Počítačové siete
TCP/IP

Sieťová vrstva v TCP/IP

- protokol IP – connection-less, unreliable
- prenos IP paketov medzi ľubovoľnými dvoma počítačmi (zariadeniami)
- fragmentácia paketov
- adresy – 4B čísla (1.2.3.4)
- časť adresy určuje sieť, druhá časť konkrétny uzol (host – počítač, zariadenie)

Módy adresácie

- unicast
  - jeden cieľ
- multicast
  - skupina
- broadcast
  - všetci v sieti
- anycast
  - jeden z množiny

Triedy IP adries

- 1.x.x.x – 126.x.x.x – A
  - 7 bitov sieť, 24 bitov host
- 128.x.x.x – 191.x.x.x – B
  - 14 bitov sieť, 16 bitov host
- 192.x.x.x – 223.x.x.x – C
  - 21 bitov sieť, 8 bitov host
- 224.x.x.x – 239.x.x.x – D – multicast
- 240.x.x.x – 255.x.x.x – E – vyhradené

Classless Inter-domain Routing

- zapĺňanie adresného priestoru
- neefektívne prideľovanie A/B/C
- maska
  - určuje, ktoré bity tvoria adresu siete
  - súvislý blok 1, súvislý blok 0
    - 255.255.0.0 = 16 bitov
    - 255.255.255.128 = 25 bitov
    - 255.192.0.0 = 10 bitov

Špeciálne IP adresy

- adresa siete
  - host = 0...0
  - slúži ako identifikátor siete
  - „neznáma“ adresa
- broadcast
  - host = 1...1
  - broadcast pre určenú sieť

Špeciálne IP adresy

- 127.0.0.0/255.0.0.0
  - loopback, lokálny počítač
- 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
  - pre súkromné siete – nesmú sa dostať do Internetu
- 255.255.255.255
  - broadcast na lokálnej sieti
- 0.0.0.0
  - „neznáma“ adresa (napr. zdroj pri BOOTP/DHCP)

Príklady IP adries

- 158.195.18.0/255.255.255.0 (24)
  - adresy 158.195.18.1 – 158.195.18.254
  - broadcast: 158.195.18.255
- 158.195.16.0/255.255.254.0 (23)
  - adresy 158.195.16.1 – 158.195.17.254
  - broadcast: 158.195.17.255
- 158.195.22.0/255.255.255.128 (25)
  - adresy 158.195.22.1 – 158.195.22.126
  - broadcast: 158.195.22.127

IP paket

- hlavička (20 až 60 B)
  - adresa odosielateľa a cieľa
  - dĺžka paketu, transportný protokol
  - time to live, fragmentačné údaje
  - kontrolný súčet hlavičky
- max. veľkosť teoreticky 65536 B
- každé IP zariadenie musí byť schopné spracovať aspoň 576 B IP paket
- umožňuje fragmentáciu paketov

Routovanie IP

- router – počítač alebo špeciálny HW s aspoň dvoma sieťovými interfejsmi/linkami
  - pre každý sieťový interfejs
    - IP adresa
    - maska siete
- routovacia tabuľka
  - adresa, maska, ďalší router, sieťový interfejs/linka
  - vyberie sa vždy najšpecifickejšia položka

Príklad routovacej tabuľky

- IP: 158.195.18.222, maska: 255.255.255.0
  - 158.195.18.0/255.255.255.0 - eth0
  - 127.0.0.0/255.0.0.0 - lo
  - 0.0.0.0/0.0.0.0 158.195.18.209 eth0
- Router:
  - IP1:158.195.18.209, maska: 255.255.255.0
  - IP2: 158.195.17.163, maska: 255.255.254.0
    - 158.195.18.0/255.255.255.0 - eth0
    - 158.195.16.0/255.255.254.0 - eth1
    - 127.0.0.0/255.0.0.0 - lo
    - 0.0.0.0/0.0.0.0 158.195.16.208 eth1

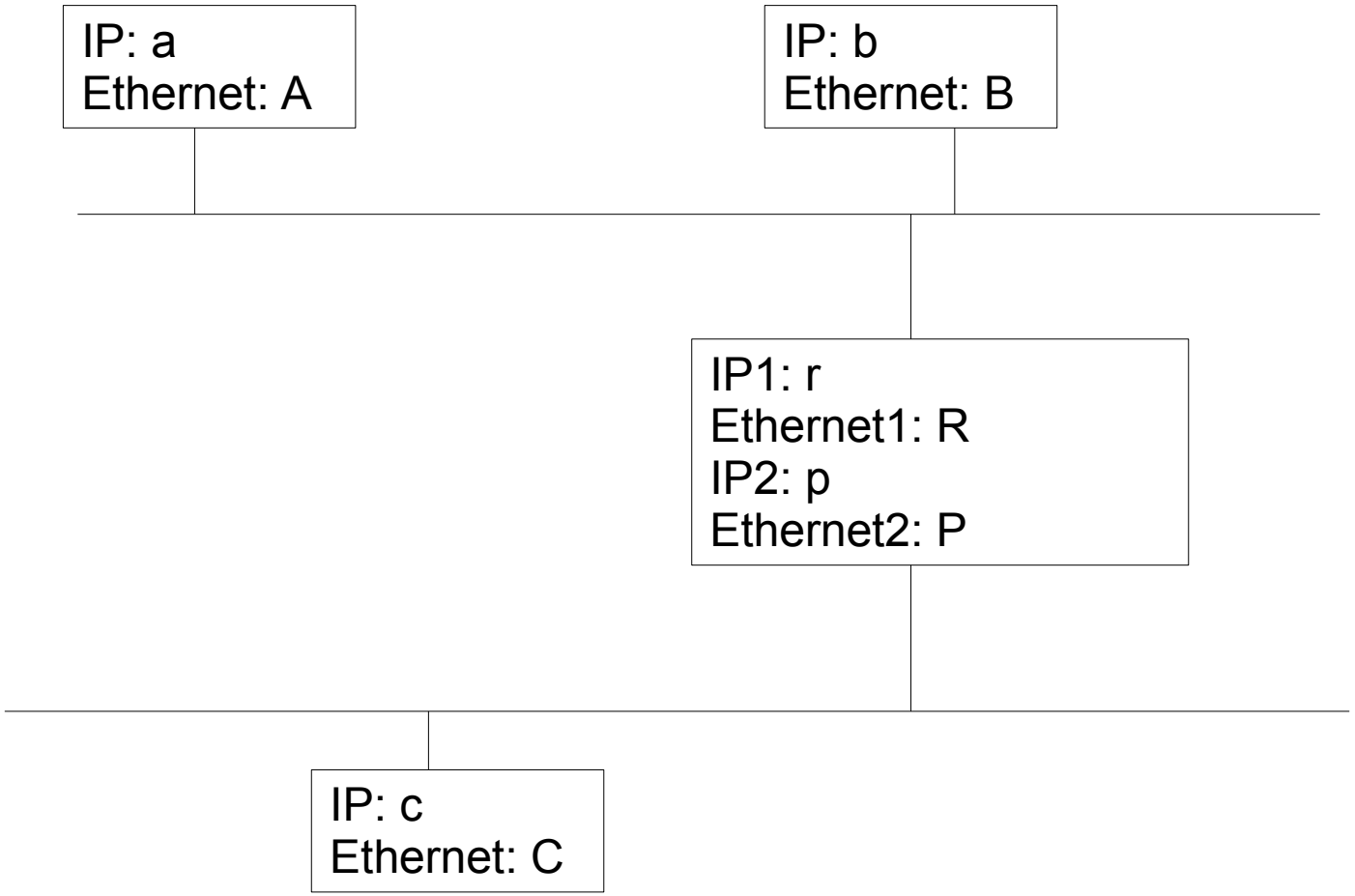
Address Resolution Protocol

- IP pracuje s IP paketmi a IP adresami
- linková vrstva pri broadcast médiu potrebuje často iné adresy (napr. Ethernet)
- ARP rieši preklad IP adresy na fyzickú (linkovú adresu)
  - vyšle broadcast “Kto má IP a.b.c.d?”
  - zariadenie s IP a.b.c.d odpovie:
    “IP a.b.c.d má zariadenie x:y:z:p:q:s”

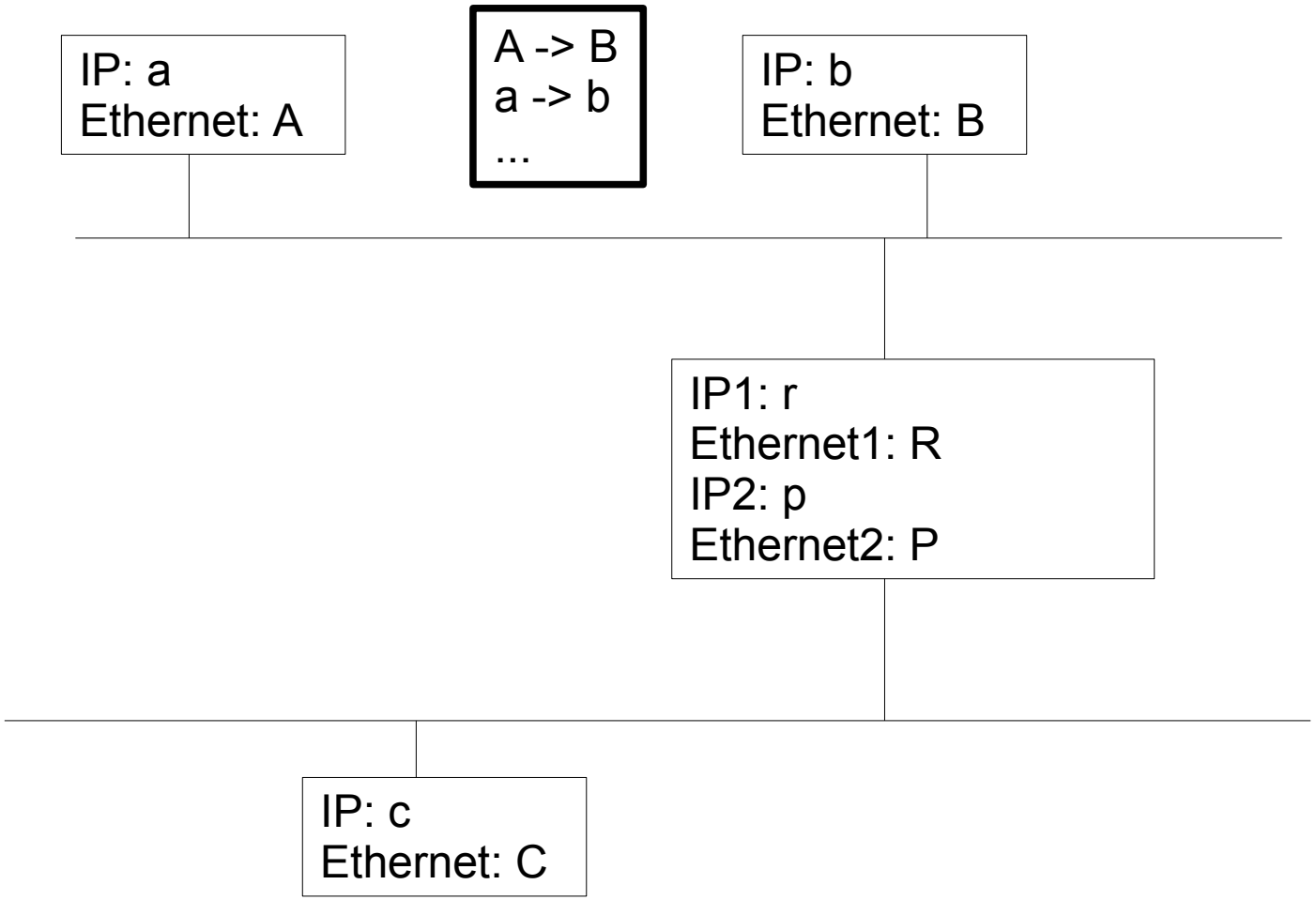
Multicast / broadcast cez Ethernet

- broadcast
  - broadcast do lokálnej siete (255.255.255.255)
  - špecifický broadcast pre vlastnú sieť
  - FF:FF:FF:FF:FF:FF
- multicast
  - 01:00:5E:X:Y:Z
  - X:Y:Z = spodných 23 bitov z IP adresy
  - 01:00:5E:00:00:00 – 01:00:5E:7F:FF:FF

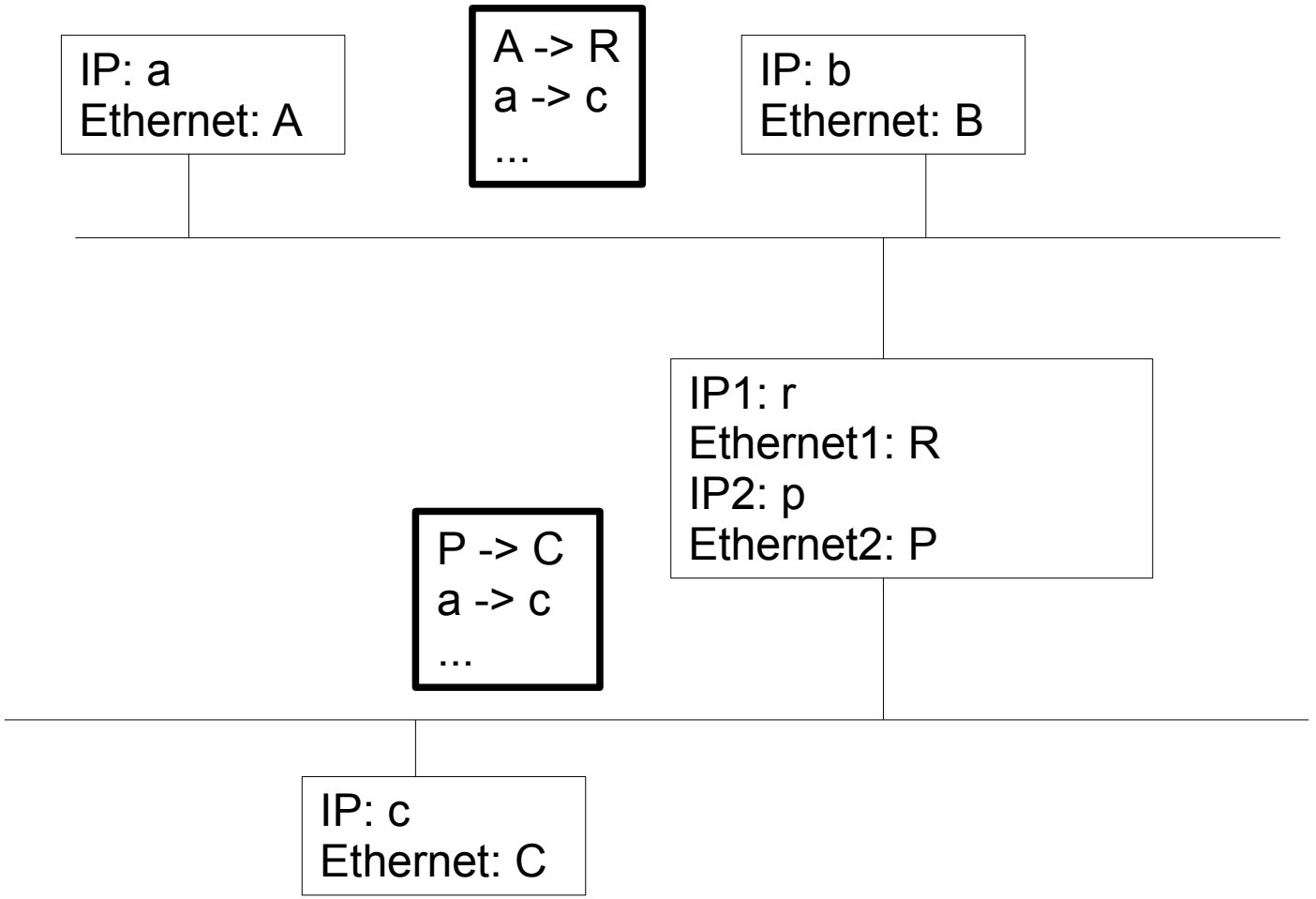
Odoslanie paketu



Odoslanie paketu (susedovi)



Odoslanie paketu (nesusedovi)



Internet Control Message Protocol

- ICMP
- diagnostika a spracovanie chýb
  - ping
  - destination unreachable
  - redirect
  - TTL exceeded
  - ...

Transportná vrstva TCP/IP

- protokoly
  - TCP (Transmission Control Protocol)
    - connection-oriented, reliable
  - UDP (User Datagram Protocol)
    - connection-less, unreliable
- poskytuje služby aplikačnej vrstve
- adresy – navyše číslo portu
  - jednoznačná identifikácia spojenia = IP adresa + port jednej strany a IP adresa + port druhej strany

User Datagram Protocol

- unreliable, connection-less služba
- hlavička
  - zdrojový a cieľový port
  - veľkosť
  - kontrolný súčet (hlavička aj dáta)

Transmission Control Protocol

- reliable, connection-oriented služba
- hlavička
  - zdrojový a cieľový port
  - sekvenčné číslo, potvrdzovacie číslo a veľkosť okna
  - príznaky, kontrolný súčet, ...
- každý paket sa potvrdzuje
- keď nepríde potvrdenie, paket sa pošle znova

Transmission Control Protocol

- vytvorenie spojenia
  - A pošle B paket s príznakom SYN
  - B pošle A paket s príznakmi SYN a ACK
  - A pošle B paket s príznakom ACK
- ukončenie spojenia
  - A pošle B paket s príznakmi FIN a ACK
  - B pošle A paket s príznakmi FIN a ACK
  - A pošle B paket s príznakom ACK

TCP – Sliding Window

→ [S=0, W=1000, F=SYN, L=0]	
← [S=0, A=1, W=1000, F=SYN+ACK, L=0]	(okno=1-1000)
→ [S=1, A=1, W=1000, F=ACK, L=0]	
→ [S=1, A=1, W=1000, F=ACK, L=500]	
← [S=1, A=501, W=1000, F=ACK, L=0]	(okno=501-1500)
→ [S=501, A=1, W=1000, F=ACK, L=500]	
→ [S=1001, A=1, W=1000, F=ACK, L=500]	(vyčerpali sme okno)
← [S=1, A=1501, W=500, F=ACK, L=0]	(okno=1501-2000)
→ [S=1501, A=1, W=1000, F=ACK, L=500]	
← [S=1, A=2001, W=0, F=ACK, L=0]	(prázdne okno – stop)
→ [S=2001, A=1, W=1000, F=ACK, L=1]	(pokus)
← [S=1, A=2001, W=0, F=ACK, L=0]	(prázdne okno – stop)
← [S=1, A=2001, W=1000, F=ACK, L=0]	(okno=2001-3000)
→ [S=2001, A=1, W=1000, F=ACK+FIN, L=500]	
← [S=1, A=2502, W=1000, F=ACK+FIN, L=0]	
→ [S=2502, A=2, W=1000, F=ACK, L=0]	

Network Address Translation (NAT)

- umožňuje komunikáciu zo siete so súkromnými adresami
- source NAT (SNAT)
  - zdroj spojenia má súkromnú adresu
- destination NAT (DNAT)
  - cieľ spojenia má súkromnú adresu
  - používa sa na sprístupnenie služby poskytovanej serverom so súkromnou adresou

Network Address Translation (NAT)

- router
  - si udržiava tabuľku „spojení“
    - adresa a port zdroja a cieľa,
    - protokol
    - preložená (vlastná) adresa a port
  - pri odosielaní prvého paketu spojenia von
    - prepíše adresu zdroja na preloženú
    - prepíše port zdroja na vlastný (voľný)
    - zapíše spojenie do tabuľky

Network Address Translation (NAT)

- router
  - pri odosielaní ďalšieho paketu spojenia von
    - nájde spojenie v tabuľke
    - prepíše adresu a port zdroja podľa tabuľky
  - pri prijatí paketu zvonku
    - nájde spojenie v tabuľke
    - prepíše adresu a port cieľa podľa tabuľky

Network Address Translation (NAT)

- DNAT
  - pri prijatí paketu zvonka na určenú verejnú adresu a port
    - ak je spojenie v tabuľke, prepíše cieľ podľa tabuľky
    - inak prepíše cieľ podľa konfigurácie a spojenie zapíše do tabuľky
  - pri odosielaní paketu von
    - nájde spojenie v tabuľke
    - prepíše zdroj podľa tabuľky

Network Address Translation (NAT)

- Ako dlho držať spojenie v tabuľke?
  - TCP – dá sa využiť sledovanie stavu spojenia
  - UDP – timeout
    - väčší timeout pre prúd UDP prúd (stream)
- Problémy s aplikačnými protokolmi
  - ak aplikačný protokol používa IP adresy a čísla portov
    - potreba podporných modulov pre udržiavanie tabuľky spojení a príp. prepisovanie dát aplikačnej vrstvy
    - napr. FTP

Aplikačná vrstva TCP/IP

- Rôzne aplikačné protokoly využívajúce TCP alebo UDP
  - WWW: HTTP – TCP/80, HTTPS – TCP/443
  - FTP – TCP/21, TCP/20
  - telnet – TCP/23
  - ssh – TCP/22
  - odosielanie e-mailov: SMTP – TCP/25
  - čítanie e-mailov: POP3 – TCP/110, IMAP - TCP/143
  - DNS – UDP/53, TCP/53