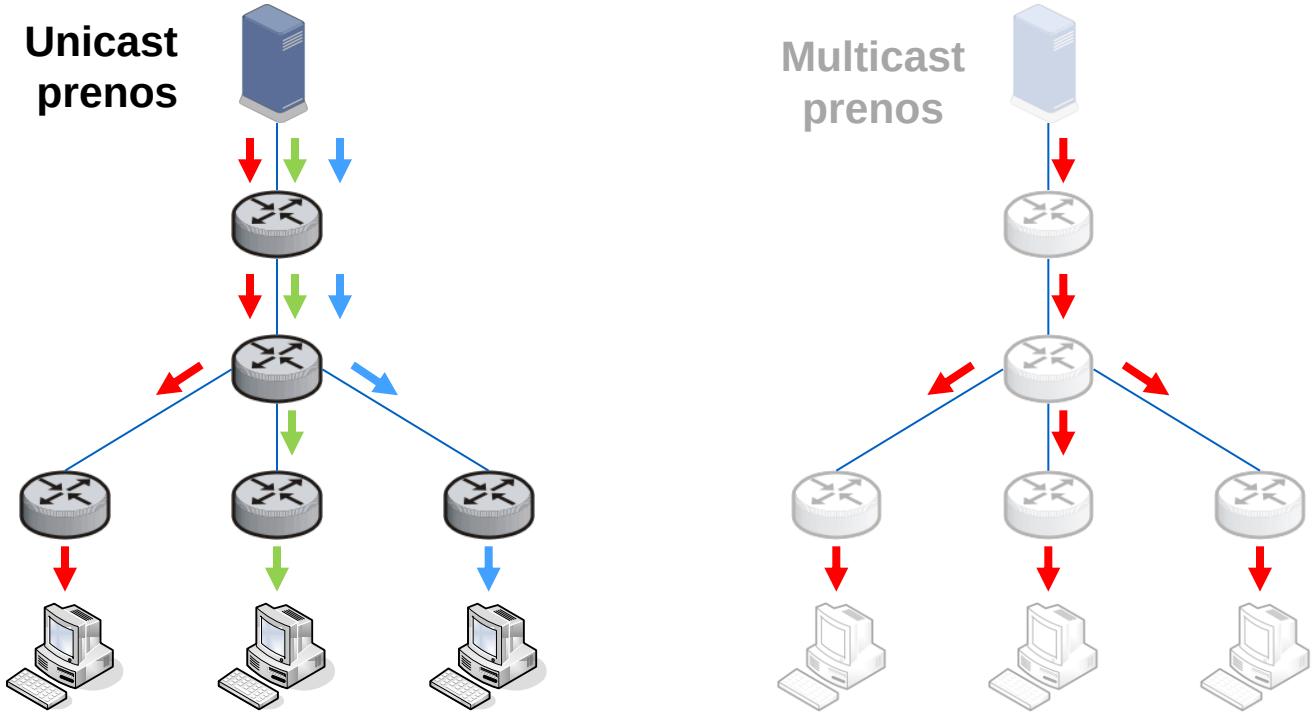
- Izmenjava informacij o dosegljivosti
- Določitev optimalne poti



Unicast prenosni način

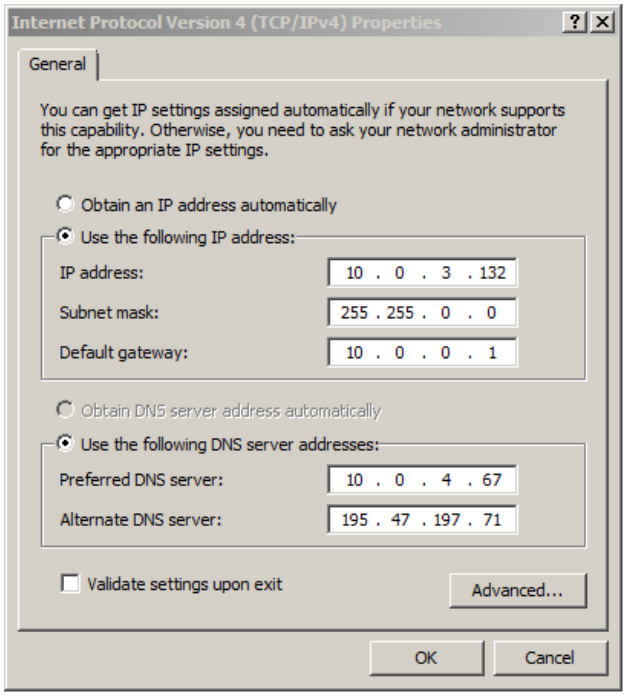
Unicast prenosni način

- **Unicast prenosni način**
  - **prenos enega podatkovnega toka enemu končnem odjemalcu**
- **Multicast prenosni način**
  - **simultan prenos enega podatkovnega toka skupini odjemalcev**



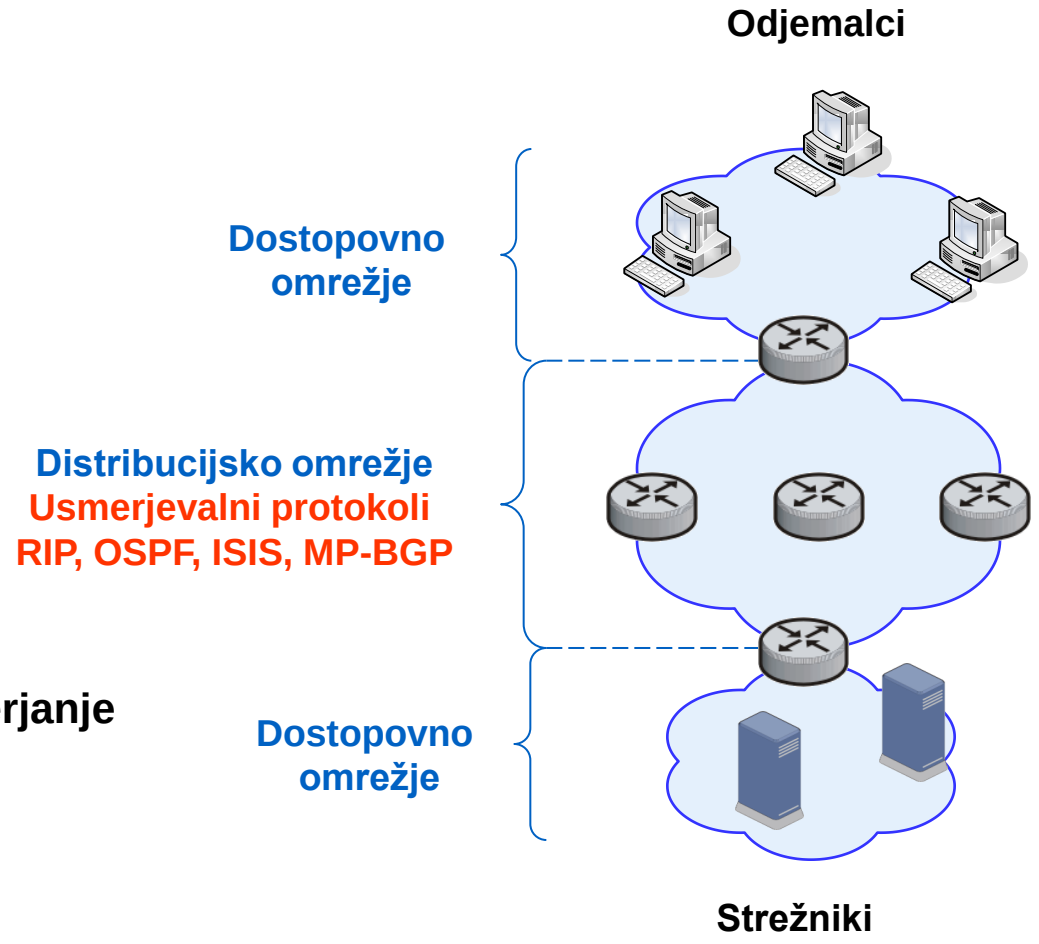
Unicast naslavljanje

- Naslavljanje je dvonivojsko – 32 bitno število
  - identifikator omrežja (angl. network ID)
  - naslov naprave (angl. host ID)
  - mejo med omrežnim delom naslova in biti za naslavljanje naprav določa maska
- Maska – 32 bitno število
  - 1: omrežni del
  - 0: del za naprave
- Primer zapisa naslova na odjemalcu
  - IP = 10.0.3.132
  - Maska = 255.255.0.0
  - DG = 10.0.0.1



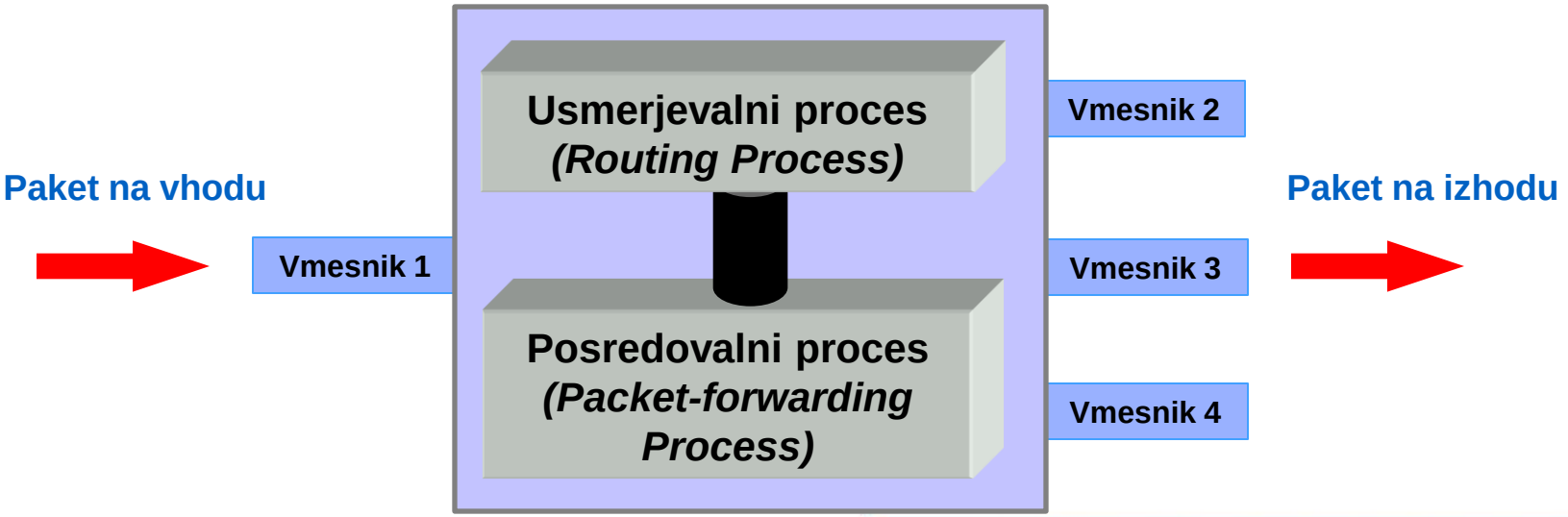
Unicast prenosni način – komponente

- Podpora za prenos paketov IP – omrežne nastavitve
  - odjemalci
    - naslov IP
    - maska
    - privzeti prehod
  - strežniki
    - naslov IP
    - maska
    - privzeti prehod
  - usmerjevalniki
    - na vsakem vmesniku
      - naslov IP
      - maska
    - podpora za unicast usmerjanje



Zgradba usmerjevalnega sistema

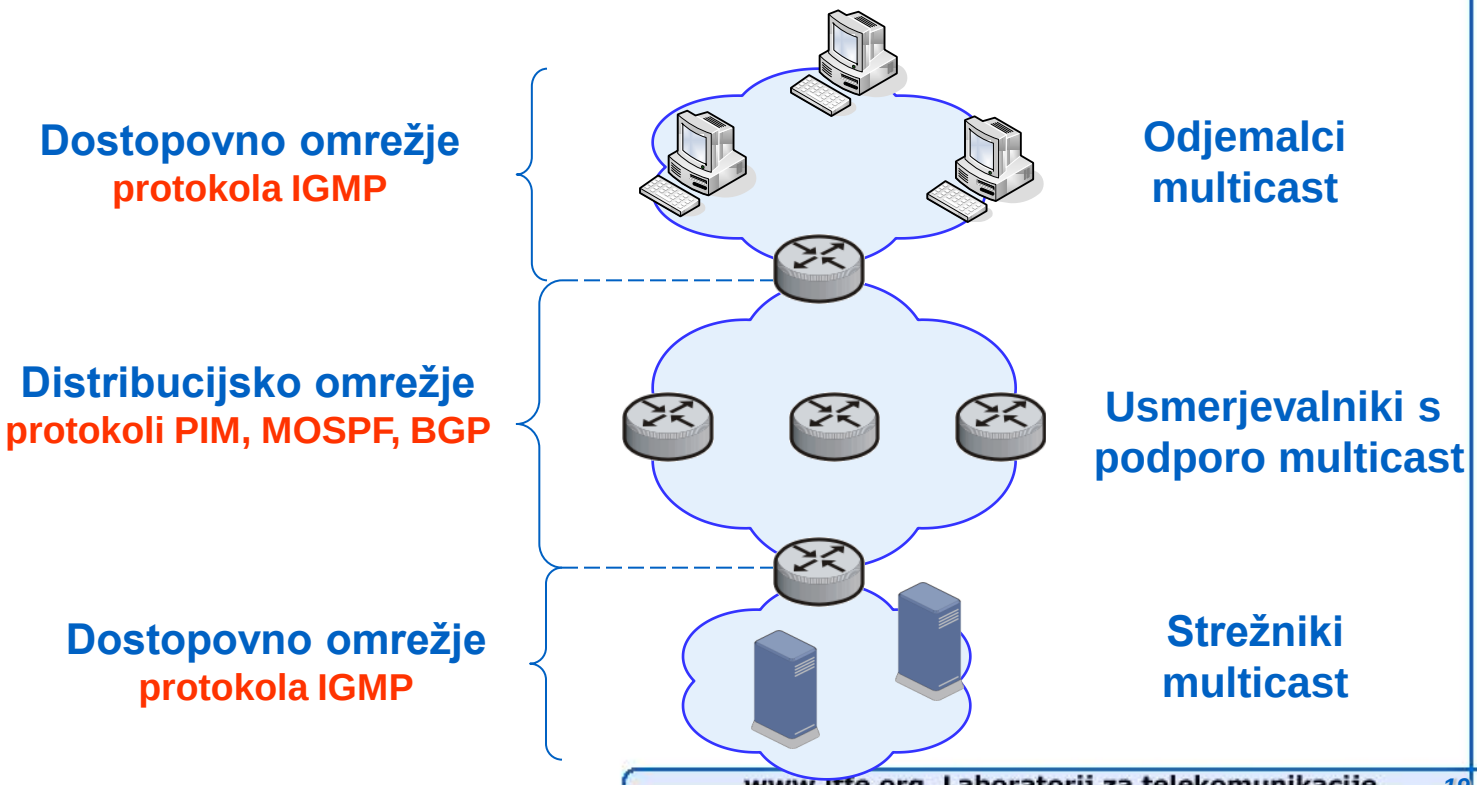
- **Usmerjevalni proces**
  - izmenjava usmerjevalnih informacij
  - določitev optimalne poti
  - izvaja se lahko v nerealnem času
- **Posredovalni proces**
  - Izbira ustreznega vmesnika “angl. longest-prefix-mach”
  - posredovanje paketov na izhodni vmesnik
  - izvajati se mora v realnem času



Multicast prenosni način

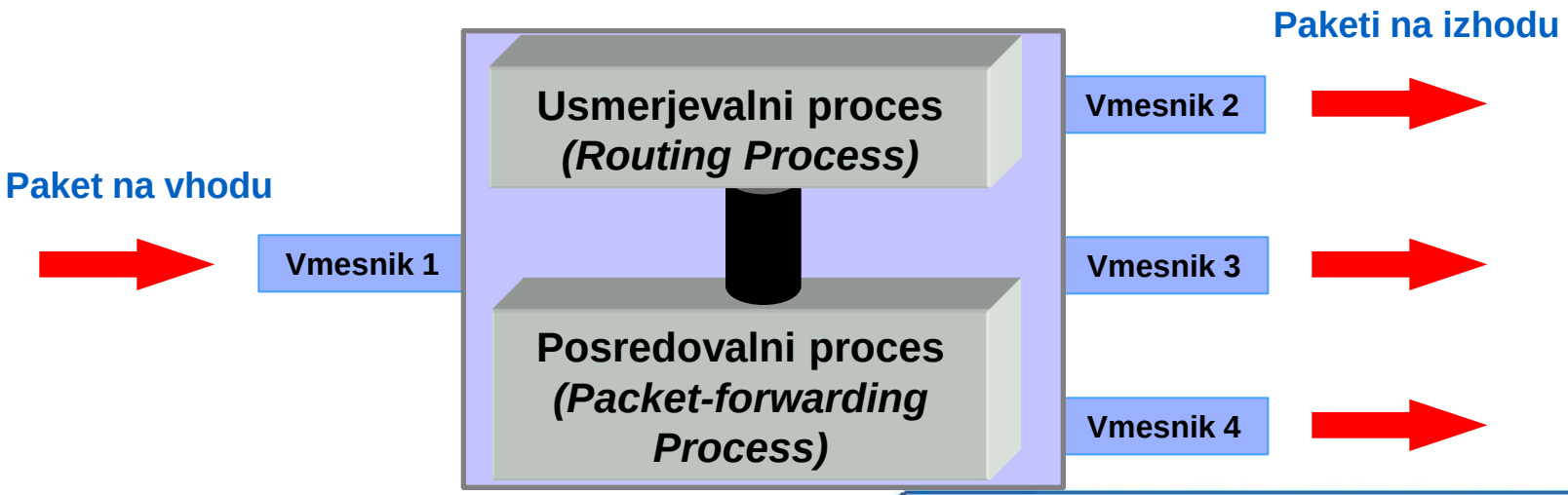
Multicast prenosni način - komponente

- Komunikacija med robnimi usmerjevalniki in odjemalci
  - protokol IGMP (IPv4)
- Komunikacija med jedrnimi usmerjevalniki
  - PIM-DM, PIM-SM, PIM-SSM, MOSPF, BGP



Multicast na usmerjevalniku

- **Unicast prenosni način**
  - kontrolna ravnina – unicast usmerjanje (RIP, OSPF, ISIS, MP-BGP)
  - podatkovna ravnina – unicast posredovanje paketov
- **Za multicast potrebujemo delujoč unicast prenosni način ter dodatne razširitev!**
  - kontrolna ravnina – multicast usmerjanje (PIM-SM/SSM)
  - podatkovna ravnina – multicast posredovanje paketov



Značilnosti multicast

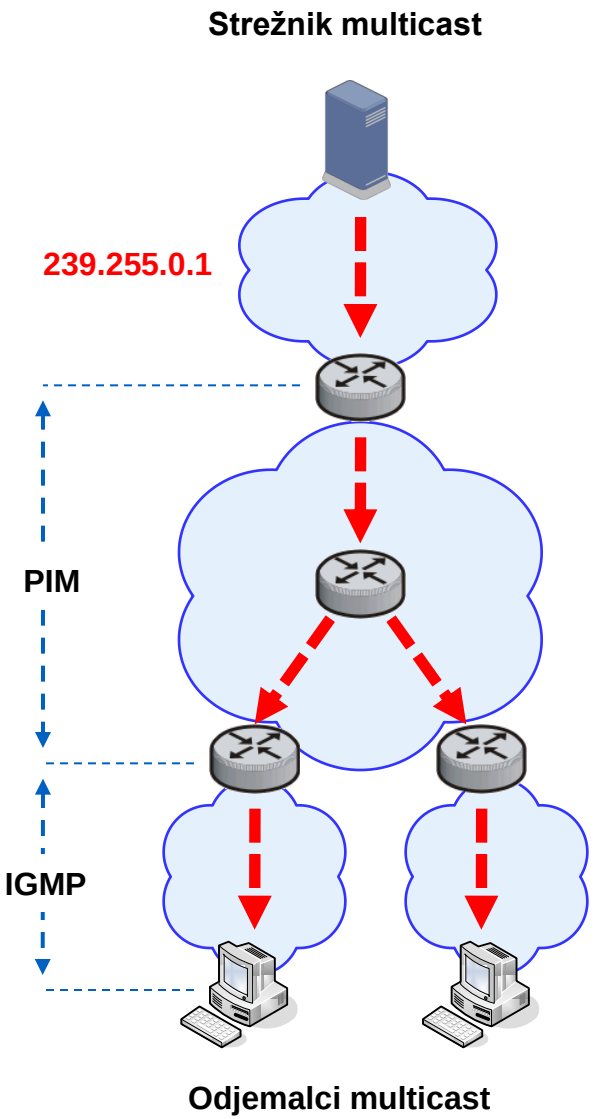
- Multicast aplikacije delujejo po principu nepovezavnih sistemov
  - za transport se uporablja protokol UDP
  - ne zagotavlja zanesljive dostave datagramov
  - ne vsebuje mehanizmov za kontrolo zamašitev v omrežju
- Posamezni datagrami lahko prihajajo v nepravilnem vrstnem redu
- Tehnologija multicast nima lastnih varnostnih mehanizmov
  - vsaka naprava lahko prične oddajat v določeno multicast skupino
  - vsaka naprava se lahko prijavi v multicast skupino

Klasičen storitveni model multicast

- Model ASM (Any Source Multicast)
  - temelji na odprtem storitvenem modelu
  - vsak terminal je lahko sprejemnik in/ali oddajnik za določeno multicast skupino oziroma multicast kanal
- Multicast skupina oz. grupa (Multicast Group)
  - skupina uporabnikov, ki sprejemajo promet na določenem multicast naslovu
  - določena je z multicast skupinskim naslovom
    - notacija (*,G)
- Prijavljanje in odjavljanje odjemalcev v multicast skupino poteka s protokolom IGMP
- Model ASM je prilagojen za aplikacije tipa ˝multipoint-to-multipoint˝
  - obstaja lahko več izvorov multicast prometa za isto multicast skupino

Koncept delovanja ASM

- Multicast strežnik oddaja podatkovni tok (datagrame IP) v izbrano multicast skupino
  - oddajnik ne ve, kdo so multicast sprejemniki ter njihovega števila
  - oddajniku ni potrebno biti prijavljen v multicast skupino, v katero oddaja podatkovni tok
  - oddajnikov v eno multicast skupino je lahko več
    - ˝multipoint-to-multipoint˝ aplikacije – (video konferenca)
- Odjemalci (terminal, PC, STB) se lahko dinamično prijavljajo in odjavljajo v multicast skupino
  - neodvisno od lokacije
  - neodvisno od njihovega števila

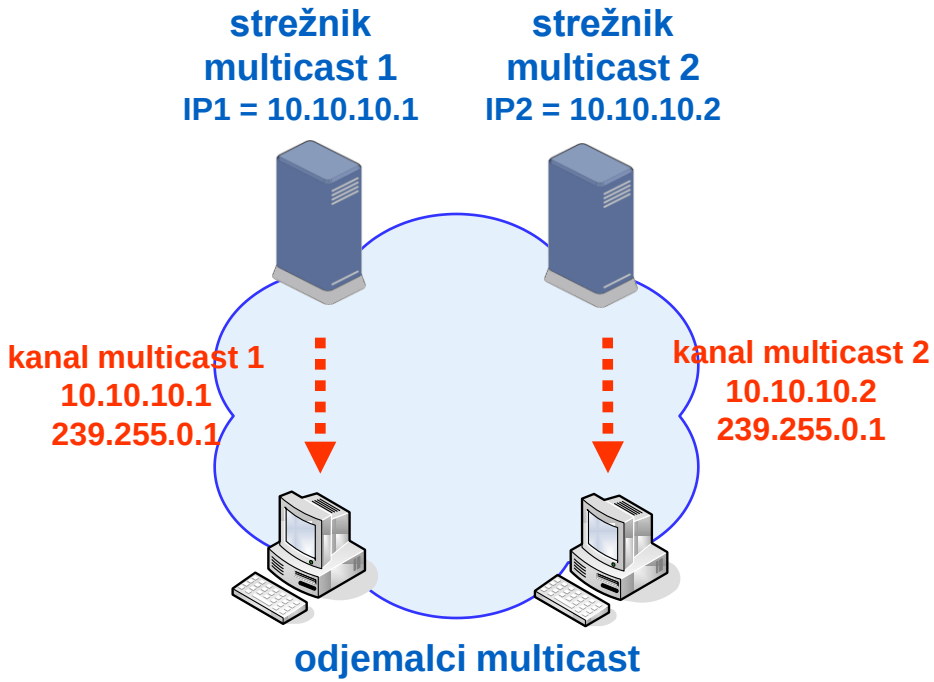


Storitveni model SSM

- SSM – Source Specific Multicast
- Multicast kanal je določen s ponornim multicast naslovom ter izvornim unicast naslovom oddajnika
  - notacija (S,G)
- Prilagojen je za aplikacije tipa ˝point-to-multipoint˝
  - en izvor multicast prometa za izbrano multicast skupino
  - internetna televizija, internetni radio
  - 3Play – IPTV
- Potrebni protokoli
  - “predelava PIM-SM” za Source Specific Multicast (PIM-SSM)
  - protokol IGMP

Koncept delovanja SSM

- Prijava odjemalca v multicast skupino
  - multicast naslova in unicast naslov multicast strežnika
- Vsak multicast kanal SSM ima
  - natanko en izvor multicast prometa
  - poljubno mnogo multicast odjemalcev
- Tipična uporaba
  - 3Play – IPTV



Vsebina

- Uvod
- Osnovni koncepti
- **Multicast naslavljanje**
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

Multicast naslavljanje 1/2

- Multicast skupinski naslovi
  - določajo skupino multicast odjemalcev
  - rezerviran blok naslovov IP ˝razred D”
    - 224.0.0.0 – 239.255.255.255
  - odjemalcem se dodeljujejo dinamično
    - protokol IGMP
- Delitev multicast naslovnega prostora
  - rezervirani lokalni in globalni naslovi
  - globalni naslovi, ki se uporabljajo v javnih omrežjih IP
  - privatni naslovi, ki se uporabljajo znotraj zasebnih domen
- Natančna razdelitev multicast naslovnega prostora
  - http://www.iana.org/assignments/multicast-addresses

Multicast naslavljanje 2/2

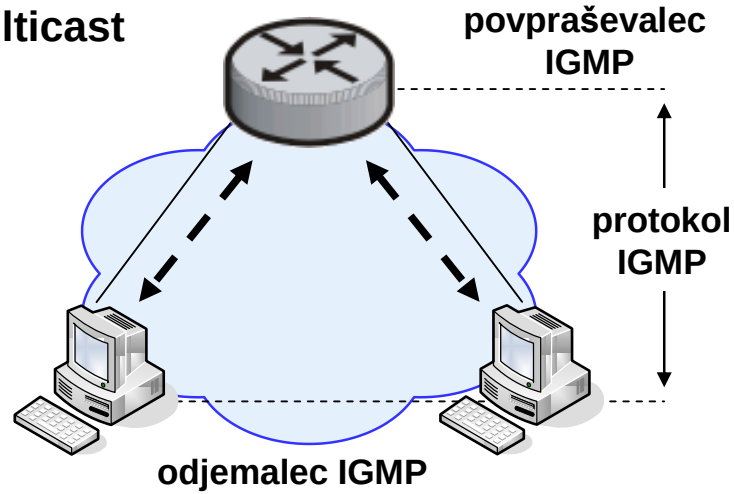
- Rezervirani naslovi
  - rezervirani lokalni ˝Link-local Control Block˝
    - 224.0.0.0 – 224.0.0.255
    - oddani s TTL = 1
      - 224.0.0.1 naslavljanje vseh multicast naprav
      - 224.0.0.2 naslavljanje vseh multicast usmerjevalnikov
      - 224.0.0.5 naslavljanje usmerjevalnikov OSPF
  - rezervirani globalni ˝Internetwork Control Block˝
    - 224.0.1.0 – 224.0.1.255
    - npr. za protokol NTP 224.0.1.1
- Globalni naslovi
  - 224.0.2.0 – 238.255.255.255
  - rezervirani naslovi za model SSM 232.0.0.0 – 232.255.255.255
- Privatni multicast naslovi
  - 239.0.0.0 – 239.255.255.255
  - podobno kot unicast privatni naslovi (RFC 1918)

Vsebina

- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- **Protokol IGMP**
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

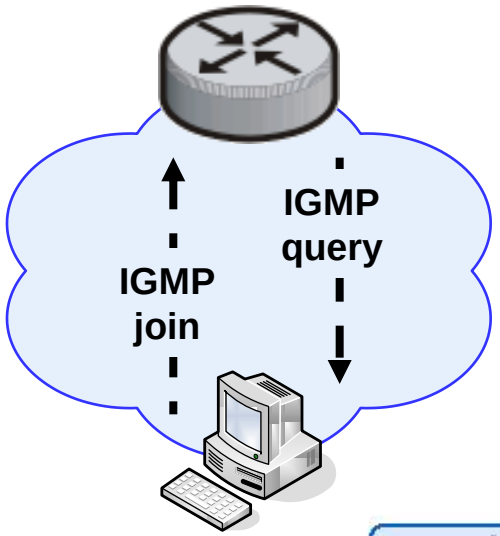
Protokol IGMP

- **Signalizacija med multicast odjemalci in robnimi usmerjevalniki**
  - multicast odjemalcem omogoča dinamično prijavljanje in odjavljanje v multicast skupino – sporočila join/leave
  - IGMP sporočila se prenašajo neposredno v datagramih IP
- **Komponente protokola IGMP**
  - odjemalec IGMP
    - funkcija na napravah (STB, PC, ostali terminali), ki so prejemniki multicast podatkovnega toka
  - querier IGMP
    - funkcija na robnem usmerjevalniku multicast
- **Verzije protokola IGMP**
  - IGMPv1 (RFC 1112)
    - podprt v Windows 95, STB
  - IGMPv2 (RFC 2236)
    - podprt v Windows NT, 98, ME, STB
    - trenutno najbolj razširjen
  - IGMPv3 (RFC 3376)
    - podprt v Windows XP, Server 2003, UNIX, Linux



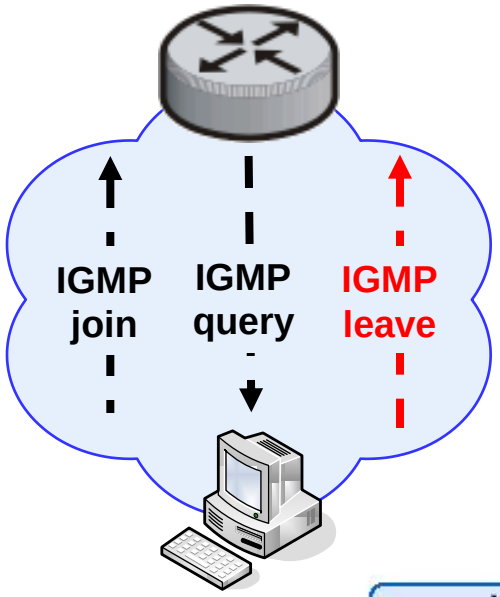
Protokola IGMPv1 in IGMPv2

- Koncept delovanja je v osnovi enak za oba protokola
  - sporočilo ˝host membership report˝ – uporabljajo odjemalci
    - zahteva za vključitev odjemalca v skupino/kanal multicast
    - odgovor na zahtevo po preverjanju stanja trenutnih odjemalcev multicast
  - sporočilo ˝host membership query˝ – uporablja usmerjevalnik
    - preverjanje stanja odjemalcev v multicast skupini
    - IGMPv1 omogoča preverjanje stanja vseh multicast skupin na določenem segmentu IP
    - IGMPv2 omogoča tudi eksplicitno preverjanje stanja specifične multicast skupine



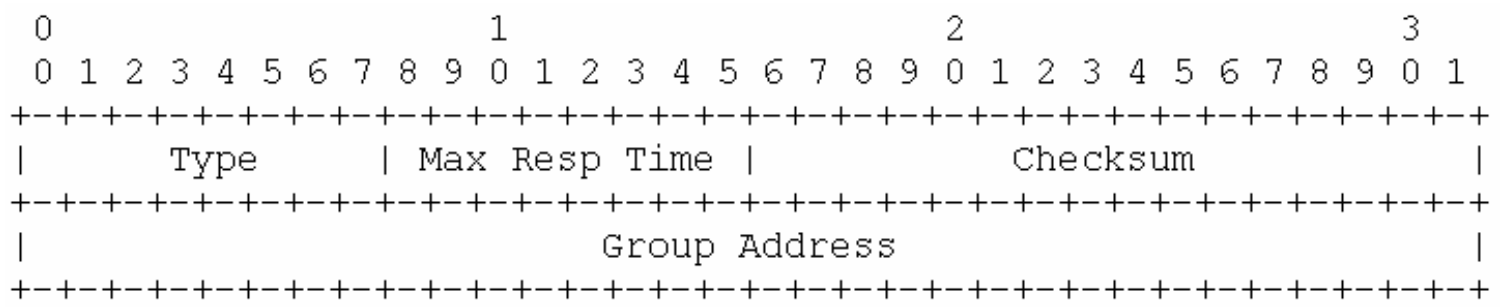
Protokola IGMPv1 in IGMPv2 – odjava

- Odjavljanje odjemalcev iz multicast skupine
  - IGMPv1 – odjavljanje temelji na konceptu periodičnega preverja stanja odjemalcev, ki so prijavljeni v multicast skupino
    - usmerjevalnik pošilja sporočila ˝host membership query˝
    - če ne dobi odgovora, po preteku časovne kontrole (tipično ~3 minute), preneha pošiljati multicast podatkovni
  - IGMPv2 – omogoča neposredno odjavo iz skupine multicast
    - odjemalec pošlje sporočilo ˝leave group˝



Format sporočila IGMPv2 1/2

- **Določeni so trije tipi sporočil ˝Type˝**
  - ***˝Membership Query˝***
    - ***General Membership Query* – preverjanje stanja vseh multicast skupin na določenem segmentu IP**
    - ***Group-Specific Membership Query* – preverjanje stanja specifične multicast skupine na segmentu IP**
  - ***˝Membership Report˝***
    - **zahteva za vključitev uporabnika v multicast skupino**
    - **odgovor na zahtevo po preverjanju stanja trenutno aktivnih odjemalcev v skupini multicast**
  - ***˝Leave Group˝***
    - **neposredna odjava odjemalca iz skupine multicast**



Format sporočila IGMPv2 2/2

- Polje ˝Max Response Time˝
  - pomen ima le v primeru sporočil ˝Membership Query˝
  - določa interval (maksimalen dovoljen čas) v katerem morajo odjemalci odgovoriti na sporočilo – privzeta nastavitev je 10 s
  - odjemalec izbere naključen čas znotraj določenega intervala
- Polje ˝Checksum˝
  - za zagotavljanje integritete sprejetih sporočil
- Polje ˝ Group Address˝
  - prenaša naslov multicast skupine
  - v primeru sporočila ˝Membership Report˝ oz. ˝Leave Group˝ se prenaša naslov skupine multicast v katero se odjemalec prijavlja oz. odjavlja
  - v primeru sporočila ˝General Membership Query˝ je vrednost polja postavljena na nič
  - v primeru sporočila ˝Specific Membership Query˝ se v polju prenaša naslov multicast skupine, na katero se sporočilo nanaša

Protokol IGMPv3

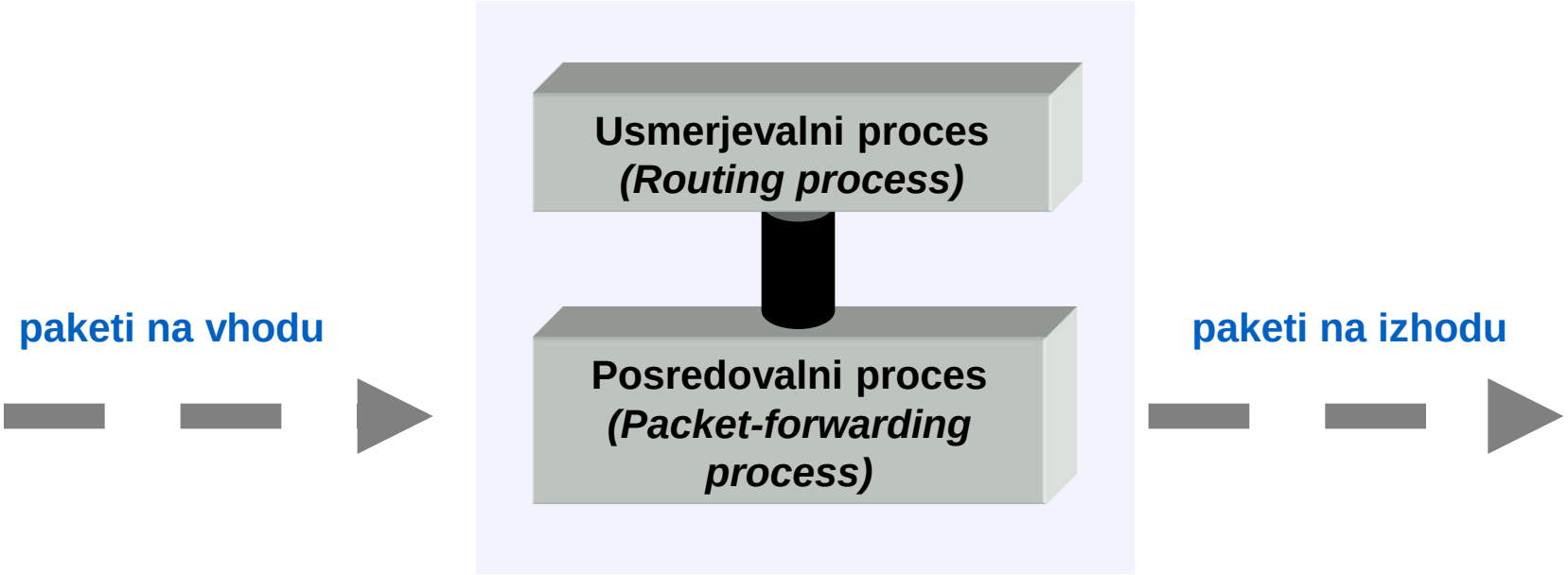
- Ključna novost, ki jo uvaja protokol IGMPv3 je možnost neposredne izbire izvora multicast prometa, ki oddaja v izbrano multicast grupo
- Odjemalci se lahko prijavljajo v multicast grupo na dva načina
  - ˝include mode˝ – odjemalec eksplicitno določi multicast strežnike od katerih bo sprejemal multicast podatkovni tok
  - ˝exclude mode˝ – odjemalec določi oddajnike od katerih ne bo sprejemal multicast podatkovnega toka
- Standard določa dva tipa sporočil IGMPv3
  - sporočilo ˝Membership Query˝
    - sporočila, ki jih uporabljajo multicast usmerjevalniki
  - sporočilo ˝Membership Report˝
    - sporočila, ki jih uporabljajo multicast odjemalci

Vsebina

- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- **Multicast usmerjanje**
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

Multicast na usmerjevalniku

- **Unicast prenosni način**
  - **kontrolna ravnina – unicast usmerjanje (RIP, OSPF, ISIS, BGP)**
  - **podakovna ravnina – unicast posredovanje paketov**
- **Za multicast potrebujemo delujoč unicast prenosni način ter dodatne razširitev**
  - **kontrolna ravnina – multicast usmerjanje (PIM-SM/DM)**
  - **podatkovna ravnina – multicast posredovanje paketov**

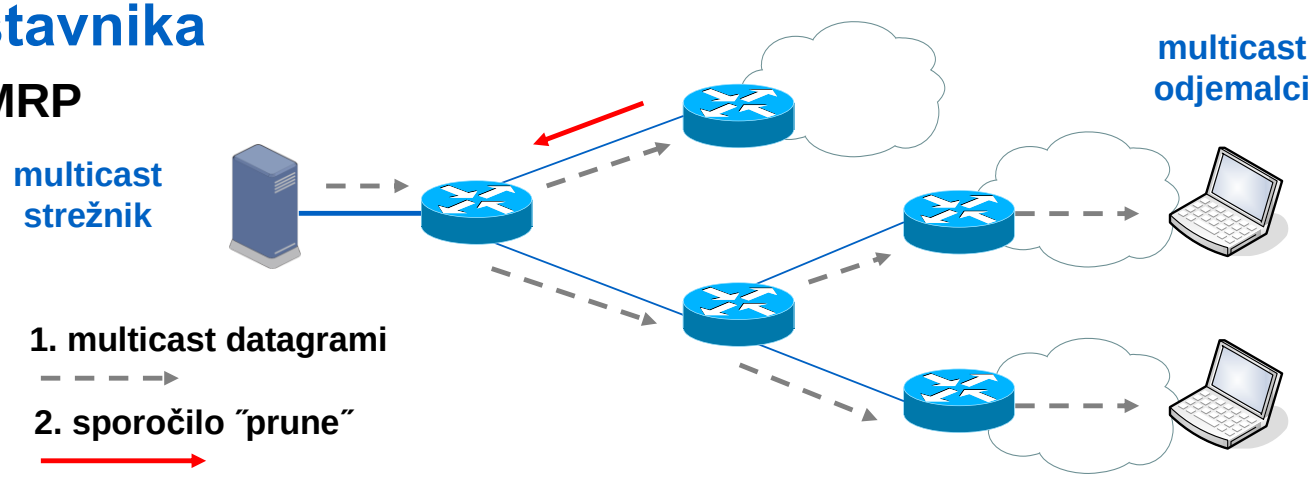


Multicast usmerjanje

- Multicast usmerjevalni protokoli
  - danes najbolj uporabljani
    - PIM-SM (Protocol Independent Multicast – Sparse Mode)
    - PIM-DM (Protocol Independent Multicast – Dense Mode)
    - DVMRP (Distance Vector Multicast Routing Protocol)
  - ostali BIDIR-PIM (BiDirectional PIM), MOSPF (Multicast Extensions for OSPF), CBT (Core Based Trees)
- Delitev multicast usmerjevalnih protokolov glede na
  - način delovanja
    - razpršeni način ˝sparse mode˝ (opt-in)
    - zgoščeni način ˝dense mode˝ (opt-out)
  - tip zgrajenega posredovalnega drevesa
    - uporaba izvornega drevesa (source based tree)
    - uporaba deljenega drevesa (shared based tree)
  - način določitve vrhnjega (upstream) usmerjevalnika
    - mehanizem RPF (Reverse Path Forwarding)
  - stopnjo interakcije, ki je potrebna s podatkovno ravnino

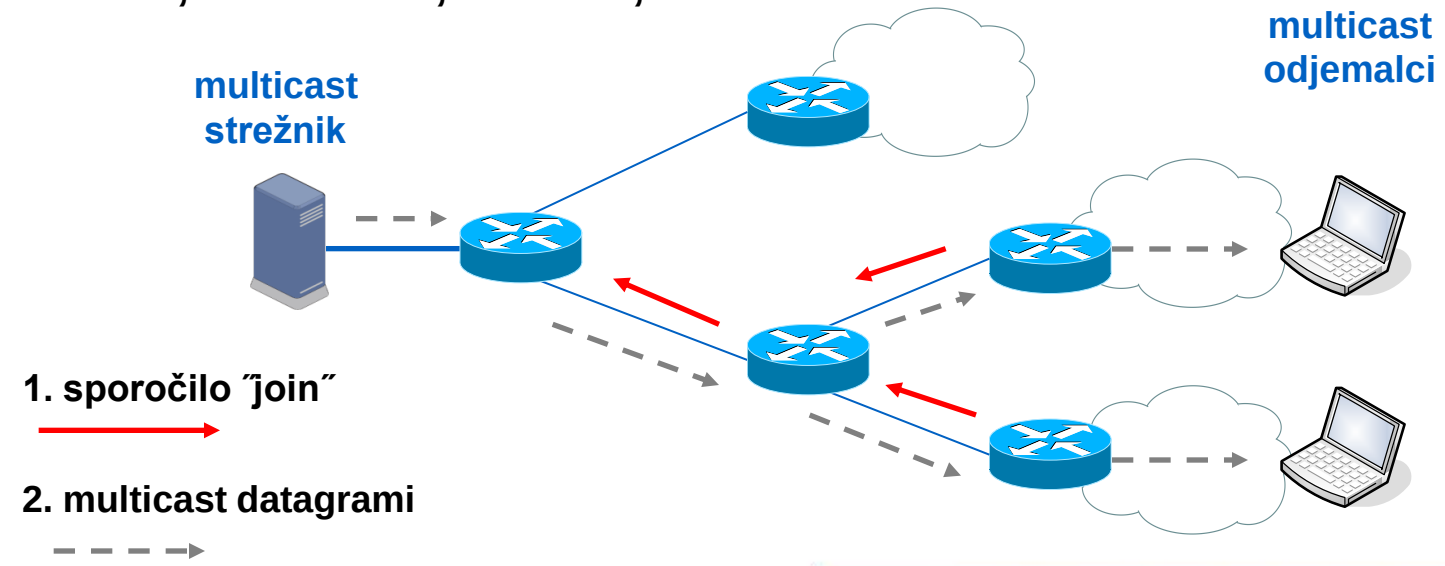
Zgoščeni način ˝dense mode˝

- Princip delovanja ˝dense mode˝
  - uporablja agresivni način “Push model˝
    - multicast promet (datagrami) se poplavlja do vseh robnih usmerjevalnikov – operacija ˝flood˝
    - usmerjevalniki, ki ne želijo sprejemat multicast prometa (nimajo aktivnih multicast odjemalcev) pošljejo sporočilo ˝prune˝
    - operaciji ˝flood & prune˝ (tipično vsake 3 min)
    - omogoča hitro distribucijo multicast vsebine
- Primeren za omrežja, kjer so multicast odjemalci koncentrirani
- Tipična predstavnika
  - PIM-DM, DVMRP



Razpršeni način ˝sparse mode˝

- Princip delovanja ˝sparse-mode˝
  - multicast sprejemniki so razpršeni po omrežju
    - poplavljanje multicast prometa skozi celotno omrežje ni zaželjeno
  - uporablja se model ˝Pull˝
    - multicast promet (datagrami) se posreduje le tistim usmerjevalnikom, ki ga eksplicitno zahtevajo – počasnejša odzivnost aplikacij
    - usmerjevalnik svojemu vrhnjemu usmerjevalniku pošlje sporočilo ˝join˝
- Tipični predstavniki
  - PIM-SM, BIDIR-PIM, MOSPF, CBT



Kontrolna & podatkovna ravnina

- **Kontrolna ravnina**
  - unicast usmerjevalni protokoli RIP, OSPF, ISIS, BGP
  - multicast usmerjevalni protokoli PIM-SM, PIM-DM
- **Podatkovna ravnina**
  - unicast in multicast posredovanje datagramov IP
- **Unicast usmerjevalna/posredovalna tabela se zgradi na osnovi izmenjanih kontrolnih sporočil (RIP, OSPF, ISIS)**
  - neposredna interakcija s podatkovno ravnino ni potrebna
- **Multicast usmerjevalna/posredovalna tabela se zgradi na osnovi izmenjanih kontrolnih sporočil (PIM-SM, PIM-DM) ter v povezavi s podatkovno ravnino**
  - potrebna je interakcija med kontrolno in podatkovno ravnino

Protokoli PIM-DM, PIM-SM

Protokoli PIM

- Skupina multicast usmerjevalnih protokolov
  - PIM-SM
    - trenutno najbolj razširjen
    - deluje v načinu ″sparse-mode″
    - uporablja lahko ″shared″ in ″source based tree″
  - PIM-DM
    - deluje v načinu ″dense-mode″
    - uporablja ″source based tree″
  - BIDIR-PIM
    - temelji na PIM-SM
    - manj razširjen
- Skupne lastnosti
  - enak format kontrolnih sporočil
  - neodvisni od uporabljenih unicast usmerjevalnih protokolov
    - statične poti, RIP, IGRP, EIGRP, IS-IS, OSPF in BGP
- PIM-SM in PIM-DM se lahko uporabljata skupaj v eni multicast domeni
  - PIM v načinu ″sparse-dense mode″

Vsebina

- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- **Ethernet multicast**
- Varnost v multicast
- Uporaba multicast

Multicast prenos na Ethernet napravah

- Klasične Ethernet komutacijske naprave obravnavajo multicast prometa na enak način kot broadcast promet
  - multicast podatkovni tok razpošlje na vse aktivne izhodne vmesnike
  - velika obremenitev Ethernet segmenta
- Mehanizem ˝IGMP snooping˝ omogoča Ethernet komutacijskim napravam dinamično preverjanje, na katerih vmesnikih se nahajajo multicast oddajniki in odjemalci
  - temelji na preverjanju poslanih sporočil IGMP (˝join˝, ˝leave˝)
  - sporočila IGMP se prenašajo v IP datagramih

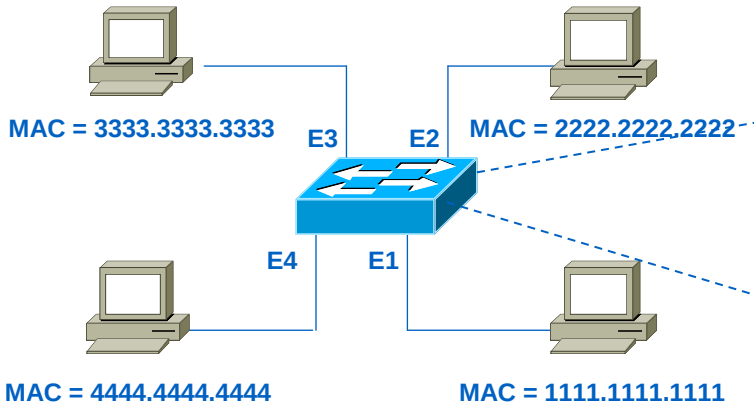


tabela MAC

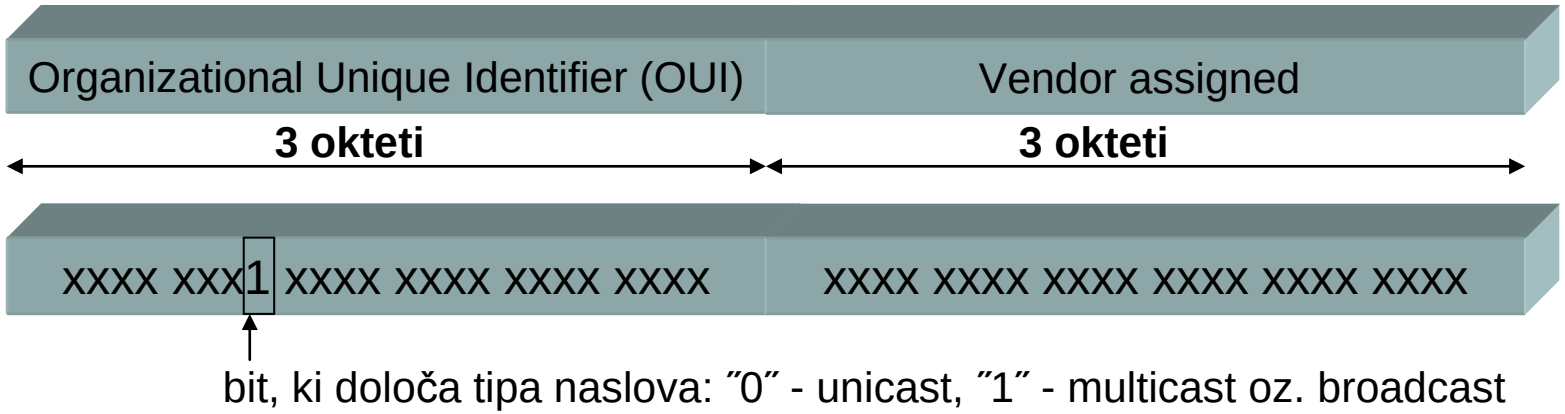
ciljni naslov MAC	izhodni vmesnik
1111.1111.1111	E1
2222.2222.2222	E2
3333.3333.3333	E3
4444.4444.4444	E4

IGMP snooping

- Izvedbe IGMP snooping
  - IGMP ˝snooping˝ z opcijo zadrževanja sporočil
    - prestrezanje in selektivno filtriranje sporočil IGMP, ki jih pošiljajo končni odjemalci robnemu usmerjevalniku multicast
  - IGMP ˝snooping˝ s funkcijo ˝proxy˝
    - komutacijskim napravam Ethernet omogoča generiranje lastnih sporočil IGMP
  - IGMP ˝immediate leave˝
    - takojšnja odjava vmesnika (odjemalca) iz multicast skupine
- Pomisleki glede implementacije funkcionalnosti ˝IGMP snooping˝ na Ethernet komutacijskih napravah
  - sporočila IGMP so poslana kot multicast promet kar pomeni, da se ne razlikujejo od ostalega multicast prometa
  - procesorska obdelava vsakega multicast paketa predstavlja veliko procesorsko obremenitev za L2 Ethernet stikala
  - potrebna je L3 funkcionalnost na stikalih Ethernet
  - posebni namenski čipi za procesiranje multicast prometa

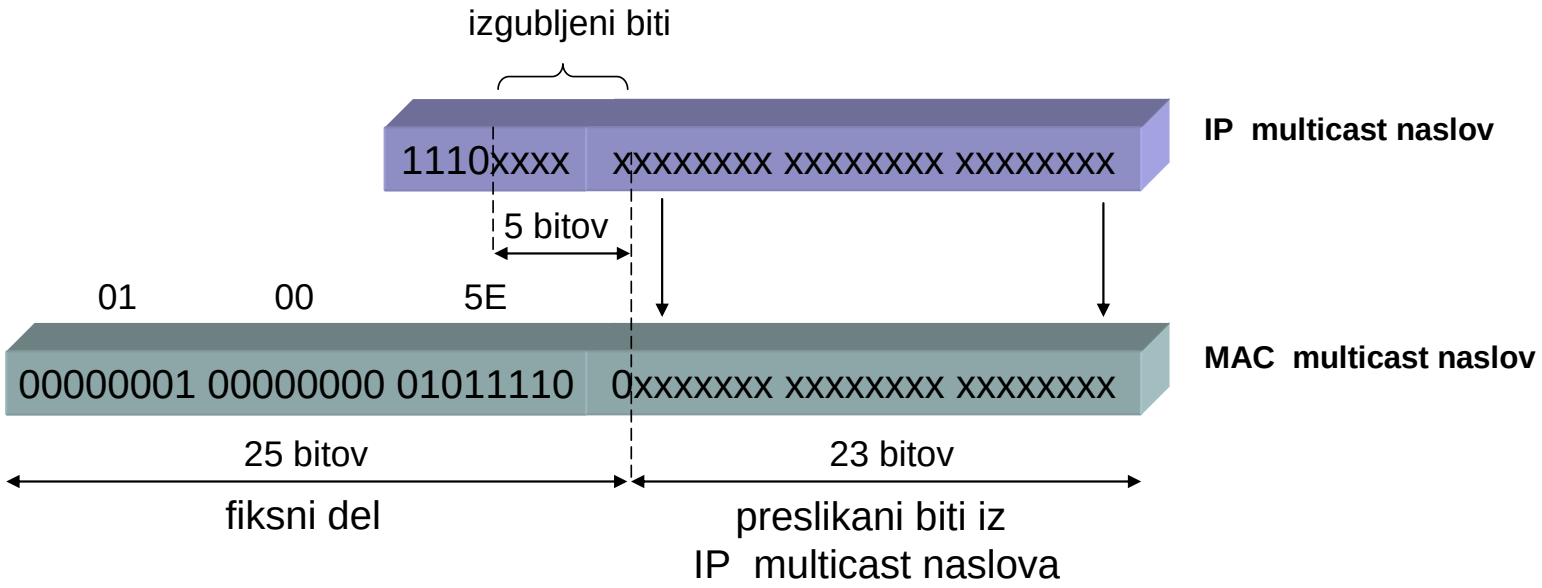
Ethernet multicast naslavljanje 1/2

- **Ethernet naslavljanje**
  - **unicast**
  - **broadcast**
  - **multicast**
- **Zgradba Ethernet naslova**

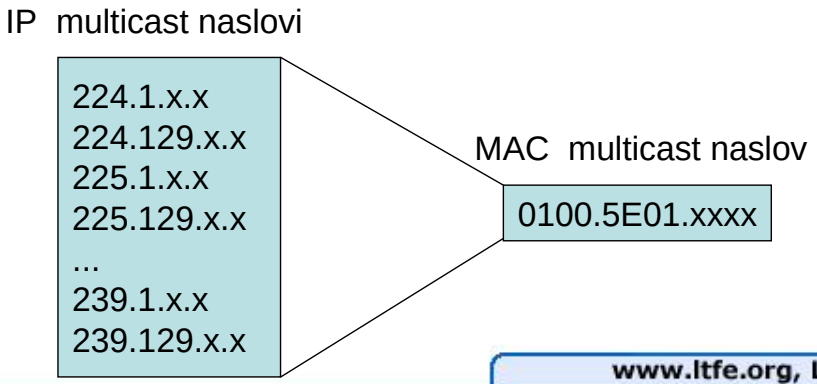


Ethernet multicast naslavljanje 2/2

- **Mapiranje med IP multicast in Ethernet multicast naslovi**



- **Naslovi multicast IP, ki se mapirajo v enak naslov multicast MAC**



Vsebina

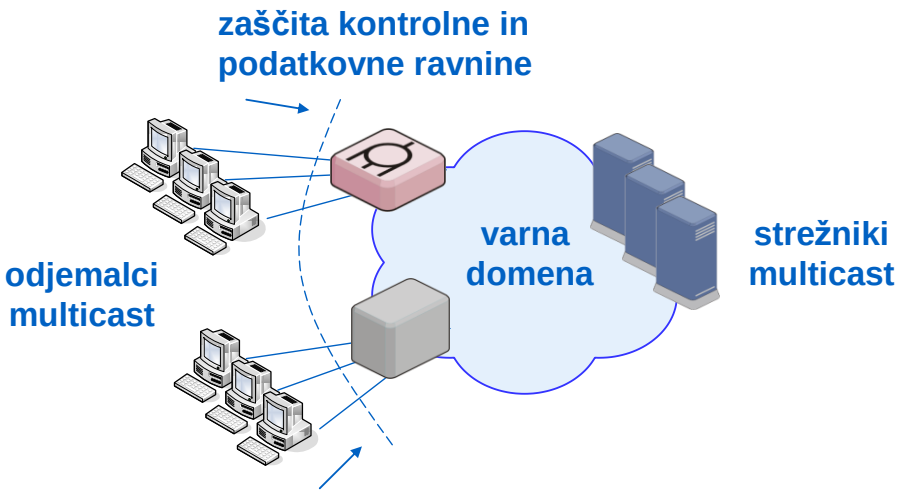
- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- **Varnost v multicast**
- Uporaba multicast

Varnost v multicast

- Tehnologija multicast nima lastnih varnostnih mehanizmov
  - ni mehanizmov za avtentikacijo in avtorizacijo uporabnikov ter kontrolo dostopa
  - vsaka naprava se lahko prijavi v multicast skupino
  - vsaka naprava lahko prične oddajat v multicast skupino
- Trije pristopi za zagotavljanje kontrole dostopa do multicast vsebin
  - zaščita vsebin na nivoju multicast aplikacij s sistemi DRM (Digital Rights Management) ali sistemi CA (Conditional Access)
  - implementacija varnostnih funkcij na elementih omrežja
    - na nivoju kontrolne ravnine, s filtriranjem sprejetih zahtev IGMP
      - na napravah kot so Ethernet stikala, robni usmerjevalnik, DSLAM
    - na nivoju podatkovne ravnine, s filtriranjem oddanega/sprejetega multicast prometa
      - na napravah kot so Ethernet stikala, DSLAM, robni usmerjevalnik
  - s protokolom MIPSec (ang. Multicast Internet Protocol Security)

Nosilna omrežna infrastruktura

- Implementacija varnostnih mehanizmov na elementih dostopovneg omrežja
  - filtriranje poslanih uporabniških zahtev IGMP
  - filtriranje oddanega uporabniškega prometa
- Slabosti
  - decentraliziran model nadzora dostopa, kar se odraža v slabi razširljivosti
  - kompleksne funkcije nadzora dostopa do storitev se prenesejo na dostopovne elemente omrežja
  - večja kompleksnost naprav



Protokol MIPsec

- Deluje na omrežnem sloju
- Celovit varnostni mehanizem
  - avtentikacija, integriteta, zaupnost in kontrola dostopa
- Slabosti
  - šifriranje je časovno in procesorsko potratno
  - model ne zagotavlja zaščite pred napadi DoS na multicast kontrolne mehanizme
- MIPSec se bo predvidoma uporabljal predvsem za izgradnjo navideznih zasebnih omrežij

Zaščita na nivoju aplikacij

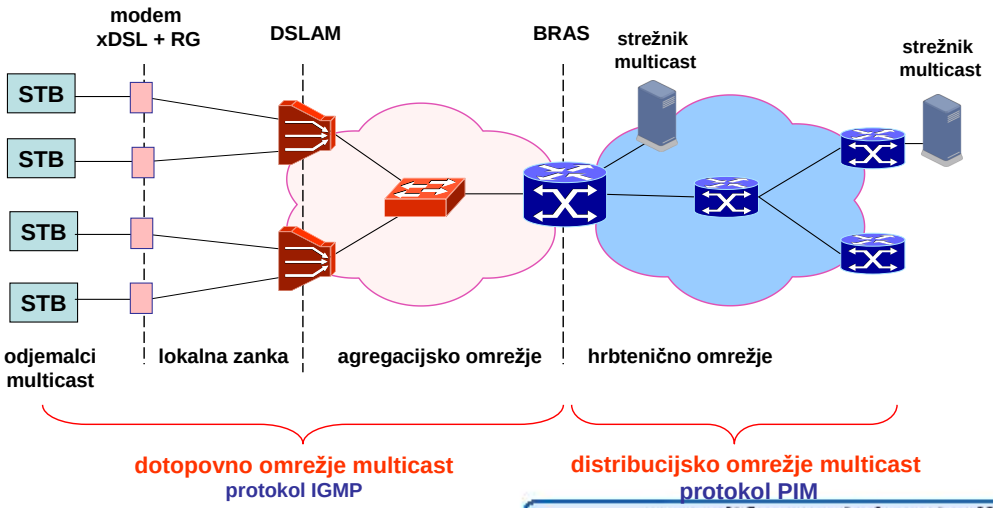
- Če ne obstaja tesna povezava med upravljalcem omrežja in ponudniki storitev
- Primer IPTV
  - sistemi DRM (ang. Digital Rights Management)
  - sistemi CA (ang. Conditional Access)
  - sistema omogočata ponudnikom storitev popoln nadzor nad dostopom do vsebin
- Ključna prednost modela je, da je vsebina zaščitena na celotni poti (šifrirana) – od multicast oddajnika do prejemnika
- Slabost
  - ne nudi zaščite pred napadi DoS

Vsebina

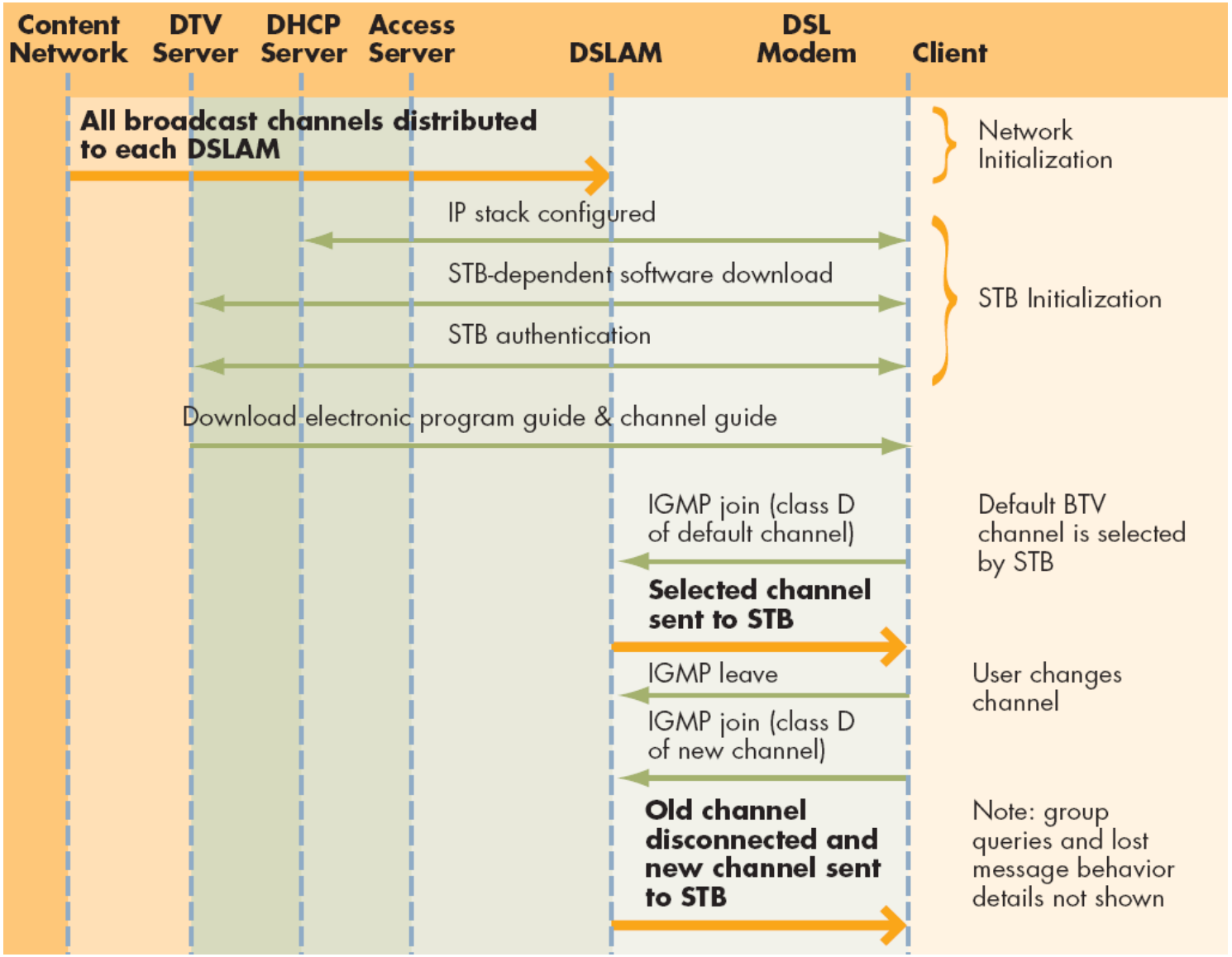
- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

Multicast elementi

- STB predstavlja končnega odjemalca multicast prometa
  - podpirati mora funkcionalnosti odjemalca IGMP
- DSLAM je Ethernet komutacijska naprava
  - podpirati mora funkcije IGMP ˝snooping˝ z razširitvami
- Agregacijsko stikalo je Ethernet komutacijska naprava
  - podpirati mora funkcije IGMP ˝snooping˝ z razširitvami
- BRAS predstavlja robni usmerjevalnik multicast
  - podpirati mora funkcionalnosti IGMP ˝querier˝ ter funkcionalnosti multicast usmerjevalnih protokolov



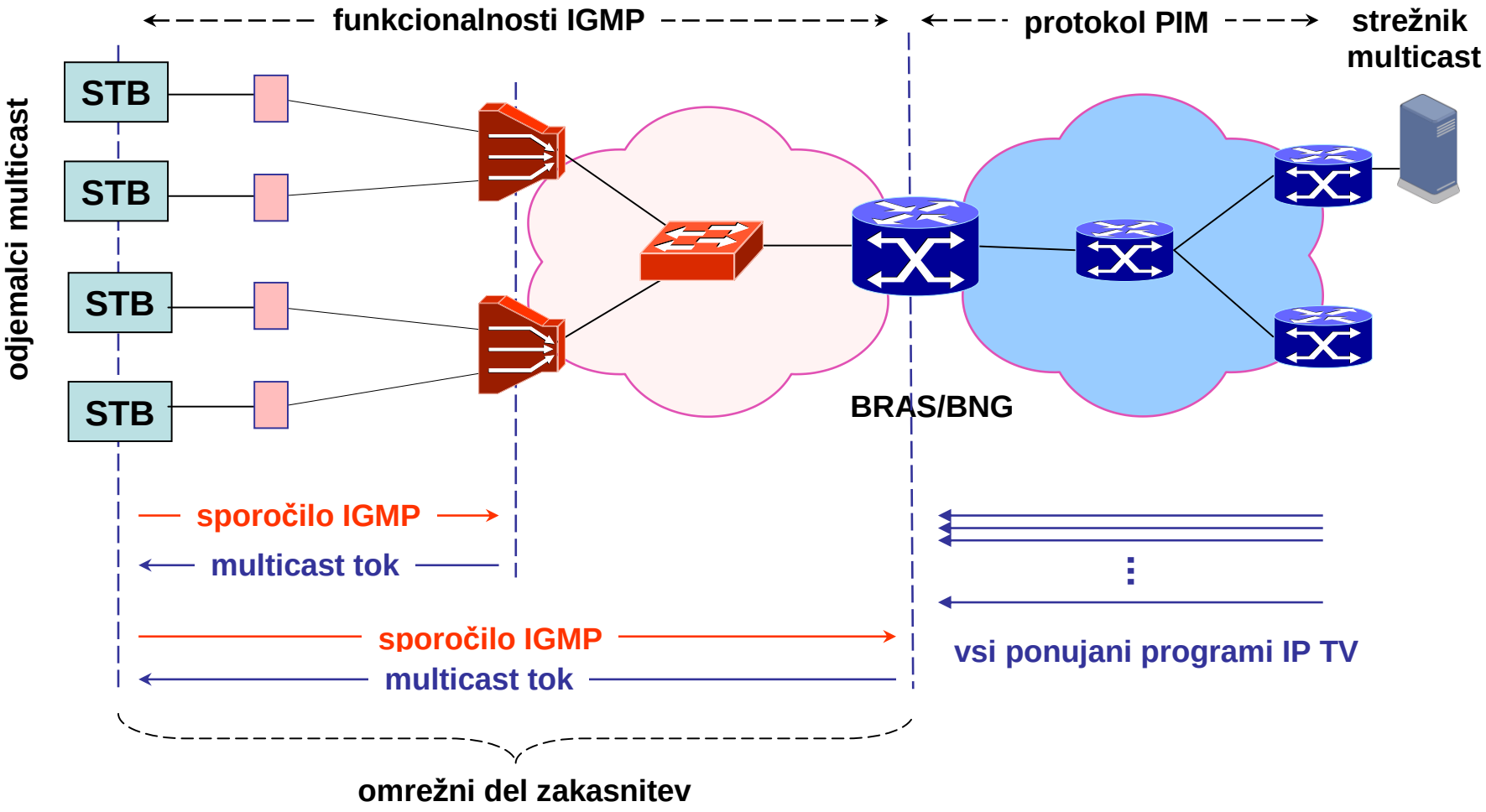
Koncept delovanja IPTV



Preklopni čas ˝zapping time˝ 1/2

- Časovni interval potreben za preklop med TV programi
- Zakasnitve na STB
  - obdelava zahtev
  - generiranje in oddaja sporočil IGMP ˝membership report˝
  - zakasnitve, ki jo vnaša izbran kodek
    - v primeru kodeka MPEG-2 (~ 500 ms)
    - v primeru kodeka MPEG-4 (nad ~ 1 s)
- Zakasnitve, ki jih vnašajo naprave in elementi dostopovnega omrežja
  - zakasnitve zaradi obdelave kontrolnih sporočil IGMP
    - izvajanje funkcij IGMP ˝snooping˝ na DSLAM ter agregacijskih stikalih
    - izvajanje funkcij IGMP na BRAS/BNG
  - zakasnitve zaradi komutacije
    - odvisne so od posamezne implementacije komutacijske naprave
  - zakasnitve zaradi razširjanja ˝propagation delay˝
    - odvisne so od fizičnega medija in njegove fizične dolžine
  - čas potreben za oddajo paketa na fizičen vmesnik ˝serialization delay˝
    - odvisen je od velikost oddajanega paketa in hitrost povezave

Preklopni čas ″zapping time″ 2/2



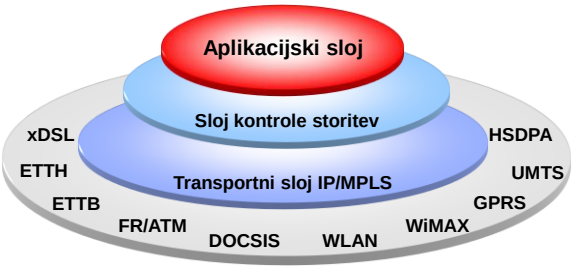
Usmerjanje v IP

Vsebina

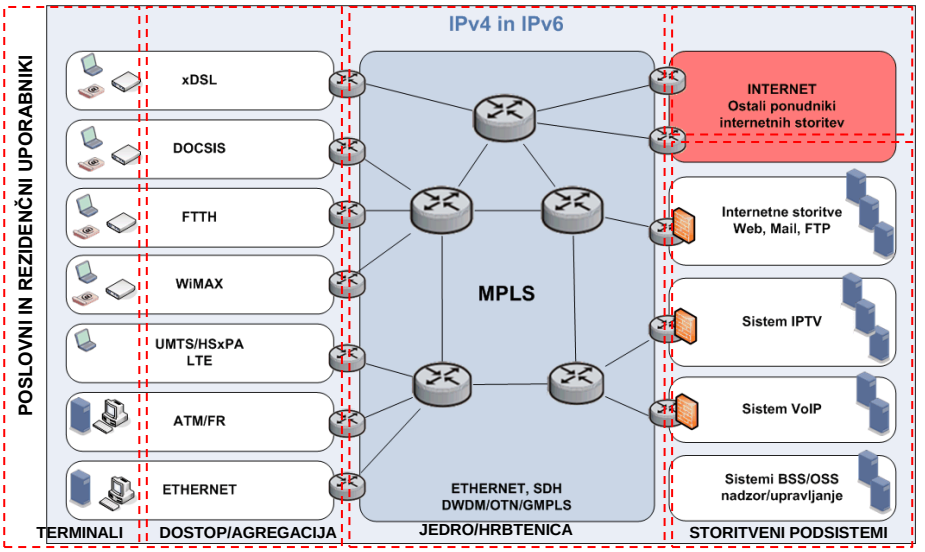
- Uvod
- Osnove usmerjanja
- Usmerjevalnik IP
- Usmerjevalni protokoli in algoritmi
- Usmerjevalni protokoli RIP, OSPF, ISIS in BGP

Koncept sodobnih omrežij

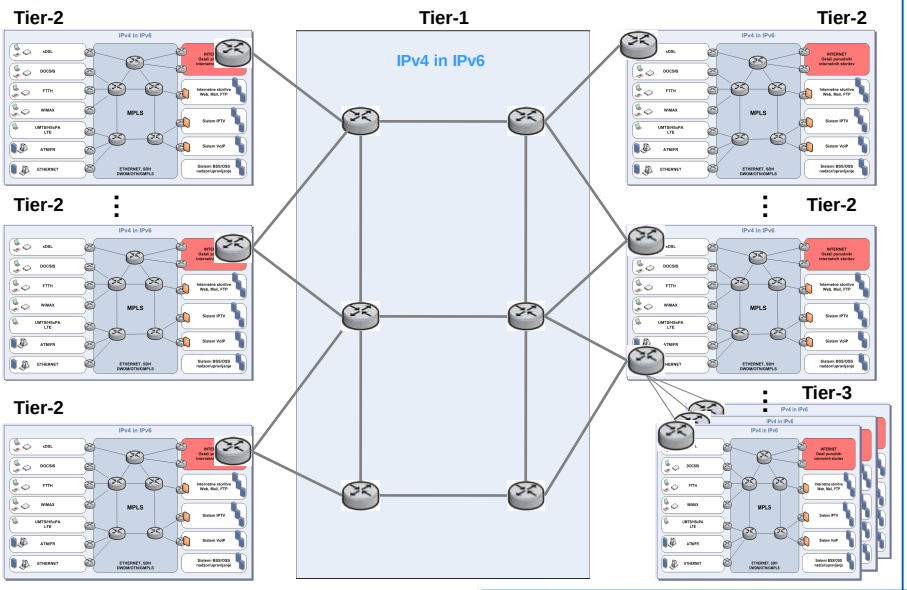
- Trije neodvisni sloji
  - aplikacijski sloj
  - sloj kontrole storitev
  - transportni sloj
- Transportni sloj
  - hrbtenica
  - distribucija (metro)
  - dostop
- Robne naprave
  - koncentracija inteligence v robnih napravah
  - zagotavljajo preprosto in razširljivo distribucijsko omrežje
  - trend: pozicija čim bližje uporabniku



Transportni sloj sodobnih omrežij

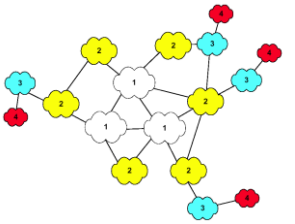


Logična shema Interneta



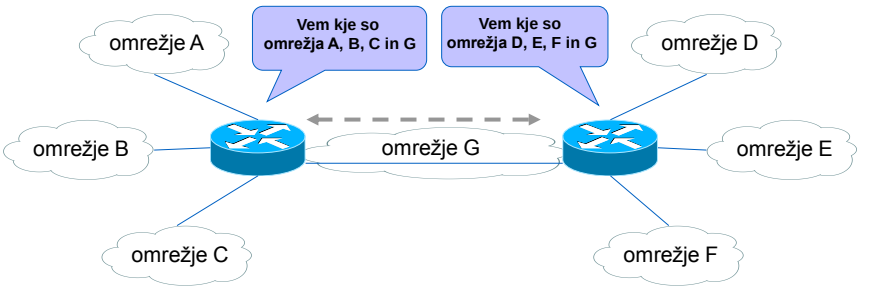
Internet

- Internet je množica medsebojno povezanih avtonomnih sistemov (Autonomous System)
  - AS je omrežje pod enotnim upravljanjem
- Vsako omrežje ima zagotovljeno popolno avtonomijo v svoji domeni
- Nobeno izmed omrežij (AS) ni kritično za delovanje celotnega interneta
  - ne predstavlja točke ˝single point of failure˝
  - v primeru izpada posameznega AS se poišče obvozna pot skozi drugo omrežja (avtonomne sisteme)



Kaj je usmerjanje?

- Izmenjava podatkov o dosegljivosti
- Izbira optimalne poti
- Usmerjevalnik
  - naprava za izvajanje procesa usmerjanja



Vsebina

- Uvod
- Osnove usmerjanja
- Usmerjevalnik IP
- Usmerjevalni protokoli in algoritmi
- Usmerjevalni protokoli RIP, OSPF, ISIS in BGP

Protokol IP

- Nepovezavno usmerjena tehnologija omrežnega (L3) sloja
- Vsak paket v glavi nosi izvorni in ciljni naslov IP
- Vročitve naslovniku ne zagotavlja
  - to prepušča višjim slojem (npr. TCP)
- Usmerjanje/posredovanje se za vsak paket izvrši v vsakem vozlišču posebej, neodvisno od ostalih paketov istega podatkovnega toka
- Usmerjevalni podatki so shranjeni v usmerjevalni tabeli
- Usmerjevalna tabela se lahko zgradi
  - statično – na roke
  - dinamično – na osnovi usmerjevalnih protokolov (RIP, OSPF, IS-IS, BGP)

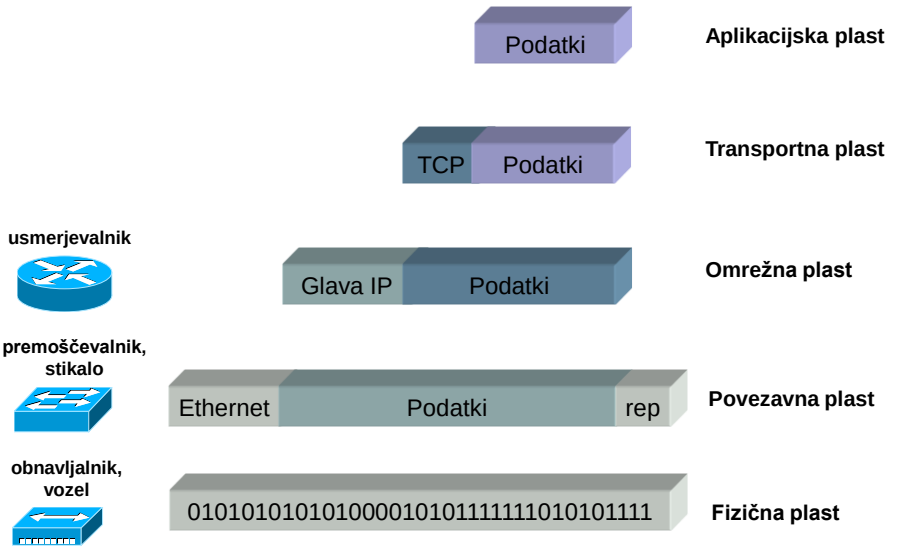
Povezaven in nepovezaven prenos

- Povezavno usmerjene komunikacije
  - vzpostavitev zveze
    - vzpostavitev povezave med izvorno in ponorno napravo, ugotavljanje pripravljenosti končne naprave
  - prenos podatkov
    - transparentna izmenjava podatkov
    - paketi potujejo po isti, vnaprej vzpostavljeni poti
  - sprostitev zveze
    - sprostitev uporabljenih naprav in prenosnih kanalov
- Nepovezavno usmerjene komunikacije
  - terminali oddajajo pakete brez predhodne vzpostavitve zveze s ciljno napravo
    - obstaja samo faza prenosa podatkov
    - vsak podatkovni paket vsebuje izvorni in ponorni naslov
    - paketi se medsebojno neodvisno prenašajo skozi omrežje
    - zaporedje oddanih in prejetih paketov ni nujno enako

Tipi komutacije - posredovanja

- **Vodovna komutacija**
  - vhodni prenosni kanal ˝žica˝ se galvansko sklopi na ustrezni izhodni prenosni kanal ˝žica˝
  - klasično telefonsko omrežje
- **Paketna komutacija – danes dominanten način komutacije**
  - posredujejo se paketi/datagrami/celice
  - povezavno usmerjena omrežja
    - stikala X.25, ATM, MPLS
    - virtualna zveza
    - predhodno se vzpostavi navidezna pot ˝cev˝
      - paketi ne vsebujejo ponornega naslova
  - nepovezavno usmerjena omrežja
    - usmerjevalnik IP
    - v vozlišču se posamezni paketi medsebojno neodvisno usmerjajo (vsak paket mora vsebovati ponorni naslov)
    - če neka povezava ali vozlišče odpove, se paketi preusmerijo na neprizadete dele omrežja

Omrežne naprave – umestitev v OSI

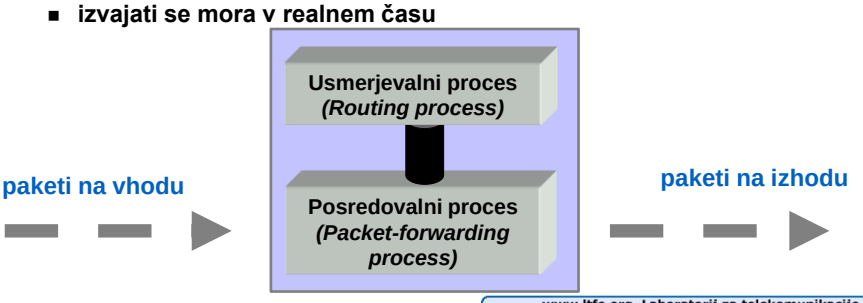


Vsebina

- Uvod
- Osnove usmerjanja
- Usmerjevalnik IP
- Usmerjevalni protokoli in algoritmi
- Usmerjevalni protokoli RIP, OSPF, ISIS in BGP

Zgradba usmerjevalnega sistema

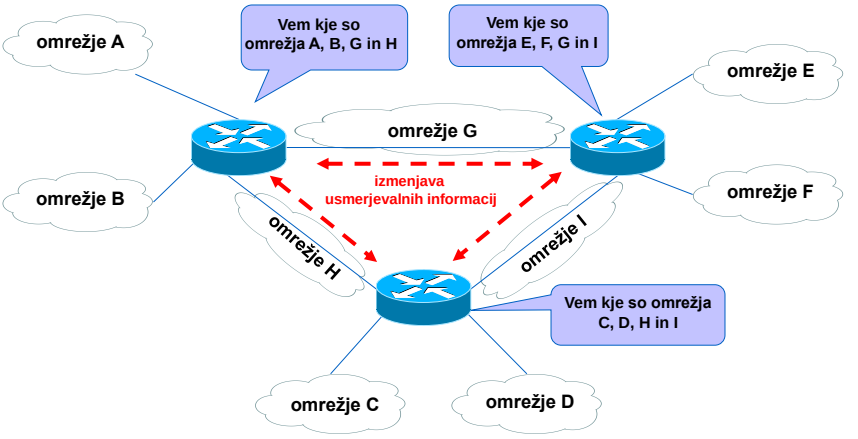
- Usmerjevalni proces
  - izmenjava usmerjevalnih informacij
  - določitev optimalne poti
  - izvaja se lahko v nerealnem času
- Posredovalni proces
  - Izbira ustreznega vmesnika “angl. longest-prefix-mach”
  - posredovanje paketov na izhodni vmesnik
  - izvajati se mora v realnem času



Usmerjanje in posredovanje

- **Usmerjevalni proces**
  - poganja usmerjevalne protokole
    - izmenjava usmerjevalnih informacij
    - odločanje o tem, kam datagram poslati, imenujemo usmerjanje (routing)
      - določitev optimalne poti
    - izgradnja usmerjevalne tabele (RIB - routing information base)
- **Posredovalni proces**
  - posredovanje paketov iz vhodnega vmesnika na izhodni vmesnik
  - skozi omrežje obstaja več poti
    - samo najbolj optimalna se zapiše v posredovalno tabelo (FIB - forwarding information base)
  - izbira ustreznega izhodnega vmesnika se izvaja po principu ujemanja v največji meri “angl. longest-prefix-mach”
- **Zmogljivost (QoS) usmerjevalnika določa posredovalni proces**

Usmerjevalnik – usmerjevalni proces



Usmerjevalnik – usmerjevalni proces

- Statično usmerjanje
  - ročna določitev posredovalnega vmesnika
    - administrator prek upravljavskega vmesnika določi pot
  - privzeta pot
    - pošiljanje vseh paketov, ki ne najdejo specifične poti po tej poti
    - poseben tip statičnega usmerjanja
- Dinamično usmerjanje
  - avtomatska določitev usmerjevalnih poti
  - uporaba usmerjevalnih protokolov

Usmerjevalnik – posredovalni proces

- Posredovalna funkcija – osnovne naloge (Fast Path)
  - sprejema paketa na vhodnem vmesniku
  - dekapsulacije datagrama IP – odstranitev okvirja L2
  - preverjanje kontrolne vsote glave IP
  - preverjanje TTL in zmanjševanje vrednosti za 1
  - ponoven izračun kontrolne vsote
  - določanje optimalne poti – longest-prefix-match
    - posredovanje na en izhoden vmesnik (unicast)
    - posredovanje na več izhodnih vmesnikov (multicast)
  - inkapsulacije datagrama IP – dodajanje ustrezne glave in repa L2
  - prenos paketa na ustrezen izhodni vmesnik, ki ga določa usmerjevalna tabela
- Posredovalna funkcija – kompleksne naloge (opcijsko)
  - fragmentacija, če je MTU manjši od velikosti paketa
  - razvrščanje paketov (classification), tipično na osnovi ACL

Vsebina

- Uvod
- Osnove usmerjanja
- Usmerjevalnik IP
- Usmerjevalni protokoli in algoritmi
- Usmerjevalni protokoli RIP, OSPF, ISIS in BGP

Usmerjevalni protokoli

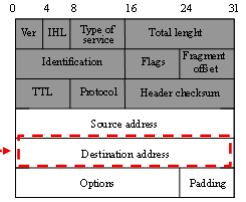
- Protokoli, ki nam poganjajo usmerjevalne algoritme
- Izgradnja usmerjevalnih tabel
  - vsak usmerjevalnik vzdržuje usmerjevalno (posredovalno) tabelo
  - vsak usmerjevalni protokol vzdržuje svojo usmerjevalno tabelo
- Usmerjevalna tabela
  - vsebuje vnose, ki določajo, prek katerega izhodnega fizičnega vmesnika mora omrežna naprava posredovati paket za ciljni naslov IP
  - zapisi v usmerjevalni tabeli

Omrežje	Maska	Vmesnik	Naslednji hop	Metrika	Starost	Vir
192.168.1.0	255.255.255.0	FE0/0	192.168.3.10	3	300	RIP
192.168.2.0	255.255.255.0	FE0/1	192.168.3.10	2		Statično
192.168.3.0	255.255.255.0	FE0/2				

Iskanje v usmerjevalni tabeli

- Ciljni naslov v glavi IP primerjamo z naborom naslovov v usmerjevalni tabeli
  - ujemanje celotnega naslova IP
  - ujemanje omrežnih naslovov
  - upoštevanje privzete (default) poti

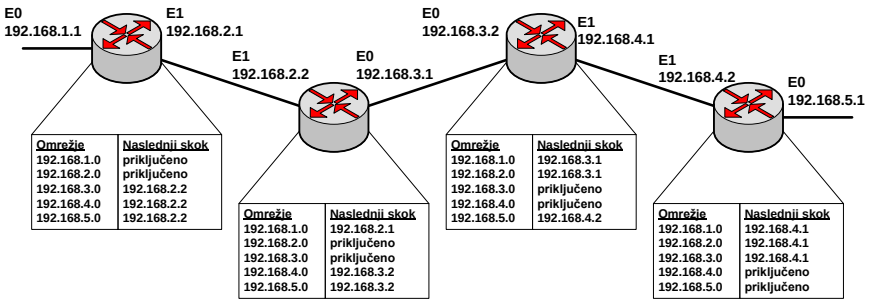
Glava datagrama IP



Omrežje	Maska	Vmesnik	Naslednji skok	Metrika	Starost	Vir
192.168.1.0	255.255.255.0	FE0/0	192.168.3.10	3	300	RIP
192.168.2.0	255.255.255.0	FE0/1	192.168.3.10	2		Statično
192.168.3.0	255.255.255.0	FE0/2				

Uporaba usmerjevalne tabele

- Primer uporabe usmerjevalne tabele pri pošiljanju IP paketa preko omrežja



Usmerjevalna tabela - Windows

- Ukaz
  - route print

```
C:\Documents and Settings\Administrator>route print
===========================================================================
Seznam vmesnikov
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 2c 7c 57 ...... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler
Miniport
===========================================================================
===========================================================================
Aktivne smeri:
Omrežni cilj        Maska omrežja    Prehod          Vmesnik
                                                     Metrika
0.0.0.0             0.0.0.0          172.16.105.2    172.16.105.128    10
127.0.0.0           255.0.0.0        127.0.0.1       127.0.0.1         1
172.16.105.0        255.255.255.0    172.16.105.128  172.16.105.128    10
172.16.105.128      255.255.255.255  127.0.0.1       127.0.0.1         10
172.16.255.255      255.255.255.255  172.16.105.128  172.16.105.128    10
224.0.0.0           240.0.0.0        172.16.105.128  172.16.105.128    10
255.255.255.255     255.255.255.255  172.16.105.128  172.16.105.128    1
Privzeti prehod:     172.16.105.2
===========================================================================
```


Usmerjevalna tabela - Linux

- Ukaz
  - route

```
administrator@PC:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref    Use Iface
172.16.4.0      *               255.255.255.0   U       0       0        0 vmnet1
172.16.105.0    *               255.255.255.0   U       0       0        0 vmnet8
10.0.0.0        *               255.255.0.0     U       1       0        0 eth0
link-local      *               255.255.0.0     U       1000    0        0 eth0
default         10.0.0.1        0.0.0.0         UG      0       0        0 eth0
```

Usmerjevalna tabela - Cisco

- Ukaz
  - show ip route

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     10.0.0.0/24 is subnetted, 7 subnets
R       10.1.1.0 [120/1] via 10.1.2.1, 00:00:23, Serial0/3/0
C       10.1.2.0 is directly connected, Serial0/3/0
C       10.1.3.0 is directly connected, FastEthernet0/0
C       10.1.4.0 is directly connected, Serial0/3/1
R       10.1.5.0 [120/1] via 10.1.4.2, 00:00:15, Serial0/3/1
R       10.1.6.0 [120/1] via 10.1.4.2, 00:00:15, Serial0/3/1
R       10.1.7.0 [120/2] via 10.1.4.2, 00:00:15, Serial0/3/1
```


Usmerjevalna tabela - Juniper

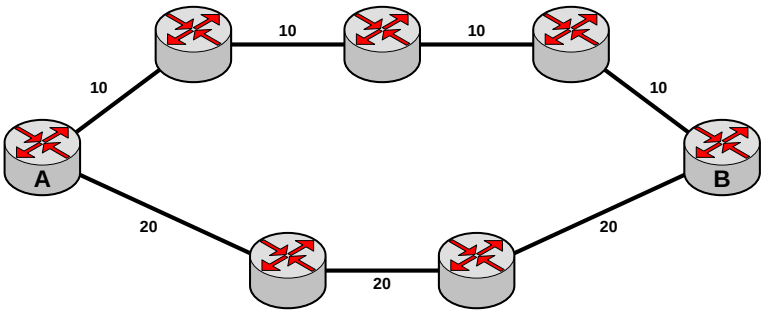
- Ukaz
  - show route table inet.0

```
user@host> show route table inet.0
inet.0: 12 destinations, 12 routes (11 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0                  *[Static/5] 00:51:57
                           > to 111.222.5.254 via fxp0.0
1.0.0.1/32                 *[Direct/0] 00:51:58
                           > via at-5/3/0.0
1.0.0.2/32                 *[Local/0] 00:51:58
                           Local
12.12.12.21/32             *[Local/0] 00:51:57
                           Reject
13.13.13.13/32             *[Direct/0] 00:51:58
                           > via t3-5/2/1.0
13.13.13.14/32             *[Local/0] 00:51:58
                           Local
13.13.13.21/32             *[Local/0] 00:51:58
                           Local
13.13.13.22/32             *[Direct/0] 00:33:59
                           > via t3-5/2/0.0
127.0.0.1/32               [Direct/0] 00:51:58
                           > via lo0.0
111.222.5.0/24             *[Direct/0] 00:51:58
                           > via fxp0.0
111.222.5.81/32            *[Local/0] 00:51:58
                           Local
```

Izbira optimalne poti

- Usmerjevalna metrika
  - vrednost določena posameznim potem
  - izbira optimalne poti na podlagi najnižje metrike
  - seštevek cen povezav na posamezni poti



Lastnosti usmerjevalnih algoritmov

- Preprost – malo režijskih stroškov
  - funkcionalno učinkovit z minimalnimi programskimi, procesorskimi ter pomnilniškimi zahtevami
- Robusten
  - pravilno delovanje tudi v ekstremnih okoliščinah (strojne okvare, hude prometne obremenitve ...)
- Hitro konvergira
  - kako hitro je, ob spremembah v omrežju, opravljen proces izbire optimalne poti med vsemi sodelujočimi usmerjevalniki

Delitve usmerjevalnih algoritmov

- Notranji, intradomain, interior – zunanji, interdomain, exterior
  - delitev glede na njihov namen: znotraj domene (RIP, OSPF, IS-IS), in med domenami (BGP)
- Single-path – Multipath
  - delitev glede na število poti, ki jih usmerjevalni algoritem podpira do iste ciljne naprave
- Flat – Hierarchical
  - ˝flat space˝: vsi usmerjevalniki so si sosedje ˝routing peers˝
  - ˝hierarchical systems˝: med usmerjevalniki obstaja hierarhija, logično grupiranje naprav – domene, področja in avtonomni sistemi
- Host-intelligent – Router-intelligent
  - izvorna naprava določi pot od izvora do cilja (source routing)
  - usmerjevalniki določijo pot do ciljne naprave (destination based routing)
- Link-state – Distance vector

Distance vector

- Usmerjanje na osnovi vektorja razdalje (Distance Vector):
  - temelji na algoritmu ˝Bellman-Ford˝
  - usmerjevalne informacije se razpošljejo le sosedom – počasna konvergenca
    - usmerjevalniki v omrežju poznajo le svoje sosede in ceno poti do njih
    - vsak usmerjevalnik periodično pošilja sosedom poznane destinacije ter njihovo ceno
    - sosedni usmerjevalnik primerja sprejeta sporočila s svojo usmerjevalno tabelo – če obstaja nova ali bolj optimalna pot se slednja prepiše v usmerjevalno tabelo
  - uporabljena metrika je dolžina poti (hop count)
  - počasna konvergenca
  - za svoje delovanje potrebujejo manj sistemskih zmogljivosti (CPU in RAM) kot algoritmi ˝link state˝
  - tipičen predstavnik je protokol RIP

Link-state

- Usmerjanje na osnovi stanja povezav
  - temelji na algoritmu ˝Dijkstra˝
  - usmerjevalne informacije se razpošljejo vsem usmerjevalnikom v omrežju – hitra konvergenca
    - usmerjevalniki poznajo celotno topologijo omrežja
    - vsak usmerjevalnik razpošlje informacije o svojih sosedih vsem usmerjevalnikom v omrežju
    - usmerjevalniki si zgradijo topologijo omrežja v obliki grafa (Link State Database) – enak pogled na omrežje
    - na osnovi algoritma ˝Dijkstra˝ si zgradijo drevo omrežja, s korenom drevesa pri sebi
  - uporabljena metrika je cena poti (numerična vrednost)
  - oglašujejo se samo spremembe v usmerjevalnih tabelah
  - omogočajo boljšo razširljivost kot ˝distance vector˝ algoritmi
  - tipična predstavnika sta protokola OSPF in IS-IS

Primerjava distance vector – link-state

- Distance vektor
  - preprost
  - za delovanje potrebuje malo sistemskih virov (CPU, RAM)
  - malo nastavitev
  - primeren za majhna omrežja
  - počasna konvergenca algoritma
  - slaba razširljivost
- Link-state
  - hitra konvergenca omrežja
  - proces oglaševanja poti in proces izračuna optimalne poti sta neodvisna
  - oglašujejo se samo spremembe v usmerjevalnih tabelah
  - za delovanje potrebuje več sistemskih virov kot algoritem ˝distance vektor˝ (CPU, RAM)

Metrika 1/2

- Dolžina poti (path length)
  - najbolj uporabljana usmerjevalna metrika
    - število skokov (hop count) na poti do ciljne naprave – vsak usmerjevalnik predstavlja en skok
- Zanesljivost
  - običajno se določa na osnovi ˝bit-error rate˝ oz. zmožnosti hitre ponovne vzpostavitve posamezne povezave
    - administrator ˝ročno˝ določi neko vrednost
- Zakasnitve
  - čas prenosa paketa od izvorne do ponorne naprave
    - na skupno zakasnitev lahko vplivajo: pasovna širina povezave, trenutna prometna obremenitev, število skokov, komutacijske zmogljivosti omrežnih naprav
- Pasovna širina
  - povezave z večjo pasovno širino imajo prednost pred ostalimi

Metrika 2/2

- Obremenjenost
  - stopnja obremenjenosti omrežnih virov
    - procesorska obremenjenost posameznega usmerjevalnika oz. stikala, ponujani promet v neko napravo (paketi/s), ...
- Cena povezave
  - cena posamezne povezave
    - iskanje optimuma med ceno, zmogljivostjo in potrebami
- Administrativne omejitve

Izbira poti med različnimi izvori

- Če usmerjevalniki vzporedno poganjajo več usmerjevalnih protokolov lahko za isto ciljno omrežje obstaja več različnih poti, ki jih izračunajo različni usmerjevalni algoritmi
  - za izračun poti je uporabljena različna metrika
- Cisco – administrativna razdalja (administrative distance)
  - administrativna razdalja določa katera izmed izračunanih poti se bo vpisala v posredovalno tabelo
  - administrativna razdalja poti je določena z usmerjevalnim protokolom
  - manjša kot je vrednost administrativne razdalje boljša je pot
    - v posredovalno tabelo se vpiše pot z manjšo administrativno razdaljo
- Juniper – prednost poti (route preference)
  - enaka funkcionalnost kot administrativna razdalja pri Ciscu

Tip poti	Privzeta administrativna razdalja
connected	0
static	1
External BGP	20
OSPF	110
IS-IS	115
RIP	120
Internal BGP	200

Izbira med potmi z različnim izvorom

- Možnih več poti do cilja z različnimi usmerjevalnimi izvori
  - statično določene poti
  - dinamično naučene poti
- Cisco – administrativna razdalja (administrative distance)
  - določa zaupanje v posamezni usmerjevalni izvor
  - nižja vrednost je boljša
  - določene privzete vrednosti
    - možna ročna sprememba
- Juniper – prednost poti (route preference)
  - enaka funkcionalnost kot administrativna razdalja pri Ciscu

Vsebina

- Uvod
- Osnove usmerjanja
- Usmerjevalnik IP
- Usmerjevalni protokoli in algoritmi
- Usmerjevalni protokoli RIP, OSPF, ISIS in BGP

Protokol RIP

- Routing Information Protocol v1 – RFC 1058
  - spada v družino ˝distance vector˝ usmerjevalnih protokolov
  - starejši protokol, uporablja se v preprostejših omrežjih
  - enostavna implementacija = malo funkcionalnosti
  - za metriko uporablja število skokov – HOP COUNT (max 15)
  - metrično dolžino računa na osnovi podatkov sprejetih od sosednjih usmerjevalnikov
  - počasna konvergenca
  - izmenjava usmerjevalnih informacij (broadcast) poteka v rednih intervalih, običajno vsakih 30 s (ob inicilaizaciji, na zahtevo)
  - ne podpira variabilnih mask (VLSM – Variable Length Subnet Mask)
- Routing Information Protocol v2 – RFC 1723
  - podpira variabilne maske VLSM
  - za izmenjavo usmerjevalnih informacij uporablja multicast
  - avtentikacija sporočil na osnovi MD5

Protokol OSPF

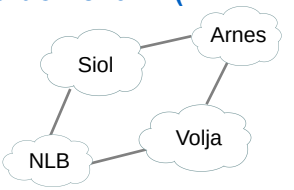
- Open Shortest Path First (RFC 2328)
  - prva OSPF (IETF) delovna skupina ustanovljena 1988
- Spada v družino ˝link-state˝ usmerjevalnih protokolov
- Deluje na osnovi algoritma ˝prvo najkrajša pot˝ (angl. SPF - Shortest Path First) Dijkstra algoritem
  - celotno sliko omrežja gradi s pomočjo teorije grafov
  - vsak usmerjevalnik vzdržuje podatkovno bazo, v kateri se nahajajo informacije o vseh povezavah v določenem področju (angl. Area) – osnova za izračun ˝najkrajše˝ poti
- Omogoča hitro konvergenco
- Podpira VLSM
- Omogoča avtentikacijo izmenjanih sporočil
- Logično grupiranje omrežij
  - delitev na področja
  - prikrivanje topologije področja

IS-IS

- Intermediate System – Intermediate System (standard OSI)
  - Standard ISO 10589 (december 1990)
- Načrtovan za OSI usmerjanje
  - lahko razširljiv
    - razširitve za IP usmerjanje v RFC 1195 – Integrated IS-IS
    - razširitve za IPv6
- Enaki principi delovanja kot OSPF
  - link-state usmerjevalni protokol
    - baza LSDB
    - SPF algoritem
  - uporaba Hello sporočil za vzpostavljanje statusa soseda
  - možnost hiearhije
  - možnost sumarizacije
  - “classless” usmerjevalni protokol
  - možnost avtentikacije

Protokol BGP

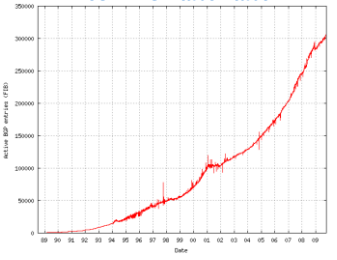
- Border Gateway Protocol
- RFC 1771 – BGPv4
- Spada v družino ˝path vector˝ usmerjevalnih protokolov (izboljšana verzija algoritma ˝distance vector˝)
  - pot se določi na osnovi ciljnega omrežja in metrike (path attribute)
  - za izmenjavo usmerjevalnih informacij uporablja protokol TCP (vrata 179)
  - celotna usmerjevalna tabela BGP se izmenja ob inicializaciji, naknadno se oglašujejo le spremembe
  - širok nabor metrike (path attributes)
- Omogoča brezrazredno usmerjanje med domenami (CIDR - Classless Inter Domain Routing)
- Dva načina delovanja
  - iBGP (interior Border Gateway Protocol)
    - znotraj avtonomnega sistema
  - eBGP (exterior Border Gateway Protocol)
    - med avtonomnimi sistemi



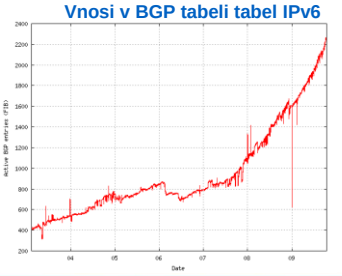
Skaliranje interneta

- Velikost usmerjevalnih tabel BGP naglo narašča
  - velikost približno odraža število omrežij povezanih v internet
- Rast pomnilniških kapacitet usmerjevalnikov mora slediti temu trendu
  - tabele IGP največjih ISPjev imajo do 9.000 vnosov
  - tabele BGP (EGP) imajo čez 300.000 vnosov

Vnosi v BGP tabeli tabel IPv4



Vnosi v BGP tabeli tabel IPv6



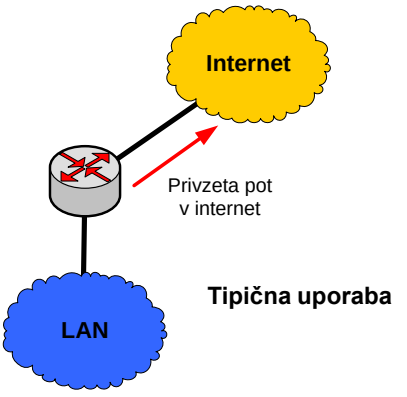
Vir: www.cidr-report.org

Statično usmerjanje

- Ročni vnos statičnih poti v usmerjevalno tabelo
- Prednosti
  - boljša kontrola usmerjanja v omrežju
- Slabosti
  - potrebna človeška intervencija v primeru izpadov
- Uporaba
  - usmerjanje v manjših omrežjih
  - določanje povzetkov poti (summary route)
  - določanje alternativnih poti

Privzeta pot

- Poseben primer statične poti
- Uporabi se v primeru, ko ni bolj specifičnega ujemanja
- IPv4 privzeta pot
  - 0.0.0.0/0
- IPv6 privzeta pot
  - ::/0



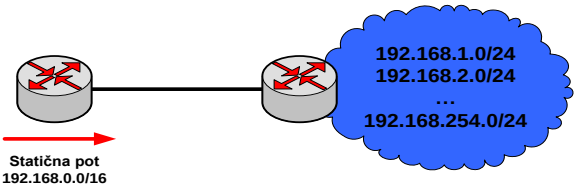
Tipična uporaba

Primer nastavitve statične poti

- Windows
  - route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
- Linux
  - route add –net 157.0.0.0 netmask 255.0.0.0 gw 157.55.80.1
- Cisco
  - ip route 157.0.0.0 255.0.0.0 157.55.80.1
- Juniper
  - set routing-options static route 157.0.0.0/8 next-hop 157.55.80.1

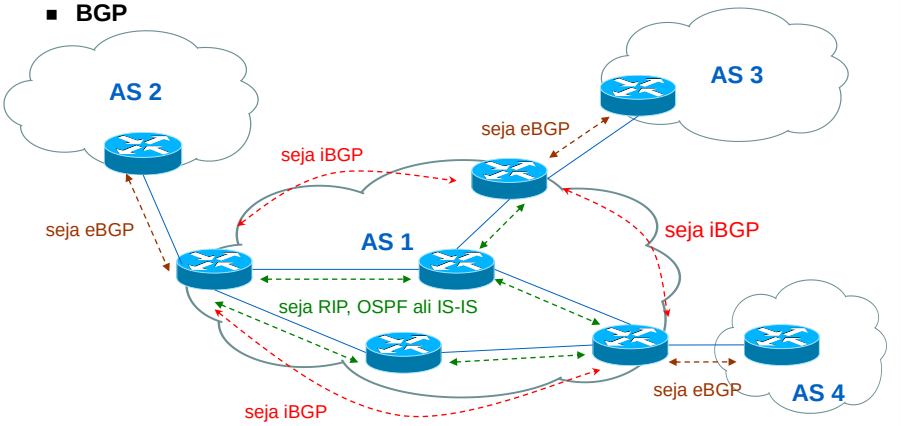
Povzetki poti

- Povzetek poti (summary route)
  - pot, ki določa več specifičnih omrežnih naslovov
  - zmanjšanje število vnosov v usmerjevalni tabeli



Umestitev usmerjevalnih protokolov

- Znotraj avtonomnega sistema
  - RIP, OSPF, IS-IS
- Med avtonomnimi sistemi
  - BGP



Primerjava protokolov 1/2

- Protokoli RIP, OSPF, ISIS (IGP)
  - mehanizem za avtomatsko iskanje sosedov (usmerjevalnikov)
  - povezovanje usmerjevalnikov v ˝omrežje˝
  - majhne usmerjevalne tabele
  - hitra konvergenca
  - oglaševane informacije se ne filtrirajo (verjamemo sosedom)
- Protokol BGP (EGP)
  - ˝ročna˝ nastavitev sosedov BGP
  - povezovanje omrežij v internetno omrežje
  - velike usmerjevalne tabele
  - počasna konvergenca
  - filtriranje oglaševanih informacij (verodostojnost sosedov je vprašljiva)

Primerjava protokolov 2/2

	LINK STATE	DISTANCE VECTOR	ADVANCE DISTANCE VECTOR	PATH VECTOR
RAZŠIRLJIVOST	DOBRA	SLABA	DOBRA	ZELO DOBRA
PASOVNA ŠIRINA	MAJHNA	VELIKA	MAJHNA	MAJHNA
POMNILNIK	VELIK	MAJHEN	ZMEREN	VELIK
CPU	VELIKA	MAJHNA	MAJHNA	ZMERNA
KONVERGENCA	HITRA	POČASNA	HITRA	ZMERNA
UPRAVLJANJE	ZMERNO	PREPROSTO	PREPROSTO	ZAHTEVNO

PROTOKOL	TIP	STANDARD	FUNKCIJA	OBNOVITVE	METRIKA	VLMS
RIPV1	D. VECTOR	JAVEN	INTERNI	30 s	HOP	NE
RIPv2	D. VECTOR	JAVEN	INTERNI	30 s	HOP	DA
IGRP	D. VECTOR	ZASEBEN	INTERNI	90 s		NE
EIGRP	A. D. VECTOR	ZASEBEN	INTERNI	PO POTREBI		DA
OSPF	LINK STATE	JAVEN	INTERNI	PO POTREBI	CENA	DA
IS-IS	LINK STATE	JAVEN	INTERNI	PO POTREBI	CENA	DA
BGP	PATH VECTOR	JAVEN	EXTERNI	PO POTREBI		DA

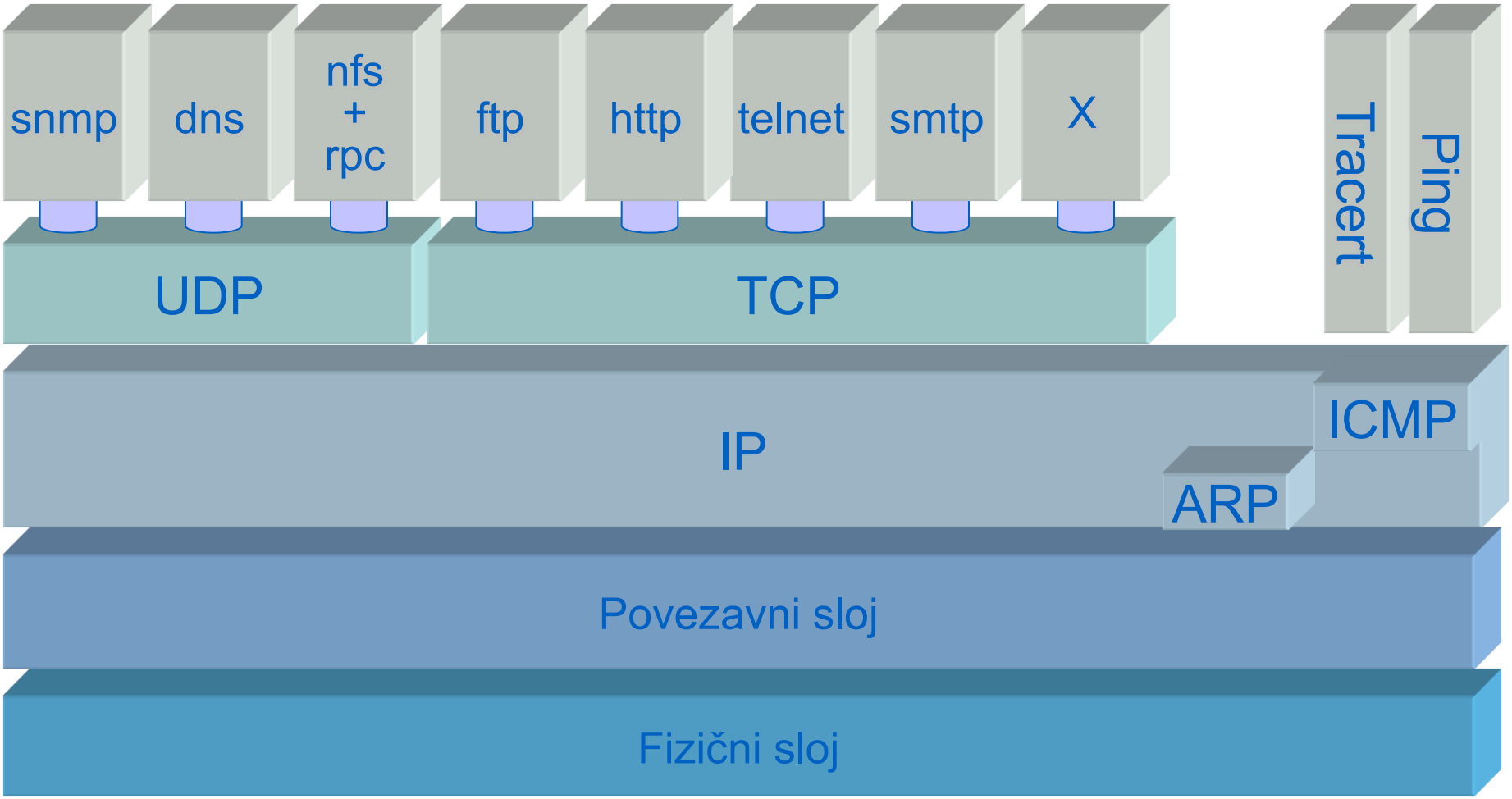
Varnostne storitve v omrežjih IP

Kazalo

- Varnostne storitve
- Varnostni mehanizmi
- Protokol IPSec

Tehnologija Ethernet

Protokoli sklad TCP/IP



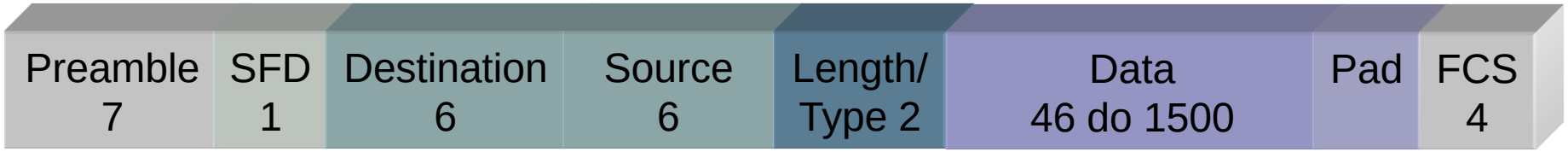
Značilnosti tehnologije Ethernet

- Tehnologija razvita za okolja LAN
- Deluje po princip ˝Plug and Play˝
  - nič ni potrebno nastaviti, vse se zgodi avtomatsko ☺
- Odprt storitveni model
  - vsak lahko komunicira z vsakim
  - za vse uporabnike se predvideva, da so legitimni
  - ni avtentikacije oddajnika in sprejemnika
    - brez preverjanja izvornih in ponornih naslovov MAC
  - ni enkripcije prenosnega kanala Ethernet
- Podatkovna in kontrolna ravnina združeni
  - stikalo Ethernet zgradi tabelo MAC na osnovi posredovalne funkcije
- Ethernet napadi
  - poplavljanje tabel MAC
  - zastrupljanje tabel ARP
  - napadi na kontrolne mehanizme STP, RSTP, MSTP

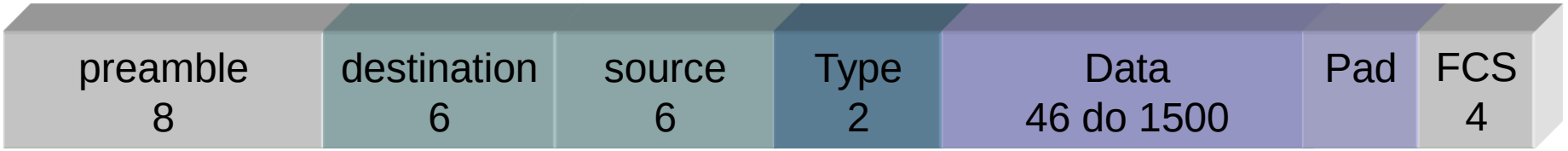
Okvir Ethernet in 802.3

- **Preamble – niz potreben za sinhronizacijo (1010 ...)**
  - **združljivost za nazaj – 10 Mbit Ethernet (asinhron)**
  - **SFD (Start Frame Delimiter) – konec sinhronizacije (niz 10101011)**
- **Destination/source**
  - **ciljni/izvorni naslov MAC**
- **Length/Type**
  - **vrednost manjša od 600 HEX – polje Length**
  - **vrednost enaka ali večja od 600 HEX - polje Type**
  - **0800HEX = IPv4, 806HEX = ARP**
- **PAD – polnilni biti**
- **FCS – polje za zapis izračunane vrednosti CRC**

Okvir IEEE 802.3



Okvir Ethernet II – DIX v2

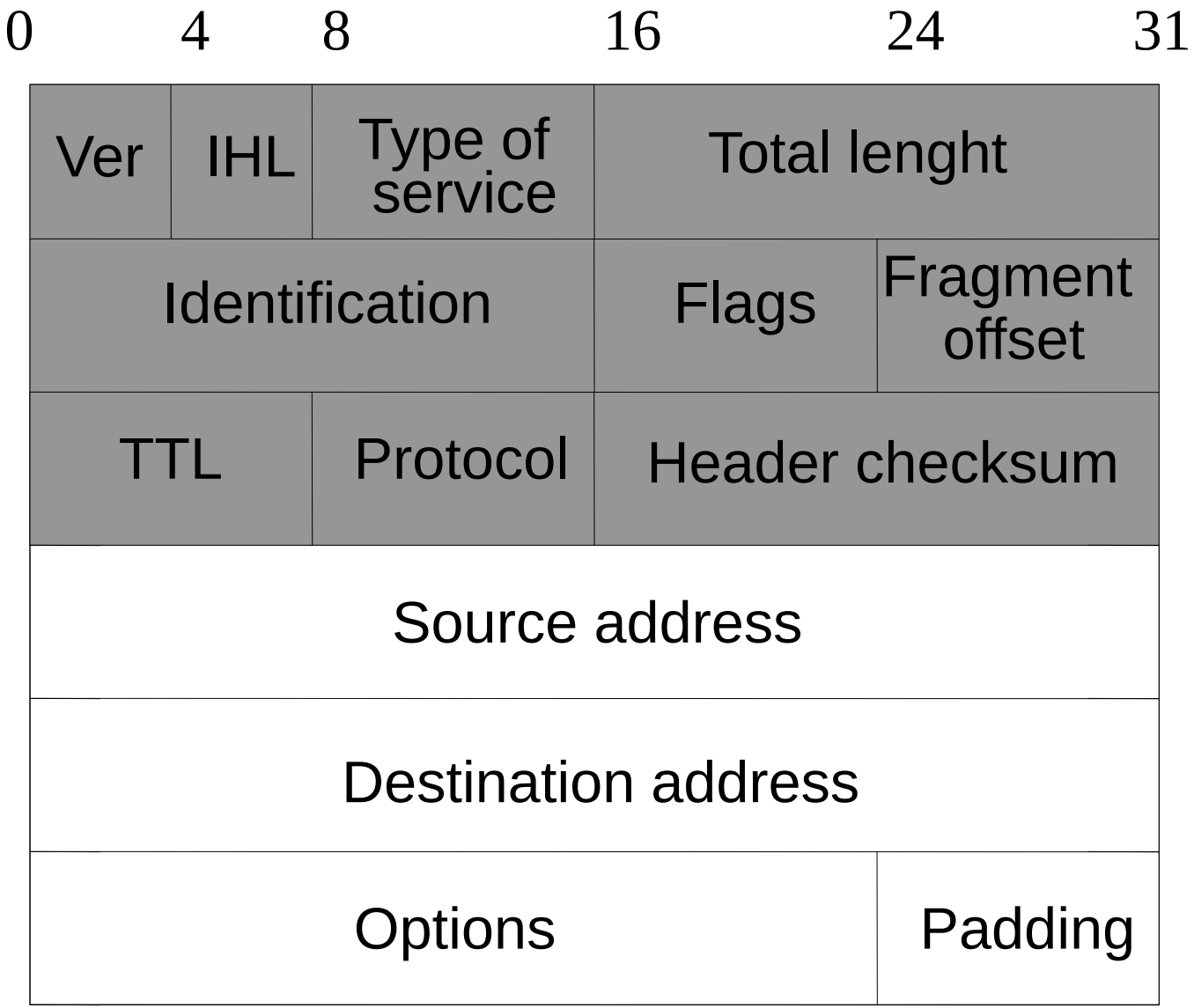


Protokol TCP/IP

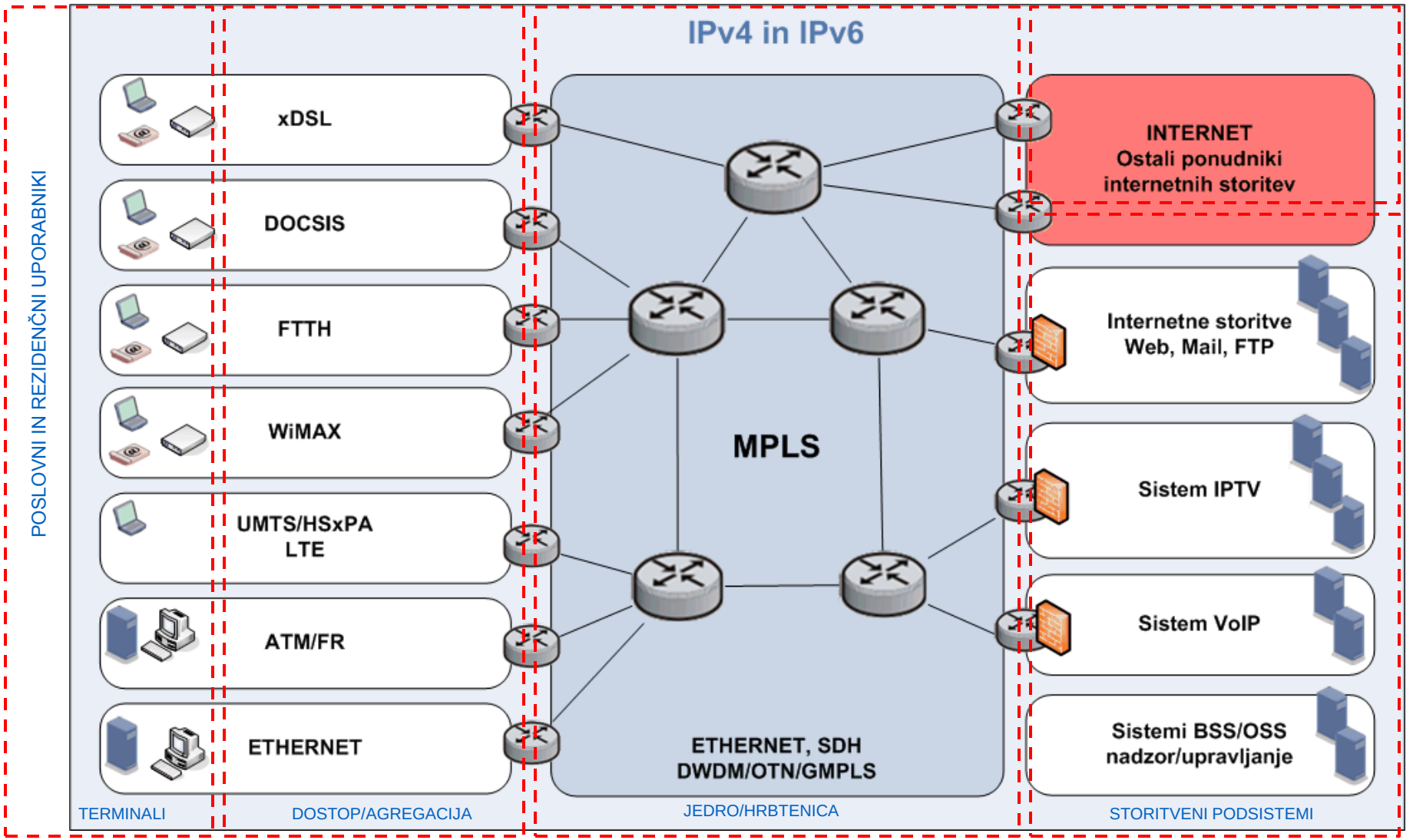
Značilnosti protokolov TCP/IP

- Značilnosti protokola IP
  - odprt storitveni model
    - vsak lahko komunicira z vsakim
    - za vse uporabnike se predvideva, da so legitimni
    - ni avtentikacije oddajnika in sprejemnika
      - brez preverjanja izvornih in ponornih naslovov
    - ni enkripcije prenosnega kanala IP
- Značilnosti protokola UDP
  - enak princip delovanja kot IP
- Značilnosti protokola TCP
  - vzpostavitev zveze
  - brez varnostnih mehanizmov
- Napadi na TCP/IP
  - DoS (ICMP poplavljanje, TCP syn, UDP flood)
  - prisluškovanje komunikacijskemu kanalu
  - IP spoofing
  - napadi na DHCP, poplavljanje ARP

Glava paketa IPv4



Sodobna omrežja



Pasti javnih omrežij

- Prisluškovanje komunikacijskemu kanalu in prestrezanje informacij
  - sniffing, snooping
- Ponarejanje informacij
- Pretvarjanje
  - spoofing
- Onemogočanje uporabe virov omrežja
  - Denial of service, DDoS
- Nepooblaščena uporaba virov omrežja
- Nepooblaščeno razkrivanje informacij
- Delitev nevarnosti:
  - notranje
    - 80 % vdorov se zgodi znotraj omrežja (Computer Security Institute – 2002)
  - zunanje

Koncept zagotavljanja varnosti

- **V fizičnem svetu:**
  - osebni dokument s sliko, geslo, podpis
  - zaupni pogovori, zapečatena pisma
  - ključavnice, video nadzor
  - ograja, vrata, ključavnica
- **V elektronskem svetu:**
  - tehnike digitalnega podpisovanja, certifikati, gesla, zgoščevalne funkcije
  - šifriranje
  - filtriranje prometa, sistemi AAA
  - stikalo, usmerjevalnik, požarni zid, sistem IDS

⟵	overjanje integriteta
⟵	zasebnost
⟵	omejevanje dostopa
⟵	naprave

Varnostne storitve

- Avtentikacija uporabnikov, naprav/aplikacij (Authentication)
  - zajamči točnost izvora podatkov z vidika, kdo in od kod
- Nadzor dostopa (Access Control)
  - preprečuje neavtoriziran dostop do omrežnih virov/storitev
- Zaupnost/zasebnost podatkov (Confidentiality)
  - preprečuje prebiranje in kopiranje podatkov, ko se prenašajo prek javnega omrežja
- Celovitost/avtentičnost podatkov (Integrity)
  - zagotavlja, da podatki niso bili kakor koli spremenjeni od svojega nastanka
- Nezatajljivost (Non-repudiation)
  - onemogoča zanikanje izvora podatkov ter vključenost v opravljane storitve
- Preprečevanje onemogočanja dostopa do virov in storitev
  - omrežni viri oziroma storitve morajo biti uporabnikom na razpolago vedno, kadar jih ti želijo uporabiti
- Časovni žigi (Timestamping)
- Zagotavljanje avtorskih pravic

Varnostni koncepti v Ethernet in TCP/IP

- Implementacija varnostnih funkcij na omrežnih elementih
  - Filtri na stikalih in usmerjevalnikih – “stateless” filtri
  - Požarne pregrade – “stateful” filtri
  - Proxy naprave in aplikacijski prehodi – emulacija odjemalcev
  - Naprave IDS/IPS – detekcija nelegitimnih omrežnih operacij
- Zaščita na nivoju transportnih protokolov
  - HTTPS, SSH, S-MIME, PGP
  - TLS/SSL
  - IPSec
  - WPA2
- Zaščita vsebin na nivoju aplikacij
  - Sistemi DRM, CA

Kazalo

- Varnostne storitve
- **Varnostni mehanizmi**
- Protokol IPSec

Kazalo – varnostni mehanizmi

- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Kriptologija

- Znanost o prevajanju nezaščitenih podatkov v zaščitene in obratno
- Delitev
  - kriptografija
    - metode za šifriranje in zakrivanje podatkov
  - kriptoanaliza
    - metode za razkrivanje šifriranih podatkov

Razvoj kriptografije

- ~ 2000 p. n. št. – Egipčani
- 1970: začetki ˝digitalne˝ kriptografije
  - IBM – g. Feistel
- 1976: dokument ˝New Directions in Cryptography˝
  - g. Diffie in g. Hellman
  - kriptografija na osnovi javnih ključev
- 1977: standard DES (Data Encryption Standard)
- 1978: postopek RSA
  - g. Rivest, g. Shamir in g. Adleman
  - prvi praktično delujoči asimetrični kriptografski postopek
- 1985: ElGamal
- 1991: prvi mednarodni standard za digitalno podpisovanje dokumentov (ISO/IEC 9796)
  - temelji na algoritmu RSA

Cezarjev algoritem

- Premik abecede za določeno število znakov
- Primer: šifriranje ukaza NAPAD (čistopis)

Postopek enkripcije:

$$f(a) \mapsto (a-k) \bmod 25$$

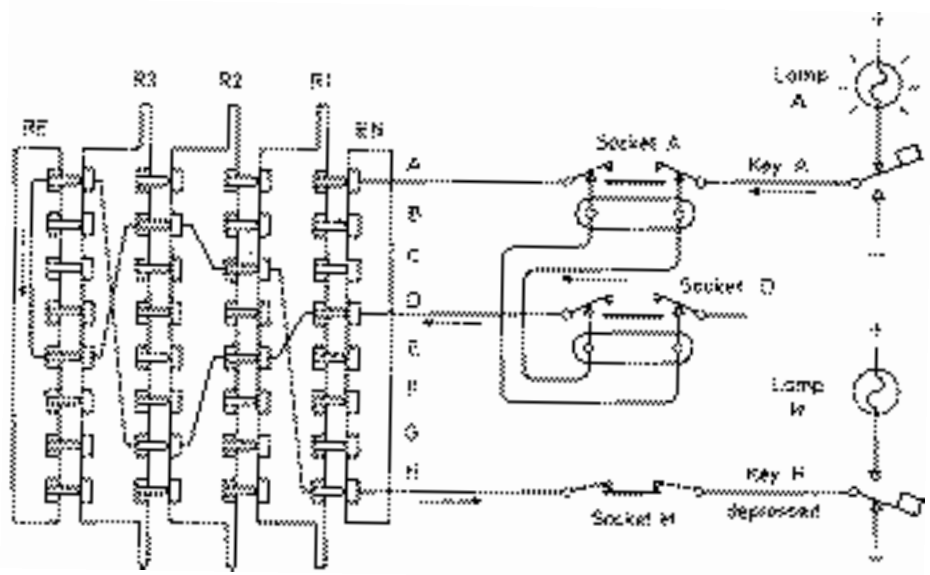
KVMVB

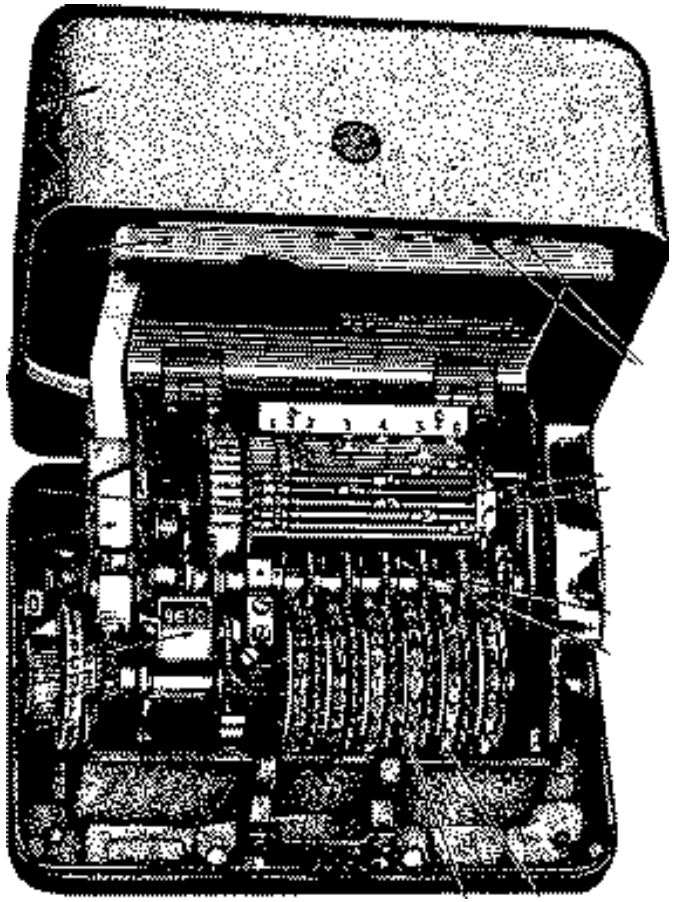
(kriptogram)

ključ: $k = 3$

- Vaja: šifrirajte svoje IME in PRIIMEK

Enigma Rotor Machine

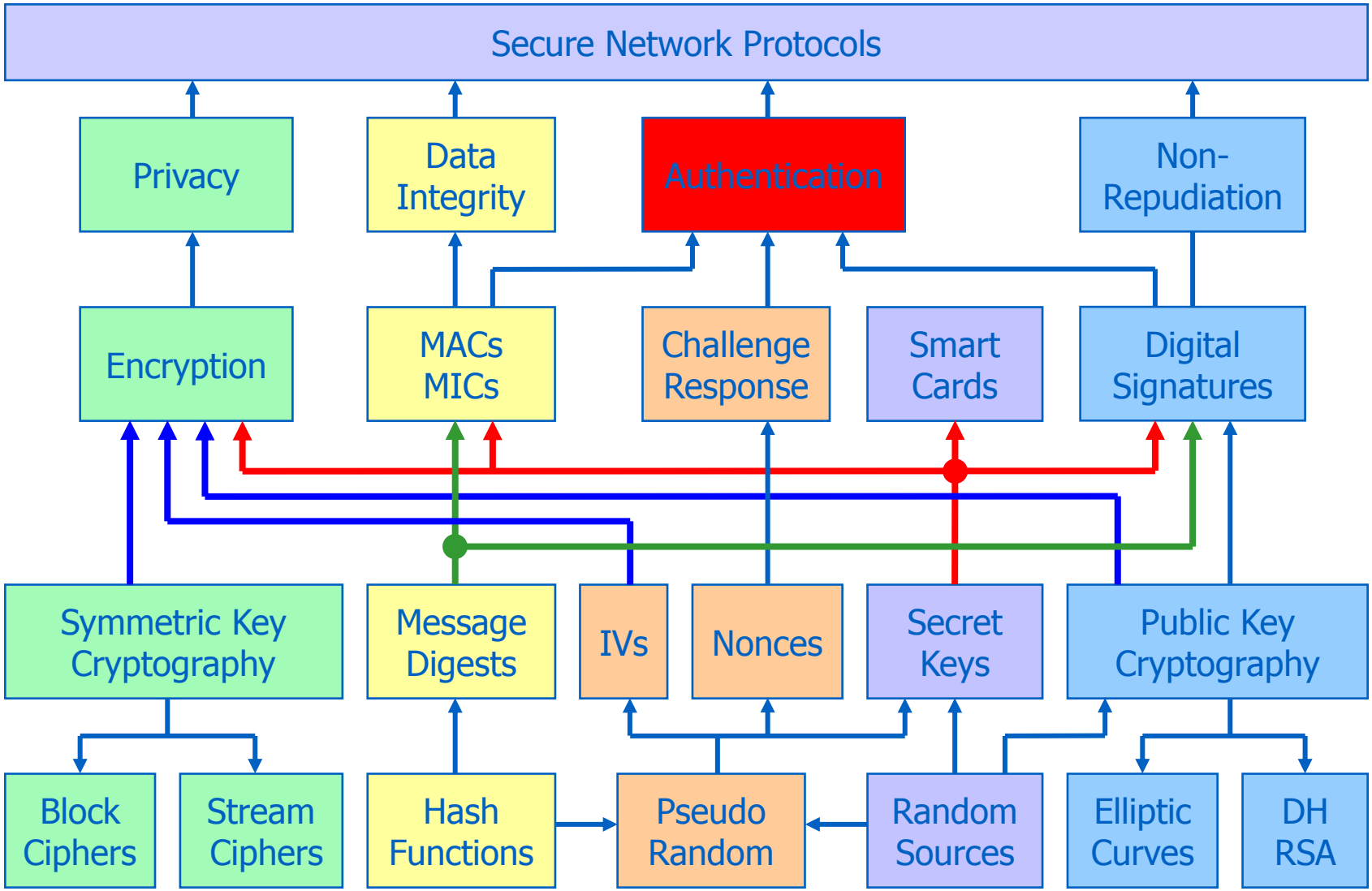




Delitev varnostnih mehanizmov

- Mehanizmi za enkripcijo
  - simetrični
  - asimetrični
  - hibridni
- Mehanizmi za zagotavljanje celovitosti
- Mehanizmi za elektronsko podpisovanje
- Mehanizmi za izmenjavo ključev
- Mehanizmi za nadzor dostopa
  - avtentikacija
  - avtorizacija
  - beleženje
- Mehanizmi za zaznavanje vdorov

Delitev varnostnih mehanizmov



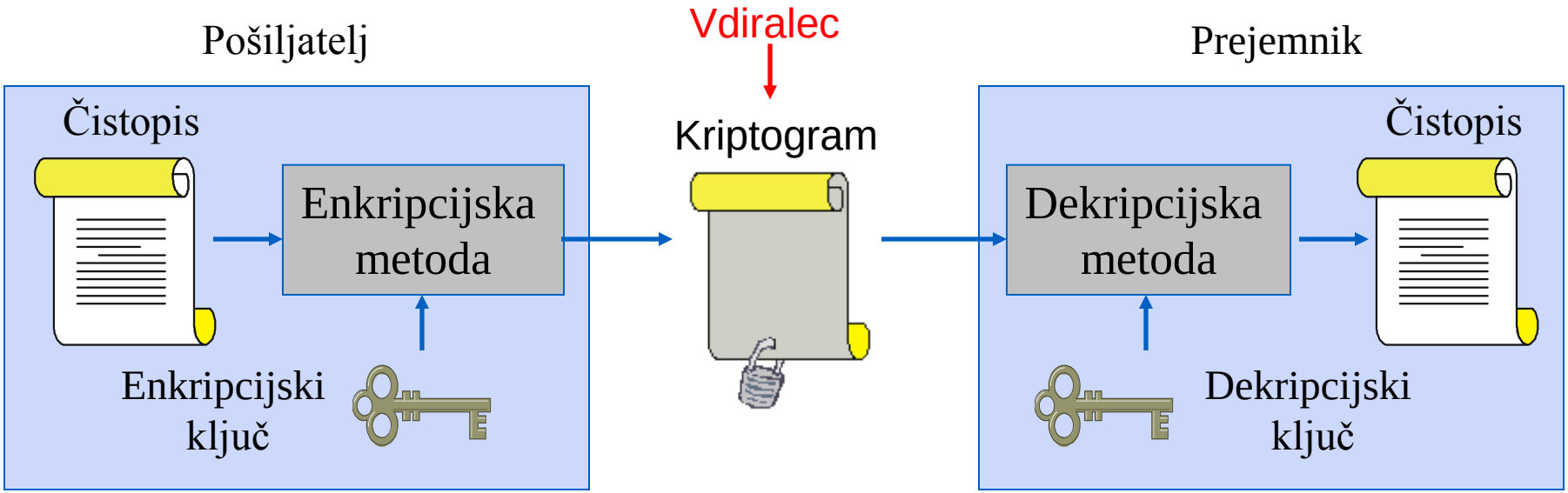
Vir: *Zurcher Hochschule Winterthur*

Kazalo – varnostni mehanizmi

- Uvod
- **Enkripcijski algoritmi**
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Enkripcija

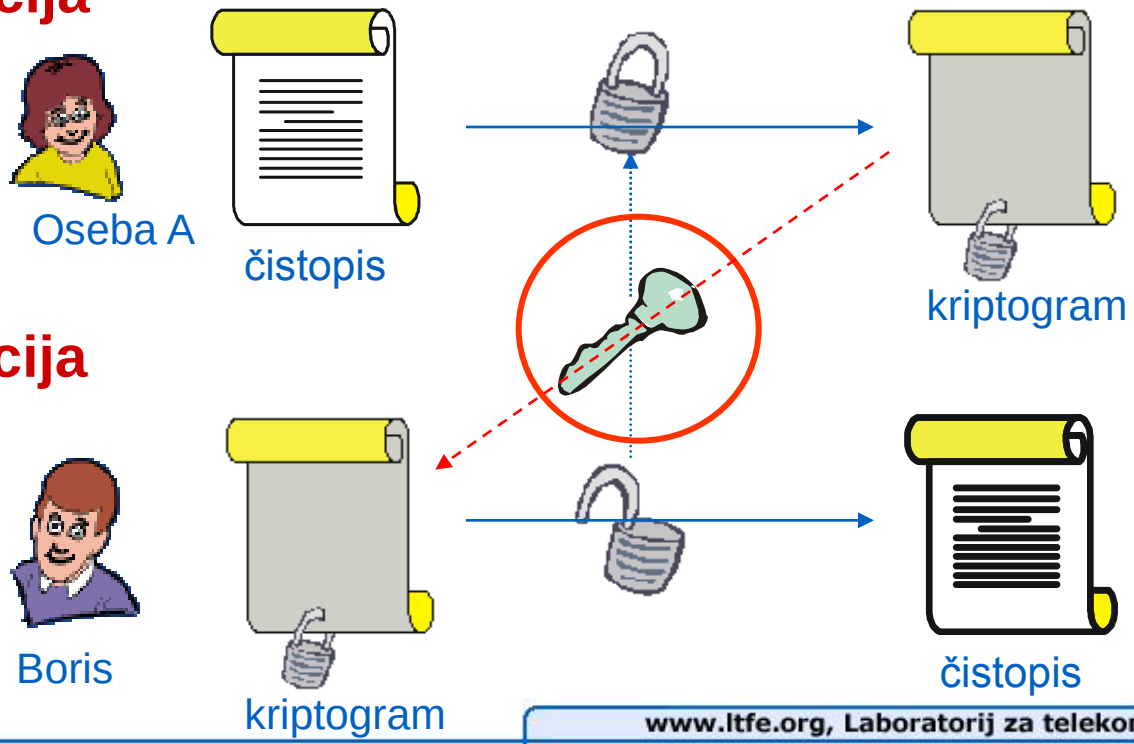
- Enkripcija/šifriranje je spreminjanje berljivih podatkov ˝čistopis˝ v obliko ˝kriptogram˝, ki onemogoča njihovo razumevanje
- V preteklosti so bile enkripcijske metode tajne
- Danes uporabljane enkripcijske metode so javne, stopnja zaščite je odvisna le od dolžine ključa



Simetrični postopki

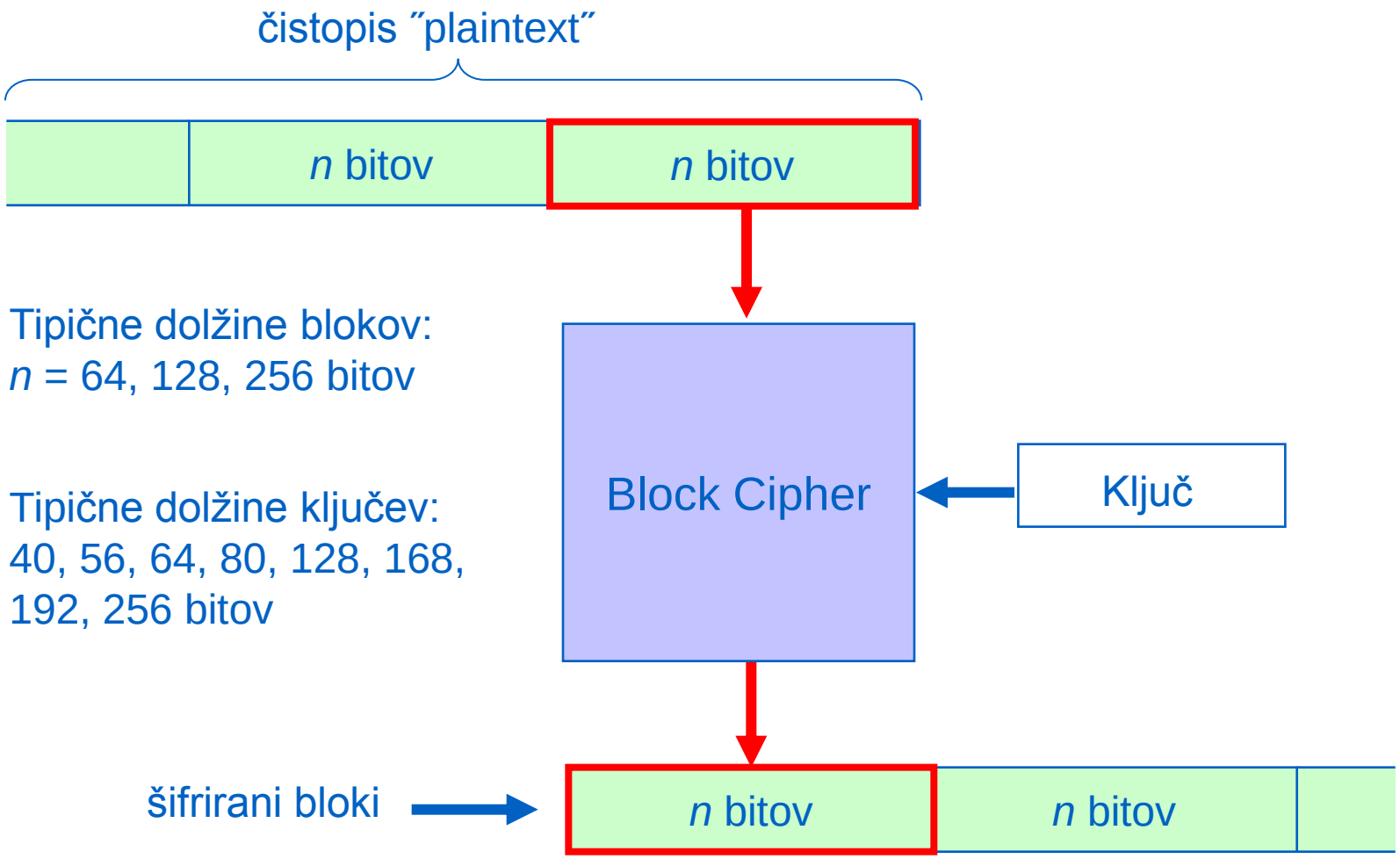
- Za komunikacijo med dvema osebama se uporablja samo en ključ
  - enak ključ za enkripcijo in dekripcijo
- Ključ mora pošiljatelj podatkov na varen način posredovati naslovniku

1. **Enkripcija**
2. **Dekripcija**



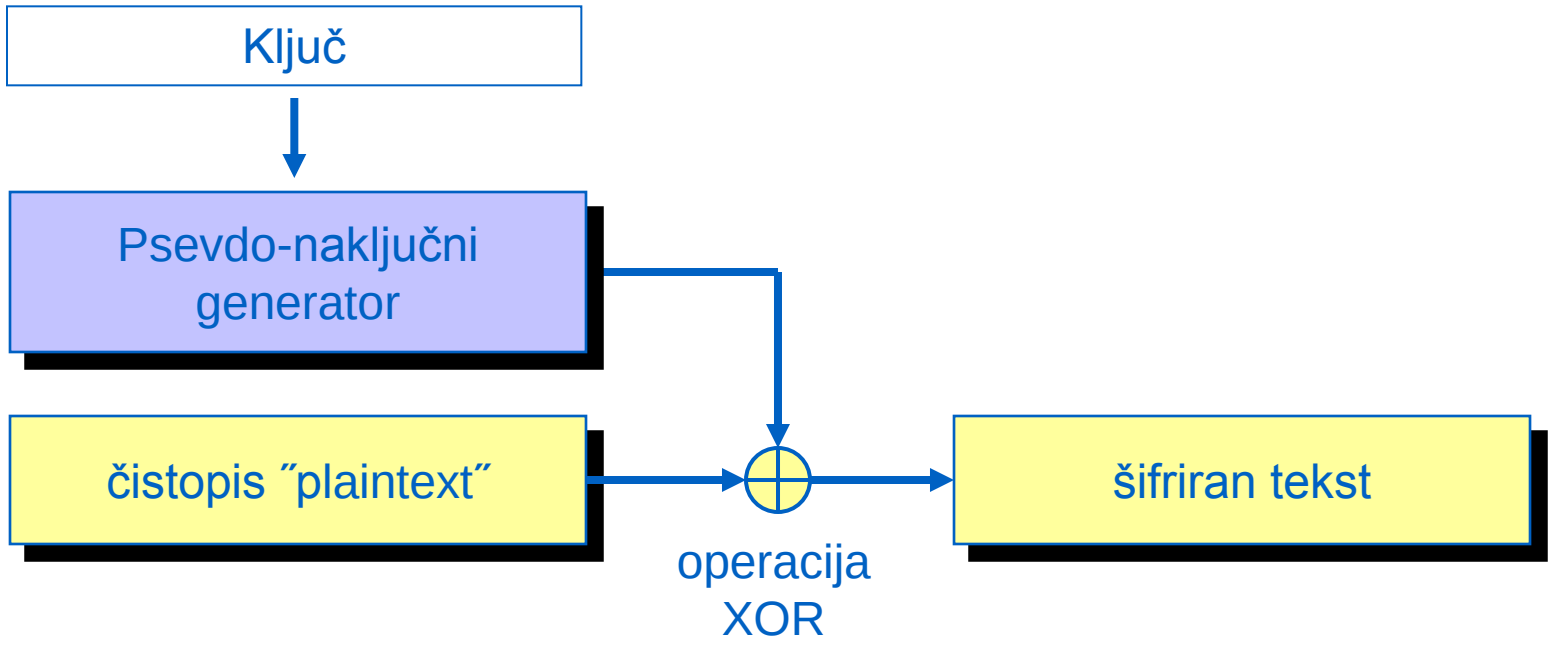
Simetrični postopki – Block Cipher

- **Princip delovanja**



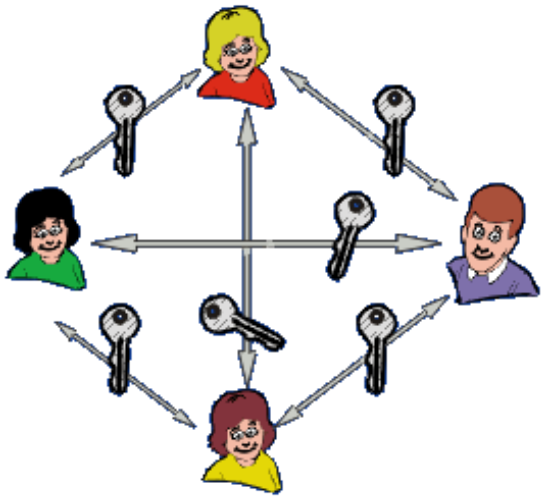
Simetrični postopki – Stream Cipher

- **Princip delovanja**

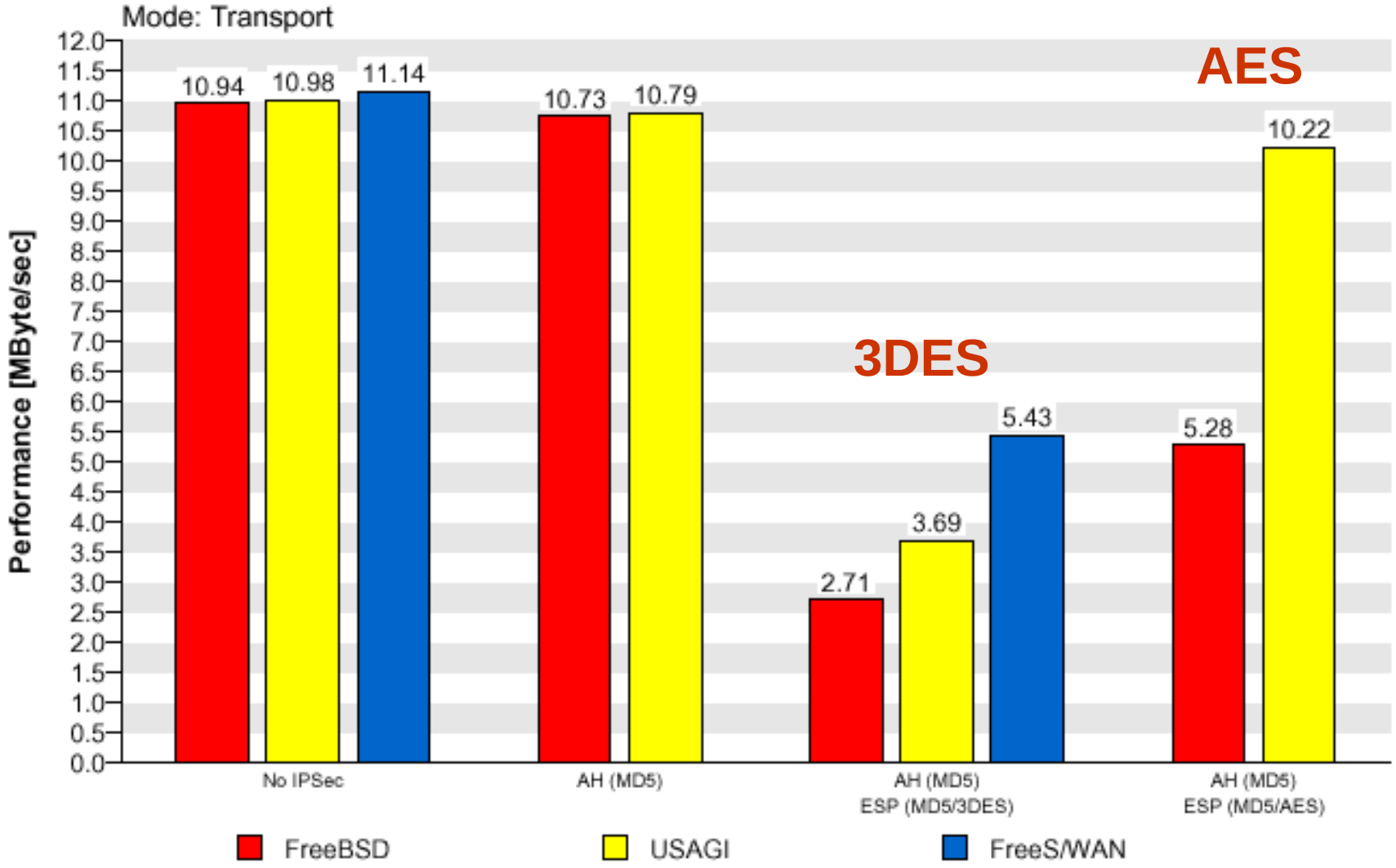


Lastnosti simetričnih postopkov

- Prednosti
  - hitrost
- Slabosti
  - težave z “varno” izmenjavo ključa med pošiljateljem in naslovnikom
  - kopičenje ključev: drugačen ključ za vsakega novega “sogovornika”
- Primeri algoritmov
  - DES (Data Encryption Standard)
    - dolžina ključa 56 bitov
  - 3DES
    - dolžina ključa 168 bitov (učinkovita 112 bitov)
  - AES (Advanced Encryption Standard)
    - dolžina ključa 128, 192, 256 bitov
  - RC2, RC4, RC5 (Rivest’s Cipher)
    - variabilna dolžina ključev
  - IDEA (International Data Encryption Algorithm)
    - dolžina ključa 128 bitov
  - enkratni ščit (velikost ključa enaka dolžini podatkov)



Primerjava algoritmov 3DES in AES



Vir: C. Karg, Research Establishment for Applied Science
http://www.dodccrp.org/Activities/Symposia/7thICCRTS

Asimetrični postopki

- Kriptografija z javnim ključem
- ″Odpravlja″ problem varne izmenjave ključev in kopičenja ključev simetričnega šifriranja
- Razvila sta ga Diffie in Hellman, algoritem je javno dostopen od leta 1976
- Enkripcijski in dekripcijski ključ sta različna
  - javni ključ uporabljen za šifriranje
  - zasebni ključ uporabljen za dešifriranje

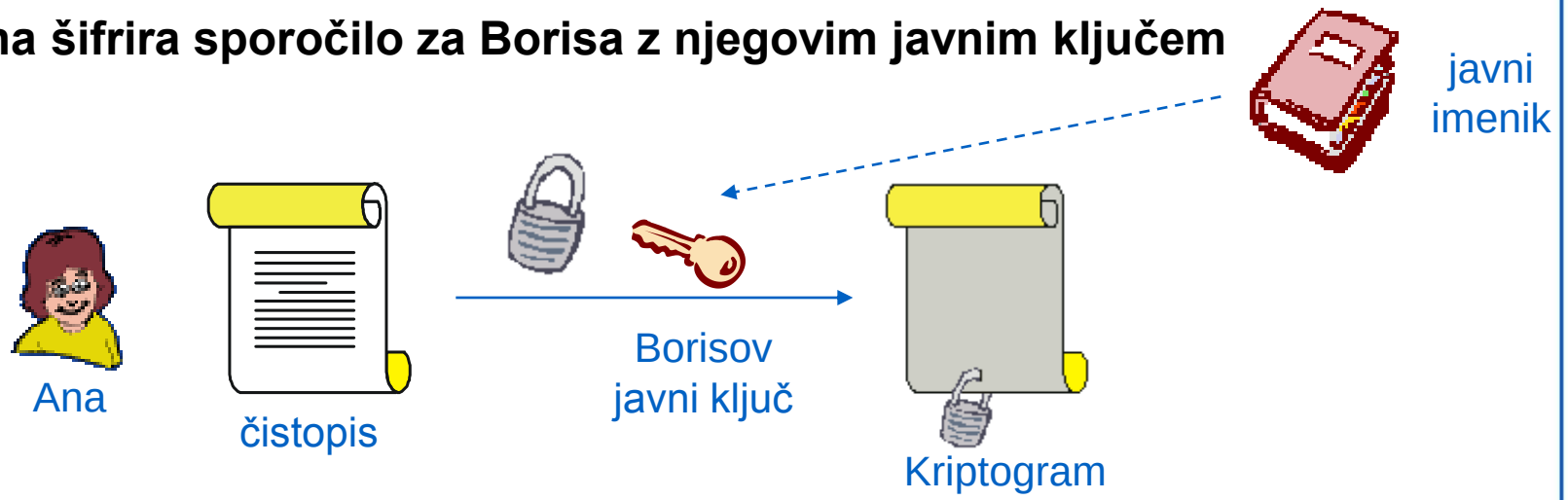
par ključev za enkripcijo

javni ključ
za enkripcijo

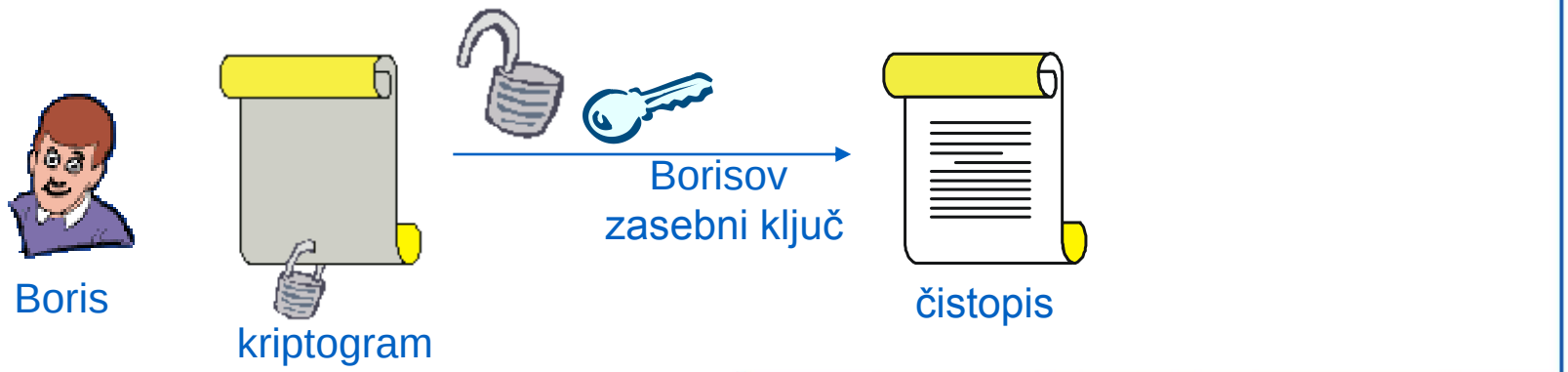
zasebni ključ
za dekripcijo

Asimetrični postopki

- **Postopek šifriranja**
  - **Ana šifrira sporočilo za Borisa z njegovim javnim ključem**



- **Postopek dešifriranja**
  - **Boris dešifrira sporočilo s svojim zasebnim ključem**



Lastnosti asimetričnih postopkov

- Ključa sta enoumno povezana
- Če poznamo javni ključ, je praktično nemogoče matematično izračunati zasebnega
- Vsak posameznik ima svoj par ključev, od katerih je eden javni, drugi pa zasebni
- Ključa izvajata inverzni operaciji
  - eden enkripcijo, drugi dekripcijo
- Če je en ključ v paru uporabljen za enkripcijo, potem ne more biti isti ključ uporabljen tudi za dekripcijo

Lastnosti javnega in zasebnega ključa

- Lastnosti javnega ključa
  - javno dostopen
  - vedno je povezan z določeno osebo/terminalom/aplikacijo
    - lastnikom para ključev
  - ponavadi je objavljen v javnem imeniku
- Lastnosti zasebnega ključa
  - ima ga samo lastnik
  - vedno je povezan z določeno osebo/terminalom/aplikacijo
    - lastnikom para ključev
  - lastnik je odgovoren skrbeti za varno hranjenje ključa
- Primeri
  - Diffie-Hellman
    - dolžina ključa 512, 768, 1024, 2048
  - RSA
    - dolžina ključa 512, 1024, 2048, 3072, 4096
  - algoritmi na osnovi eliptičnih krivulj
    - dolžina ključa 112, 160, 224, 256, 384, 512

Primerjava postopkov

- **Simetrični postopki**
  - hitrost
  - primerni za zaščito lokalno shranjenih podatkov
  - težave z izmenjavo ključev
  - število ključev narašča z $N(N\text{-}1)/2$
    - problem N^2
- **Asimetrično postopki**
  - enostavna izmenjava ključev
  - število ključev narašča linearni
  - počasnost
  - kompleksnost algoritmov
  - problem generiranja naključnih praštevil

Primerjava dolžine ključev 1/2

- Priporočilo – RSA Laboratories (6 maj, 2003)
  - tehnologija iz leta 1996 (vredna 10 M $) je omogočala razbiti 56 bitni ključ DES v 6 minutah
  - tehnologija iz leta 2003 (vredna 10 M $) je omogoča razbiti 56 bitni ključ DES v 14 sekundah
    - Moor-ov zakon – hitrost strojne obdelave/$ se podvoji vsakih 18 mesecev
- Primerjava dolžine asimetričnih in simetričnih ključev (algoritma RSA in DES)
  - 1024-bitni asimetrični ekvivalenten 80-bitnem simetričnem
    - uporaben za podatke, ki potrebujejo učinkovito zaščito do leta 2010
  - 2048-bitni asimetrični ekvivalenten 112-bitnem 3DES
    - uporaben za podatke, ki potrebujejo učinkovito zaščito do leta 2030
  - 3072-bitni asimetrični ekvivalenten 128-bitnem simetričnem
    - uporaben za podatke, ki potrebujejo učinkovito zaščito po letu 2030

Primerjava dolžine ključev 2/2

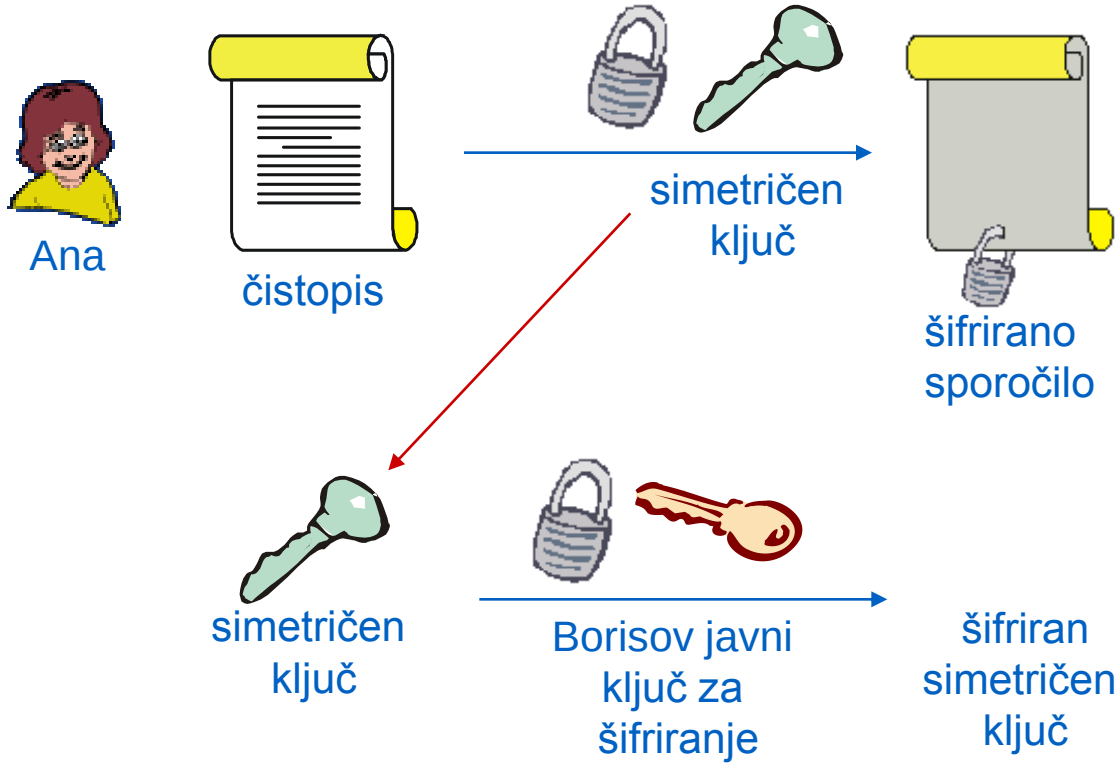
Postopek/dolžina ključa	K[bit]	K[bit]	K[bit]	K[bit]	K[bit]	K[bit]
Simetrični	56	80	112	128	192	256
Asimetrični (RSA)	512	1024	2048	3072	7680	15360
Asimetrični (na osnovi eliptičnih krivulj)	112	160	224	256	384	512
Razmerje RSA/eliptični	5:1	6:1	9:1	12:1	20:1	30:1

Hibridni postopki

- Kombinacija simetričnih in asimetričnih postopkov
- Za enkripcijo se uporablja simetrični postopek (hitra enkripcija)
- Za izmenjavo ključev simetričnega postopka pa se uporablja asimetrični postopek (varna izmenjava ključev)
- Primer uporabe:
  - PGP (Pretty Good Privacy)

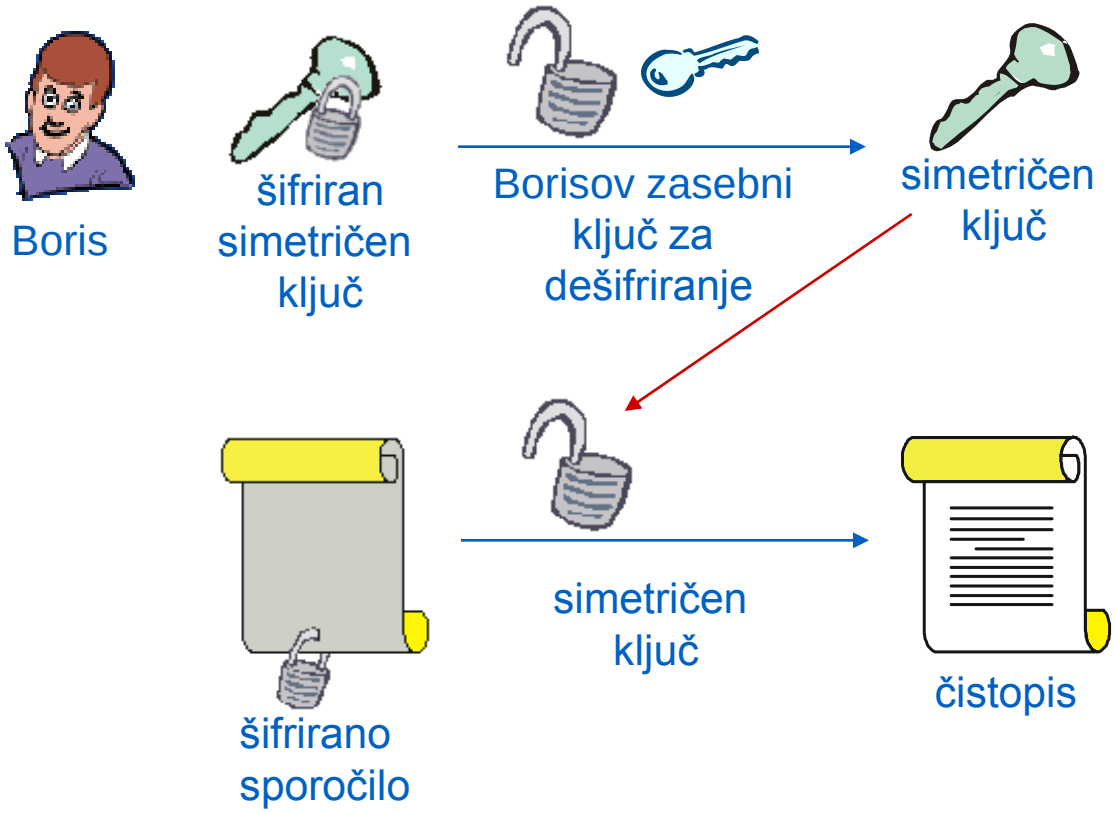
Hibridni postopki 1/2

- **Šifriranje**
  - **Ana šifrira sporočilo za Borisa s simetričnim ključem**
  - **simetričen ključ šifrira z Borisovim javnim ključem**
  - **Ana pošlje Borisu šifrirano sporočilo in šifriran simetrični ključ**



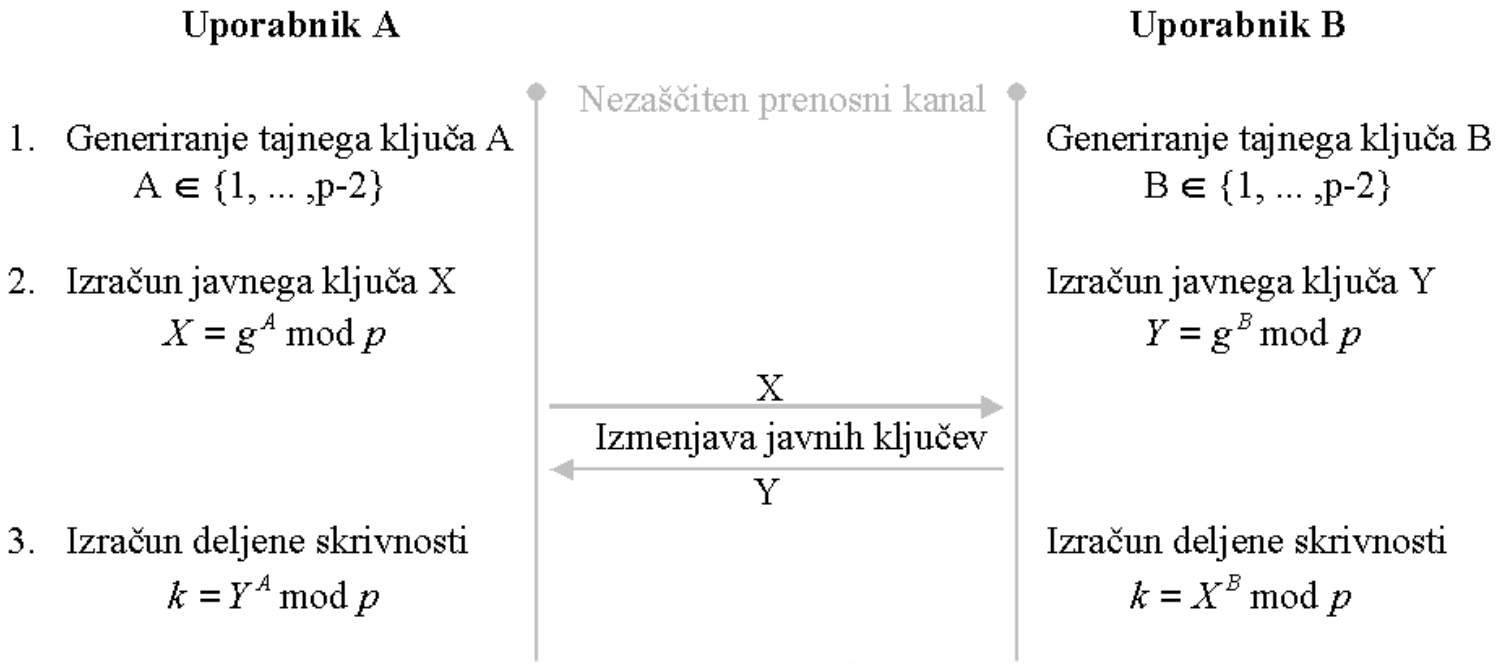
Hibridni postopki 2/2

- **Dešifriranje**
  - **Boris dešifrira simetričen ključ s svojim zasebnim ključem**
  - **z dešifriranim simetričnim ključem dešifrira sprejeto sporočilo**



Algoritem Diffie-Hellman

- **Omogoča varno izmenjavo tajnega ključa brez predhodno izmenjanih skrivnosti**
  - **algoritem definira dva parametra *p* in *g*, ki sta javna**
    - ***p* – praštevilo**
    - ***g* – celo število manjše od p; za vsak *n* = [1, ..., *p*-1] mora obstajati število *k*, da velja enačba** $n = g^k \bmod p$
- **Ranljiv na napad ˝man-in-the-middle˝**



Kazalo – varnostni mehanizmi

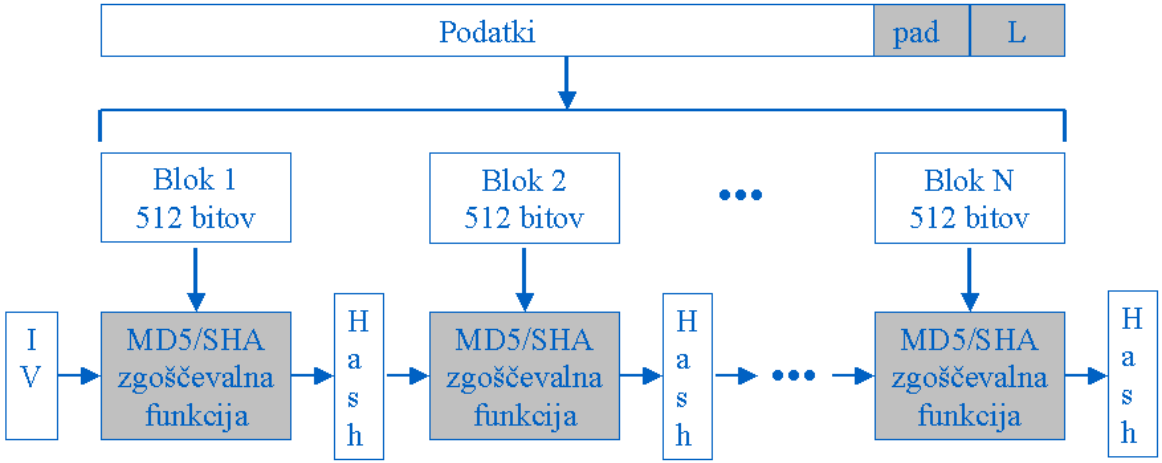
- Uvod
- Enkripcijski algoritmi
- **Zgoščevalni algoritmi**
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Zgoščevalni postopki

- **Zgoščevalni postopek (*One-way Hash Function*) preslika poljubno dolg niz znakov v blok konstantne dolžine, ki predstavlja nekakšen "prstni odtis" oziroma povzetek vhodnega niza (*Message Digest*)**
- **Lastnosti zgoščevalnih postopkov**
  - **nemogoče je najti dve različni sporočili, ki bi ju algoritem preslikal v enak povzetek**
  - **niz podatkov se vedno preslika v enak povzetek**
  - **iz povzetka ni mogoče dobiti originalen, vhodni niz podatkov (od tu ime "*One-way Hash Function*")**
  - **vsaka sprememba vhodnega niza povzroči spremembo povzetka**
- **Najbolj znani zgoščevalni postopki**
  - **MD5 (*Message Digest*)**
  - **SHA-1, SHA-2 (*Secure Hash Algorithm*)**

Blok diagram algoritma HASH

- Vhodne podatke razdelimo na bloke konstantne dolžine
- Zadnji blok dopolnimo do polne dolžine (*padding*)
- Obdelujemo blok za blokom
  - za obdelavo prvega bloka uporabimo zgoščevalno funkcijo in vektor
- Rezultat predstavlja zadnji povzetek (*Hash*)
  - povzetek na izhodu zgoščevalne funkcije je vedno enake dolžine



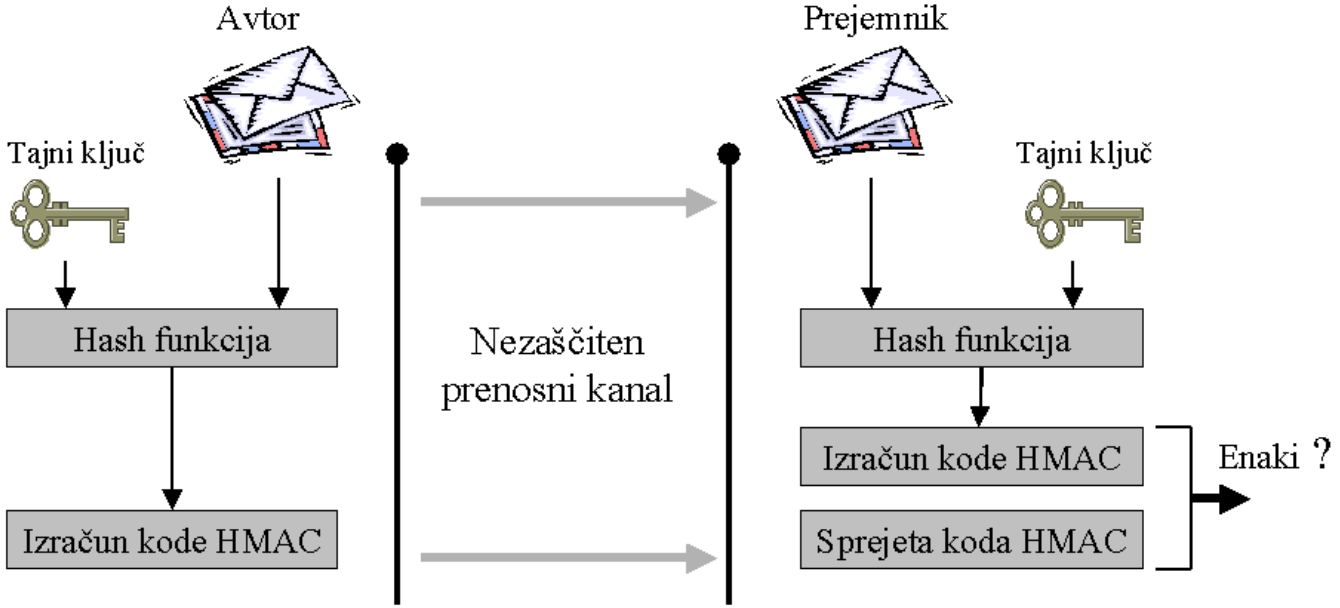
L – Dolžina vhodnih podatkov

Vektor IV – Inicializacijski vektor je standardiziran vhodni niz, katerega dolžina je odvisna od velikosti izhodnega povzetka (128/160/256/384/512 bitov)

Hash – povzetek na izhodu zgoščevalne funkcije (128/160/256/384/512 bitov)

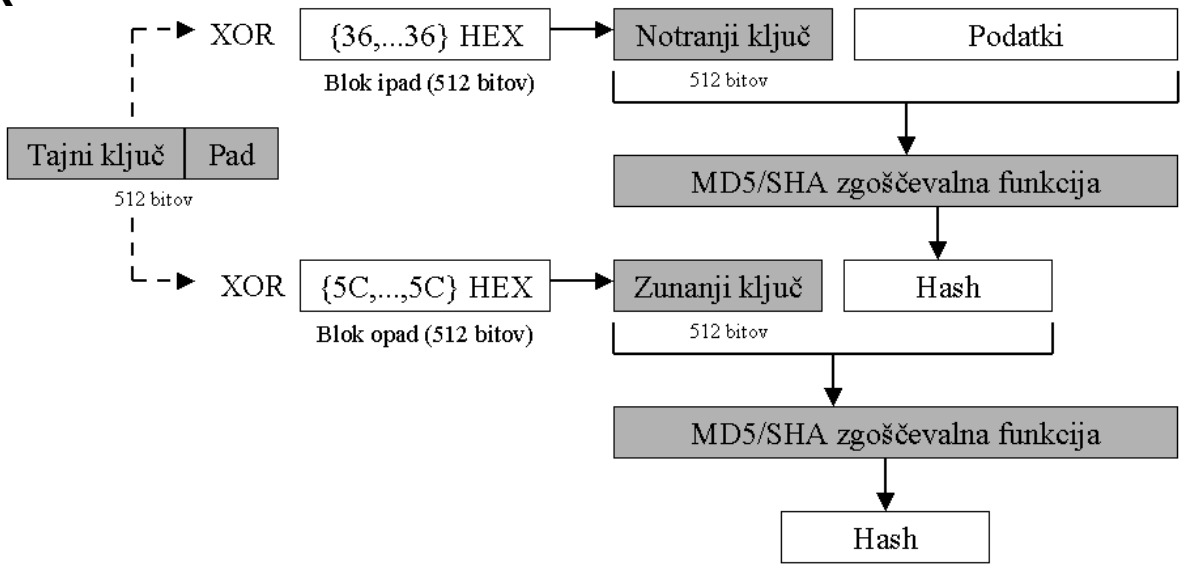
Mehanizemi MAC

- Message Authentication Codes
- Zagotavljajo celovitost podatkov na osnovi tajnega ključa
- Mehanizem HMAC (Hash MAC)
  - mehanizem MAC, ki za svoje delovanje uporablja zgoščevalne funkcije (MD5, SHA-1, SHA-2)
  - HMAC-MD5 oziroma HMAC-SHA-1
- HMAC se uporablja za zagotavljanje celovitosti podatkov



Blok diagram mehanizma HMAC

- **Princip delovanja**
  - tajni ključ razširimo do dolžine 512 bitov
  - z operacijo XOR med tajnim ključem in blokom ipad dobimo notranji ključ
  - sestavljen niz obdelamo z zgoščevalno funkcijo
  - z operacijo XOR med tajnim ključem in blokom opad dobimo zunanji ključ, ki ga dodamo vmesnemu povzetku
  - sestavljen niz ponovno obdelamo z zgoščevalno funkcijo, ki da končni povzetek



Kazalo – varnostni mehanizmi

- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Digitalni/elektronski podpis

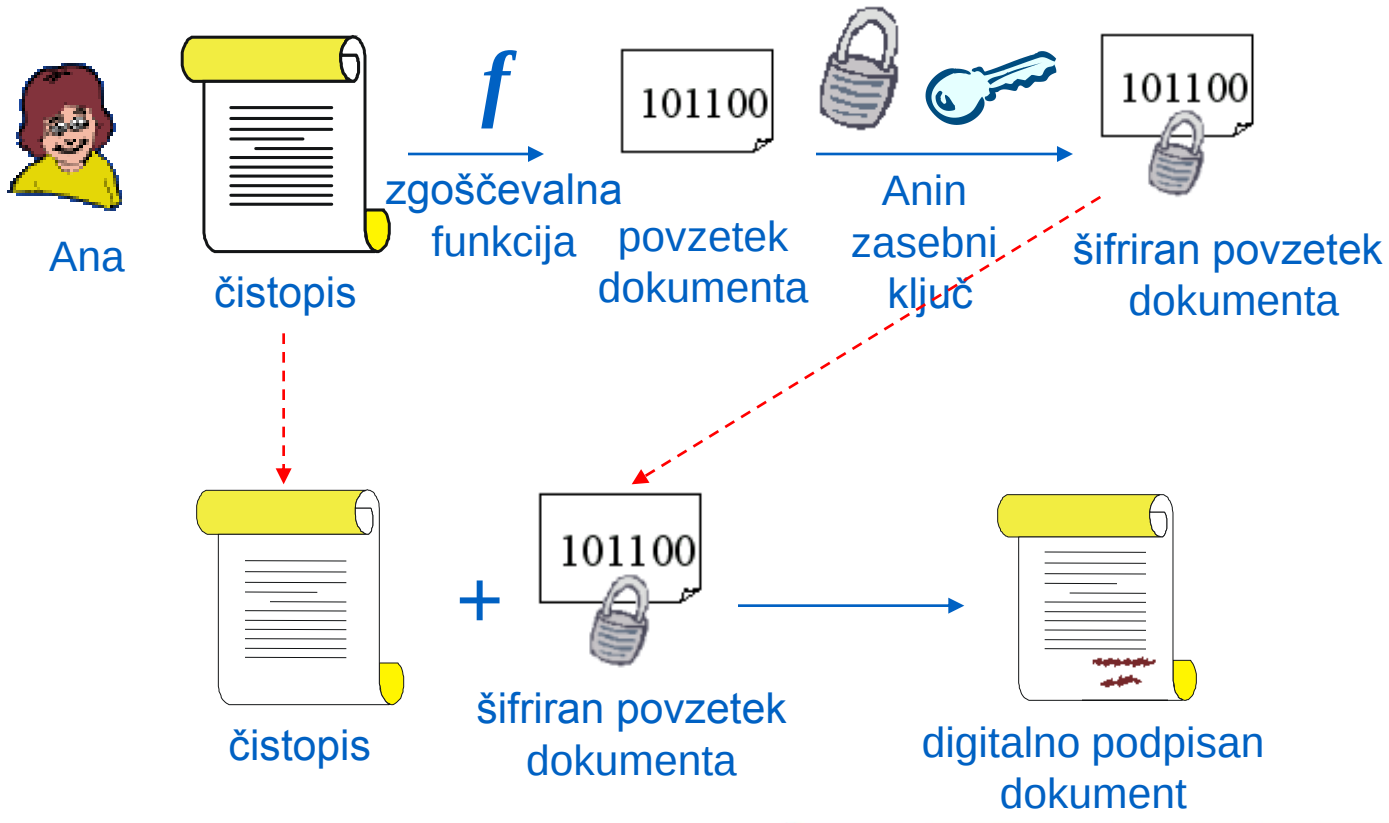
- Povzetek dokumenta (HASH) šifriran z avtorjevim zasebnim ključem (asimetrični postopek)
- Elektronski podpis omogoča:
  - overjanje
    - identificira pošiljatelja
  - celovitost
    - možnost identifikacije spremembe od trenutka, ko so podatki digitalno podpisani
  - nezatajljivost
    - podpisovalec svojega podpisa ne more zanikati
  - čas nastanka dokumenta
    - uporaba časovnih žigov
  - digitalni podpis nam ne zagotavlja zasebnosti podatkov
    - potrebna je kombinacija z enkripcijo

Digitalno podpisovanje 1/3

- **Pri digitalnem podpisovanju uporabimo postopek asimetričnega šifriranja zgoščenih podatkov ravno v obratnem vrstnem redu**
  - **izkorišča lastnosti šifriranja z javnim ključem, ki omogoča, da podatke šifriramo tudi z zasebnim ključem in dešifriramo z javnim ključem**
  - **izračunamo povzetek podatkov (zgoščevalni algoritem)**
  - **povzetek podatkov podpisovalec šifrira z lastnim zasebnim ključem → digitalni podpis**
  - **verodostojnost prejetih podatkov prejemnik preveri z javnim ključem pošiljatelja**

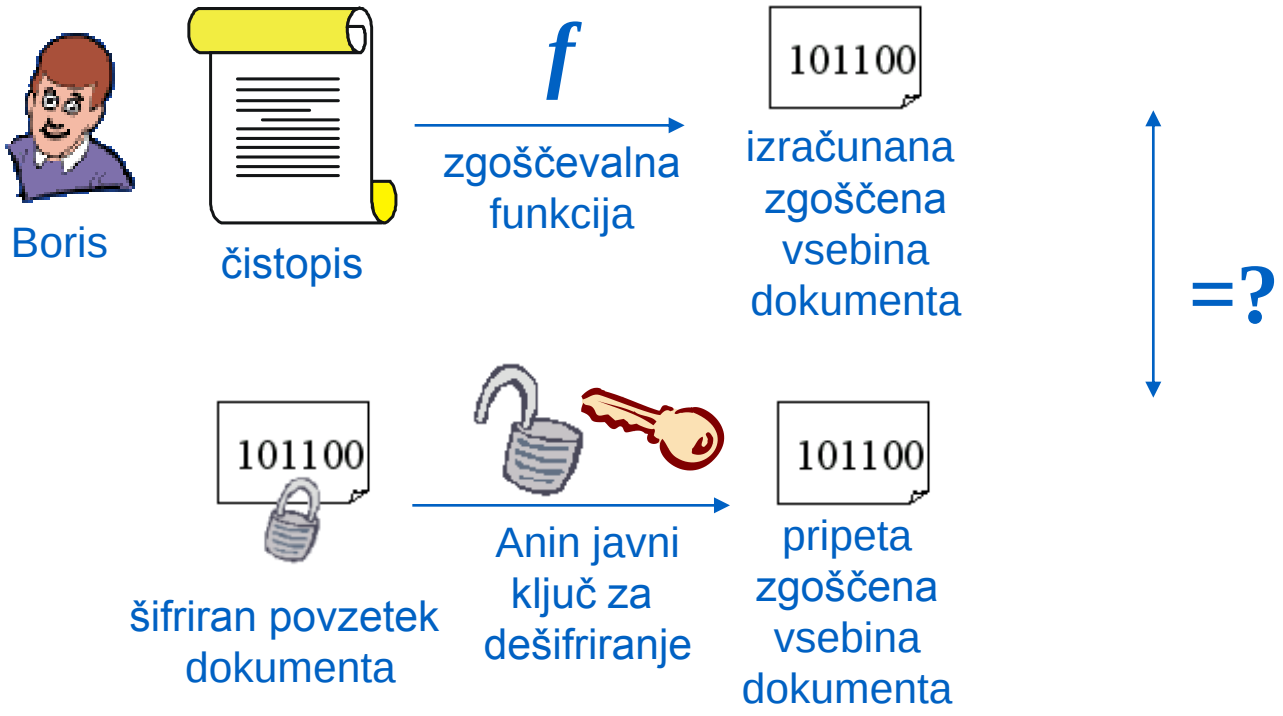
Digitalno podpisovanje 2/3

- **Podpisovanje dokumenta**
  - **Ana naredi povzetek dokumenta in ga šifrira s svojim zasebnim ključem**
  - **čistopis z dodanim šifriranim povzetkom predstavlja digitalno podpisan dokument**



Digitalno podpisovanje 3/3

- **Preverjanje digitalnega podpisa**
  - **Boris iz čistopisa izračuna povzetek dokumenta**
  - **iz pripetega povzetka dobi originalni povzetek (dešifriranje pripetega povzetka)**
  - **v primeru enakosti obeh povzetkov je digitalni podpis veljaven**



Hranjenje zasebnega ključa

- Na disku
  - nikoli naj ne bo shranjen na disku v nešifrirani (plain text) obliki
  - šifriran z uporabo varnega gesla
- Na pametni kartici (Smart Card)
- Na napravah TR (Tamper-Resistant)
  - najvišja stopnja varnosti
  - onemogočen dostop do zasebnega ključa (omogočena je le uporaba ključa)
  - tipično se uporabljajo se za hranjenje zasebnih ključev overitelje

Kazalo – varnostni mehanizmi

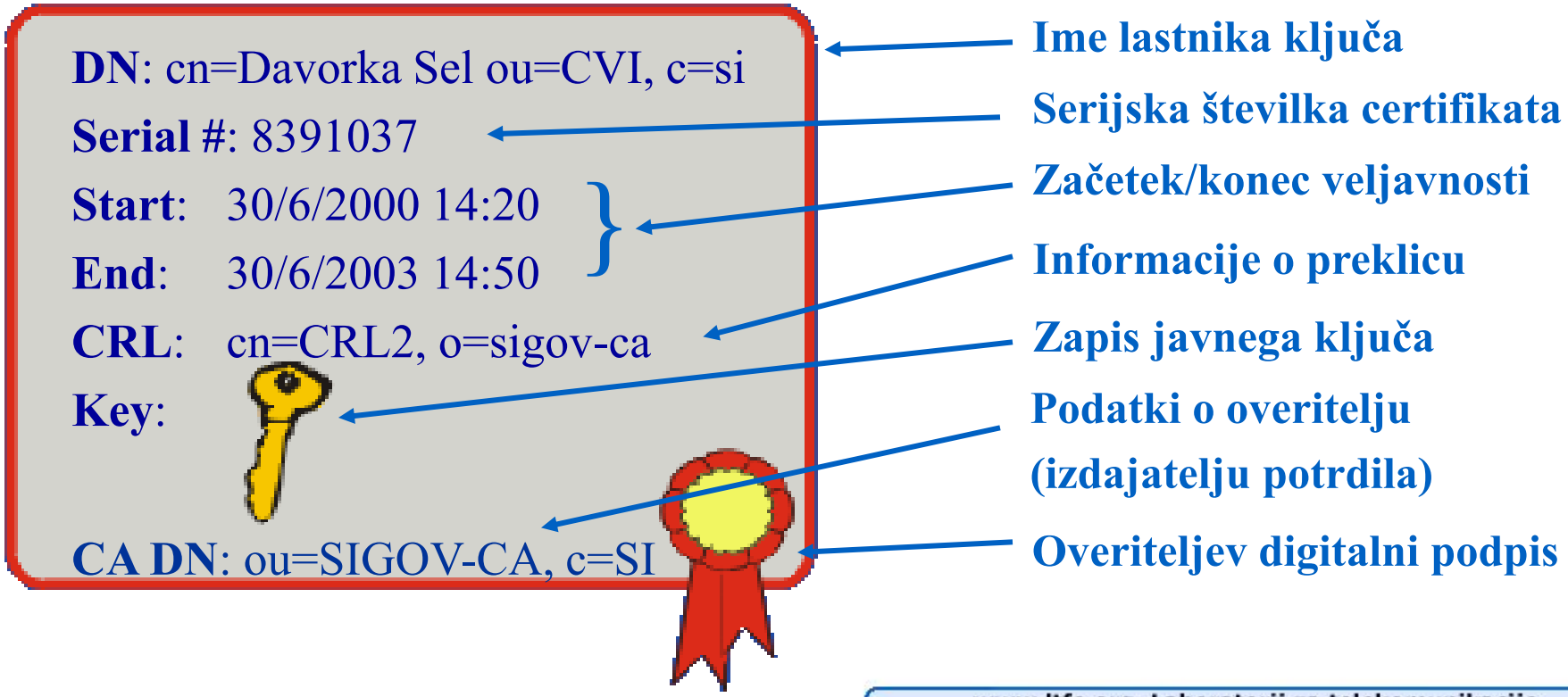
- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- **Digitalno potrdilo, Sistemi PKI**
- Sistemi AAA

Digitalna potrdila 1/3

- Digitalna potrdila (certifikati) zagotavljajo verodostojnost javnih ključev
- ISO/IEC 9594-8/ITU-T Recommendation X.509
- Digitalna potrdila vsebujejo:
  - javni ključ
  - podatke o lastniku javnega ključa
  - podpis overitelja, ki je potrdilo izdalo
  - ostale potrebne parametre
- Overitelj (CA – Certifying Authority, RA – Registration Authority) je ustanova, ki je pooblaščena za izdajanje in upravljanje z digitalnimi potrdili (javnimi ključi)
- Za uporabnike predstavlja točko zaupanja
- Overitelj jamči za istovetnost podatkov v digitalnem potrdilu o imetniku

Digitalna potrdila 2/3

- Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP)
  - **člen 15: "Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost."**

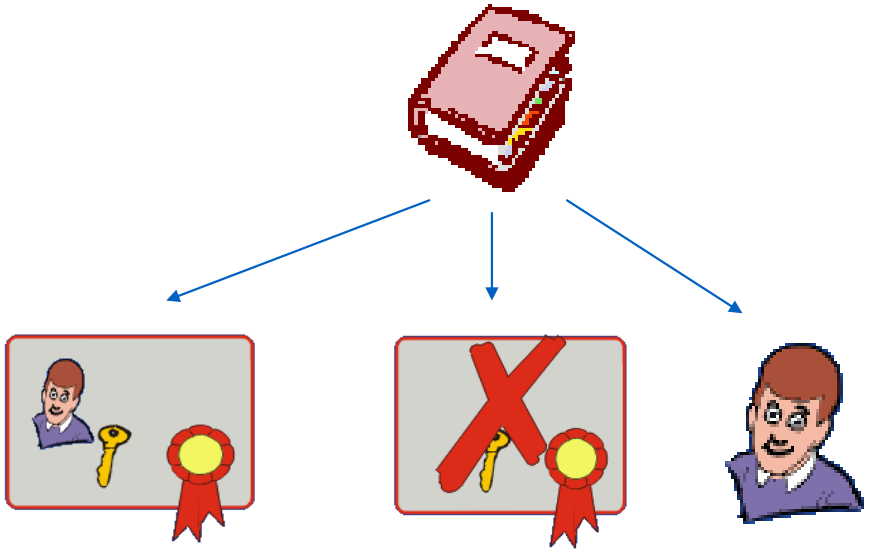


Digitalna potrdila 3/3

- Digitalno potrdilo (javni ključ) omogoča:
  - šifriranje podatkov (šifriranje z javnim ključem)
  - digitalno podpisovanje dokumentov
- S stališča celotnega koncepta varnosti v elektronskem poslovanju nam digitalna potrdila nudijo naslednje varnostne storitve
  - zaupnost, ki je zagotovljena s šifriranjem podatkov
  - overjanje pošiljatelja, zagotovljena z digitalnim podpisom
  - Nezatajljivost lastništva poslane informacije oziroma pošiljatelja
  - celovitost sporočila, kar pomeni, da samo del sporočila ni bil spremenjen ali drugače popravljen brez vednosti pošiljatelja
- Digitalno potrdilo lahko pripada različnim entitetam
  - osebi
  - organizaciji
  - podjetju
  - napravi/aplikaciji

Javni imeniki

- **Javni imeniki shranjujejo izdana potrdila**
  - **pri njih dobimo javni ključ izbranega uporabnika**
  - **vodijo seznam preklicanih digitalnih potrdil**
  - **vodijo seznam podatkov o uporabnikih, katerim so izdali digitalna potrdila**
    - **ime, priimek**
    - **elektronski naslov**
  - **vodijo evidenco o politikah delovanja z digitalnimi potrdili**



Infrastruktura javnih ključev

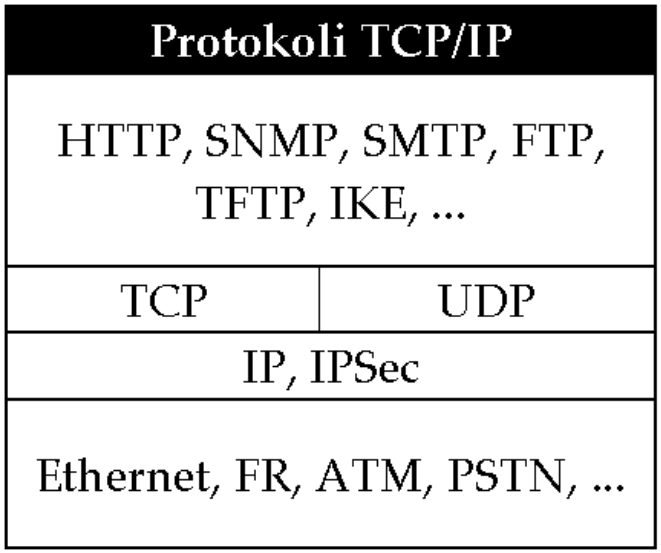
- PKI (Public Key Infrastructure)
- Koncept PKI določa
  - vrsto storitev
  - postopke ugotavljanja identitete
  - algoritme in protokole za varno upravljanje z javnimi ključi
  - koncept delovanja overitelja (Certifying Authority, Registration Authority)
- Tipične storitve, ki jih omogoča PKI
  - ugotavljanje istovetnosti entitet
  - izbira/določitev javnega ključa
  - registracija javnih ključev
    - izdaja novih certifikatov
  - preklic izdanih certifikatov
  - overjanje izdanih certifikatov

Kazalo

- Varnostne storitve
- Varnostni mehanizmi
- **Protokol IPSec**

Umestitev protokola IPSec

- **Aplikacijski sloj**
  - SSH, PGP, S/MIME, Kerberos
- **Transportni sloj**
  - SSL, TLS, WTLS
- **Omrežni sloj**
  - IPSec
- **Povezavni sloj**
  - CHAP, PPTP, L2TP, WEP (WLAN)
- **Fizični sloj**
  - Frequency Hopping, HW šifriranje



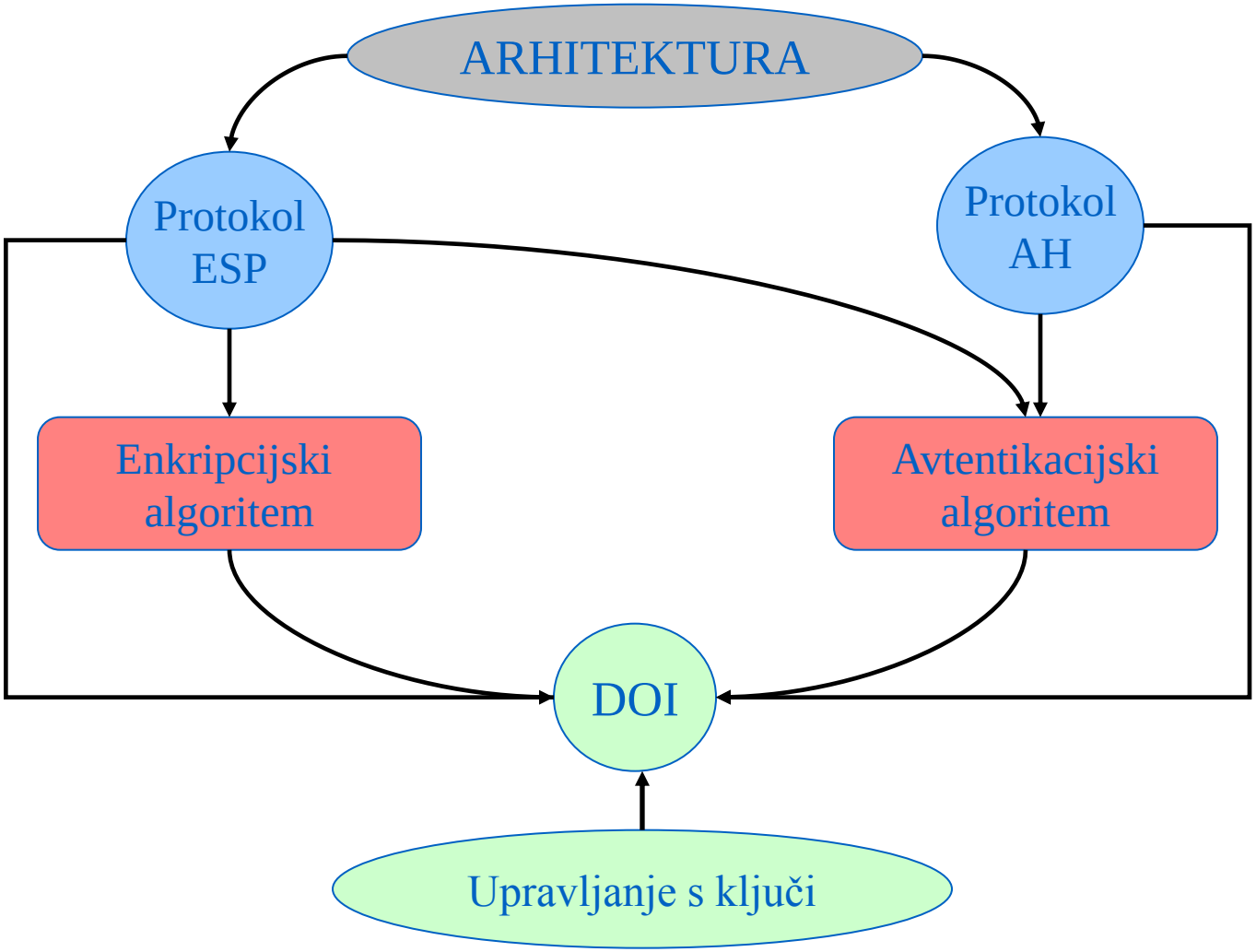
IPSec – Internet Protocol Security

- Začetek razvoja leta 1992 v IETF, kot del standarda IPv6
- Trenutno se vgrajuje v produkte, ki podpirajo IPv4
- Definiran z dokumentom RFC 2401
- Razlogi za IPSec:
  - TCP/IP nima lastnih varnostnih mehanizmov
    - zasebnost
    - celovitost podatkov
    - avtentikacija sodelujočih
- Osnovna vodila razvoja:
  - zagotoviti zaščito podatkov na omrežnem sloju
  - protokol naj bo transparenten za uporabnika in aplikacije
  - temelji naj na znanih kriptografskih mehanizmih
  - dosežen nivo varnosti naj bo odvisen le od uporabljenih kriptografskih mehanizmov
- Ključna aplikacija, za katero se danes uporablja protokol IPSec, so navidezna zasebna omrežja

Varnostne storitve

- Avtentikacija izvora podatkov
- Zaupnost podatkov
- Celovitost podatkov
- Nadzor dostopa
- Delno prekrivanje prometnega pretoka
- Zaščita pred podvajanjem datagramov IP
  - zaščita pred DoS, DDoS
- Dodatna storitev: stiskanje (kompresija) podatkov

Arhitektura



Protokola varnosti

- **Protokol AH (Authentication Header)**
  - definiran z RFC 2402
  - varnostne storitve
    - avtentikacija izvora podatkov
    - celovitost podatkov
    - zaščita pred podvajanjem paketov

  } **Avtentikacija podatkov** (HMAC-MD5, HMAC-SHA-1 ...)

- **Protokol ESP (Encapsulation Security Payload)**
  - definiran z RFC 2406
  - varnostne storitve
    - zaupnost podatkov
    - avtentikacija izvora podatkov → **Enkripcija podatkov** (DES, 3DES ...)
    - nepovezavna celovitost podatkov
    - delno prekrivanje prometnega pretoka
    - zaščita pred podvajanjem paketov

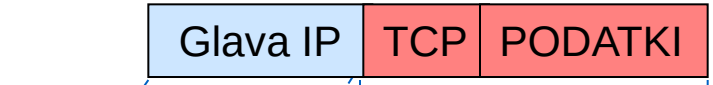
  } **Avtentikacija podatkov** (HMAC-MD5, HMAC-SHA-1 ...)

Varna zveza

- Varna zveza (SA – Security Association)
  - je enosmerna logična povezava med dvema napravama IPSec
  - zagotavlja varnostne storitve prenašanemu prometu
  - varni zvezi nudi varnostne storitve protokol AH ali ESP
    - v okviru ene varne zveze je lahko vzpostavljen le en protokol varnosti!
  - torej, v primeru dvosmerne komunikacije med napravama IPSec sta vzpostavljeni dve varni zvezi
- Varno zvezo definirajo trije parametri:
  - identifikator varnosti (SPI – Security Parameter Index)
  - naslov IP ponorne naprave
  - identifikator protokola varnosti (identifikator protokola AH oziroma ESP)
- Tipi varnih zvez oziroma prenosni načini:
  - transportni način – zaščiti podatke višje ležečih protokolov
  - tunelski način – zaščiti celoten paket IP

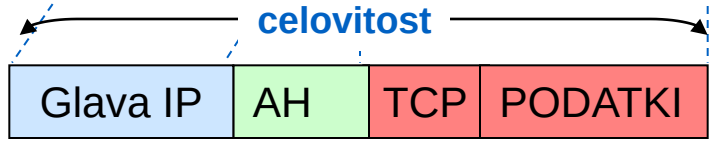
Prenosni načini

Originalni paket IP

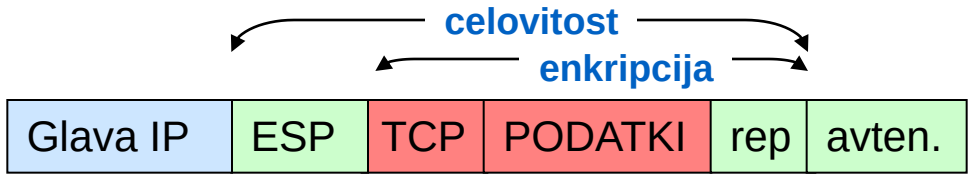


Transportni način

Protokol AH



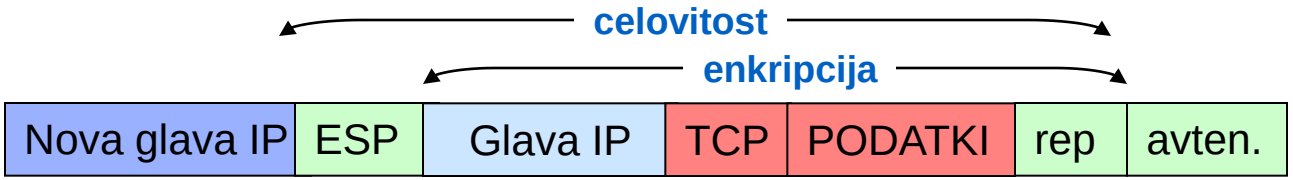
Protokol ESP



Tunelski način

Protokol AH

Protokol ESP



Naprave IPSec

- Terminali – so izvori in ponori prometa
- Varnostni prehodi – prenašajo in usmerjajo promet
- Med dvema gostiteljema je možen transportni in tunelski način prenosa

- Tunelski način prenosa je vedno obvezen, kadar je vsaj eden izmed udeležencev varne zveze varnostni prehod

Upravljanje varnih povezav

- Ročno vnesemo potrebne parametre oziroma dogovorjene vrednosti
  - identifikator varnosti, uporabljene protokole in algoritme, ključe za avtentikacijo in enkripcijo
- Avtomatsko s protokolom IKE (Internet Key Exchange)
  - definiran z RFC 2409 (v postopku standardizacije je IKEv2)
  - namenjen je za:
    - vzpostavljanje, vzdrževanje in rušenje varnih povezav IPSec
  - skrbi za:
    - avtentikacijo sodelujočih strani
    - izmenjavi enkripcijskih ključev
    - izmenjavo parametrov, ki so potrebni za vzpostavitev varnih zvez IPSec
  - princip delovanja:
    - 1. FAZA – vzpostavitev varne zveze IKE (dvosmerna povezava)
      - enkripcijski algoritem, zgoščevalni algoritem, avtentikacijska metoda, parametri za izvajanje algoritma Diffie – Hellman, ostali atributi varne zveze IKE
    - 2. FAZA – vzpostavitev varnih zvez IPSec (enosmerne povezave)
      - protokol AH oziroma ESP, enkripcijski algoritem, zgoščevalni algoritem, ostali atributi varne zveze IPSec

Princip delovanja IKE

1. PC 1 pošlje paket Varnostnemu prehodu 1

PAKET IP →

2. Varna prehoda izmenjata parametre za vzpostavitev varne zveze IKE

IKE SA ⟷ IKE FAZA 1 ⟷ IKE SA

3. Varna prehoda izmenjata parametre za vzpostavitev varnih zvez IPSec

IPSec SA ⟷ IKE FAZA 2 ⟷ IPSec SA

4. Paket potuje skozi tunelsko povezavo do PC2

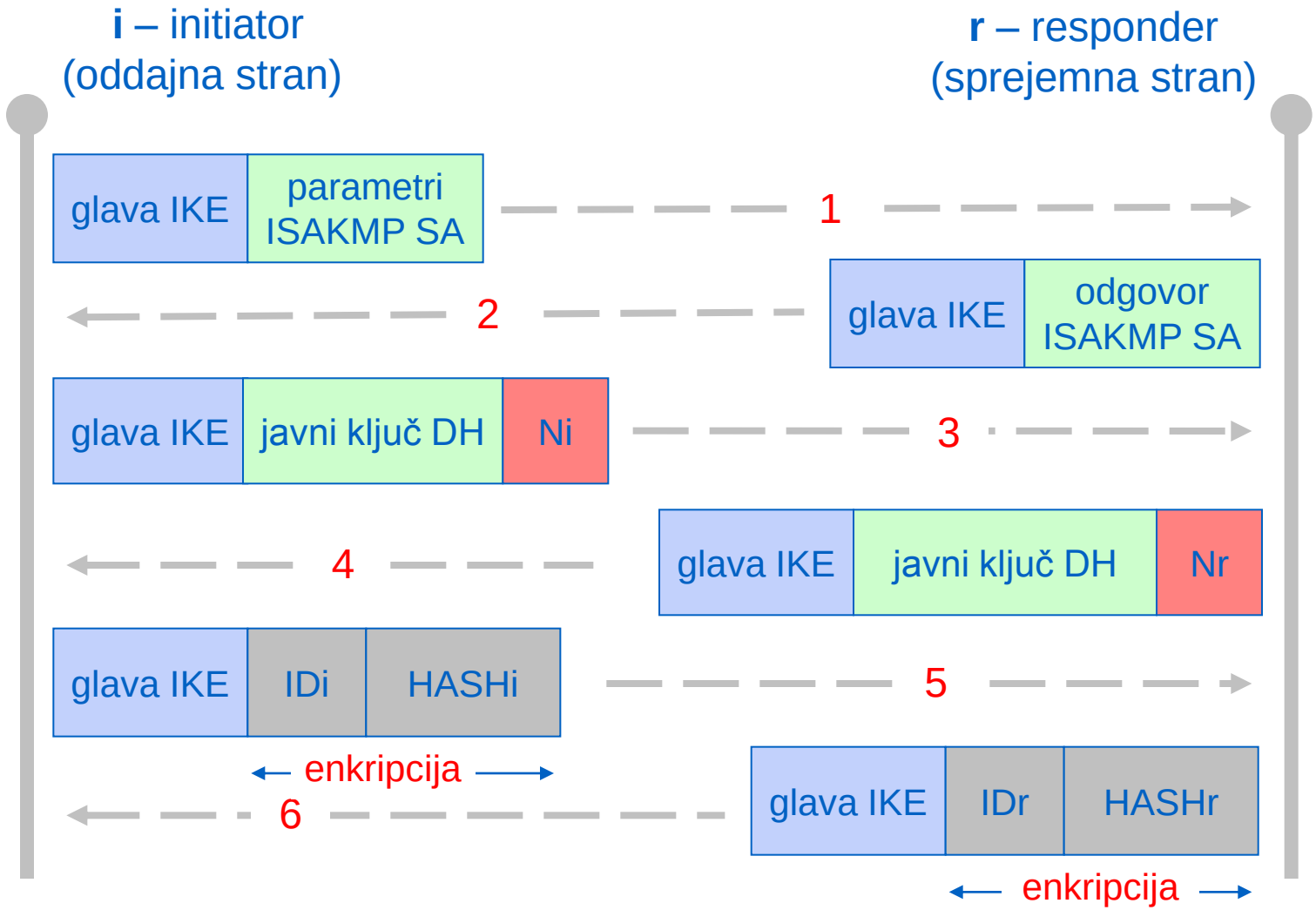
Tunelska povezava

PAKET IP →

5. Rušenje tunelske povezave

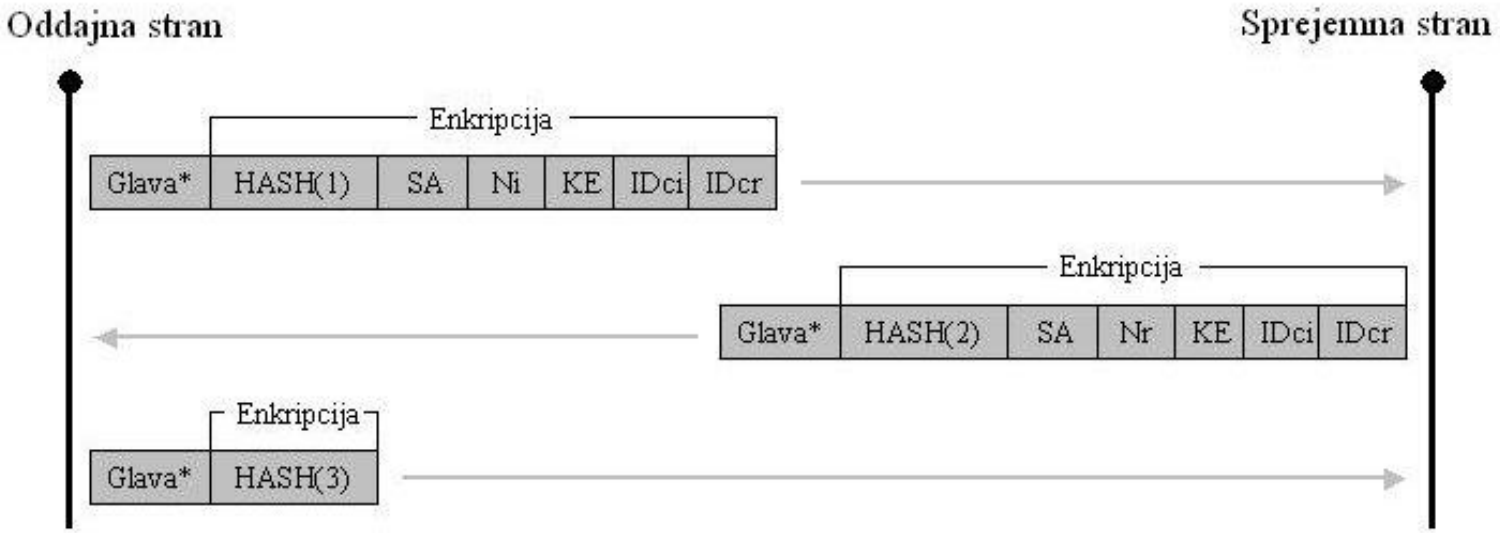
IKE faza 1 – Main Mode

- **Avtentikacija na osnovi predhodno izmenjanih skrivnosti**



IKE faza 2 – Quick Mode

- **Razlaga polj:**
  - **polje HASH prenaša povzetek zgoščevalnega postopka**
  - **polje SA prenaša podatke potrebne za pogajanje, oziroma že določene parametre varne zveze IPSec**
  - **polji Ni in Nr prenašata ostale potrebne podatke *(Nonce Payload)***
  - **opcijsko polje KE prenaša javne ključe**
  - **opcijski polji IDci in IDcr prenašata identifikacijske podatke**
    - **v primeru, ko varna prehoda ne vzpostavljata varne zveze za lasten promet (npr. tunelsko povezavo)**



Parametri varne zveze IKE

Parametri varne zveze IKE	Nabor razpoložljivih parametrov
Enkripcijski algoritem	DES-CBC, 3DES-CBC, IDEA-CBC, CAST-CBC, RC5-R16-B64-CBC, Blowfish-CBC
Zgoščevalni algoritem	MD5, SHA-1, Tiger
Avtentikacijska metoda	RSA podpis, DSS podpis, javni ključi RSA, izboljšani način javnih ključev, predhodno izmenjan ključ
Skupina matematičnih funkcij *(Group Description)*	768 - bitna MODP skupina, 1024 - bitna MODP skupina, EC2N skupina,
Tip matematične skupine *(Group Type)*	MODP, ECP, EC2N
Življenjski čas varne zveze - enota *(Life Type)*	Sekunde, kilobiti *(kilobytes)*
Psevdo naključna funkcija PRF	Ni še definirano
Dolžina enkripcijskega ključa	V primeru, če je njegova dolžina variabilna
Velikost skupine Diffie-Hellman	Velikost polja v bitih
Način vzpostavitve varne zveze IPSec	Hitri način, novi način *(New Group Mode)*

Parametri varne zveze IPSec

Parametri varne zveze IPSec	Nabor razpoložljivih parametrov	
Enkripcija s protokolom ESP	DES_IV64, DES, 3DES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, DES_IV32, RC4, NULL	
Avtentikacija s protokolom AH	HMAC-MD5, HMAC-SHA-1, DES-MAC	
Kompresija podatkov *(IPCOMP)*	OUI, DEFLATE, LZS	
Atributi varne zveze *(SA attributes)*	Enota življenjskega časa	Sekunda, kilobiti *(kilobytes)*
	Življenjski čas varne zveze	V sekundah
	Oakly skupina potrebna za PFS	
	Prenosni način	Tunelski, transportni
	Avtentikacijski algoritem za protokol ESP	HMAC-MD5, HMAC-SHA-1, DES-MAC, KPDK, NULL
	Privatni kompresijski algoritem	Implementacija lastnih kompresijskih algoritmov
	Rezervirani atributi	

Primerjava med IKEv1 in IKEv2

- **Zakaj protokol IKEv2?**
  - **IKEv1 ne podpira avtentikacije uporabnika in ostalih avtentikacijskih mehanizmov**
  - **problem transparentnosti za naprave NAT**
  - **kompleksnost protokola IKEv1 (slabo dokumentiran)**

	IKEv1	IKEv2
Standardizacija	RFC 2407/2408/2409	draft
Delovanje protokola	Faza 1 (3. ali 6. sporočil) Faza 2 (3. sporočila)	Faza 1 (4. sporočila) Faza 2 (2. sporočili)
Avtentikacija	Digitalni podpis, predhodno izmenjani ključi, koncept javnih ključev	Digitalni podpis, predhodno izmenjani ključi
Prikrivanje identitete	Opcijsko	Vedno
Perfect Forward Secrecy	Opcijsko	Opcijsko
Zaščita pred DOS	-	Opcijsko
HASH	Del sporočila	Celotno sporočilo
Razširjena avtentikacija	-	EAP
DHCP	-	Da

NAT – Network Address Translation

- Omogoča prenaslavljanje izvornega/ponornega naslova IP v nek drug naslov IP
- V omrežja IP vpelje koncept odjemalec-strežnik
  - problemi z aplikacijami, ki prenašajo izvorne naslove IP v okviru aplikacijskih protokolov
  - problemi z aplikacijami, ki ne dovolijo spreminjanja vrednosti glave IP in TCP/UDP
- Delovanje:
  - statični NAT
    - sprememba polj v glavi IP
  - dinamični NAT/PAT
    - sprememba polj v glavi IP (NAT)
    - sprememba polj v glavi IP in TCP/UDP (PAT)
- Naprava, ki opravlja funkcijo NAT mora za pakete, katerim je bila spremenjena glava IP oziroma TCP, ponovno izračunati kontrolno vsoto ˝checksum˝
  - kontrolna vsota glave TCP/UDP se izračuna tudi na osnovi zapisov v poljih glave IP (izvorni/ponorni naslov IP, protokol)

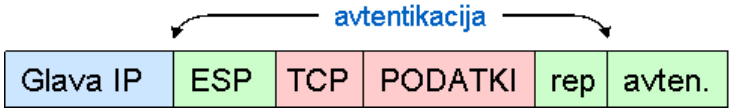
NAT in IPSec

- **Protokol AH**
  - zagotavlja celovitost celotnega paketa IP vključno z glavo
  - protokol AH (v tunelskem ali transportnem načinu prenosa) ne deluje skozi naprave, ki opravljajo funkcijo NAT

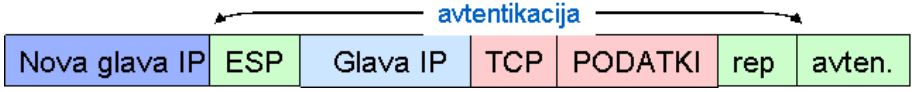
AH – transportni način

AH – tunelski način

- **Protokol ESP**
  - zagotavlja celovitost le prenašanih podatkov (brez zunanje glave IP)
  - sprememba vrednosti v zunanji glavi IP (NAT) ne vpliva na proces avtentikacije IPSec
    - še vedno pa je potreben ponoven izračun kontrolne vsote glave TCP/UDP?
    - izkop preverjanja kontrolne vsote glave TCP/UDP na strani sprejemnika?



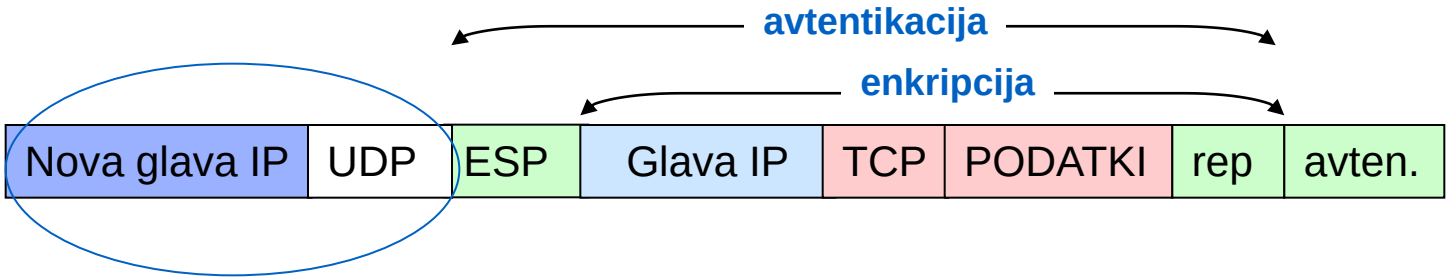
ESP – transportni način



ESP – tunelski način

IPSec NAT Traversal

- **Med zunanjo glavo IP in glavo ESP vstavimo glavo UDP**
  - **v primeru prenosa paketa skozi napravo, ki opravlja funkcijo NAT bo nova kontrolna vsota ˝checksum˝ zapisana v zunanji glavi IP in UDP**



spremenjena polja v primeru prenosa prek naprave NAT

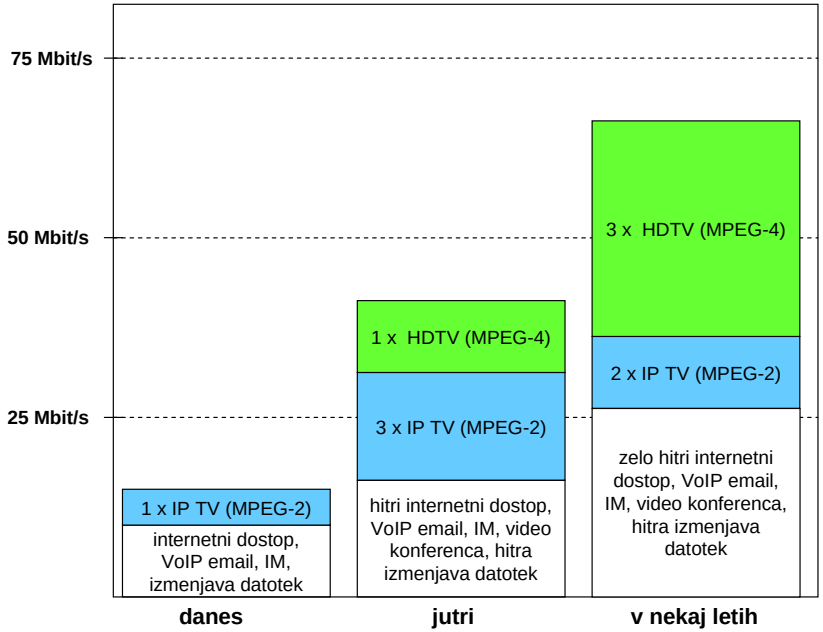
Prometno načrtovanje xDSL

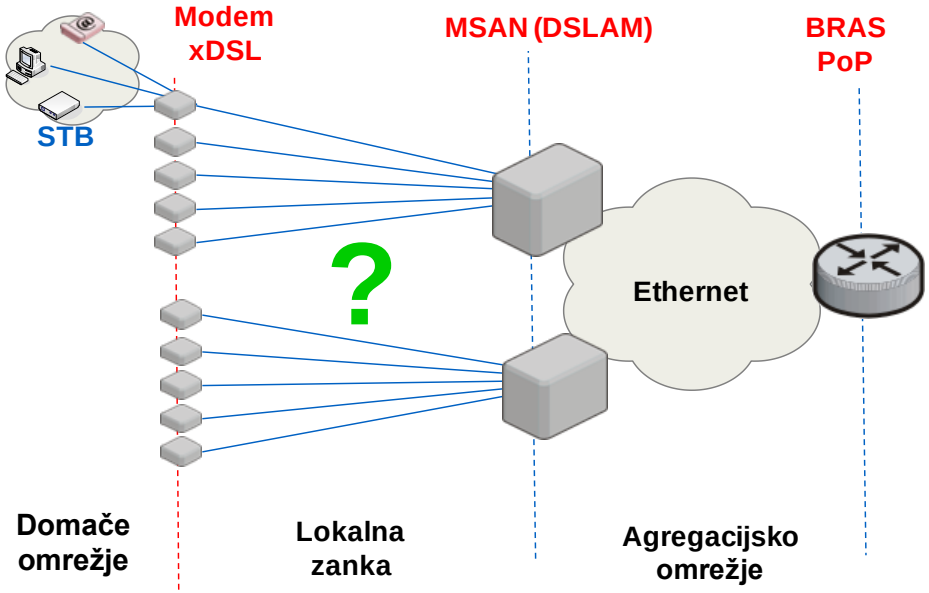
Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- Izbira agregacijskega modela
- Izbira opreme

Potrebe po pasovni širini

- Zahtevana pasovna širina na uporabnika določa uporabljeno tehnologijo v lokalni zanki





Prometna analiza za 3play naročnika

- **Prometna analiza za 1 naročnika**
  - pasovna širina – internet
    - simetrična : UL/DL = 2 Mbit/s
    - asimetrična: UL = 512 Kbit/s, DL = 2 Mbit/s
  - pasovna širna – IP TV (1 TV Kanal, kvaliteta “SD TV”)
    - ~5 Mbit/s (DL) – kodek MPEG-2
    - ~2 Mbit/s (DL) – kodek MPEG-4
  - pasovna širina – VoIP
    - promet RTP (G711) z upoštevano signalizacijo (SIP): UL/DL = 100Kbit/s

Kodek	velikost paketa	Število paketov na sekundo	Velikost paketa VoIP	Potrebna pasovna širina
G.711	160 oktetov	50	200 oktetov	80 Kbit/s
G.711	240 oktetov	33	280 oktetov	74 Kbit/s
G.729A	20 oktetov	50	60 oktetov	24 Kbit/s

- **Pasovna širina lokalne zanke**
  - v smeri proti uporabniku (internet, IPTV, VoIP) = 7.1 Mbit/s
  - v smeri proti omrežju?

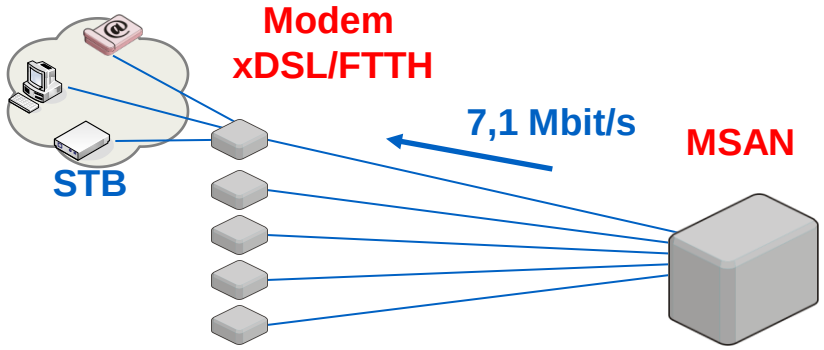
Kazalo

- Prometno načrtovanje naročniške zanke
- **Prometno načrtovanje MSAN**
- Izbira agregacijskega modela
- Izbira opreme

Prometna analiza za MSAN (DSLAM)

- **Prometna analiza za MSAN**
  - na MSAN bo priključenih 600 naročnikov
  - vsi naročniki bodo uporabljali: internet, VoIP, IPTV
- **Skupna potrebna pasovna širina na vmesniku MSAN**
  - 7,1 Mbit/s/uporabnika × 600 uporabnikov = 4,3 Gbit/s?
  - upoštevamo dobitek statističnega multipleksa => 731 Mbit/s

Storitev	Enota	Povprečna pasovna širina	Koncentracija	Skupna pasovna širina
HSI	600 naročnikov	2 Mbit/s	1:10	120 Mbit/s
VoIP	600 naročnikov	100 Kbit/s	0.18 (Erlang)	11 Mbit/s
IPTV	120 TV programov	5 Mbit/s	-	600 Mbit/s



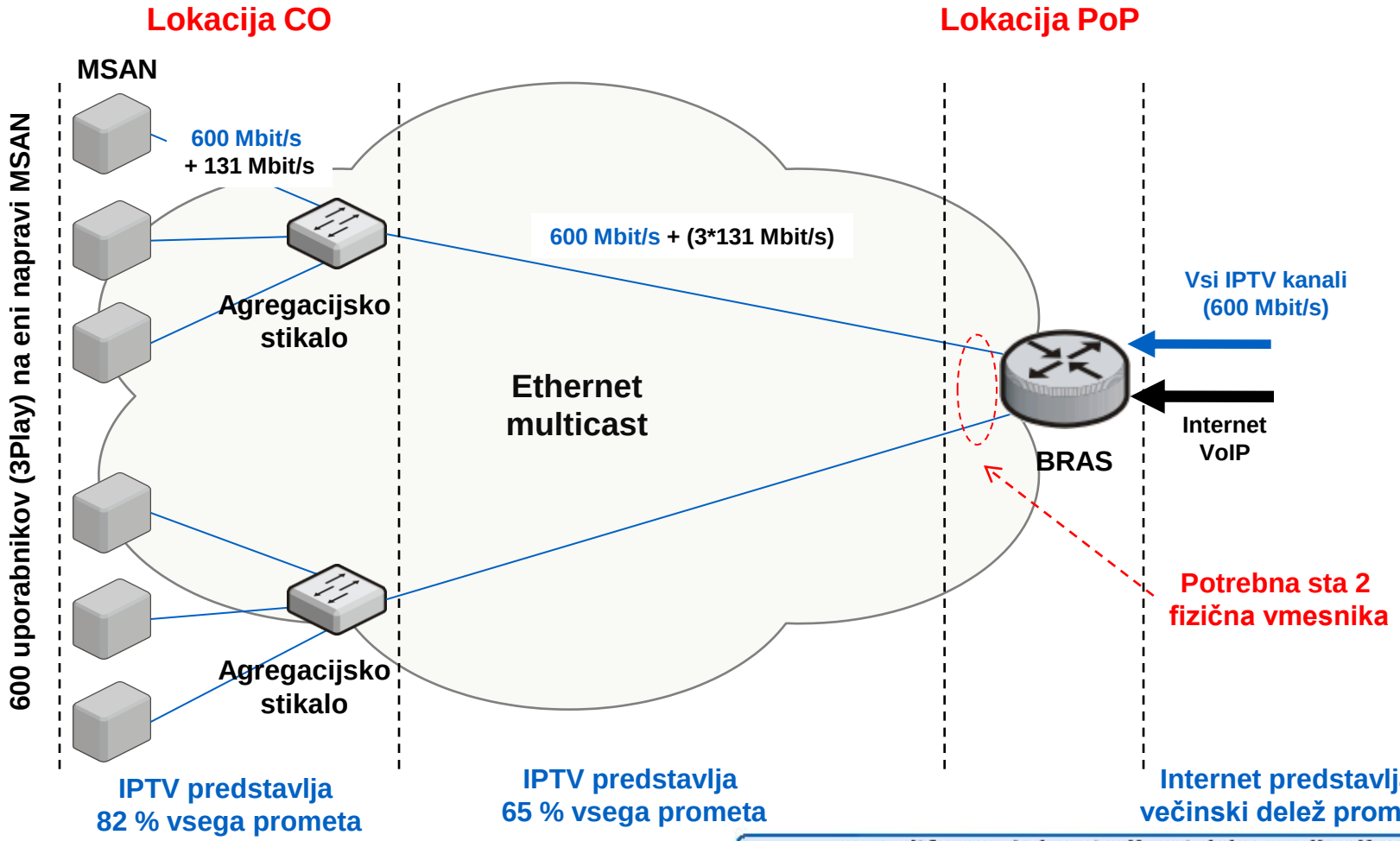
IPTV (multicast) predstavlja
82 % vsega prometa

Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- **Izbira agregacijskega modela**
- Izbira opreme

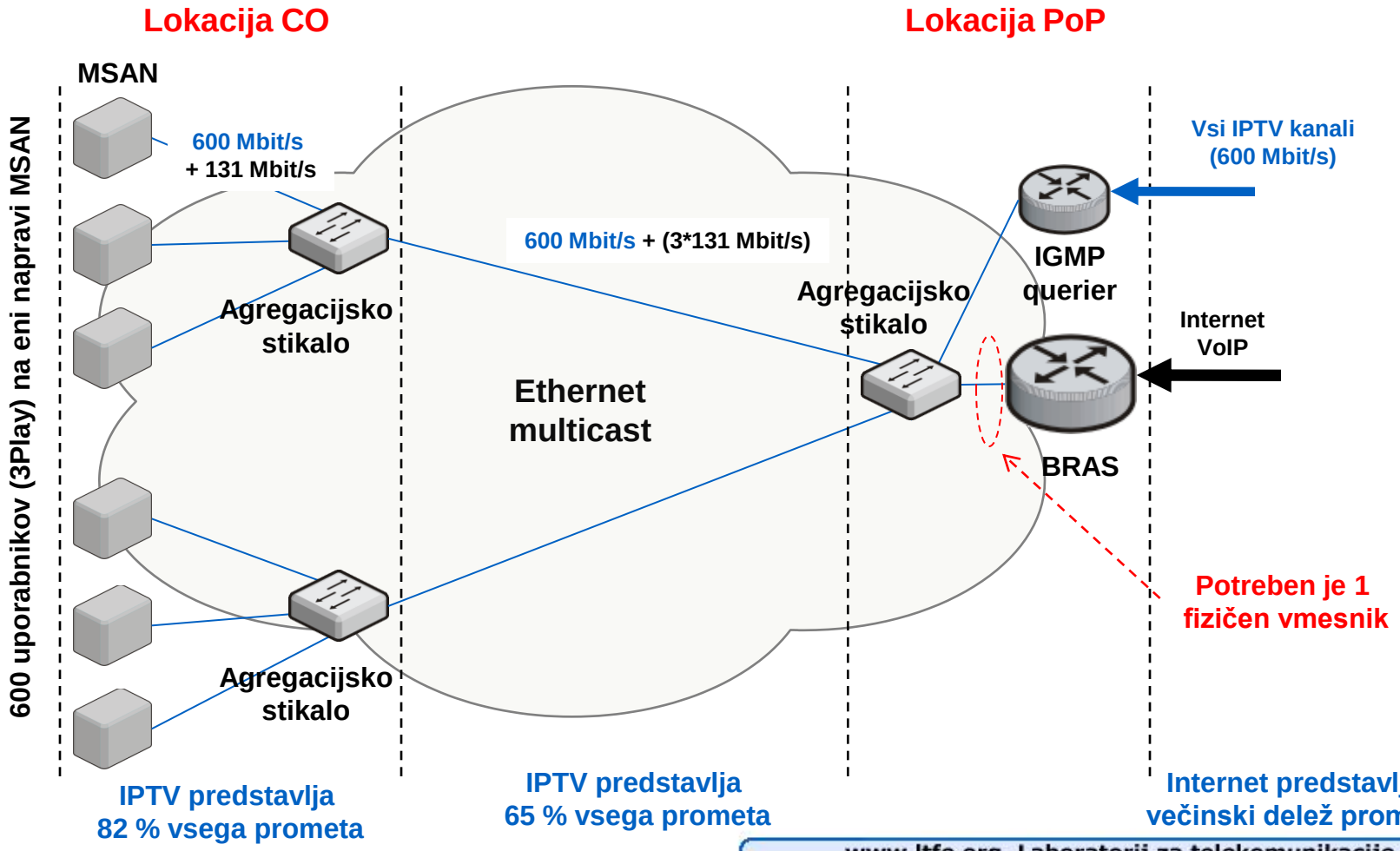
Agregacijski model – IPTV prek BRAS

- **Značilnosti rešitve**
  - **Single Edge model, eno nivojska agregacija, topologija zvezda**



Agregacijski model – IPTV mimo BRAS

- **Značilnosti rešitve**
  - **Dual Edge model, dvo nivojska agregacija, topologija zvezda**

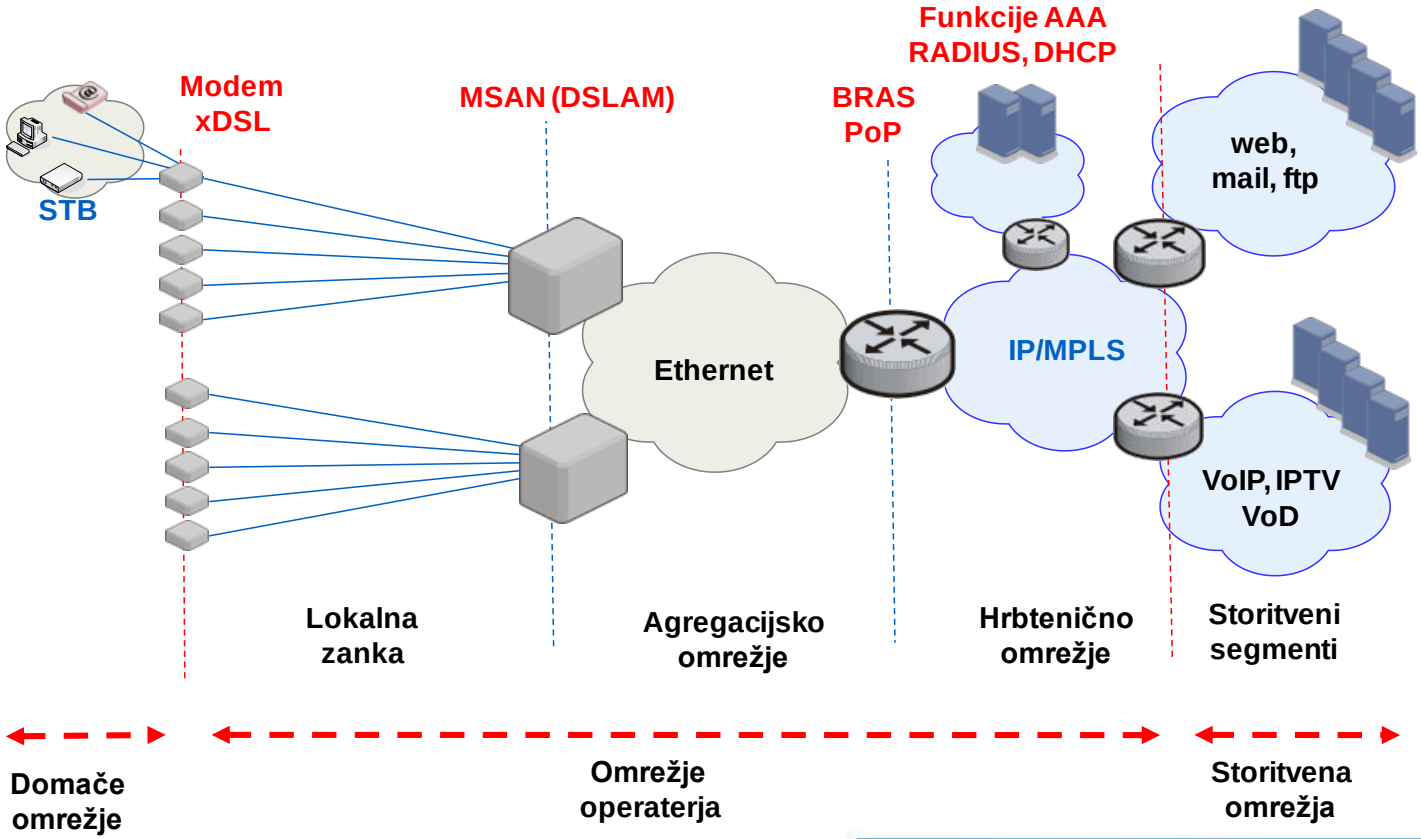


Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- Izbira agregacijskega modela
- Izbira opreme

Zmogljivosti in funkcionalnosti opreme

- **Določitev potrebnih funkcionalnosti naprav**
  - **Katere funkcije se izvajajo v HW (FPGA/ASIC)?**
  - **Katere funkcije se lahko v SW (CPU)?**



Zmogljivosti naprav

- Ethernet stikala
  - kateri vmesniki (GE, 10GE, 40GE), število vmesnikov
    - hitrost Ethernet stikalne matrike – paketi na sekundo (pps)
    - število (HW) čakalnih vrst
  - število vnosov v tabelo MAC
  - napredne funkcionalnosti
    - IGMP Snooping, DHCP relay – število zahtev
- Usmerjevalniki/BRAS
  - kateri vmesniki (GE, 10G, 40GE), število vmesnikov
    - hitrost IP posredovalne matrike – paketi na sekundo (pps)
    - število (HW) čakalnih vrst
  - število vnosov v usmerjevalno tabelo
  - napredne funkcionalnosti
    - terminacija PPP – število sej, hitrost vzpostavljanja sej
    - IGMP querier, DHCP relay – število zahtev
    - Radius – število zahtev
    - IP session aware – število sej

Primer izračuna zmogljivosti

- **Hitrost posredovanja = X pps × 64 oktetov [Mbit/s]**
  - **pri izračunu je upoštevana najmanjša velikost paketa IP (64 oktetov)**

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
7304-NSE-150			3,500,000(PXF) 800,000(RP)	1,792 409.6	No
7304-NPE-G100			1,099,000	562.69	No
7301	79,000	40.448	1,018,000	521.22	No
7401	20,000	10.24	300,000 (Also has PXF)	153.6	30-Dec-04
7000-RP	2,500	1.28	30,000	15.36	31-Jul-97
7500-RSP2	5,000	2.56	220,000	112.64	16-Feb-03
7500-RSP4/4+	8,000	4.096	345,000	176.64	15-Dec-07
7500-RSP8	22,000	11.264	470,000	240.64	15-Dec-07
7500-RSP16	29,000	14.848	530,000	271.36	15-Dec-07
7500-VIP2/40	Punts to RSP[1]		60,000 – 95,000	30.7 – 48.6	30-Apr-04
7500-VIP2/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-May-03
7500-VIP4/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-Dec-07
7500-VIP4/80	Punts to RSP[1]		140,000 – 210,000	71.7 – 107.5	15-Dec-07
7500-VIP6/80	Punts to RSP[1]		140,000 – 219,000	71.7 – 112.1	15-Dec-07
7600-MSFC2(Sup2)	20,000 (500,000 for software-switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic - 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	1-Mar-07
7600-MSFC2A(Sup32)			15,000,000[2]	7,680.00	No
7600-MSFC3(Sup720)	20,000 (500,000 for software switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic – 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	No

10 Mbit/s vs 15 Gbit/s!

These are testing numbers, usually with FE to FE, GigE to GigE or POS to POS, no services enabled. As you add ACL's, encryption, compression, etc - performance will decline significantly from the given numbers, unless it is a hardware-assisted platform, such as the ASR 1000, 7600 or 12000, which process QoS, ACL's, and other features in hardware (or when a hardware assist is installed, for instance an AIM-VPN in a 3745 will offload the encryption from the CPU). Every situation is different - please simulate the true environment to get applicable performance values

http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

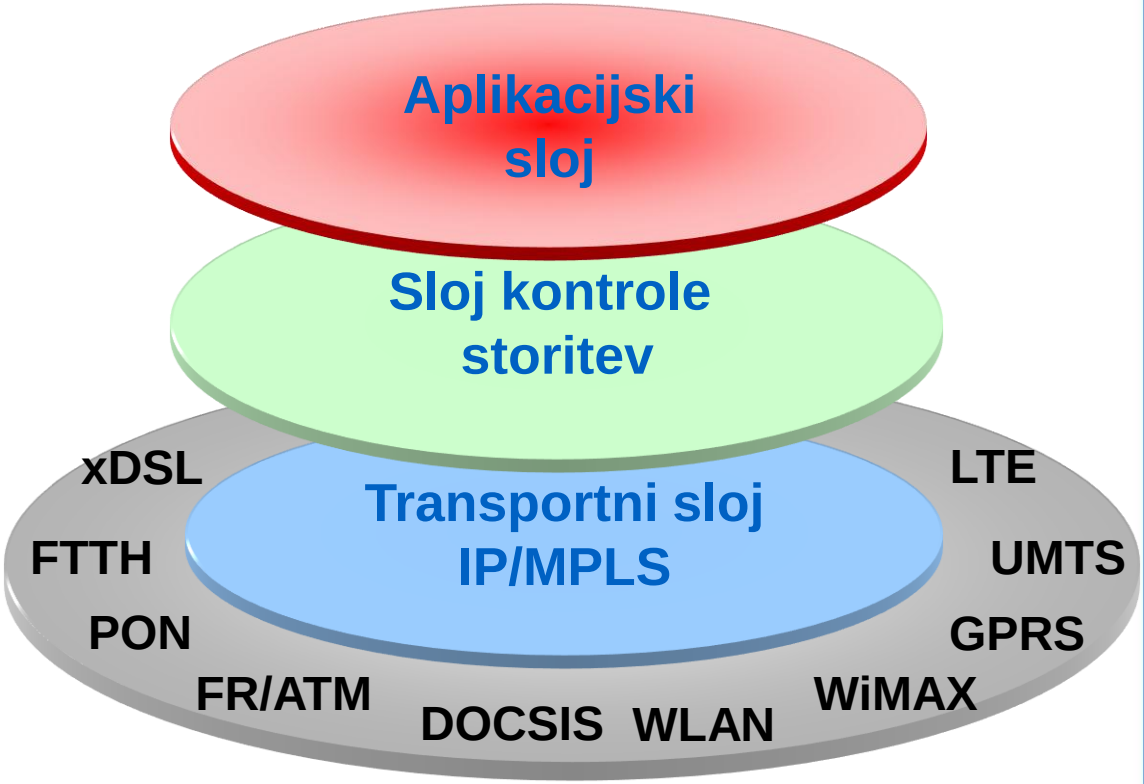
Omrežno načrtovanje

Vsebina

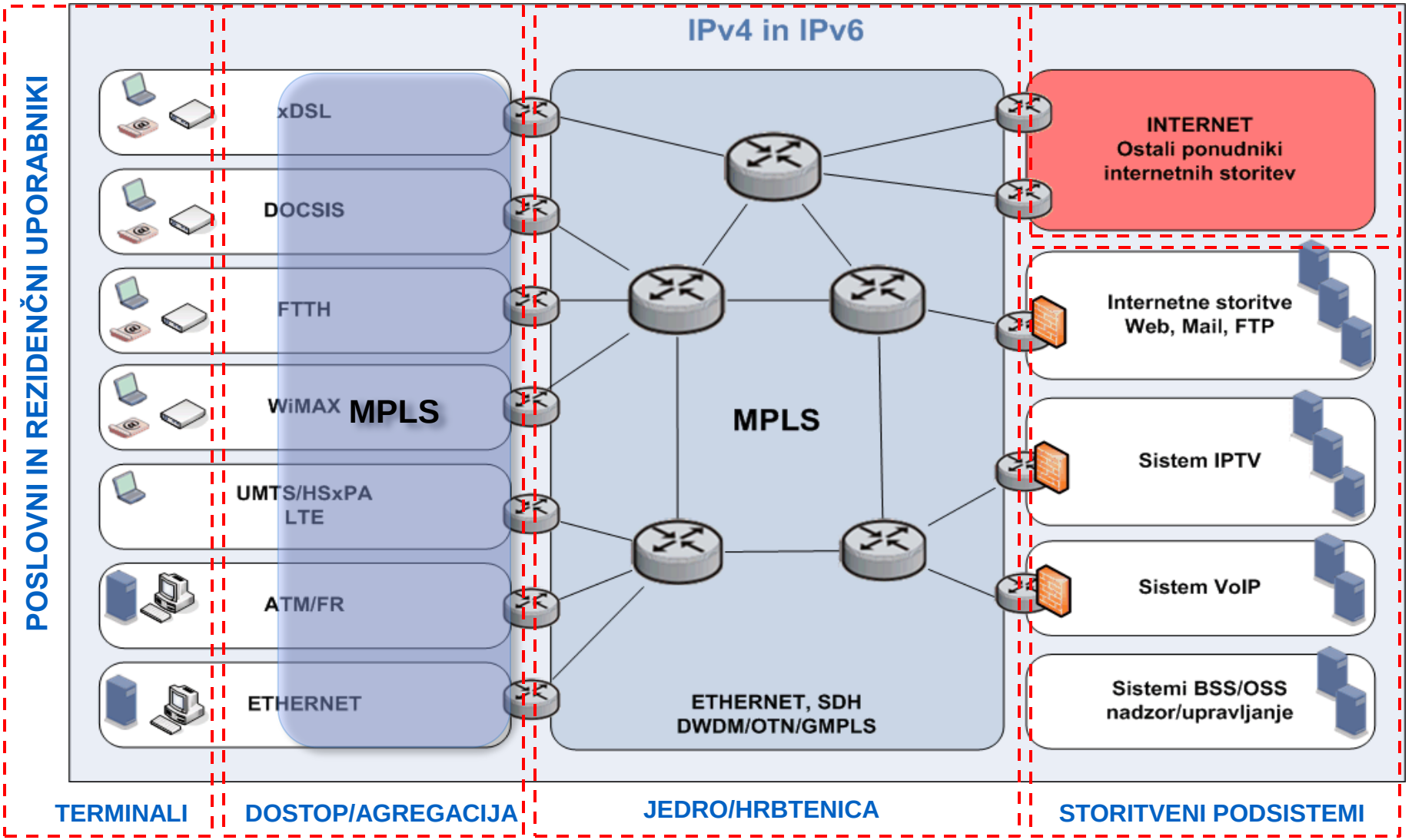
- *Uvod*
- *Prometna analiza*
- *Agregacijski modeli*
- *Dostopovne topologije*
- *Storitveni modeli*

Koncept delovanja sodobnih omrežij

- Trije neodvisni sloji
  - aplikacijski sloj
  - sloj kontrole storitev
  - transportni sloj
- Transportni sloj
  - hrbtenica
  - agregacija (Metro)
  - dostop
- Robne naprave
  - koncentracija inteligence v robnih napravah
  - zagotavljajo preprosto in razširljivo agregacijsko/ hrbtenično omrežje
  - trend: pozicija čim bližje uporabniku



Transportni sloj sodobnih omrežij



Tehnologije v hrbtenici

- IP/MPLS/GMPLS
  - IPv4 in IPv6 zagotavlja naslavljanje, usmerjanje in kontrolne funkcije
  - MPLS/GMPLS zagotavlja posredovalne in TE funkcije
- Transport in vmesniki
  - SDH, NG-SDH
    - velika razširjenost tehnologije med operaterji
    - znanje, zanesljivost, zaščitni mehanizmi, odličen OAM
  - Ethernet
    - nizka cena vmesnika
    - velike hitrosti 1 Gbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/s
    - vse večja zanesljivost
    - izpopolnjujejo se mehanizmi OAM
    - PBT (PBB-TE), T-MPLS, PW (pseudowire)
  - sistemi xWDM

Sodobna hrbtenična omrežja

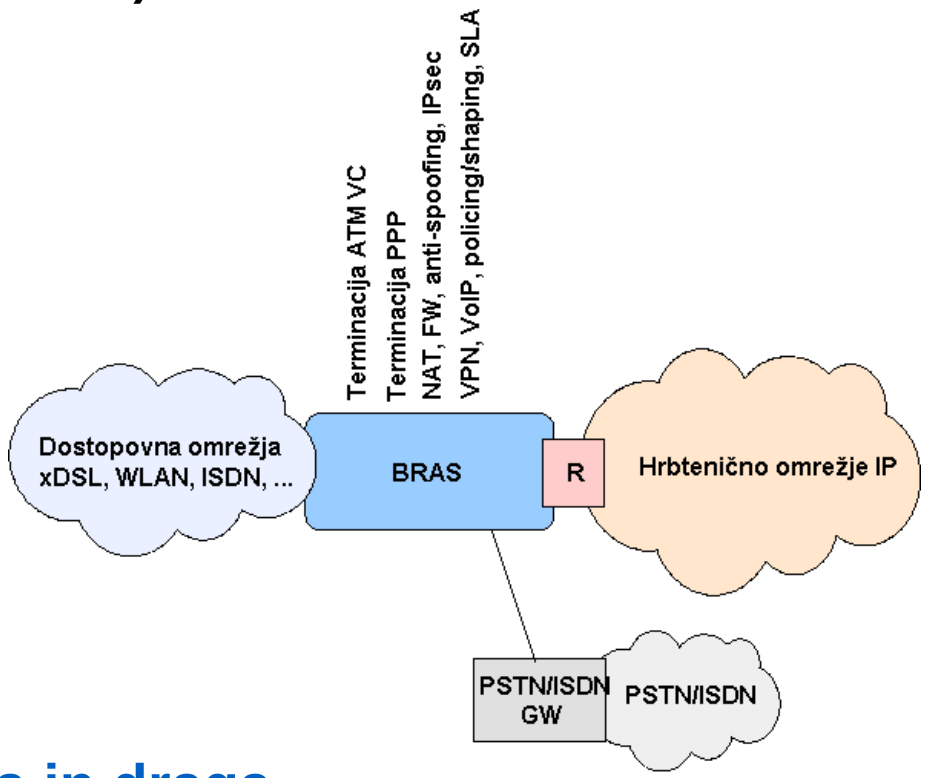
- **Potrebne funkcionalnosti in mehanizmi v sodobnih hrbteničnih omrežjih**
  - navidezna zasebna omrežja (angl. VPN – Virtual Private Network)
  - zaščitni mehanizmi (angl. Protection)
  - kakovost storitev (angl. QoS – Quality of Service)
  - prometni inženiring (angl. TE – Traffic Engineering)
- **Katero tehnologijo uporabiti?**
  - Cena
  - Zmogljivost
  - Razširljivost/skalabilnost
  - Kompleksnost
  - Upravljanje
  - Standardizacija

Tehnologije na dostopu

- Na dostopu se uporabljajo različne tehnologije, odvisno od obstoječih izhodišč operaterjev in cene
  - Fiksni dostopovni sistemi
    - xDSL, kabelska omrežja
    - FTTH, xPON
  - Brezžični dostopovni sistemi
    - WMAN (WiMAX), WLAN (WiFi)
  - Mobilni dostopovni sistemi
    - GPRS, UMTS, HSPA, LTE
- Ethernet, ki je bil do nedavnega LAN tehnologija, postaja prevladujoča tehnologija v agregaciji in hrbtenici
- ATM, ki je bila nekoč prevladujoča hrbtenična tehnologija, se danes (še) uporablja na dostopu (UMTS, xDSL)

Rob omrežja

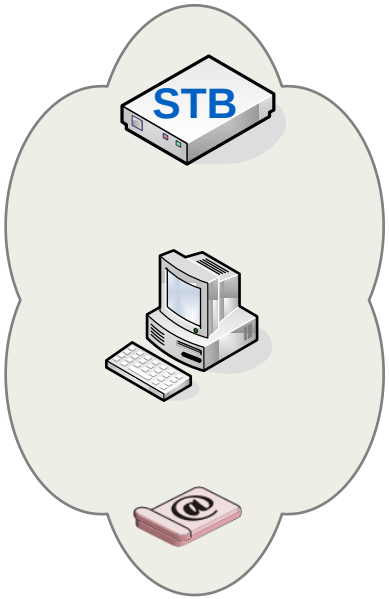
- **Pozicija, kjer se nahajajo prehodi za izbiro storitev – BRAS, SSS, SSG, GGSN**
  - terminacija povezav in različnih dostopovnih omrežij/tehnologij
  - terminacija sej PPP (PPPoE in PPPoA)
  - avtentikacija uporabnikov
  - izbira storitev
  - usmerjanje prometa
  - tuneliranje prometa L2TP
  - storitve DHCP, NAT, FW, IPsec, MPLS, VPN
  - QoS, krmiljenje prometa
- **Vse vrste vmesnikov**
  - Ethernet, ATM, FR, SDH
- **Naprava BRAS je kompleksna in draga**



Omrežno načrtovanje xDSL

Definicija problema

Uporabnik
3Play



?

Storitve

Internet,
mail, ftp

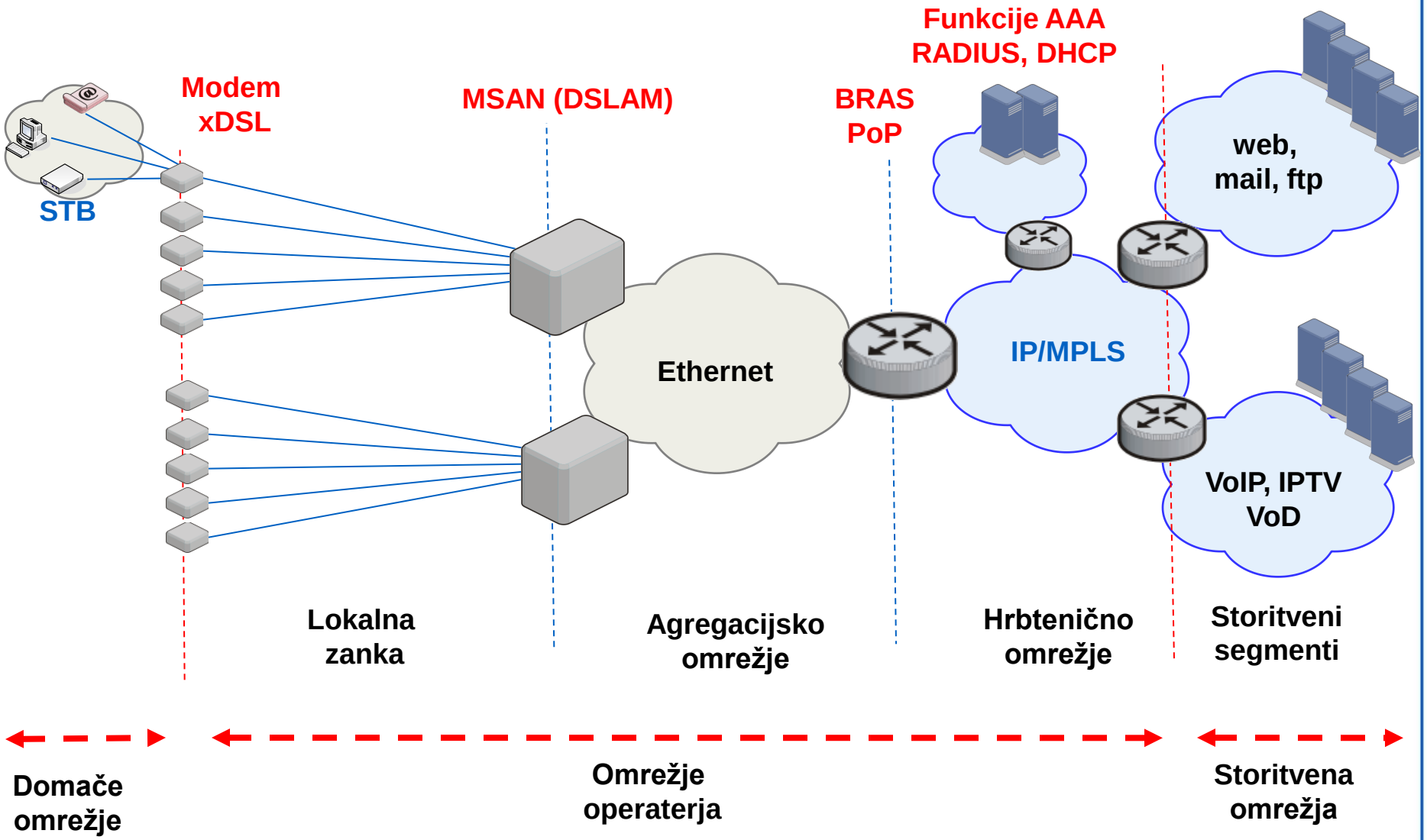
NSP

VoIP, IPTV
VoD

ASP

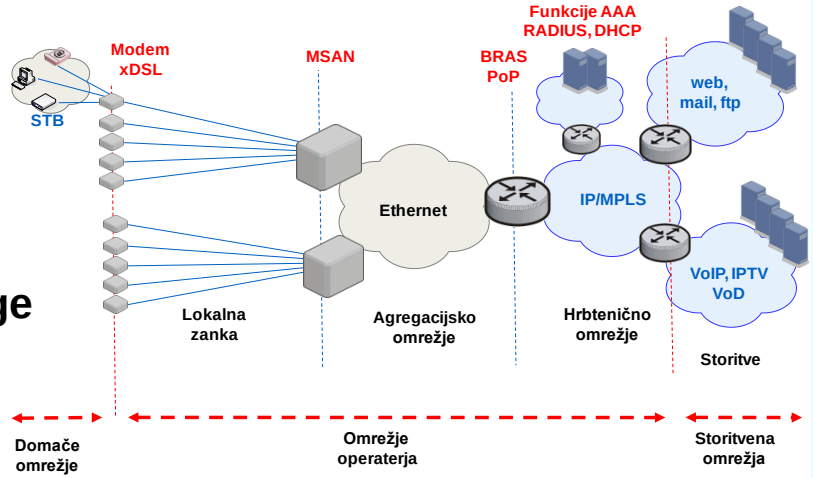
Domače omrežje → ← Omrežje operaterja → ← Storitvena omrežja →

Komponente sistema xDSL



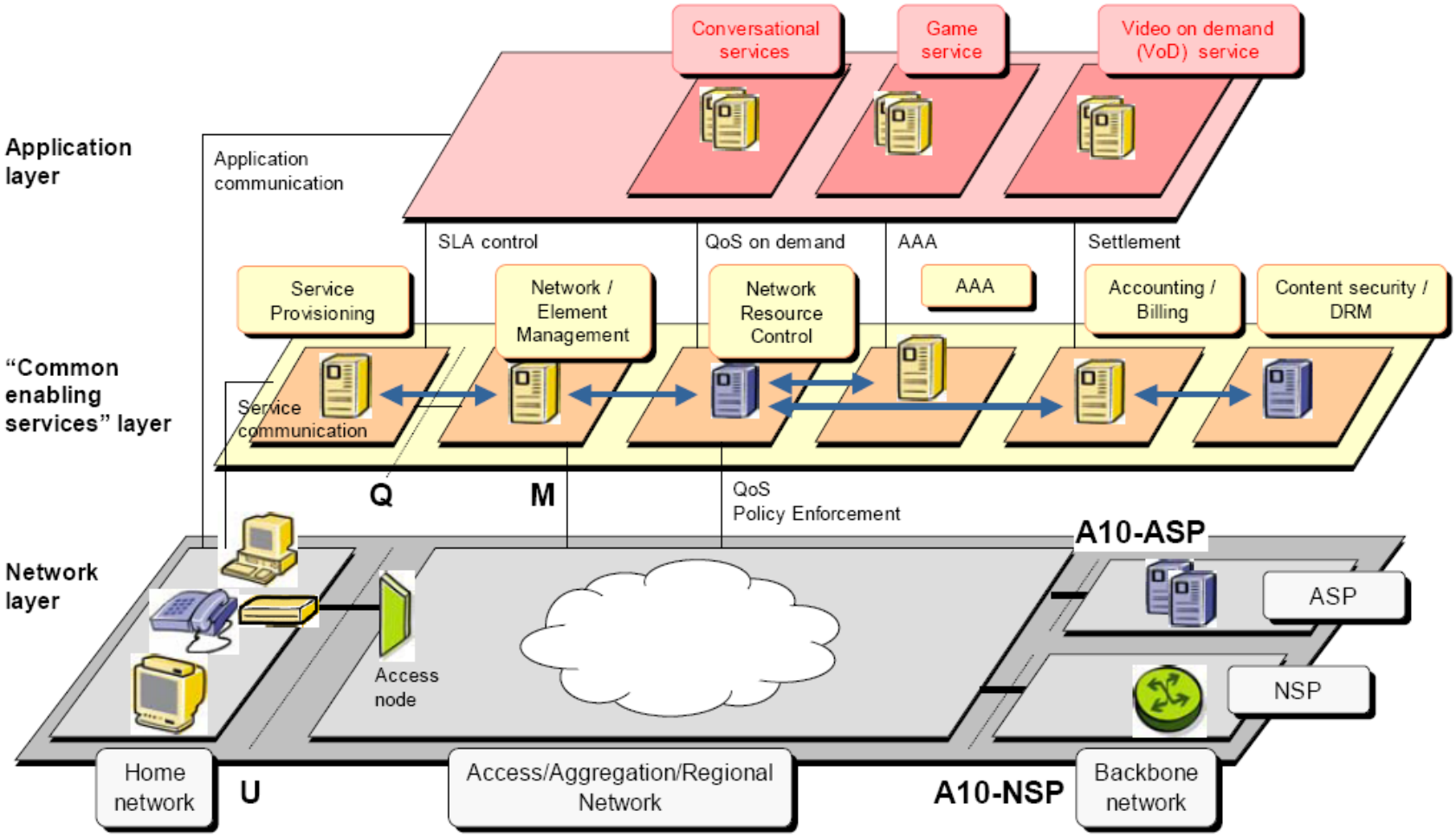
Izhodišča pri načrtovanju 1/2

- 3Play, Multi Play – prenos vseh vrst prometa/storitev prek enotne omrežne infrastrukture
  - VoIP, internet, IPTV, video na zahtevo, VPN
- Iskanje rešitev za
  - izbor dostopovne tehnologije
    - prometna analiza
  - agregacijski model
    - ATM, Ethernet, Single Edge, Dual Edge
    - topologija omrežja (ring, mesh)
    - redundanco, veliko razpoložljivost
  - storitveni model
    - zagotavljanje funkcij AAA (PPPoE, DHCP)
    - način avtentikacije uporabnikov/naprav
    - avtomatsko nastavitev mrežnih in ostalih parametrov terminalov
    - nadzor dostopa/uporabe storitev
  - ločevanje prometnih tokov, sledljivost uporabnikov
  - zagotavljanje QoS



Izhodišča pri načrtovanju 2/2

- **Standardizacija – storitvena arhitektura TR 144**

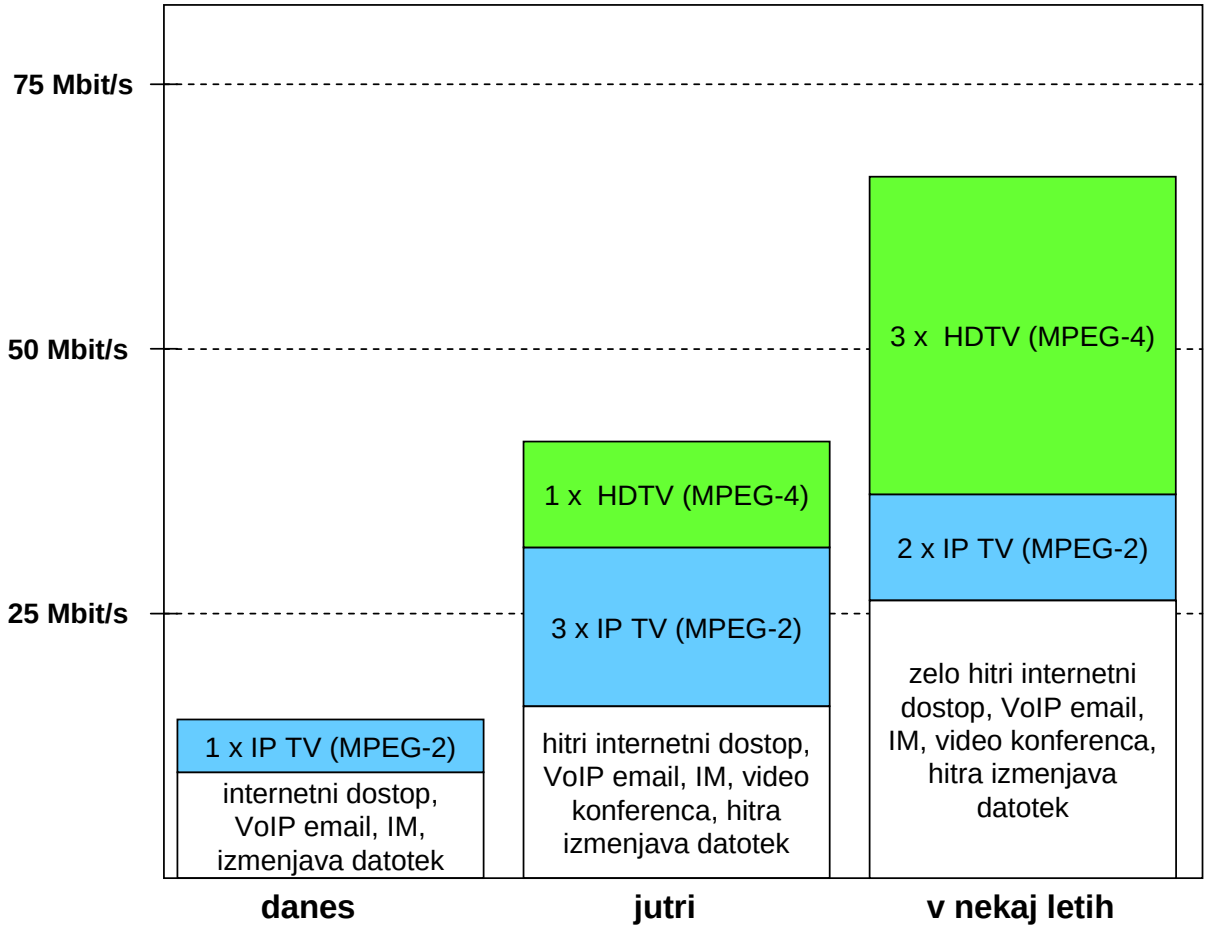


Vsebina

- *Uvod*
- ***Prometna analiza***
- *Agregacijski modeli*
- *Dostopovne topologije*
- *Storitveni modeli*

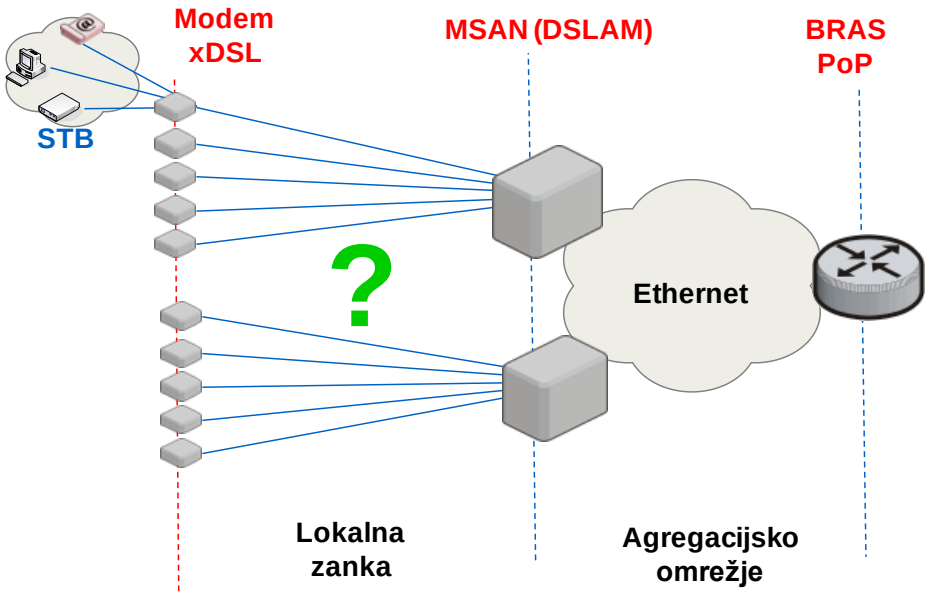
Potrebe po pasovni širini

- **Zahtevana pasovna širina na uporabnika določa uporabljeno tehnologijo v lokalni zanki**



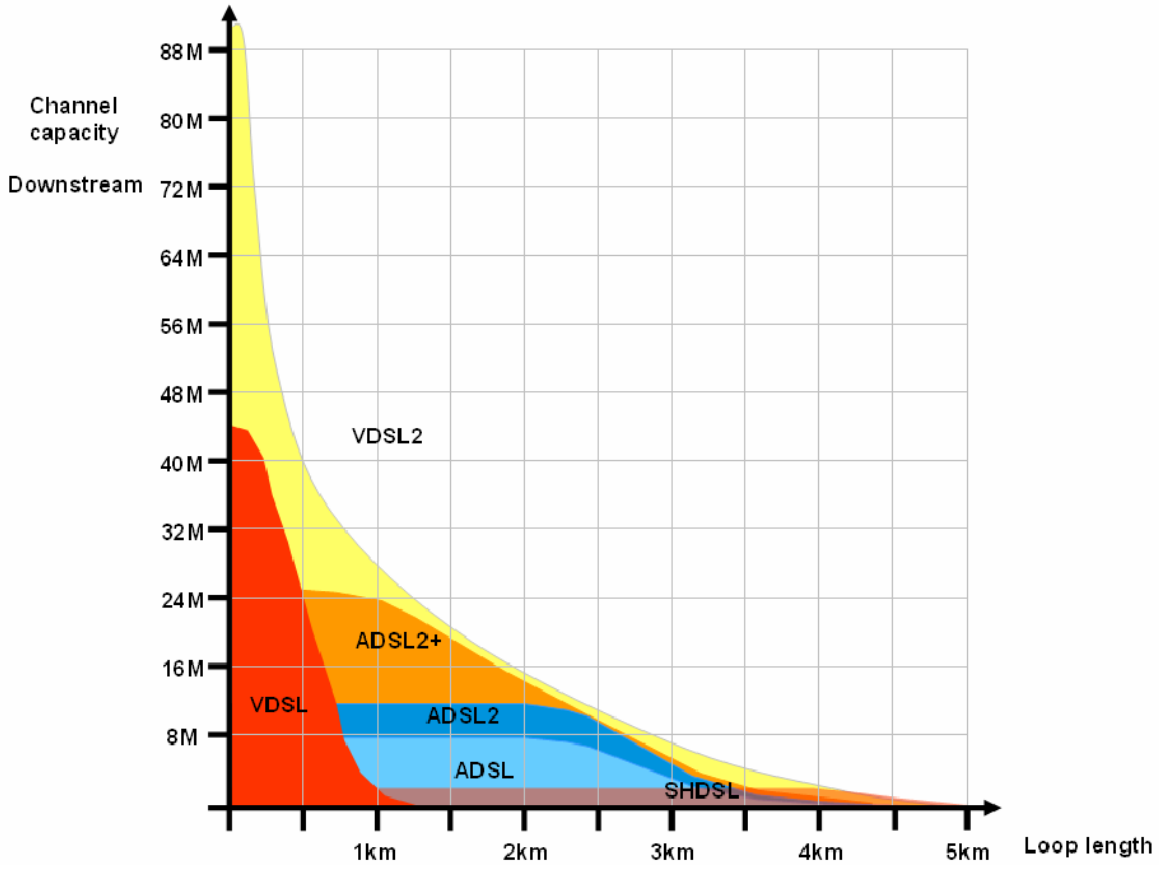
Teoretične zmogljivosti sistemov xDSL

- ADSL (ITU G.992.1 Annex B)
  - DL 12.0 Mbit/s, UL 1.8 Mbit/s
- ADSL2+ (ITU G.992.5 Annex M)
  - DL 24.0 Mbit/s, UL 3.3 Mbit/s
- VDSL
  - DL 52 Mbit/s, UL 16 Mbit/s
- VDSL2
  - DL 100 Mbit/s, UL 100 Mbit/s



Realne zmogljivosti sistemov xDSL

- Dosežena hitrost je odvisna od dolžine in kvalitete naročniške zanke

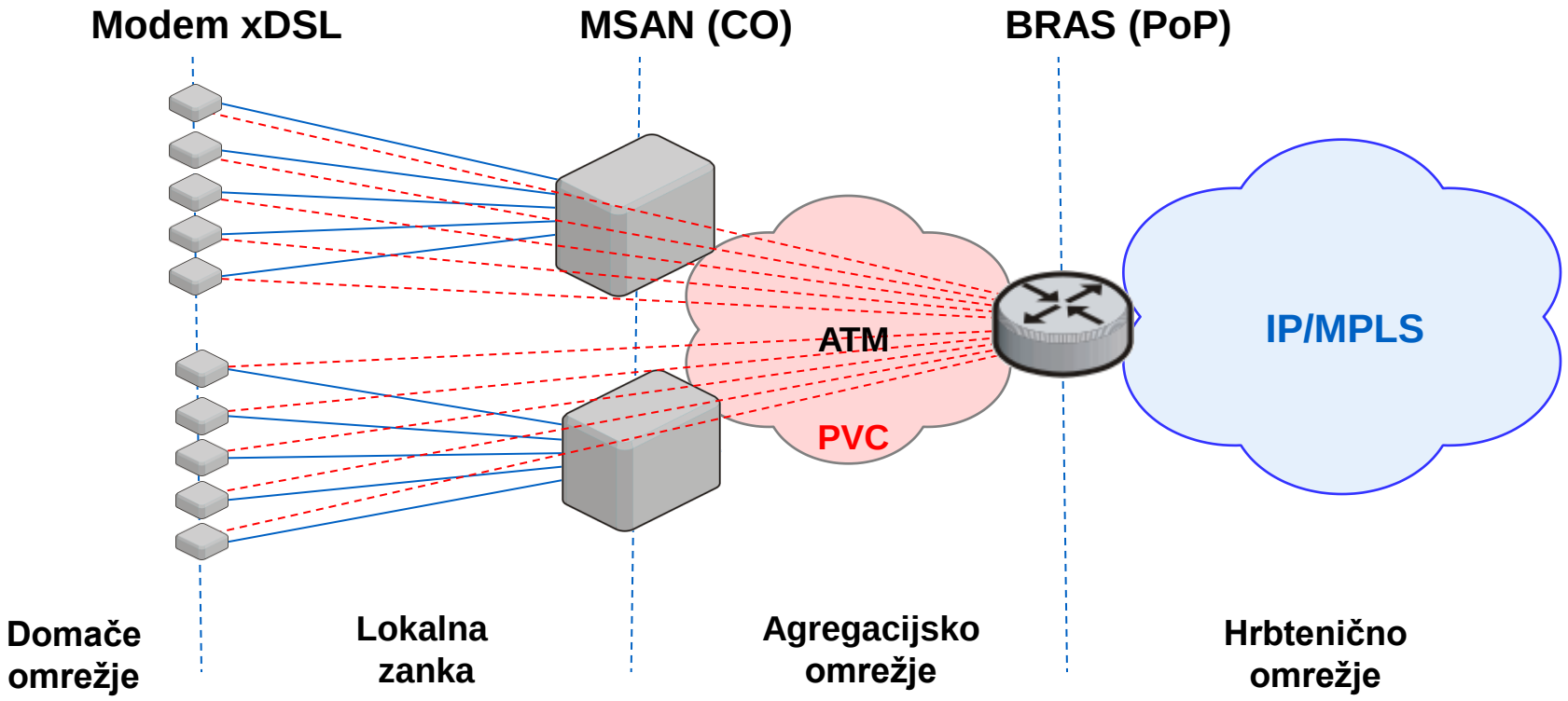


Vsebina

- *Uvod*
- *Prometna analiza*
- ***Agregacijski modeli***
- *Dostopovne topologije*
- *Storitveni modeli*

ATM agregacijski model 1/2

- **Dostopovno in agregacijsko omrežje je zgrajeno na osnovi tehnologije ATM**
  - **v lokalni zanki: ATM prek DSL do uporabnika**
  - **v agregaciji: povezovanje MSAN prek stikal ATM na BRAS**

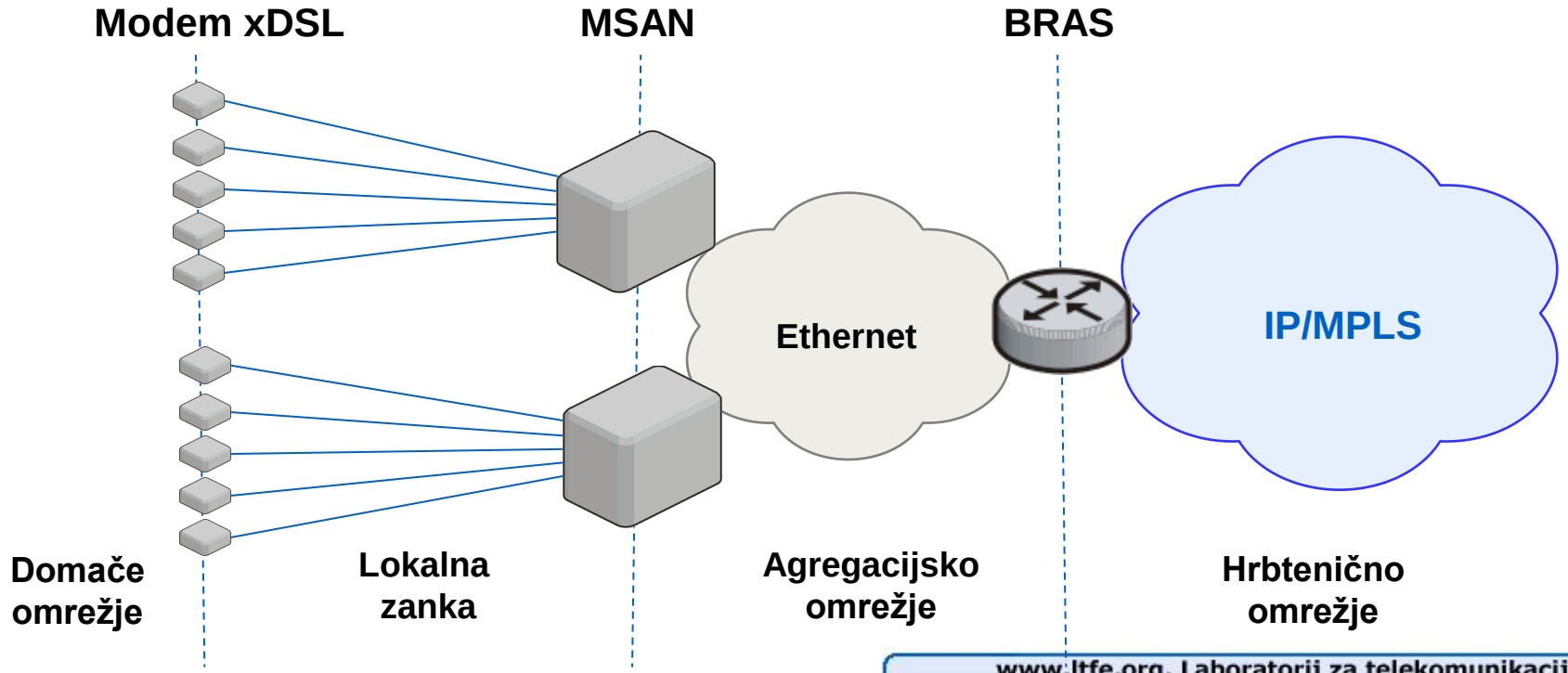


ATM agregacijski model 2/2

- Na strani uporabnika se nahaja
  - modem ADSL, ki tipično deluje v načinu ˝bridging˝
    - Ethernet over ATM
  - obstoječa terminalna oprema je osebni računalnik
    - opcijsko televizijski komunikator (STB – Set-Top-Box) in telefon IP
- Uporabnike se priključuje prek povezav PVC na BRAS
  - vsakega uporabnika se poveže v svoj PVC
  - ves promet (HSI, VoIP, IPTV) uporabnika se prenaša prek ene povezave PVC do BRAS
  - omogoča centralen nadzor in preprosto upravljanje
- Slabosti modela
  - multicast se zaključuje na BRAS
    - v agregacijskem delu omrežja ni podpore za multicast prenosni način
    - v dostopovnem omrežju predstavlja multicast promet večinski delež prometa – IPTV se težko zagotovi vsem uporabnikom
  - majhne prenosne hitrosti vmesnikov ATM (155 Mbit/s in 622 Mbit/s)

Ethernet agregacijski model 1/2

- Agregacijski del omrežja temelji na tehnologiji Ethernet
  - v lokalni zanki: Ethernet/xDSL do uporabnika
  - v agregaciji: povezovanje MSAN prek Ethernet stikal na BRAS
- Naprava DSLAM izvaja funkcije Ethernet stikala
  - Ethernet MSAN: naprava L2, ki podpira funkcionalnosti bridging (802.1D), VLAN, QoS (802.1p), IGMP snooping, DHCP relay



Ethernet agregacijski model 2/2

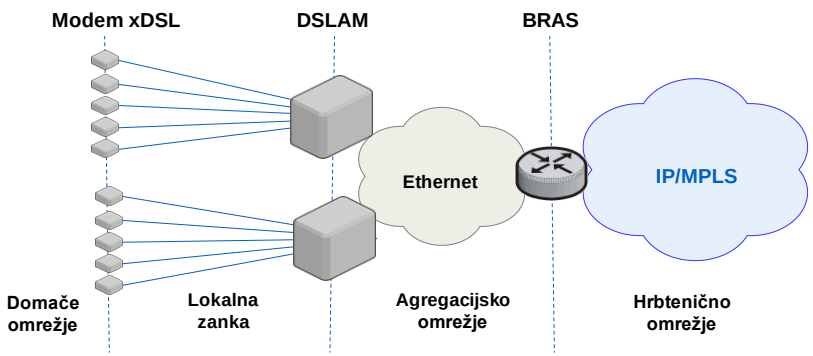
- Agregacijsko omrežje podpira multicast prenosni način
  - Tehnologija Ethernet že v osnovi podpira multicast prenosni način
  - IPTV se lahko zagotovi vsem uporabnikom
- Ločevanje prometnih tokov uporabnikov
  - VLAN na uporabnika (model 1:1 VLAN)
  - VLAN na storitev (model 1:N VLAN)
- Del inteligence se prenese na agregacijska stikala in naprave DSLAM
  - IGMP snooping, DHCP relay, PPPoE VSA
  - varnostne funkcije
- Omejitve tehnologije Ethernet
  - število vnosov v tabele MAC na Ethernet stikalih
  - število logičnih omrežij VLAN
- Potrebno je bolj skrbno načrtovanje omrežja

Robno vozlišče IP – BRAS/BNG

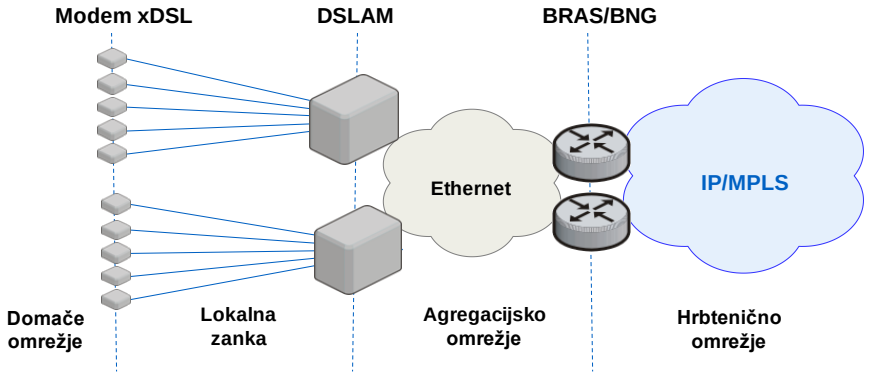
- **BRAS**
  - prva L3 (IP) naprava, ki ločuje uporabnike od hrbtenice IP/MPLS
  - funkcionalno najbolj bogata naprava
- **Zagotavlja dve ločeni funkciji**
  - terminacijo oz. agregacijo različnih dostopovnih tehnologij
    - Ethernet/VLAN in ATM
  - funkcijo storitvenega prehoda
    - podpora sistemom AAA
      - interakcija s portalskimi strežniki (policy server, WEB)
      - terminacija sej PPP (PPPoE) in DHCP
    - izvaja QoS
      - krmiljenje in glajenje prometa, označevanje in razvrščanje
    - podpora za multicast
      - IGMP querier, PIM-SM
    - varnostne funkcije FW, ACL, NAT
    - preusmeritve in tuneliranje prometa do drugih ponudnikov storitev in aplikacij
      - podpora za L2 VPN in L3 VPN
    - podpora za SLA

Število in vloga robnih vozlišč IP

- **Dva pristopa**
  - Single Edge in Dual Edge model
- **Kompromis med**
  - nižjo ceno dostopovnega omrežja (nižji “CAPEX”)
    - zagotovi se z vpeljavo več robnih vozlišč IP in decentralizacijo inteligence na več “cenejših” robnih naprav
    - večja kompleksnost upravljanja
  - centraliziranim nadzorom uporabnikov (nižji “OPEX”)
    - BRAS izvaja centralen nadzor nad uporabniki in storitvami
    - manjša kompleksnost upravljanja



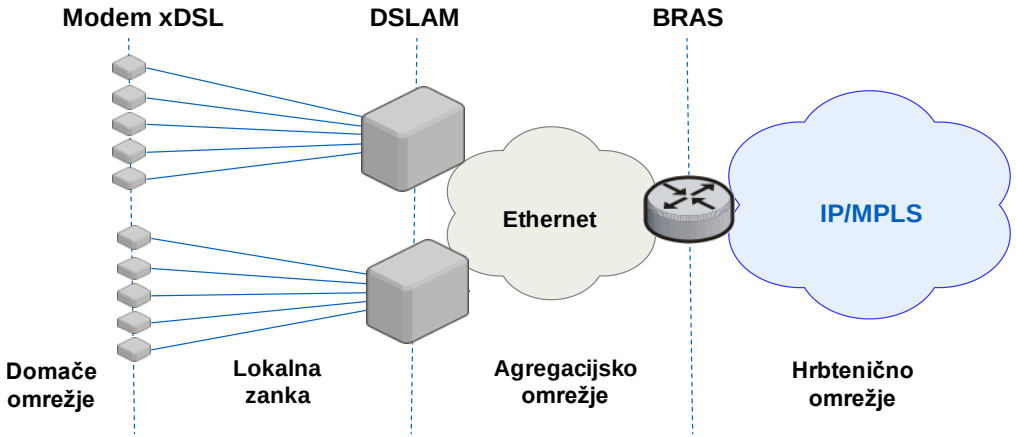
Single Edge



Dual Edge

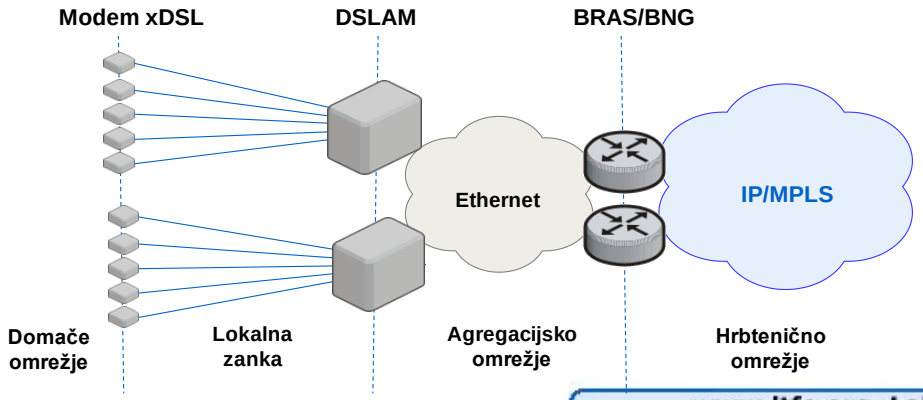
Single Edge model

- **Single Edge**
  - izhaja iz tradicionalnih implementacij xDSL (ATM agregacijski model)
    - optimiziran za zagotavljanje storitev HSI
  - vse uporabniške seje se zaključujejo v centralni točki – BRAS
    - centralizirana agregacija in terminacija PPP sej
    - centralizirano dodeljevanje parametrov IP na osnovi protokola DHCP
    - centraliziran nadzor na varnostjo v omrežju
    - centralizirano upravljanje z uporabniškim prometom oziroma uporabniškim priključkom – povezava s strežnikom AAA (RADIUS)
    - centralizirana multicast funkcionalnost



Dual Edge model

- **Dual Edge**
  - uporaba funkcionalno manj bogatih naprav za zagotavljanje prometno zahtevnih storitev – npr. IPTV
    - video promet, ki danes predstavlja večinski delež prometa na dostopu, se pelje mimo naprave BRAS
  - slabosti pristopa
    - poveča se število naprav, ki jih je potrebno upravljati
    - v omrežju je potrebna dodatna naprava IP, ki zagotavlja funkcijo multicast usmerjevalnika
    - promet v smeri proti uporabnikom vstopa v agregacijsko omrežje prek dveh vstopnih točk
      - težje upravljanje s prometnimi tokovi in z razpoložljivo pasovno širino

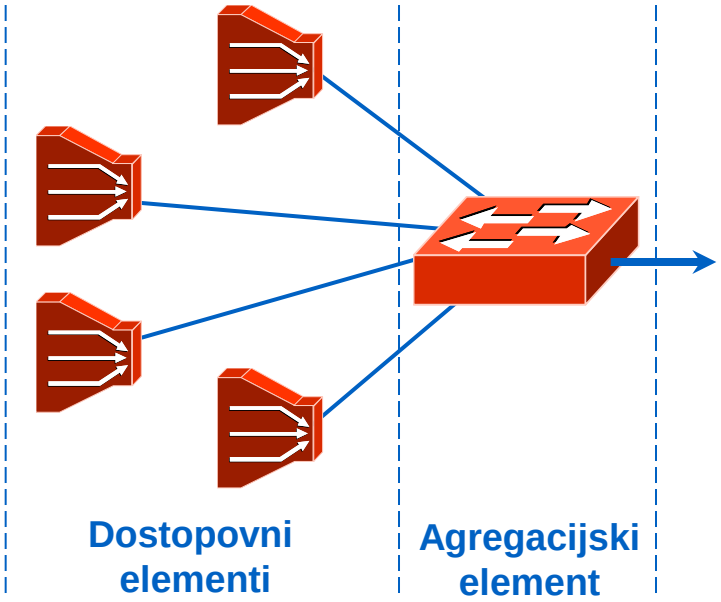


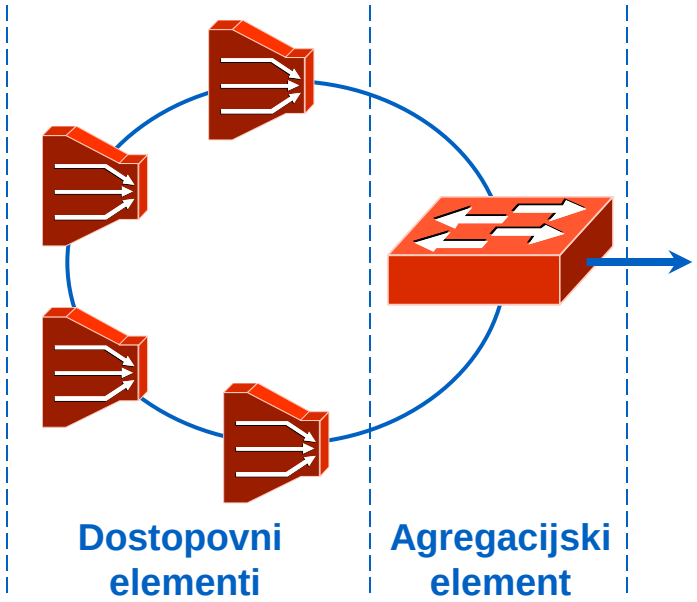
Vsebina

- *Uvod*
- *Prometna analiza*
- *Agregacijski modeli*
- ***Dostopovne topologije***
- *Storitveni modeli*

Dostopovne topologije 1/5

- Eno nivojska agregacija
- Osnovna načina povezovanja omrežnih elementov
  - topologija zvezda
  - topologija obroč





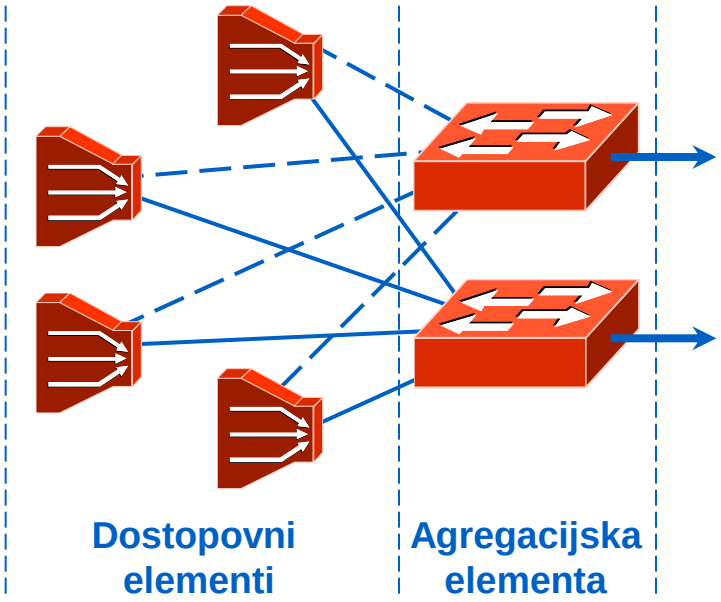
Dostopovne topologije 2/5

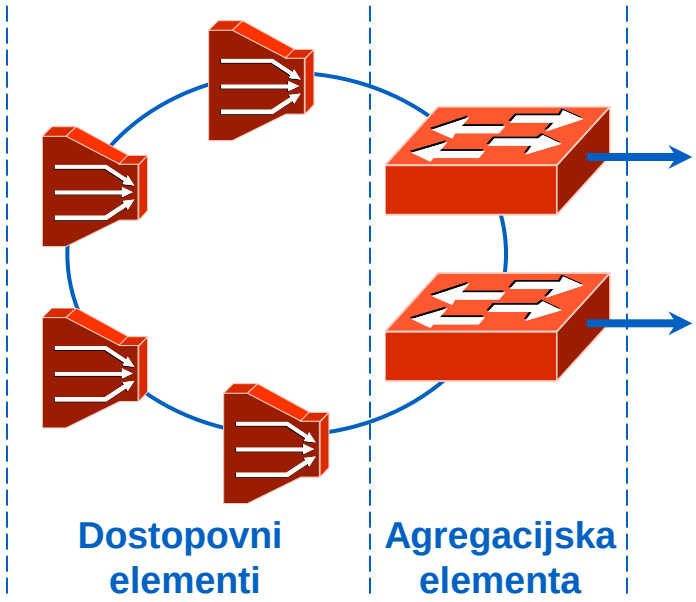
- **Primerjava topologije zvezda in obroč**

Topologija zvezde	Topologija obroča
vsak dostopovni element ima lastno povezavo na agregacijski element (rezervirana pasovna širina)	razpoložljivo pasovno širino si delijo vsi elementi v obroču (razširljivost odvisna od večjega števila elementov)
manjše zakasnitve – dostopovni element je povezan direktno na agregacijski element	večje zakasnitve – večje število naprav prek katerih potuje promet
hitra konvergenca mehanizmov STP, RSTP, MSTP	počasnejša konvergenca mehanizmov STP, RSTP, MSTP
fizična povezava med dostopovnim in agregacijskim elementom ni zaščitena	omogoča zaščito fizične povezave ter vmesnika – redundantna pot
manjše zakasnitve pri prenosu kontrolnih sporočil IGMP	večje zakasnitve pri prenosu kontrolnih sporočil IGMP
lažja kontrola učenja naslovov MAC	težja kontrola učenja naslovov MAC
na agregacijskem elementu je potrebno zagotoviti večje število fizičnih vmesnikov – število potrebnih vmesnikov je enako številu dostopovnih elementov	na agregacijskem elementu sta za vsak obroč potrebna le dva fizična vmesnika
mehanizem za preprečevanje zank (STP, MSTP, RSTP) ni potreben	v omrežju je potrebna implementacija enega izmed mehanizmov za preprečevanje zank (STP, MSTP, RSTP)
	nižja cena v primeru nove implementacije

Dostopovne topologije 3/5

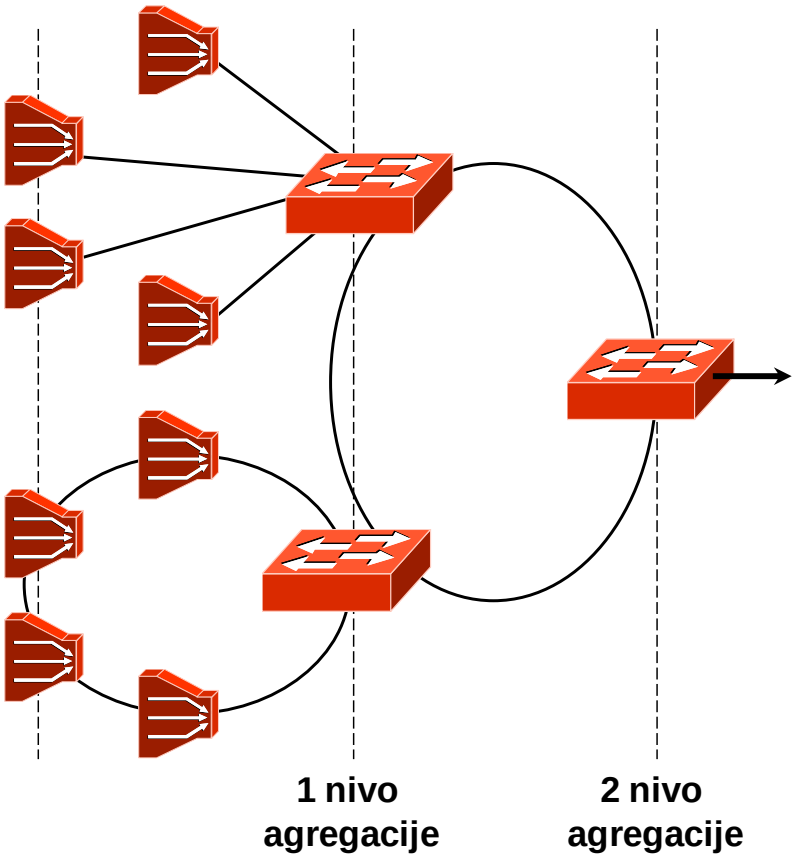
- Eno nivojska agregacija
- Zagotavljanje visoke razpoložljivosti
  - dvojno vpetje zvezde na dva agregacijska elementa
  - dvojno vpetje obroča na dva agregacijska elementa





Dostopovne topologije 4/5

- Več nivojska agregacija
  - vsaka izmed posameznih stopenj agregacije je lahko izvedena na osnovi topologije obroča ali topologije zvezde



Dostopovne topologije 5/5

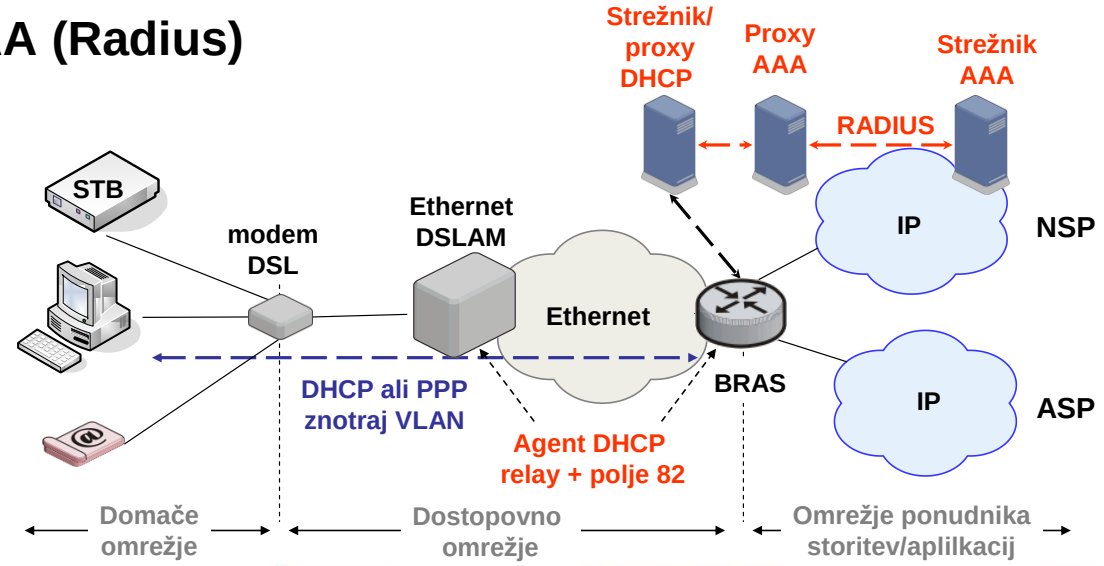
- **Pomanjkljivosti več nivojske agregacije**
  - **povečanje zakasnitev zaradi večjega števila naprav prek katerih se prenaša promet**
    - **potencialno daljši odzivni čas aplikacij**
    - **Npr. zakasnitve pri prenosu kontrolnih sporočil IGMP povečujejo potreben odzivni čas za preklop med posameznimi programi TV**
  - **v primeru redundantnih povezav je v omrežju Ethernet potrebna implementacija enega izmed mehanizmov za preprečevanje zank (STP, MSTP, RSTP)**
  - **večje število naprav, ki jih je potrebno upravljati**

Vsebina

- *Uvod*
- *Prometna analiza*
- *Agregacijski modeli*
- *Dostopovne topologije*
- ***Storitveni modeli***

Storitveni model

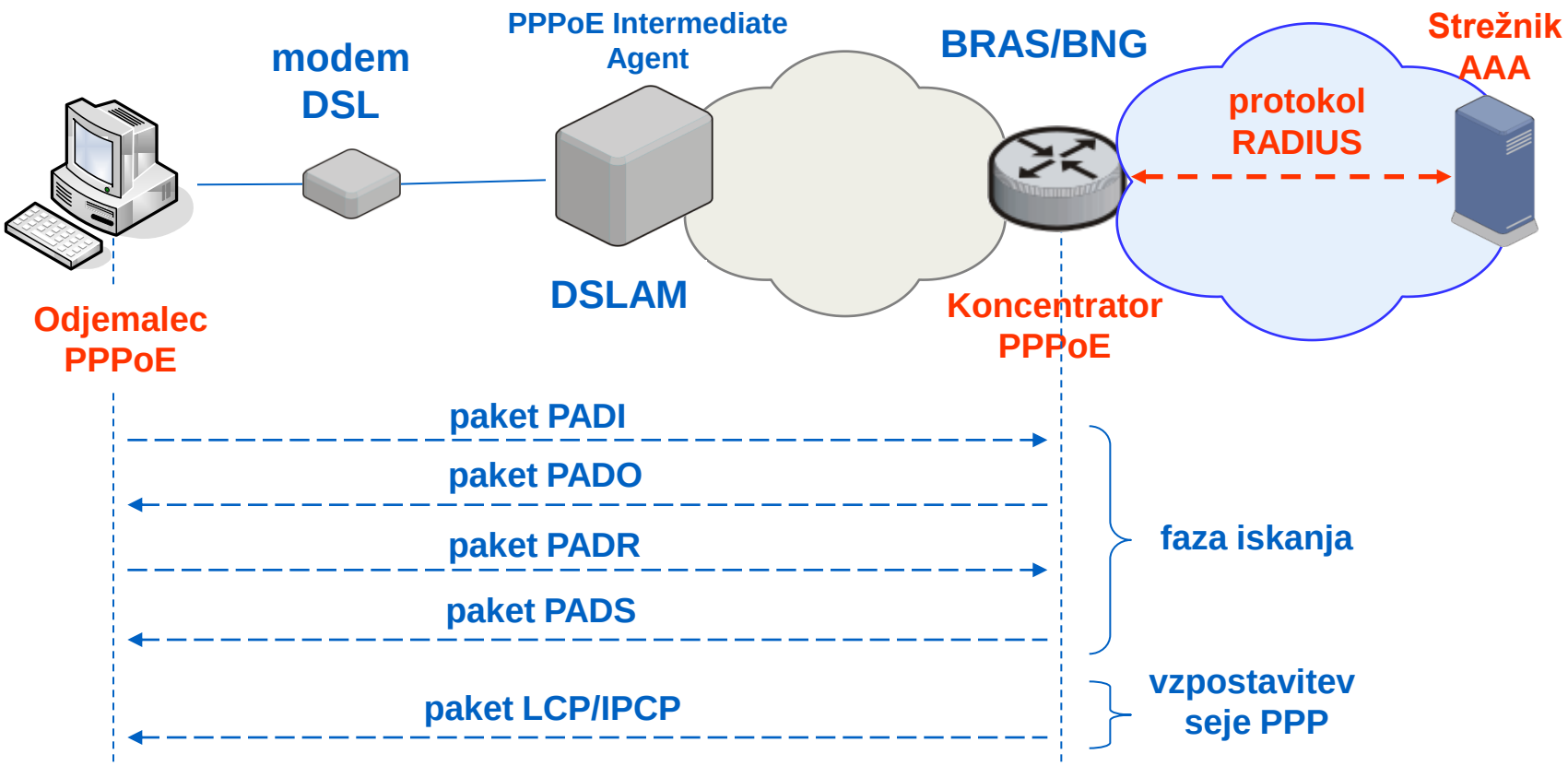
- **Izhodišča pri vpeljavi novih storitev**
  - preprosta, varna in uporabnikom prijazna uporaba storitev
  - koncept ˝plug-and-play˝
- **Zahtevane funkcionalnosti nosilne omrežne infrastrukture**
  - avtentikacija in avtorizacija uporabnikov ter terminalne opreme
  - avtomatska nastavitev inicializacijskih parametrov terminalne opreme
    - nastavitev parametrov IP
  - opcije, ki omogočajo uporabnikom dinamično izbiro storitve
  - interakcija s sistemi AAA (Radius)
- **V DSL se uporabljajo**
  - RADIUS
  - PPPoE
  - DHCP



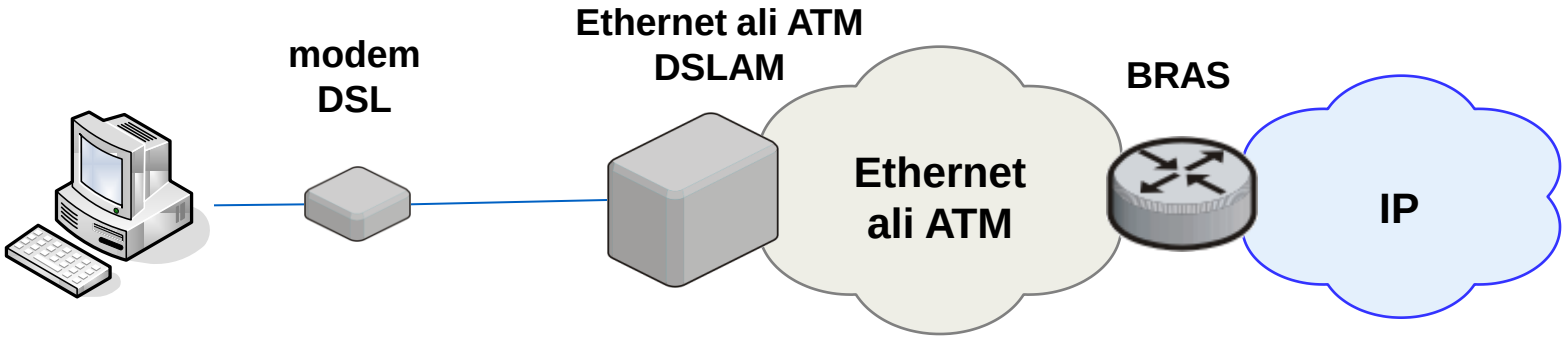
Storitveni model – protokol PPP

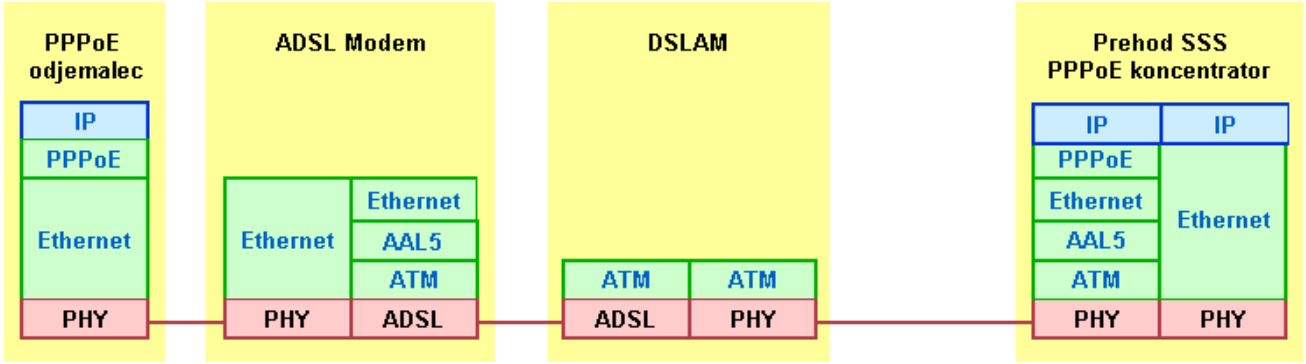
- Protokol, ki je bil v osnovi razvit za potrebe klicnega dostopa ˝dial-up˝ v omrežjih PSTN/ISDN
- Funkcionalnosti protokola PPP
  - mehanizem za nastavitev parametrov povezave
  - avtentikacija in avtorizacija uporabnikov
    - protokol PAP ali CHAP
  - opcije za dinamično izbiro storitev oziroma ponudnika storitev
    - protokola PAP ali CHAP ter razširitev uporabniškega imena
    - uporabnik@podjetje.si, uporabnik@isp.net
  - avtomatsko dodeljevanje mrežnih parametrov terminalni opremi
    - mehanizem IPCP (IP Control Protocol)
  - v povezavi s sistemi AAA omogoča zaračunavanje storitev
- Pomanjkljivosti protokola PPP
  - ne omogoča ˝multicast˝ prenosnega načina
    - multicast promet predstavlja večinski del prometa na dostopu
  - na napravah CPE je potrebno stalno vzdrževanje sej PPP
  - problem terminacije in vzdrževanja velikega števila sej PPP na BRAS

Koncept delovanja PPPoE

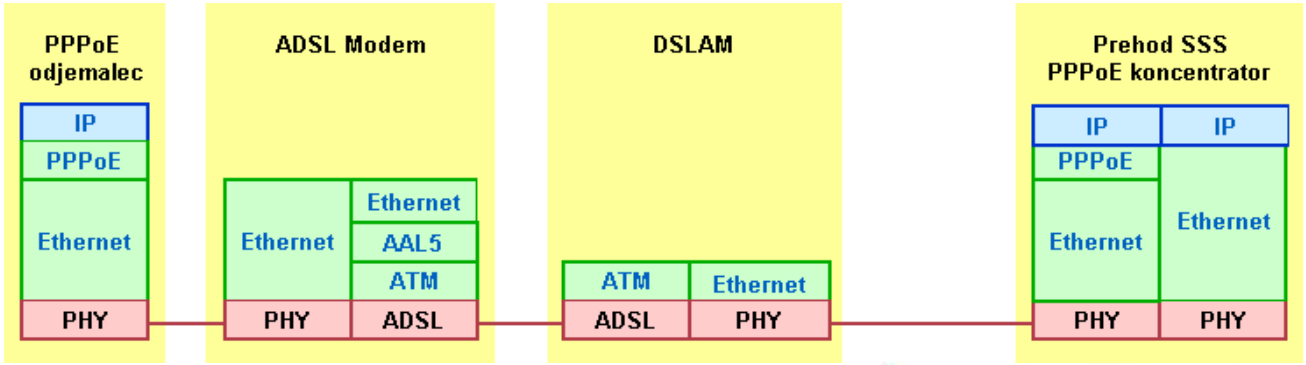


Protokolni sklad za model PPPoE





Agregacija na osnovi ATM

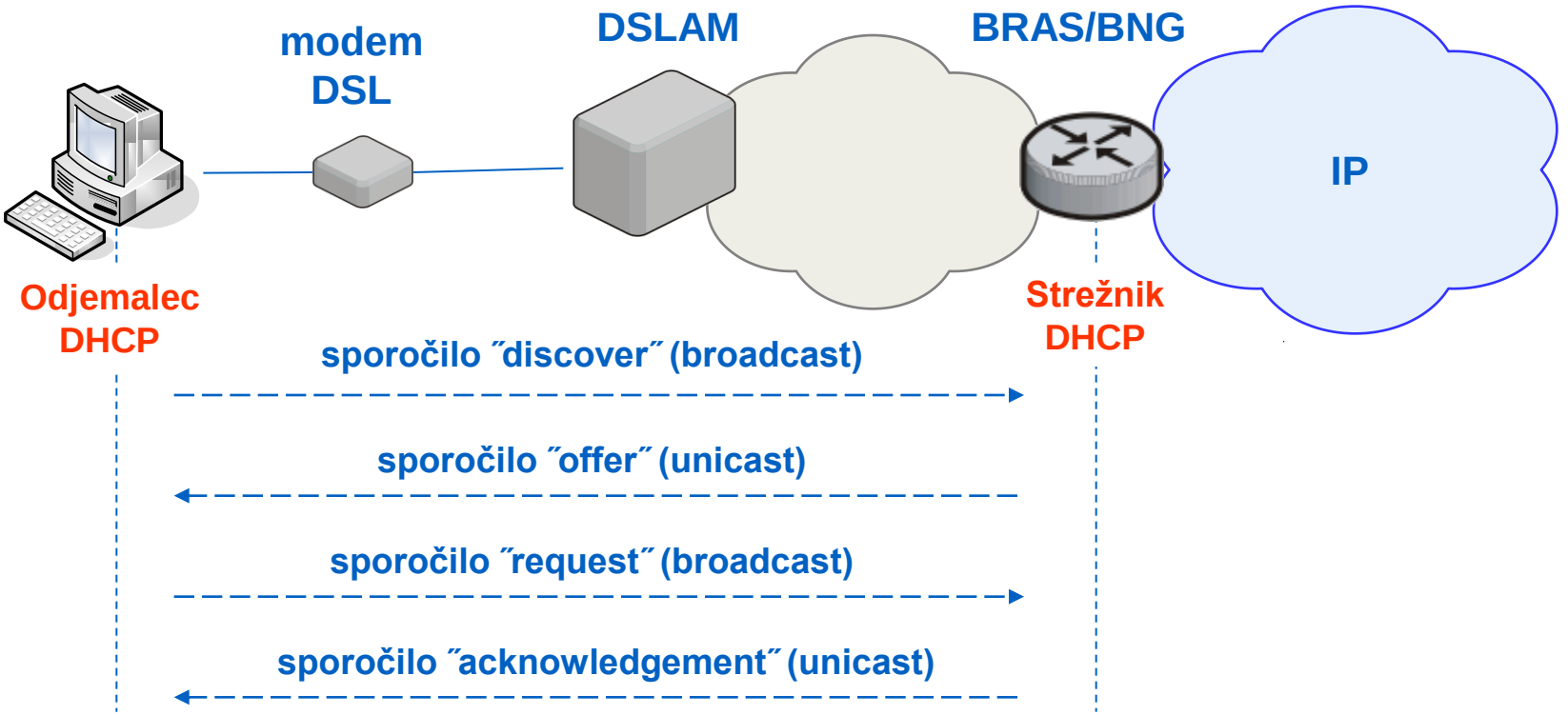


Agregacija na osnovi Ethernet

Storitveni model – protokol DHCP

- Protokol, ki je bil načrtovan za delovanje v omrežjih LAN
- V osnovi omogoča le avtomatsko nastavitev terminalov brez dodatnega ovijanja uporabniškega prometa
  - ločitev kontrolne funkcije od uporabniškega prometa
  - boljša razširljivost sistema
  - omogočen je multicast prenosni način
- Za zagotavljanje dodatnih funkcionalnosti (avtentikacija uporabnikov, možnost izbire storitve, izboljšani varnostni mehanizmi) so potrebne razširitve protokola DHCP
  - dodatna opcijska polja
  - agent DHCP ˝relay˝
  - DHCP v kombinaciji s spletnim portalom
  - DHCP v kombinaciji z mehanizmom IEEE 802.1X

Koncept delovanja DHCP



Razširitve protokola DHCP

- Dodatna opcijska polja
  - opcijsko polje 82
    - omogoča mapiranje poslanih zahtev DHCP s fizičnim vmesnikom ali logično povezavo uporabnika
  - opcijsko polje 77
    - omogoča dinamično izbiro storitev in avtentikacijo uporabnikov
- Agent DHCP ˝relay˝
  - funkcija DHCP ˝relay“ na napravah DSLAM in BRAS omogoča dodajanje informacije (opcijsko polje 82) o logičnem ali fizičnem vmesniku s katerega je bila poslana zahteva DHCP
  - omogoča posredno avtentikacijo uporabnika oziroma terminalne opreme
- Avtentikacijski mehanizmi
  - statično mapiranje naslovov IP in Ethernet MAC
    - možna je preprosta zloraba

Razširitve protokola DHCP

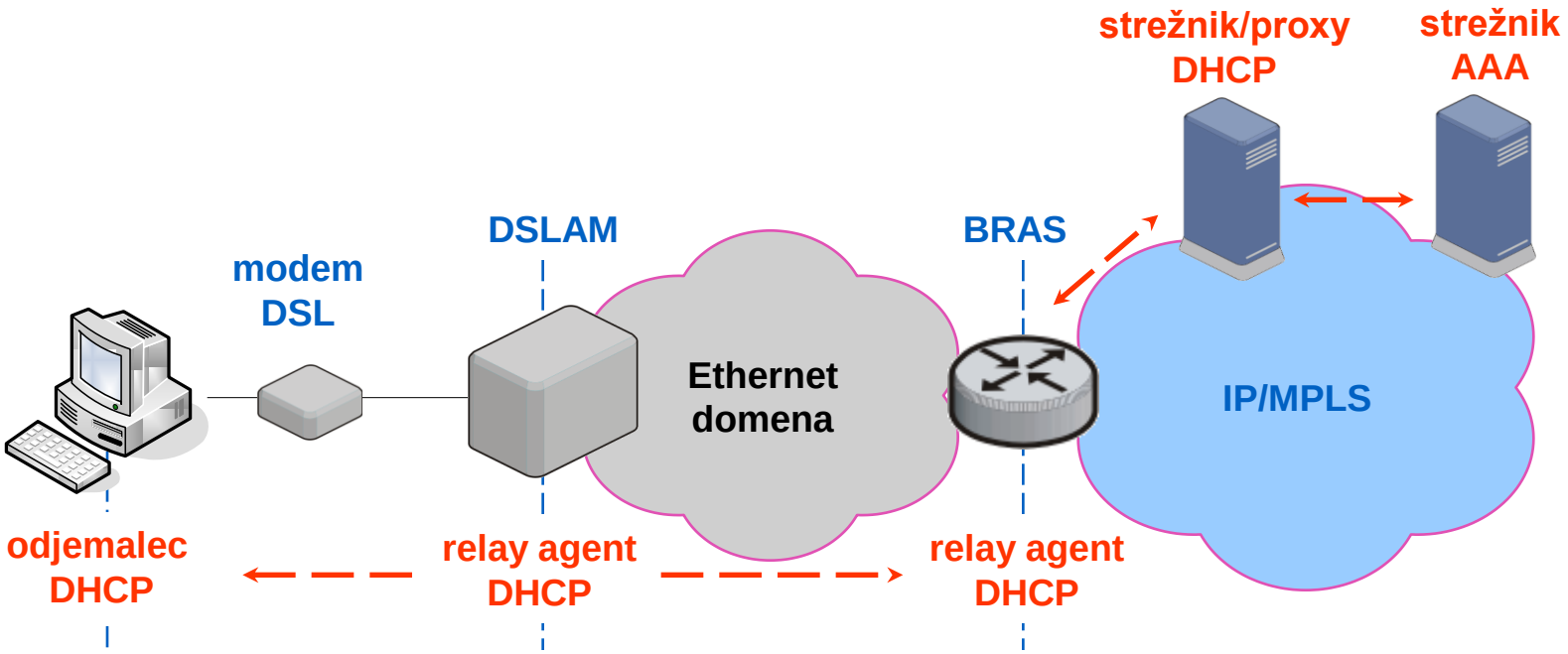
- **Opcijska polja DHCP**

Opcijsko polje	Ime polja	Namen polja	Referenca
43	Vendor Specific Information	Parametri specifični za posameznega proizvajalca opreme.	RFC 2132
60	Vendor class identifier	Identifikator proizvajalca terminalne opreme.	RFC 2132
67	Boot File Name	Ime konfiguracijske datoteke.	RFC 2132
77	User Class Information	Avtentikacija uporabnika in dinamična izbira storitve.	RFC 3004
82	Relay Agent Information	Mapiranje poslanih zahtev DHCP s fizičnim vmesnikom ali logično povezavo.	RFC 3046
120	SIP Servers DHCP Option	Naslov strežnika SIP.	RFC 3361
128	TFTP Server IP address[48]	Naslov strežnika TFTP na katerem se nahaja konfiguracijska datoteka telefona IP.	
129	Call Server IP address	Naslov klicnega strežnika.	
134	Diffserv Code Point	Vrednost polja DSCP.	
150	TFTP server address	Naslov strežnika TFTP.	

http://datatracker.ietf.org/wg/dhc/

Razširitve protokola DHCP

- DHCP relay
  - naprava DSLAM ali BRAS doda informacije (opcijsko polje 82) o logičnem ali fizičnem vmesniku s katerega je bila poslana zahteva DHCP
  - posredna avtentikacija uporabnika in terminalne opreme



Storitveni modeli DHCP 1/2

- **Fiksna izbira storitev in avtentikacija uporabnika na osnovi naslova Ethernet MAC**
  - **mapiranjem med naslovom Ethernet MAC in uporabnikom na strežniku DHCP oziroma sistemu AAA**
    - **za vsakega uporabnika in terminalno opremo je potrebno narediti vnos, ki ga povezuje s storitvami do katerih je upravičen**
    - **dodatni upravljalski stroški**
    - **možna je preprosta zloraba**
  - **nivo varnosti se lahko poveča z uporabo agenta DHCP ˝relay˝ in opcijskega polja 82 na napravi DSLAM**
    - **vezava uporabnika in terminalne opreme na uporabniški vmesnik na napravi DSLAM**
    - **mobilnost uporabnika in prenosljivost terminalne opreme sta onemogočena**
  - **rešitev se tipično uporablja v trenutnih implementacijah storitev IPTV in VoIP**

Storitveni modeli DHCP 2/2

- **Dinamična izbira storitev in avtentikacija uporabnikov na osnovi spletnega portala**
  - uporabniku se omogoči dostop do spletnega portala na katerem se izvede avtentikacija in izbira storitve
    - spletni portal izvaja interakcijo med sistemi AAA in strežnikom DHCP (prehodom BRAS)
  - ob uspešno izvedeni avtentikaciji in avtorizaciji je strežnik DHCP (oziroma naprava BRAS) obveščen o izbrani storitvi uporabnika
    - terminalni opremi se dodelijo se novi parametri IP, ki ji omogočajo dostop do izbrane storitve
  - pomanjkljivosti modela
    - omejena je na terminalno opremo, ki ima podprt spletni vmesnik
    - potreben je dodaten spletni strežnik, ki omogoča izvajanje interakcije med sistemi AAA, strežnikom DHCP oziroma napravo BRAS
    - naprava BRAS mora podpirati dodatne preusmeritvene in odjemalske funkcije, ki so v splošnem kompleksne in drage
- **Dinamična izbira storitve in avtentikacija uporabnikov z mehanizmom 802.1X**

Primerjava modelov PPP in DHCP

- Storitveni model DHCP se razvija v smeri podpore ekvivalentnih funkcij, kot jih ponuja mehanizem PPP
- Ključne prednosti modela DHCP
  - podpora za multicast prenosni način
  - ločitev kontrolne funkcije od posredovalne omogoča dobro razširljivost sistema
- V trenutnih implementacijah omrežij DSL še vedno prevladuje kombinacija modelov PPP in DHCP
  - za dostop do interneta se uporablja mehanizem PPPoE
  - za zagotavljanje storitev IPTV in VoIP se uporablja mehanizem DHCP

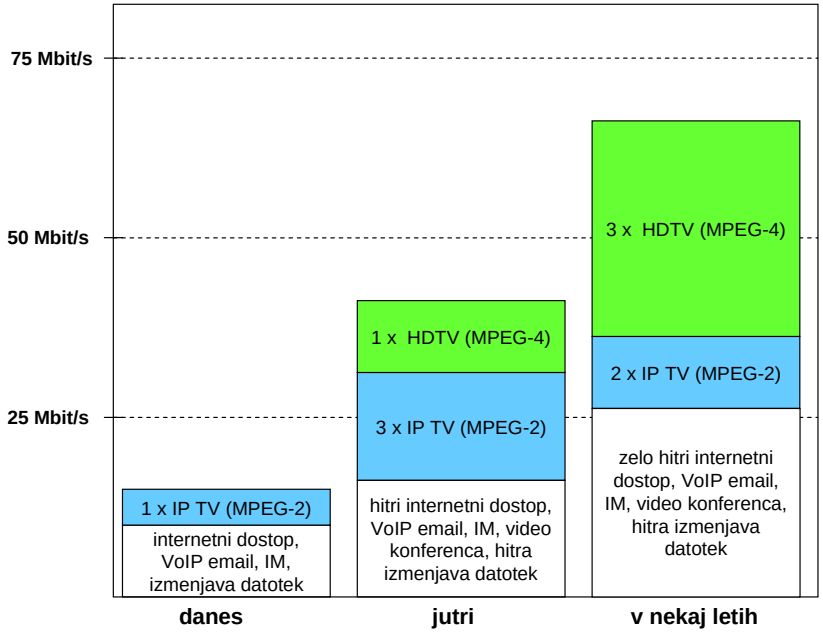
Prometno načrtovanje xDSL

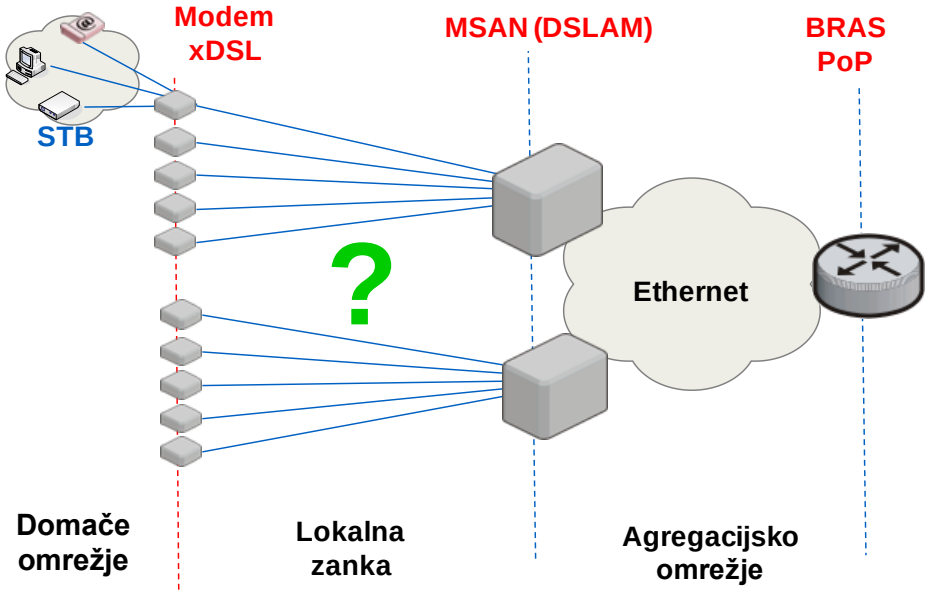
Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- Izbira agregacijskega modela
- Izbira opreme

Potrebe po pasovni širini

- Zahtevana pasovna širina na uporabnika določa uporabljeno tehnologijo v lokalni zanki





Prometna analiza za 3play naročnika

- **Prometna analiza za 1 naročnika**
  - pasovna širina – internet
    - simetrična : UL/DL = 2 Mbit/s
    - asimetrična: UL = 512 Kbit/s, DL = 2 Mbit/s
  - pasovna širna – IP TV (1 TV Kanal, kvaliteta “SD TV”)
    - ~5 Mbit/s (DL) – kodek MPEG-2
    - ~2 Mbit/s (DL) – kodek MPEG-4
  - pasovna širina – VoIP
    - promet RTP (G711) z upoštevano signalizacijo (SIP): UL/DL = 100Kbit/s

Kodek	velikost paketa	Število paketov na sekundo	Velikost paketa VoIP	Potrebna pasovna širina
G.711	160 oktetov	50	200 oktetov	80 Kbit/s
G.711	240 oktetov	33	280 oktetov	74 Kbit/s
G.729A	20 oktetov	50	60 oktetov	24 Kbit/s

- **Pasovna širina lokalne zanke**
  - v smeri proti uporabniku (internet, IPTV, VoIP) = 7.1 Mbit/s
  - v smeri proti omrežju?

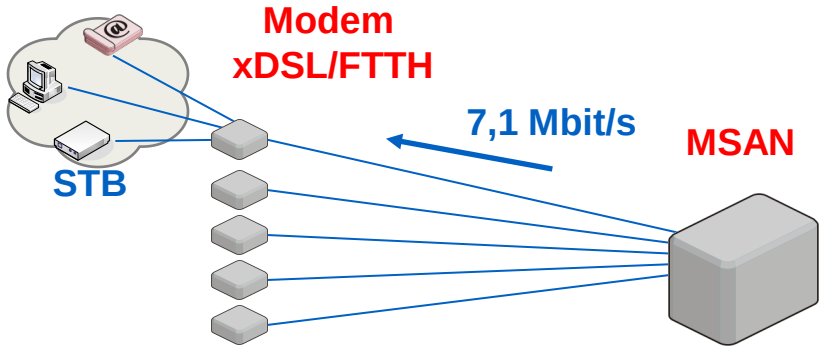
Kazalo

- Prometno načrtovanje naročniške zanke
- **Prometno načrtovanje MSAN**
- Izbira agregacijskega modela
- Izbira opreme

Prometna analiza za MSAN (DSLAM)

- **Prometna analiza za MSAN**
  - na MSAN bo priključenih 600 naročnikov
  - vsi naročniki bodo uporabljali: internet, VoIP, IPTV
- **Skupna potrebna pasovna širina na vmesniku MSAN**
  - 7,1 Mbit/s/uporabnika × 600 uporabnikov = 4,3 Gbit/s?
  - upoštevamo dobitek statističnega multipleksa => 731 Mbit/s

Storitev	Enota	Povprečna pasovna širina	Koncentracija	Skupna pasovna širina
HSI	600 naročnikov	2 Mbit/s	1:10	120 Mbit/s
VoIP	600 naročnikov	100 Kbit/s	0.18 (Erlang)	11 Mbit/s
IPTV	120 TV programov	5 Mbit/s	-	600 Mbit/s



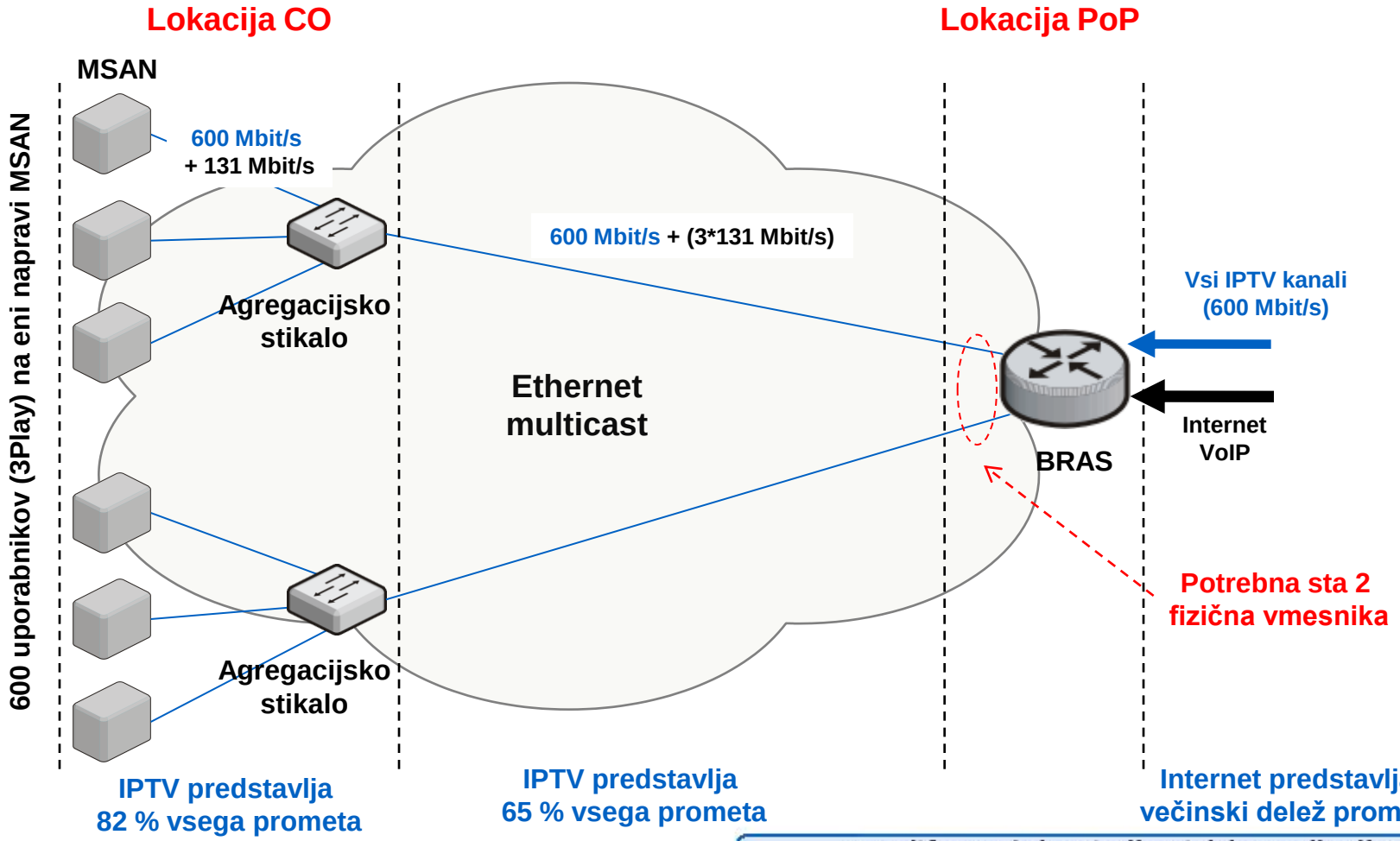
IPTV (multicast) predstavlja
82 % vsega prometa

Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- **Izbira agregacijskega modela**
- Izbira opreme

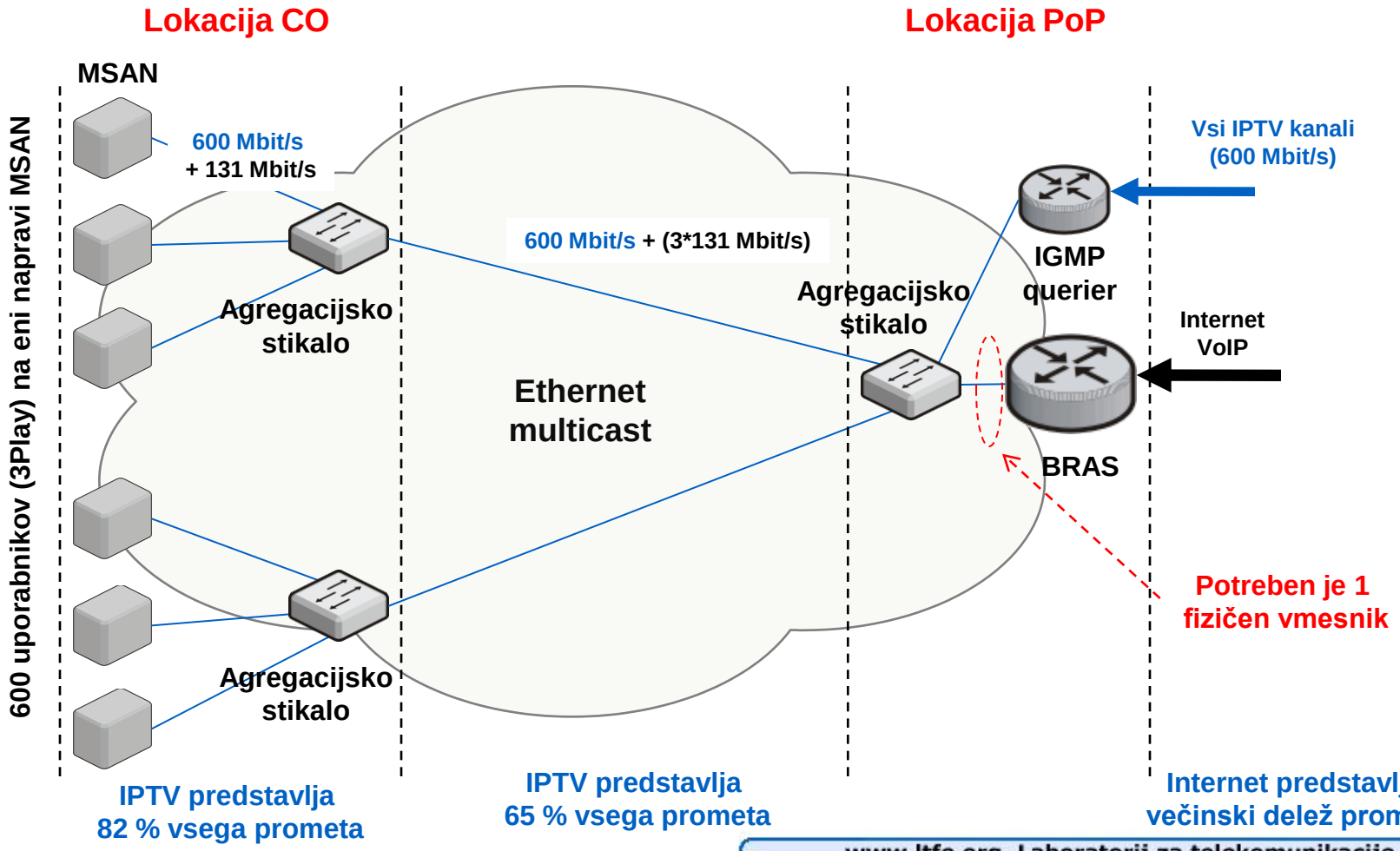
Agregacijski model – IPTV prek BRAS

- **Značilnosti rešitve**
  - **Single Edge model, eno nivojska agregacija, topologija zvezda**



Agregacijski model – IPTV mimo BRAS

- **Značilnosti rešitve**
  - **Dual Edge model, dvo nivojska agregacija, topologija zvezda**

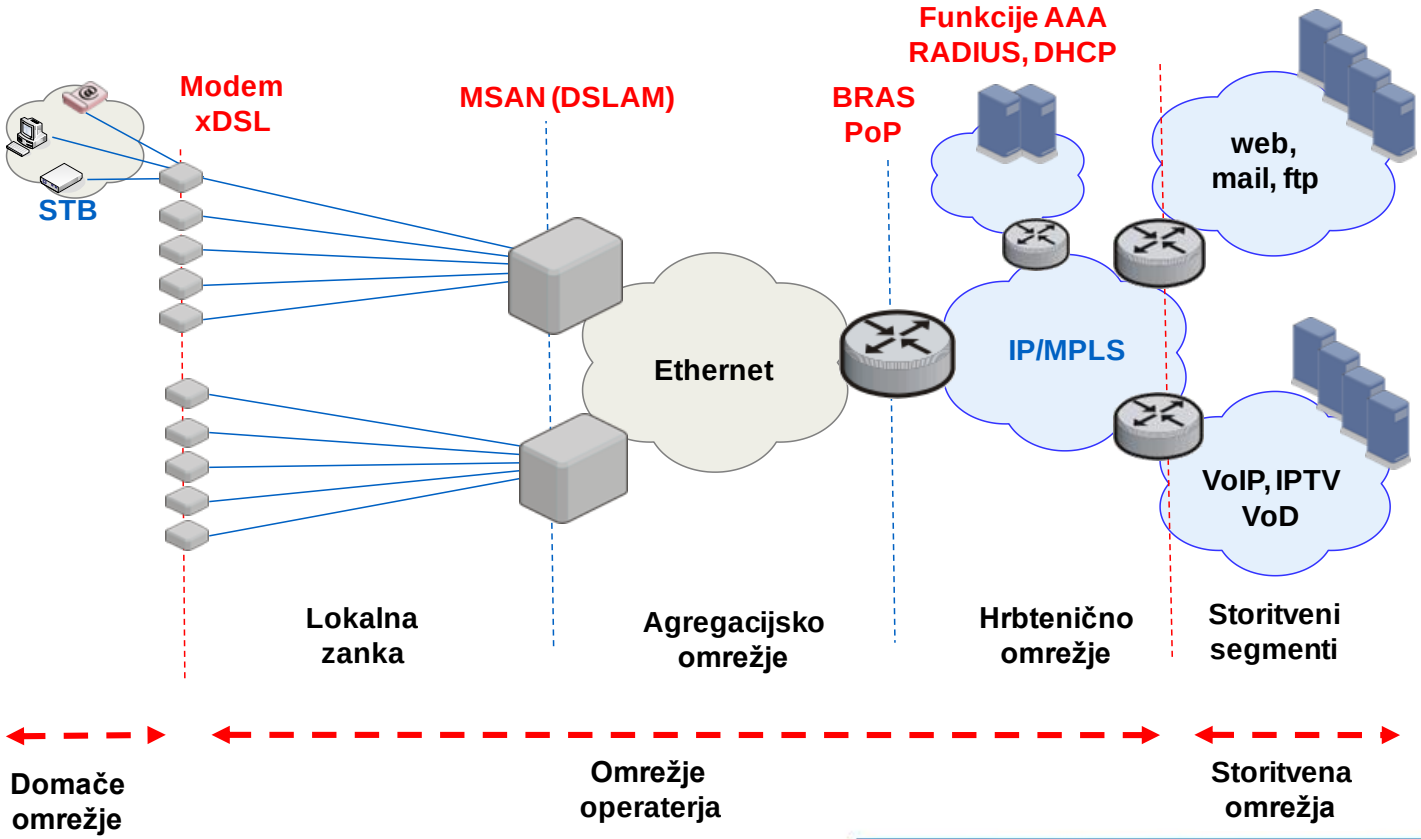


Kazalo

- Prometno načrtovanje naročniške zanke
- Prometno načrtovanje MSAN
- Izbira agregacijskega modela
- Izbira opreme

Zmogljivosti in funkcionalnosti opreme

- **Določitev potrebnih funkcionalnosti naprav**
  - **Katere funkcije se izvajajo v HW (FPGA/ASIC)?**
  - **Katere funkcije se lahko v SW (CPU)?**



Zmogljivosti naprav

- Ethernet stikala
  - kateri vmesniki (GE, 10GE, 40GE), število vmesnikov
    - hitrost Ethernet stikalne matrike – paketi na sekundo (pps)
    - število (HW) čakalnih vrst
  - število vnosov v tabelo MAC
  - napredne funkcionalnosti
    - IGMP Snooping, DHCP relay – število zahtev
- Usmerjevalniki/BRAS
  - kateri vmesniki (GE, 10G, 40GE), število vmesnikov
    - hitrost IP posredovalne matrike – paketi na sekundo (pps)
    - število (HW) čakalnih vrst
  - število vnosov v usmerjevalno tabelo
  - napredne funkcionalnosti
    - terminacija PPP – število sej, hitrost vzpostavljanja sej
    - IGMP querier, DHCP relay – število zahtev
    - Radius – število zahtev
    - IP session aware – število sej

Primer izračuna zmogljivosti

- **Hitrost posredovanja = X pps × 64 oktetov [Mbit/s]**
  - **pri izračunu je upoštevana najmanjša velikost paketa IP (64 oktetov)**

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
7304-NSE-150			3,500,000(PXF) 800,000(RP)	1,792 409.6	No
7304-NPE-G100			1,099,000	562.69	No
7301	79,000	40.448	1,018,000	521.22	No
7401	20,000	10.24	300,000 (Also has PXF)	153.6	30-Dec-04
7000-RP	2,500	1.28	30,000	15.36	31-Jul-97
7500-RSP2	5,000	2.56	220,000	112.64	16-Feb-03
7500-RSP4/4+	8,000	4.096	345,000	176.64	15-Dec-07
7500-RSP8	22,000	11.264	470,000	240.64	15-Dec-07
7500-RSP16	29,000	14.848	530,000	271.36	15-Dec-07
7500-VIP2/40	Punts to RSP[1]		60,000 – 95,000	30.7 – 48.6	30-Apr-04
7500-VIP2/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-May-03
7500-VIP4/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-Dec-07
7500-VIP4/80	Punts to RSP[1]		140,000 – 210,000	71.7 – 107.5	15-Dec-07
7500-VIP6/80	Punts to RSP[1]		140,000 – 219,000	71.7 – 112.1	15-Dec-07
7600-MSFC2(Sup2)	20,000 (500,000 for software-switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic - 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	1-Mar-07
7600-MSFC2A(Sup32)			15,000,000[2]	7,680.00	No
7600-MSFC3(Sup720)	20,000 (500,000 for software switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic – 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	No

10 Mbit/s vs 15 Gbit/s!

These are testing numbers, usually with FE to FE, GigE to GigE or POS to POS, no services enabled. As you add ACL's, encryption, compression, etc - performance will decline significantly from the given numbers, unless it is a hardware-assisted platform, such as the ASR 1000, 7600 or 12000, which process QoS, ACL's, and other features in hardware (or when a hardware assist is installed, for instance an AIM-VPN in a 3745 will offload the encryption from the CPU). Every situation is different - please simulate the true environment to get applicable performance values

http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

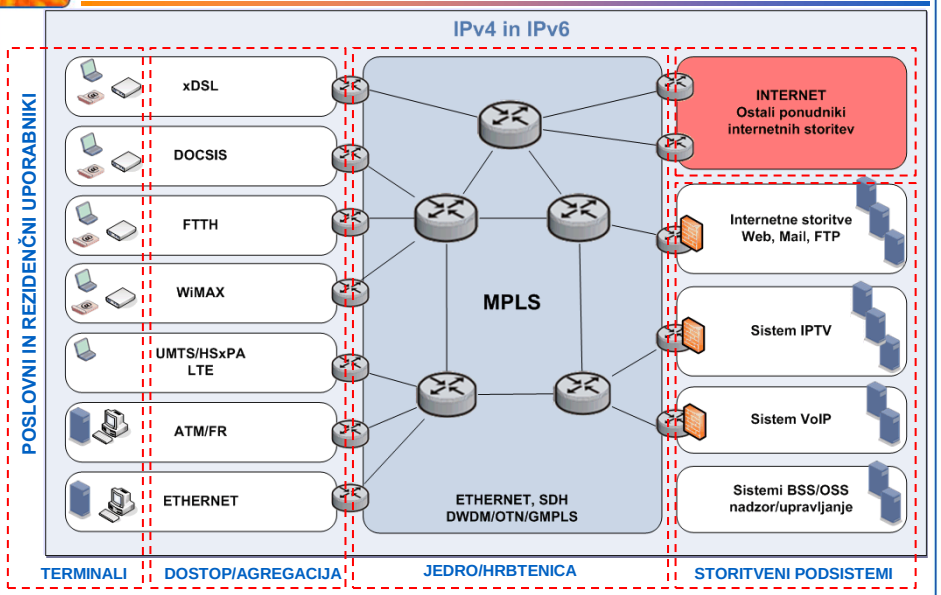
Večprotokolna komutacija z zamenjavo label

MPLS – MultiProtocol Label Switching

Sodobna omrežja

- Potrebne funkcionalnosti in mehanizmi v sodobnih omrežjih
  - navidezna zasebna omrežja (angl. VPN – Virtual Private Network)
  - zaščitni mehanizmi (angl. Protection)
  - kakovost storitev (angl. QoS – Quality of Service)
  - prometni inženiring (angl. TE – Traffic Engineering)
- Katero tehnologijo uporabiti?
  - cena
  - zmogljivost
  - razširljivost/skalabilnost
  - kompleksnost
  - upravljanje
  - standardizacija

Transportni sloj sodobnih omrežij



Omrežne storitve 1/2

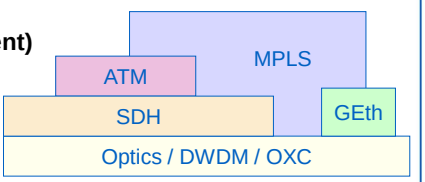
	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Podatkovna raven	Globalno naslavljanje		Unicast naslavljanje	-	✓	✓	-
			Multicast naslavljanje	-	✓	✓	-
			Anycast naslavljanje	-	✓	✓	-
	Lokalno naslavljanje		Unicast naslavljanje	✓	✓	✓	✓
			Multicast naslavljanje	✓	✓	✓	✓
			Anycast naslavljanje	-	✓	✓	-
			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

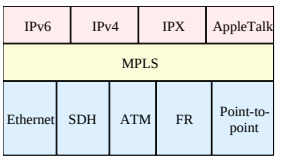
Uvod v MPLS

- **Izhodišče**
  - IP kot “najbolj razširjen” L3 protokol
  - ATM tehnologija z odličnimi koncepti, vendar slabo prilagojena IP-ju
- **Tehnologija, ki bo združila najboljše koncepte iz ATM in IP**
  - IP kontrolna ravnina (naslavljanje in usmerjanje IP)
  - koncept label (analogija VPI/VCI ATM, lokalen pomen)
- **Tehnologija naj ne bo vezana na nobeno specifično L1/L2 tehnologijo oziroma noben specifičen L3 protokol**
- **Začetki - več samostojnih poizkusov podjetij (1995)**
  - IP Switching (Ipsilon/Nokia)
  - Tag Switching (Cisco)
  - IP Navigator (Cascade/Ascend/Lucent)
  - ARIS (IBM)
- **Standardizacija v IETF**
  - nevtralno ime – MPLS



Glavne ideje MPLS

- Ločiti
  - posredovalne funkcije (labela, MPLS glava)
  - od usmerjevalnih funkcij (usmerjanje IP)
- En sam posredovalni mehanizem, ki ...
  - zamenjava label
  - “povezavno naravnana” tehnologija
- ... podpira več različnih usmerjevalnih mehanizmov
  - izboljšati zmogljivost in razširljivost (IP) posredovanja
  - omogočiti enostavnejše eksplicitno usmerjanje in prometni inženiring
- Koncept zamenjave label deluje prek različnih L1 in L2 tehnologij
  - različna poimenovanja, različna “implementacija” label
  - MPLS glava na SDH, VCI/VPI na ATM, lambda na OXC, ...
- Fleksibilnost pri določanju FEC in mapiranju le-teh na LSP
  - FEC so paketi, ki jih omrežje obravnava na enak način
- Hierarhija na osnovi sklada label

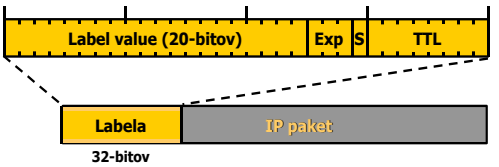


Osnovni koncepti MPLS

- 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. IP), ki so na usmerjevalniku LSR obravnavani na enak način

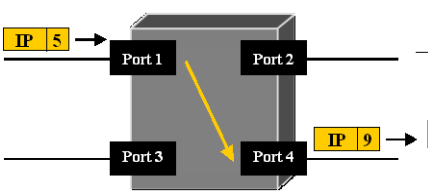
Osnovni koncepti – glava MPLS

- 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)
    - 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

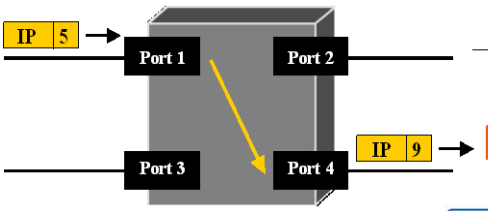
- Angl. LSR – Label Switched Router
  - vhodni, tranzitni, izhodni
  - nad glavo MPLS lahko izvaja tri osnovne operacije
    - vstavitev labele/glave MPLS
    - zamenjava labele/glave MPLS
    - odstranitev labele/glave MPLS
- Zamenjava glave MPLS
  - vhodni vmesnik in labela določata
    - operacijo: vstavi, 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
  - LSP je enosmeren (simplex) tunel skozi omrežje MPLS
  - predstavlja zaporedje enega ali več hopov z zamenjavo label
    - analogija ATM in FR navideznim potem/kanalom



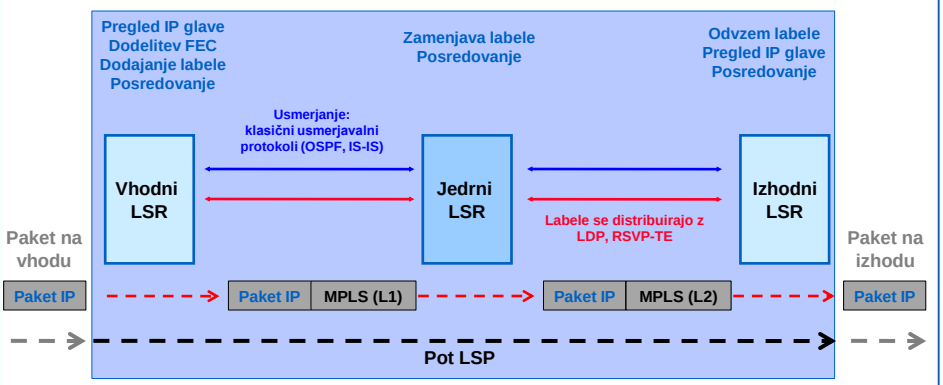
Vhod (port, labela)	Izhod (port, labela)	Labela Operacija
(1, 2)	(2, 7)	Zamenjava
(1, 4)	(3, 7)	Zamenjava
(1, 5)	(4, 9)	Zamenjava
(2, 3)	(3, 2)	Zamenjava

Osnovni koncepti – razred FEC

- Ekvivalentni posredovalni razred
  - FEC – Forwarding Equivalence Class
- Predstavlja pretok paketov (npr. IP), ki so 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
  - naslov/subnet IP – ciljni, izvorni
  - polje ToS/DSCP

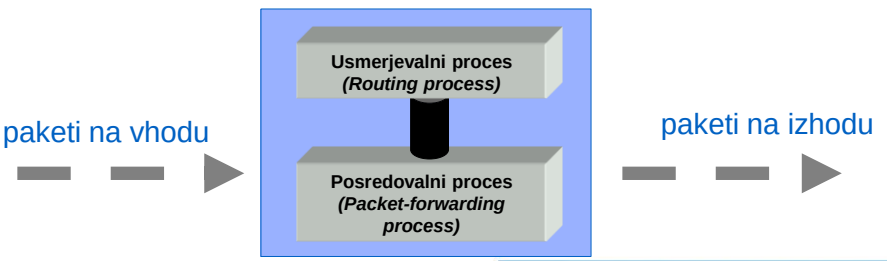
Delovanje MPLS

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



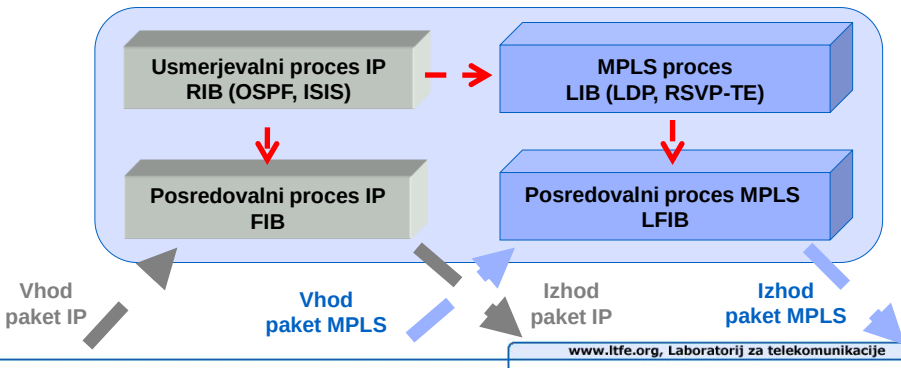
Zgradba usmerjevalnika IP

- **Usmerjevalni proces – kontrolna ravnina**
  - izmenjava usmerjevalnih informacij
  - določitev optimalne poti skozi omrežje
  - izvaja se lahko v nerealnem času (sekunde)
- **Posredovalni proces – podatkovna ravnina**
  - določitev ustreznega izhodnega vmesnika
  - posredovanje paketa IP na izhodni vmesnik
  - izvajati se mora v realnem času (mikro sekunde)



MPLS na usmerjevalniku IP

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



Signalizacija v MPLS

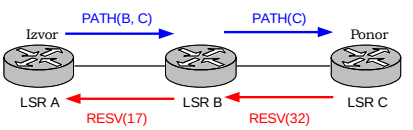
- Mehanizmi za izmenjavo label med usmerjevalniki LSR
- Protokol za distribucijo label
  - angl. LDP – Label Distribution Protocol
  - protokol za avtomatsko vzpostavljanje LSP
  - izbere isto pot kot uporabljen usmerjevalni protokol IGP (OSPF, IS-IS)
- Protokol rezervacije virov s prometno razširitvijo
  - angl. RSVP-TE – Resource Reservation Protocol - Traffic Extension
  - podpora eksplicitno (prometni inženiring) vzpostavljenim potem
  - pot je določena glede na metriko IGP ter parametre TE
- Protokol za distribucijo label z omejitvam
  - angl. CR-LDP – Constraint based-Label Distribution Protocol
  - predstavlja nadgradnjo protokola LDP za potrebe prometnega inženiringa
  - podpora eksplicitno vzpostavljenim potem
  - ni zaživel v operaterskih okoljih

Protokol LDP

- Zagotavlja, da imajo sosednji usmerjevalniki skupen pogled na povezavo med labelami in razredi FEC
  - za usmerjanje se uporabljajo običajni protokoli IGP
  - izbere isto fizično pot kot uporabljen usmerjevalni protokol IGP (OSPF, IS-IS)
  - deluje v načinu ˝hard state˝, eksplicitno vzpostavljanje in rušenje poti
- Sporočila LDP
  - ˝Discovery message˝
    - uporablja se za odkrivanje novih sosedov LSR
    - sporočilo ˝hello˝ (UDP) se pošlje vsem usmerjevalnikom LSR (naslov multicast)
    - nadaljnja komunikacija med LSR-ji poteka na osnovi protokola TCP
  - ˝Session message˝
    - uporablja se za vzpostavljanje, vzdrževanje in rušenje sej LDP
  - ˝advertisment messages˝
    - oglaševanje label
  - notification messages
    - obveščanje o napakah

Protokol RSVP-TE

- Predstavlja nadgradnjo protokola za rezervacijo virov
  - angl. RSVP – Resource Reservation Protocol
- Omogoča vzpostavljanje point-to-point poti LSP, ki zadoščajo zahtevam (TE)
- Za prenos sporočil uporablja protokol IP
  - protokol mora sam poskrbeti za ponovno oddajo izgubljenih paketov
- Deluje v načinu ˝soft state˝
  - za ohranjanje LSP je potrebno pošiljanje “refresh” sporočil
- Za distribucijo label uporablja metodo ˝downstream-on-demand˝
  - dve vrsti sporočil: PATH (zahteva) in RESV (odgovor)



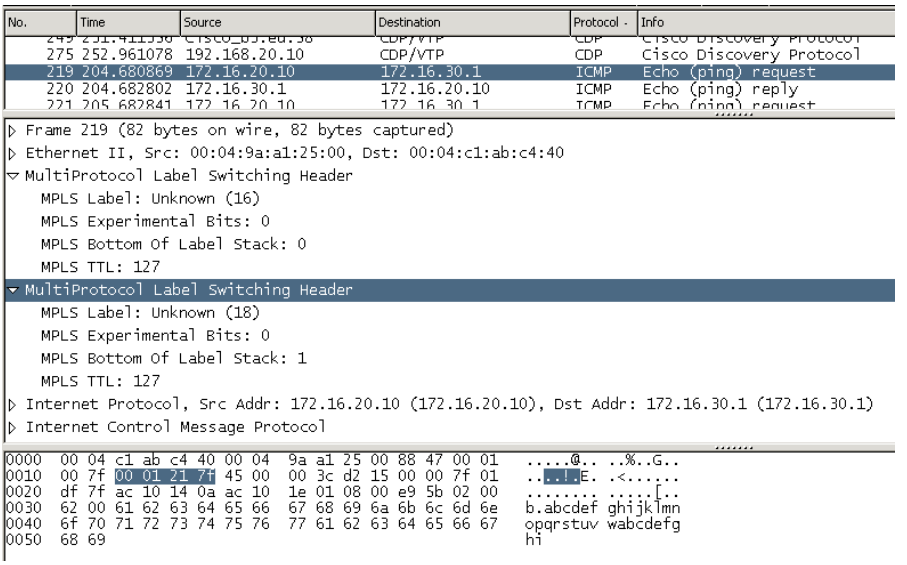
Protokol CR-LDP

- Predstavlja nadgradnjo protokola LDP
- Omogoča vzpostavljanje point-to-point poti LSP, ki zadoščajo zahtevam (TE)
- Za prenos sporočil uporablja protokol TCP
  - odkrivanje sosedov na osnovi multicast 'HELLO' sporočil (protokol UDP)
- Deluje v načinu ˝hard state˝, eksplicitno vzpostavljanje in rušenje poti
  - osveževanje poti ni potrebno

Primerjava RSVP-TE in CR-LDP

	RSVP-TE	CR-LDP
Transport	protokol IP	protokola UDP (hello&discovery) in TCP (adjacency)
Stanje vzpostavljenih povezav	˝soft state˝ (potrebno je periodično osveževanje)	˝hard state˝ (stalna povezava, osveževanje ni potrebno)
pobudnik vzpostavitve	vhodni LSR	izhodni LSR
varnostni mehanizmi	DA (MD5)	DA (IPSec, MD5)
Podpora za multicast	NE	NE
Združevanje LSP (multipoint-to-point)	DA	DA
Preprečevanje zank	DA	DA
Hitra preusmeritev poti (FRR)	DA	DA
Vrste poti	stroge, ohlapne	stroge, ohlapne
Razširljivost	Delna	Dobra

Primer zajetega paketa MPLS



Uporaba/aplikacije MPLS

- Integracija ATM stikal in usmerjevalnikov (zgodovina)
  - MPLS ni samo integracija IP in ATM, to je le ena izmed aplikacij MPLS
- Eksplicitno usmerjanje
  - prometni inženiring
  - hitre preusmeritve (Fast ReRoute)
- Navidezna zasebna omrežja
  - BGP/MPLS VPN (L3 MPLS VPN)
  - FR/ATM/Ethernet/PPP/HDLC prek MPLS (L2 MPLS VPN)
- Kakovost storitev
- MPLS kot kontrolna ravnina za druge L1/L2 tehnologije
  - GMPLS (MPλS)

Telekomunikacije in informacijske tehnologije
Laboratorij za telekomunikacije
Fakulteta za elektrotehniko

Virtualizacija v omrežjih

Univerza v Ljubljani
Fakulteta za elektrotehniko
Laboratorij za telekomunikacije

Ljubljana, maj 2011

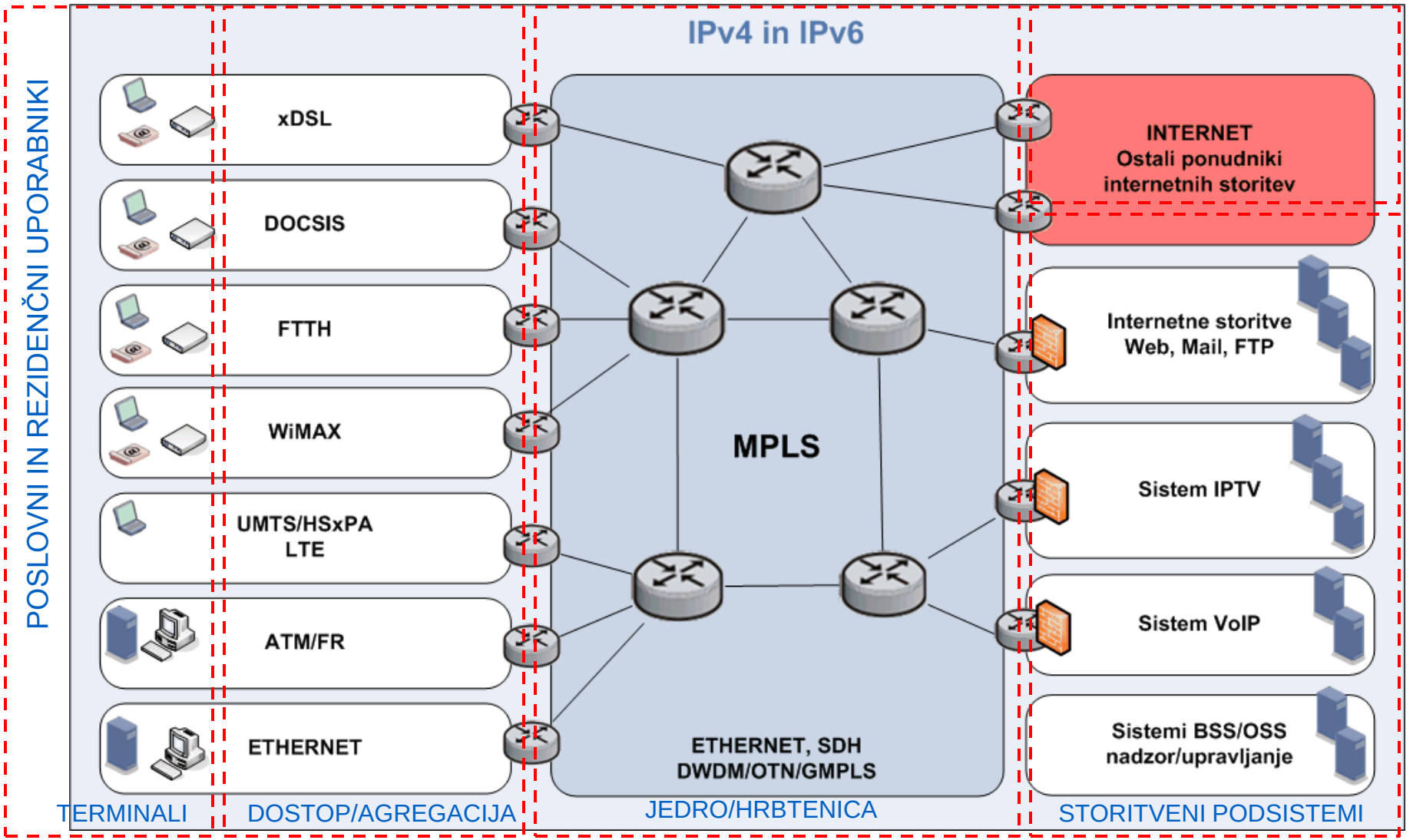
Vsebina

- 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

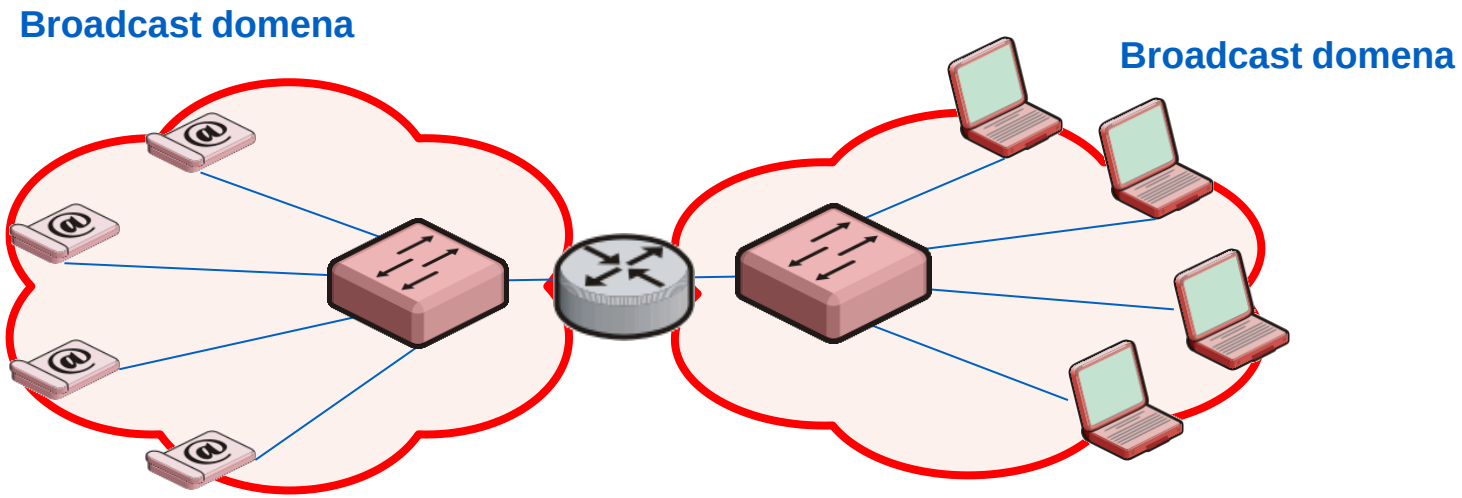
- Uvod
- Transportne tehnologije
  - Ethernet
  - IP
  - MPLS
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

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

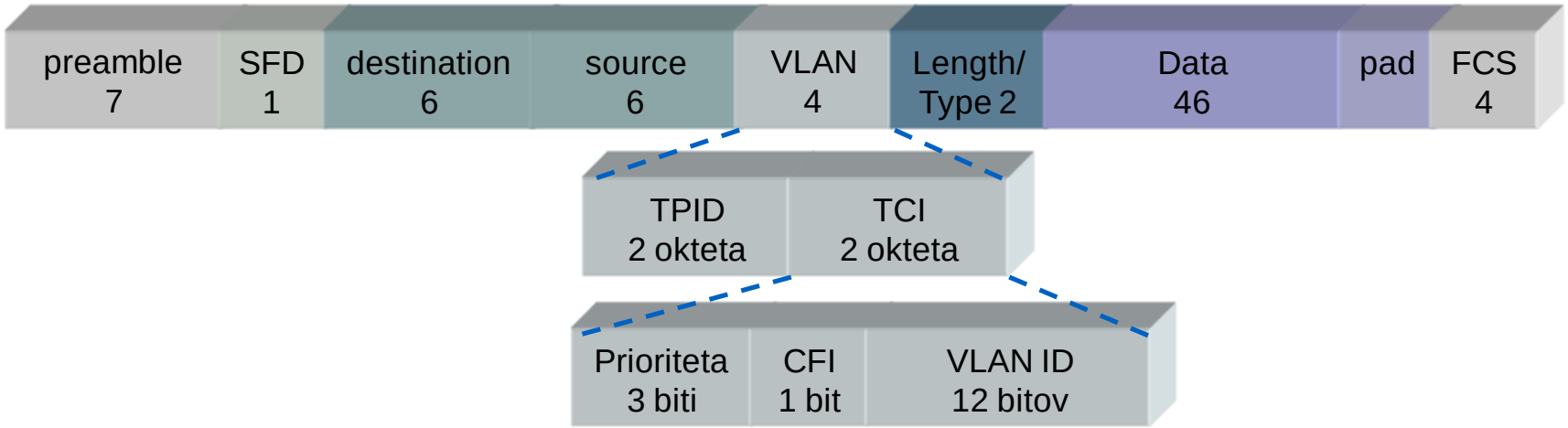
- Uporabniška vsebina se prenaša v okvirjih Ethernet
  - uporabniška vsebina – paketi IPv4, IPv6, ARP, MPLS
- Naloga okvirja Ethernet
  - prenos “bitov – uporabniške vsebine” prek fizičnega medija
  - naslavljanje Ethernet naprav, odkrivanje napak pri prenosu
- Vsebina in velikost okvirja Ethernet je 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

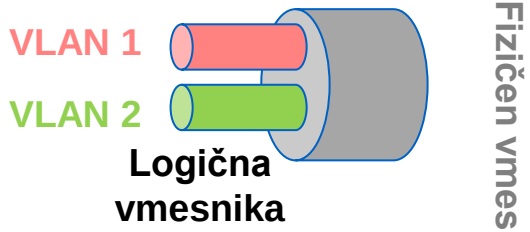
Tehnologija VLAN

- 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)

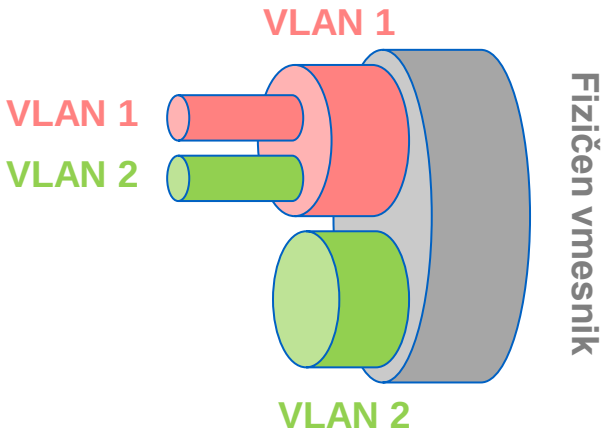


VLAN virtualizacijski mehanizmi 1/3

- 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)



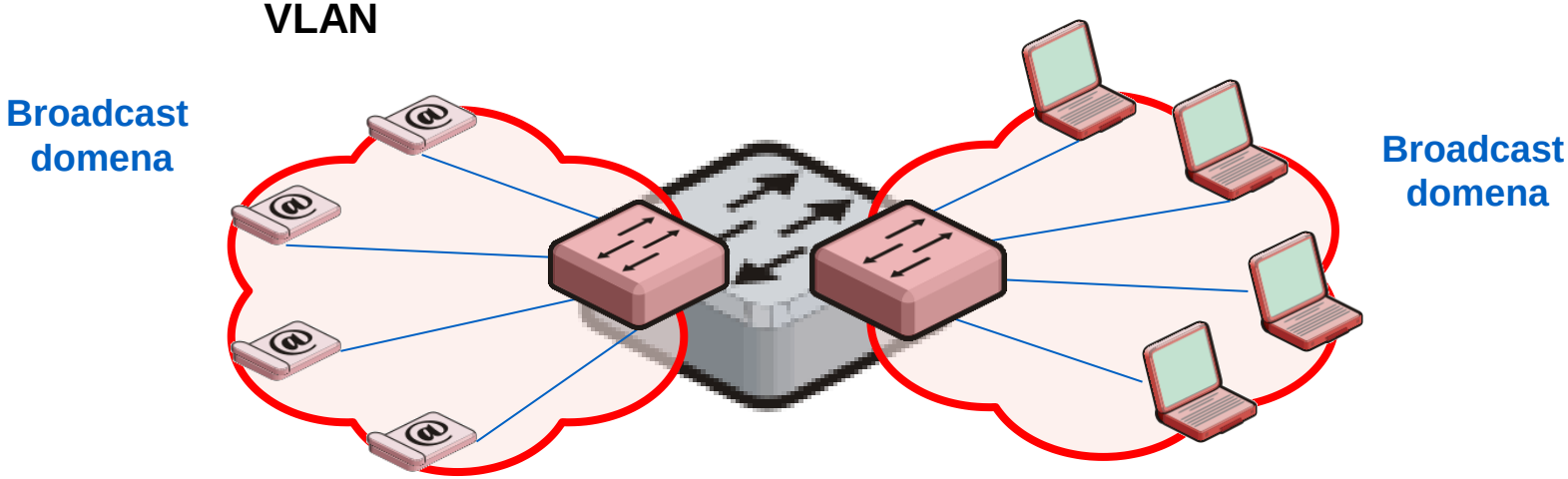
Koncept VLAN



Koncept QinQ

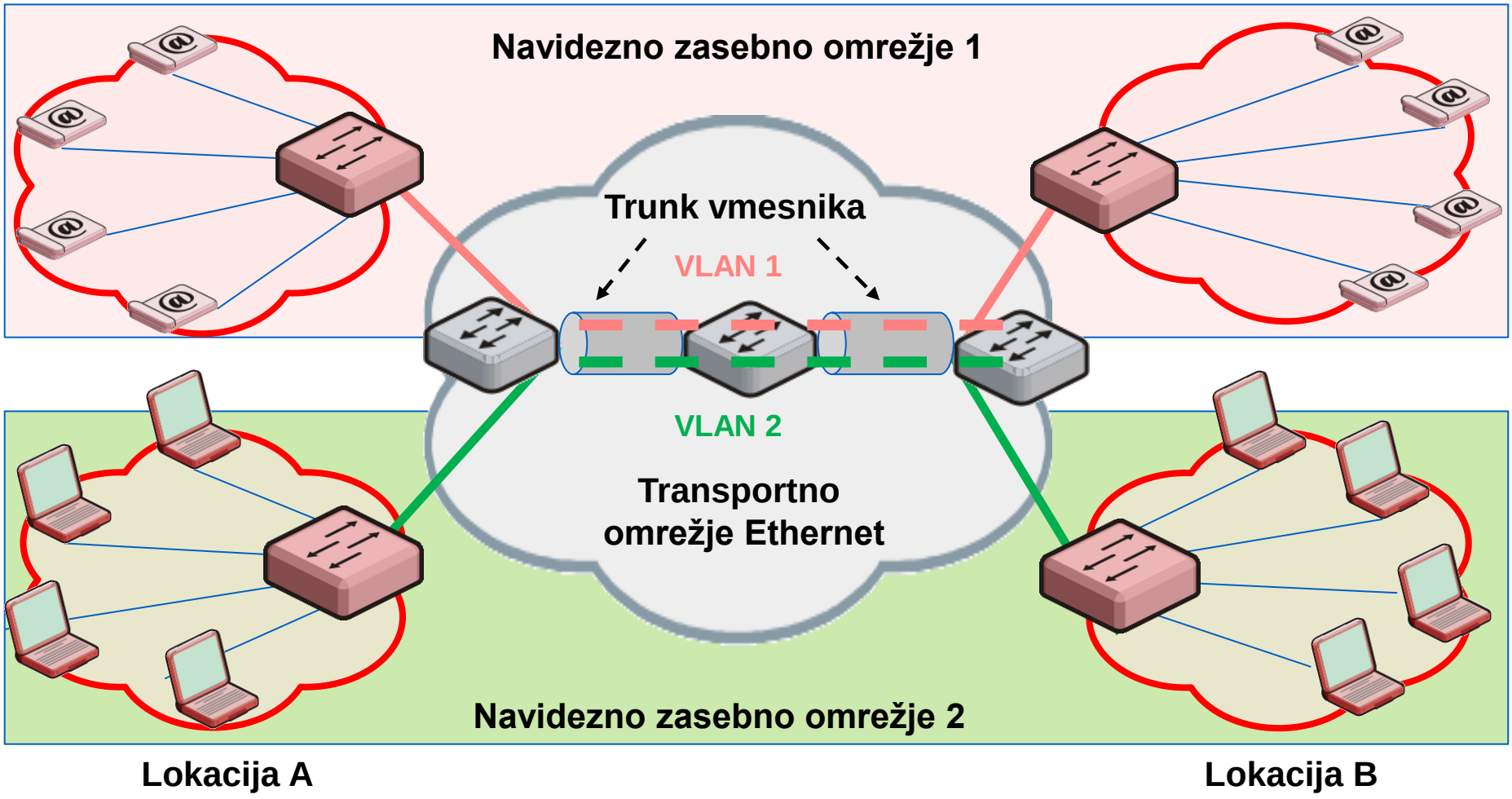
VLAN virtualizacijski mehanizmi 2/3

- 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

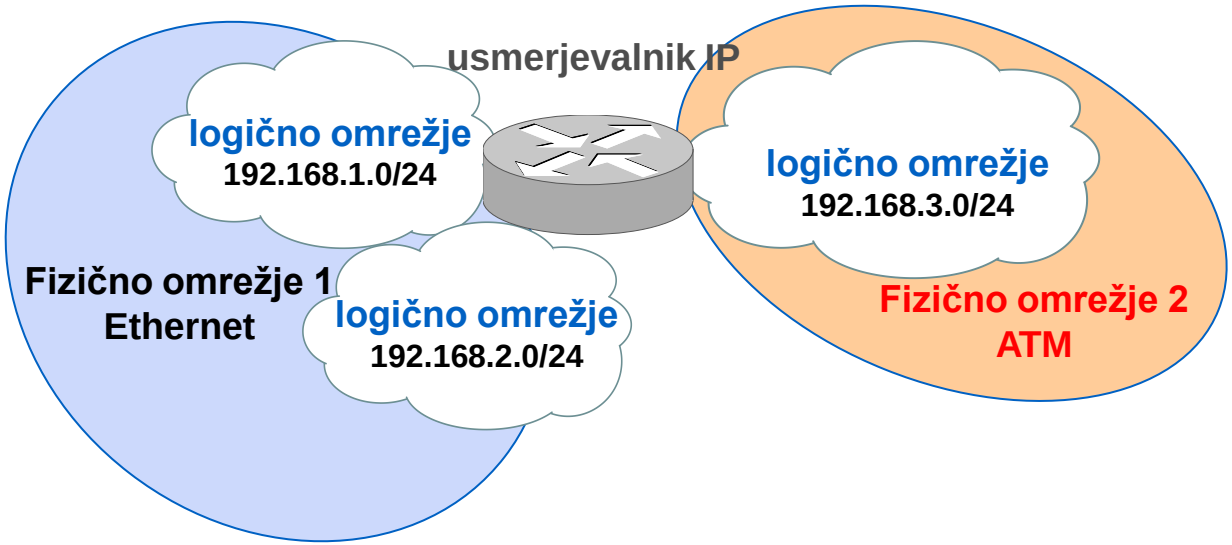


Vsebina

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

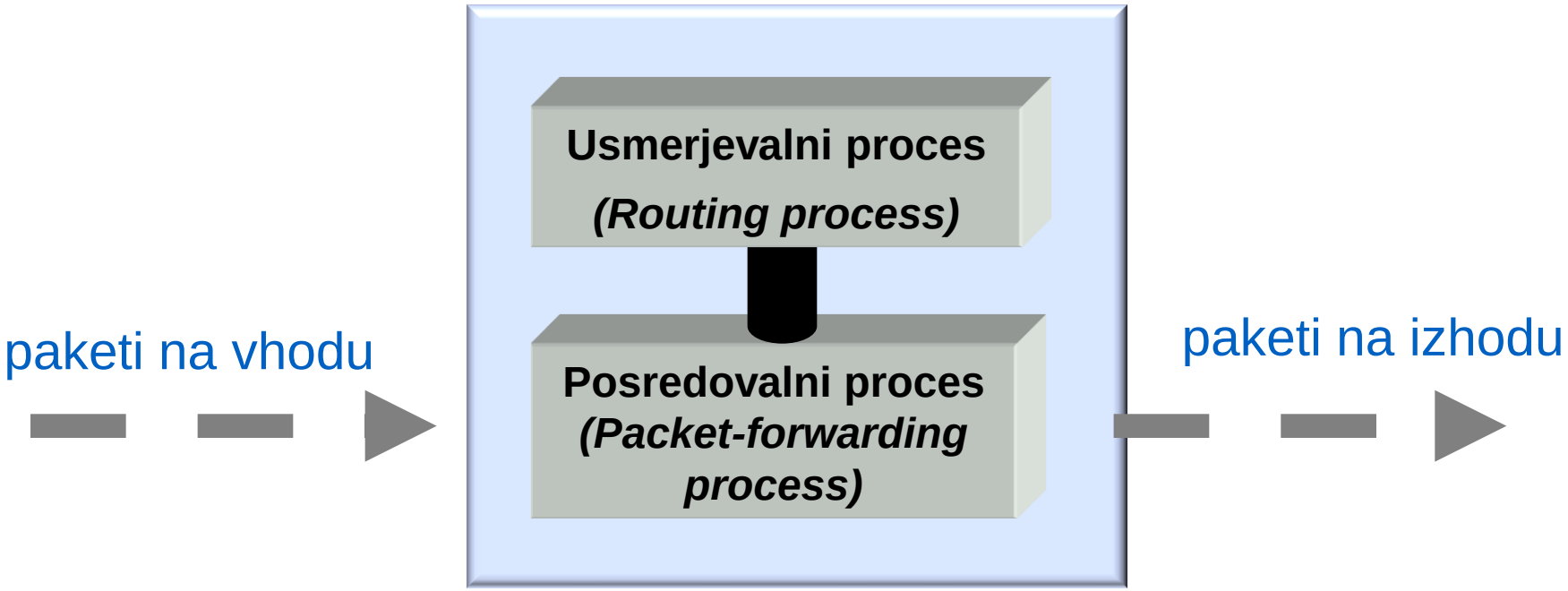
Naloge protokola IP

- 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

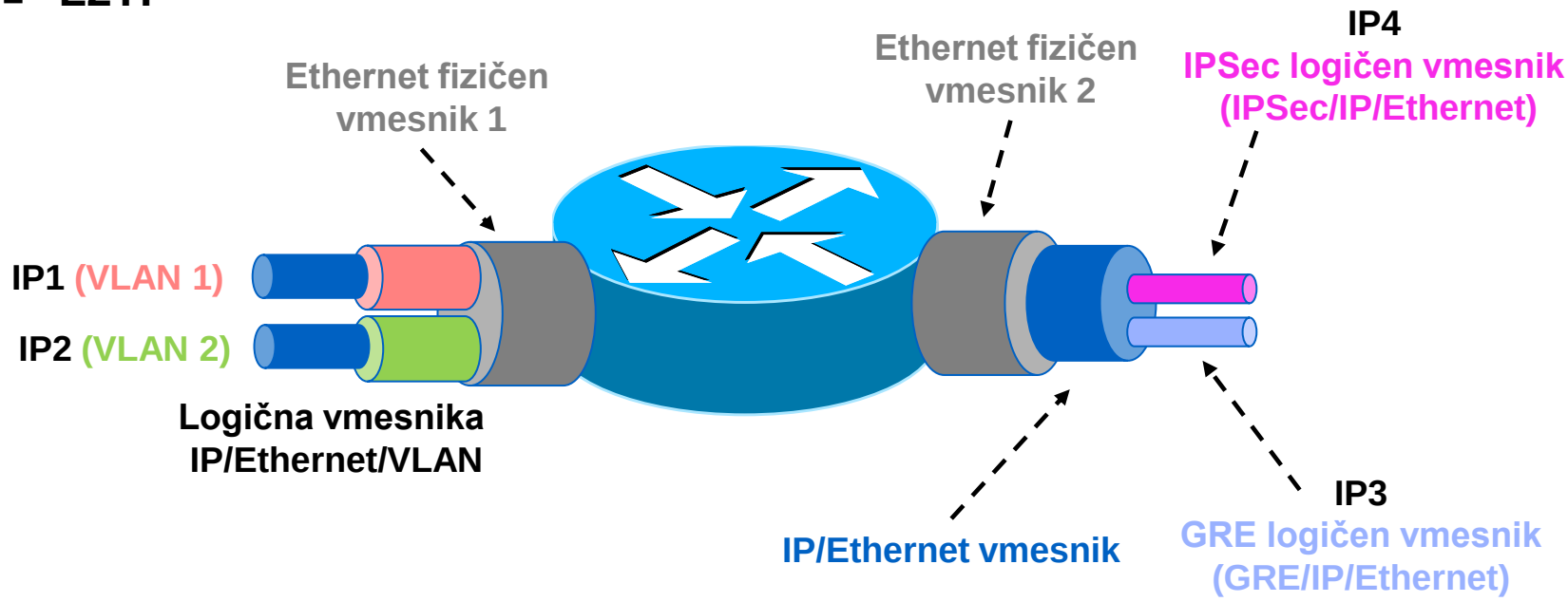


Usmerjanje in posredovanje

- **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

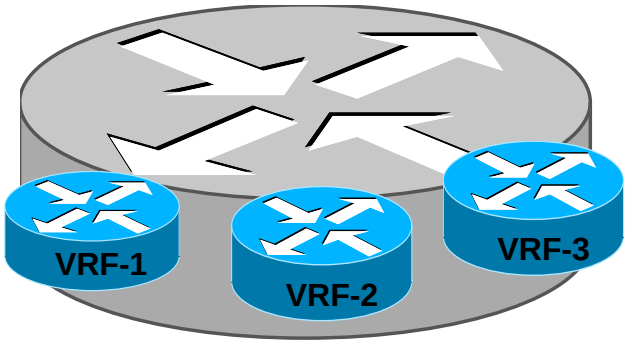
IP virtualizacijski mehanizmi 1/3

- **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



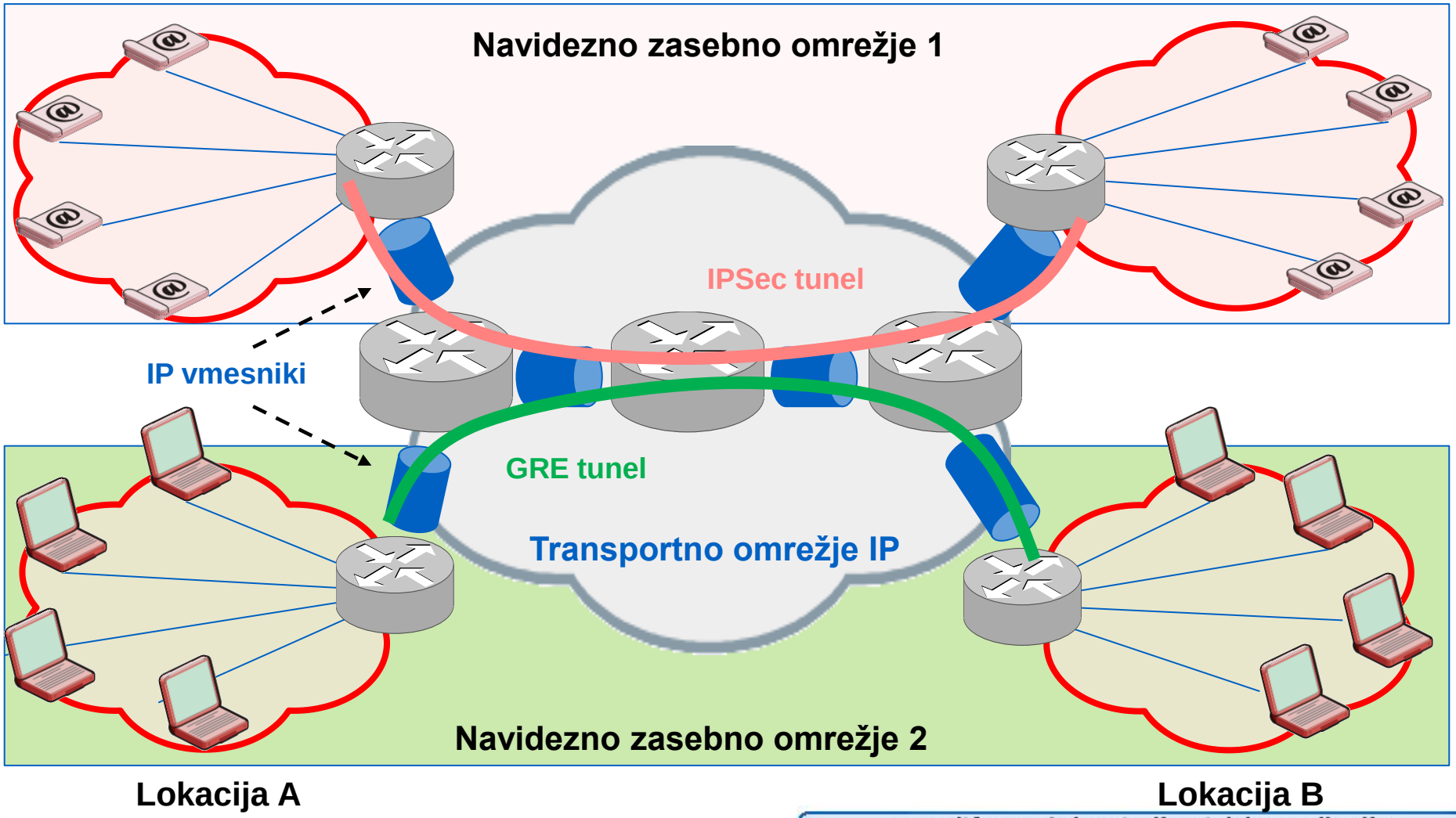
IP virtualizacijski mehanizmi 2/3

- **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

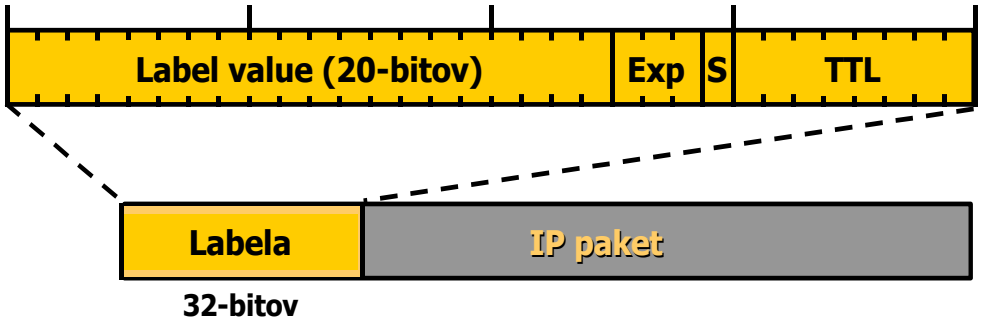
- Uvod
- **Transportne tehnologije**
  - Ethernet
  - IP
  - **MPLS**
- Navidezna zasebna omrežja
- IPSec VPN
- L3 MPLS VPN
- L2 MPLS VPN

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

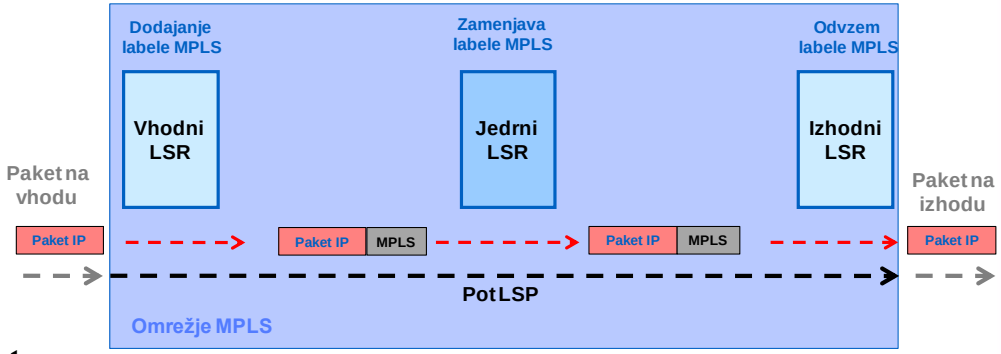
Osnovni koncepti – glava MPLS

- 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

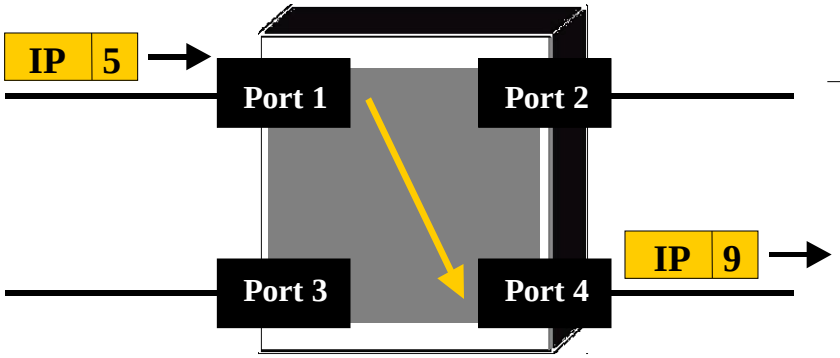


Osnovni koncepti – usmerjevalnik LSR

- **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



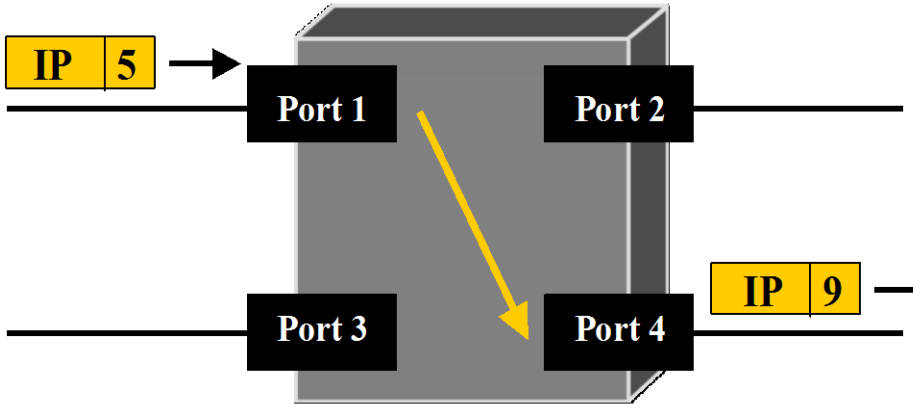
- **Zamenjava glave MPLS**
  - vhodni vmesnik in labela določata
    - operacijo: dodaj, zamenjaj, odstrani
    - izhodni vmesnik in izhodno labelo
  - podoben posredovalni mehanizem je bil uporabljen v ATM in FR



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



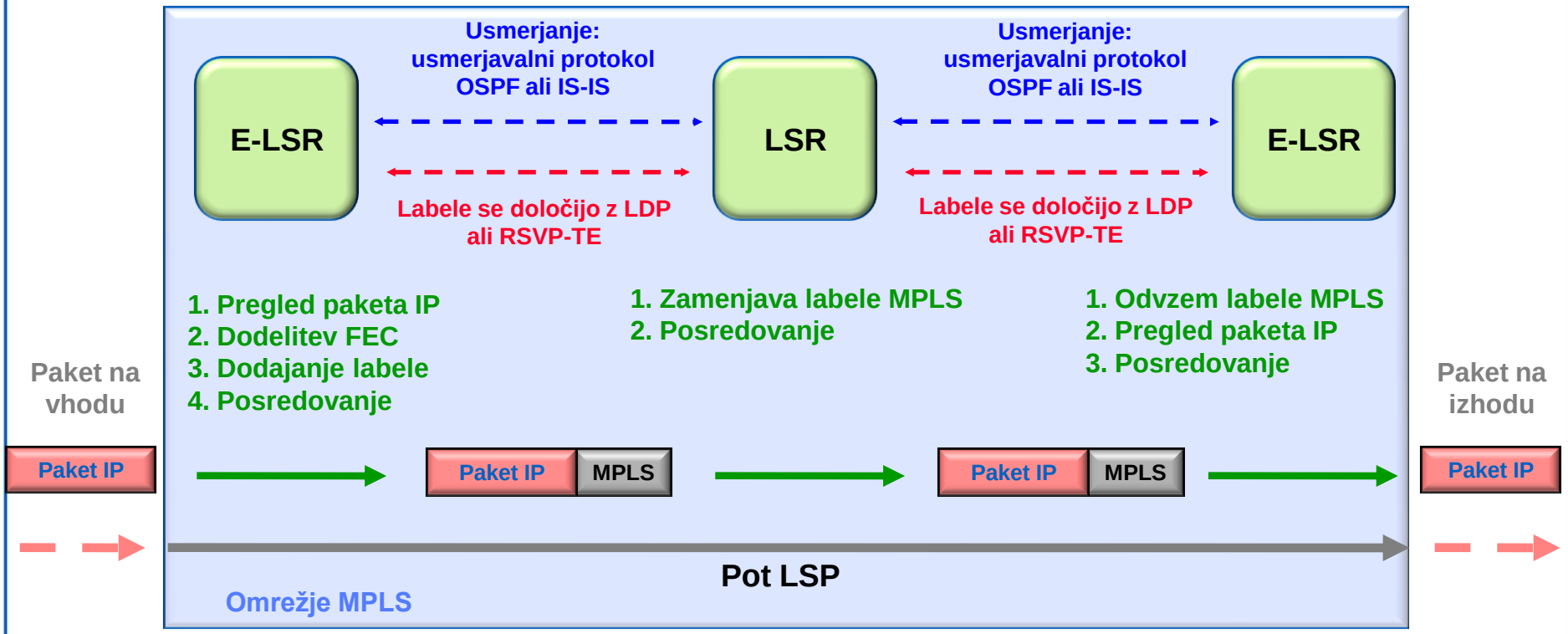
Vhod (port, labela)	Izhod (port, labela)	Labela Operacija
(1, 2)	(2, 7)	Zamenjava
(1, 4)	(3, 7)	Zamenjava
(1, 5)	(4, 9)	Zamenjava
(2, 3)	(3, 2)	Zamenjava

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

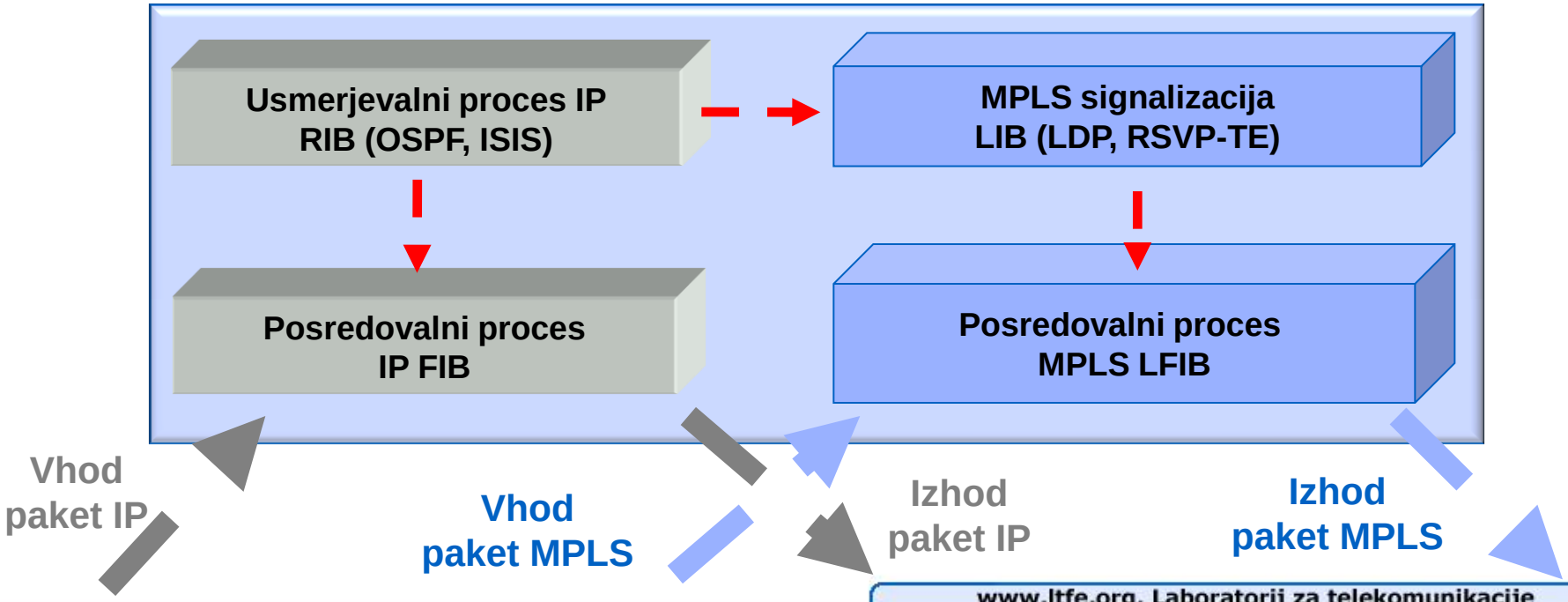
Delovanje MPLS

- **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



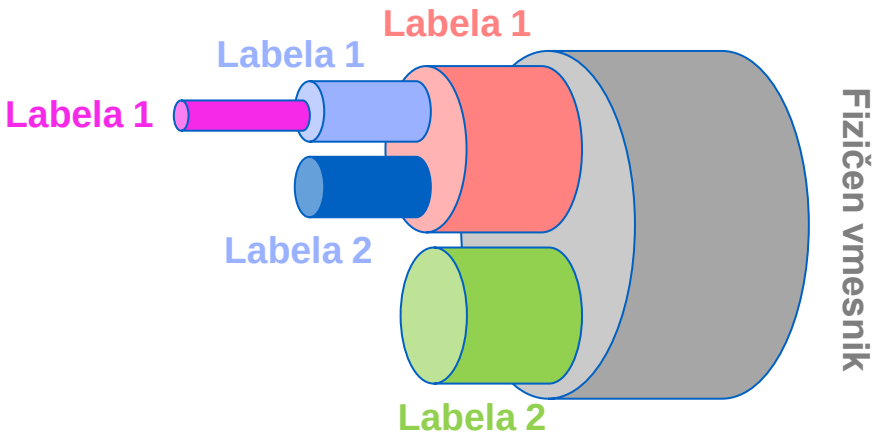
MPLS na usmerjevalniku IP

- 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

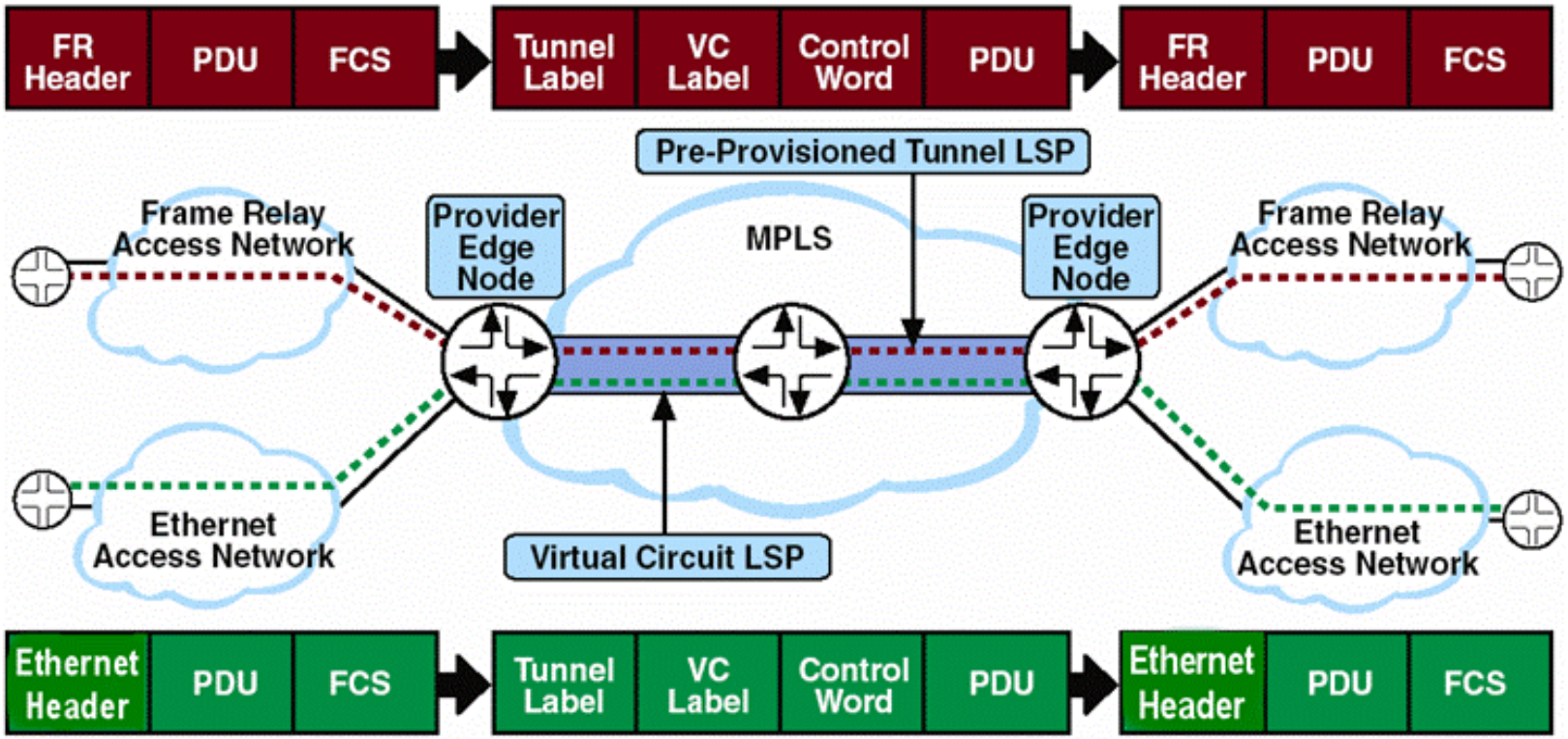
- Logični vmesniki na usmerjevalniku IP/MPLS
  - povezovanje z logičnimi vmesniki - labela MPLS
- Tunelski mehanizmi
  - MPLS LSP
- Virtualizacija usmerjevalnika
  - mehanizem VRF – VPN Routing and Forwarding



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

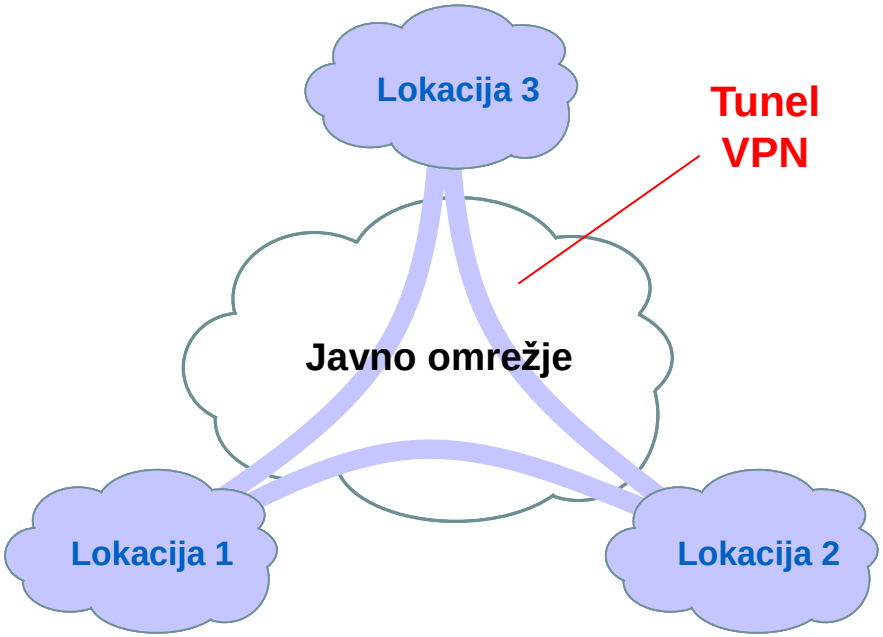
VPN – Virtual Private Network

- **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)**

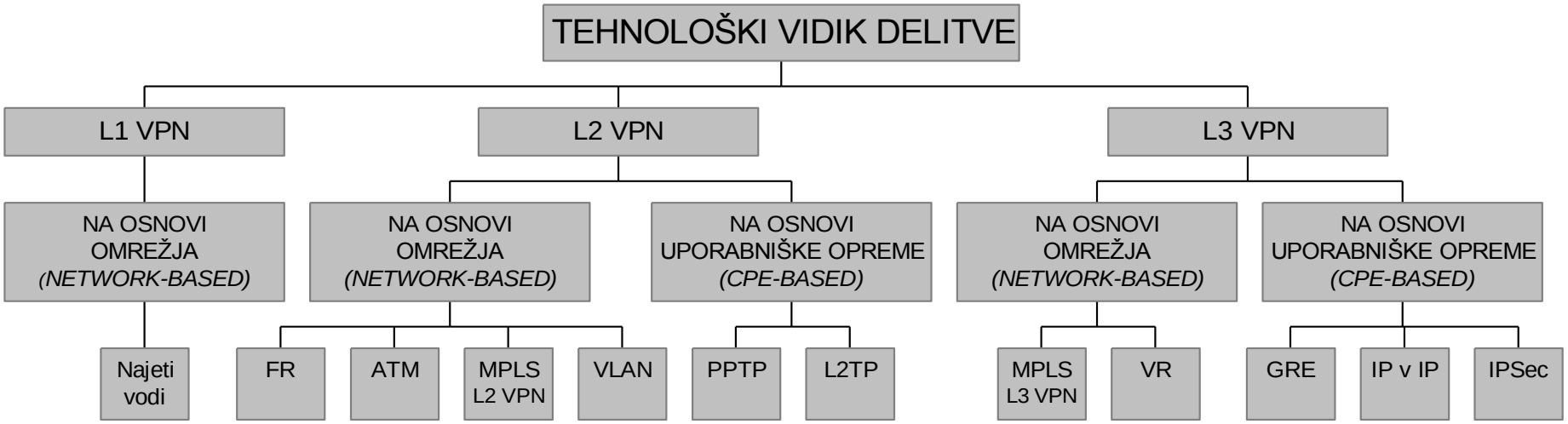
Osnovni koncepti VPN

- **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



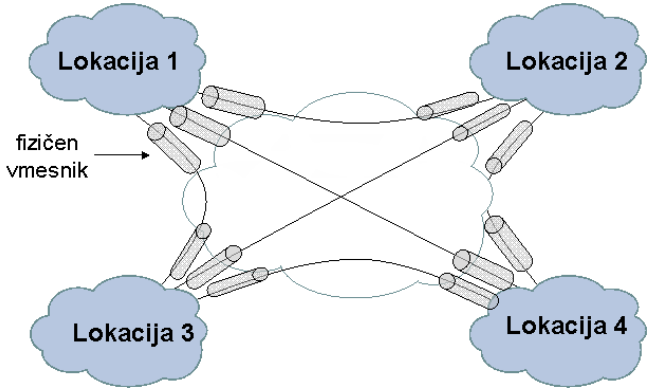
Delitev rešitev VPN

- **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**

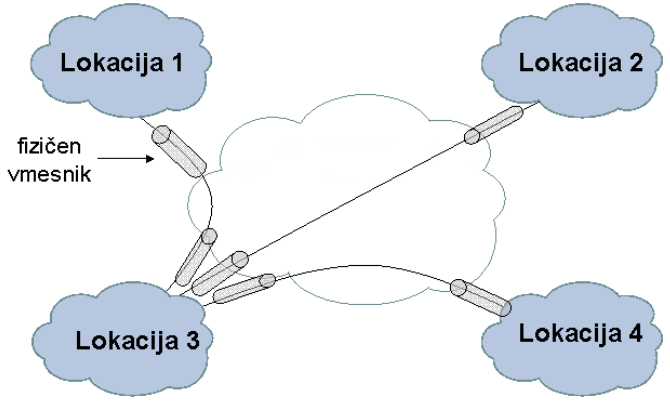


Tradicionalne rešitve VPN

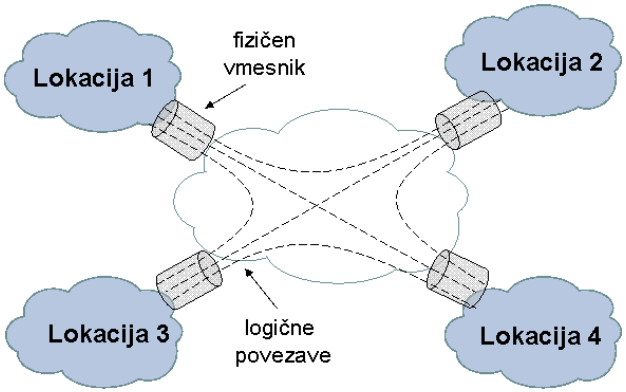
- **Najeti vodi (SDH, LL)**
  - **popolna mreža povezav**



  - **topologija zvezda**

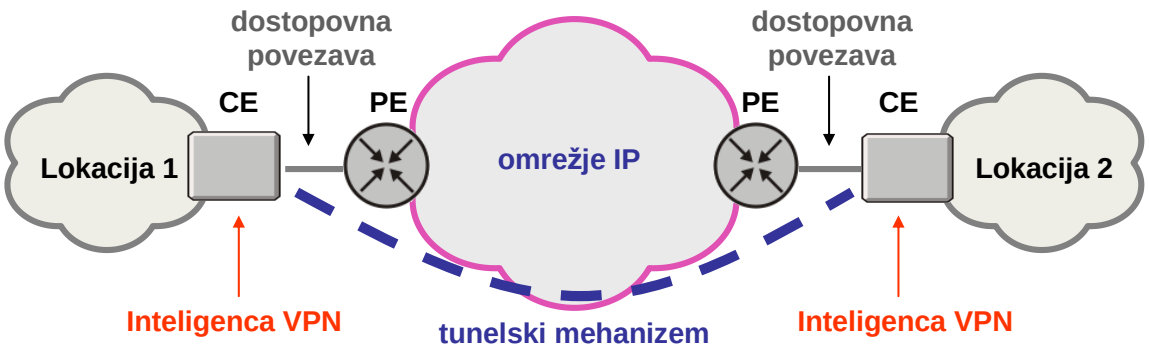


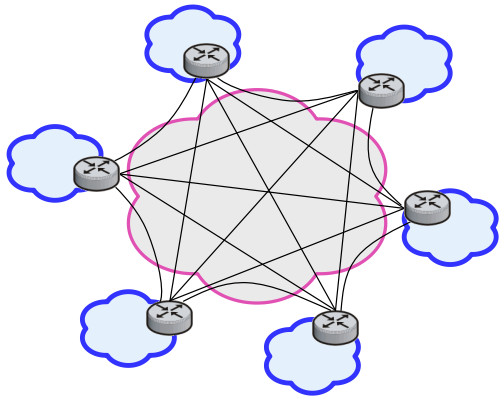
- **Povezave L2 (ATM, FR)**
  - **popolna mreža povezav**



Rešitve na osnovi uporabniške opreme

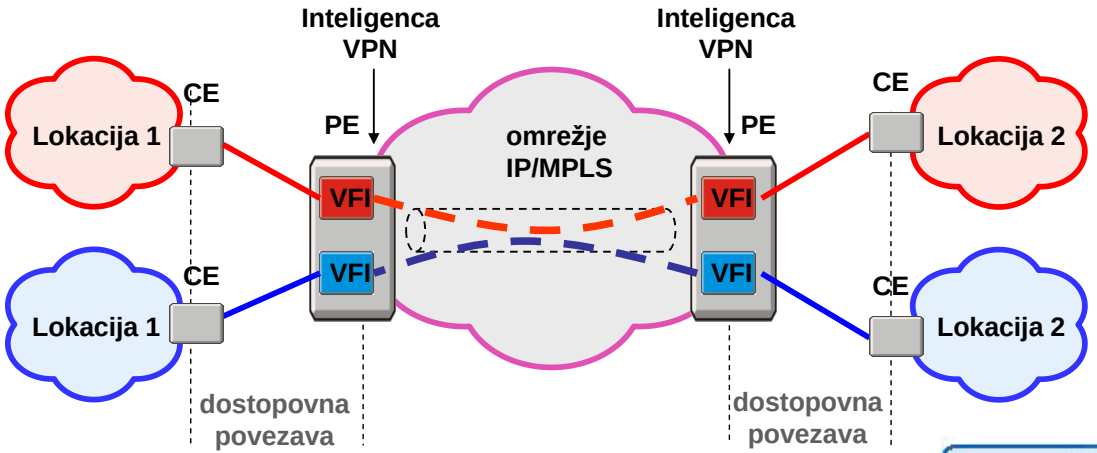
- CPE – Customer Premises Equpment
- Vse potrebne informacije o omrežju VPN so vsebovane v napravah CPE
- Uporabnik sam poskrbi za gradnjo tunelov prek javnega omrežja
  - za optimalno usmerjanje je potrebna popolna mreža povezav (N^2 problem)
- Funkcionalnosti VPN so vgrajene v omrežne naprave, kot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

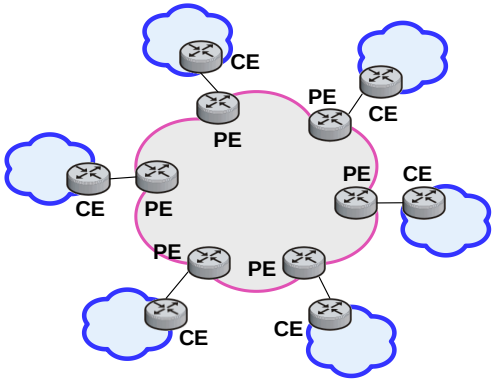




Omrežne rešitve (network-based)

- 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

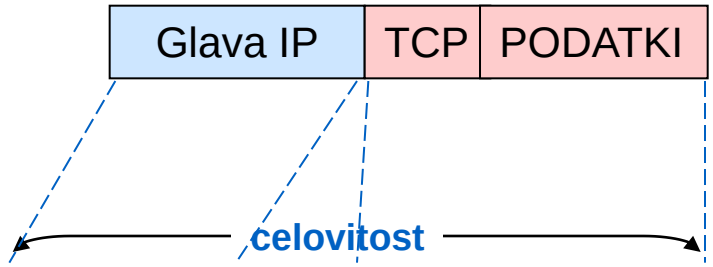
Varnostne storitve protokola IPSec

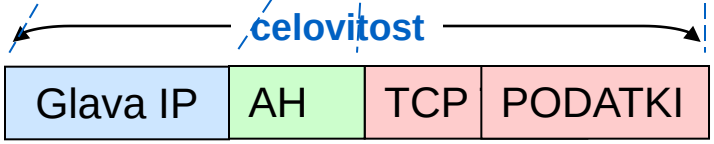
- Avtentikacija izvora podatkov
  - zajamči točnost izvora podatkov
- Zaupnost podatkov
  - preprečuje prebiranje in kopiranje podatkov, ko se prenašajo prek javnega omrežja
- Nepovezavna celovitost podatkov
  - zagotavlja, da podatki v času prenosa skozi omrežje niso bili spremenjeni
- Nadzor dostopa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

Prenosna načina IPSec

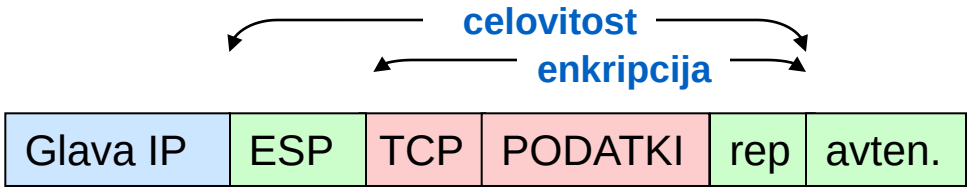
- **Transportni način**

  Originalni paket IP





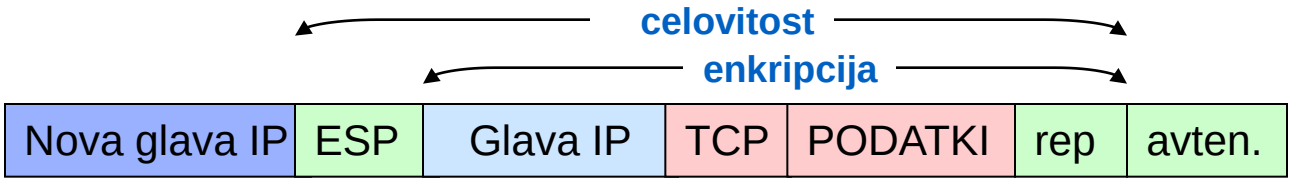
Protokol AH



Protokol ESP

- **Tunelski način**

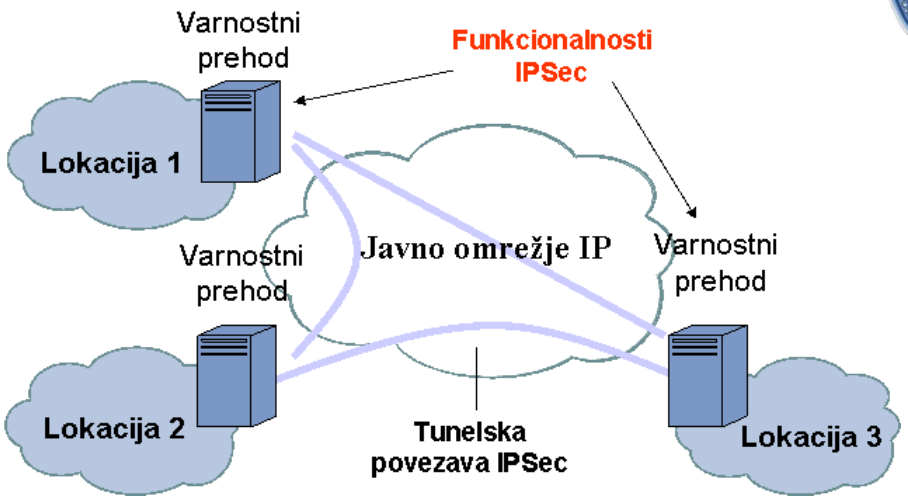
Protokol AH



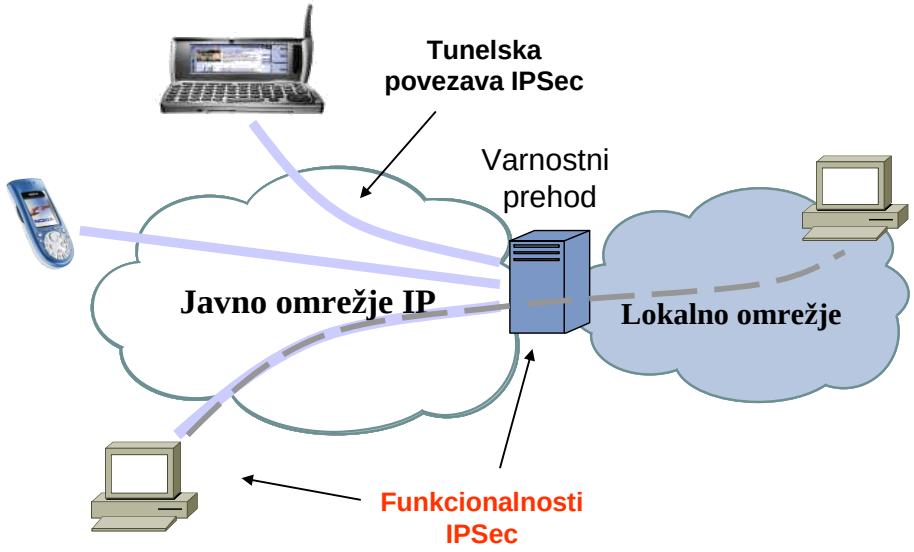
Protokol ESP

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

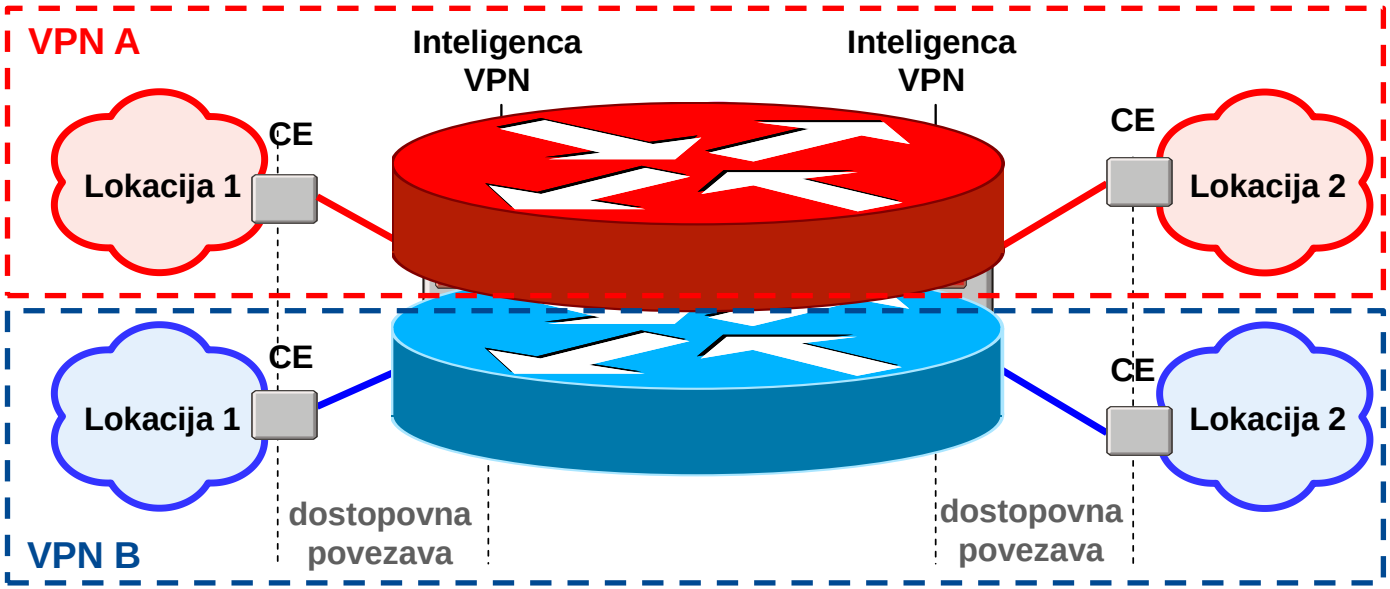
- Prednosti
  - celovit varnostni mehanizem
  - implementacija je možna prek katerega koli omrežja IP
    - mobilna omrežja
    - brezžična omrežja
    - fiksna omrežja
  - omogoča globalno pokrivanje
- Slabosti
  - problem vzdrževanja velikega števila tunelov
    - N^2 - problem

Vsebina

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

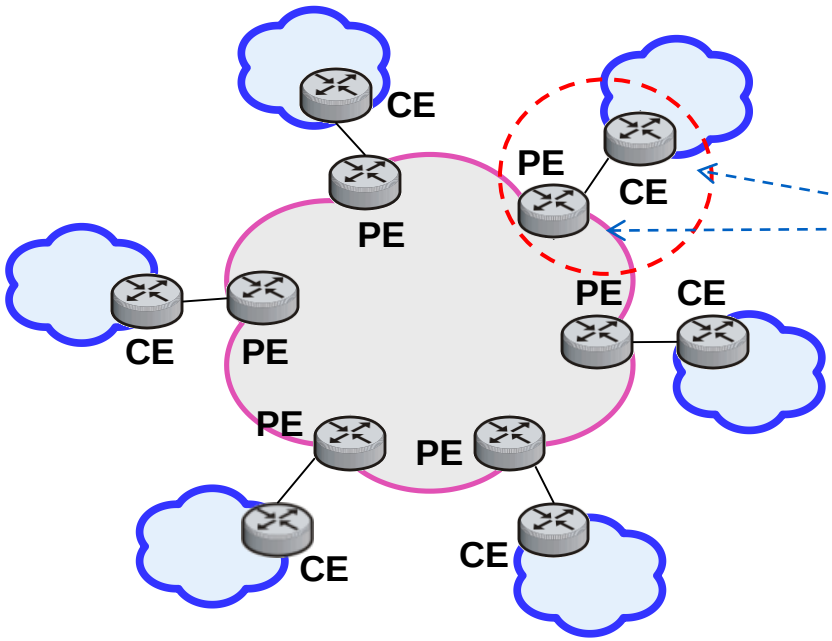
Povezavni model BGP/MPLS VPN

- 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

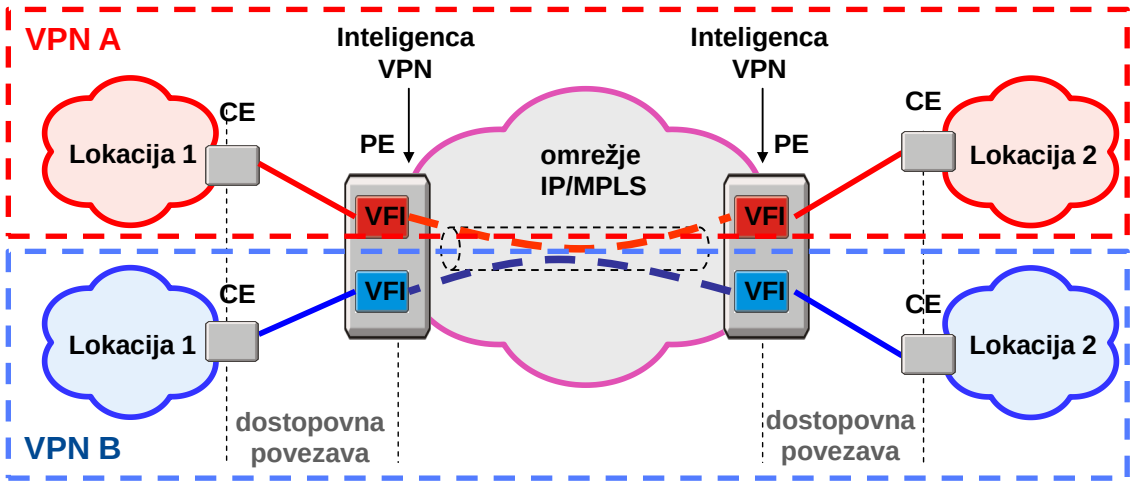
- **Za dodajanje nove lokacije v omrežje VPN je potrebno nastaviti samo robni napravi PE in CE**
  - **Za signalizacijo in distribucijo VPN informacij poskrbijo mehanizmi BGP/MPLS VPN – signalizacij s protokolom MP-BGP**



V primeru dodajanja nove lokacije je potrebna samo nastavitve (PE, CE)

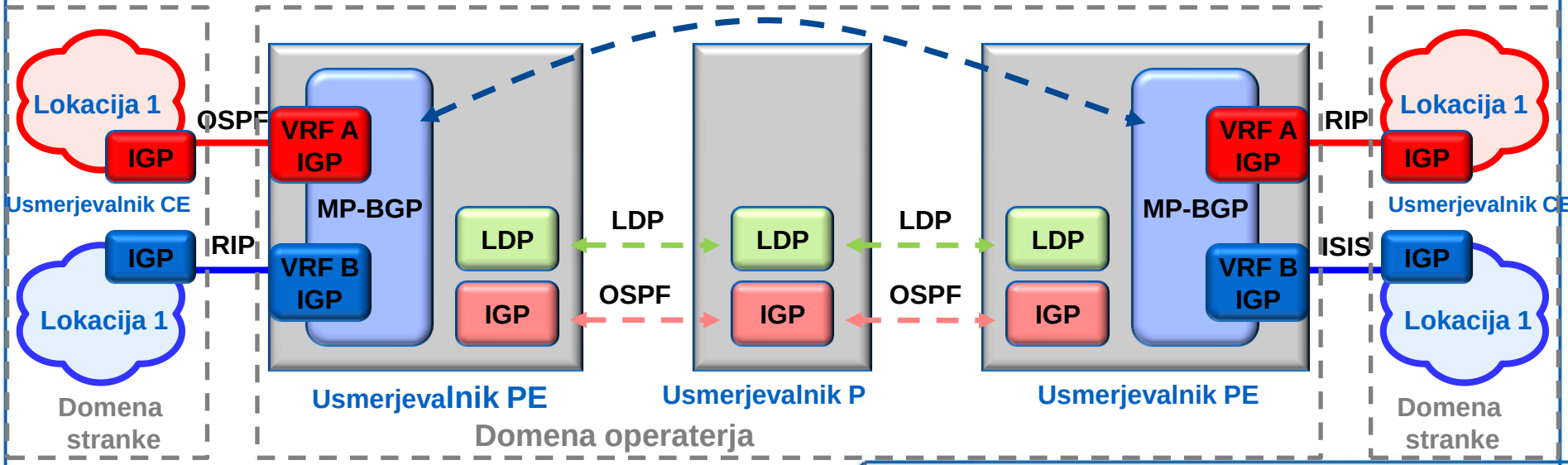
Arhitektura MPLS VPN

- 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



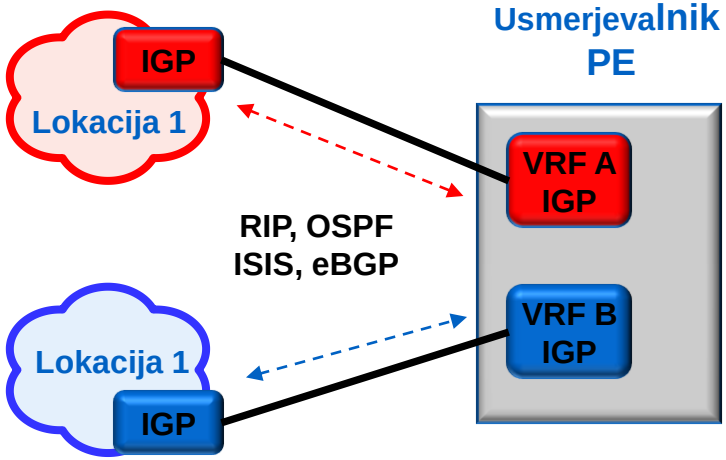
Komponente BGP/MPLS VPN 1/3

- **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)**



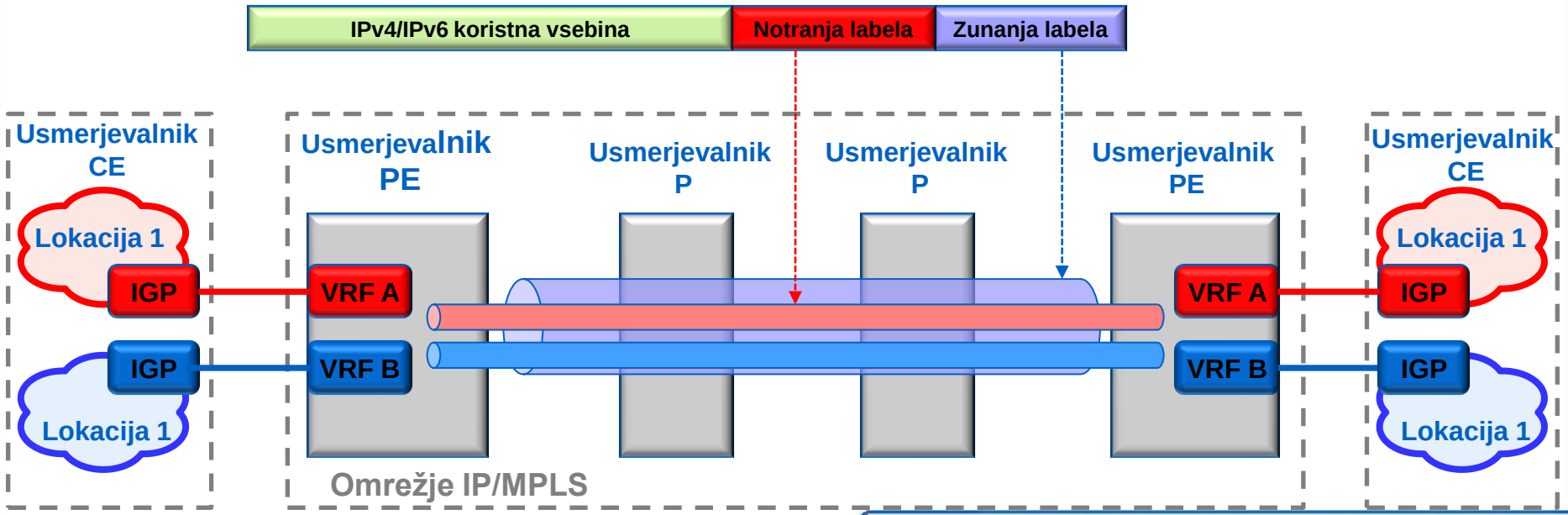
Komponente BGP/MPLS VPN 2/3

- 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**

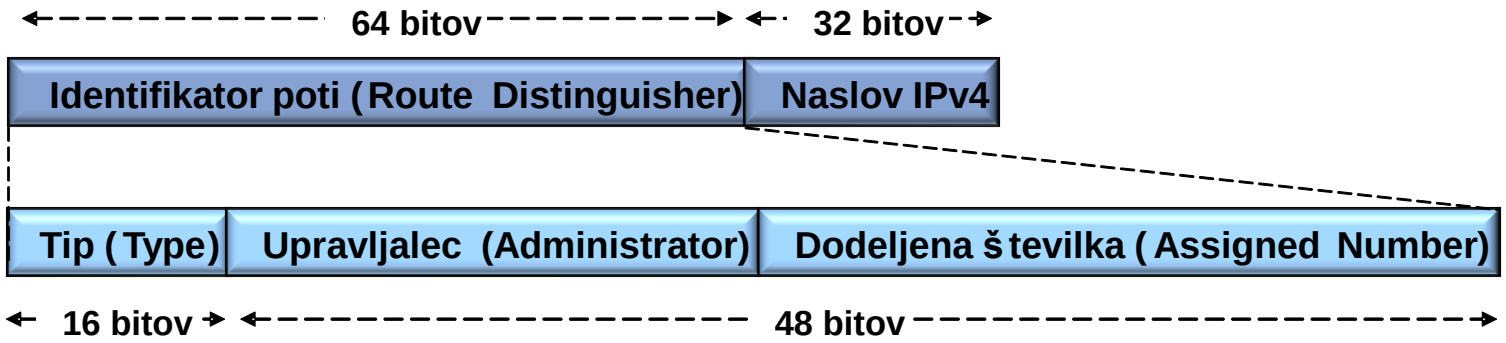


Protokol MP-BGP

- 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

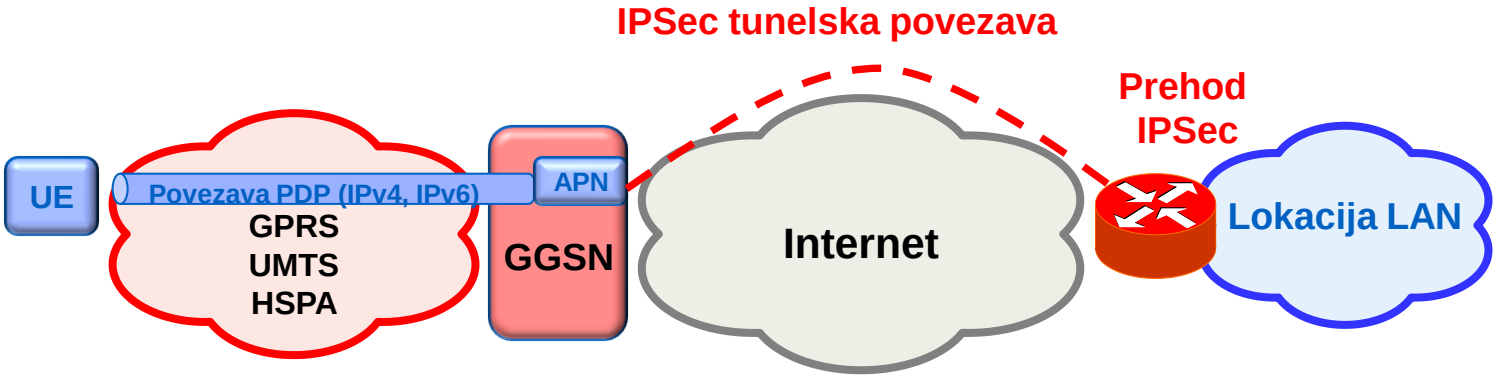
Naslovna shema VPN-IPv4

- **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)

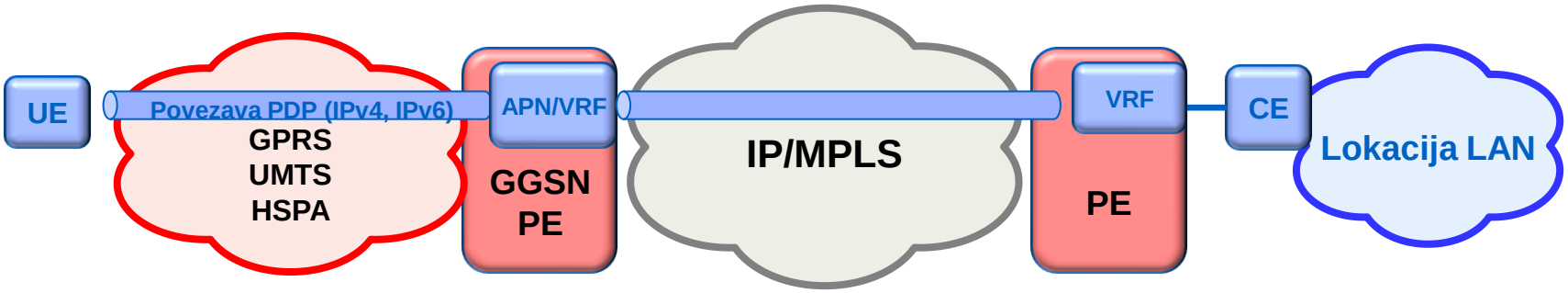


Primer uporabe MPLS in APN VPN

- **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

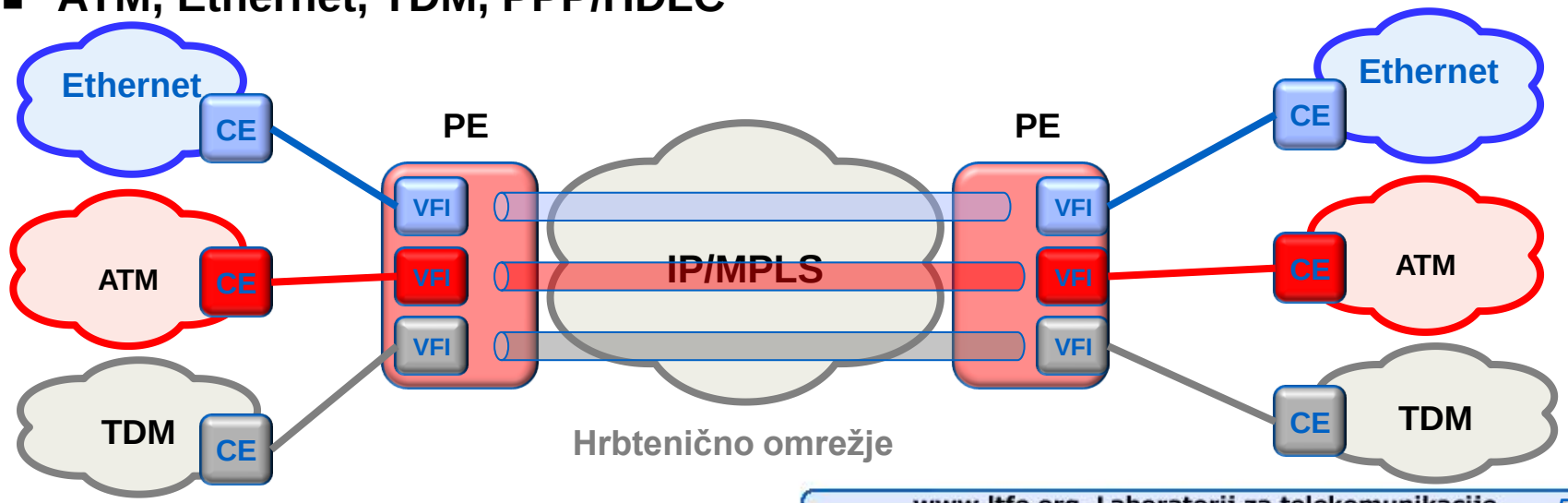
- V segmentu storitev IP VPN prevladujejo BGP/MPLS VPN rešitve
  - največkrat uporabljani topologiji sta “full mesh” in “hub and spoke”
- Uporabnik mora popolnoma zaupati ponudniku storitev
  - ponudnik storitev poskrbi za načrtovanje omrežja, usmerjanje, vzdrževanje in upravljanje
  - ponudnik mora 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

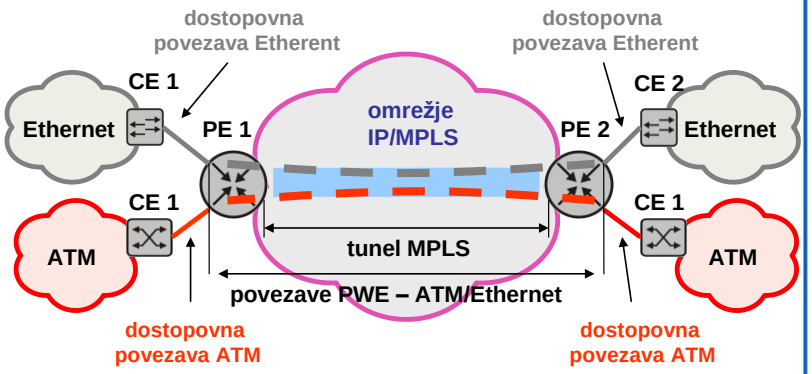
L2 MPLS VPN

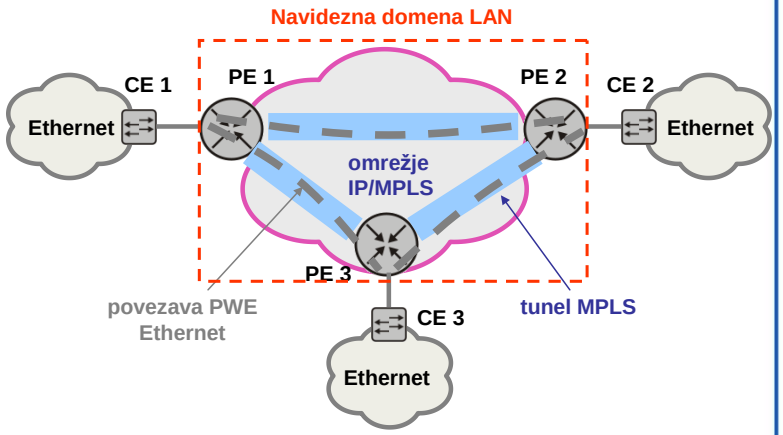
- Motivacija
  - ena transportna infrastruktura (MPLS) za vse vrste prometa
- Možnost prenosa “katerega koli” tipa prometa
  - ATM celice, ATM AAL5, FR, Ethernet, Ethernet VLAN, PPP/HDLC, Sonet/SDH, TDM
  - velika teorija poenotenja (še ena)
- Ponudnik storitev ne sodeluje pri usmerjanju prometa
  - 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

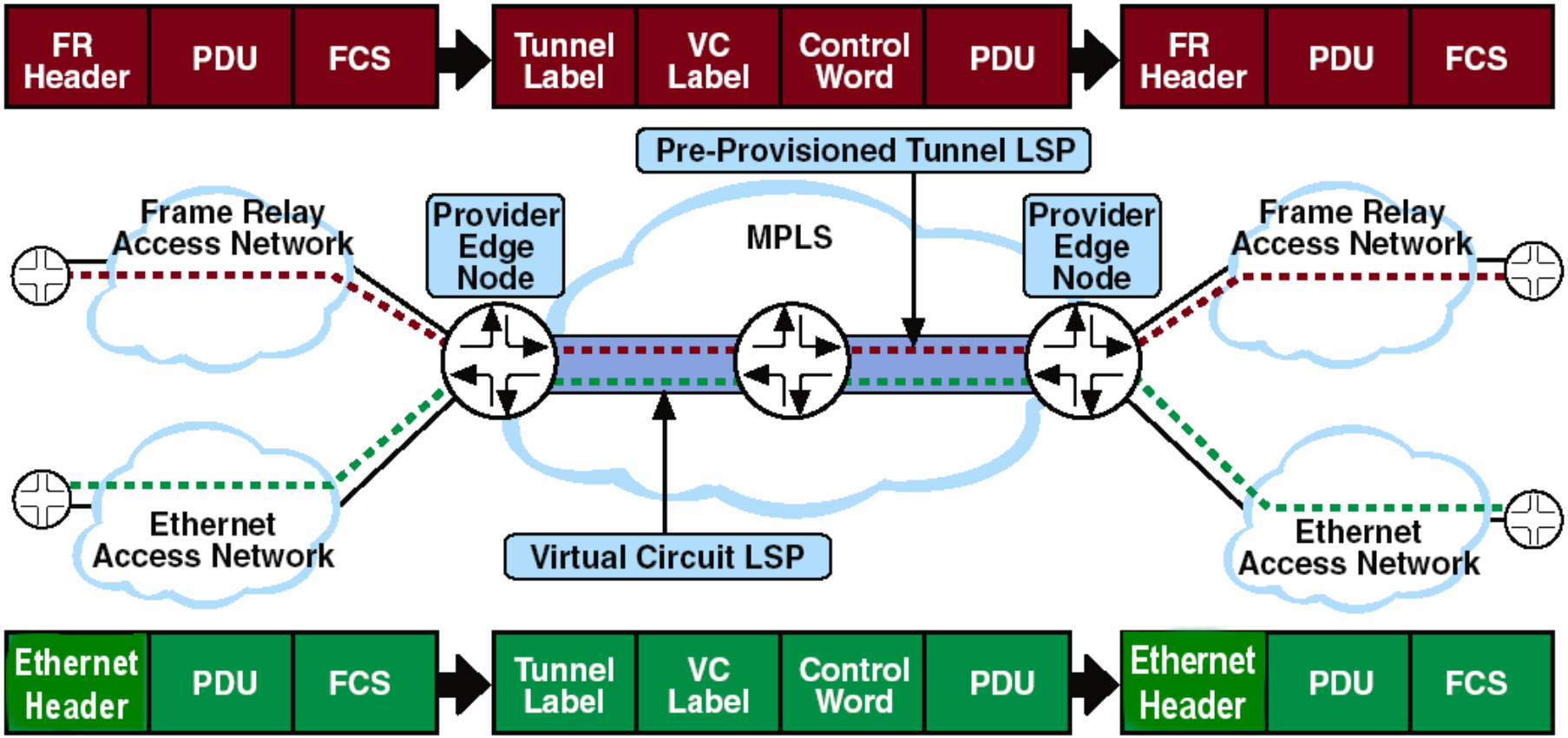
VPWS

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

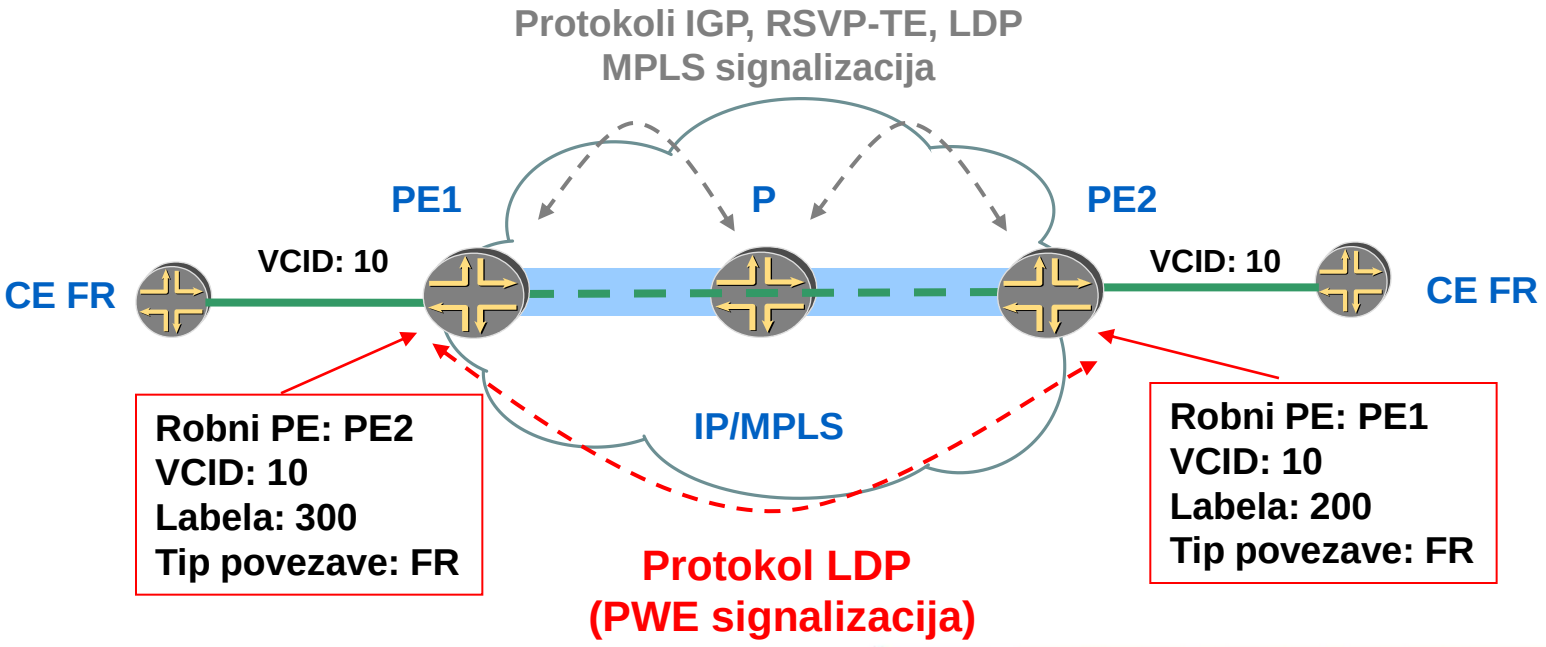
Povezavni model VPWS

- Primer inkapsulacije FR in Ethernet prek IP/MPLS



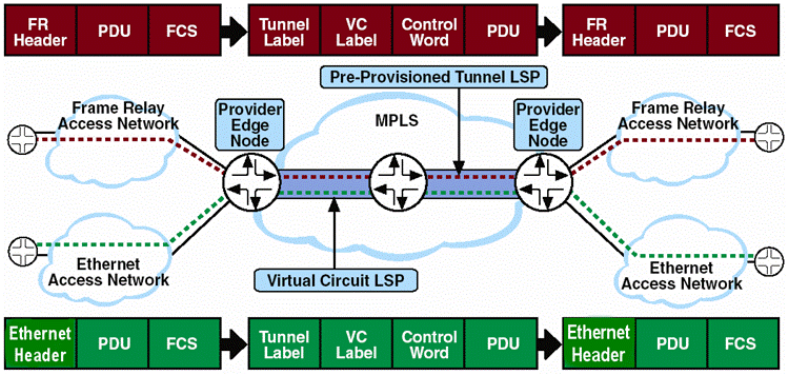
Signalizacija VPWS

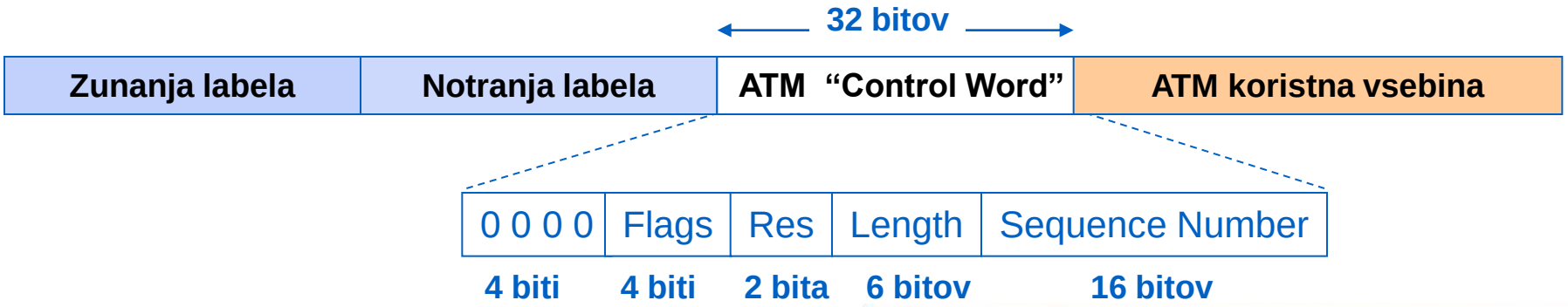
- V hrbteničnem omrežju MPLS (IP/MPLS signalizacija)
  - protokoli RIP, OSPF, IS-IS, BGP (IGP)
  - protokoli LDP, RSVP-TE (distribucija label)
- Med robnimi napravami PE (PWE signalizacija)
  - protokol MP-BGP
  - protokol LDP
- Primer: LDP



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

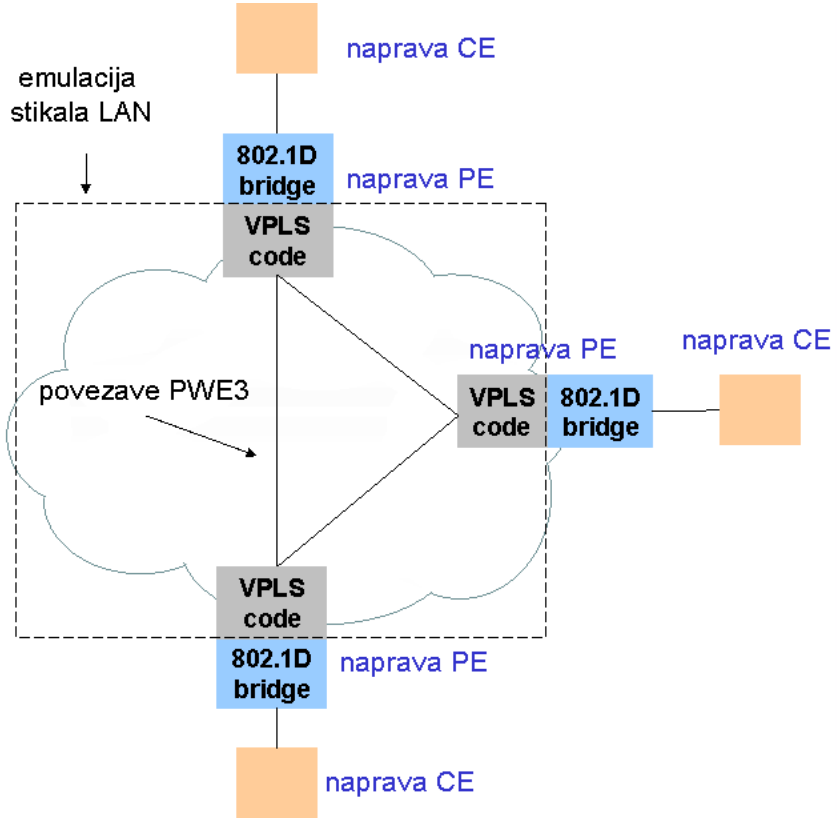
- Prenos ATM celic – "ATM cell mode"
  - "1:1 celični način":
    - vsak VPC (Virtual Path Connection) oziroma VCC (Virtual Channel Connection) se prenaša v svoji povezavi PWE
    - boljši izkoristek pasovne širine
    - ni potrebno prenašati VPI/VCI v primeru VCC ter VCI v primeru VPC
  - "N:1 celični 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

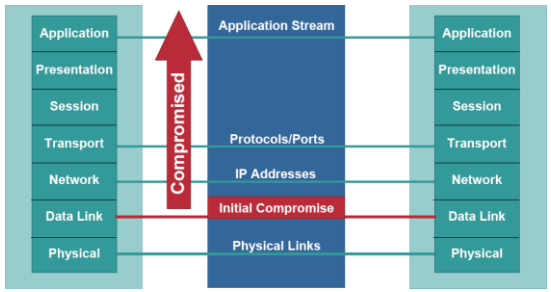
- **Signalizacija zagotavlja dve ločeni funkciji**
  - iskanje naprav PE, ki sodelujejo v izbranem VPLS
  - izmenjava parametrov za vzpostavitev povezav PWE
- **Draft Kompella**
  - draft-ietf-l2vpn-vpls-bgp-03.txt
  - signalizacija temelji na protokolu MP-BGP
    - koncept BGP/MPLS VPN
    - omogoča “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

Varnostne naprave

Ljubljana, maj 2011

Umestitev varnostnih naprav

- Glede na sloje na katerem naprava oz mehanizem deluje
  - Ethernet stikalo, usmerjevalnik IP, požarna pregrada, sistem za preprečevanje vdorov (IPS), aplikacijski prehod
- Glede na varnostne funkcije in vrsto zaščite
  - Statični in dinamični filtri, proxy in snooping funkcije, poglobljen pregled vsebine
  - Zaščita kontrolne ravnine – npr. filtriranje sporočil IGMP
  - Zaščita podatkovne ravnine – npr. dovoljen dostopa do strežnika samo na TCP port 80
- Komunikacijski model OSI
  - posamezen sloj se ne zaveda "ogroženosti" drugega
  - varnost sistema je enaka varnosti najšibkejšega člena



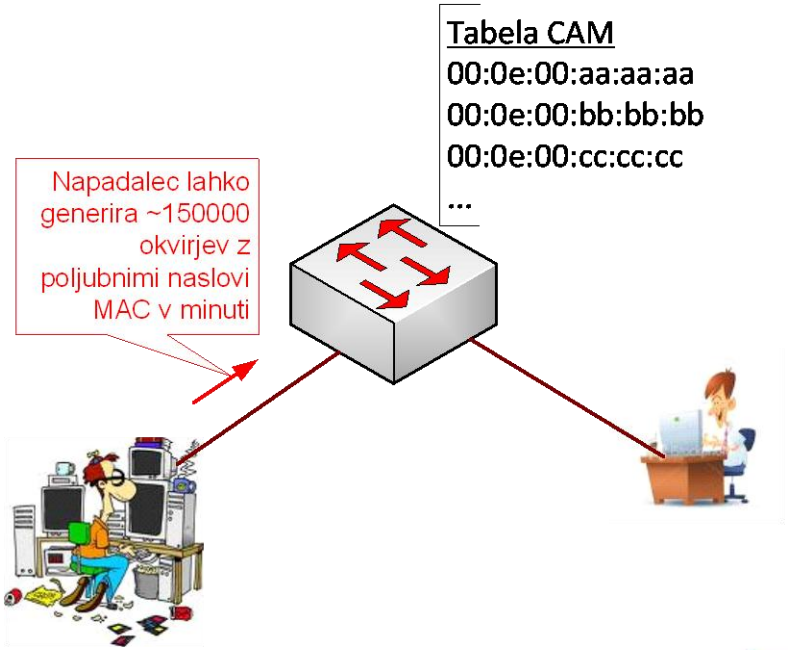
Ethernet varnostni mehanizmi

Napadi na Ethernet mehanizme

- Tipični napadi
  - poplavljanje tabele MAC
  - VLAN hopping
  - zastrupljanje tabel ARP
  - napadi na DHCP

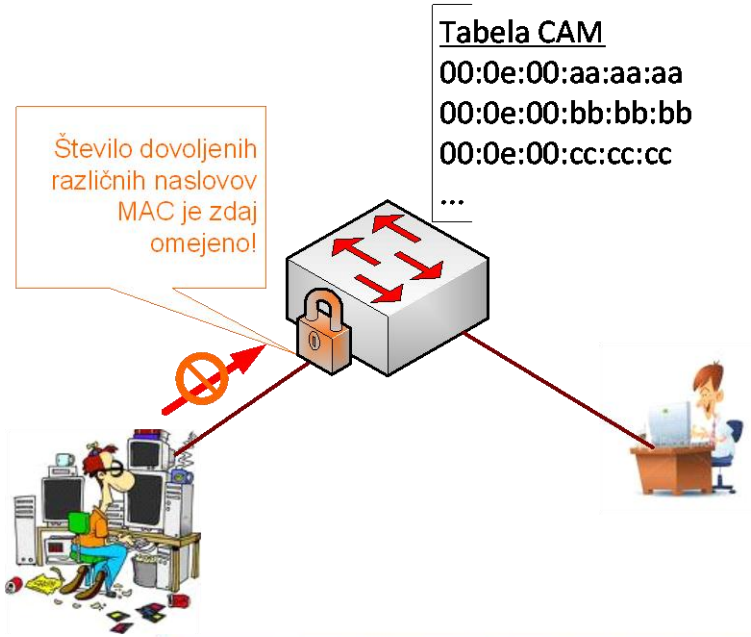
Manipulacije z naslovi MAC 1/2

- **Preplavljanje tabele MAC (angl. MAC Overflow)**
  - **napad izkorišča**
    - **način vpisovanja naslovov MAC v MAC-tabelo**
    - **končno velikost tabele MAC**
  - **stikalo posreduje ves promet, ki je namenjen na neznani naslov MAC (neznani izhoden vmesnik) na vse aktivne izhodne vmesnike**
  - **stikalo preide v HUB način delovanja**



Manipulacije z naslovi MAC 2/2

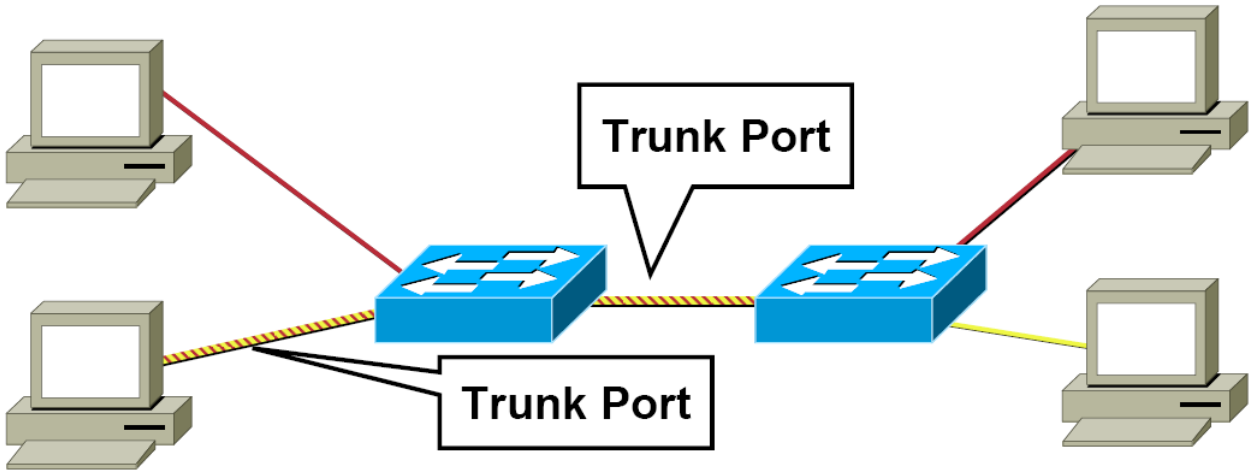
- Zaščitni mehanizem
  - PORT SECURITY
    - omejuje število MAC-naslovov, ki jih lahko stikalo registrira na posameznem vmesniku
    - določa obnašanje vmesnika v primeru poskusa preseganja limite
      - dekativacija vmesnika
  - Filtriranje naslovov MAC
    - kreirajo se pravila za filtriranje Ethernet okvirjev glede na naslove MAC-vira in/ali ponora



VLAN hopping

- Iskorišča lastnosti povezav tipa trunk
- Switch spoofing
  - napadalec predstavi svojo povezavo kot povezavo tipa trunk
  - s tem postane član vseh omrežij VLAN

- Zaščitni mehanizem
  - Pravilna implementacija in nastavitev stikala

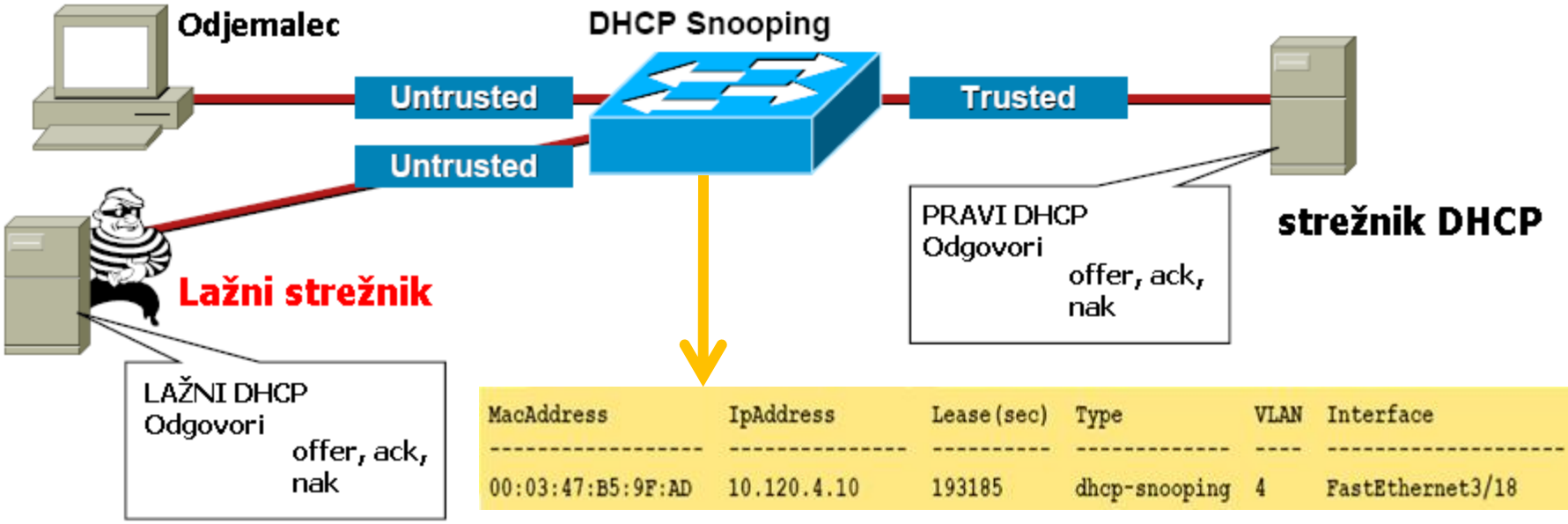


Napadi na DHCP

- "DHCP Starvation"
  - napadalec pošilja veliko število DHCP-zahtev z različnimi izvornimi naslovi MAC
  - strežnik DHCP izčrpa nabor naslovov, ki jih ima na voljo za dodeljevanje uporabnikom
    - napad tipa DoS – onemogočanje storitve DHCP
  - Zaščitni mehanizem
    - omejevanje števila različnih MAC-naslovov na posameznem vmesniku stikala Ethernet
- Kraja identitete strežnika DHCP "Rogue attack"
  - napadalec se predstavlja kot strežnik DHCP
  - dodeljuje nelegitimne nastavitvene parametre
  - lahko preusmeri promet na svojo napravo
  - Zaščitni mehanizem
    - DHCP snooping

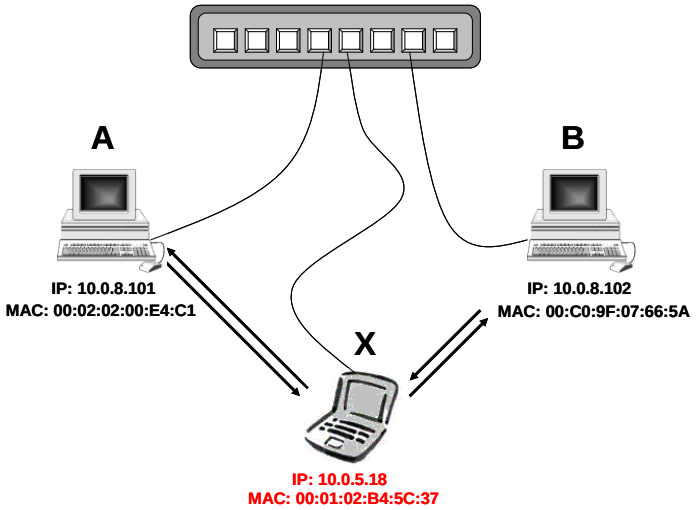
DHCP snooping

- Mehanizem implementiran na stikalu Ethernet
  - stikalo pregleduje vsebino sporočil DHCP
- Stikalo gradi dinamično tabelo o dodeljenih naslovih IP
  - Tabela gradi kombinacije vnosov MAC – IP, veljavnost dodeljenega naslova in druge parametre



Zastrupljanje tabele ARP 1/2

- **Zastrupljanje tabele ARP**
  - ustvarijo se napačne relacije med naslovi IP in MAC



Gostitelj	Naslov IP	Naslov MAC
A	10.0.8.101	00:02:02:00:E4:C1
B	10.0.8.102	00:C0:9F:07:66:5A
X	10.0.5.18	00:01:02:B4:5C:37

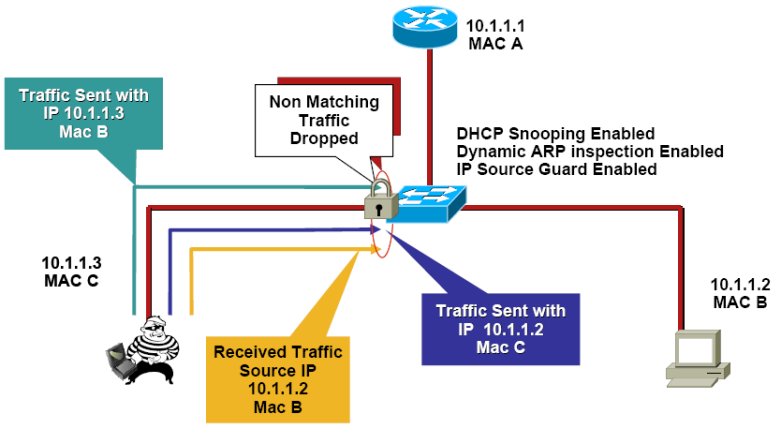
- **PC X izvaja napad zastrupljanja tabel ARP**
  - PC X posreduje nelegitimen odgovor ARP gostitelju PC A, v kateremu sporoča
    - "Jaz sem 10.0.8.102 (PC B), moj naslov MAC je 00:01:02:B4:5C:37"
  - PC X posreduje nelegitimen odgovor ARP gostitelju PC B, v kateremu sporoča
    - "Jaz sem 10.0.8.101 (PC A), moj naslov MAC pa se glasi 00:01:02:B4:5C:37"
  - Napadalec lahko pregleduje sporočila, ki si jih posredujeta gostitelja PC A in PC B

Zastrupljanje tabele ARP 2/2

- Zaščitni mehanizem “Dynamic ARP Inspection”
  - pregledovanje posredovanih sporočil ARP
  - izkorišča podatkovno bazo, ki jo gradi mehanizem “DHCP snooping”
  - dovoljuje ARP-sporočila z IP-MAC preslikavo, ki se ujema z vpisi v tabeli “DHCP snooping”

Spoofing

- Pošiljanje paketov z nelegitimnim izvornim naslovom
  - nelegitimen MAC
    - napadalec pošilja okvirje z nelegitimnim MAC-naslovom
  - nelegitimen IP
    - napadalec pošilja okvirje z nelegitimnim IP-naslovom
- Zaščitni mehanizem
  - IP Source Guard
    - pregleduje tabelo DHCP snooping za vsak paket, ki prehaja prek Ethernet stikala
    - pogleda že prisotne naslove: IP, MAC ali IP in MAC



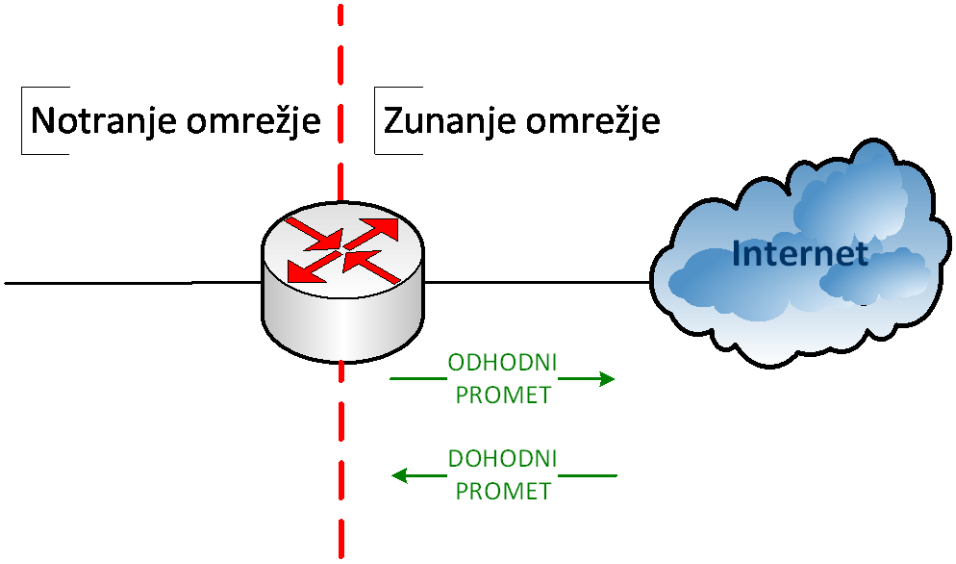
Varnostni mehanizmi IP

Varnostni mehanizmi IP

- **Dodatne varnostne funkcionalnosti omogočajo omrežnim napravam vpeljavo širokega nabora varnostnih storitev**
  - skrivanje naslovne sheme in topologije omrežja
    - mehanizem NAT in PAT na usmerjevalniku/požarni pregradi
  - nadzor dostopa do omrežja, naprav in omrežnih storitev na osnovi filtriranja prometa
    - Statični filtri na usmerjevalniku – filtri na naslove IP in port TCP/UDP
    - Dinamični filtri na požarni pregradi – filtri na naslove IP in port TCP/UDP
  - poglobljen pregled vsebine paketov, do aplikacijskega nivoja
    - Preverjanje ali je promet na vratih številka 80 (TCP) res HTTP
    - Sistemi IDS/IPS
  - emulacija odjemalcev
    - Aplikacijski prehodi, proxy naprave

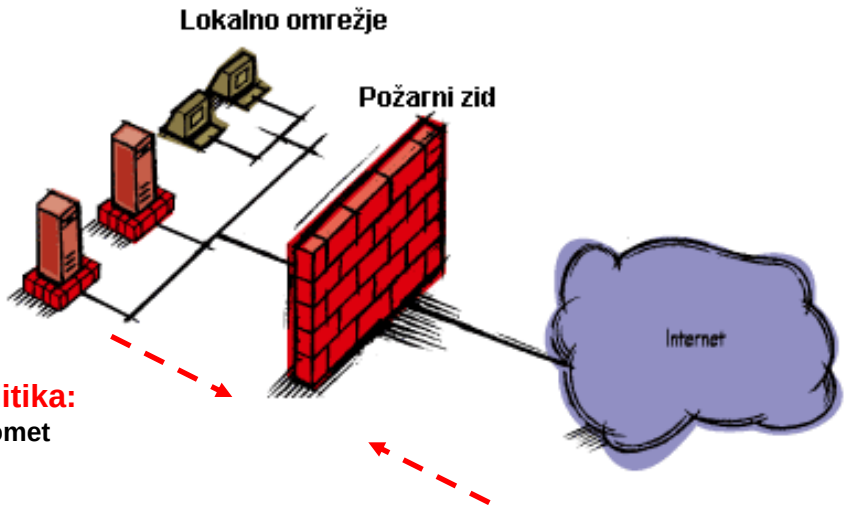
Filtri za nadzor dostopa

- Predstavljajo osnoven nivo kontrole prometnih tokov
- Na podlagi kriterijev (naslov IP, port TCP/UDP) določajo ali podatkovne enote (paket IP) posredovati naprej ali jih blokirati
  - odločitveni kriterij
    - izvorni/ponorni naslov IP, izvorna/ponorna številka vrata TCP/UDP in druge posebnosti protokolov
  - onovna naloga vključenega filtra
    - paket posreduj naprej
    - blokiraj paket



Požarni zid

- Loči lokalno omrežje od zunanjega omrežja
  - Zagotovi večji nivo varnosti uporabnikom v lokalnem omrežju
  - Namenska naprava oziroma funkcionalnost
  - Implementira se bolj "inteligentna" kontrola prometa



Odhodna politika:
- Dovoli ves promet

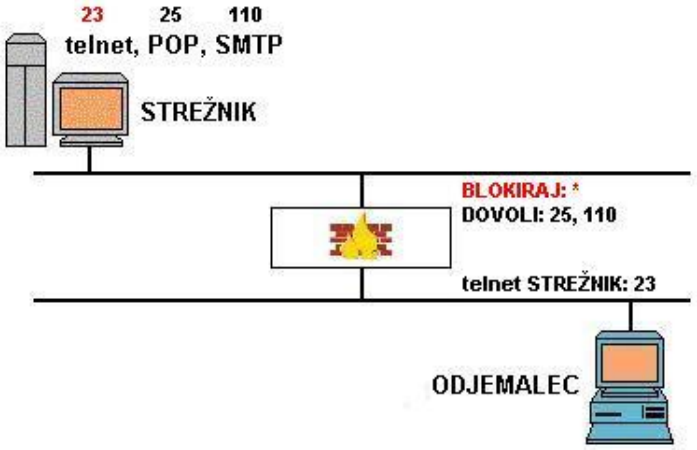
Dohodna politika:
- Dovoli ves promet, ki je bil vzpostavljen iz lokalnega omrežja
- blokiraj vse ostalo

Požarni zid

- Požarni zid je dober toliko, kot njegova varnostna politika
- Osnovne naloge:
  - dovoli
  - blokiraj
- Oblike implementacije:
  - namenska omrežna naprava
  - programski modul na gostitelju, ki komunicira z obstoječim skladom TCP/IP
- Delitev požarnih zidov:
  - paketno sito (Packet Filter)
  - sistem popolnega nadzora (Stateful Inspection System)
  - aplikacijski prehod

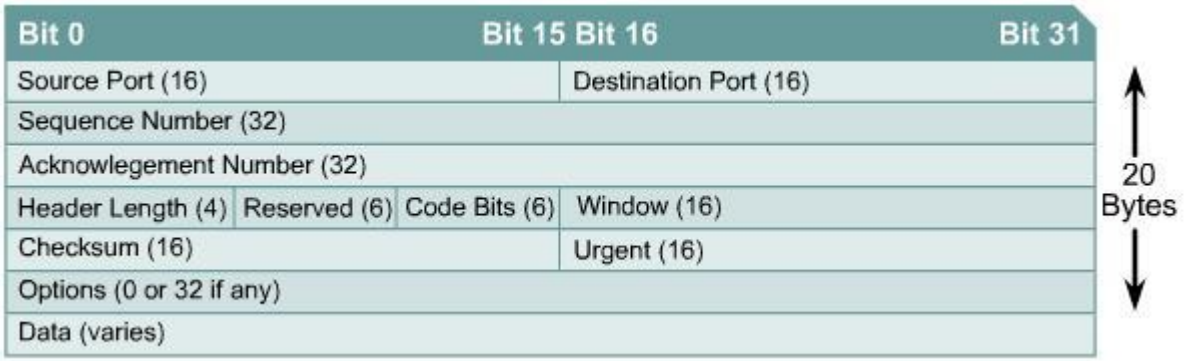
Požarni zid

- **Način kreiranja varnostne politike:**
  - vse, kar ni eksplicitno prepovedano, je dovoljeno
    - primer varnostne politike iz domačega omrežja v internet
  - vse, kar ni ekplicitno dovoljeno, je prepovedano
    - primer varnostne politike iz interneta v domače omrežje
- **Nastavitev varnostne politike glede na naslovov IP ter vrata TCP/UDP:**
  - Strežnik lahko gosti več storitev (npr. HTTP in FTP)
  - Požarni zid zapira / odpira ustrezna vrata (porte) do strežnika

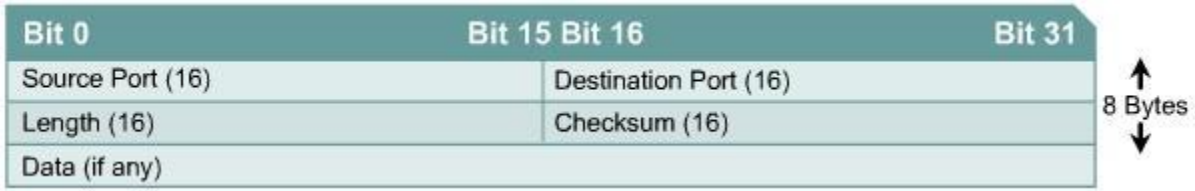


Požarni zid – zavedanje seje

- **Uporaba polja TCP SYN v zaglavju segmenta TCP:**
  - **dovoljene so le predhodno vzpostavljene zveze**
  - **pobudnik zveze postavi zastavico SYN, prenehanje zveze FIN**
    - **požarni zid poleg IP naslova in porta TCP/UDP pregleduje tudi vrednost zastavic SYN in FIN – zavedanje seje**



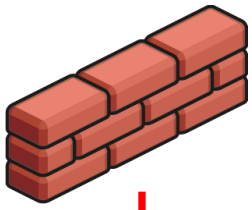
- **UDP je nepovezavno orientiran protokol:**
  - **uporaba časovnikov – UDP sej je odprta 30 sekund**



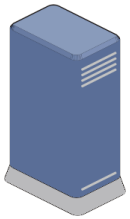
Požarni zid – zavedanje stanja seje

IP = 1.1.1.1

Domače omrežje



Internet



IP = 2.2.2.2

SYN = 1	S TCP = 2000 D TCP = 80	S IP = 1.1.1.1 D IP = 2.2.2.2

Zahteva za komunikacijo s spletnim strežnikom

Požarni zid zgradi tabelo z vnosom:
Dovoli zahteve iz interneta
SIP = 2.2.2.2 & DIP= 1.1.1.1
STCP = 80 & DTCP = 2000
Blokiraj vse ostale zahteve z interneta

S IP = 2.2.2.2 D IP = 1.1.1.1	S TCP = 80 D TCP = 2000	SYN = 1 ACK=1

Odgovor spletnega strežnika poslan odjemalcu

FIN = 1	S TCP = 2000 D TCP = 80	S IP = 1.1.1.1 D IP = 2.2.2.2

Rušenje povezave s spletnim strežnikom

Požarni zid pobriše tabelo

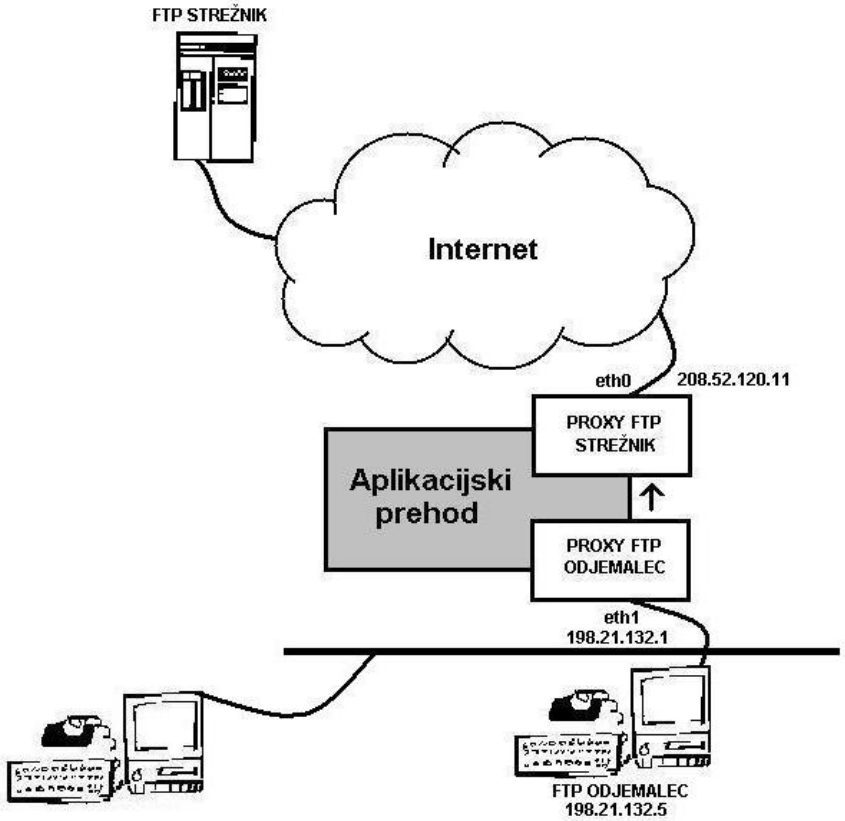
Blokiraj vse ostale zahteve z interneta

Spletni strežnik vzpostavlja sejo

S IP = 2.2.2.2 D IP = 1.1.1.1	S TCP = 80 D TCP = 2000	SYN = 1

Aplikacijski prehod - PROXY

- PROXY sistem = PROXY strežnik + PROXY odjemalec
- Vmesni element med strežniško in odjemalčevo aplikacijo
- Ni direktne komunikacije med entitetama



Demilitarized Zone - DMZ

- Omrežje DMZ v IT svetu – nevtralna cona med omrežjema
  - Trusted
  - Untrustred
- V DMZ območje se postavi javne stežnike (mail, splet ...)
- Pravila
  - DOVOLI PROMET IZ:
    - untrusted > DMZ
    - trusted > DMZ
    - trusted > untrusted
  - BLOKIRAJ PROMET IZ:
    - untrusted > trusted
    - DMZ > trusted