Višja strokovna šola Velenje

Informatika Murska Sobota

Računalniške komunikacije in omrežja II

ARHITEKTURA TCP/IP

II. del

2. predavanje

- Predavatelj: dr. Iztok Fister
- E-pošta: iztok.fister@mdi2.net
- Gradivo na naslovu: ftp.scv.si

Murska Sobota, november 2009

Vsebina

- **Protokol IP**
  - **IPv6**
  - **ICMP in IGMP**
  - **ARP in RARP**
  - **Vrata in kanali**
- **Protokol UDP**
- **Protokol TCP**

IPv6 1/6

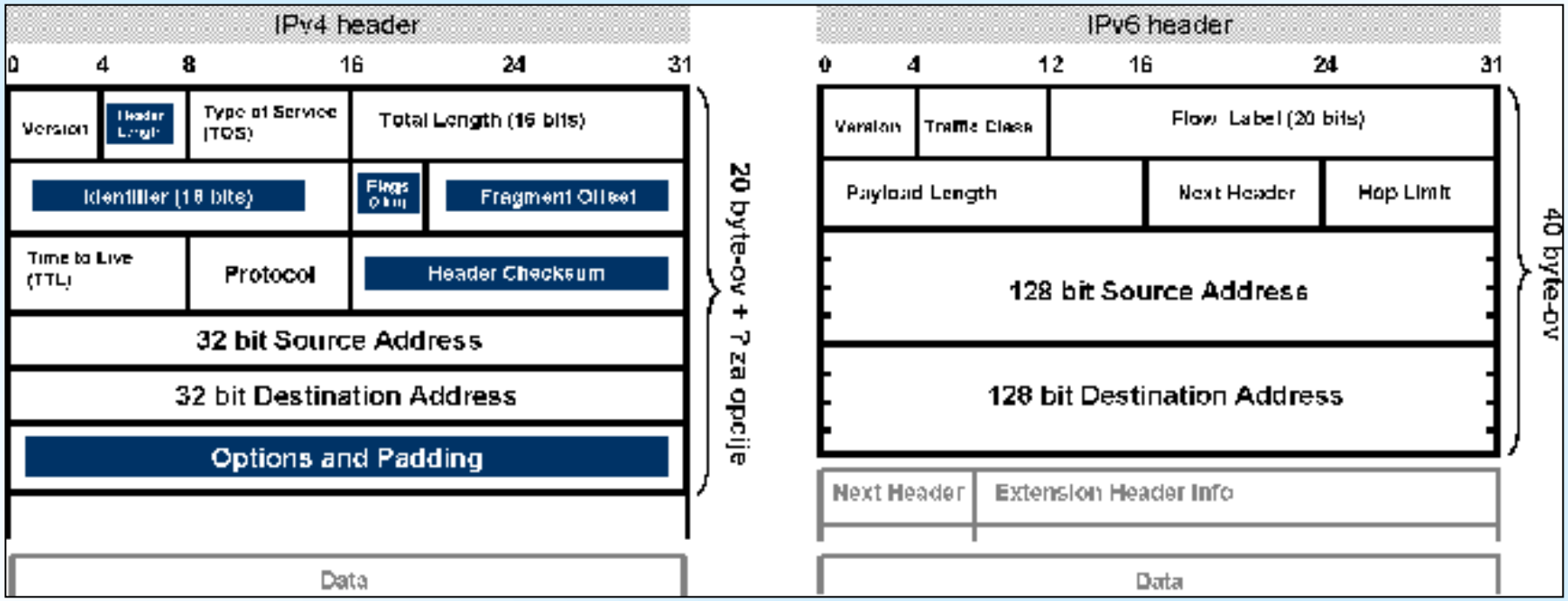
- **Vzroki za nastanek IPv6:**
  - **naslovni prostor IPv4 (4.10^9 gostiteljev) postaja pretesen,**
  - **razvoj mobilnih naprav, IP-telefonije, IP-televizije, ipd. povečuje število naslovov,**
  - **zagotavljanje kakovosti storitev (QoS),**
  - **povečanje omrežne varnosti.**
- **Prvič opisan v dokumentih leta 1995**
- **Postal protokol nove generacije**

IPv6 2/6

- **Značilnosti IPv6:**
  - **Neomejen naslovni prostor ($7{,}9.10^{28}$)**
  - **32-bitne (4 bajtov) naslove IPv4 razširimo na 128-bitne (16 bajtov)**
  - **Z IPv6 pokrivamo nekaj tisoč naslovov IP na m^2 zemeljske površine**
  - **Naslove IPv6 pišemo heksadecimalno**
  - **16 bitne vrednosti ločimo z dvopičji**
  - **Zaporedne ničle v zapisu opustimo**
  - **Primer: 2001:798:110:2002:100::1**

IPv6 3/6

- **Primerjava glave datagrama IPv4 in paketa IPv6**



- **Število polj IPv4 zmanjšano s 13 na 8**
- **Učinkovitejša in hitrejša obdelava usm.**

IPv6 4/6

- **Polja glave IPv6 iz IPv4:**
  - **ToS (IPv4) -> tip prometa (angl. Traffic Class) (IPv6): kakovost storitev,**
  - **TTL (IPv4) -> odštevalnik (angl. Hop Limit).**
- **Novost v IPv6:**
  - **oznaka pretoka (angl. Flow Label): racionalno procesiranje spletnih paketov.**
- **Prednosti IPv6:**
  - **samodejna konfiguracija in mobilnost,**
  - **enostaven prehod iz IPv4 v IPv6.**

IPv6 5/6

- **Lastnosti glave IPv6**
  - **Osnovna glava paketa IPv6 je fiksna in dolga 40 bajtov**
  - **Vsebuje najnujnejše informacije za posredovanje paketa prek omrežja**
  - **Osnovni glavi lahko sledi več zaglavij (angl. Extension Headers)**
  - **Vsebina zaglavij je namenjena ciljnemu gostitelju (poenostavi delo usmerjanja)**
  - **Izjema je zaglavje opcij (angl. Hop-by-Hop Options), ki vpliva na delo usmer.**

IPv6 6/6

- **Razširitev osnovne glave z zaglavji omogoča:**
  - **naprednejše usmerjanje prometa,**
  - **dodatne možnosti naslavljanja na ciljnih gostiteljih,**
  - **podporo mobilnosti,**
  - **varnostne mehanizme,**
  - **ohranjanje preproste osnovne zgradbe protokola.**

ICMP 1/4

- **Internet Control Message Protocol (ICMP) uporabljamo za:**
  - **sporočanje omrežnih napak,**
  - **sporočanje omrežnih preobremenitev,**
  - **pomoč pri odpravljanju napak (angl. troubleshoting),**
  - **obveščanje o zakasnitvah.**

ICMP 2/4

- **Lastnosti ICMP:**
  - **uporablja IP, t.j. sporočila ICMP so ovita v IP datagrame.**
  - **namenjen sporočanju napak, ne prinaša dodatne zanesljivosti.**
  - **sporoča napake o vsakem datagramu, razen sporočil ICMP (problem rekurzije).**
  - **pri fragmentiranih IP datagramih se pošlje napaka za fragment 0.**
  - **sporočila ICMP se nikoli ne pošiljajo kot odgovor na Broadcast ali Multicast.**

ICMP 3/4

- **ICMP aplikacija ping:**
  - **uporablja sporočili ICMP Echo in Echo Replay,**
  - **ugotavlja dosegljivost gostitelja na omrežju.**

```
C:\>ping 192.168.225.101
Pinging 192.168.225.101 with 32 bytes of data:
Reply from 192.168.225.101: bytes=32 time=1ms TTL=128
Reply from 192.168.225.101: bytes=32 time<1ms TTL=128
Reply from 192.168.225.101: bytes=32 time<1ms TTL=128
Reply from 192.168.225.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.225.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

ICMP 4/4

- **ICMP aplikacija traceroute**
  - **uporaben pri odpravljanju napak.**

```
C:\ >tracert www.google.com

Tracing route to www.l.google.com [64.233.183.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.225.1
  2    30 ms    30 ms    30 ms  192.168.10.5
  3    30 ms    30 ms    30 ms  193.189.186.102
  4    30 ms    30 ms    30 ms  193.77.12.97
  5    40 ms    40 ms    40 ms  kklag1-176-57.net.uta.at [212.152.176.57]
  6    92 ms   101 ms    91 ms  vie3-core.pos0-0.swip.net [130.244.205.49]
  7    92 ms    92 ms    92 ms  fra2-core.pos12-0.swip.net [130.244.193.154]
  8    93 ms    83 ms    83 ms  64.233.183.99

Trace complete.
```

IGMP 1/2

- **Internet Group Management Protocol (IGMP)**
  - **integralni del plasti IP,**
  - **dopušča ali prepoveduje gostiteljem v omrežju odzivati se na IP Multicating,**
  - **usmerjevalnikom omogoča preverjanje, ali v določenem omrežju obstaja kakšen gostitelj, ki odgovarja na Multicast,**
  - **članstvo v Multicast grupi je dinamično,**
  - **gostitelj se pridruži Multicast grupi s pošiljanjem sporočil IGMP.**

IGMP 2/2

– **Multicast naslovi**

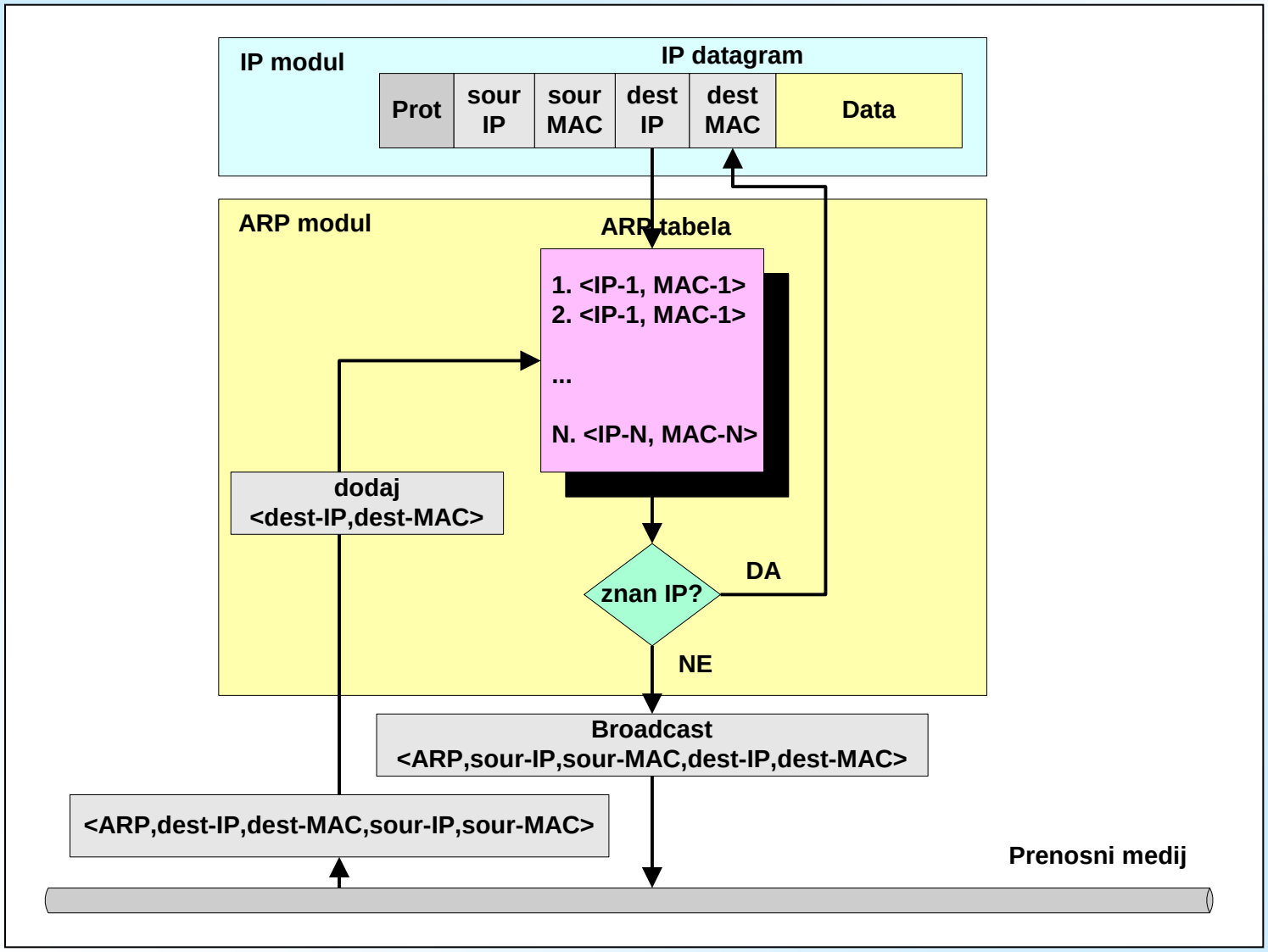
IP multicast naslov	Opis
224.0.0.0	Osnovni naslov (rezerviran)
224.0.0.1	Vsi gostitelji multicast grupe.
224.0.0.2	Vsi usmerjevalniki multicast grupe.
224.0.0.5	OSPF usmerjevalniki.
224.0.0.6	OSPF DR usmerjevalniki.
224.0.0.9	RIP-2 usmerjevalniki.
224.0.1.24	WINS-strežniki.

ARP 1/5

- **Address Resolution Protocol (ARP)**
  - **specifičen standardni protocol,**
  - **konvertira logične IP naslove v fizične omrežne naslove MAC,**
  - **služi IP protokolu za razrešitev logičnih naslovov,**
  - **uporablja translacijsko tabelo,**
  - **če naslova v tabeli ni, modul ARP pošlje v omrežje Broadcast.**

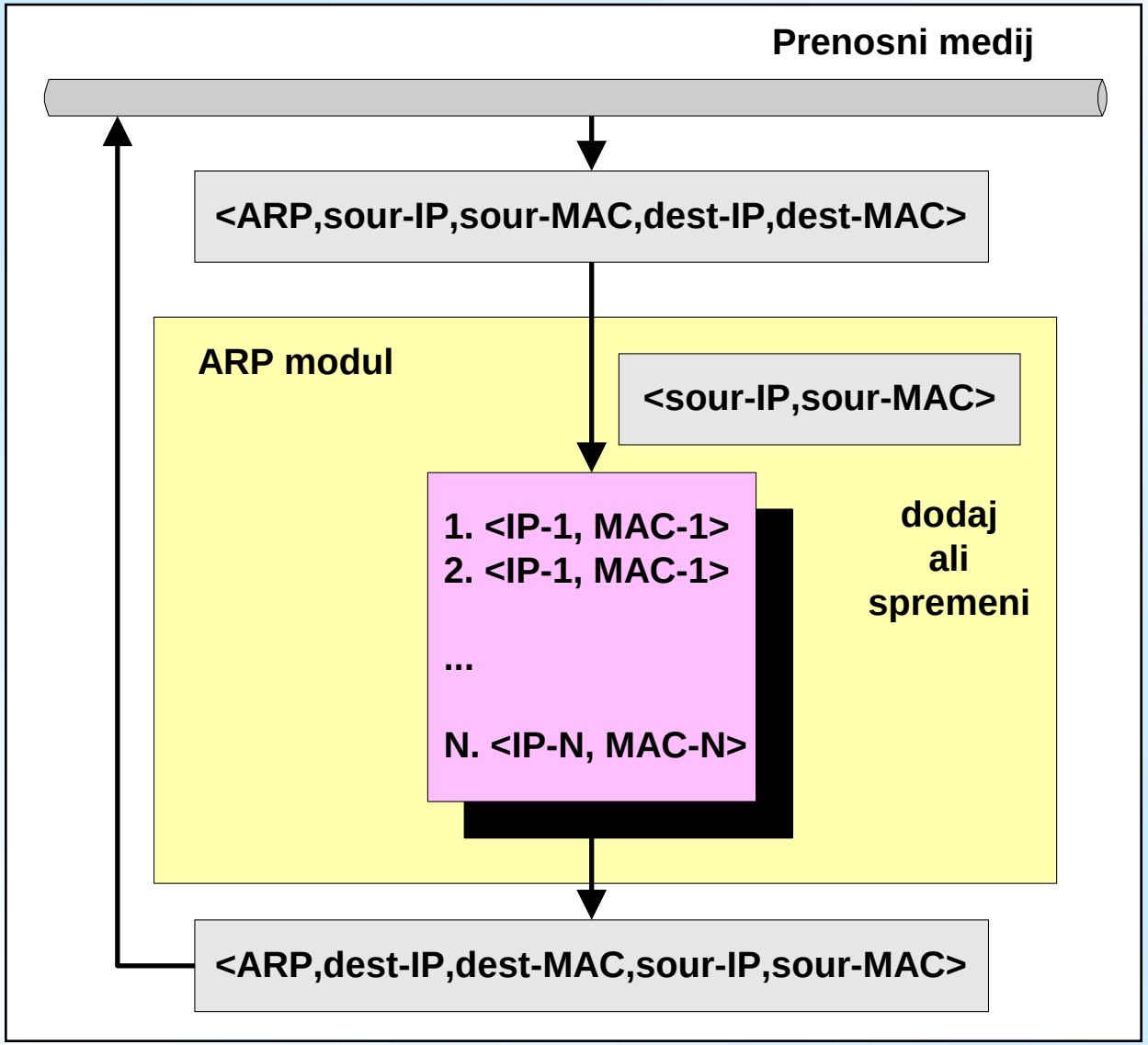
ARP 2/5

- **Generiranje ARP naslovov - pošiljatelj**



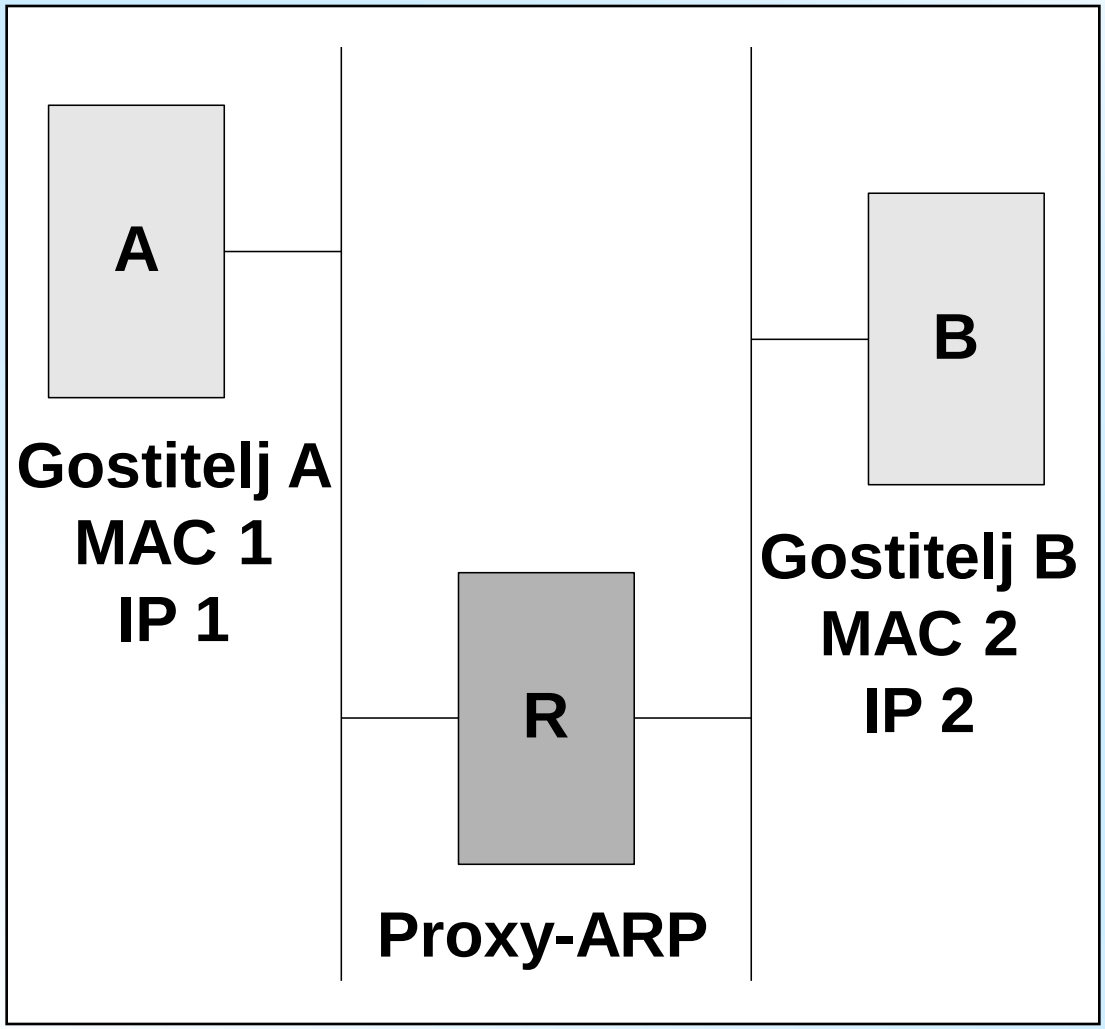
ARP 3/5

- **Generiranje ARP naslovov - naslovnik**



ARP 4/5

- **Proxy-ARP koncept**



ARP 5/5

- Lastnosti transparentnega omrežja:
  - navadni gostitelji ne poznajo pojma podomrežja in uporabljajo standardni IP usmerjevalni program.
  - usmerjevalniki uporabljajo:
    - usmerjevalni algoritem za podomrežja,
    - modificirani modul ARP, ki zna odgovarjati na podomrežne zahteve drugih gostiteljev.

RARP

- Reverse Address Resolution Protocol (RARP)
  - uporabljajo delovne postaje brez diskov (NC-ji), ki se nalagajo iz mreže in svojega IP naslova ne poznajo,
  - iz MAC naslova dodeli IP naslov,
  - deluje kot omrežni strežnik,
  - za delovanje potrebuje predkonfigurirano podatkovno bazo o preslikavah MAC naslovov v IP naslove.

Vrata in vtičnice 1/4

- **Vrata (ports) in vtičnice (sockets)**
  - **omogočajo, da enolično identificiramo povezave, programe in gostitelje neodvisno od PID. Lastnosti PID:**
    - **PID (process ID) – aplikacijski proces, ki ga sistem prepozna po številki. Ta se spremeni, ko proces znova zaženemo.**
    - **PID med različnimi OS ni enolično določen.**
    - **Strežniški proces lahko komunicira z več odjemalci hkrati, t.j. tudi identifikacija povezave ni unikatna.**

Vrata in vtičnice 2/4

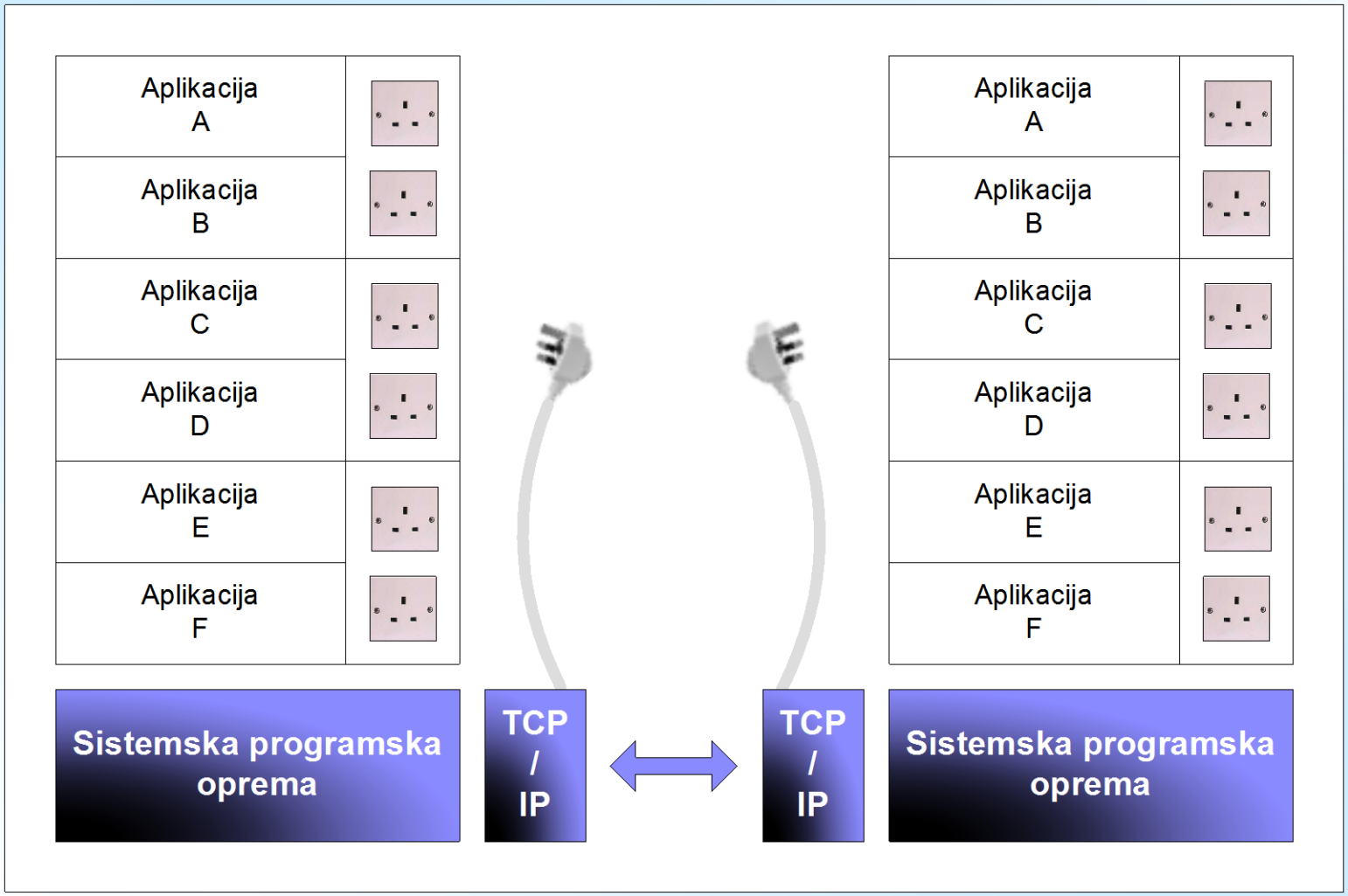
- **Vrata (ports)**
  - **vsak proces se predstavi protokolu TCP/IP s številko vrat.**
  - **vrata so 16-bitno število, ki ga protokol gostitelj-gostitelj uporablja za identifikacijo naslovnika sporočila (aplikacija ali višje-nivojski protokol).**
  - **tipi:**
    - **splošno znana: pripadajo standardnim strežnikom (Telnet, FTP…), določene preko IANA (Internet Assigned Names Authority).**
    - **kratkotrajna: uporabljajo uporabniški programi, določene strežniško.**

Vrata in vtičnice 3/4

- **Vtičnice (sockets) 1/2**
  - **eden izmed TCP/IP API, ki omogoča aplikaciji dostop do komunikacijskih protokolov,**
  - **posebne vrste datotek, ki jih uporablja proces pri zahtevanju omrežnih storitev od OS (dvosmerna, znakovna povezava),**
  - **definicije:**
    - **naslov kanala:** ⟨prot,l_nasl,l_proc⟩
    - **pogovor je komunikacijska povezava med dvema procesoma.**
    - **zveza:** ⟨prot,l_nasl,l_proc,o_nasl,o_proc⟩
    - **pol-zveza:** ⟨prot,l_nasl,l_proc⟩ **ali** ⟨prot,o_nasl,o_proc⟩
    - **vtičnica: je končna točka komunikacije, ki se lahko naziva in naslavlja v omrežju.**

Vrata in vtičnice 4/4

- **Vtičnice (sockets) 2/2**

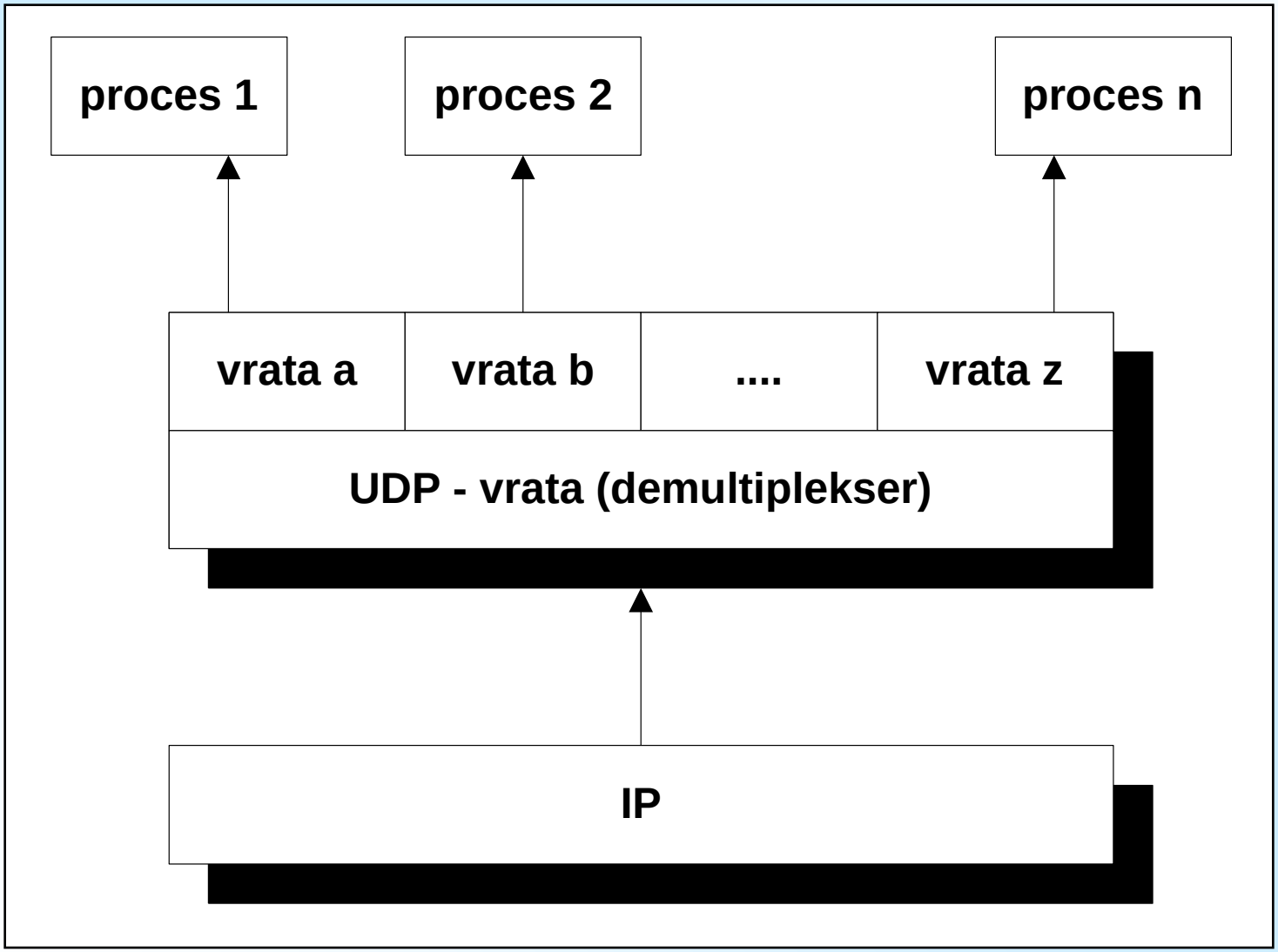


Protokol UDP 1/3

- **Značilnosti protokola UDP:**
  - **aplikacijski vmesnik do protokola IP.**
  - **nezanesljiv, brez popravljanja napak in nadzora pretoka.**
  - **v vlogi multiplekser/demultiplekser za pošiljanje in sprejemanje datagramov skozi določena vrata.**
  - **plast UDP je zelo tanka, kar pomeni majhne stroške.**
  - **aplikacije za identifikacijo ponora potrebujejo identifikacijo procesa in ne sistema kot celote, kar omogoča uporaba vrat.**

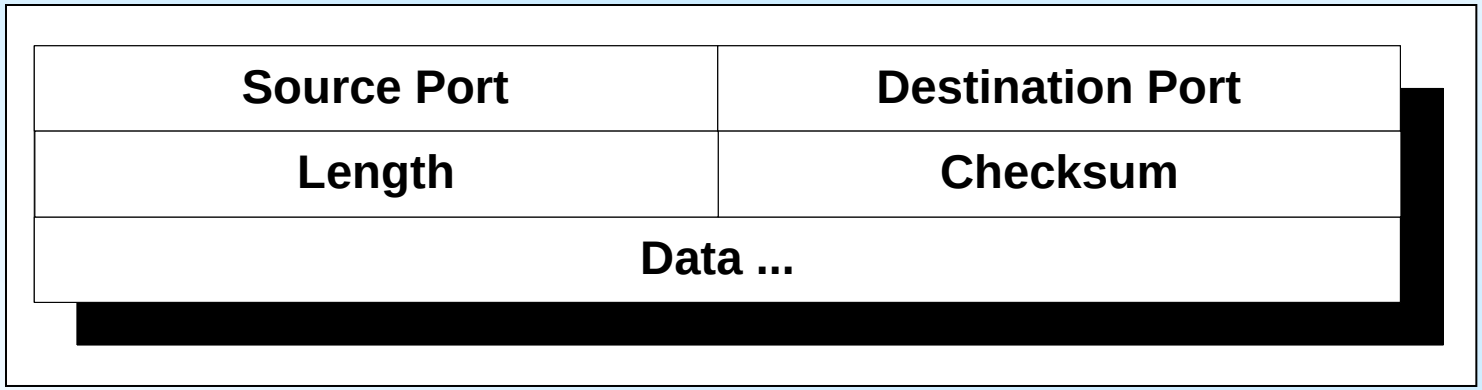
Protokol UDP 2/3

– Princip delovanja UDP



Protokol UDP 3/3

- Format UDP datagrama
  - UDP datagram ovijemo v IP datagram,
  - IP datagram > 576 bajtov lahko fragmentiramo,



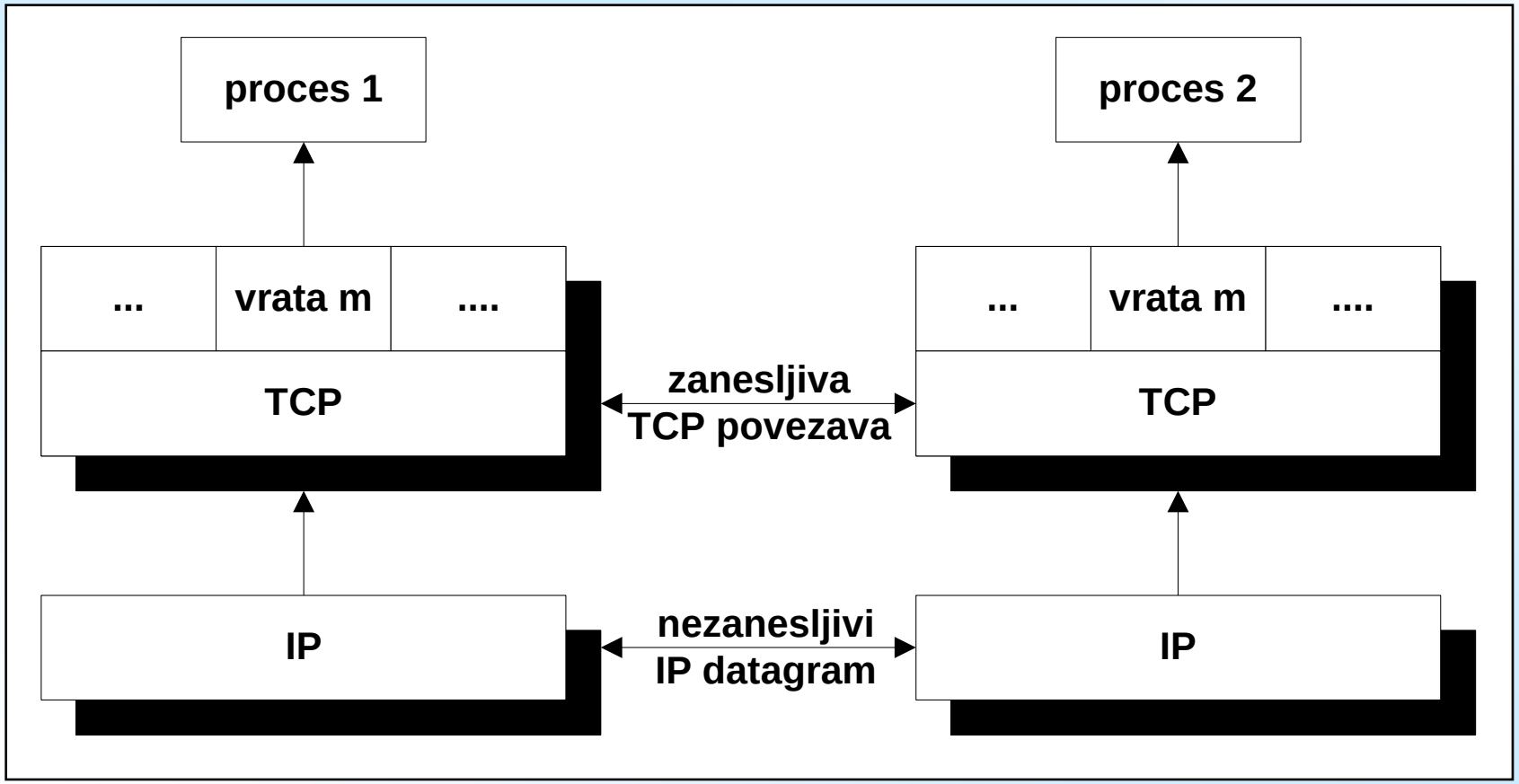
  - UDP datagram ima 16-bajtno glavo.
- UDP aplikacije: TFTP, DNS, RPC, SNMP, LDAP

Protokol TCP 1/13

- **Značilnosti TCP**
  - **omogoča odpravljanje napak, nadzor pretoka in zanesljivost,**
  - **povezavno orientiran protokol, ki omogoča povezano storitev med pari procesov,**
  - **dva procesa komunicirata med seboj s TCP API, t.j. z vrati in vtičnicami (IPC),**
  - **večina uporabniških aplikacijskih protokolov (Telnet, FTP) uporablja TCP.**

Protokol TCP 2/13

– TCP povezava med procesoma (IPC)



Protokol TCP 3/13

- **Lastnosti TCP (1/2)**
  - **Znakovni prenos podatkov: s stališča aplikacije TCP prenaša zvezen tok (stream) bajtov skozi omrežje (funkcija *push*).**
  - **Zanesljivost: TCP pošilja bajte v blokih in od ponornega TCP pričakuje potrditev sprejema (ACK).**
  - **Nadzor pretoka: ponorni TCP pri pošiljanju ACK izvornemu gostitelju javi število bajtov, ki jih lahko še sprejme, preden pride do prekoračitve njegovega internega pomnilnika - princip drsnega okna.**

Protokol TCP 4/13

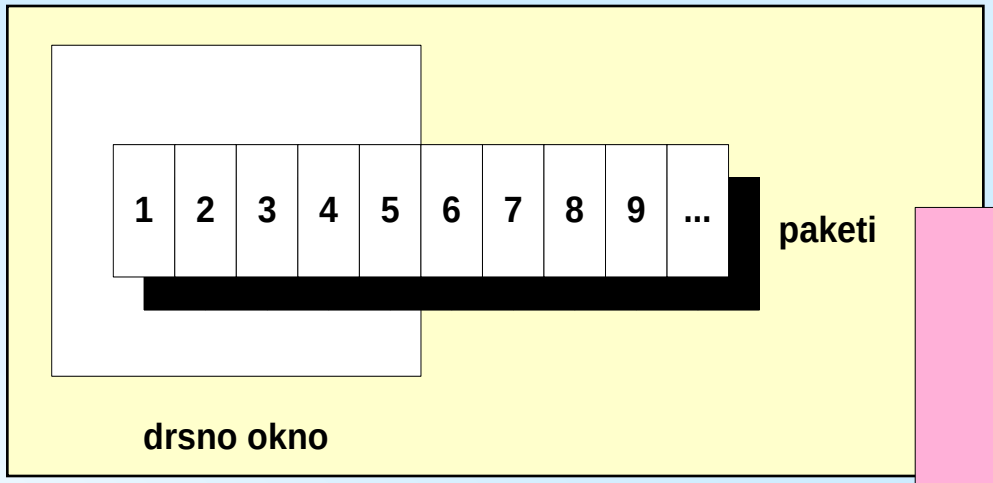
- **Lastnosti TCP (2/2):**
  - **Multipleksiranje: izvršeno z uporabo vrat podobno kot pri UDP.**
  - **Logične povezave: je kombinacija statusnih informacij vtičnic, zaporedno številko in velikost oken. Vsaka povezava je enolično določena s paroma vtičnic uporabljenih v procesih pošiljanja in sprejemanja.**
  - **Dvosmerne povezave: TCP omogoča hkraten prenos podatkov v obe smeri.**

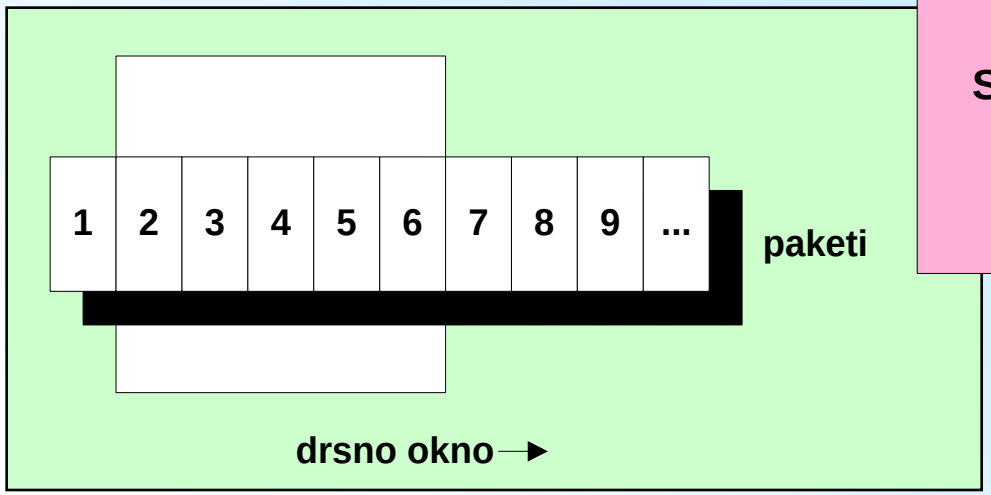
Protokol TCP 5/13

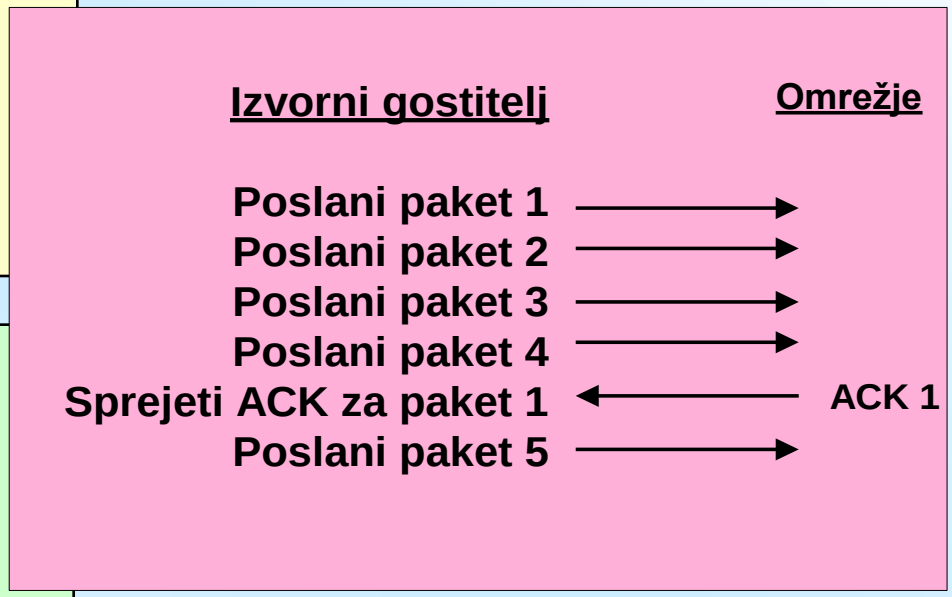
- **Princip drsnega okna**
  - **vsi paketi za prenos tvorijo drsno okno,**
  - **izvor pošlje vse pakete v drsnem oknu ne da bi sprejel potrditev (ACK), vendar za vsakega posebej starta timeout timer,**
  - **ponor mora potrditi vsak sprejeti paket in ga označi z zaporedno številko zadnjega uspešno sprejetega paketa.**
  - **izvor pomakne drsno okno ob vsaki potrditvi ACK.**

Protokol TCP 6/13

– Primer drsnega okna 1/2







Protokol TCP 7/13

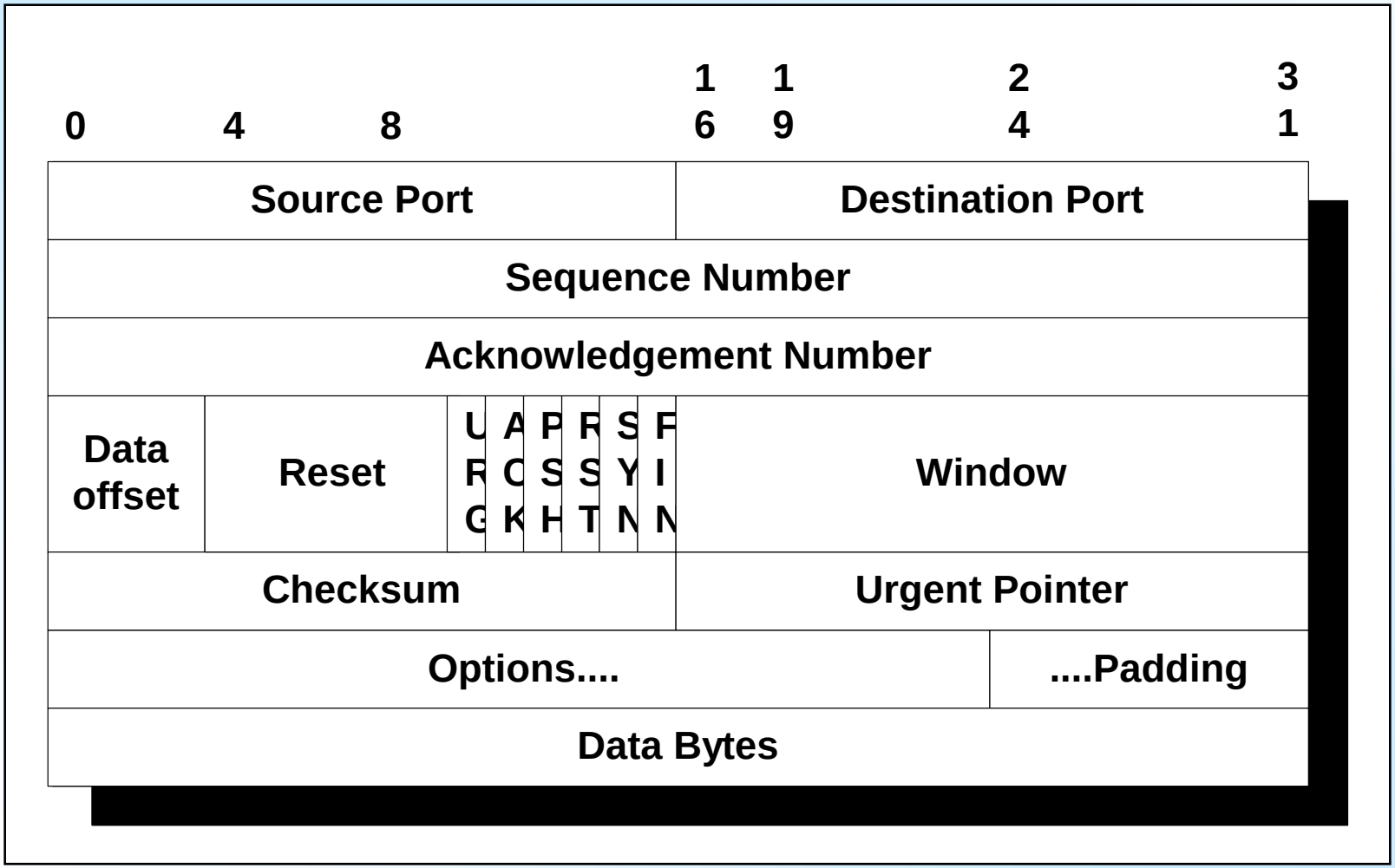
- **Primer drsnega okna 2/2**
  - **po prejemu ACK 1 lahko izvor pošlje paket 6. Nastopita dve možnosti:**
    - **paket 2 izgubimo: izvor ne dobi ACK 2 in drsno okno ostane na poziciji 1,**
    - **paket 2 prispe, izgubimo pa ACK 2: izvor sprejme ACK 3 in pomakne drsno okno.**

Protokol TCP 8/13

- Drsno okno zagotavlja:
  - zanesljiv prenos,
  - boljši izkoristek prenosnega pasu omrežja,
  - nadzor pretoka, ker lahko ponorni gostitelj počaka s potrditvijo glede na velikost prostega pomnilnika in velikost drsnega okna.
- V TCP drsno okno realiziramo na bajtni in ne na paketni osnovi.

Protokol TCP 9/13

– **Format TCP segmenta**



Protokol TCP 10/13

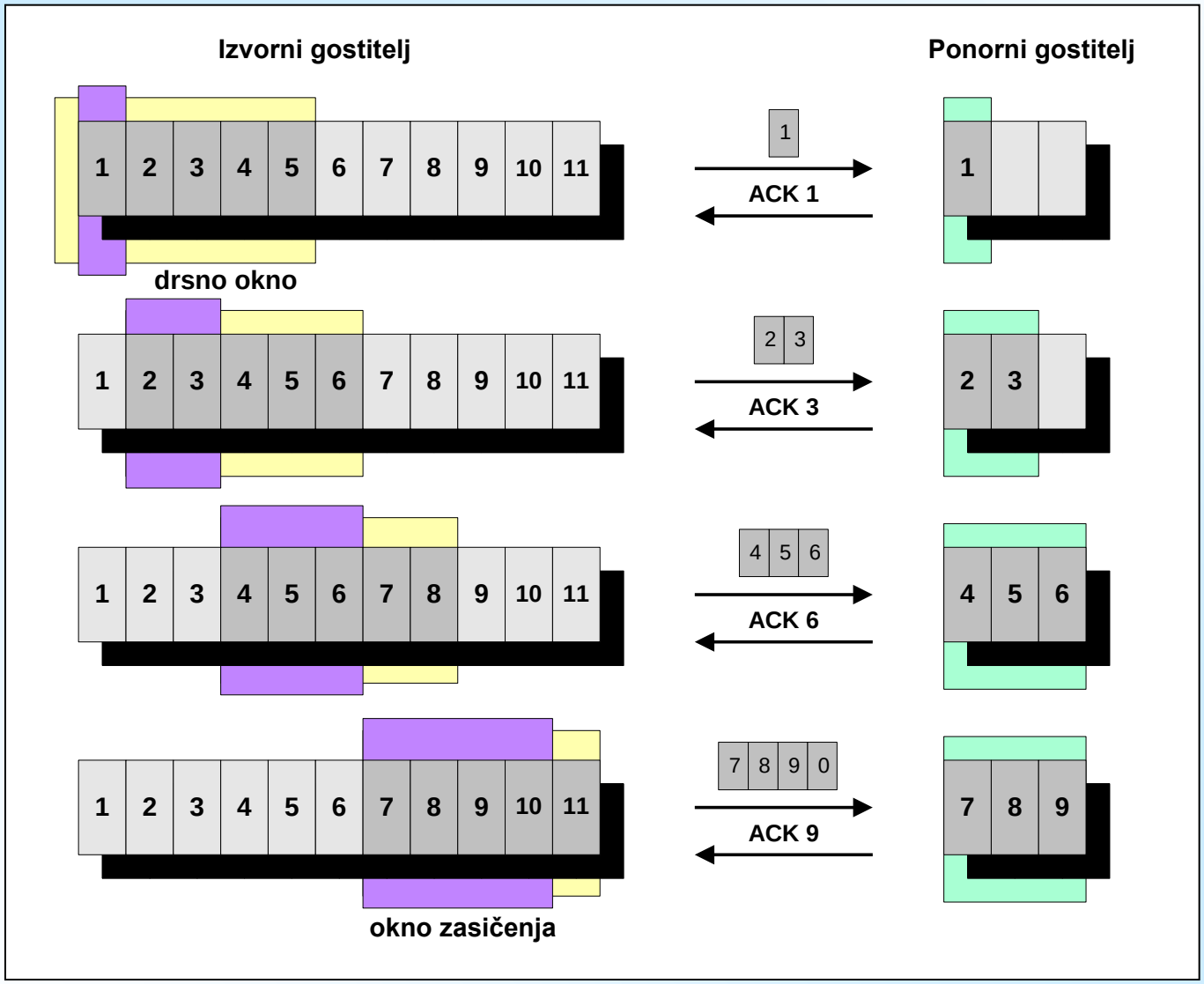
- Opis pomembnejših polj
  - **Sequence Number**: zaporedna številka prvega podatkovnega bajta v tem segmentu.
  - **Acknowledgement number**: vrednost naslednje zaporedne številke, ki jo ponor pričakuje. Zahteva nadzorni bit ACK.
  - **Window**: določa število podatkovnih bajtov, ki jih lahko ponor še sprejme.
  - **Checksum**: 16-bitni 1'komplement vsote vseh 16-bitnih besed v psevdo-IP-glavi.

Protokol TCP 11/13

- **TCP nadzor zasičenja**
  - **izvornemu gostitelju preprečuje, da bi zasedel vse kapacitete omrežja.**
  - **algoritmi za nadzor zasičenja:**
    - **počasni zagon (angl. slow start),**
    - **izogibanje zasičenju (angl. congestion avoidance),**
    - **hitra ponovitev (angl. fast retransmit),**
    - **hitra obnovitev (angl. fast recovery)**

Protokol TCP 12/13

– Primer nadzora nasičenja



Protokol TCP 13/13

- **Počasni zagon**
  - **nadzor hitrosti pošiljanja paketov izvornega gostitelja, t.j. izvor odda v omrežje toliko paketov, koliko jih lahko ponor sprejme.**
  - **TCP doda izvoru okno zasičenja.**
  - **vsak ACK povečuje okno zasičenja za 1.**
  - **velikost drsnega okna nadzoruje ponorni gostitelj in je odvisna od velikosti pomn.**
  - **velikost okna zasičenja nadzira izvorni gostitelj in je odvisna od prenosne kapacitete omrežja.**

Primer 1/3

- **Naslov IP gostitelja je 202.88.48.97 njegova maska 255.255.255.224. Iz navedenih podatkov ugotovite:**
  - **V kateri razred naslovov IP spada naslov IP gostitelja?**
  - **Številko omrežja gostitelja (netID).**
  - **Številko njegovega podomrežja (subnetID).**
  - **Številko gostitelja v omrežju (hostID).**
  - **Koliko podomrežij podpira omenjena maska podomrežja?**
  - **Koliko gostiteljev lahko uporabimo v omenjenem podomrežju?**

Primer 2/3

- **Naslov IP gostitelja je 193.189.186.100 njegova maska 255.255.255.192. Iz navedenih podatkov ugotovite:**
  - **V kateri razred naslovov IP spada naslov IP gostitelja?**
  - **Številko omrežja gostitelja (netID).**
  - **Številko njegovega podomrežja (subnetID).**
  - **Številko gostitelja v omrežju (hostID).**
  - **Koliko podomrežij podpira omenjena maska podomrežja?**
  - **Koliko gostiteljev lahko uporabimo v omenjenem podomrežju?**

Primer 3/3

- **Naslov IP gostitelja je 86.61.67.112 njegova maska 255.252.0.0. Iz navedenih podatkov ugotovite:**
  - **V kateri razred naslovov IP spada naslov IP gostitelja?**
  - **Številko omrežja gostitelja (netID).**
  - **Številko njegovega podomrežja (subnetID).**
  - **Številko gostitelja v omrežju (hostID).**
  - **Koliko podomrežij podpira omenjena maska podomrežja?**
- **Koliko gostiteljev lahko uporabimo v omenjenem podomrežju?**