Multicast

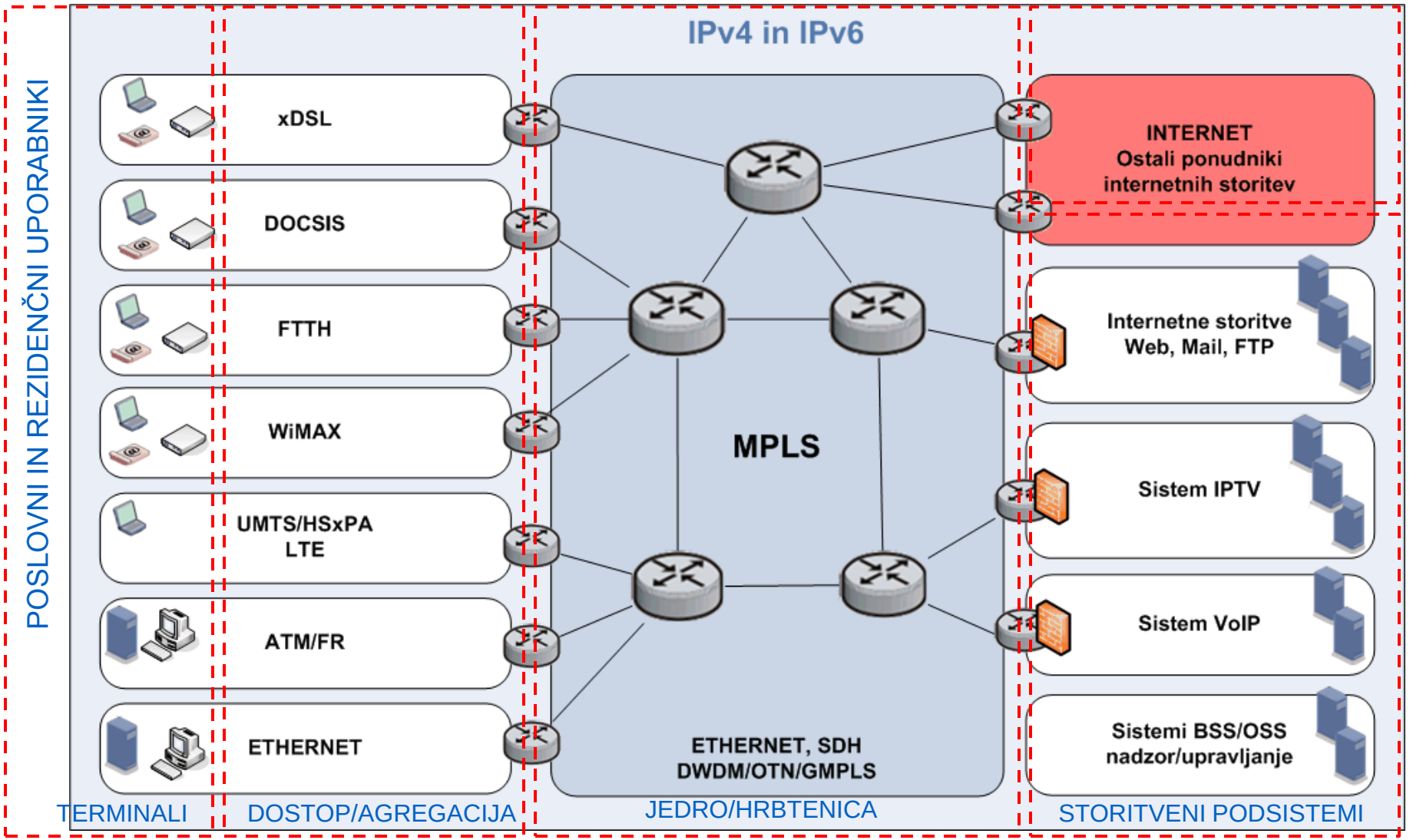
Univerza v Ljubljani
Fakulteta za elektrotehniko
Laboratorij za telekomunikacije

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

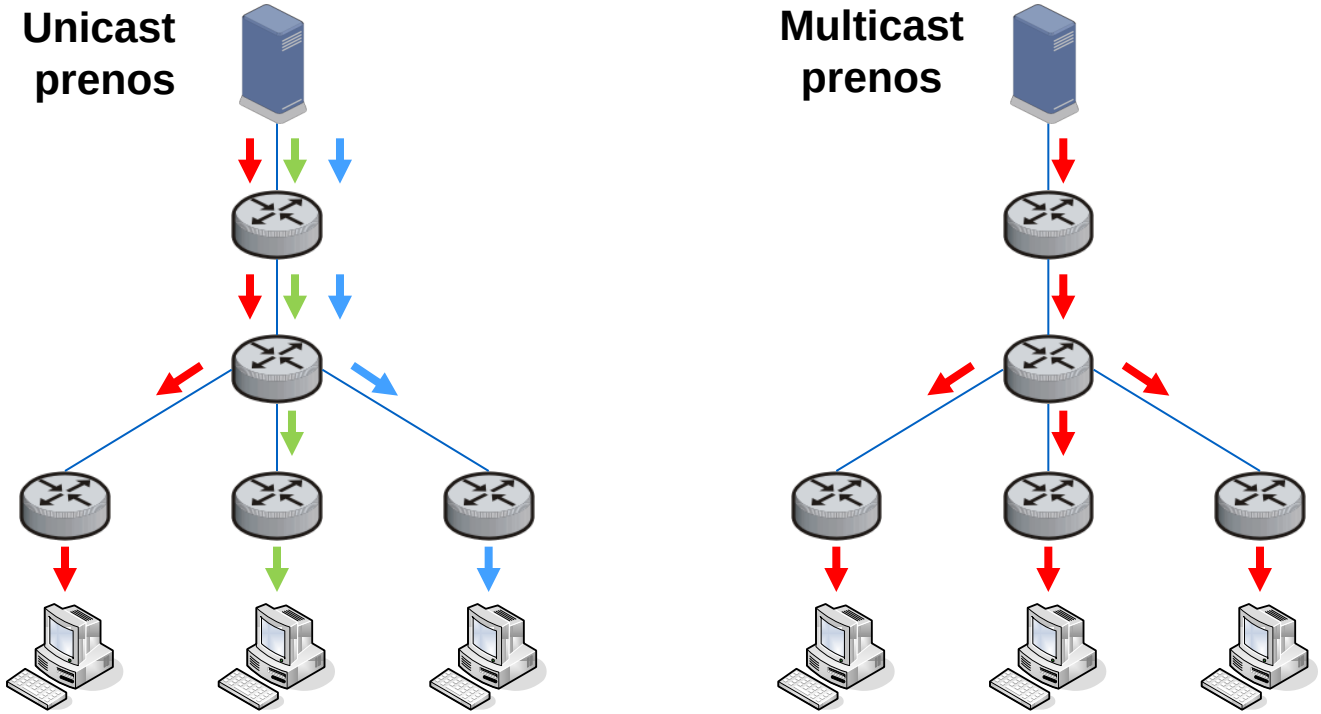
	Omrežne storitve			Tehnologije			
				Ethernet	IPv4	IPv6	MPLS
Kontrolna in upravljavska raven	Varnostne storitve	Zaščita podatkovne ravnine	Avtentikacija	-	IPSec, SSL,HMAC	IPSec, SSL, HMAC	-
			Nadzor dostopa	filtri ACL	IPSec, SSL, filtri ACL, Relay,	IPSec, SSL, filtri ACL, Relay,	filtri ACL
			Zasebnost/enkripcija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

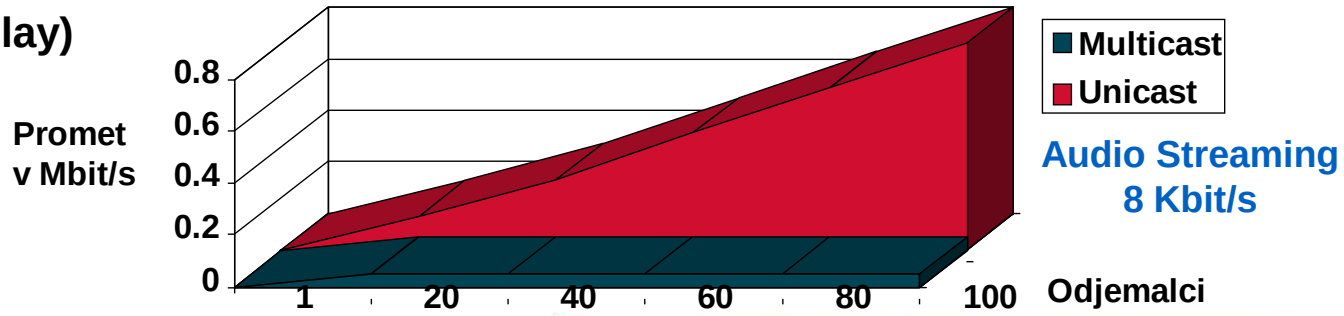
Primerjava unicast in multicast

- **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

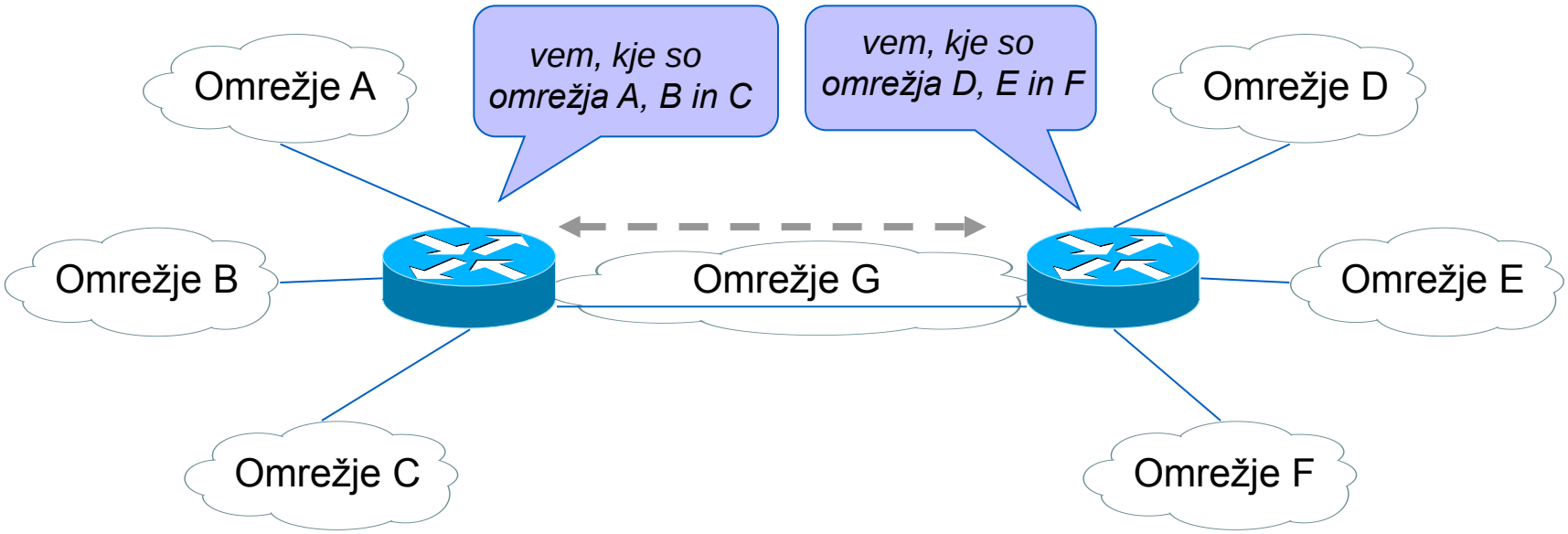
- Protokol IP
  - odprt storitveni model
    - vsak lahko komunicira z vsakim
    - za vse uporabnike se predvideva, da so legitimni
    - ni avtentikacije oddajnika in sprejemnika
      - brez preverjanja izvornih in ponornih naslovov
    - ni enkripcije prenosnega kanala
- Protokol UDP
  - nepovezavno 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?

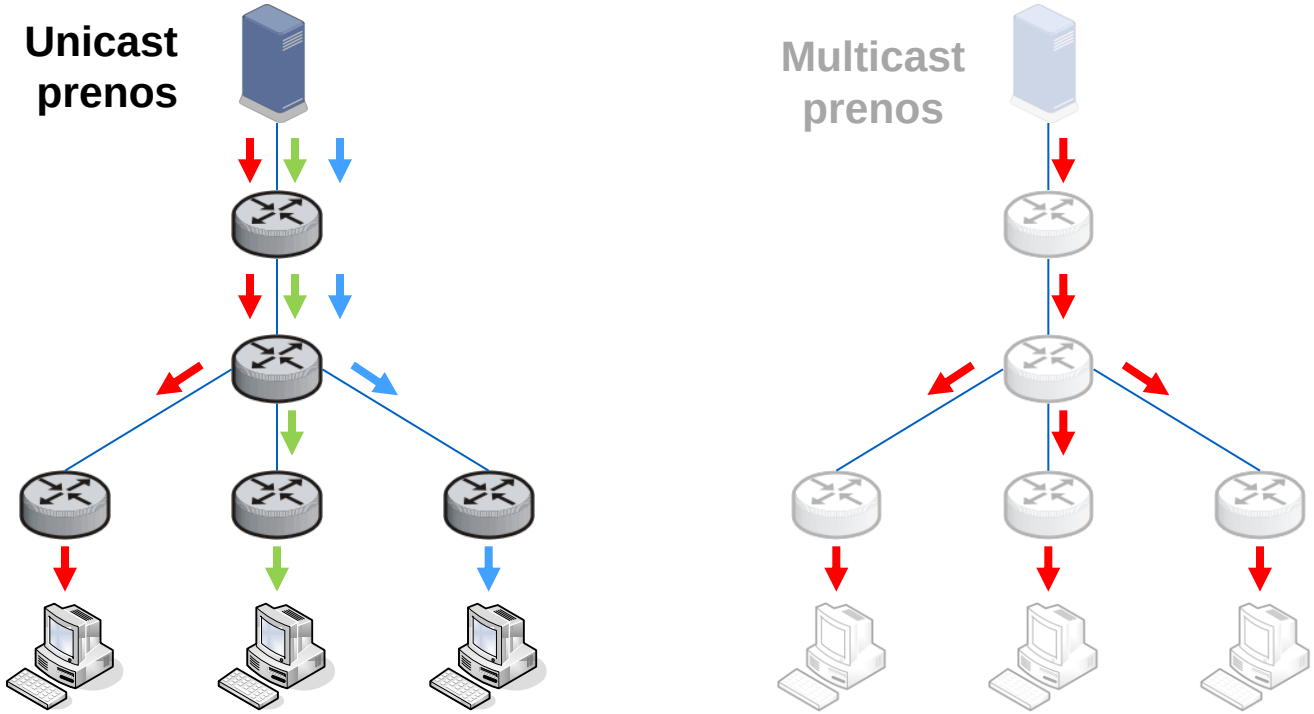
- Izmenjava informacij o dosegljivosti
- Določitev optimalne poti



Unicast prenosni način

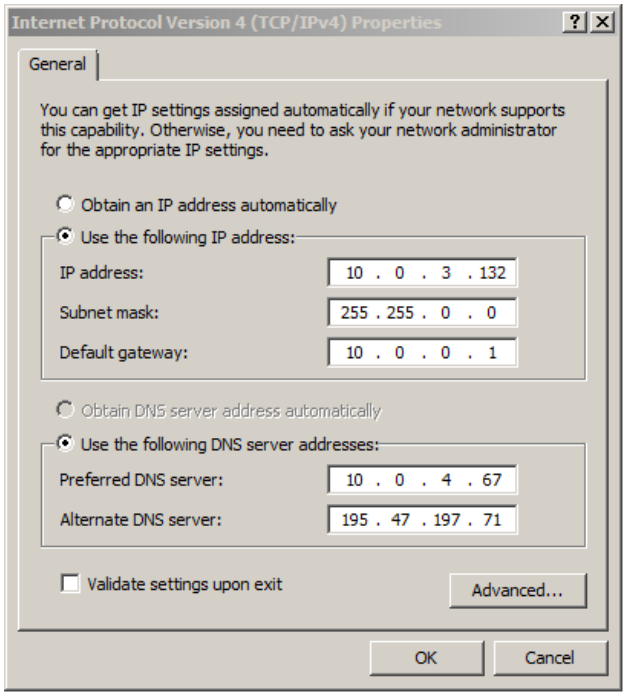
Unicast prenosni način

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



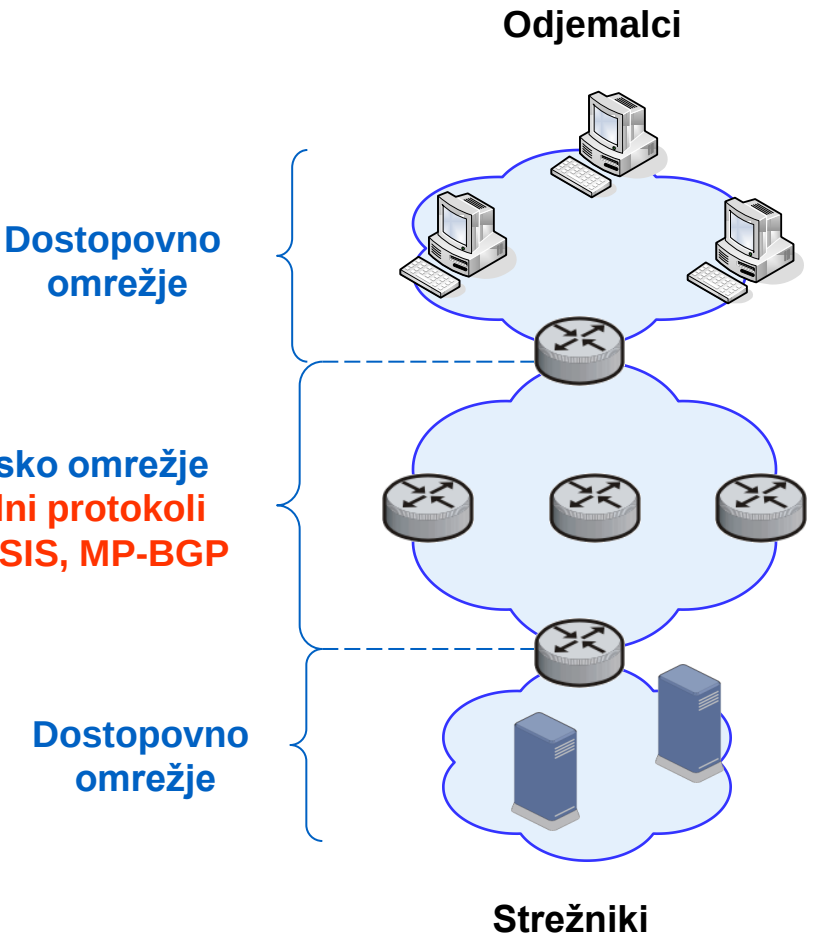
Unicast naslavljanje

- 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



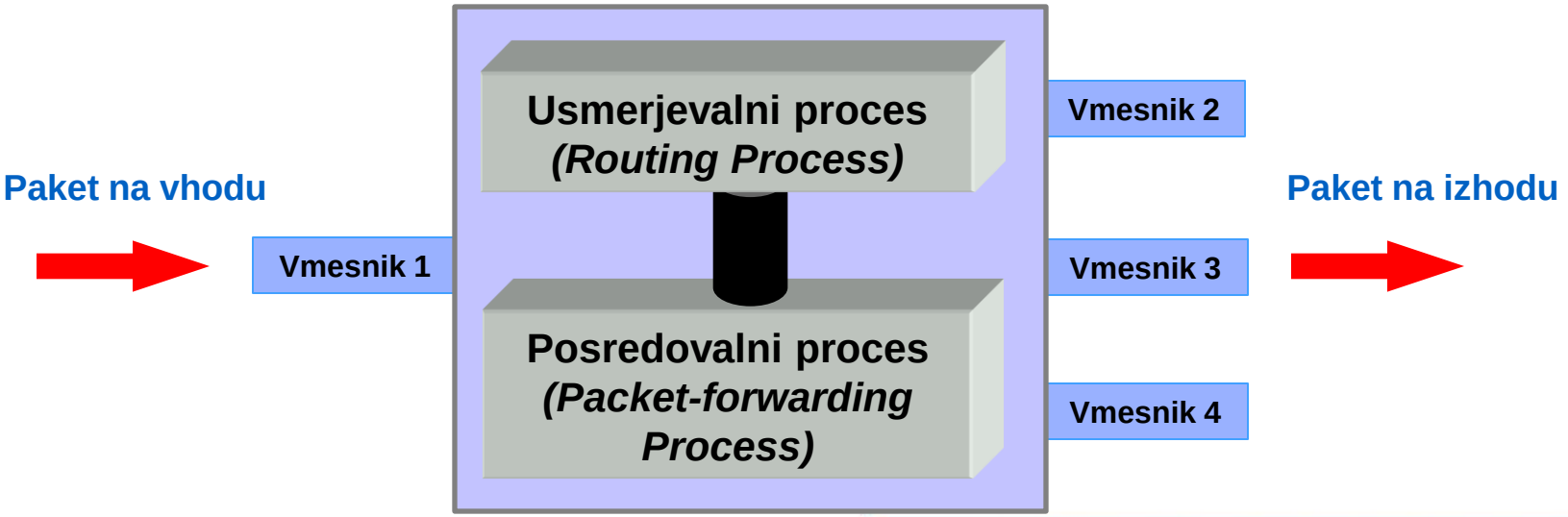
Unicast prenosni način – komponente

- 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

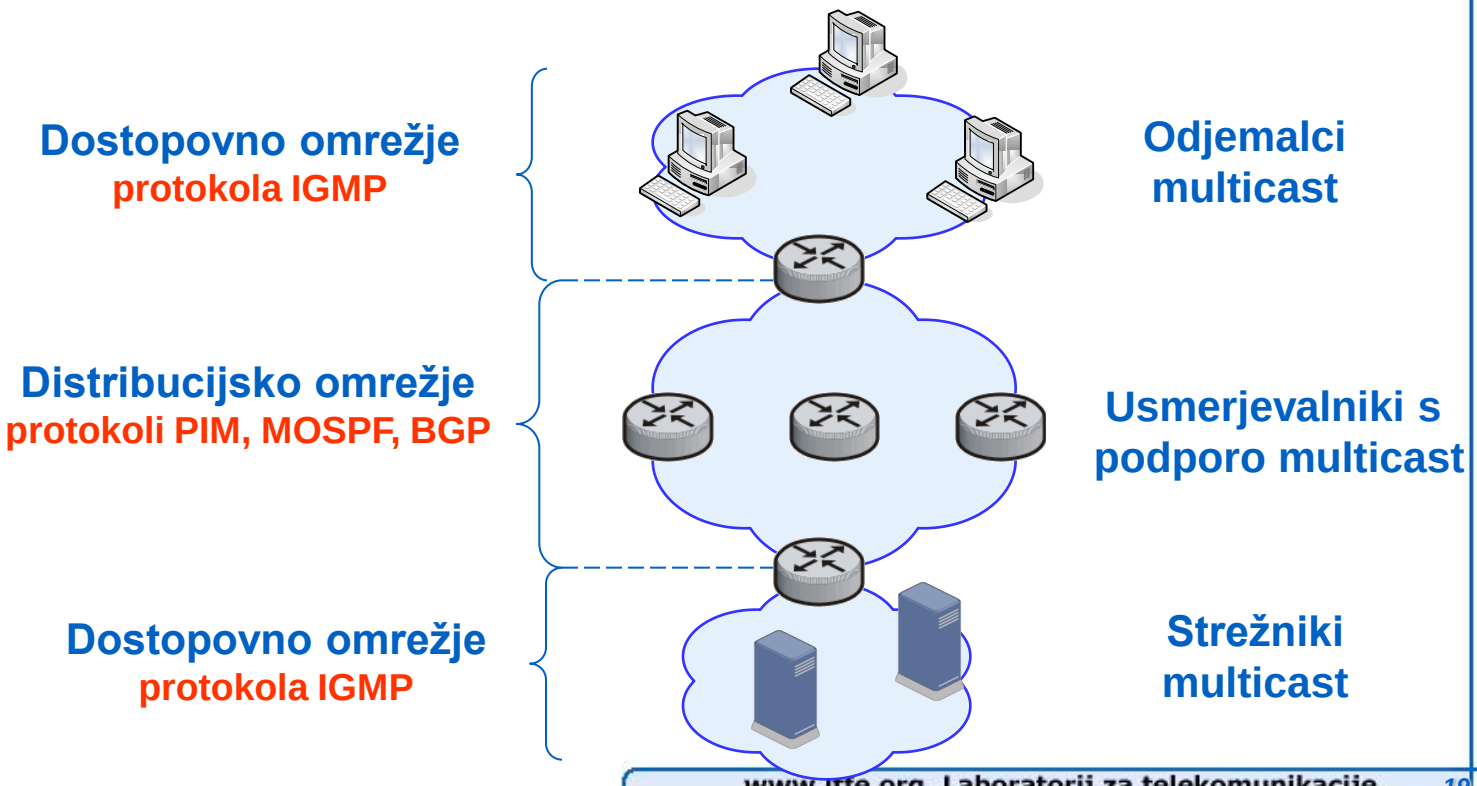
- **Usmerjevalni proces**
  - izmenjava usmerjevalnih informacij
  - določitev optimalne poti
  - izvaja se lahko v nerealnem času
- **Posredovalni proces**
  - Izbira ustreznega vmesnika “angl. longest-prefix-mach”
  - posredovanje paketov na izhodni vmesnik
  - izvajati se mora v realnem času



Multicast prenosni način

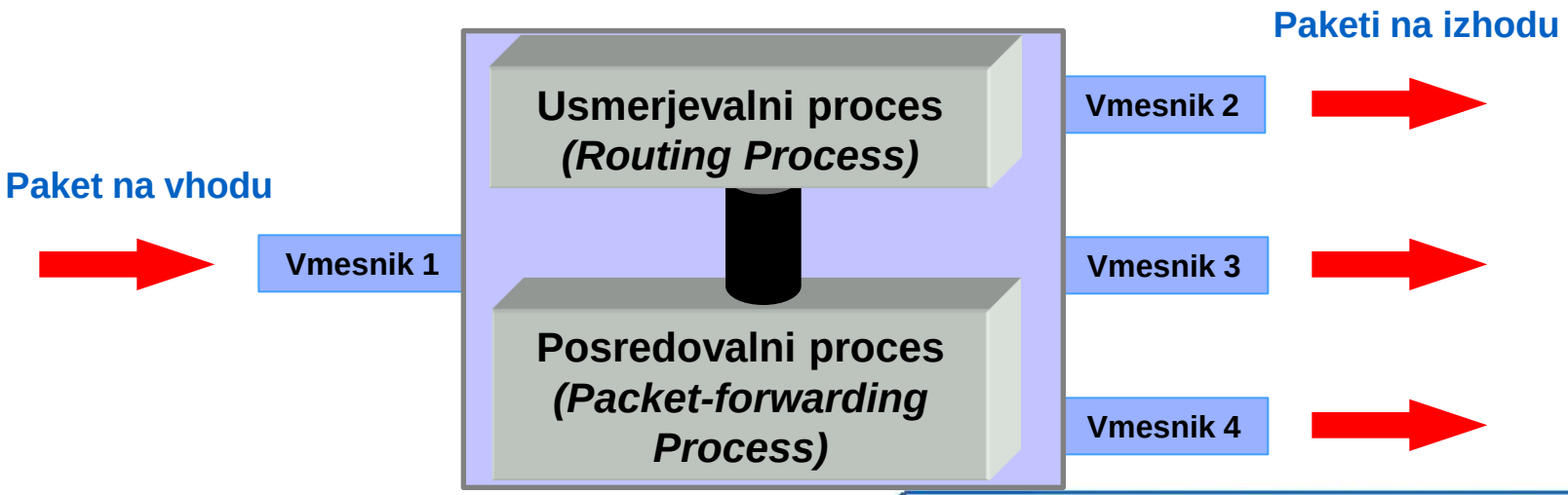
Multicast prenosni način - komponente

- 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

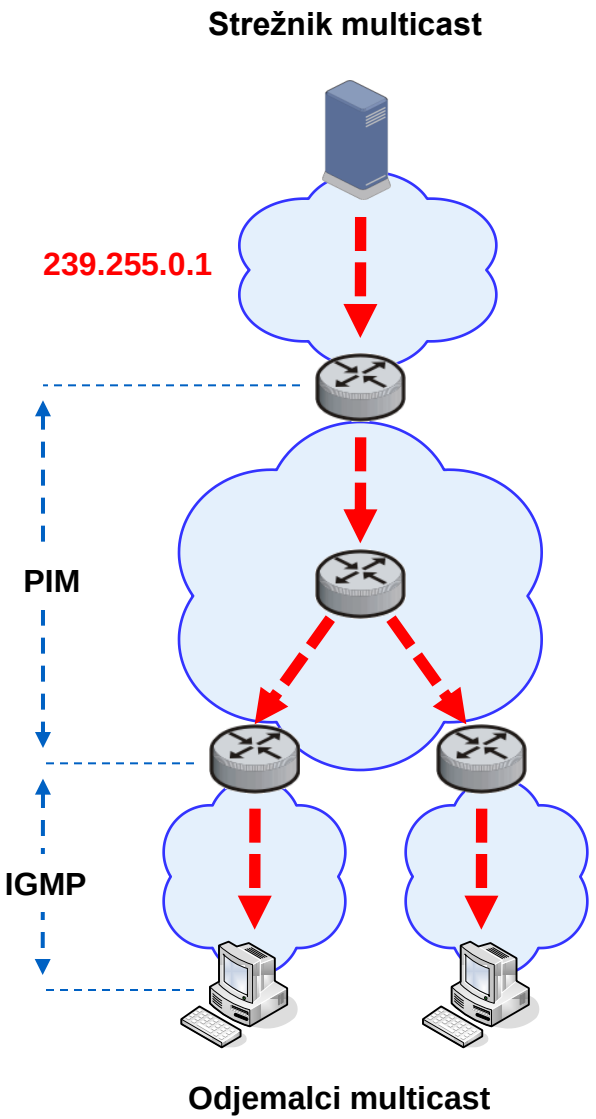
- Multicast aplikacije delujejo po principu nepovezavnih sistemov
  - za transport se uporablja protokol UDP
  - ne zagotavlja zanesljive dostave datagramov
  - ne vsebuje mehanizmov za kontrolo zamašitev v omrežju
- Posamezni datagrami lahko prihajajo v nepravilnem vrstnem redu
- Tehnologija multicast 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

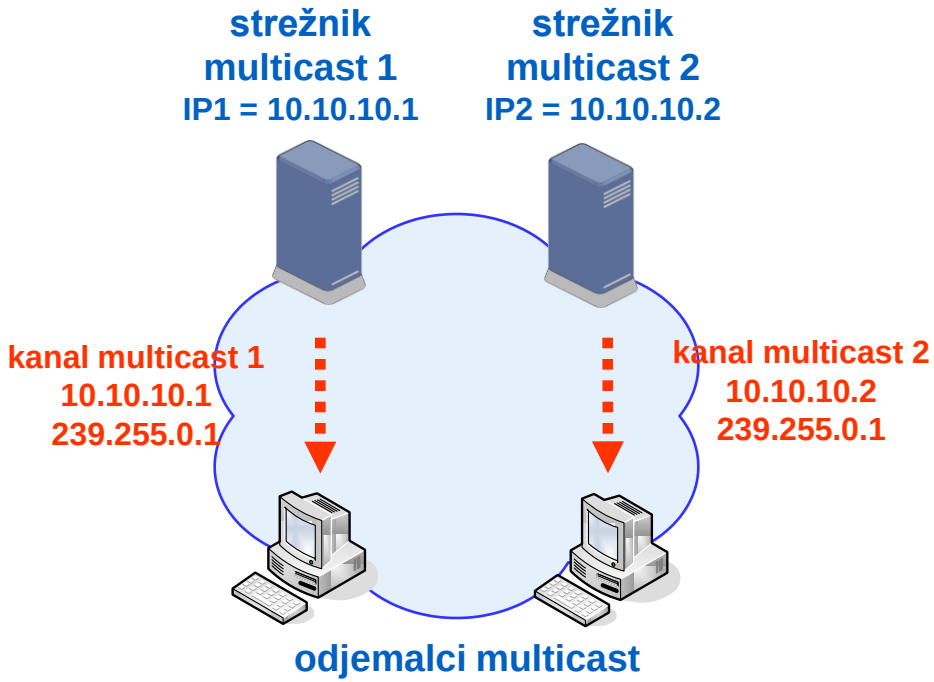


Storitveni model SSM

- 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

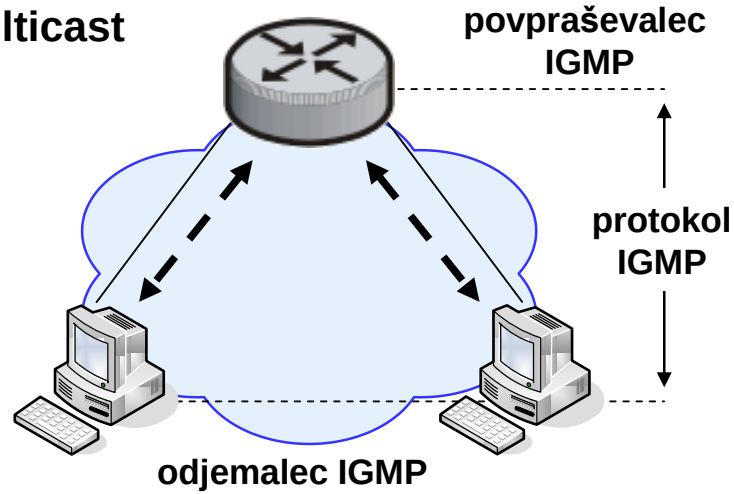
- Rezervirani naslovi
  - rezervirani lokalni ˝Link-local Control Block˝
    - 224.0.0.0 – 224.0.0.255
    - oddani s TTL = 1
      - 224.0.0.1 naslavljanje vseh multicast naprav
      - 224.0.0.2 naslavljanje vseh multicast usmerjevalnikov
      - 224.0.0.5 naslavljanje usmerjevalnikov OSPF
  - rezervirani 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

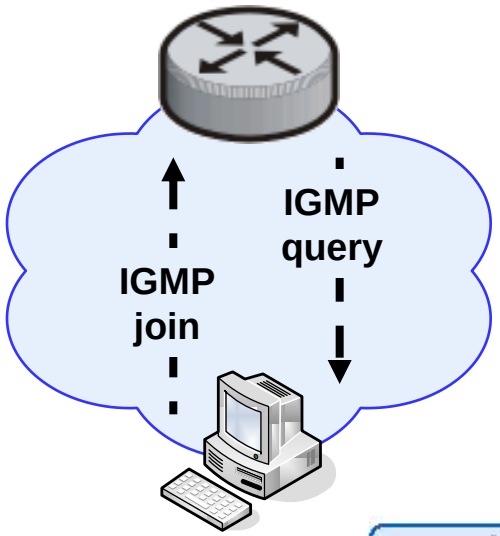
Protokol IGMP

- **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



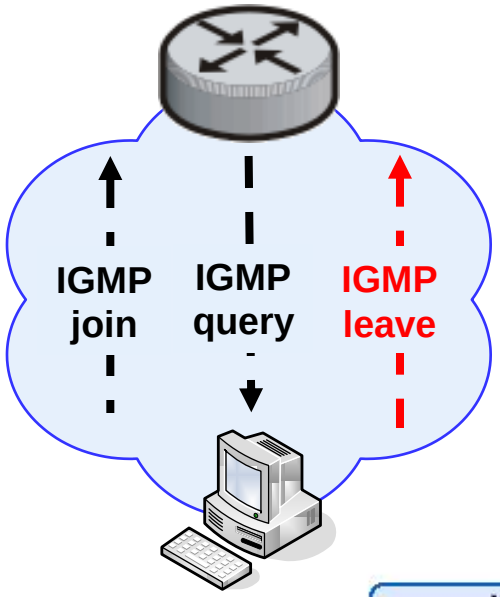
Protokola IGMPv1 in IGMPv2

- 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



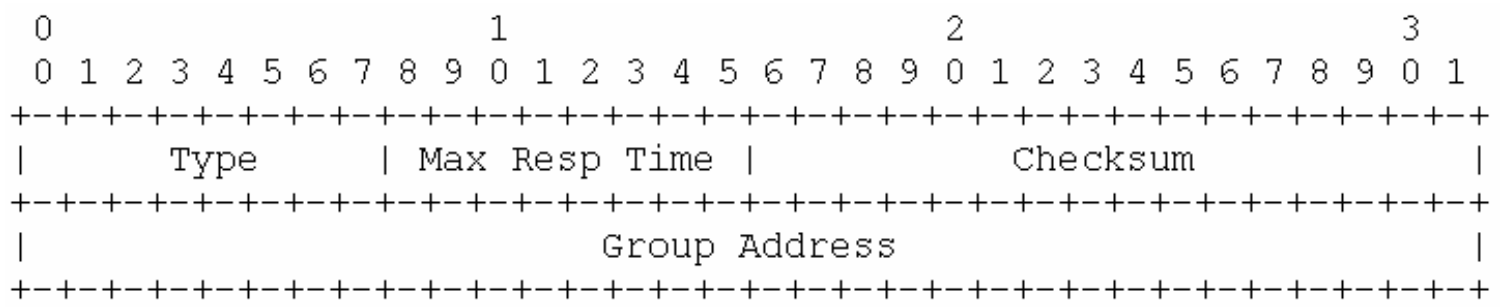
Protokola IGMPv1 in IGMPv2 – odjava

- 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

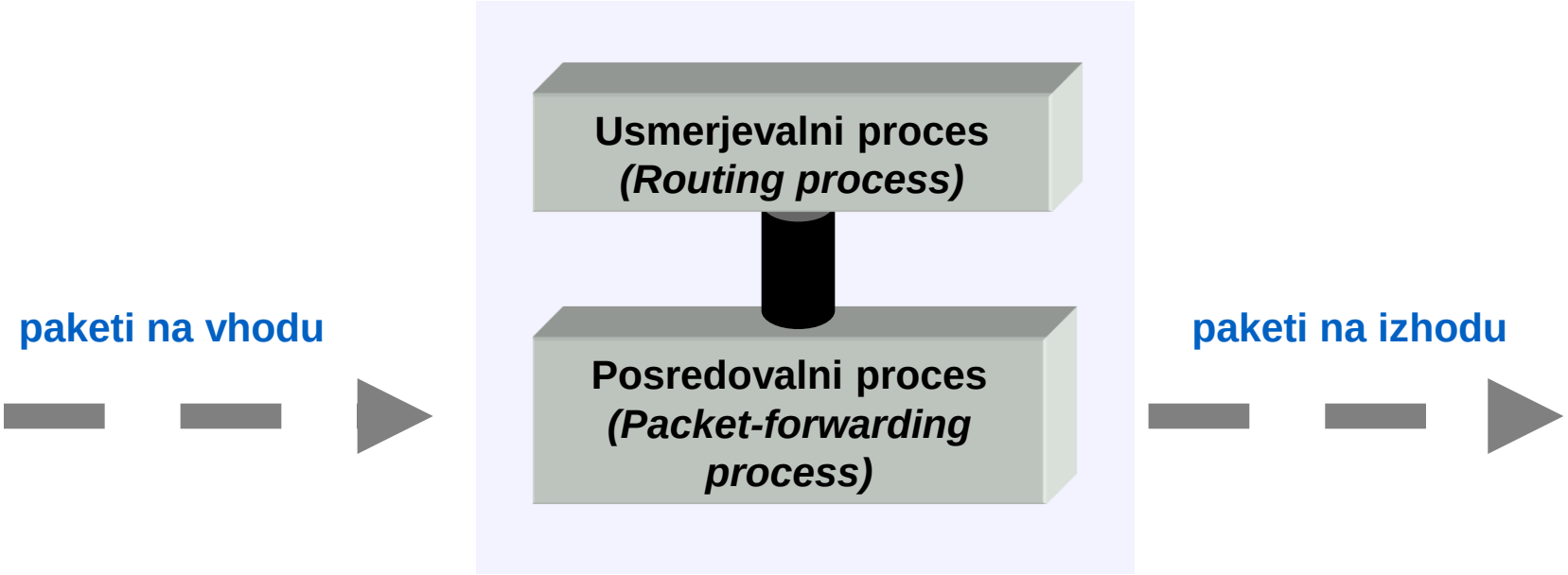
- Ključna novost, ki jo uvaja protokol IGMPv3 je možnost neposredne izbire izvora multicast prometa, ki oddaja v izbrano multicast grupo
- Odjemalci se lahko prijavljajo v multicast grupo na dva načina
  - ˝include mode˝ – odjemalec eksplicitno določi multicast strežnike od katerih bo sprejemal multicast 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**

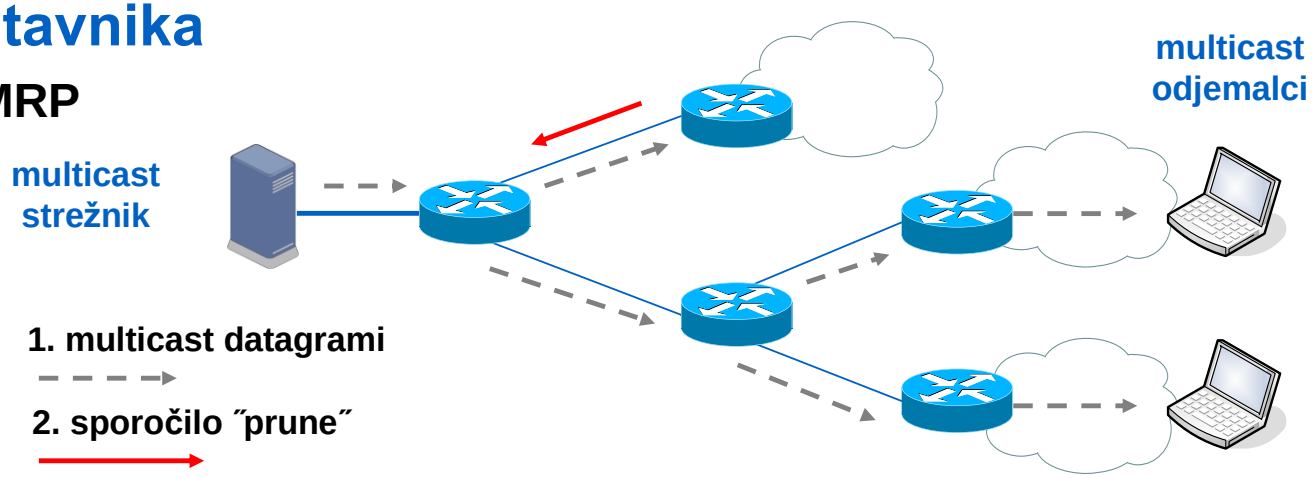


Multicast usmerjanje

- 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

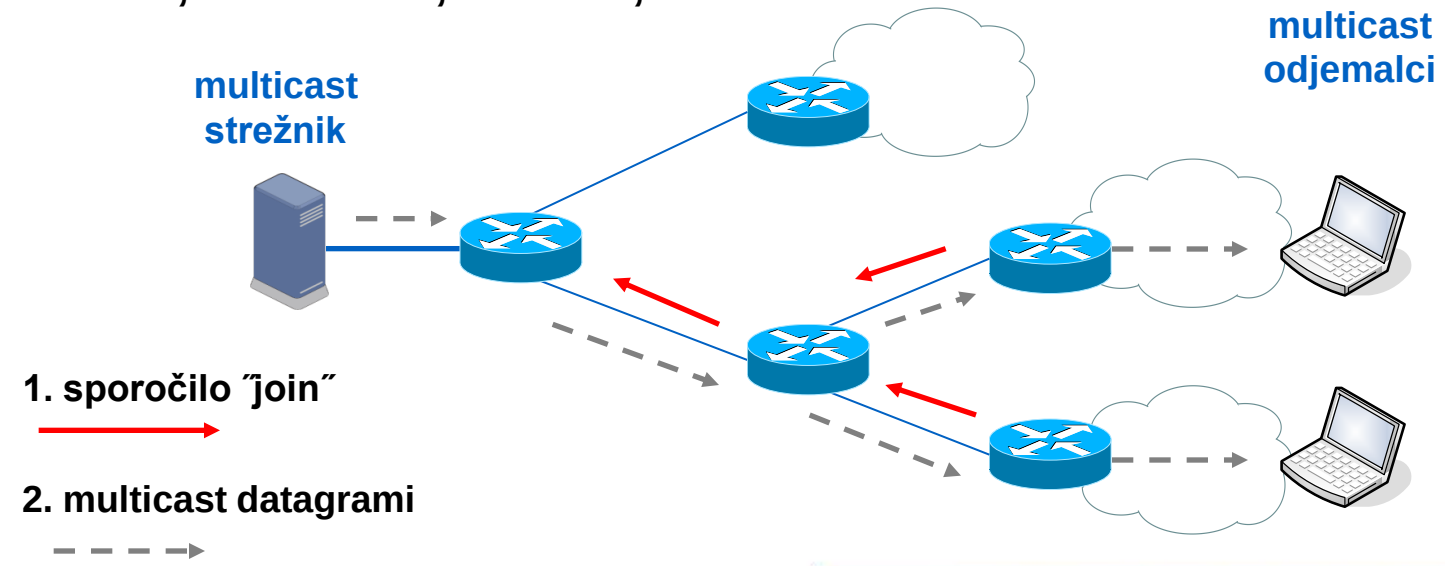
Zgoščeni način ˝dense mode˝

- 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

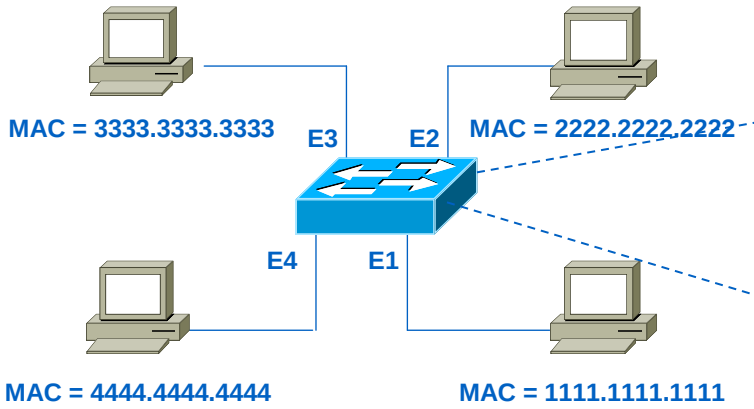


tabela MAC

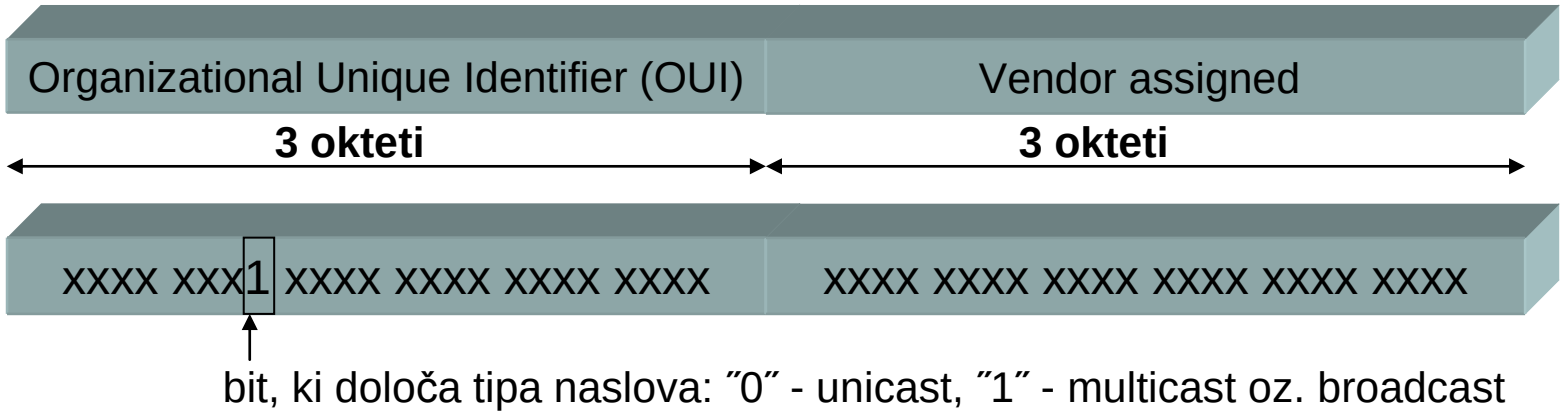
ciljni naslov MAC	izhodni vmesnik
1111.1111.1111	E1
2222.2222.2222	E2
3333.3333.3333	E3
4444.4444.4444	E4

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

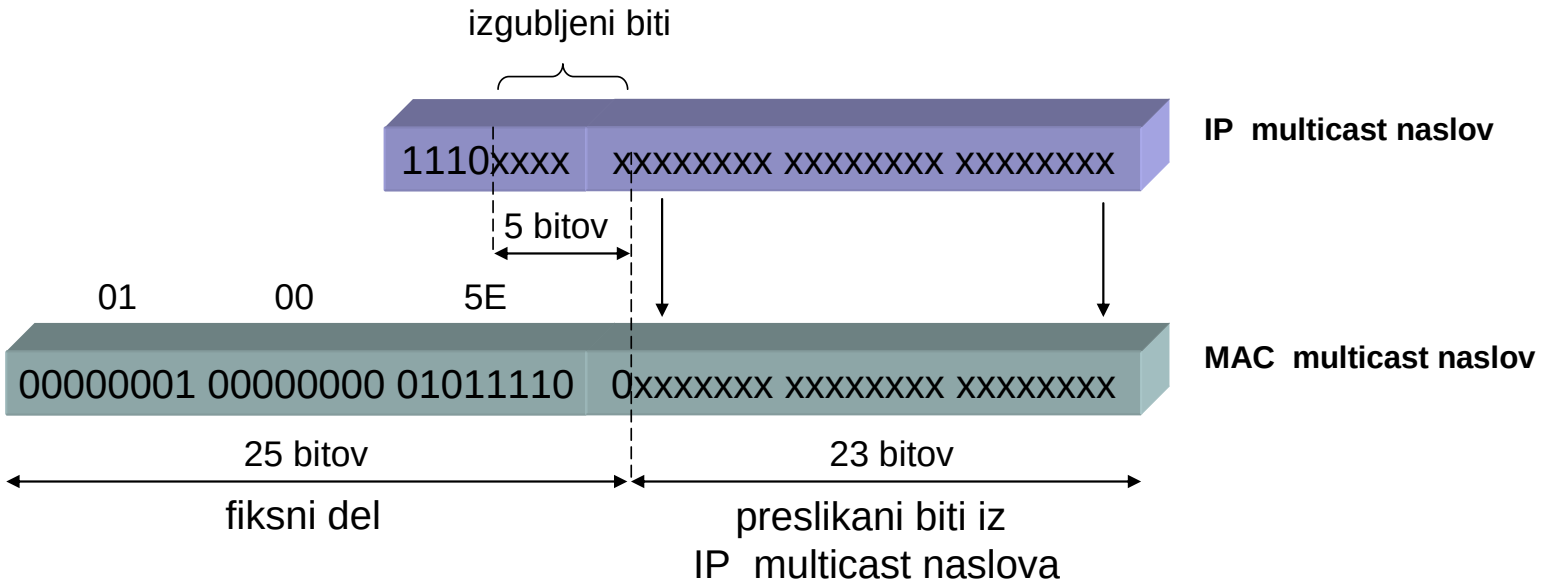
Ethernet multicast naslavljanje 1/2

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

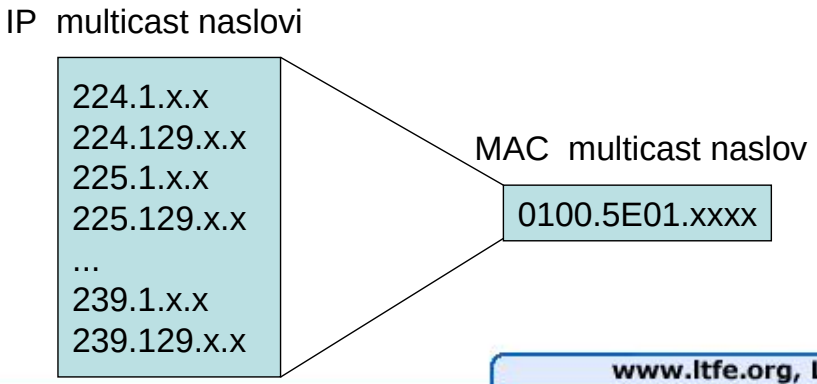


Ethernet multicast naslavljanje 2/2

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



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



Vsebina

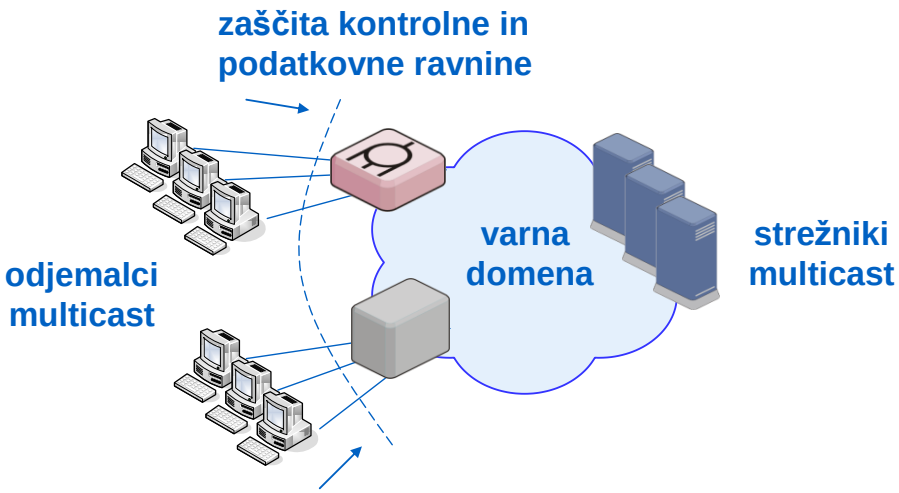
- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- **Varnost v multicast**
- Uporaba multicast

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

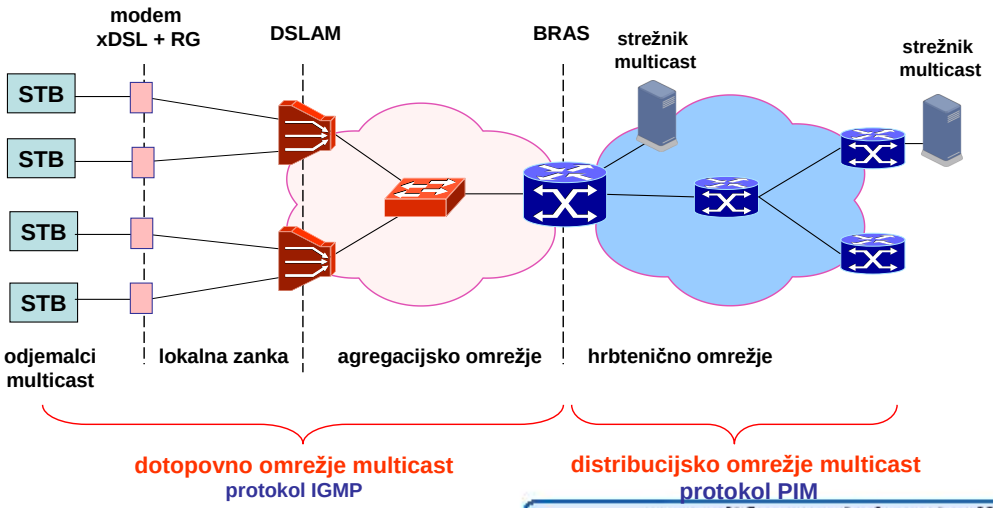
- Če ne obstaja tesna povezava med upravljalcem omrežja in ponudniki storitev
- Primer IPTV
  - sistemi DRM (ang. Digital Rights Management)
  - sistemi CA (ang. Conditional Access)
  - sistema omogočata ponudnikom storitev popoln nadzor nad dostopom do vsebin
- Ključna prednost modela je, da je vsebina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

Vsebina

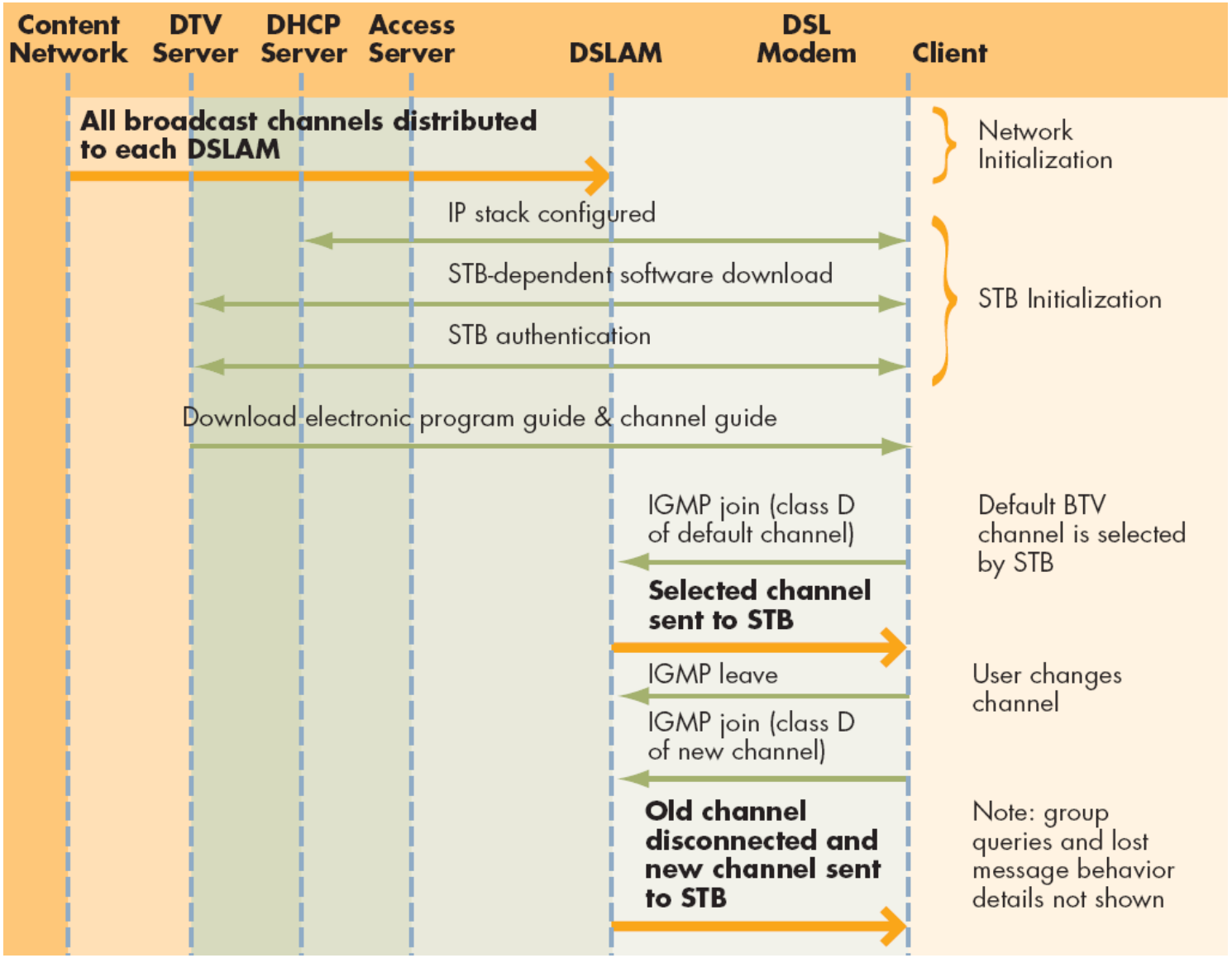
- Uvod
- Osnovni koncepti
- Multicast naslavljanje
- Protokol IGMP
- Multicast usmerjanje
- Ethernet multicast
- Varnost v multicast
- Uporaba multicast

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