

# Komunikacijski protokoli in omrežna varnost

## Razpošiljanje (*multicast*)

1

---

---

---

---

---

---

---

---

### Razpošiljanje

- **Načini naslavljanja:**
  - **unicast** (tradicionalno): pošiljanje enemu ciljnemu IP naslovu (unikaten v Internetu / lokalnemu omrežju)
  - **broadcast** (oddajanje): „naslavljanje vseh prejemnikov“ v podomrežju (npr. iskanje usmerjevalnika ali strežnika, nujno sporočilo); ne dostavlja paketov izven lokalne mreže
- Kako poslati samo izbrani skupini naslovov, tudi izven lokalne omreže?
  - **multicast** naslavljanje (razpošiljanje) omogoča dostavo skupinam ne glede na meje podomrežij
  - IGMP (*Internet Group Management Protocol*) se uporablja za upravljanje s skupinami

2

---

---

---

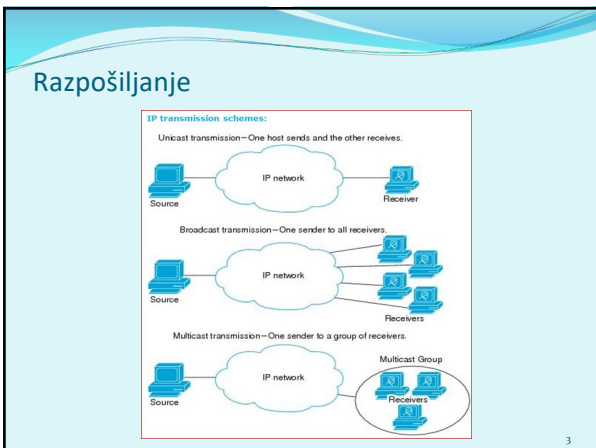
---

---

---

---

---



3

---

---

---

---

---

---

---

---

### Razpošiljanje - primer

Poslati želimo 4 od 6 računalnikov v omrežju. Kako?

- unicast**: potrebujemo 6 kopij istega paketa, večkratno pošiljanje obremenjuje medij
- broadcast**: naslovi vse računalnike, filtriranje pravih prejemnikov prepustimo protokolom na višjim plastem.
- multicast**: pošljemo „posebnemu naslovu“, ki predstavlja SKUPINO prejemnikov, ki poslušajo pakete, naslovljene na ta naslov
  - podobno kot *broadcast*: paket dobijo vsi
  - vendar: filtriranje se izvede na omrežnem nivoju - IP (včasih lahko tudi na povezavnem nivoju)

4

---

---

---

---

---

---

---

---

### Razpošiljanje: usmerjanje paketov

- broadcast** paketov usmerjevalniki ne posredujejo (dobili bi jih vsi!), torej ostajajo znotraj lokalnega omrežja
- usmerjanje pri razpošiljanju** je praktično: en sam paket usmerjevalniki razmnožijo in posredujejo samo preko tistih vmesnikov, kjer so poslušatelji paketa. Ime skupine je 32 bitno število (skoraj)

5

---

---

---

---

---

---

---

---

### Razpošiljanje: usmerjanje paketov

- Izzivi protokola**:
  - postopek razpošiljanja:
    - odkrivanje, kje so prejemniki paketa,
    - razpošiljanje zahteva dodatno delo: usmerjevalni protokoli, posredovanje informacije o poslušateljih,
    - razpošiljalni naslovi ne oblikujejo (pod)mrež -> maska ima 32 bitov. V usmerjevalnih tabelah zato zahtevajo posebne vnose
    - izziv: *lahko imajo tudi več posebnih vnosov, zakaj?*
  - varnost:
    - ali lahko paket razpošlje vsakdo ali samo član skupine?
    - prisluškovalec se lahko naroči na poslušanje paketov in postane legitimni prejemnik
  - zanesljivost:
    - kaj narediti, če samo en prejemnik javi, da ni dobil paketa?

6

---

---

---

---

---

---

---

---

### Razpošiljanje

naročanje na multicast promet (IGMP)

multicast usmerjanje (PIM)

7

7

---

---

---

---

---

---

---

---

### Aplikacije razpošiljanja

- pošiljanje velikih datotek preko omrežja (glavni urad podružnicam) – zanesljivi prenos.
- nadgradnja programske opreme v velikem omrežju
- podatkovni tokovi (*data streaming*) – npr. pošiljanje podatkov o delnicah vsem finančnim družbam)
- audio/video tokovi podatkov (*streaming*)
- video na zahtevo (spremljanje TV programa)
- izvedba konferenc (pomislek: boljša uporaba konferenčnega centra, ki odloča, kdo lahko govori in čigave pakete posredovati drugim)
  - izziv: premisli, kako izgleda izvedba konference z *multicast pristopom*
- aplikacije v realnem času z RTP, ki se uporablja za zagotavljanje tekoče in kakovostne dostave v okoljih, kjer se uporablja razpošiljanje

8

8

---

---

---

---

---

---

---

---

### Naslavljanje IPv4 in IPv6

9

9

---

---

---

---

---

---

---

---



## Prijava na multicast promet: protokola IGMP in MLD

Click here to Enroll Now ▶

13

---

---

---

---

---

---

---

---

## Protokol IGMP

- mrežni protokol je IPv4 paketu in številka protokola je 2
- RFC 2236, *Internet Group Management Protocol, Version 2*, RFC 3376, *Internet Group Management Protocol, Version 3*
  - obvezno: poiščite ga na spletu ter ga preberite – literatura!
  - izziv: poiščite še ostale RFC dokumente, ki se ukvarjajo z IGMP
- IGMP skrbi za upravljanje s tem, kdo so prejemniki razpošiljanih sporočil. Omogoča:
  - pridružitve skupini
  - izstop iz skupine
  - zaznavanje drugih vmesnikov v skupini

14

---

---

---

---

---

---

---

---

## Protokol IGMP

- IGMP komunikacija poteka med odjemalcem in najbližjim razpošiljevalnim usmerjevalnikom
- na podlagi protokola IGMP usmerjevalniki dobijo nalogo povezati se v strukturo razpošiljevalnega drevesa

15

---

---

---

---

---

---

---

---

### Verzije IGMP

Obstajajo verzije IGMP v1, v2 in v3.

- IGMPv1: Vmesniki se lahko pridružijo skupinam. Sporočila za izstop ne obstajajo. Usmerjevalniki uporabljajo mehanizem s pretekom časa, da odkrivajo skupine, ki za vmesnik niso zanimive.
- IGMPv2: Dodana sporočila za izstop iz skupine. S tem omogočeno hitrejša sporočanja usmerjevalniku o prekinitvi dostave nepotrebne prometa.
- IGMPv3: Večje spremembe v protokolu. Vmesniki lahko določijo SEZNAM drugih vmesnikov, od koder želijo prejemati promet. Promet od ostalih vmesnikov omrežje prepreči.

16

16

---

---

---

---

---

---

---

---

### Protokol IGMP

- IGMP sporočilo je dolgo 8 zlogov

8	16	32
type	max. resp. time	checksum
multicast group address		

- **type** - tip sporočila:
  - 17 (0x11): Group Membership Query (odkrivanje članov skupine)
  - 18 (0x12): Group Membership Report IGMP v1 (objava prejemnika)
  - 22 (0x16): Group Membership Report IGMP v2 (objava prejemnika)
  - 34 (0x22): Group Membership Report IGMP v3 (objava prejemnika)
  - 23 (0x17): Leave Group Report IGMP v2 (objava, da je prejemnik zapustil skupino)
- **response time** - čas, v katerem se mora prejemnik klica IGMP Group Membership Query, odzvati
- **checksum** - kontrolna vsota (ne pokriva IP glave)
- **multicast group address** - IPv4 naslov razpošiljevalne skupine

17

17

---

---

---

---

---

---

---

---

### Protokol IGMP

- Kako z IGMP udejaniti upravljanje s skupinami?

Dejanje	IGMP sporočilo	IP Destination Address	IGMP Multicast Group Address
pridružiti se želim skupini	Group Membership Report	naslov skupine	naslov skupine
kdo vse je član določene skupine?	Group Membership Query	naslov skupine	naslov skupine
katero skupino obstajajo?	Group Membership Query	vsi vmesniki (224.0.0.1)	0.0.0.0
sam član skupine, o kateri se porzveđuje, želim se odzvati, da sem član	Group Membership Report	naslov skupine	naslov skupine
zapustiti želim skupino	Group Leave Report	vsi usmerjevalniki (224.0.0.2)	naslov skupine

18

18

---

---

---

---

---

---

---

---

### Protokol IGMP

- Posebno sporočilo: IGMPv3 Group Membership report

Type	Not used	Checksum
Not used		Number of Addresses
Multicast Group Address Response		
Multicast Group Address Responses...		

- *Type*= 0x22
- odgovori vseh vmesnikov v skupini so zbrani v istem paketu
- vmesnik čaka na odgovore drugih prejemnikov v skupini, preden odgovori sam
  - posebna oblika paketa torej omogoči izogibanje podvojenemu multicast prometu

19

---

---

---

---

---

---

---

---

### Protokol IGMP: prijava na vir

**korak 1:**

- za pridružitve skupini, se pošlje GMR (*group membership request*) sporočilo z vrednostjo TTL=1
  - dostava samo najbližjemu usmerjevalniku
- usmerjevalnik evidentira, da mora skupinske pakete posredovati novemu naročniku
  - kako? – povezavni razpošiljevalni naslov / kopije datagramov na IP naslov

20

---

---

---

---

---

---

---

---

### Protokol IGMP: prijava na vir

**korak 2:**

- usmerjevalnik sporoči sosednjim usmerjevalnikom, da ima novega naročnika. Če bi vsak usmerjevalnik sporočil enako naprej, pride do problema - paketi bi se posredovali navzkrižno preko vseh povezav v omrežju. Rešitvi:
  - **uporablja se RPL algoritem** (*Reverse Path Lookup*): zavržemo vse multicast pakete, ki pridejo od usmerjevalnikov, ki ne povezujejo z izvorom paketa po najbližji poti
  - **usmerjevalniki imajo posebne usmerjevalne protokole** za multicast promet: npr. protokol PIM-SM (*Protocol Independent Multicast - Sparse Mode*)

21

---

---

---

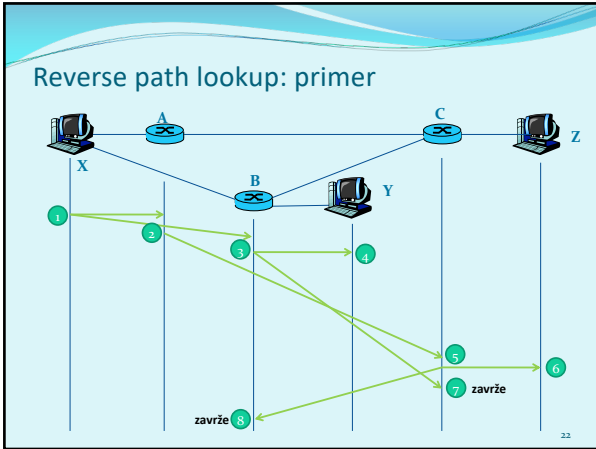
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

### Protokol MLD

- Multicast Listener Discovery:
  - RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*, in
  - [RFC 3810, Multicast Listener Discovery Version 2 \(MLDv2\) for IPv6](#)
- *obvezno: poiščite ga na spletu ter ga preberite – literatura!*
  - *kaj je to Robustness Variable in čemu služi?*
- *izziv: poiščite razlike med MLD in IGMP*
- *izziv: kaj pa sobivanje IGMP (IPv4) in MLD (IPv6)?*

23

---

---

---

---

---

---

---

---

---

---

### Protokol MLD

- Dejansko je protokol za IPv6 za razpošiljanje in ima enako funkcionalnost kot IGMP

24

---

---

---

---

---

---

---

---

---

---



### Protokol IGMP in MLD

- MLD:
 

0	1	2	3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31			
Type	Code	Checksum	
Maximum Response Delay	Reserved		
Multicast Address			
- IGMP:
 

0	1	2	3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31			
Type	Max Resp Time	Checksum	
Group Address			

35

25

---

---

---

---

---

---

---

---

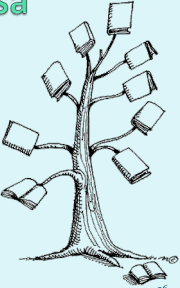
---

---

---

---

### Razpošiljevalna drevesa



36

26

---

---

---

---

---

---

---

---

---

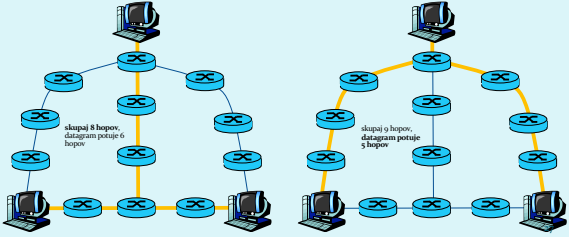
---

---

---

### Razpošiljanje prometa

- paketi se gibljejo v obliki razpošiljevalnega drevesa
- drevo lahko optimizira različne kriterije:
  - slika 1: skupna dolžina poti (število hopov) vseh datagramov
  - slika 2: najkrajša pot za vsak datagram posebej (minimalno vpeto drevo)



37

27

---

---

---

---

---

---

---

---

---

---

---

---

### Usmerjanje multicast

- Naloga usmerjanja: najti drevo povezav, ki povezuje vse usmerjevalnike v isti razpošiljalni skupini
- Za komunikacijo med usmerjevalniki potrebujemo razpošiljalne usmerjevalne protokole (aplikacijski protokoli, ki delujejo v pomoč omrežni plasti), kot so: PIM, DVMRP, MOSPF in BGP.

kako rdeče usmerjevalnike povezati v skupno drevo?

28

---

---

---

---

---

---

---

---

### Dve rešitvi iskanja razpošiljalnega drevesa

- uporaba enega samega drevesa za vse usmerjevalnike za usmerjanje razpošiljalnega prometa se določi eno samo drevo (*group-shared tree*) - slika levo
- določitev ločenega drevesa za vsakega udeleženca v skupini (*source-based tree*); za N članov skupine imamo torej N dreves (za vsako razpošiljalno skupino) - slika desno

skupno drevo

ločeno drevo za A (modro) in drevo za B (roza)

29

---

---

---

---

---

---

---

---

### Določanje skupnega drevesa (group-shared)

- iskanje drevesa z **minimalno skupno ceno** (uporablja se Steinerjev algoritem za vpeta drevesa, problem je NP poln), slika levo ali
- določitev **centralnega vozlišča** (*rendez-vous point*) –kako usmerjati do njega je znano iz pravil za unicast usmerjanje; usmerjevalnik se pridruži drevesu, ko na poti do centralnega vozlišča naleti na prvo vozlišče, ki je že v drevesu, slika desno

minimalna skupna cena

E je centralno vozlišče

30

---

---

---

---

---

---

---

---

### Določanje dreves posameznih pošiljateljev (source-based)

- Iskanje **drevesa najkrajših poti** v grafu (uporaba Dijkstrovega algoritma, ki išče drevo najkrajših povezav glede na podano začetno vozlišče), *slika levo*
  - usmerjevalniki morajo poznati stanja vseh povezav (*link-state*)
- ali
- Uporaba **RPL (Reverse Path Lookup)**: ne sprejemamo sporočil od usmerjevalnikov, ki niso na najbližji poti do izvora sporočila, *slika desno*
  - drevo je prekrivno omrežje (*overlay network*) v celotnem omrežju

31

---

---

---

---

---

---

---

---

### Usmerjanje razpošiljanja

32

---

---

---

---

---

---

---

---

### Usmerjevalni protokoli

- skrbijo za oglaševanje skupin v omrežju
- delimo jih po 2 kriterijih (2x2=4 skupine)
  - razpršeno / gosto (*sparse-mode / dense-mode*)
    - sparse-mode*: posamezna vozlišča zahtevajo vključitev v drevo (*pull* princip)
    - dense-mode*: razpošiljene pakete razpošljemo po vsem omrežju, usmerjevalniki se odjavljajo, če so nepotrebni (*push* princip). Tu dva načina:
      - oddaja in odreži (*broadcast and prune*): uporaba *prune* in *graft* sporočil; struktura se občasno reinitializira
      - domenska (*domain-wide*) poročila: usmerjevalniki z oddajanjem prijavljajo odjemalce na promet
  - intra (znotraj domene) / interdomain (med domenami)

33

---

---

---

---

---

---

---

---

## Usmerjevalni protokoli

- obstaja povezava med načinom delovanja in vrsto drevesa, ki ga protokol gradi

Protokol	Način delovanja	vrsta drevesa	Vrsta
PIM-SM	sparse	skupno	znotraj in med domenami
PIM-DM	dense	posamezno	znotraj domen
CBT	sparse	skupno	znotraj in med domenami
MOSPF	dense	posamezno	znotraj domen
BGMP	dense	posamezno	znotraj domen
DVMRP	dense	posamezno	znotraj in med domenami

34

34

---

---

---

---

---

---

---

---

---

---

## PIM-SM (Protocol Independent Multicast - Sparse Mode)

- PIM-DM: dense-mode, posamezno drevo
- PIM-SM: sparse-mode, skupno drevo, včasih posamezno
  - izziv: preberi RFC 4601 in ga preuči
- protokola PIM-SM in PIM-DM sta primerna za usmerjevalnike, ki že izvajajo unicast usmerjanje. Sta neodvisna od unicast protokola
- sporočila uporabljajo IP mrežni protokol s številko protokola protokola 103
- sporočila med usmerjevalniki so unicast ali multicast na naslov 224.0.0.13 (vsi PIM usmerjevalniki)

35

35

---

---

---

---

---

---

---

---

---

---

## Delovanje PIM-SM

**vzpostavitev arhitekture**

- kandidati zagonski (bootstrap) usmerjevalniki (c-BSR) oznanijo svojo prisotnost (tip sporočila BOOTSTRAP) in izberejo glavni zagonski usmerjevalnik BSR
- kandidati osrednji (rendezvous) usmerjevalniki (c-RP) oznanijo prisotnost BSR usmerjevalniku (tip sporočila CANDIDATE-RP-ADVERTISEMENT)
- BSR izbere dokončni centralni usmerjevalnik (RP) za vsako skupino in jih oznanji s sporočili tipa BOOTSTRAP

**pošiljanje podatkov**

- PIM-SM usmerjevalniki se zaznajo in vzdržujejo komunikacijo s sporočili HELLO
- vmesnik, ki pošilja podatke na skupinski naslov, razpošlje datagram na lokalni segment mreže
- izbrani usmerjevalnik na mreži (designated router) enkapsulira datagram v tip sporočila REGISTER in ga pošlje RP
- RP dekapulira datagram in ga razpošlje po razpošiljevalnem drevesu

**vzdrževanje naročnine**

- kadar RP zazna, da v skupini ni več prejemnikov, pošlje sporočilo REGISTER-STOP vsem izbranim usmerjevalnikom
- kadar se novi uporabnik želi pridružiti skupini, pošlje sporočilo JOIN/PRUNE s seznamom vseh želenih skupin in dovoljenih prejemnikov

36

36

---

---

---

---

---

---

---

---

---

---

### Oblika paketa - vsebina glave

- Glava dolga 32 bitov
- version = 2
- tip:

vrednost	pomen
0	hello
1	register
2	register stop
3	join/prune
4	bootstrap
5	assert
6	candidate-rp-advertisement

37

---

---

---

---

---

---

---

---

---

---

### Oblika paketa PIM-SM - paket HELLO

- namenjen vzdrževanju povezav med usmerjevalniki
- v primeru, da se izbrani usmerjevalnik za pošiljanje razpošiljevalnega prometa ne odzove, se izbere drugi
- paket vsebuje množico TLV vrednosti, kot so npr. potek časa, v katerem je pričakovan odgovor

38

---

---

---

---

---

---

---

---

---

---

### Oblika paketa PIM-SM - paket REGISTER in REGISTER-STOP

- sporočilo REGISTER nosi vsebino razpošiljevalnega sporočila do osrednjega usmerjevalnika (*unicast*)
  - B (*border router*) - sporočilo prišlo usm., ki je neposredno povezan z vmesnikom,
  - N (*null*) - paket je prazen, za vzpostavitev povezanosti
- sporočilo REGISTER STOP pošlje osrednji usmerjevalnik izbranemu usmerjevalniku, z njim sporoči naj ne pošilja sporočil (prejemnikov ni / sporočila dobiva že od drugje)

39

---

---

---

---

---

---

---

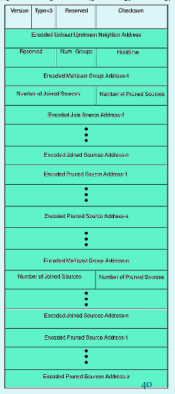
---

---

---

### Oblika paketa PIM-SM - JOIN/PRUNE

- omogoča prejemniku, da se prijavi/odjavi od prejetanja razpošiljevalnega prometa
- PIM-SM ima *Number of Pruned sources* enak 0 (ker uporablja skupno drevo)
- Polja za prijavo/odjavo:
  - *Encoded Join Source Address*
  - *Encoded Pruned Source Address*



40

---

---

---

---

---

---

---

---

---

---

---

---

### Drugi usmerjevalni protokoli

- MOSPF
  - *Multicast OSPF*
  - ima dodano le posebno obliko paketa, ki oznanja razpošiljevalni promet
    - *izziv: poišči RFC dokumente, ki opisujejo MOSPF in jih preberi!*
- DVMRP
  - *Distance Vector Multicast Routing Protocol*
  - prenaša se ga v IGMP paketih (tip 13)
    - *izziv: preberi RFC 1075 in prouči delovanje tega protokola*

41

---

---

---

---

---

---

---

---

---

---

---

---

### MBONE

- povezava omrežij, zmožnih razpošiljevalnega prometa
  - sprva znotraj interneta, tvorile so ga delovne postaje z navideznimi povezavami
    - *izziv: preberi RFC 2715*
  - 1995: MBONE vsebuje 901 usmerjevalnikov (uporablja se DVMRP) in je v 20 državah
  - 1999: 4178 usmerjevalnikov, uporablja se vse bolj RTP, ponudniki storitev postajajo preobremenjeni
  - IETF ustanovi delovno skupino MBONED z nalogo, da vzpostavi multicast usmerjanje preko celega interneta (razvoj protokola *MSDP: Multicast Source Discovery Protocol*)
    - *izziv: preberi RFC 1112, kaj je to Any Source Multicast arhitektura (ASM)?*

42

---

---

---

---

---

---

---

---

---


---

---

---

Naslednjič gremo naprej!

- overovljenje, avtorizacija in beleženje - AAA!



43

---

---

---

---

---

---

---