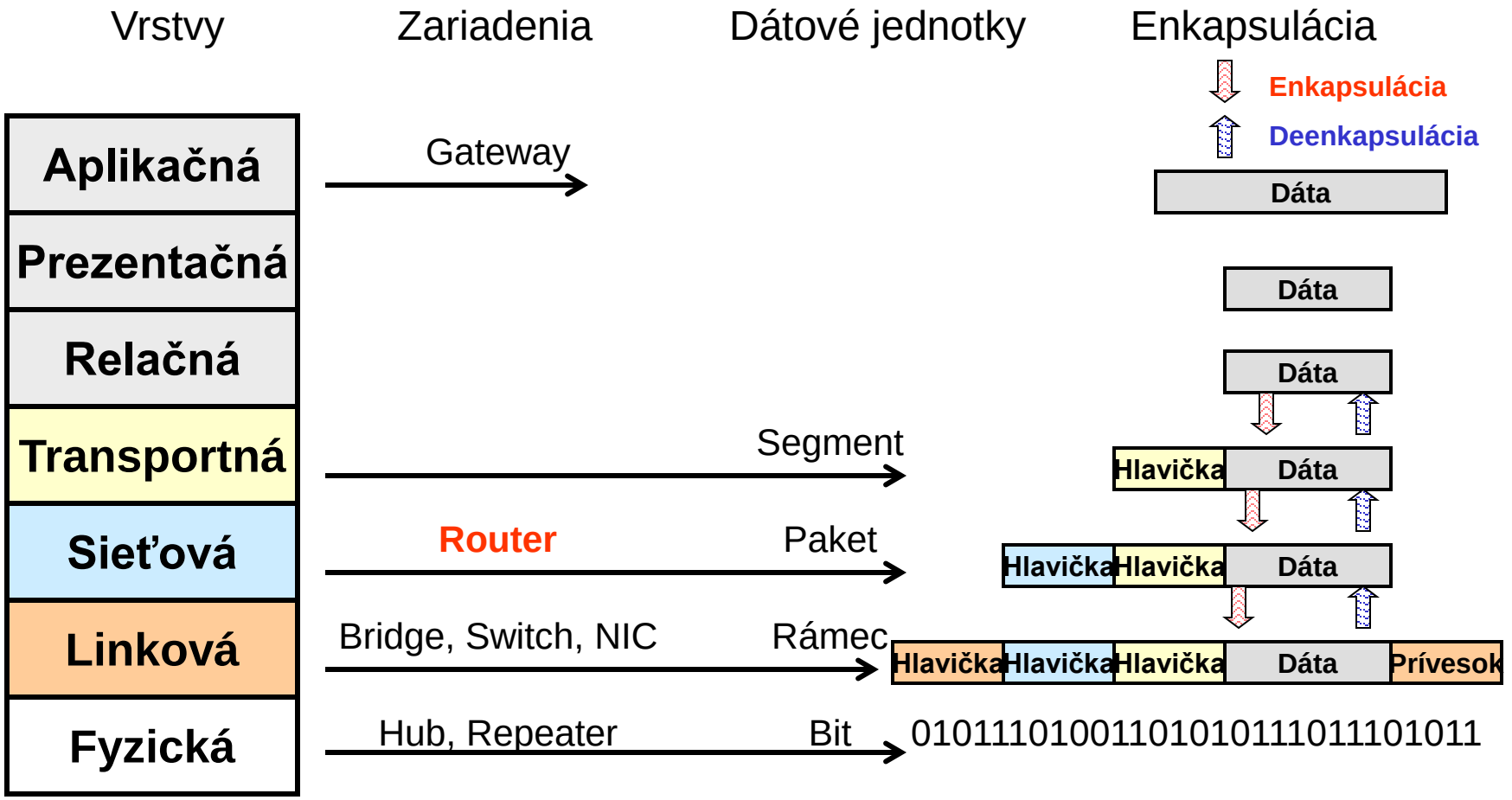
TCP/IP

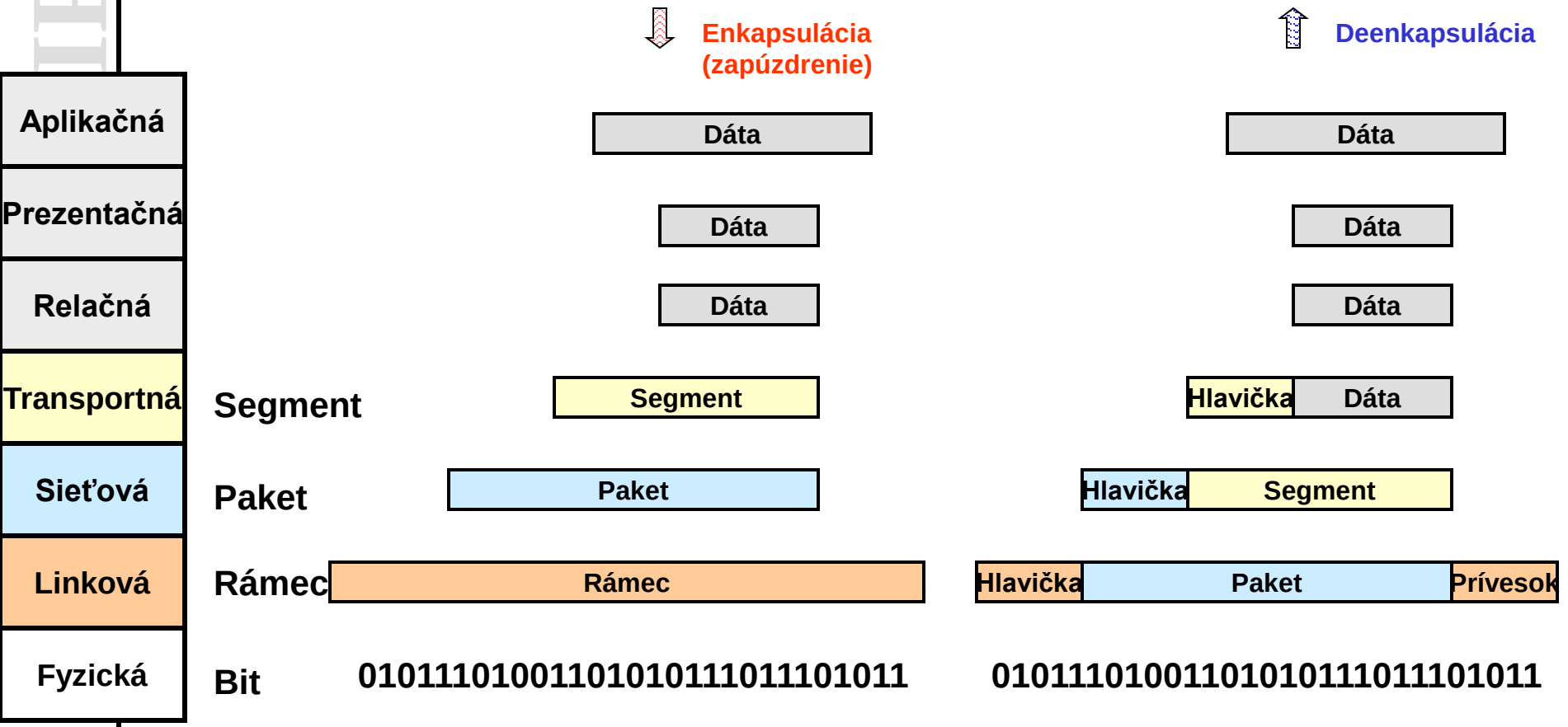
Pavol Segeč
Katedra Informačných Sietí
palo@frkis.utc.sk

ISO OSI RM model

TCP/IP



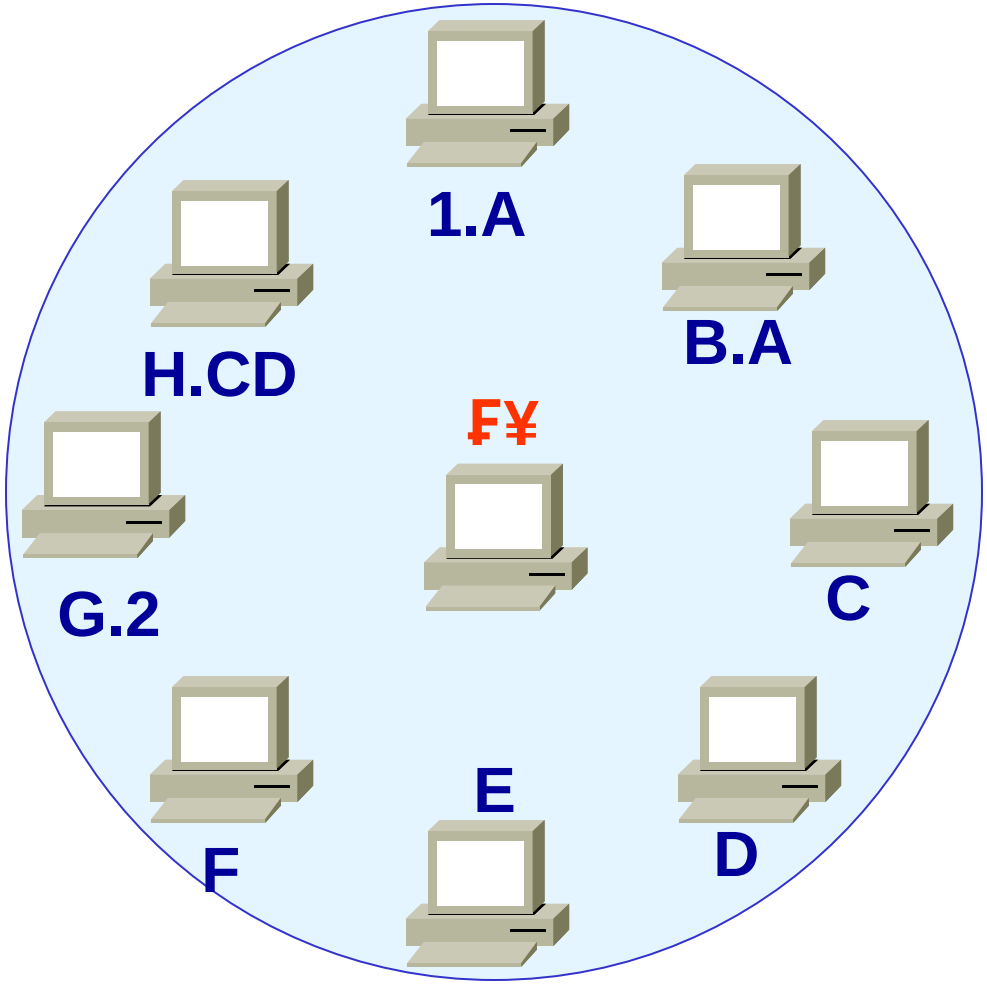
OSI RM komunikácia



Fyzická a logická adresa

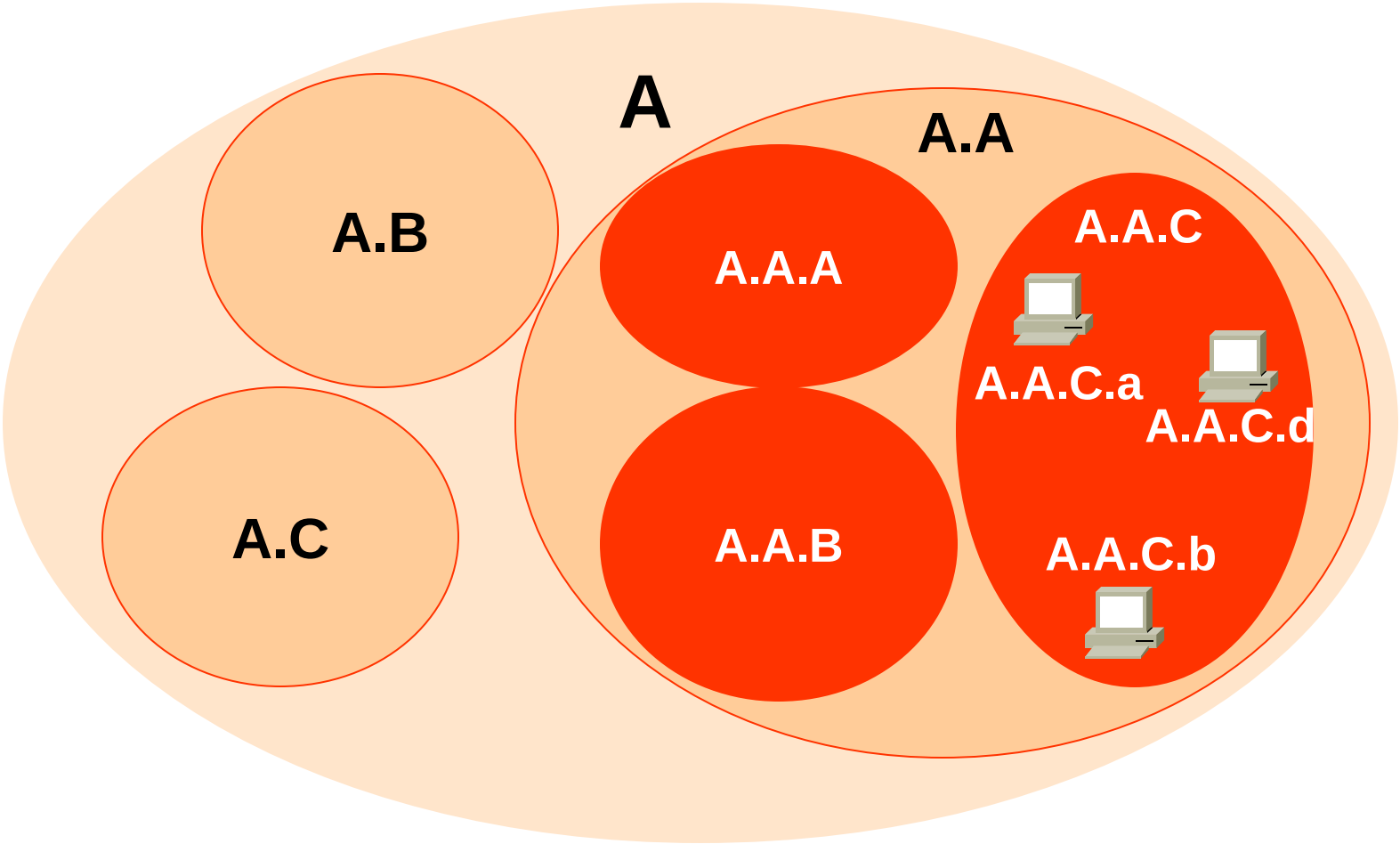
- Jednoznačná identifikácia
- ***Fyzická adresa*** (hardvérová adresa):
  - Linková vrstva
  - Fyzický určuje komunikačný systém (**napr. 44-45-53-54-00-00**)
  - Zviazané so sieťovým HW rozhraním (kartou)
  - Viac rozhraní = viac fyzických adries
- ***Logická adresa:***
  - Často sieťová vrstva
  - Pridelená softvérovo
  - Jedno hw rozhranie = jedna or viac logických adries
  - Umožňuje logicky členiť adresný priestor

Adresné systémy - plošné



- každý systém je rovnocenný
- každý systém je nezávislý
- neexistujú väzby
- nedokážem vytvárať logické celky
- príklad MAC ethernet adresy

Adresné systémy - hierarchické



Paketový prenos

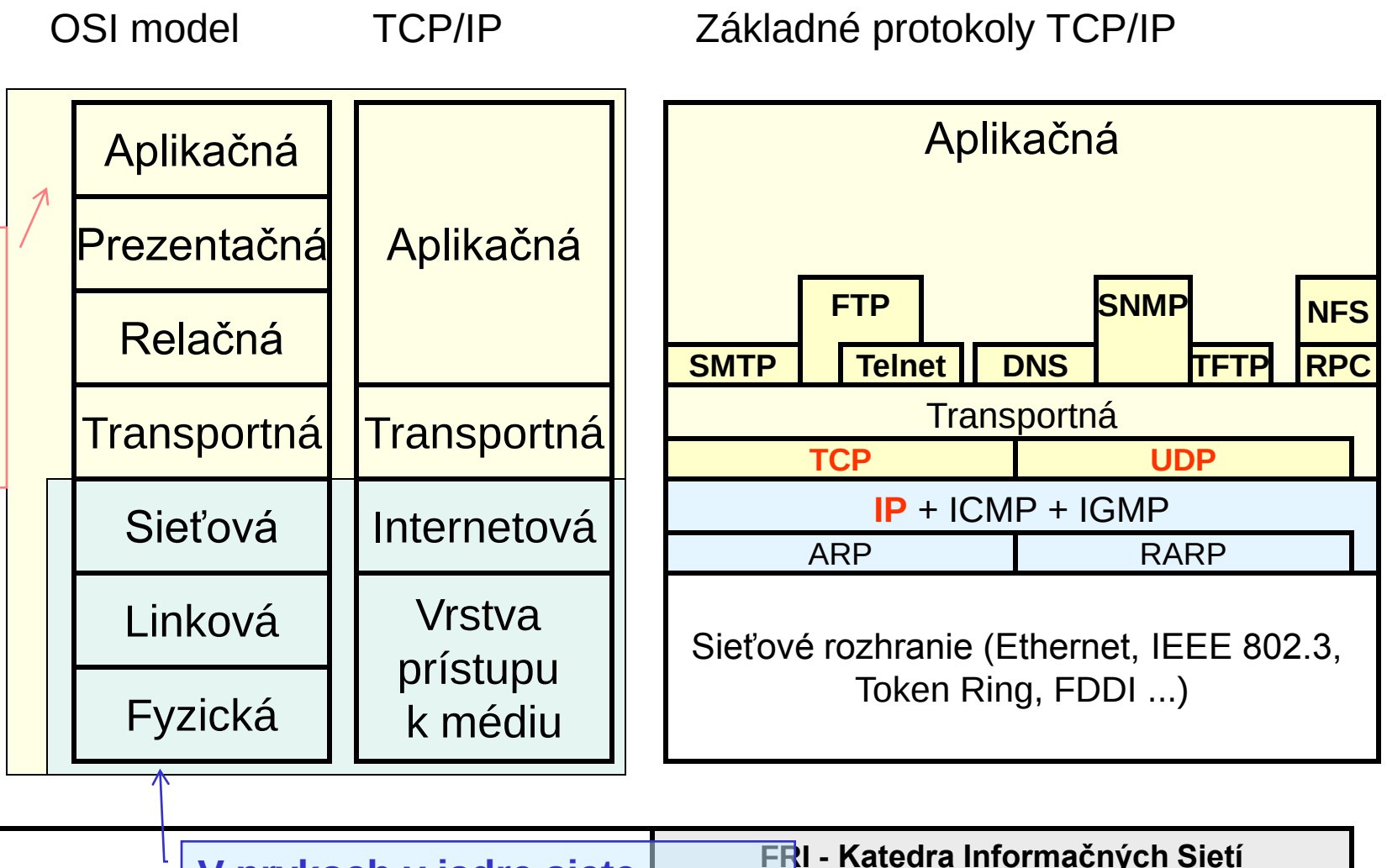
- Používa dátové bloky (pakety) premenlivej dĺžky
- Každý paket: nezávislý dátový blok => potrebujem dodať doplnkové info potrebné k prenosu paketu => hlavička, resp. prívesok
- Dáta môžu prísť poprehadzované
- Dáta sa môžu stratiť
- Nevýhoda: prenášam „neužitočné informácie“, negarantuje prenosové pásmo, zaťaženie každého prenosového uzla
- Výhoda: Efektívne a ekonomické využitie prenosového pásma (dáta sú prenášané len vtedy, keď sú nejaké určené k prenosu)

Technológia TCP/IP

Prečo úspech:

- Prehľadný, jednoducho pochopiteľný RM sieťový model
- je nezávislá od fyzického sieťového HW (integruje rôzne druhy LAN, MAN, WAN sietí)
- používa logický adresný systém (umožňuje jednoznačne adresovanie zariadení v škálovateľnom rozsahu od malých sietí až po Internet)
- používa otvorené, voľne dostupné protokolové štandardy (implementované v množstve rôznych HW a OS platforiem)
- jadro siete pokiaľ možno čo najjednoduchšie, zložitosť v okrajoch siete („inteligencia“)
- ponúka množstvo štandardizovaných aplikačných protokolov pre kompletné, široko dostupné užívateľské služby
- pracuje s prepájaním paketov

TCP/IP model vs. ISO OSI RM



Vrstva prístupu k médiu

• LAN a WAN štandardy definujú protokoly na oboch spodných vrstvách ISO OSI modelu

- **LAN**:
  - IEEE 802.3 (Ethernet (10Base2, 10Base5,10BaseT,100BaseT a pod.)
  - IEEE 802.5 (Token Ring)
  - FDDI
- **WAN**
  - služby s prepojovaním okruhov
    - POTS
    - N-ISDN
  - služby s prepojovaním paketov
    - Frame Relay
    - X.25

- **WAN**
  - Siete s prepojovaním buniek
    - ATM
    - SMDS (Switched Multimegabit Data Service)
  - Dedikované digitálne služby
    - E1, E3, T1, T3 (1.5 až 44 Mb)
    - Rodina xDSL
    - SONET
  - Iné Wan technológie
    - Dial-up
    - Káblové modemy
    - Wireless networks

Prečo vlastne TCP/IP?

- Prečo IP keď mám LAN a WAN protokoly a štandardy?
- Rôznorodosť technológií s ich výhodami aj nevýhodami

LAN

- mnohobodový prístup k médiu
- vysoko rýchlostný
- geograficky limitovaný priestor
- nevhodný adr. systém pre veľké siete

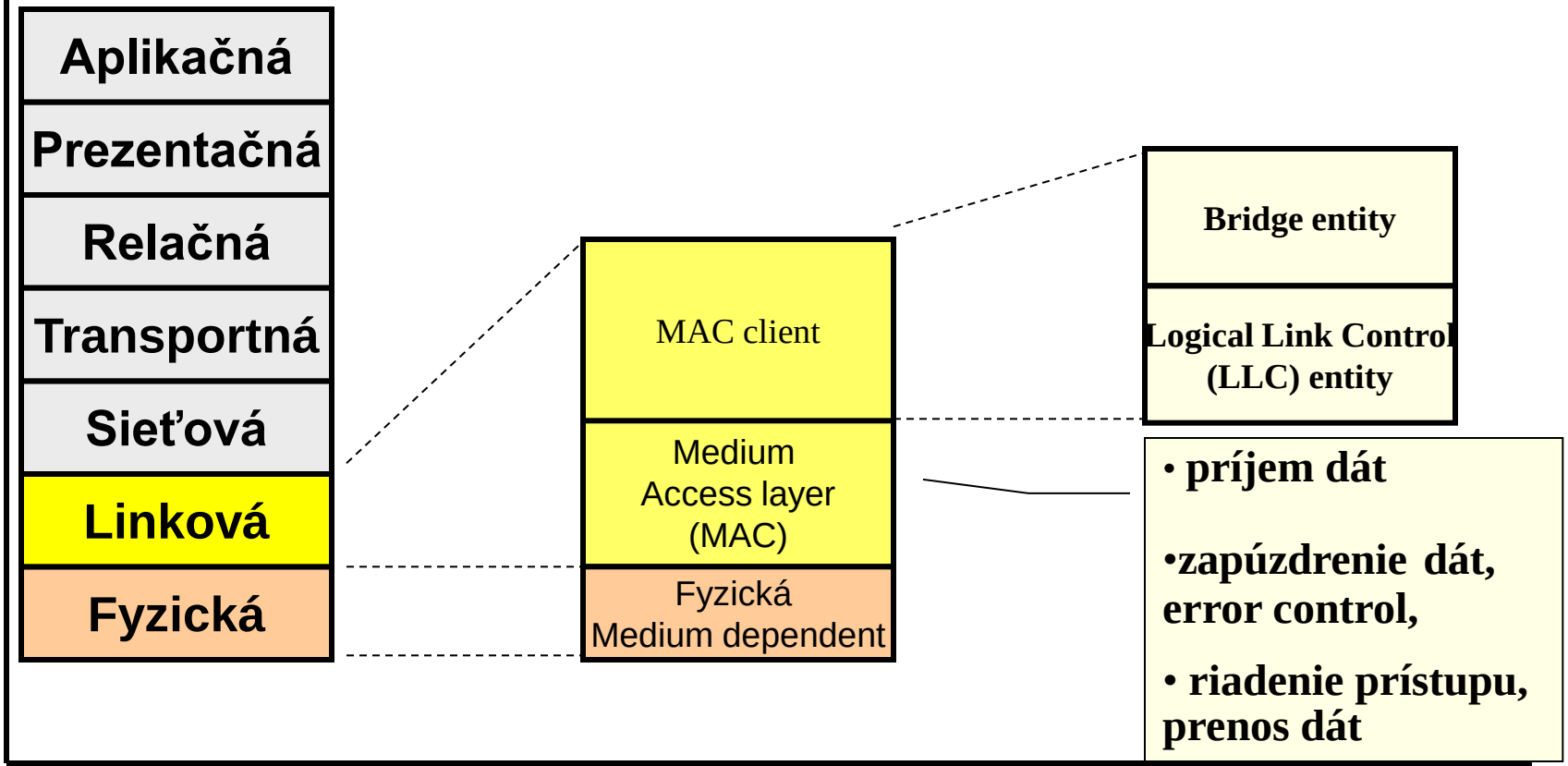
WAN

- zvyčajne spojenia bod bod
- pôvodne s nižšími rýchlosťami
- veľké geografické rozpätie
- vhodné do backbone
- nevhodný adr. systém

IP ukrýva rôznorodosť a ponúka jednotnú IP konektivitu

Ethernet/IEEE 802.3

• LAN technológia (10Base2 [thin coax], 10Base5 [thick coax], 10BaseT [Ethernet], 100BaseT [FastEthernet], 1000BaseT [GigaEthernet], 10GBase…)



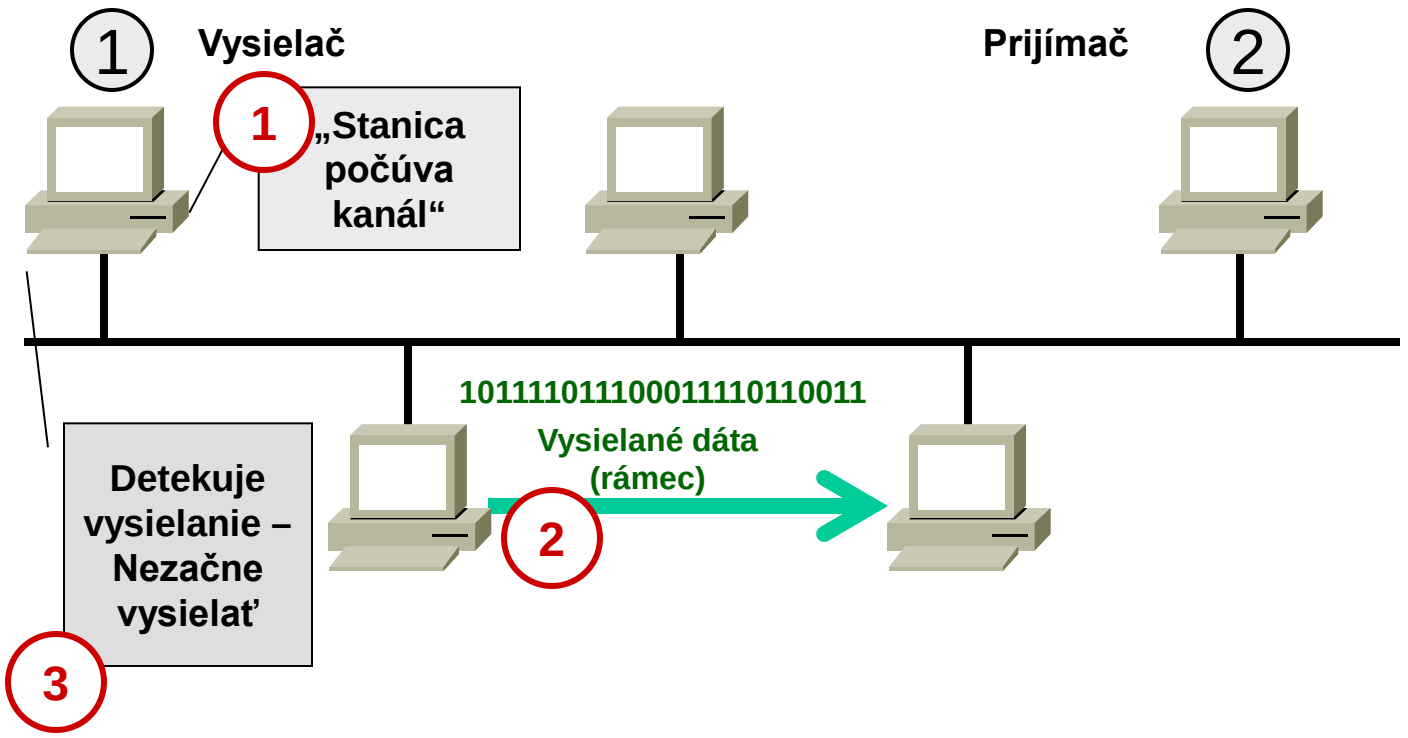
LAN typu Ethernet (L2 OSI RM)

- Počítač musí byť jednoznačne určený - adresa
- Ethernet: používa **fyzické** adresovanie (napálená MAC adresa v NIC)
- Ethernet adresa 48 bitov (24 bit OUI + 24 bit číslo)
- Typy adries:
  - unicast,
  - multicast
  - broadcast
- Použitý prístupový **mechanizmus CSMA/CD**
- Použitý plošný adresný systém (neumožňuje logické členenie siete):
  - prvých 24 bitov: označuje výrobcu OUI (karta iných výrobcov úplne iné adr.)
  - druhých 24 bitov: prideľuje výrobca

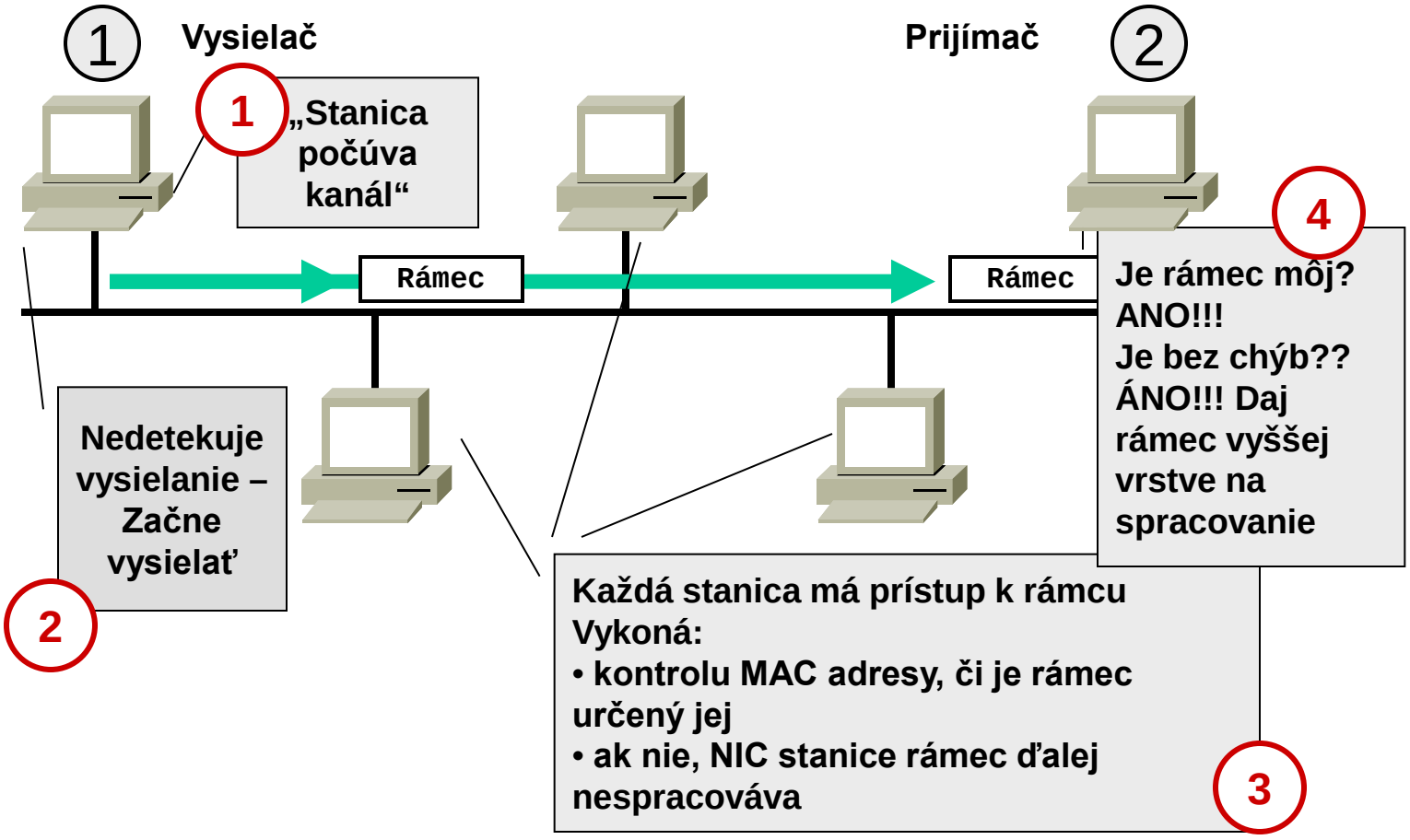
Formát rámca

Preambula	Adresa príjemcu	Adr. odosielateľa	Dĺžka,typ	Dáta	Kontol. súčet (CRC)
8B	6B	6B	2B	46B až 1500B	8B

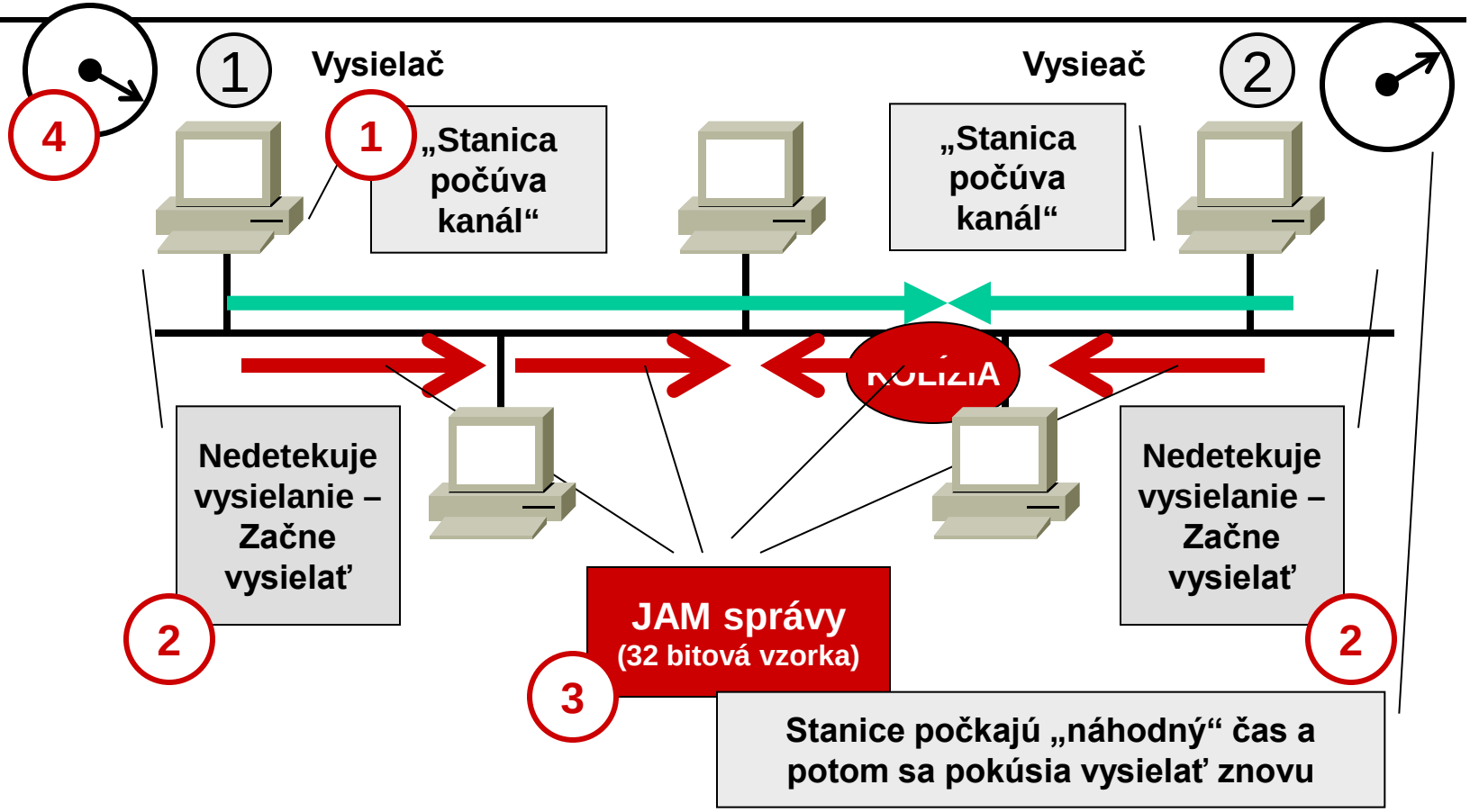
Princíp činnosti 1.



Princíp činnosti 2.



Kolízie 3.


1
Vysielač
Vysieač
2
4
1
„Stanica počúva kanál“
„Stanica počúva kanál“
KOLÍZIA
Nedetekuje vysielanie – Začne vysielať
Nedetekuje vysielanie – Začne vysielať
2
2
JAM správy
(32 bitová vzorka)
3
Stanice počkajú „náhodný“ čas a potom sa pokúsia vysielať znovu

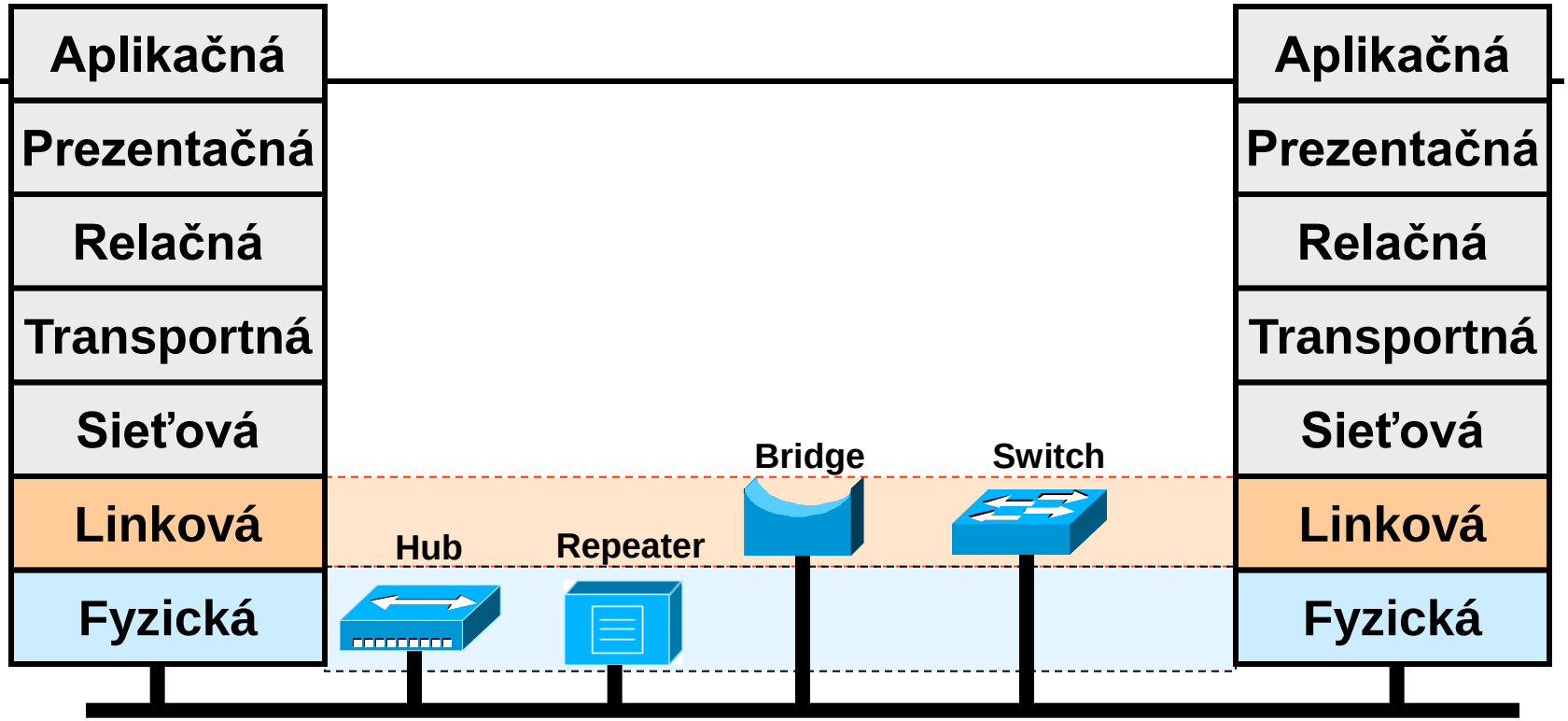
Použitie

- Používa sa v LAN sieťach Ethernet a IEEE 802.3
- Optimálne pri využití siete do 30 -40%, ináč veľké oneskorenia
- Nevýhodná pri veľkom počte krátkych správ (veľa kolízií)
- Veľmi efektívna cesta prepojenia veľa „host počítačov“ pomocou zdieľaného média

- => prechod na topo hviezda

Ethernet zariadenia

TCP/IP

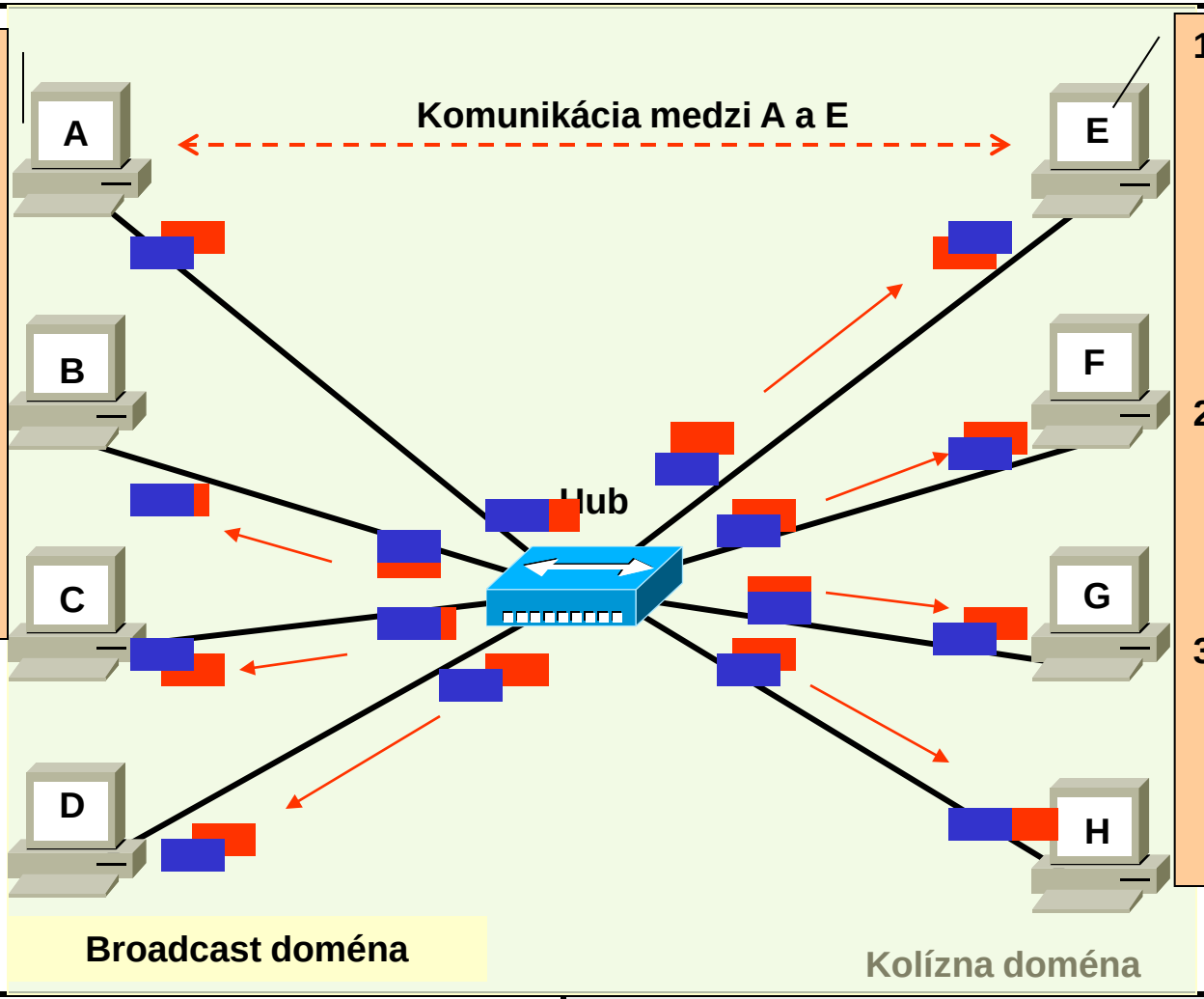


HUB, Opakovač – rozširuje kolíznu doménu (rast kolízií znižuje pripustnosť), rozširuje broadcast doménu (rast broadcast prevádzky znižuje priepustnosť)

Prepínač, Most, NIC – delí kolíznu doménu (1 port = 1 kolízna doména), riadi prevádzku (dokáže si pamätať, ktorá MAC adresa na ktorom porte), rozširuje broadcast doménu, má „inteligentné“ vlastnosti (učenie sa)

Komunikácia - hub

1. Načúva kanál
2. Vytvorí rámec (nevie MAC adr host E, použije broadcast adr)
3. Pošle rámec



1. Na základe vyššieho protokolu zistí že dáta sú určené jemu
2. Formuluje rámec s odpoveďou (vie zdroj adr)
3. Odošle rámec

- prepínač

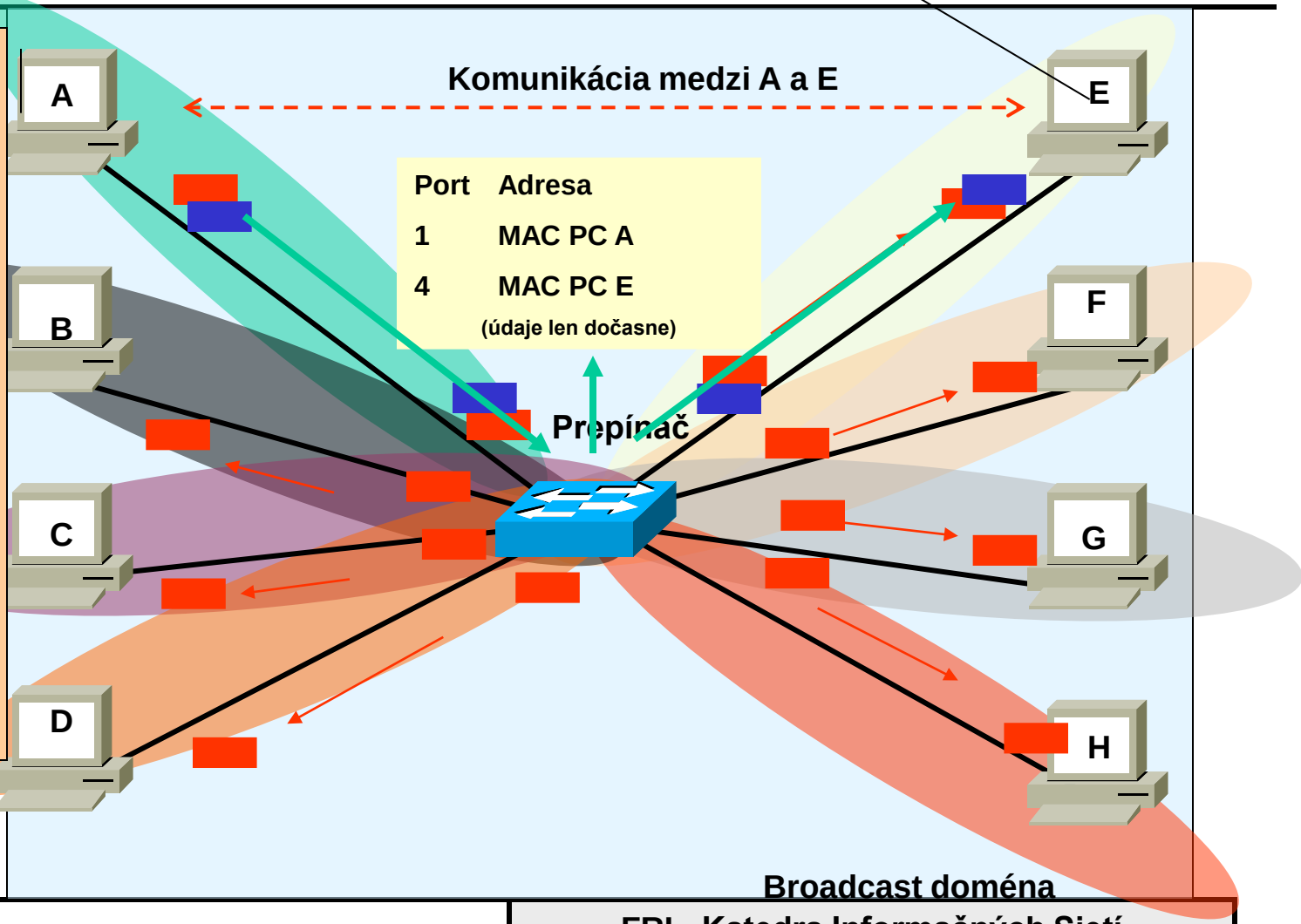
1. Na základe vyššieho protokolu zistí že dáta sú určené jemu
2. Formuluje rámec s odpoveďou
3. Odošle rámec

1. Načúva kanál
2. Vytvorí rámec

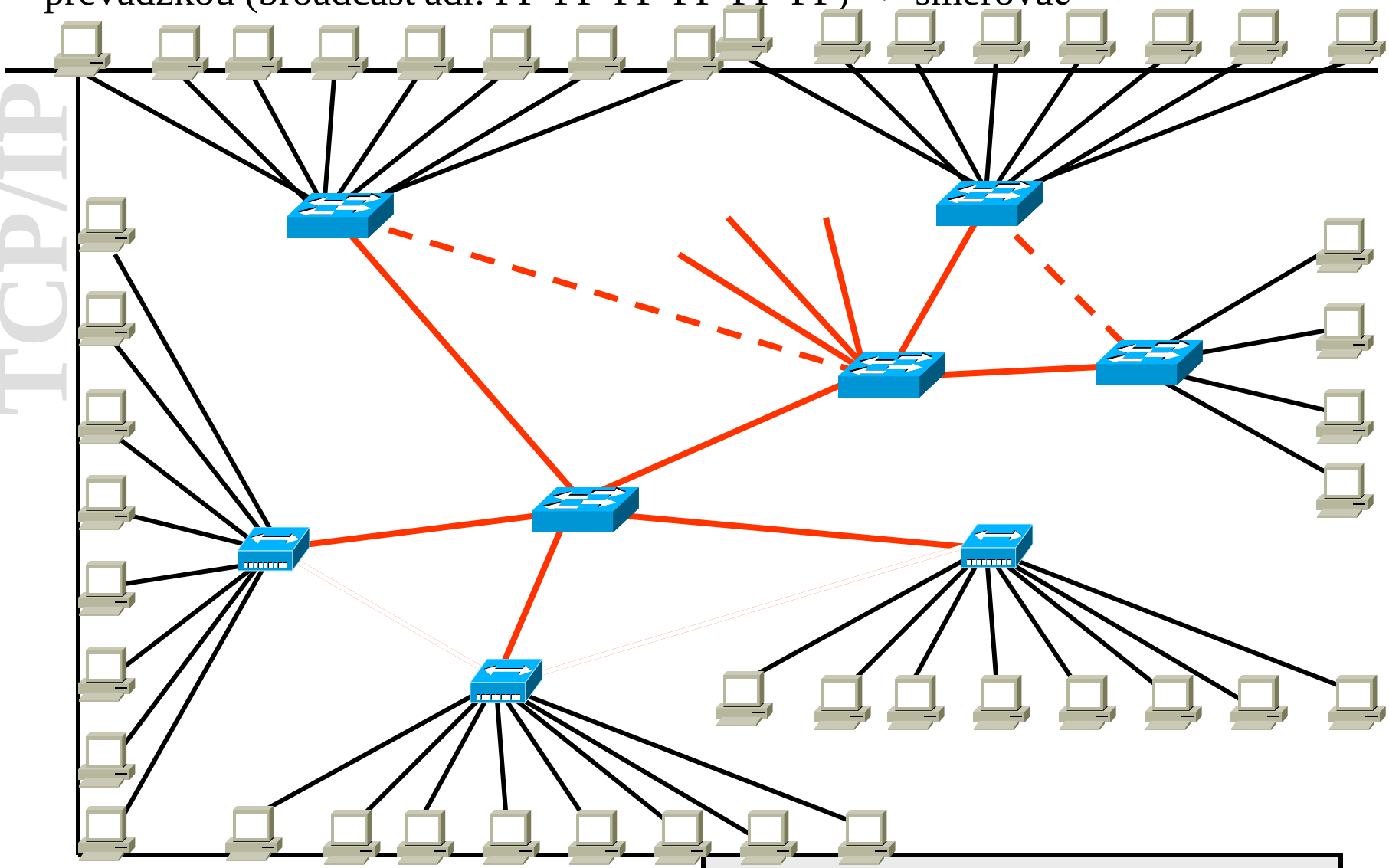
2a. Nevie MAC adresu PC E, použije ako Destination adr. broadcast

2b. Vie MAC adresu PC E

3. Odošle rámec



• pri opakovačoch rastúci počet kolízií (oneskorenie šírenia signálu a pod.) => riešenie => použijem prepínač => celkovo nárast zahltenia siete broadcastovou prevádzkou (broadcast adr. FF-FF-FF-FF-FF-FF) => smerovač



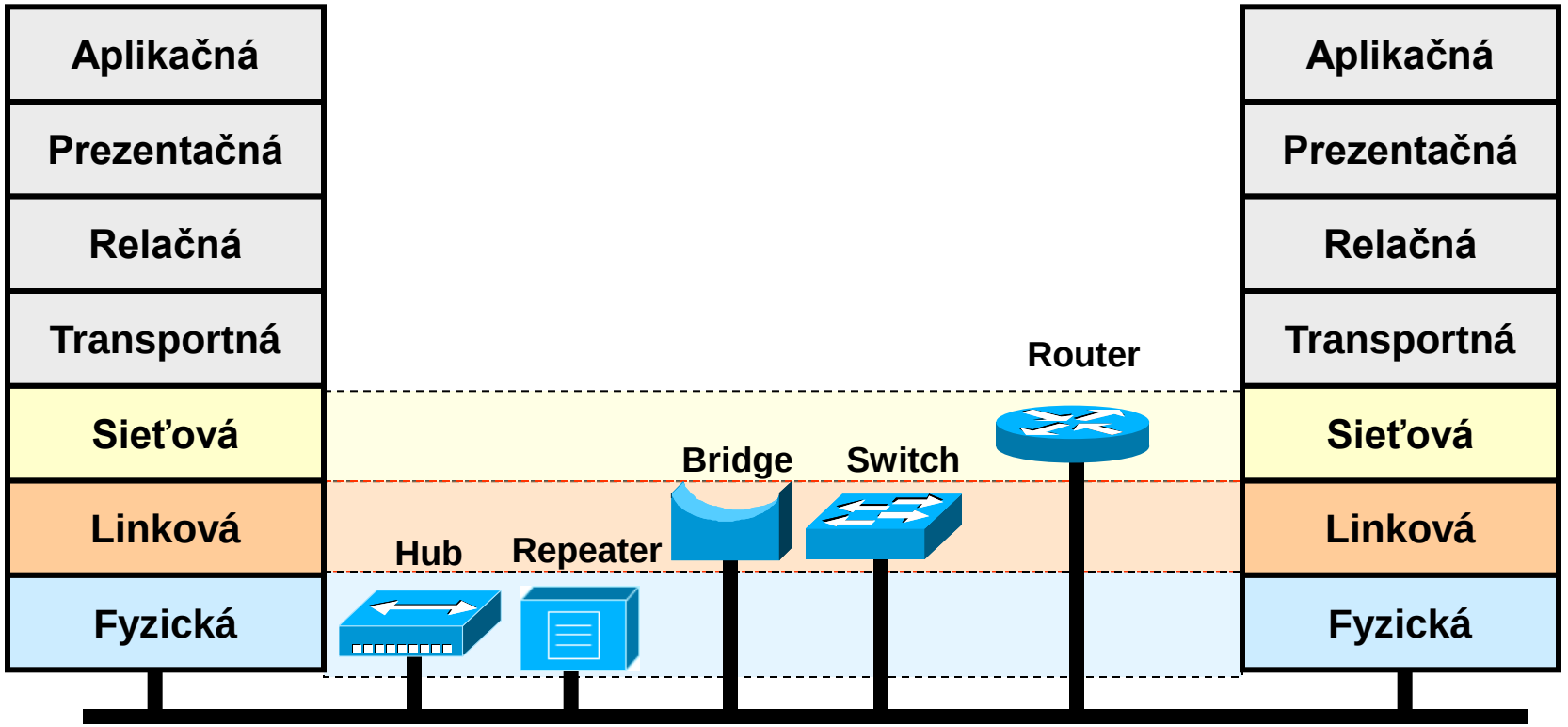
TCP/IP Internetworking

- Ponúka prostriedky integrujúce rôzne typy sietí:
  - Definuje **pakety** (dátové bloky) pre prenos dát sieťou (IP protokol)
  - vhodný **adresný systém** - IP adresovanie (IP protokol)
  - mechanizmy prekladu sieťovej adresy (IP adresy) na linkovú adresu (napr. MAC adresu (ARP protokol))
  - smerovanie dát sieťou - **smerovacie protokoly** (RIP, OSPF atď protokoly).
  - Transportné protokoly - TCP a UDP protokoly
  - Monitoring a testovanie siete – ICMP protokol

Internetová vrstva

- Dátový blok: **PAKET**
- Ukrýva pred užívateľom nižšiu vrstvu (ponúka jednotnú konektivitu)
- Zabezpečuje konektivitu medzi ľubovoľnými dvomi host systémami (sieťovo dostupnými, aj keď v odlišných fyzických sieťach a geo. oblastiach) (zdanie priamej konektivity)
- Poskytuje logický, hierarchický adresný systém (log členenie sietí)
- **Smerovanie a výber cesty**
- Zariadenie => **SMEROVAČ =>** výber cesty a smerovanie paketov
- Protokoly:
  - smerované: **IP protokol** (nesú dáta)
  - Smerovacie: (RIP, OSPF a pod.) (smerovače si vymieňajú info o sieti)

Zariadenia – smerovač (router)

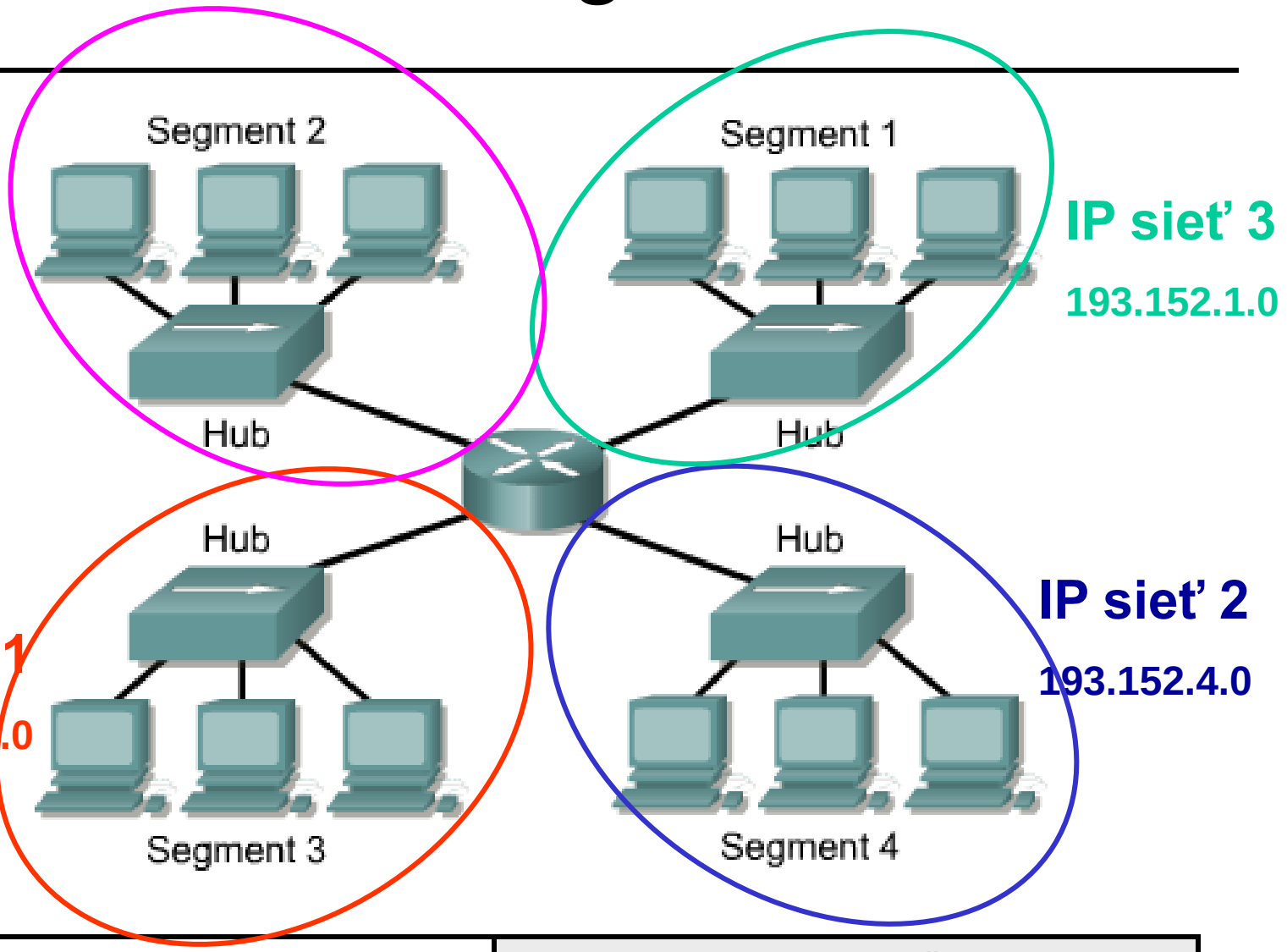


Smerovač

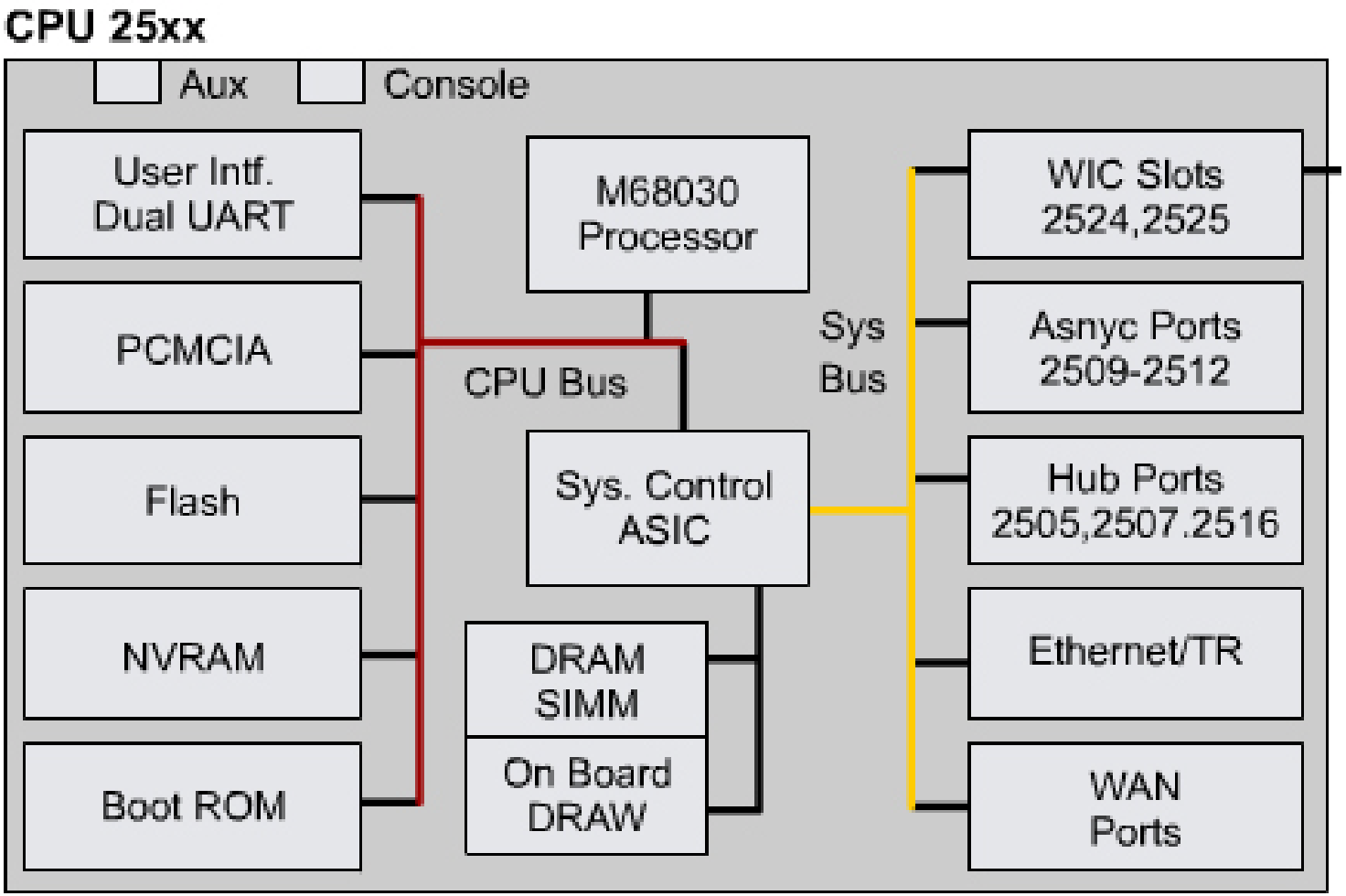
Router (smerovač): najdôležitejší stavebný prvok IP siete

- Prepája segmenty alebo celé siete
- nachádza sa na rozhraní sietí s inými sieťovými adresami (iné IP adresné priestory)
- ponúka široký sortiment hw rozhraní (LAN, MAN, WAN, telco)
- spracováva každý cez neho idúci paket
- **hl. úloha** získavanie informácií o sieti a smerovanie a prepínanie paketov (routing and forwarding)
- množstvo iných úloh (rozčleňuje broadcastové domény-segmentácia, fragmentácia, bezpečnosť, a pod

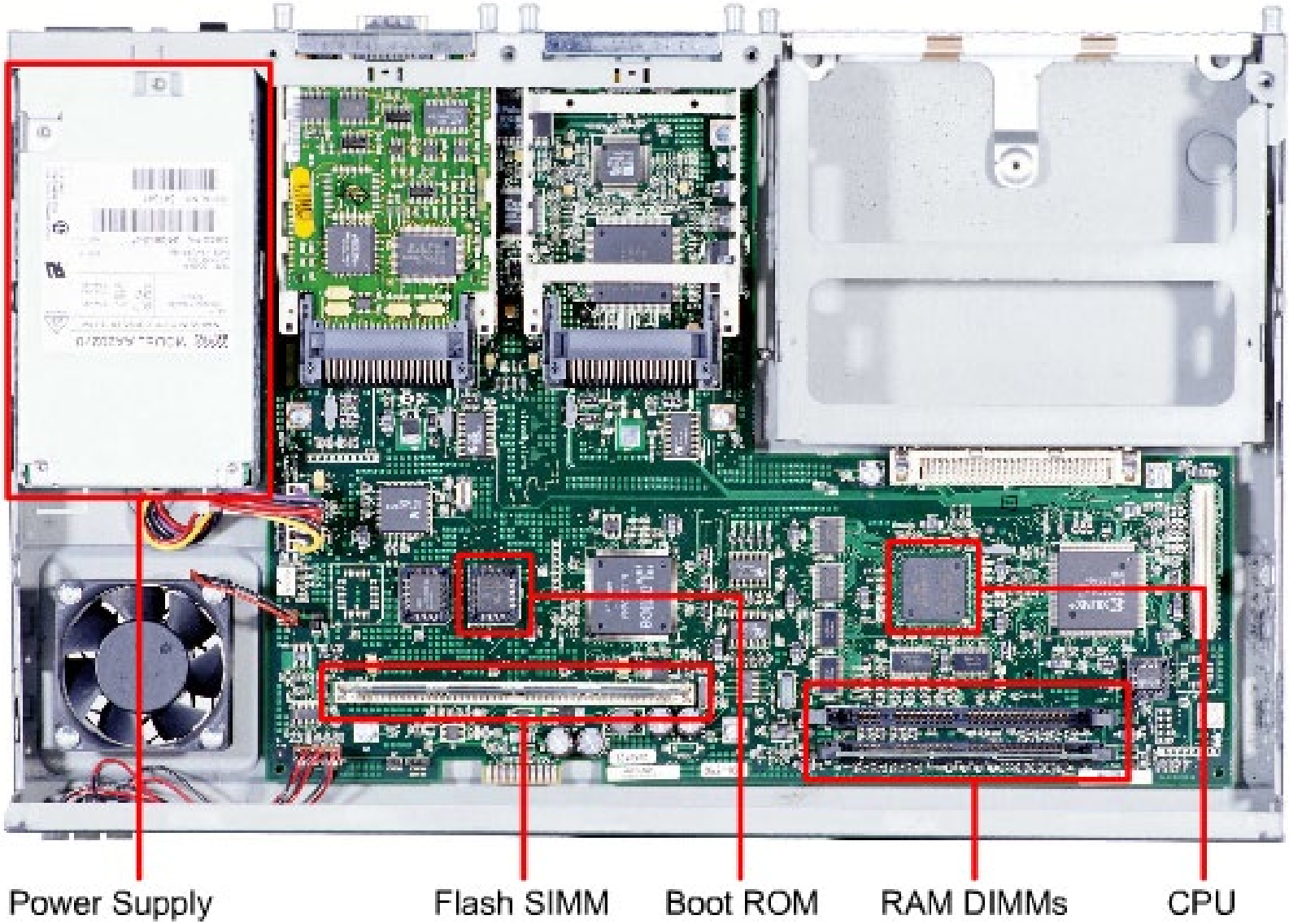
Smerovač - segmentácia



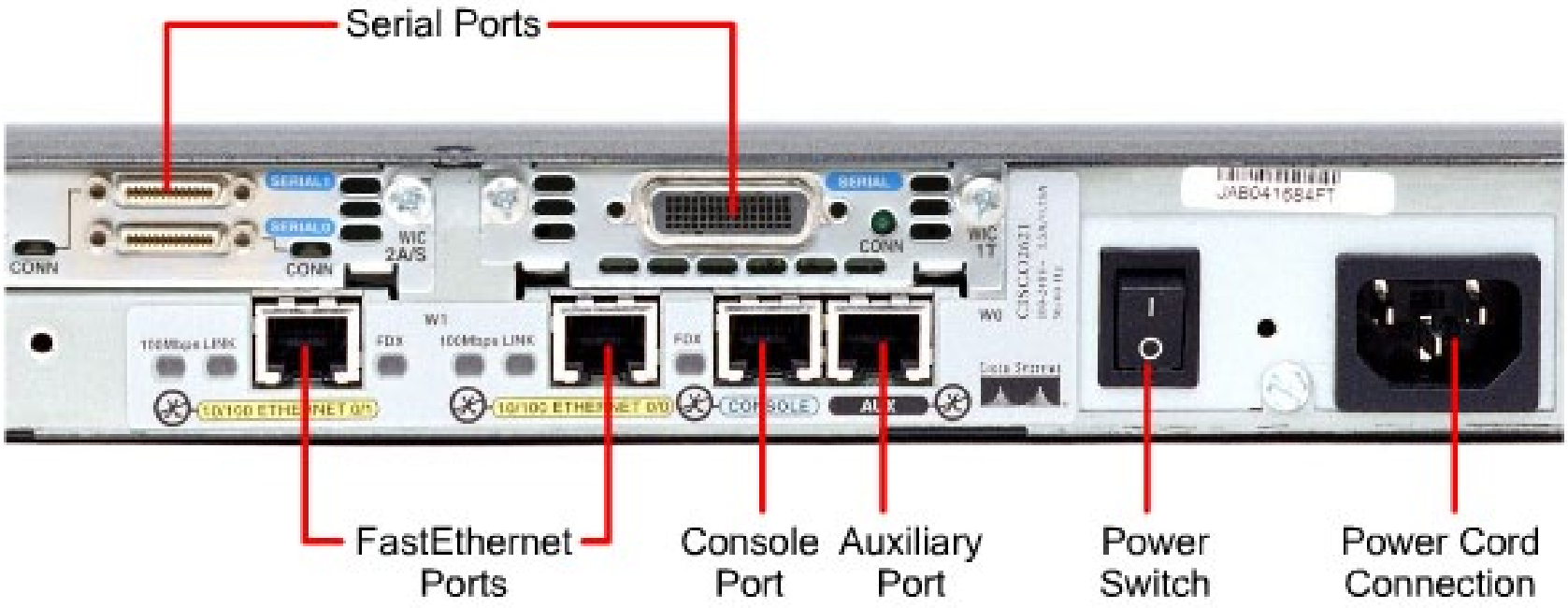
Smerovač – interné komponenty



Smerovač – zakladná doska 2600



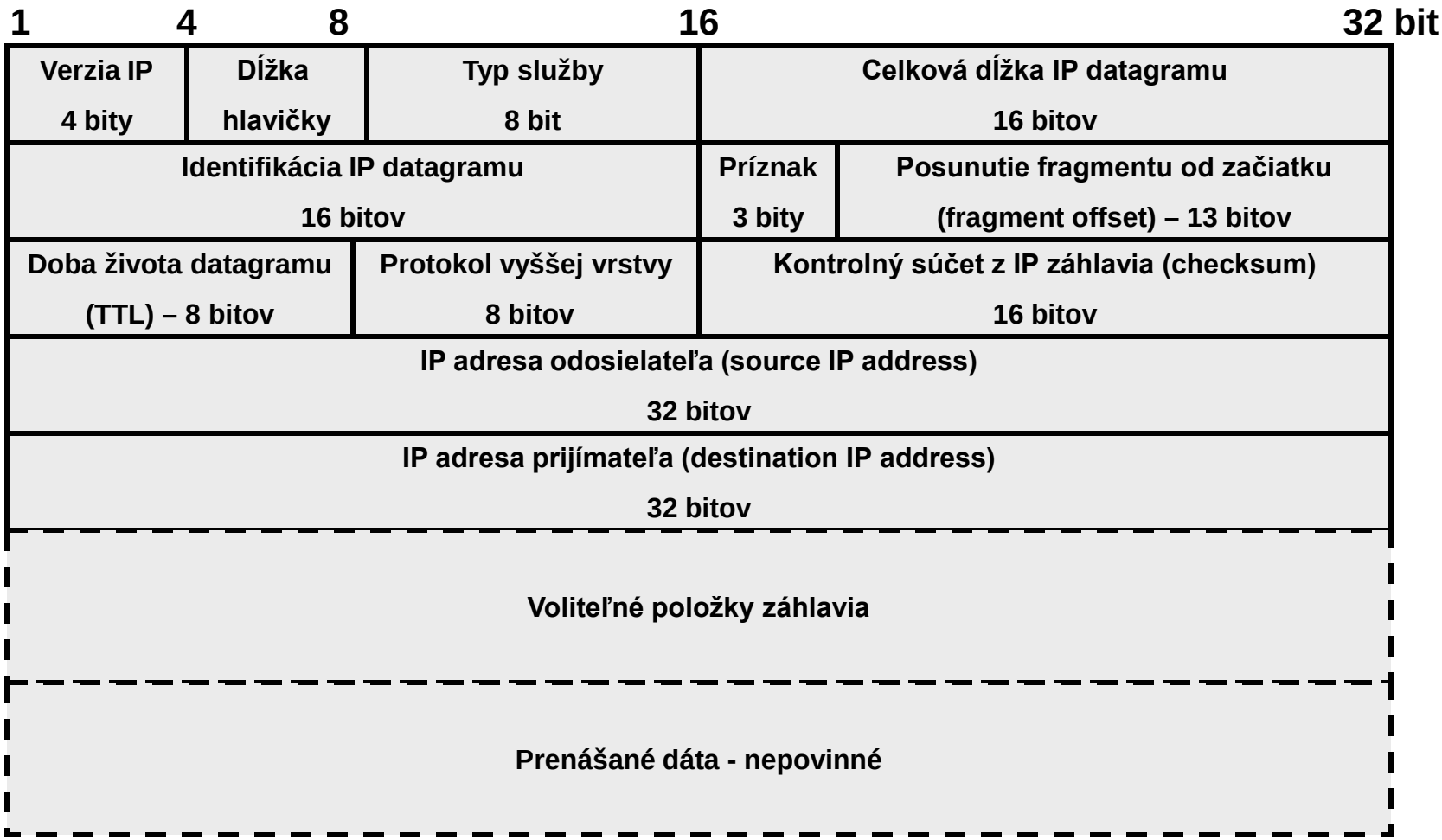
Smerovač – vonkajší pohľad



Internet protokol (IP)

- Najdôležitejší protokol (všetky dáta vyšších vrstiev idú cez IP)
- **Funkcie:**
  - Definuje PDU: štruktúru paketu (IP datagram)
  - Definuje adresnú schému (každé zariadenie musí byť jednoznačne identifikovateľné)
  - definuje fragmentáciu a mechanizmy pre „znovu zloženie“ paketu
- **Vlastnosti:**
  - Nespojovo orientovaný (connectionless) (nevytvára okruh)
  - „Nespoľahlivý“ protokol (nerobí error kontrolu a „recovery“)
  - Typu best-effort

IP paket


1
4
8
16
32 bit
Verzia IP
4 bity
Dĺžka
hlavičky
Typ služby
8 bit
Celková dĺžka IP datagramu
16 bitov
Identifikácia IP datagramu
16 bitov
Príznak
3 bity
Posunutie fragmentu od začiatku
(fragment offset) – 13 bitov
Doba života datagramu
(TTL) – 8 bitov
Protokol vyššej vrstvy
8 bitov
Kontrolný súčet z IP záhlavia (checksum)
16 bitov
IP adresa odosielateľa (source IP address)
32 bitov
IP adresa prijímateľa (destination IP address)
32 bitov
Voliteľné položky záhlavia
Prenášané dáta - nepovinné

Ethereal & WinPcap

- www.ethereal.com analyzátor
- http://winpcap.polito.it/ paketový driver na odchytávanie paketov

IP paket - Net analyzer

```
⊟Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 158.193.152.51
   Version: 4
   Header length: 20 bytes
  ⊞Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 434
   Identification: 0x1282
  ⊟Flags: 0x04
     .1.. = Don't fragment: Set
     ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (0x06)
   Header checksum: 0x78a1 (correct)
   Source: 158.193.152.108 (158.193.152.108)
   Destination: 158.193.152.51 (158.193.152.51)
```

IP paket (2)

- **Verzia (version):** 4 bity, verzia IP protokolu, môže byť 4 alebo novšia 6 (IP next generation)
- **Dĺžka hlavičky (header length):** 4 bity, dĺžka záhlavia (udáva sa v 4 bytoch), udáva sa preto, že niekedy sú voliteľné položky záhlavia
- **Typ služby (Type of service - TOS):** 8 bitov, žiadaný typ služby pre datagram, historicky (až doteraz), sa neuplatnila; dnes DiffServ QoS architektúra
- **Celková dĺžka datagramu (total length):** 16 bitov, celková dĺžka datagramu (max 2^{16}– 1=65 535B)
- **Identifikácia datagramu (identification):** 16 bitov, jednoznačná identifikácia datagramu - číslo, vkladá OS, použité pri fragmentácií
- **Príznak (flags):** 3 bity,

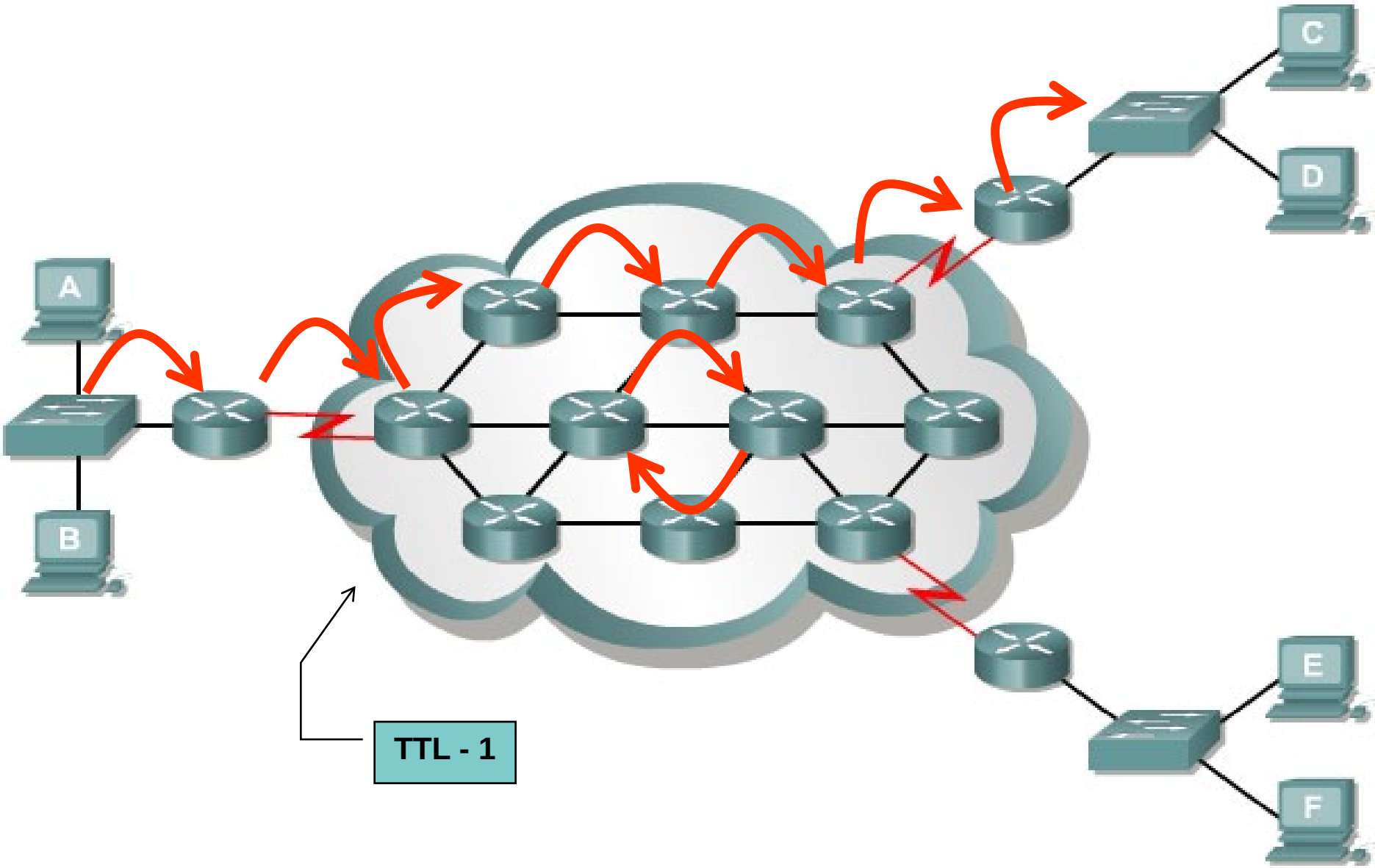
0	DF	MF

  - 0, musí byť 0, rezervované
  - DF: Don´t fragment, 0 – fragmentácia povolená, 1 – fragmentácia zakázaná
  - MF: More fragments, 0 – toto je posledný fragment, 1 – toto nie je posledný fragment
- **Posunutie fragmentu (frag. offset):** 13 bitov, pri fragmentácií udáva kam fragment patrí v počte 64 bit kusov, prvý fragment má hodnotu 0

IP paket (3)

- **Doba života datagramu (time to live-TTL):** 8 bitov, ochrana proti zacykleniu datagramu, hodnota nastavená OS (or programátorom), prechod routrom dekrementuje hodnotu, TTL 0-datagram zahodený.

Hop by Hop



IP paket (4)

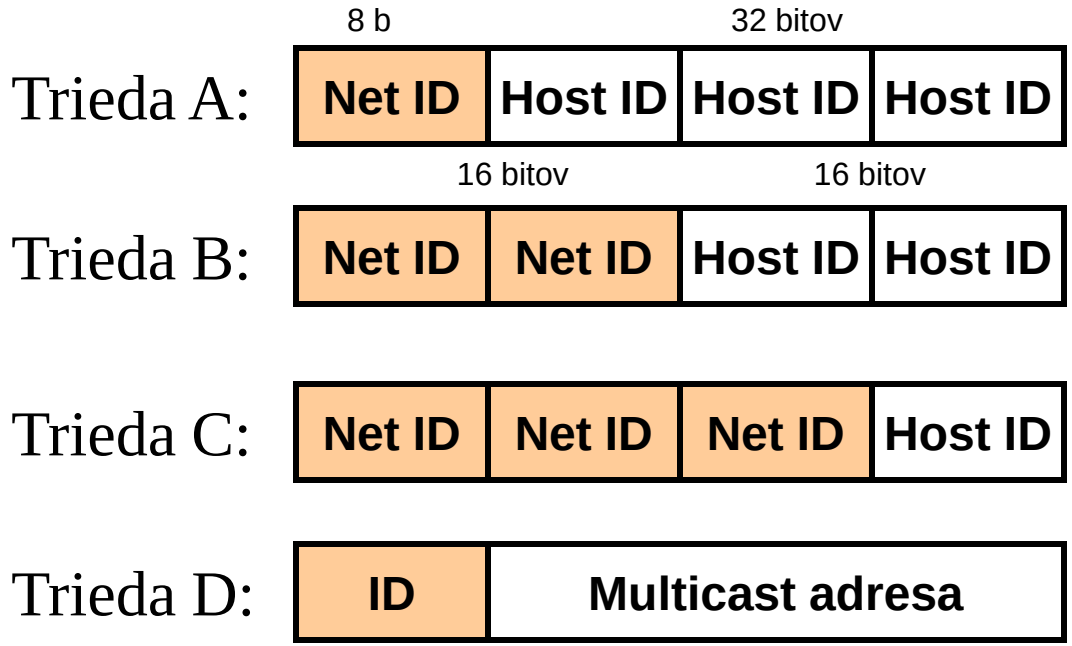
- **Protokol vyššej vrstvy (protocol):** 8bitov, identifikácia neseného protokolu vyššej vrstvy, UDP=17, TCP=6, ICMP=1
- **Kontrolný súčet cez IP záhlavie (header checksum):** 16 bitov, kontrolný súčet
- **IP adresa odosielateľa (source IP address):** 32 bitov, adresa odosielateľa
- **IP adresa príjemcu (destination IP address):** 32 bitov, adresa príjemcu
- **Voliteľné položky (options):** variabilná dĺžka, položky môžu a nemusia byť v pakete, príklad: source routing, record route, internet timestamp a pod

IP adresovanie

- Logické adresovanie (siete logické celky oddelené smerovačmi)
- Adresa dlhá 32 bitov (IPv4, 2^{32} adries)
  - 128 bitov IPv6 (2^{128} adries)
    - (napr.: CA32:F123:C210:1234:0000:0000:0000:1A11)
- Každé IP zariadenie musí mať **jednoznačnú** adresu
- IP adresa - identifikácia zariadenia IP protokolom
- Tvar:
  - decimálna notácia: 158.193.152.112
  - binárna: 10011110.11000001.10011000.01110000
  - Hexa: 9E.C1.98.70 (hlavne pri IPv6)
  - domain name : fr326c.fri.utc.sk (potrebujem mechanizmus na preklad adries a mien)
- Polia:

  - Pre potreby smerovania

Triedy IP adries – historické delenie



Najvyšší bit vždy 0: adresy 0 až 126

127 sietí s 16 777 214 počítačmi

Najvyššie dva bity 10: adresy 128 až 191

16 385 sietí s 65 534 počítačmi

Najvyššie tri bity vždy 110: adresy 192 až 223

2 097 153 sietí s 253 počítačmi

Najvyššie štyri bity 1110: adresy 224 až 239

Multicastové adresy

Trieda E: adresy 240 až 255 (prvý byte), adresy vyhradené pre budúce použitie

- Nezískava sa jedna IP adresa, ale adresný priestor
- Smerovače na základe prvých bitov zisťovali NET ID

Vyhradené adresy

- V každej triede sú vždy vyhradené dve adresy
  - 1) adresa siete: všetky Host ID sú **NULY** (binárne)
    - napr. Trieda A: 111.0.0.0 alebo trieda B 158.193.0.0, použité pri smerovaní do siete, ktorá obsahuje hosta
  - 2) broadcast adresa: Host ID sú samé jednotky (binárne)
    - napr. Trieda A: 111.255.255.255, adresa všetkých Hostov
- **Privátne adresy:**
  - 10.0.0.0 až 10.255.255.255
  - 172.16.0.0 až 172.31.255.255
  - 192.168.0.0 až 192.168.255.255

Privátne siete (intranety) bez pripojenia na Internet alebo pripojené cez napr. NAT alebo proxy

- 127.0.0.1 – programovateľná slučka (loopback)

  - má každý počítač v sieti

Využitie? Sub-sieťovanie

Sieťová maska – princíp (1)

- Použitie: určenie adresy siete
- Štandardné sieťové masky
  - Pre adr. typu A je to: 255.0.0.0; pre adr. typu B:255.255.0.0 etc.
- Operácia binárny súčin:
  - Kde leží počítač (na ktorej sieti) s IP adresou 158.193.152.112 ?

10011110.11000001.10011000.01110000

* 11111111.11111111.00000000.00000000

10011110.11000001.00000000.00000000

Čo je 158.193.0.0

Sieťová maska

Poznáme: IP adresu uzla = 193.12.99.18, masku siete=255.255.255.0

193.12.99.18	=	11000001	00001100	01100011 00010010
255.255.255.0	=	11111111	11111111	11111111 00000000
193.12.99.0	=	11000001	00001100	01100011 00000000

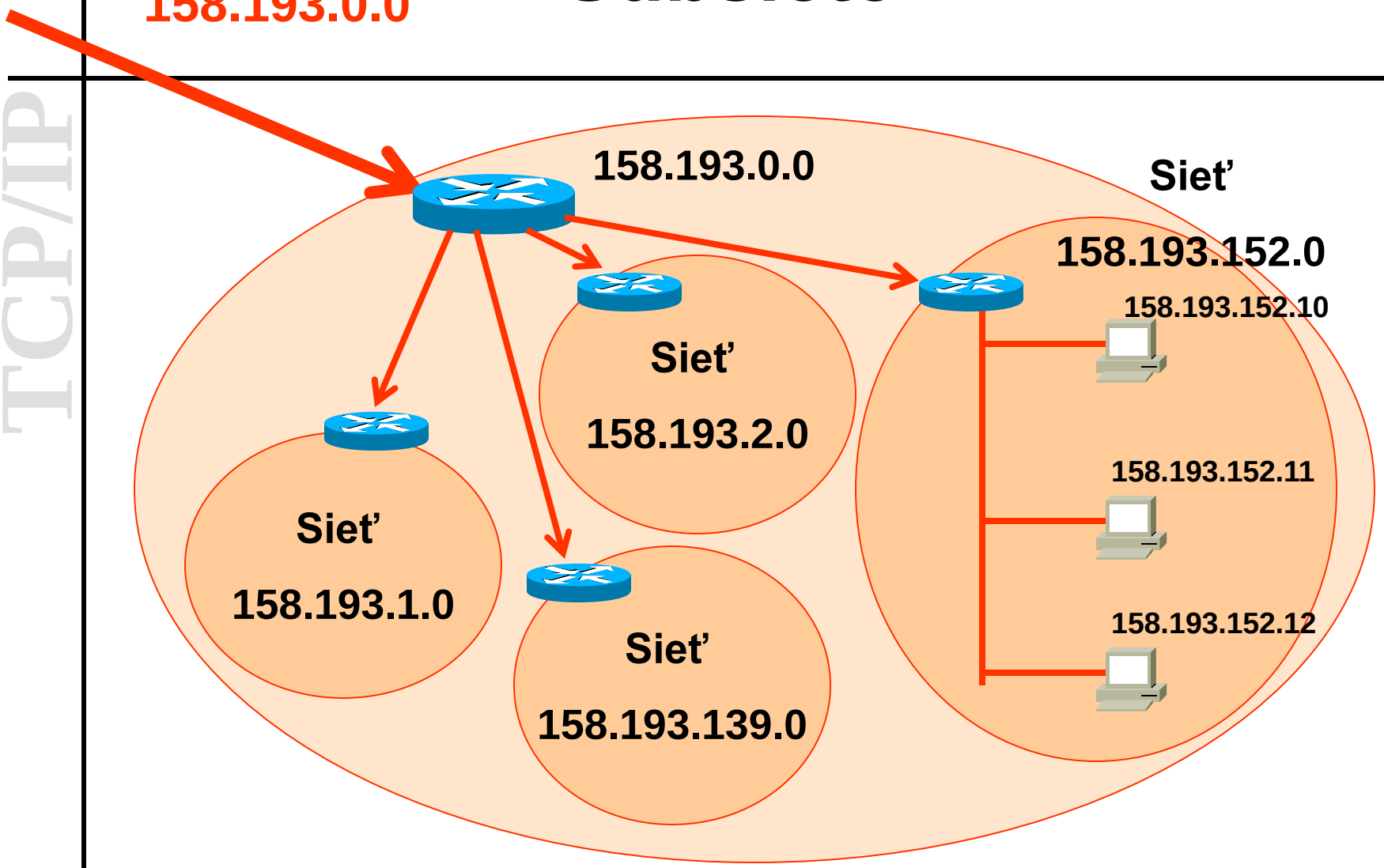
IP adresa siete = 193.12.99.0

poznáme: IP adresu uzla = 112.229.26.10,masku siete=255.0.0.0

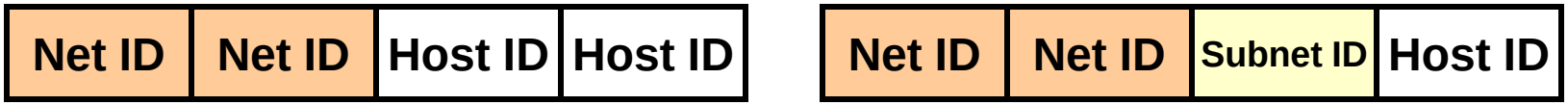
112.229.26.10	=	01110000	11100101	00011010 00001010
255.0.0.0	=	11111111	00000000	00000000 11100000
112.0.0.0	=	01110000	00000000	00000000 00000000

IP adresa siete = 112. 0.0.0

Subsiete


158.193.0.0
158.193.0.0
Sieť
158.193.152.0
158.193.152.10
Sieť
158.193.2.0
158.193.152.11
Sieť
158.193.1.0
158.193.152.12
Sieť
158.193.139.0

Subsiete - princíp



Príklad: pridelená adresa typu B **158.193.0.0** a potrebujem predať ďalej administratívu podsietí

Riešenie: vypožičiam si niekoľko bitov z Host ID – otázka koľko? (tu 8)

Získam $2^8 - 2$ subsietí, každá môže mať $2^8 - 2$ počítačov

Sieťová maska: 255.255.255.0

– Kde leží počítač (na ktorej subsieti) s IP adresou 158.193.152.112 ?

10011110.11000001.10011000.01110000

* 11111111.11111111.11111111.00000000

10011110.11000001.10011000.00000000

Čo je 158.193.152.0

Subsiete (3)

Poznáme: IP adresu uzla = 195.229.26.10, masku podsiete = 255.255.255.**224**

195.229.26.10 = 11000011 11100101 00011010 00001010

255.255.255.224 = 11111111 11111111 11111111 **111**00000

195.229.26.224 = 11000011 11100101 00011010 11100000

IP adresa siete = 195. 229.26.224

IP adresa uzla = 147.229.22.85 maska podsiete = 255.255.**255.192**

147.229.22.85 = 10010011 11100101 00010110 01010101

255.255.255.192 = 11111111 11111111 **11111111 11**000000

147.229.22.64 = 10010011 11100101 00010110 01000000

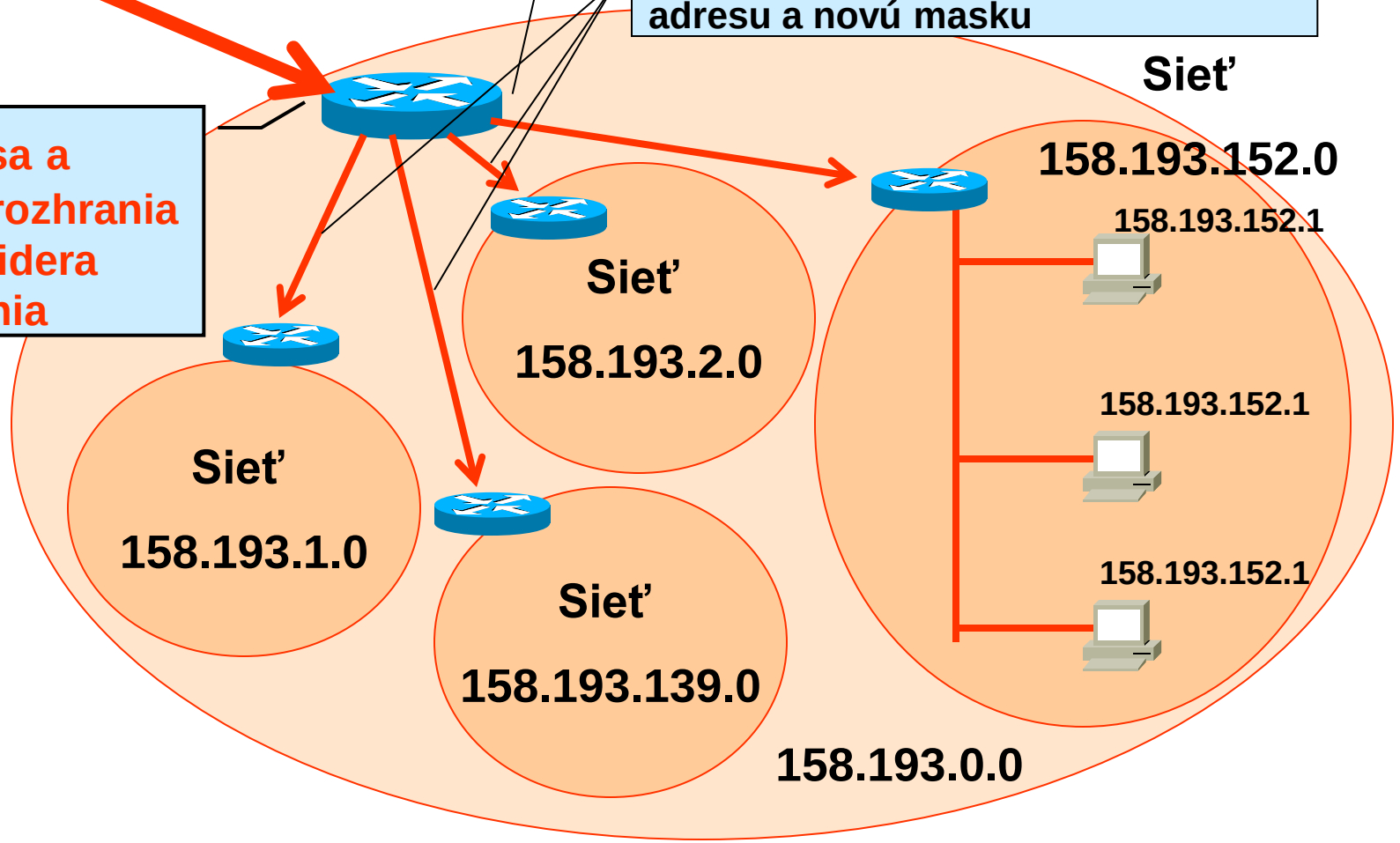
Subsiete(4)

158.193.0.0

Potrebné:

- rozhranie do každej novej subsiete
- každému rozhraniu priradiť IP adresu a novú masku

IP adresa a maska rozhrania na providera pripojenia



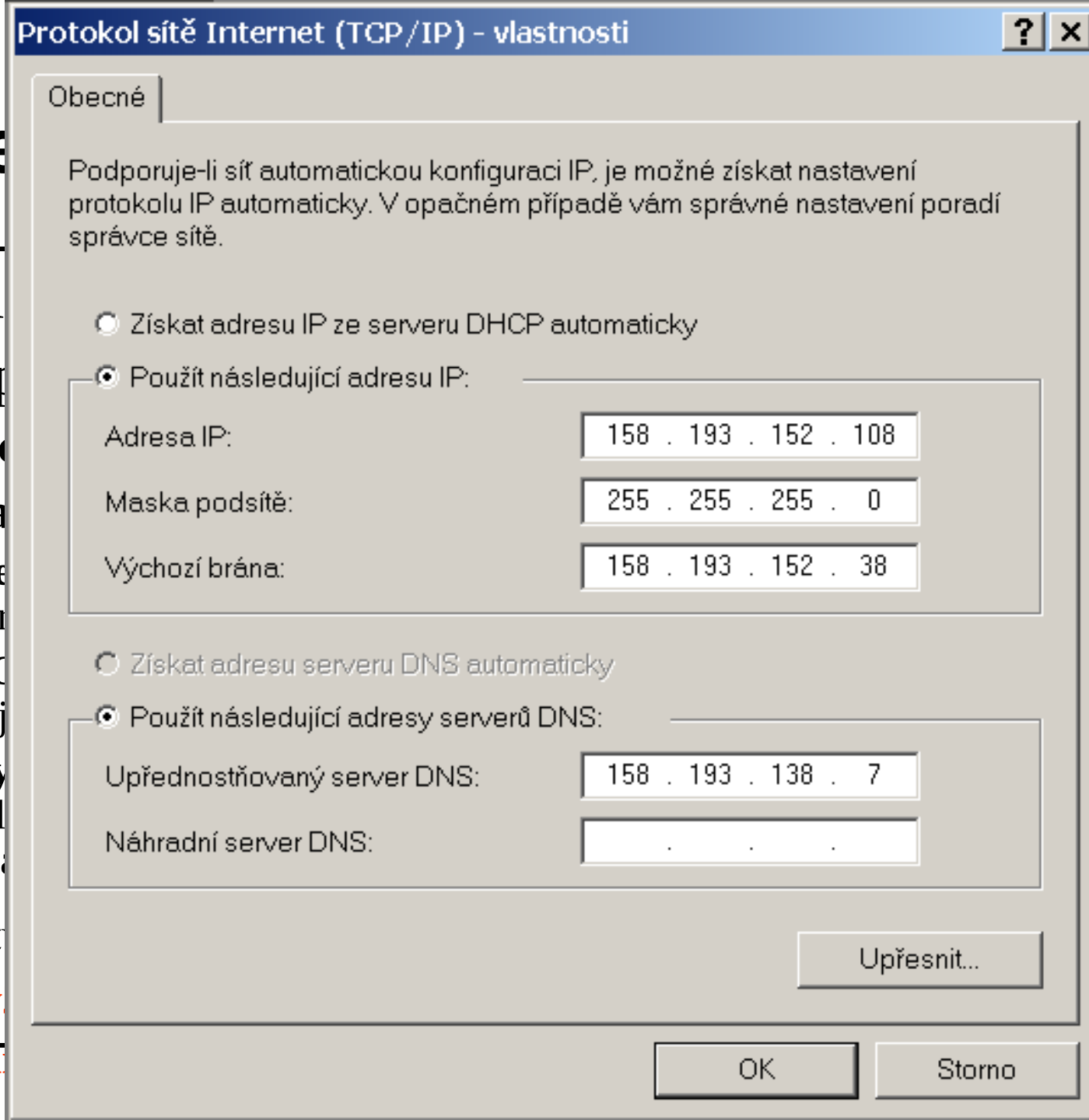
Unicast, Broadcast, Multicast IP adresy

- **Unicast adresa**: identifikuje jedného príjemcu
- Broadcast a Multicast adresa: identifikácia skupiny príjemcov
- **Broadcast adresa**: nemá selektívnu vlastnosť, určené všetkým hostom v sieti, subsieti
- **Anycast**

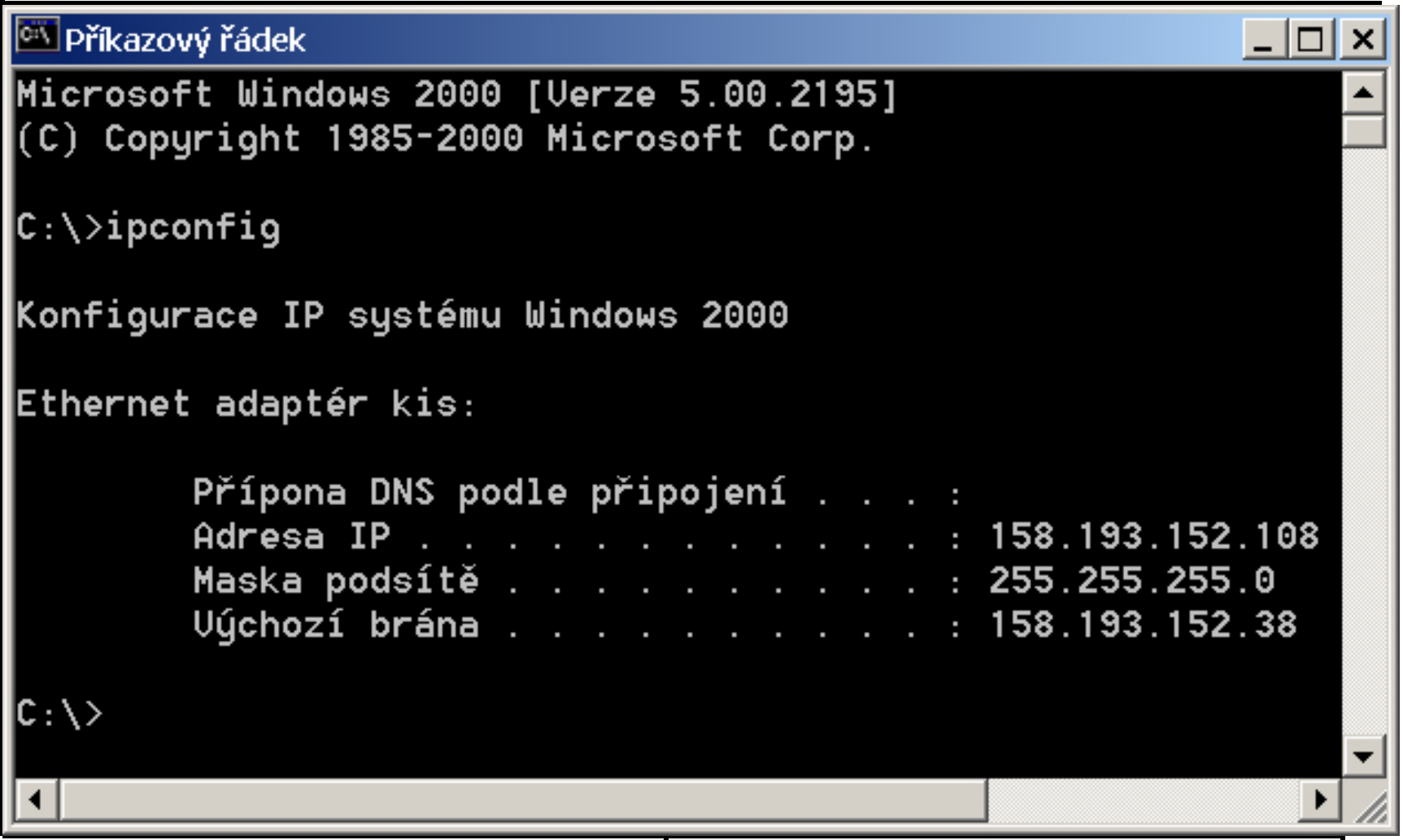
Pride

TCP/IP

- Host ID a
- Spôsoby p
  - 1) **Stati**
  - 2) **Dyna**
    - A) **Re** server
    - B) **BO** svojej
    - C) **Dy** pridel nová
- ako zistiť akt
  - **ipconfig (w**
  - **ifconfig (Li**



Výstup ipconfig



Výstup ifconfig

TCP/IP

Ifconfig>

```
eth0   Link encap:Ethernet  HWaddr 00:04:75:72:57:B1
       inet addr:158.193.152.51  Bcast:158.193.152.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:470952 errors:0 dropped:0 overruns:1 frame:0
       TX packets:41089 errors:0 dropped:0 overruns:0 carrier:1
       collisions:0 txqueuelen:100
       RX bytes:49587592 (47.2 Mb)  TX bytes:37838174 (36.0 Mb)
       Interrupt:5 Base address:0xa400

lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:3924  Metric:1
       RX packets:53 errors:0 dropped:0 overruns:0 frame:0
       TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:27733 (27.0 Kb)  TX bytes:27733 (27.0 Kb)
```

Komunikácia v IP sieťach

1. **V rámci jedného segmentu** (rovnaká IP adresa siete komunikujúcich – Net ID, nie je v ceste Router):
   - musím zistiť fyzickú adresu (napr. MAC) adresu cieľa
2. **Mimo segment**: (zistiť fyzickú adresu next hop zariadenia)
   - cez default gateway/router
   - cez proxy ARP (zvyčajne ním býva router)

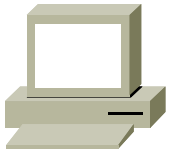
- Riešiť problém prekladu sieťovej adr. na fyzickú adr.
- **Address Resolution Protocol (ARP):** preklad IP adresy (logickej) na adresu linkovej vrstvy (fyzickú)
  - súčasť internet vrstvy, resp. IP protokolu

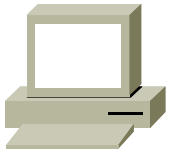
Komunikácia v rámci jedného segmentu

Host A
napr. web browser
IP: 158.193.152.108
S.mask: 255.255.255.0

Host B
napr. lokálny WWW server
IP: 158.193.152.39
S.mask: 255.255.255.0

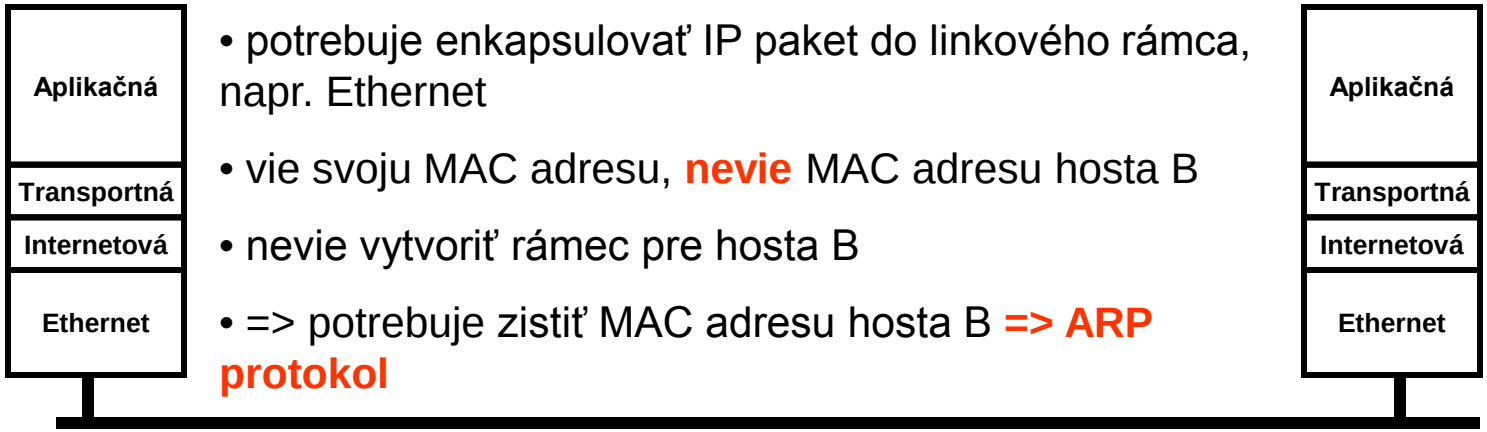
Host A chce komunikovať s hostom B



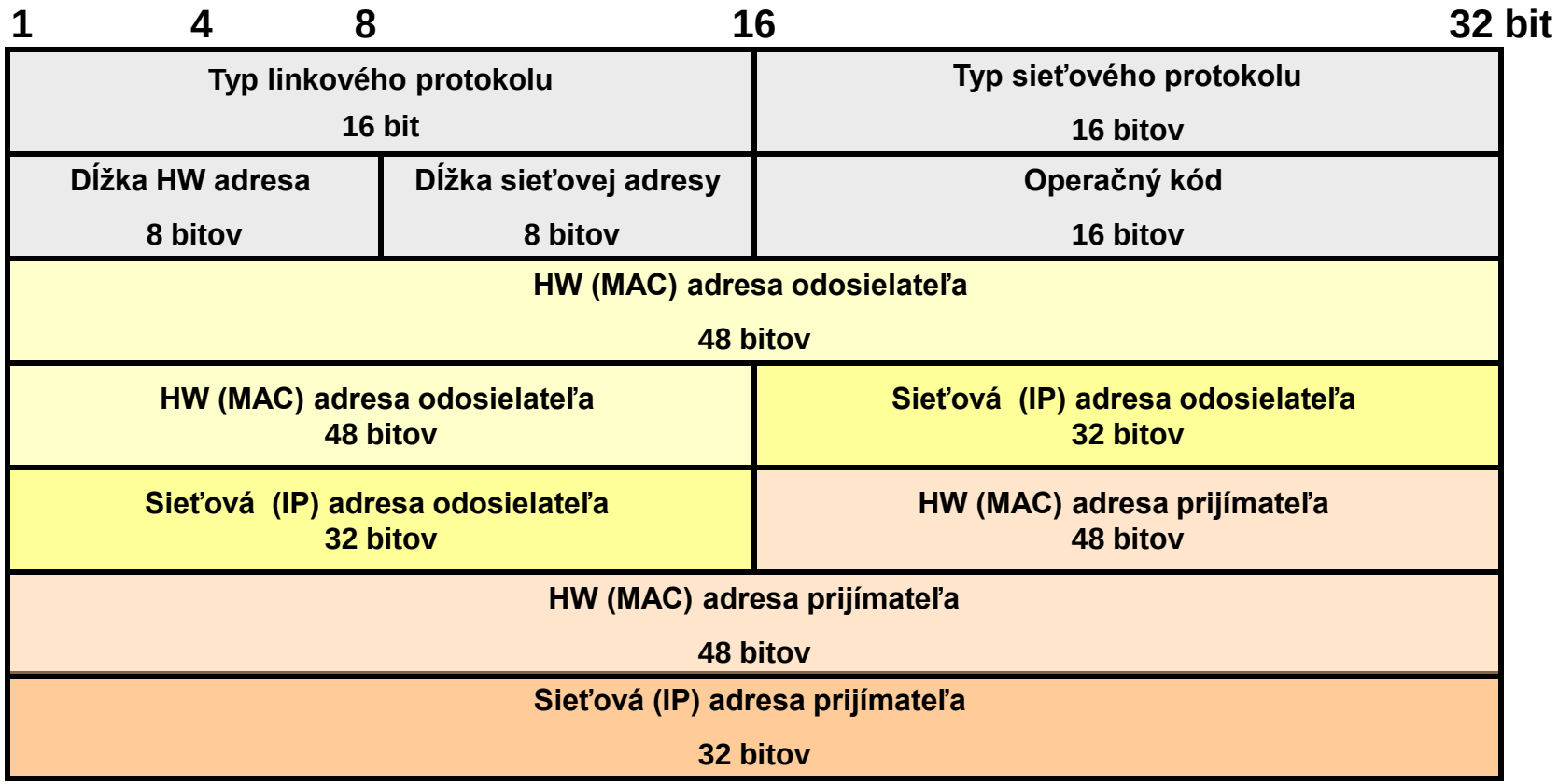


HOST A:

- Vie IP adresu hosta B, aj svoju IP adresu => vie zostaviť IP paket
- potrebuje enkapsulovať IP paket do linkového rámca, napr. Ethernet
- vie svoju MAC adresu, **nevie** MAC adresu hosta B
- nevie vytvoriť rámec pre hosta B
- => potrebuje zistiť MAC adresu hosta B **=> ARP protokol**



ARP rámec



Typ link. protokolu: hodnota 1 Ethernet

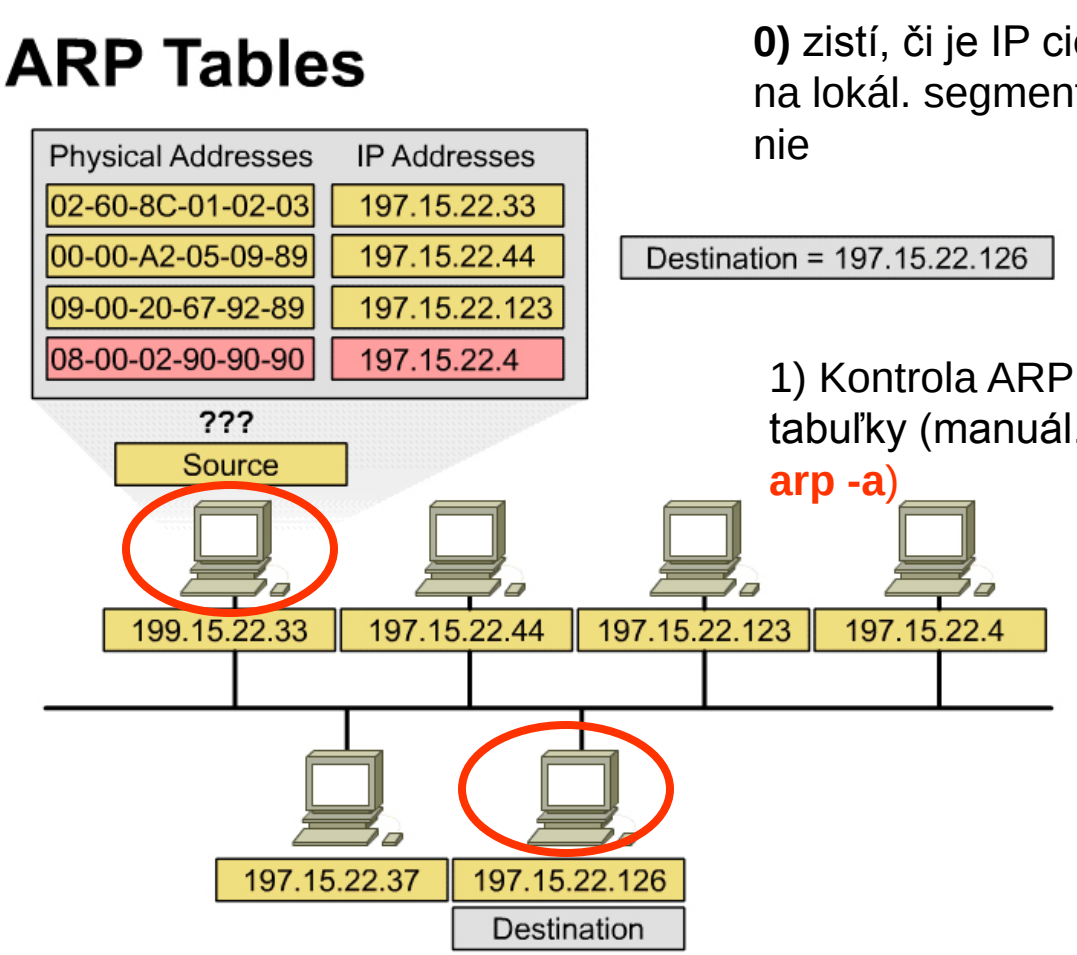
Typ sieťového prot.: 2048 (0x800) IP

Dĺžka MAC adresy: hodnota 6

Dĺžka IP adresy: hodnota 4

Operačný kód: 1 ARP request, 2 ARP reply, 3 RARP request, 4 RARP reply

Address Resolution Protocol (ARP)



0) zistí, či je IP cieľa na lokál. segmente or nie

Destination = 197.15.22.126

1) Kontrola ARP tabuľky (manuál. výpis **arp -a**)

2) Zdrojová stanica vyšle na Broadcast MAC adresu *ARP Request* správu

3) Každá stanica príjme rámec a podá ho vyššej vrstve na spracovanie

4) Stanica s cieľovou IP adresou odpovie zdroju cez *ARP reply*

5) Zdroj pridá mapovanie MAC na IP do tabuľky

6) Ak nie je ARP odpoveď => taká stanica nexistuje => **ERROR**

Komunikácia v rámci jedného segmentu

Host A

napr. web browser

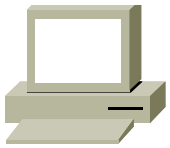
IP: 158.193.152.108

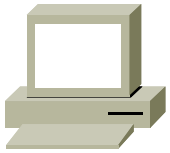
Host B

napr. lokálny WWW server

IP: 158.193.152.39

Host A chce komunikovať s hostom B

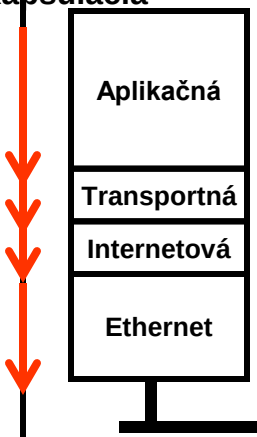


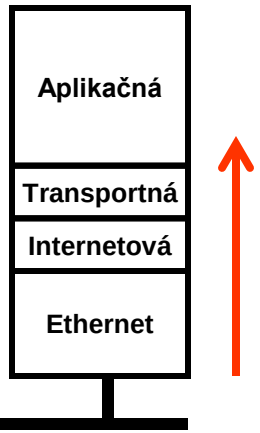


HOST A:

- Vie IP adresu hosta B, aj svoju IP adresu => vie zostaviť IP paket
- potrebuje enkapsulovať IP paket do linkového rámca, napr. Ethernet
- vie svoju MAC adresu, ***VIE*** MAC adresu hosta B
- ***VIE*** vytvoriť rámec pre hosta B

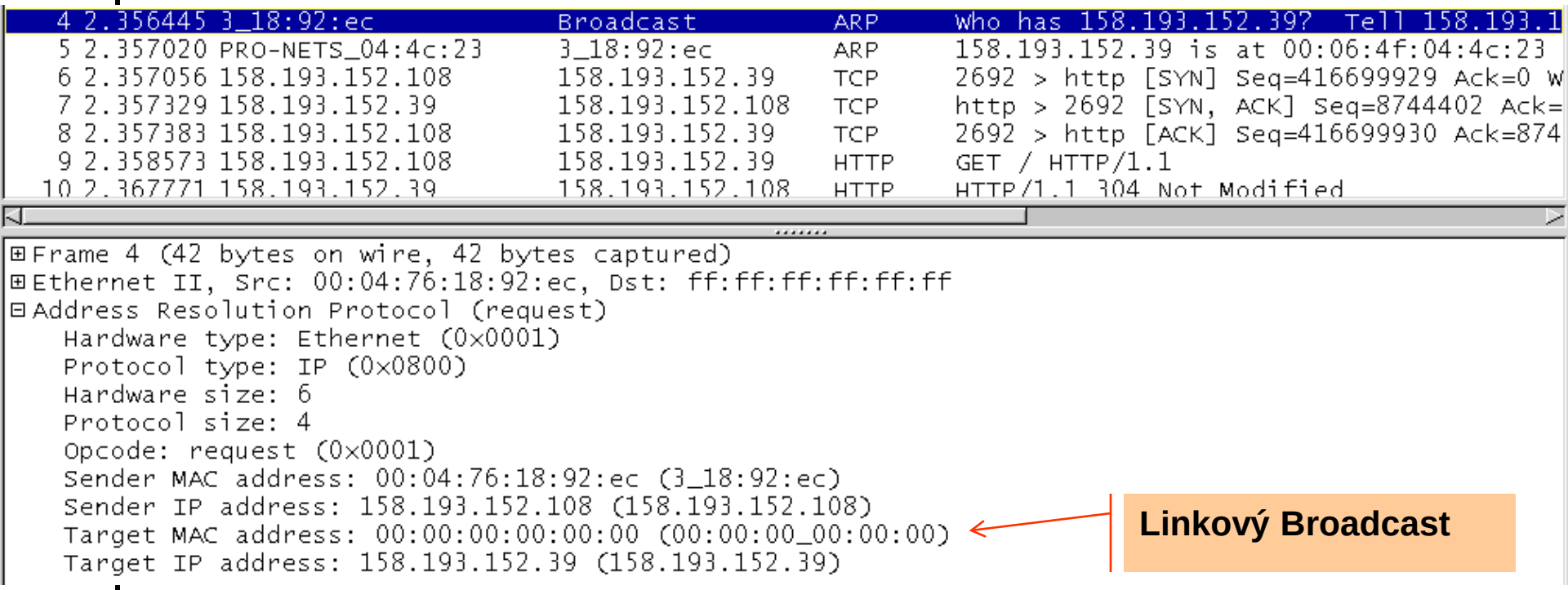
enkapsulácia





Prebehne komunikácia

ARP dotaz z net analyzatora



Linkový Broadcast

Výpis z ARP tabuľky

- Tabuľka si udržuje položky dynamicky (po uplynutí intervalu ich maže)

- **arp –a (**win, linux**)**

  Rozhraní: 158.193.152.108 on Interface 0x1000004

  internetová adresa fyzická adresa typ

PC s nikým dlhšie nekomunikoval

- **arp -a**

  Rozhraní: 158.193.152.108 on Interface 0x1000004

  internetová adresa fyzická adresa typ

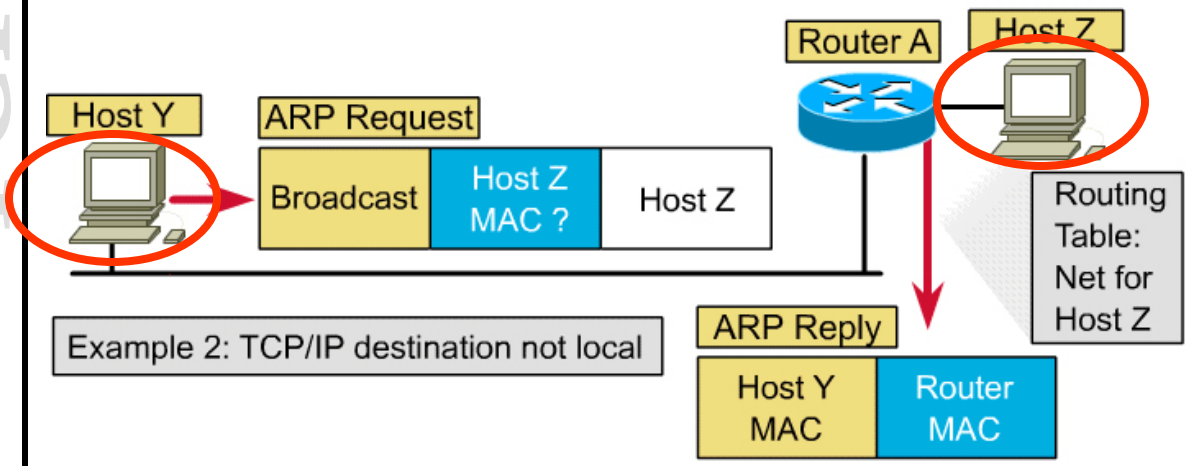
  158.193.152.38 00-e0-29-3c-35-56 dynamická

  158.193.152.39 00-06-4f-04-4c-23 dynamická

  158.193.152.51 00-04-75-72-57-b1 dynamická

Po komunikácií

Komunikácia mimo segment
Proxy ARP



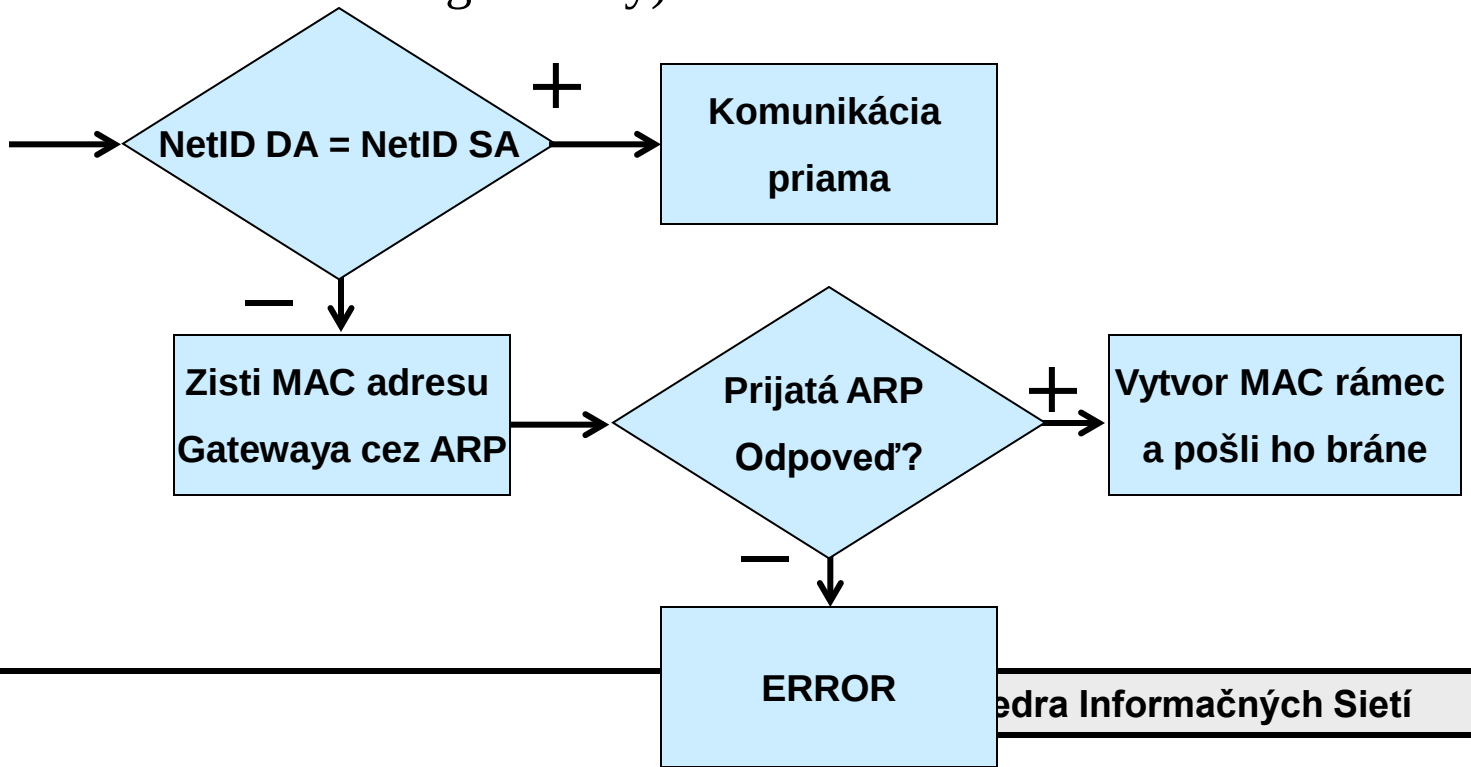
ARP request je **broadcast** rámec, router broadcasty filtruje a neprepúšťa ich na výstupné porty

Router stanici **Y** odpovie na ARP dotaz svojou MAC adresou a vystupuje v komunikácii ako proxy

Na Routry musí bežať Proxy démon

Komunikácia mimo segment default gateway / router

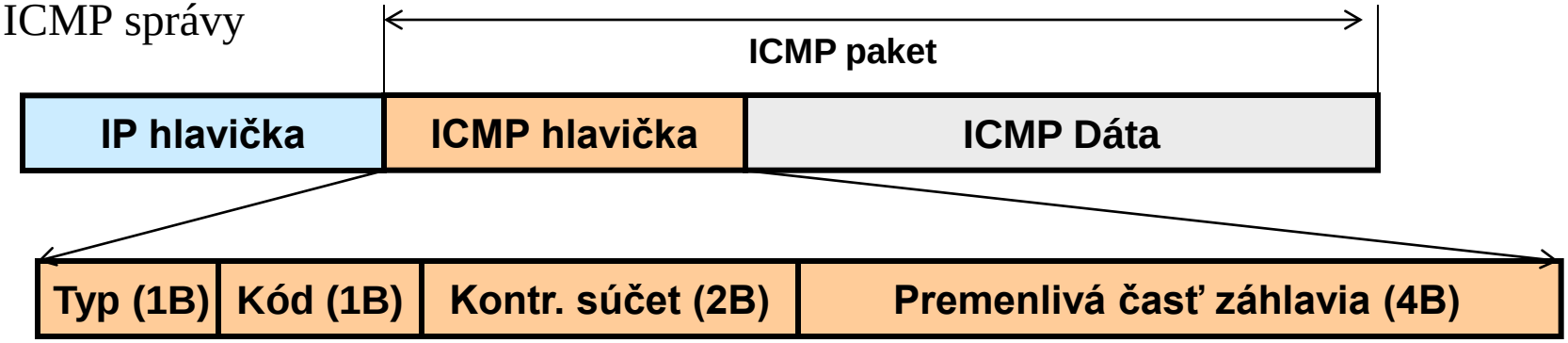
- Host pozná:
  - Svoju IP adresu (SA), cieľovú IP adresu (DA)
  - Svoju MAC adresu (SMA)
  - IP adresu smerovača / brány (alebo zistí ARP procesom pre zadanú IP adresu gw-brány)



Internet Control Message Protocol (ICMP)

TCP/IP

- Súčasť IP protokolu
- ICMP správy enkapsulované priamo do IP paketu
- použitie: signalizácia rôznych situácií, chýb
- ICMP správy



- Nedoručiteľný IP datagram (T=3)

(viac správ odlíšených kódom)

- Zníž rýchlosť odosielania (T=8)

(viac správ odlíšených kódom)

- Zmeň smerovanie (T=5)

(viac správ odlíšených kódom)

- Žiadosť o Echo (T=8,K=0)
- Odpoveď na Echo (T=0,K=0)
- Odpoveď na žiadosť o smerovaní (T=9,K=0)
- Žiadosť na smerovanie (T=10,K=0)
- Čas vypršal (T=11)

(viac správ odlíšených kódom)

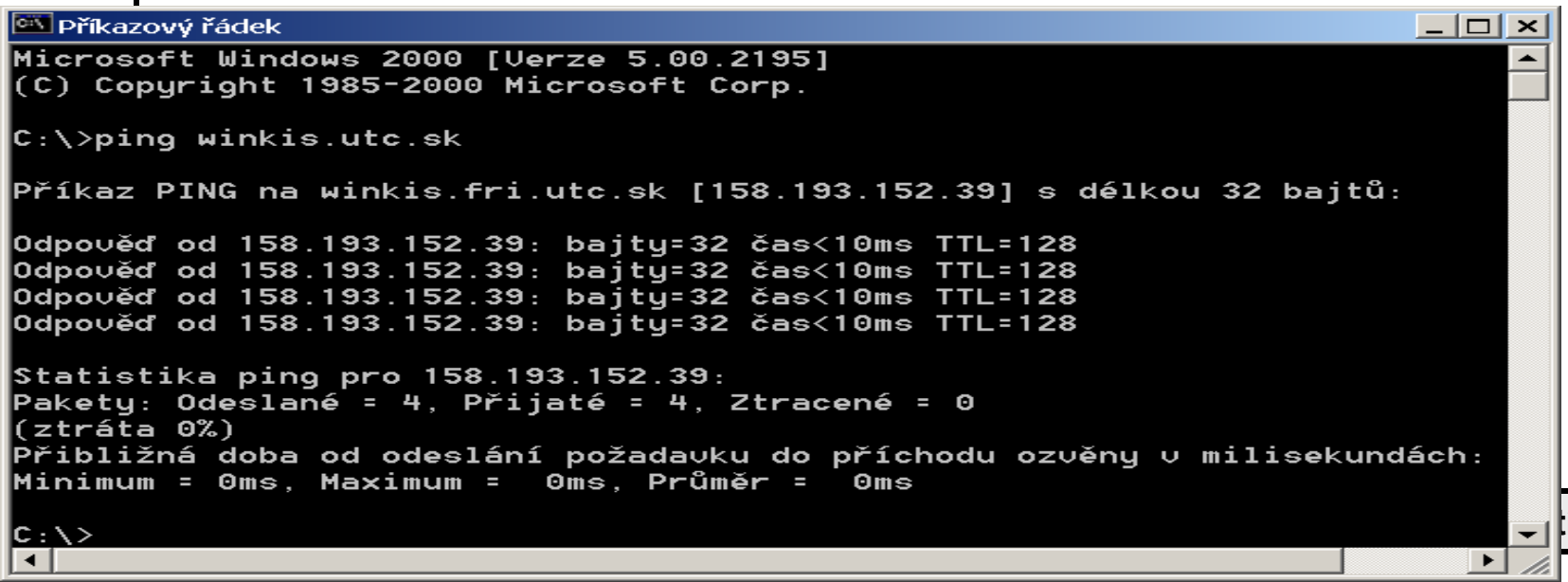
- Chybný parameter (T=12)

(viac správ odlíšených kódom)

- Požiadavka a odpoveď na čas. synchro
- Žiadosť o masku podsiete a odpoveď

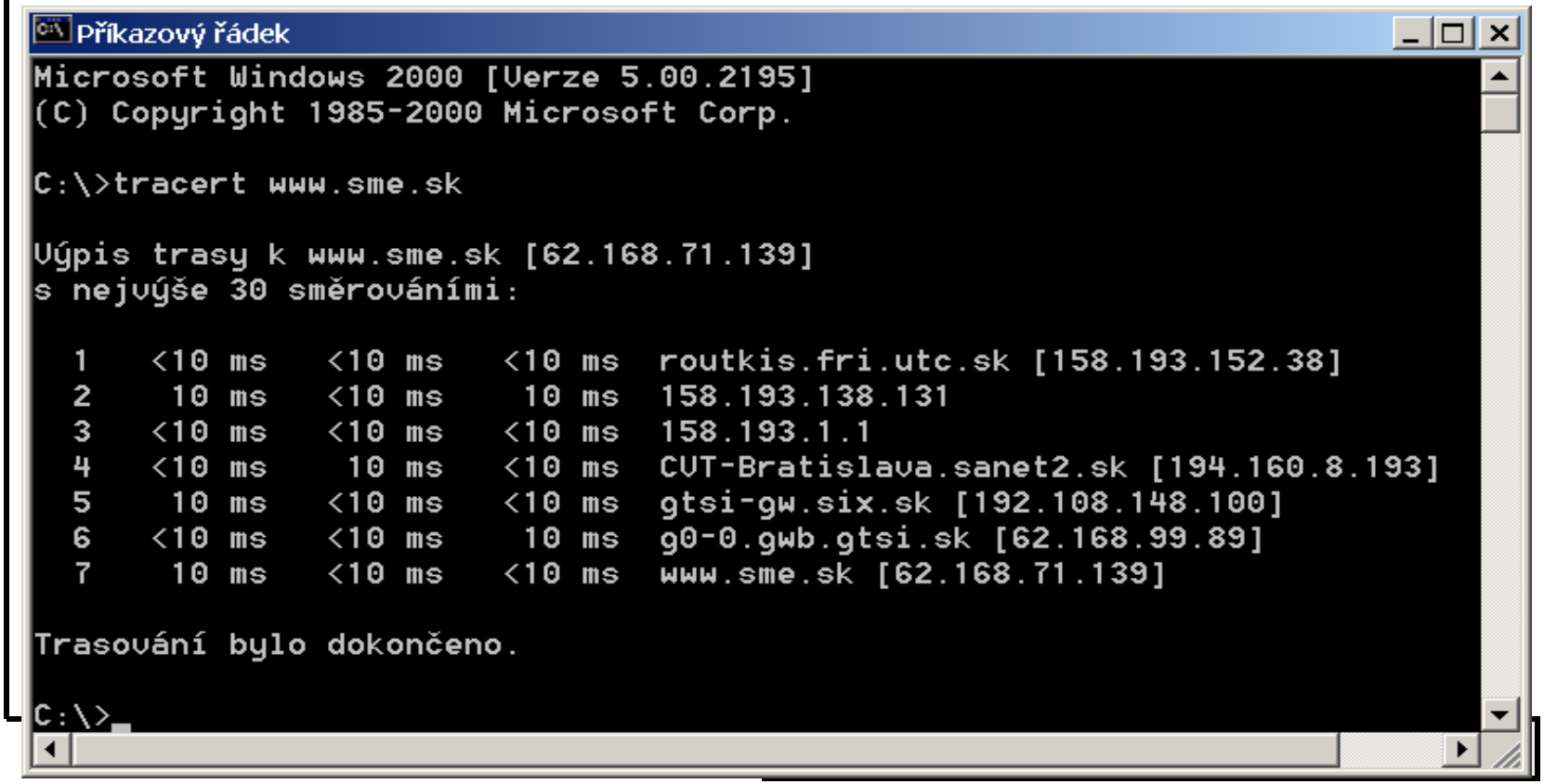
Ping

- Najznámejšia aplikácia ICMP protokolu
- Ping (Packet InterNet Groper)
  - testuje sieťovú dostupnosť hosta
  - používa ICMP echo, ICMP echo reply
  - príkaz: **ping [-switches] host_adress [size [packets]]**

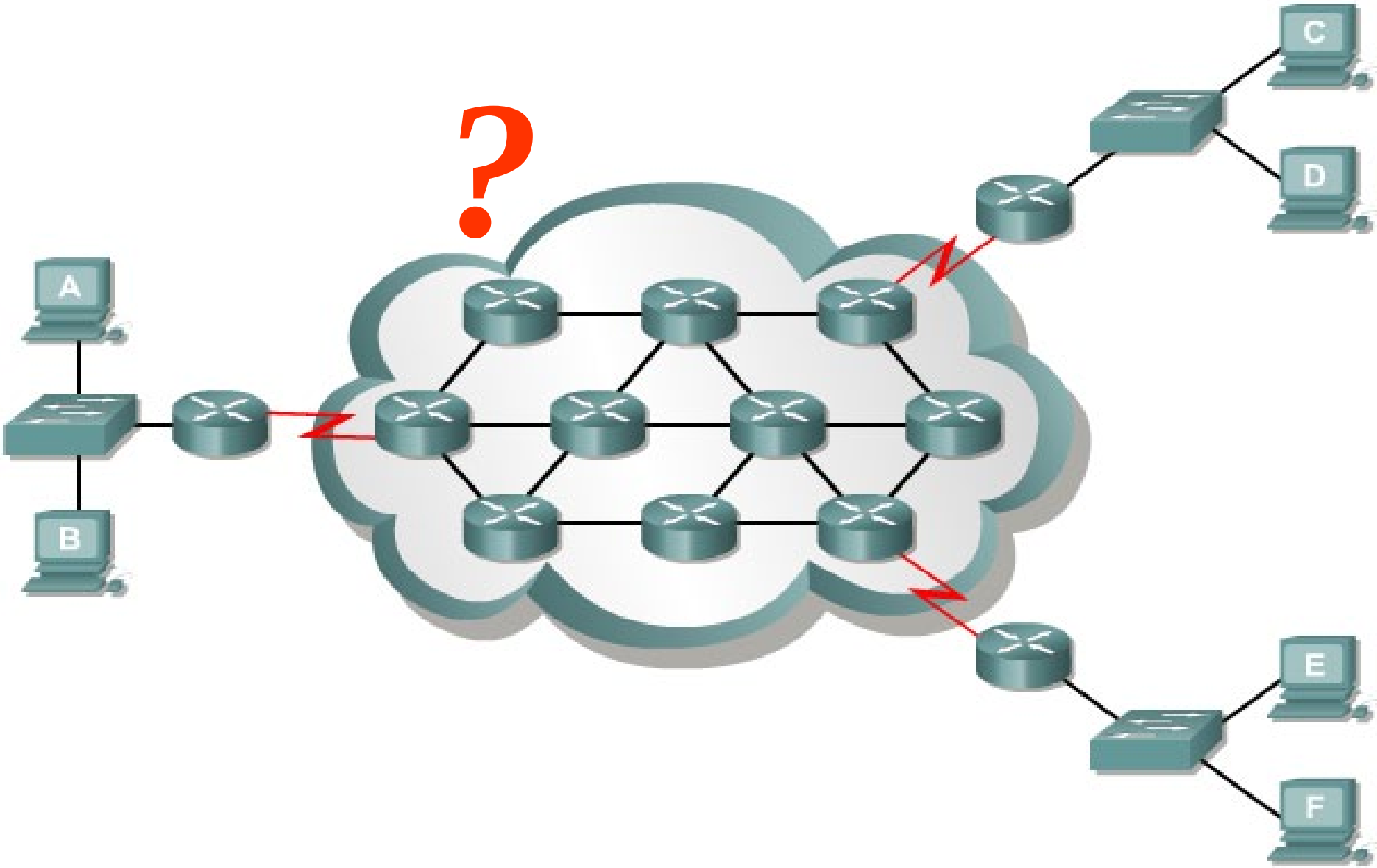


Traceroute

- Debugovanie sieťového spojenia
- zisťovanie cesty IP datagramov od daného hosta po cieľový host
- Príkaz: traceroute (linux) tracert (w2k) (pathping w2k)



Smerovanie



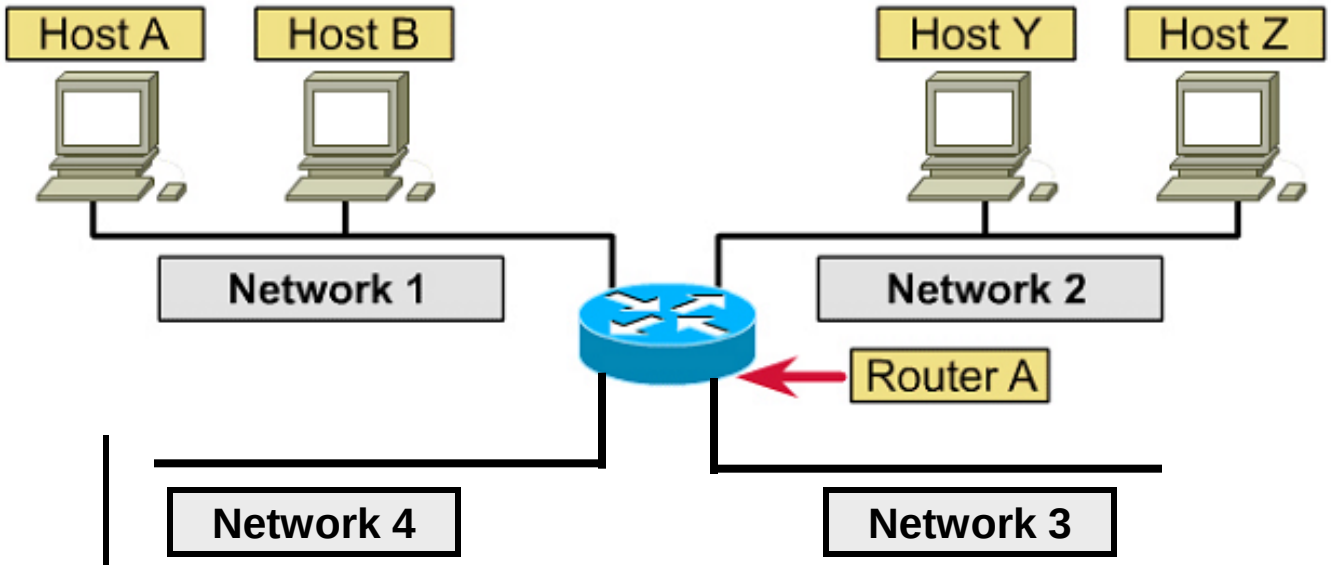
Smerovanie IP paketu - IP routing

- **Smerovanie**: proces výberu ďalšej cesty paketu na základe informácií v hlavičke paketu
  - **Priame** (direct routing): medzi dvomi stanicami na jednej sieti (rovnaké netID)
  - **Nepriame** (indirect routing): prostredníctvom smerovača
- smerovanie vykonávané na základe obsahu smerovacej tabuľky
- tabuľka budovaná:
  - **staticky**: manuálne zadávané položky (pre väčšie siete pracné, použitie stub nets)
  - **dynamicky**: pomocou smerovacích protokolov
- smerovanie vykonáva smerovač
- smerovač:
  - číta IP hlavičku paketu, ale nemení IP adresy !!!

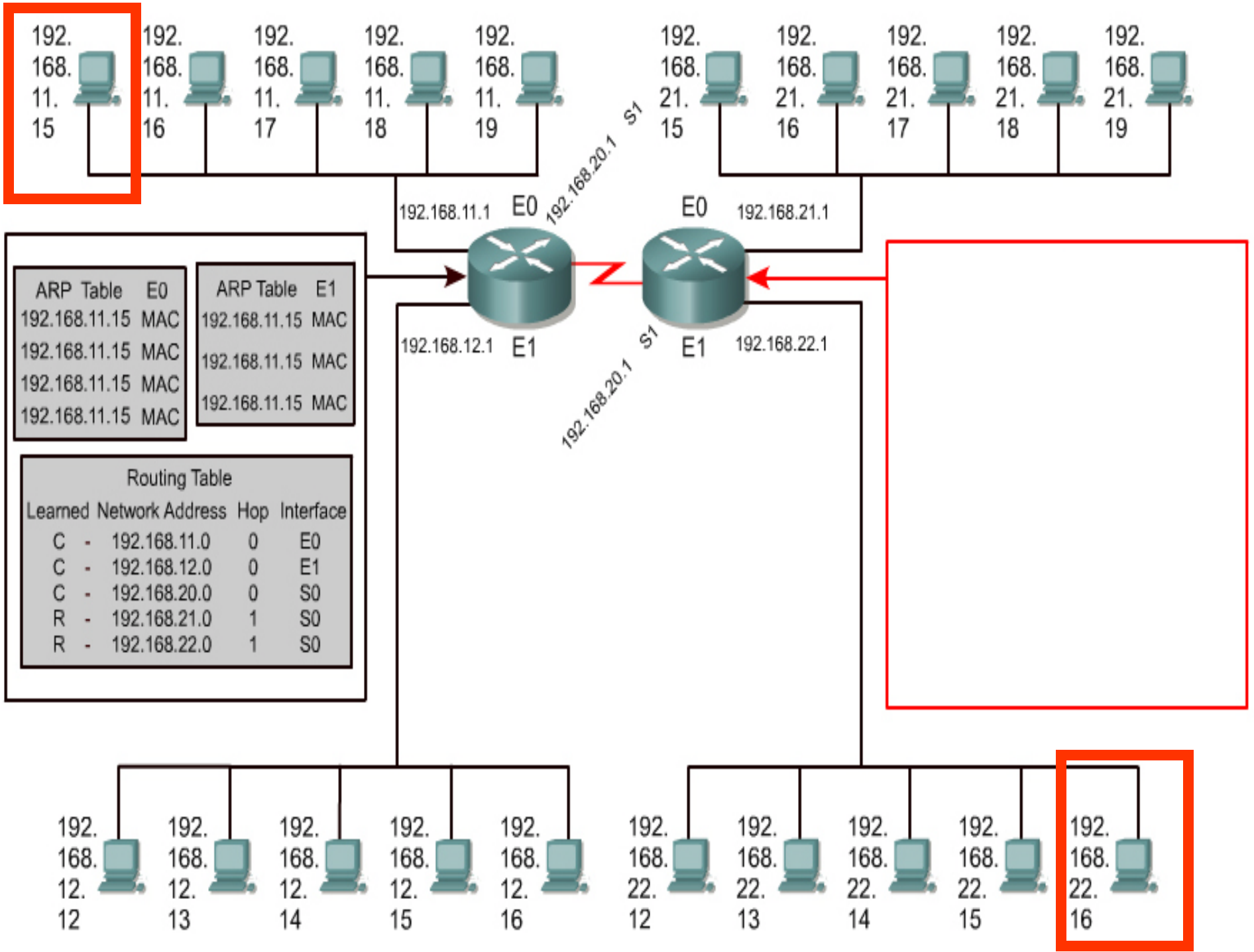
Priame smerovanie

- Cieľová IP adresa AND maska siete
- ak výsledok zhodný s adresou siete odosielateľa = priame smerovanie
- prebehne proces priamej komunikácie (ARP atď)

Nepriame smerovanie - komunikácia cez smerovač

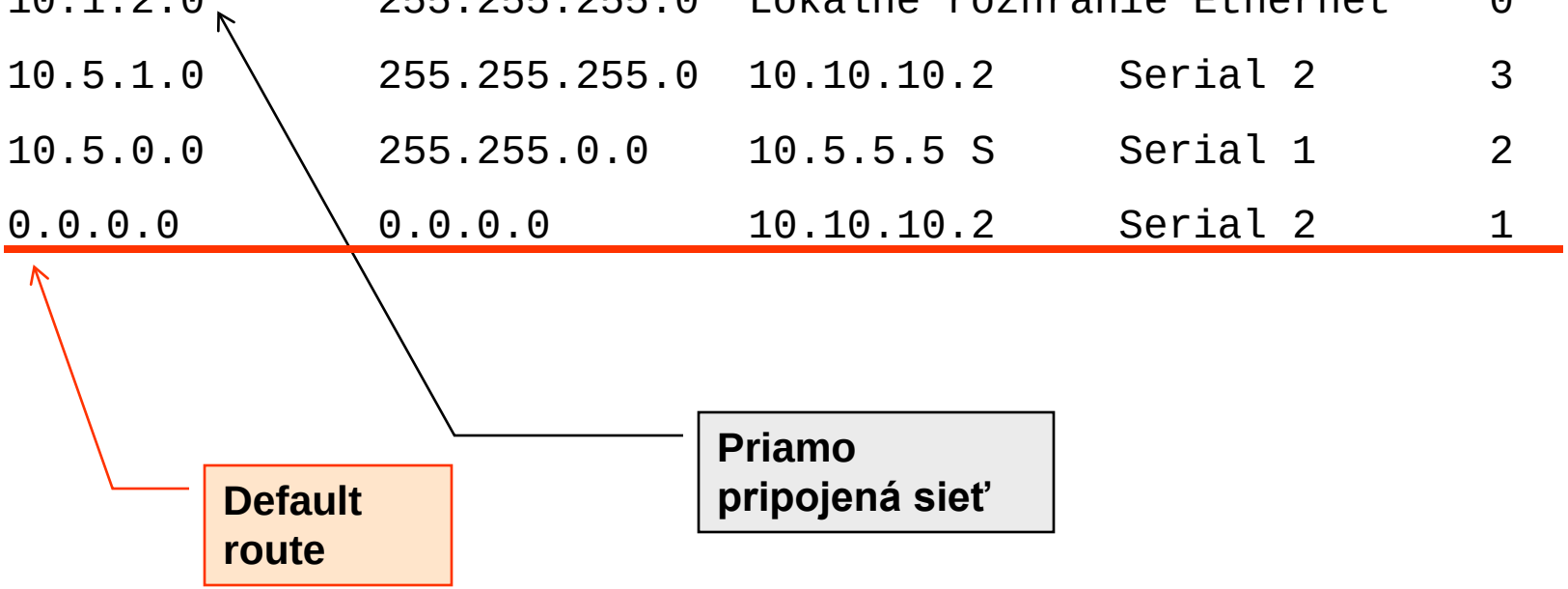


1. Cieľ. adresa AND maska
2. Host v inej sieti
3. Paket musí byť poslaný smerovaču
4. Musí prebehnúť ARP proces zisťovania link adresy smerovača
5. Vytvorenie rámca
6. Odoslanie rámca smerovaču
7. Spracovanie paketu z rámca, výber cesty
8. Odoslanie rámca


192.168.11.15
192.168.11.16
192.168.11.17
192.168.11.18
192.168.11.19
192.168.21.15
192.168.21.16
192.168.21.17
192.168.21.18
192.168.21.19
192.168.20.1 S1
192.168.11.1 E0
E0 192.168.21.1
192.168.12.1 E1
S1 E1 192.168.22.1
192.168.20.1
ARP Table E0
192.168.11.15 MAC
192.168.11.15 MAC
192.168.11.15 MAC
192.168.11.15 MAC
ARP Table E1
192.168.11.15 MAC
192.168.11.15 MAC
192.168.11.15 MAC
Routing Table
Learned Network Address Hop Interface
C - 192.168.11.0 0 E0
C - 192.168.12.0 0 E1
C - 192.168.20.0 0 S0
R - 192.168.21.0 1 S0
R - 192.168.22.0 1 S0
192.168.12.12
192.168.12.13
192.168.12.14
192.168.12.15
192.168.12.16
192.168.22.12
192.168.22.13
192.168.22.14
192.168.22.15
192.168.22.16

Smerovacia tabuľka

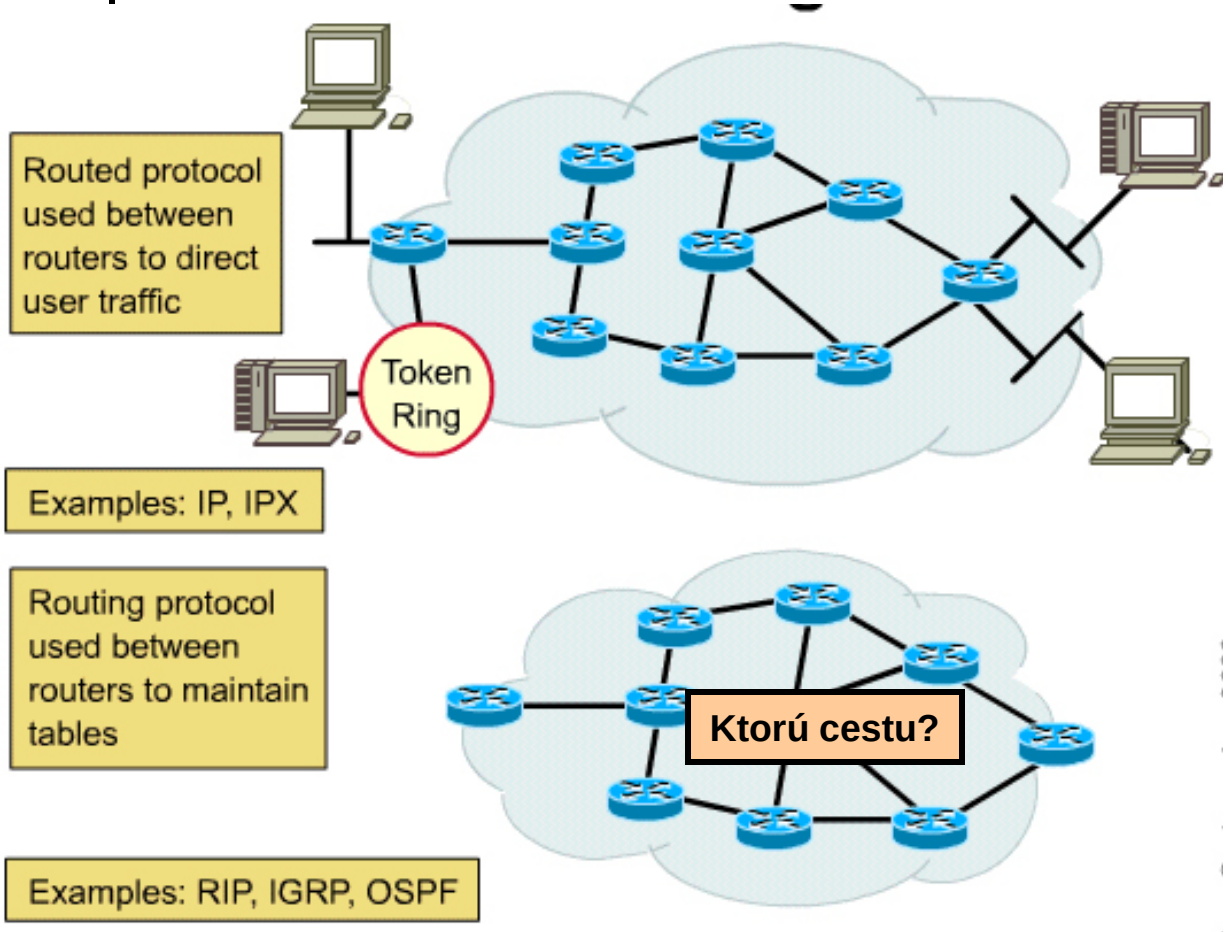
Sieť	Maska	Next Hop	Sieťové rozhranie	Metrika
192.168.1.0	255.255.255.0	192.168.254.5	Serial 1	4
10.1.2.0	255.255.255.0	Lokálne rozhranie Ethernet		0
10.5.1.0	255.255.255.0	10.10.10.2	Serial 2	3
10.5.0.0	255.255.0.0	10.5.5.5 S	Serial 1	2
0.0.0.0	0.0.0.0	10.10.10.2	Serial 2	1



Statické smerovacie tabuľky

- Statické
  - Vyžaduje manuálnu konfiguráciu
  - Nedokáže sa automaticky prispôsobiť zmeneným podmienkam v sieti (manual. zásah)
  - Pre siete s jednou cestou do/zo siete
  - Žiadne dáta
  - bezpečnosť

Dynamické smerovacie protokoly

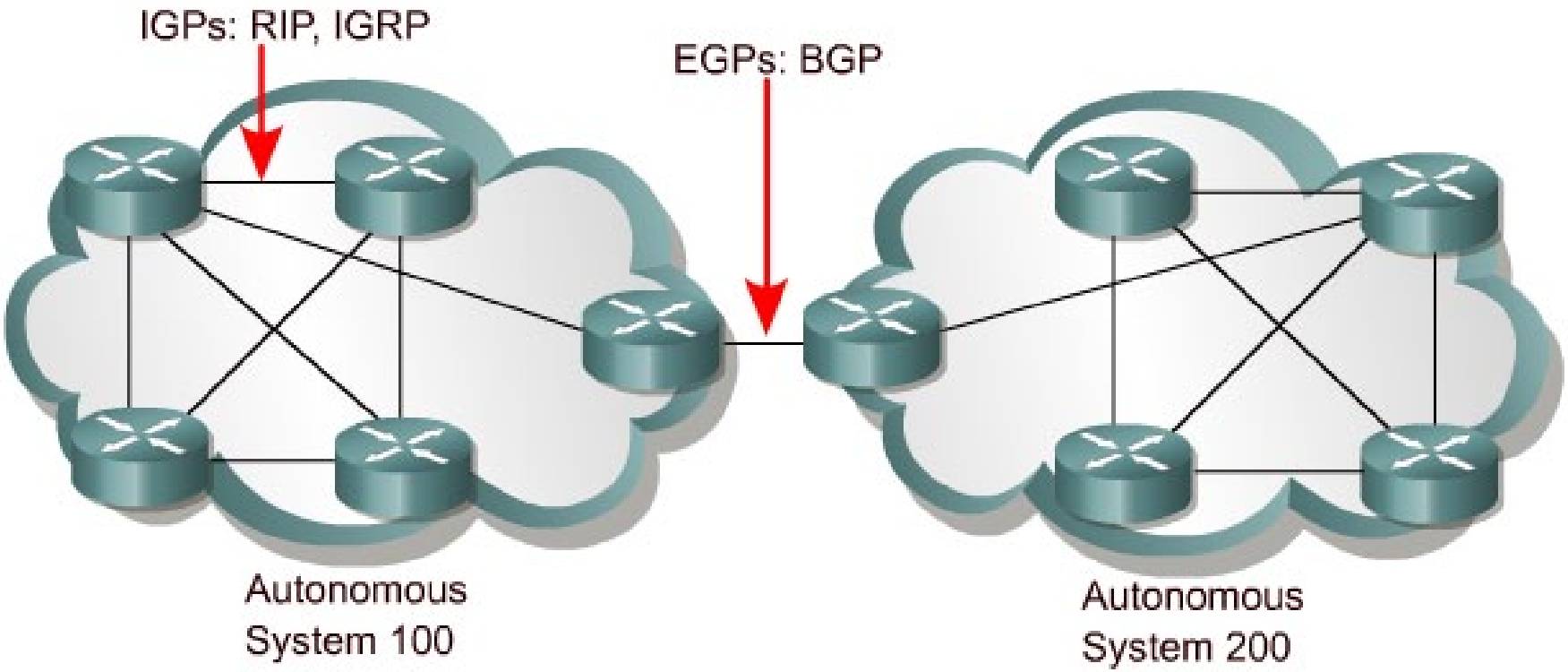


- Používané na výmenu smerovacích tabuliek a zdieľanie smerovacích informácií
- Umožňujú smerovaču vybrať vhodnú cestu
- Použité rôzne algoritmy => generujú hodnotu metriky
- Čím nižšie metrika pre danú cestu, tým lepšie
- **Metrika** na výber cesty
  - Hop count
  - Delay
  - Bandwidth
  - Utilization
  - Cena ...

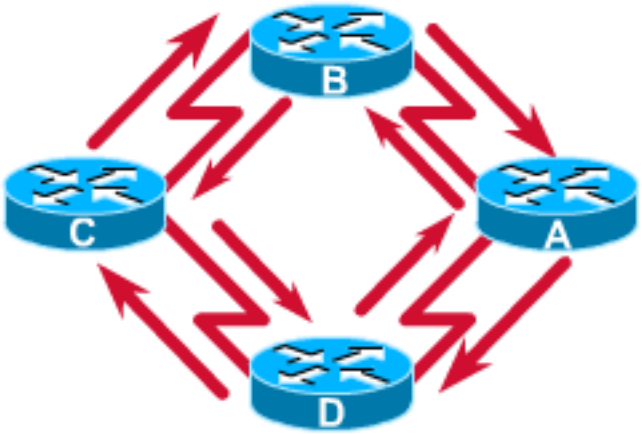
Dynamické smerovacie protokoly

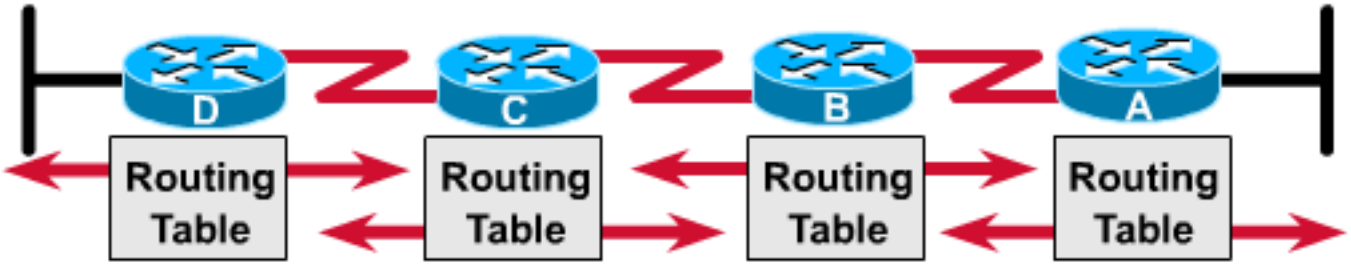
- Typy podľa použitého algoritmu:
  - **1) Distance vector protocols:** Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP),
  - **2) Link State Protocols:** Open Shortest Path First (OSPF)
  - **3) Hybridné smerovacie protokoly** (mix 1 a 2, EIGRP)
- Iné členenie:
  - 1) **Interior Routing Protocols**: RIP, IGRP, EIGRP, OSPF
  - 2**) Exterior Routing Protocols:** Border Gateway Protocol

IGP & EGP


IGPs: RIP, IGRP
EGPs: BGP
Autonomous
System 100
Autonomous
System 200

Distance vector



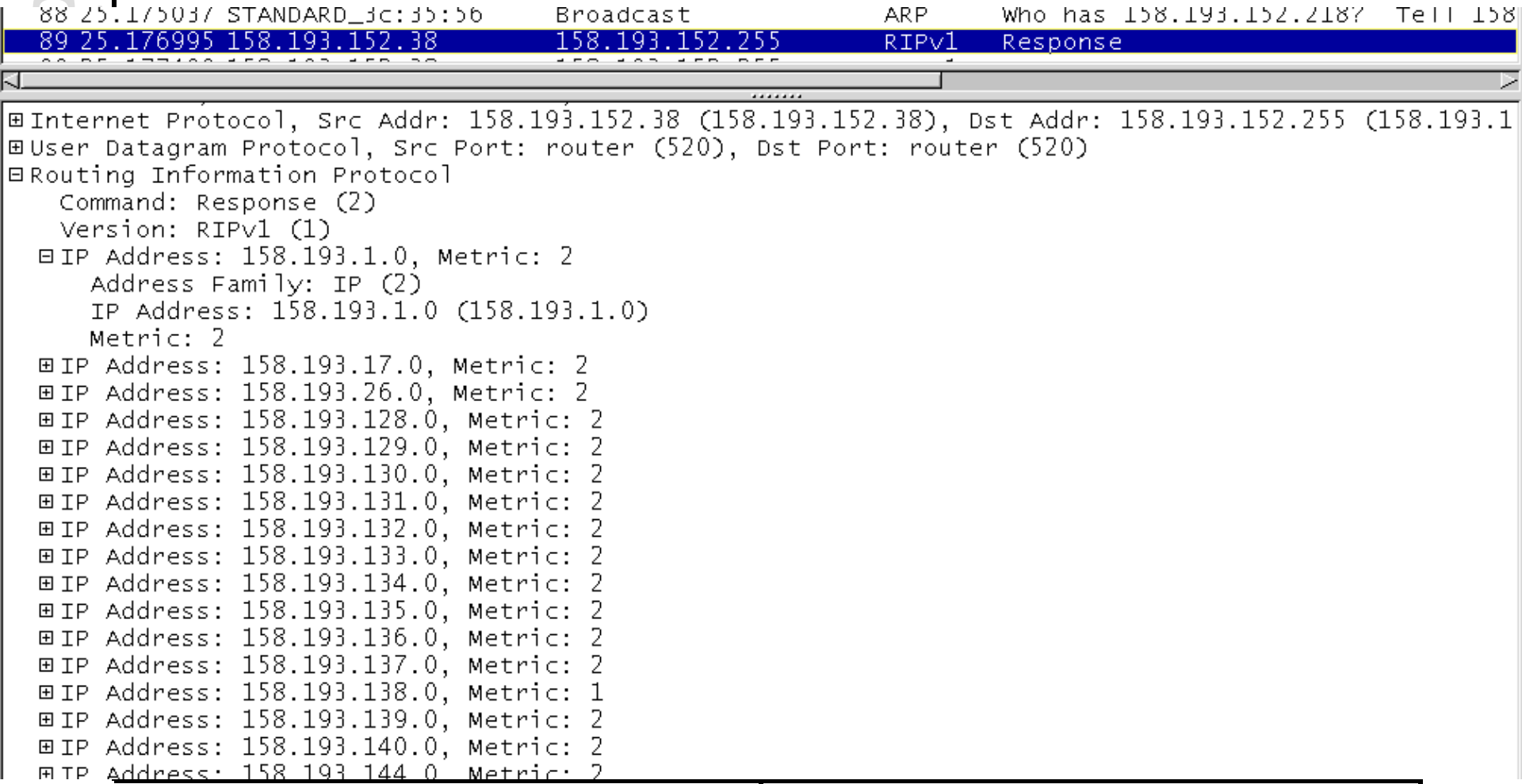


- vektor je cieľová sieť, cez ktorý hop a metrika
- Periodický update smerovacích tabuliek medzi susedmi
- z tab. sa vyberá najnižšia hodnota pre danú cestu, smer
- hodnota sa kumuluje
- pomalá konvergencia
- možnosť vzniku slučiek (split horizon, defin. max. počet hopov, hold down timers, spúšťaný update)
- router nemá komplexnú znalosť siete

Routing Information Protocol (RIP)

- Distance vector
- jediná metrika počet „hopov“
- update každých 30 sekúnd (v pakete je jeho route tabuľka (RIPv1) a sieťová maska (RIPv2))
- maximálny počet „hopov“ 15 (použitie pre malé siete, nad 15 je sieť klasifikovaná ako nedostupná)
- nie vždy vyberie najrýchlejšiu cestu (nezohľadňuje faktory ako zaťaženie linky, priepustnosť a podobne)
- generuje veľa prevádzky
- pomalšia konvergencia

RIP

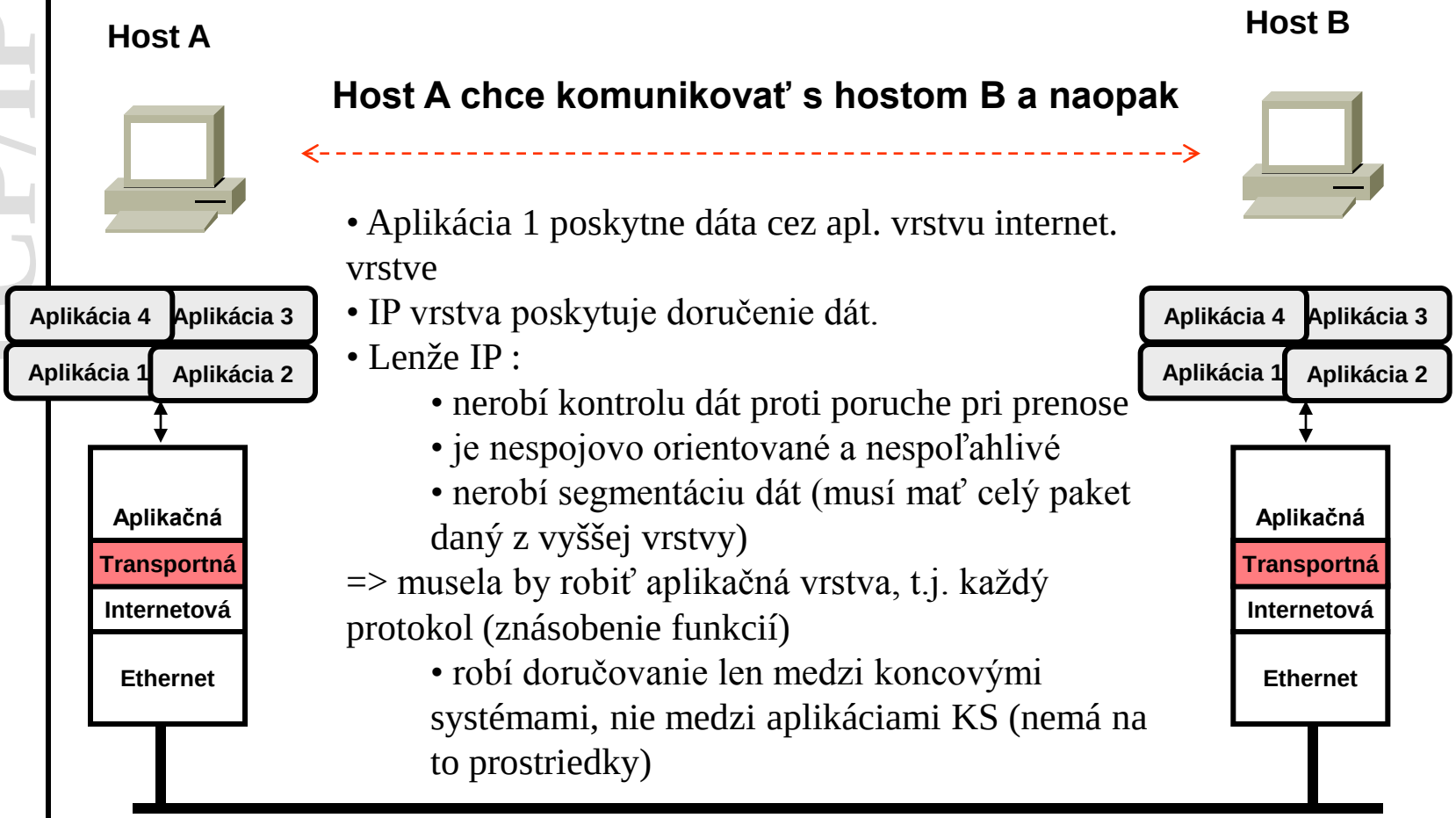

88 25.175037 STANDARD_3c:35:56 Broadcast ARP Who has 158.193.152.218? Tell 158
89 25.176995 158.193.152.38 158.193.152.255 RIPv1 Response
Internet Protocol, Src Addr: 158.193.152.38 (158.193.152.38), Dst Addr: 158.193.152.255 (158.193.1
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
Command: Response (2)
Version: RIPv1 (1)
IP Address: 158.193.1.0, Metric: 2
Address Family: IP (2)
IP Address: 158.193.1.0 (158.193.1.0)
Metric: 2
IP Address: 158.193.17.0, Metric: 2
IP Address: 158.193.26.0, Metric: 2
IP Address: 158.193.128.0, Metric: 2
IP Address: 158.193.129.0, Metric: 2
IP Address: 158.193.130.0, Metric: 2
IP Address: 158.193.131.0, Metric: 2
IP Address: 158.193.132.0, Metric: 2
IP Address: 158.193.133.0, Metric: 2
IP Address: 158.193.134.0, Metric: 2
IP Address: 158.193.135.0, Metric: 2
IP Address: 158.193.136.0, Metric: 2
IP Address: 158.193.137.0, Metric: 2
IP Address: 158.193.138.0, Metric: 1
IP Address: 158.193.139.0, Metric: 2
IP Address: 158.193.140.0, Metric: 2

Link State protokoly

- *link-state advertisements (LSAs)* pakety (určené všetkým routrom)
- Topologická databáza (smerovač má znalosť siete)
- SPF algoritmus (Dijkster), a výsledný SPF strom
- Smerovacia tabuľka pre každú cestu (presná znalosť siete)

- V počiatku veľká záťaž => potom len updates pri topo zmenách
- Väčšie pamäťové nároky
- Rýchla konvergencia
- Rôzne parametre na určenie metriky (lepšie smerovacie rozhodnutie)

Prečo treba transportnú vrstvu?



- Aplikácia 1 poskytne dáta cez apl. vrstvu internet. vrstve
- IP vrstva poskytuje doručenie dát.
- Lenže IP :
  - nerobí kontrolu dát proti poruche pri prenose
  - je nespojovo orientované a nespoľahlivé
  - nerobí segmentáciu dát (musí mať celý paket daný z vyššej vrstvy)

=> musela by robiť aplikačná vrstva, t.j. každý protokol (znásobenie funkcií)

  - robí doručovanie len medzi koncovými systémami, nie medzi aplikáciami KS (nemá na to prostriedky)

- ako rozlíšiť ktorej aplikácii patria ktoré dáta??

Transportná vrstva

- Zabezpečuje transport dát aplikácií
- Multiplexovanie dát
- poskytuje end-to-end
  - spoľahlivý (Transmission Control Protocol (TCP))
  - aj nespoľahlivý transport dát (User Datagram Protokol (UDP))
  - riadenie toku (sliding window)
- zavádza pojem „portu“, resp. portového čísla (na odlíšenie komunikácií aplikačných protokolov vyššej vrstvy)

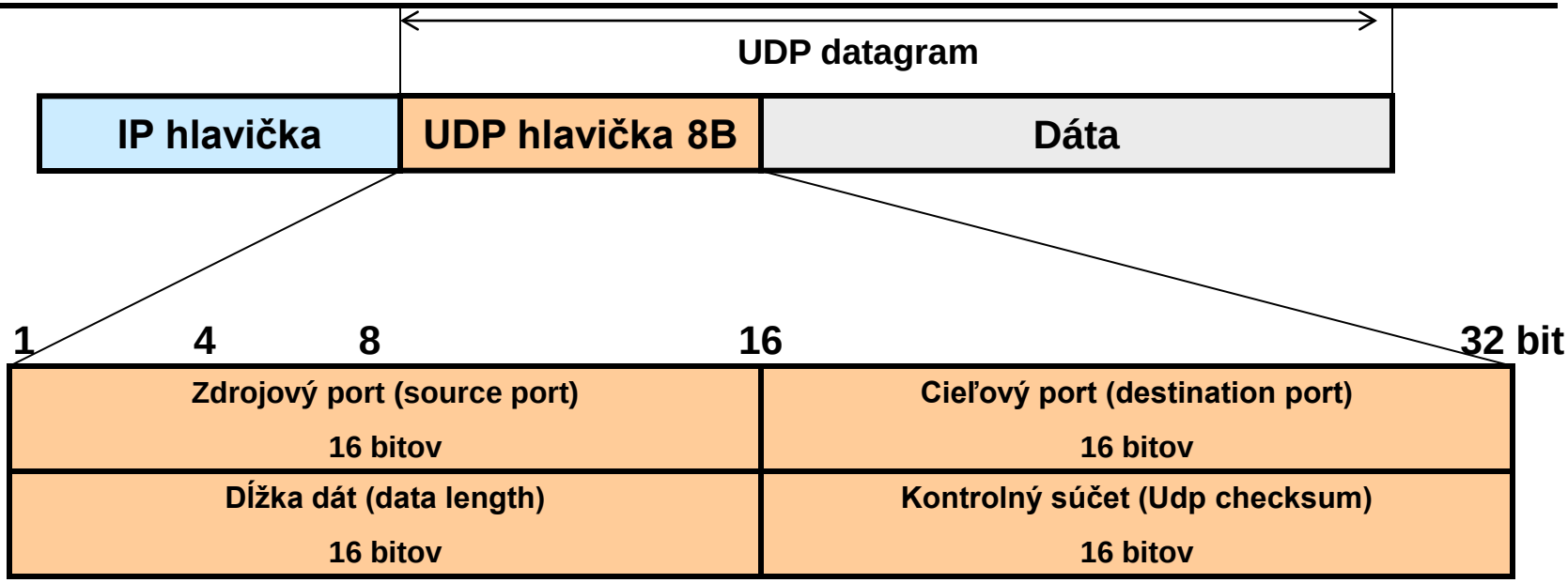
Portové čísla

- Používa aj TCP a UDP, aj keď nezávisle (napr. služba UDP port: 2000 nemusí byť rovnaká ako TCP služba port: 2000)
- Použitie:
  - odlíšenie rozdielnych komunikácií, ktoré prebiehajú v rovnakom čase
  - Protokol (TCP or UDP) + zdrojová (cieľová) IP adresa + zdrojový (cieľový) port = SOCKET (identifikácia komunikačnej služby na lokálnom systéme)
- delenie:
  - čísla < 1023: rezervované pre verejné, všeobecne známe aplikácie (napr. FTP 21, Telnet 23, SMTP 25, DNS 53, WWW 80, POP 110)
  - čísla > 1023: neregulované
- pri nadväzovaní spojenia zvyčajne source port # nad 1023

User Datagram Protocol (UDP)

- Poskytuje nespojovú službu prenosu správ (datagramov) s nezaručenou spoľahlivosťou
  - t.j. nerobí kontrolu doručenia datagramu
  - nerobí kontrolu dátového toku
  - nerobí potvrdzovanie
- použitie:
  - posielanie datagramov medzi aplikačnými procesmi
  - rozlišuje medzi viacerými procesmi na danom počítači
- UDP nerobí segmentáciu dát => dáta musia byť rozdelené na prenos vyššou vrstvou, resp. pri prijatí poskladané do dátového toku vyššou vrstvou

UDP datagram



Source port: identifikátor vysielacieho procesu
Destination port: cieľový port
Total length: dĺžka UDP datagramu
UDP checksum: kontrolná suma cez celý datagram

Príklad UDP datagramu

```
⊞Frame 54 (491 bytes on wire, 491 bytes captured)
⊞Ethernet II, Src: 00:04:76:18:92:ec, Dst: 00:e0:29:3c:35:56
⊞Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 195.37.77.101 (195.37.77
⊟User Datagram Protocol, Src Port: 2729 (2729), Dst Port: 5060 (5060)
    Source port: 2729 (2729)
    Destination port: 5060 (5060)
    Length: 457
    Checksum: 0xbb82 (correct)
⊟Session Initiation Protocol
    Request line: REGISTER sip:palo SIP/2.0
  ⊞Message Header
```

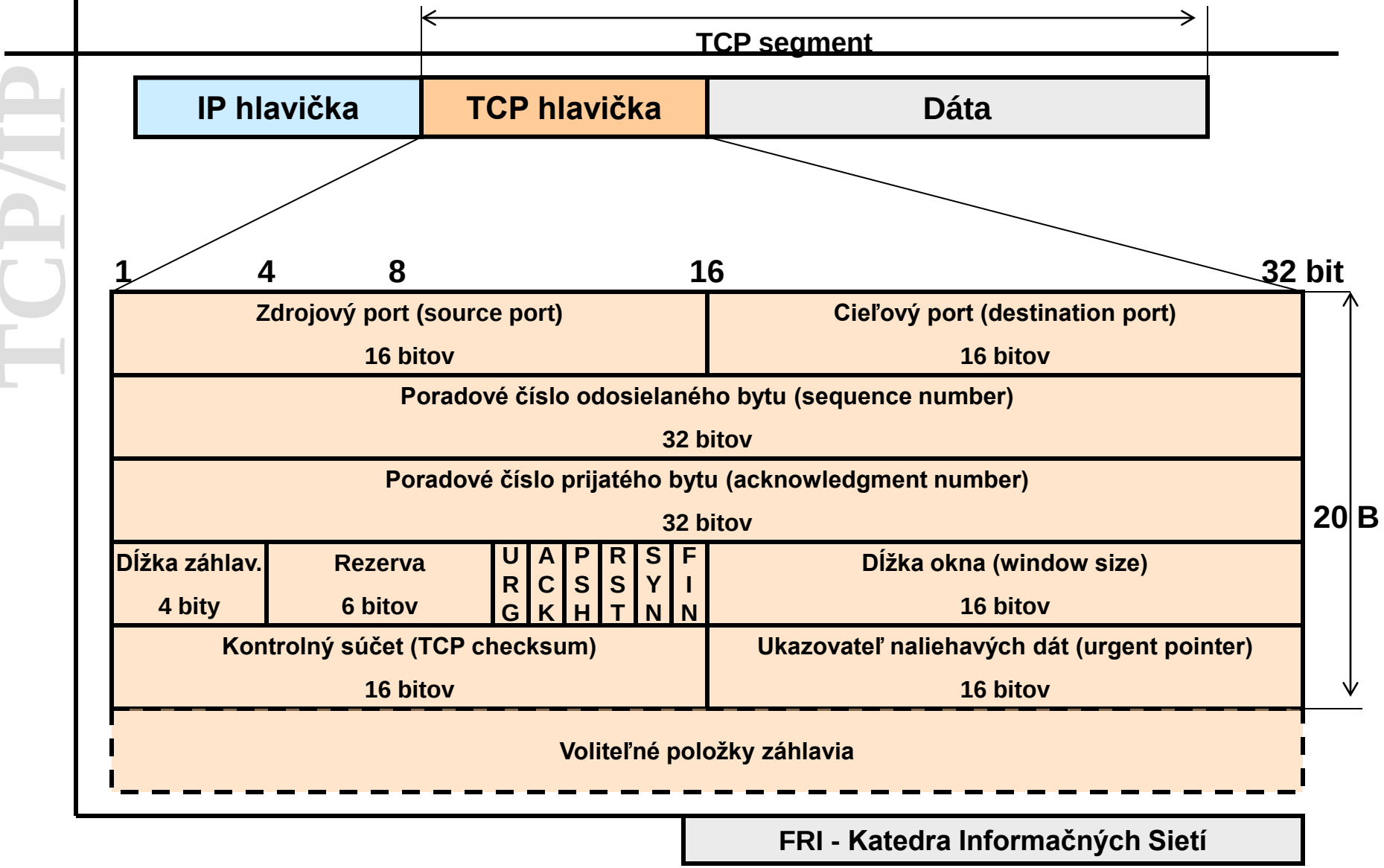
Použitie UDP

- Aplikácie pre ktoré je TCP robustné
  - IP telefónia
  - multimediálne spojenia
  - Multicastové spojenia
  - DNS
  - news a pod.

Transmission Control Protocol (TCP)

- Spojovo orientovaná služba
  - vytvára, riadi a ruší „virtuálny spojovací kanál“ medzi procesmi
  - kanál je definovaný dvojicou soketov
- zaručuje spoľahlivé prenesenie dát (Reliability):
  - robí pozitívne potvrdzovanie doručených dát a znovu prenos stratených
- Riadenie toku
  - princíp kĺzajúceho okna (Sliding window)
- dátový tok delí na segmenty (dátový blok na úrovni Transportnej vrstvy pre TCP) a v cieli ho spätne spája zo segmentov - stream dátový prenos
- Multiplexovanie (porty)
- Full duplex

Formát TCP segmentu



Formát TCP segmentu (2)

- **Zdrojový port (source port):** port procesu odosielateľa
- **cieľový port (destination port):** port procesu adresáta
- **poradové číslo odosielaného bajtu (sequence number):** poradové číslo prvého bajtu v dátovej časti segmentu vzhľadom na celkový počet prenesených bajtov TCP toku, max dĺžka 2^{32}-1, po prekročení od 0
- **poradové číslo prijatého bajtu (acknowledgment number):** poradové číslo bajtu, ktorý je príjemca schopný prijať (t.j. potvrdenie prijatia všetkých predchádzajúcich bajtov)
- **Dĺžka záhlavia (Dta offset):** dĺžka záhlavia v násobkoch 32 bitov (4B)
- **Rezerva (Reserved):** rezervované pre budúce použitie
- **URG:** TCP segment nesie naliehavé dáta
- **ACK:** platí nastavenie poľa „**Poradové číslo prijatého bytu“**
- **PSH:** použitie nie je ustálené, zvyčajne indikuje nesenie užívateľských aplikačných dát

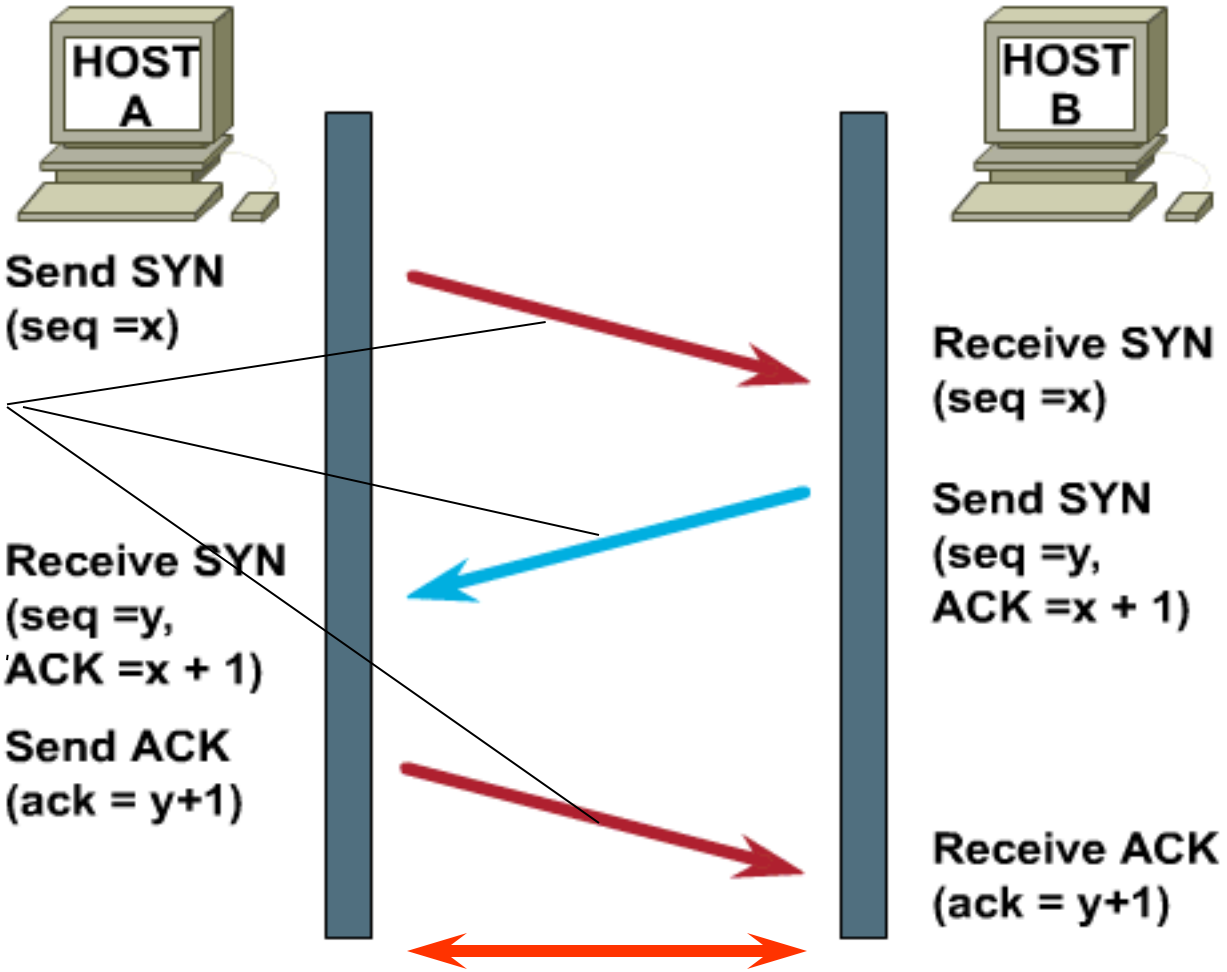
Formát TCP segmentu (3)

- **RST:** odmietnutie vytvoriť TCP spojenie
- **SYN:** synchronizácia medzi zdrojom a cieľom pri novom poradovom číslovaní
- **FIN:** ukončenie spojenia po prenose dát
- **Dĺžka okna (window):** vyjadruje prírastok v počte bajtov, ktoré si príjemca želá prijať
- **Kontrolná suma (checksum):** kontrolná suma aj cez dátovú časť
- **Ukazovateľ naliehavých dát (urgent pointer):** platí len ak je nastavená položka URG
- **Voliteľné položky (Options):**

Príklad TCP segment

```
⊞Frame 112 (54 bytes on wire, 54 bytes captured)
⊞Ethernet II, Src: 00:04:76:18:92:ec, Dst: 00:e0:29:3c:35:56
⊞Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 158.193.1.10 (158.193.1.
⊟Transmission Control Protocol, Src Port: 2734 (2734), Dst Port: 3128 (3128), Seq: 1348324435, Ack:
    Source port: 2734 (2734)
    Destination port: 3128 (3128)
    Sequence number: 1348324435
    Acknowledgement number: 2836239687
    Header length: 20 bytes
  ⊟Flags: 0x0010 (ACK)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...1 .... = Acknowledgment: Set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..0. = Syn: Not set
      .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6bfe (correct)
```

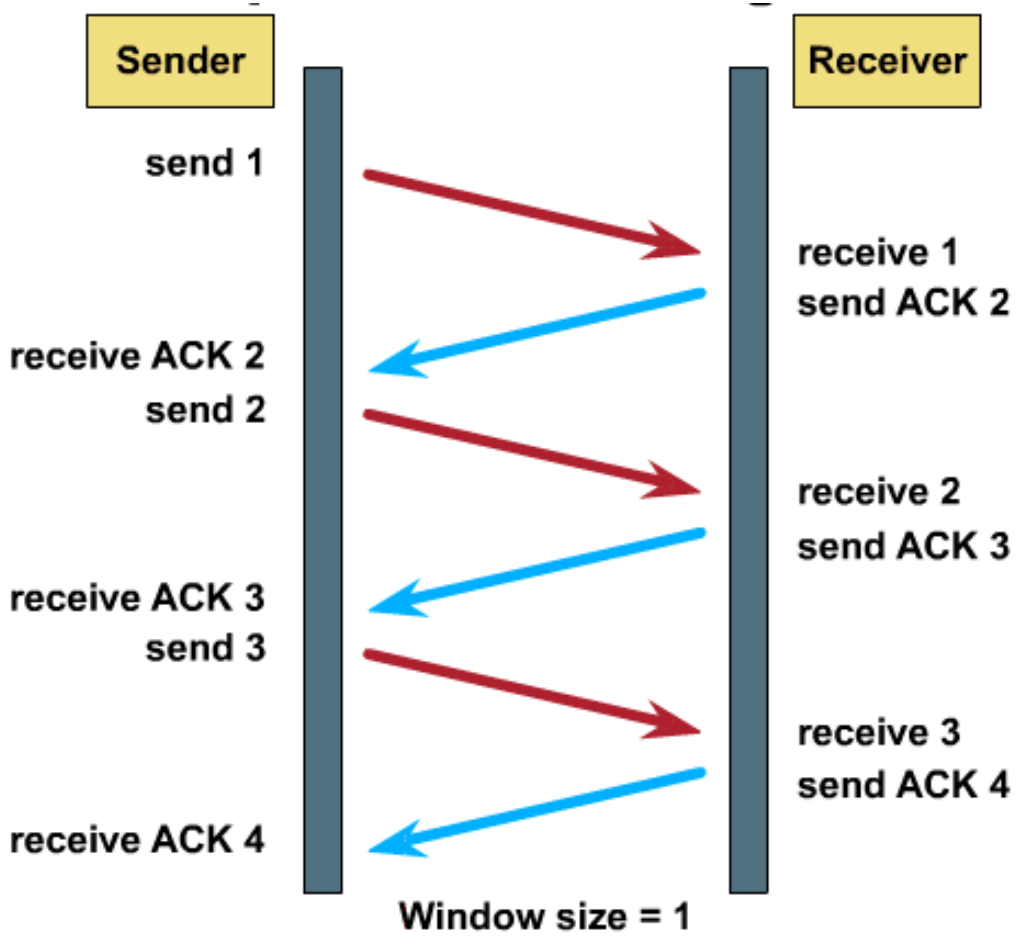
Založenie TCP spojenia - Three way handshake



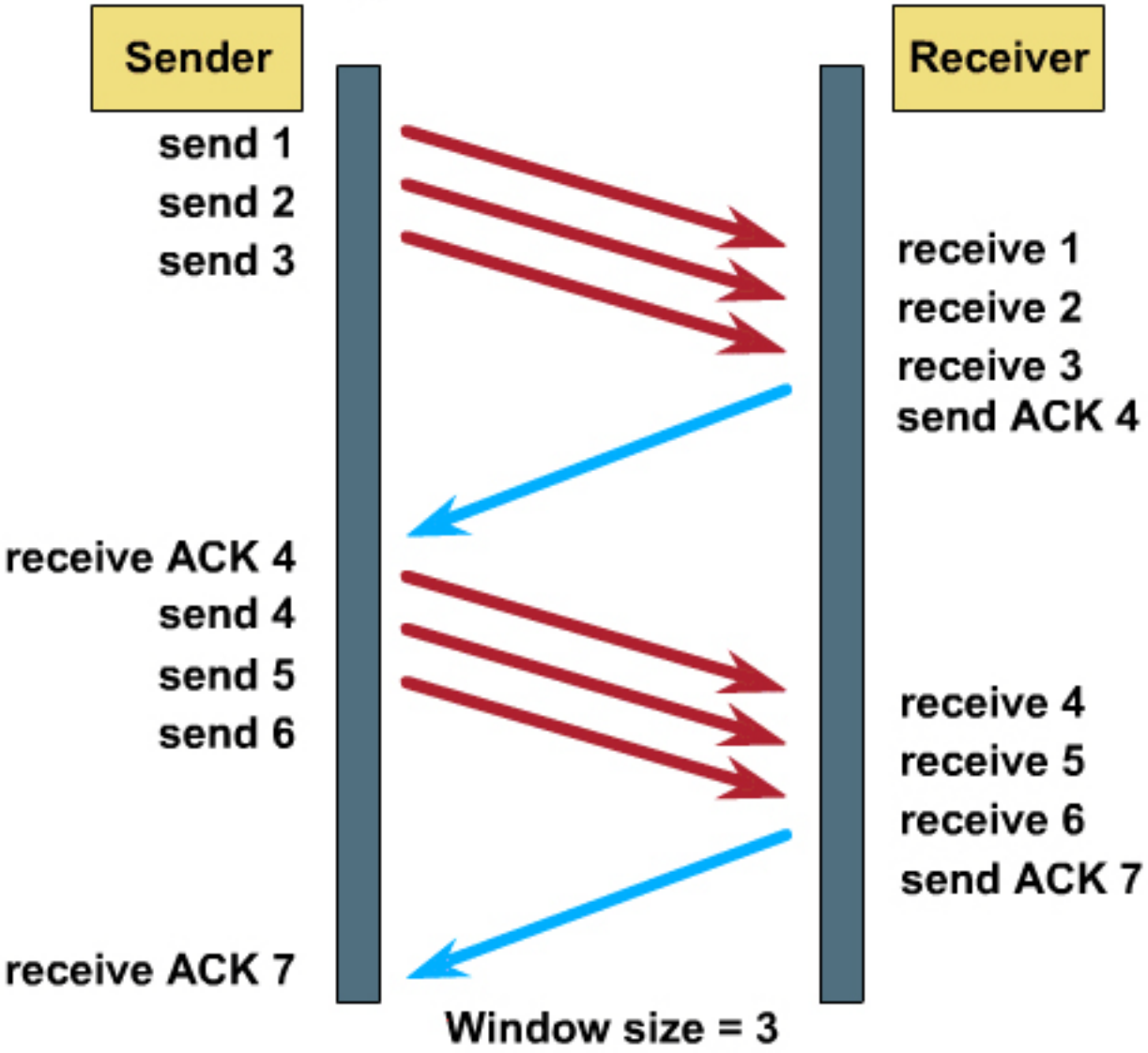
Segmenty neobsahujú užívateľské dáta

1,5 RTT oneskorenie

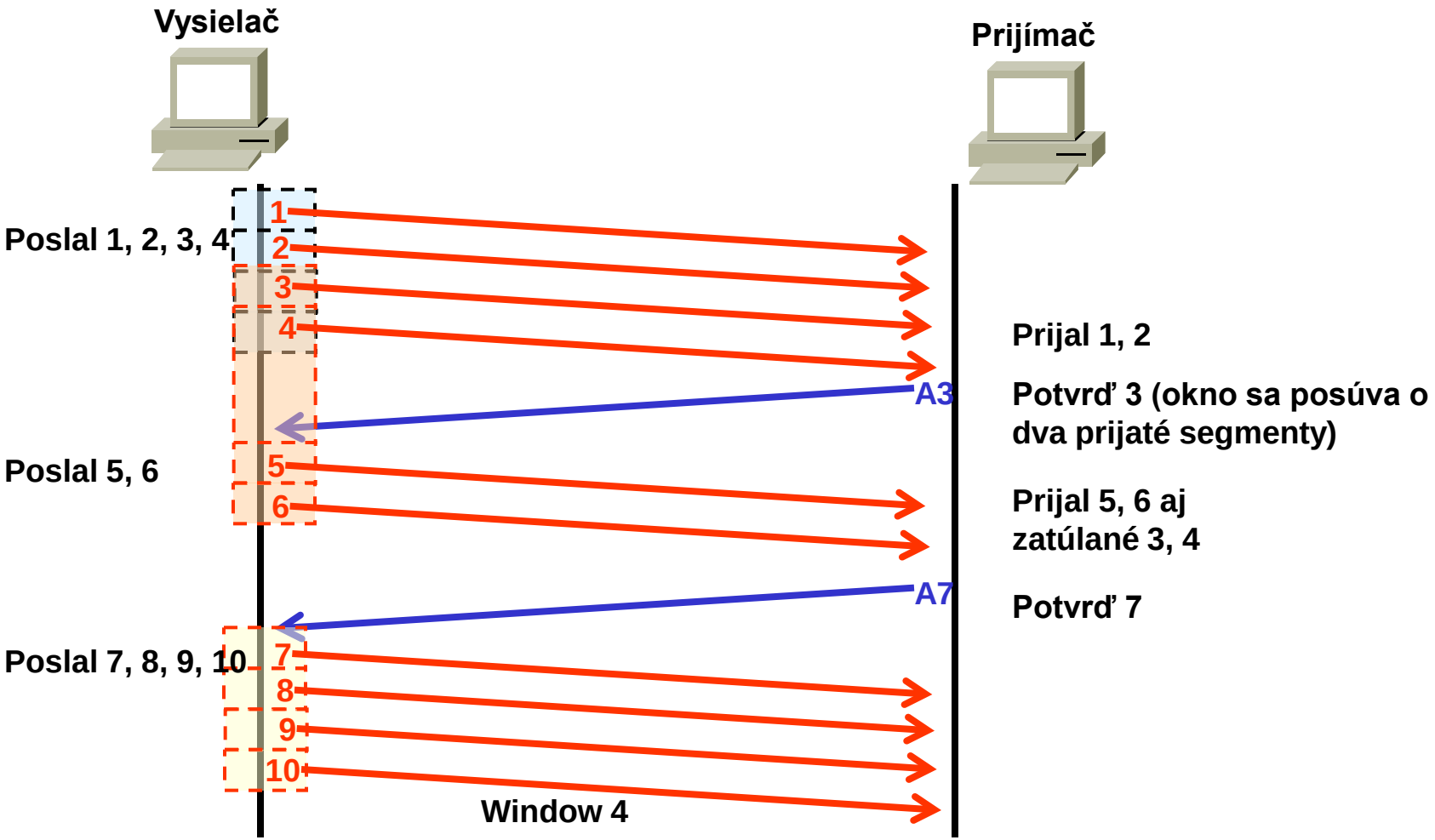
Jednoduché potvrdzovanie

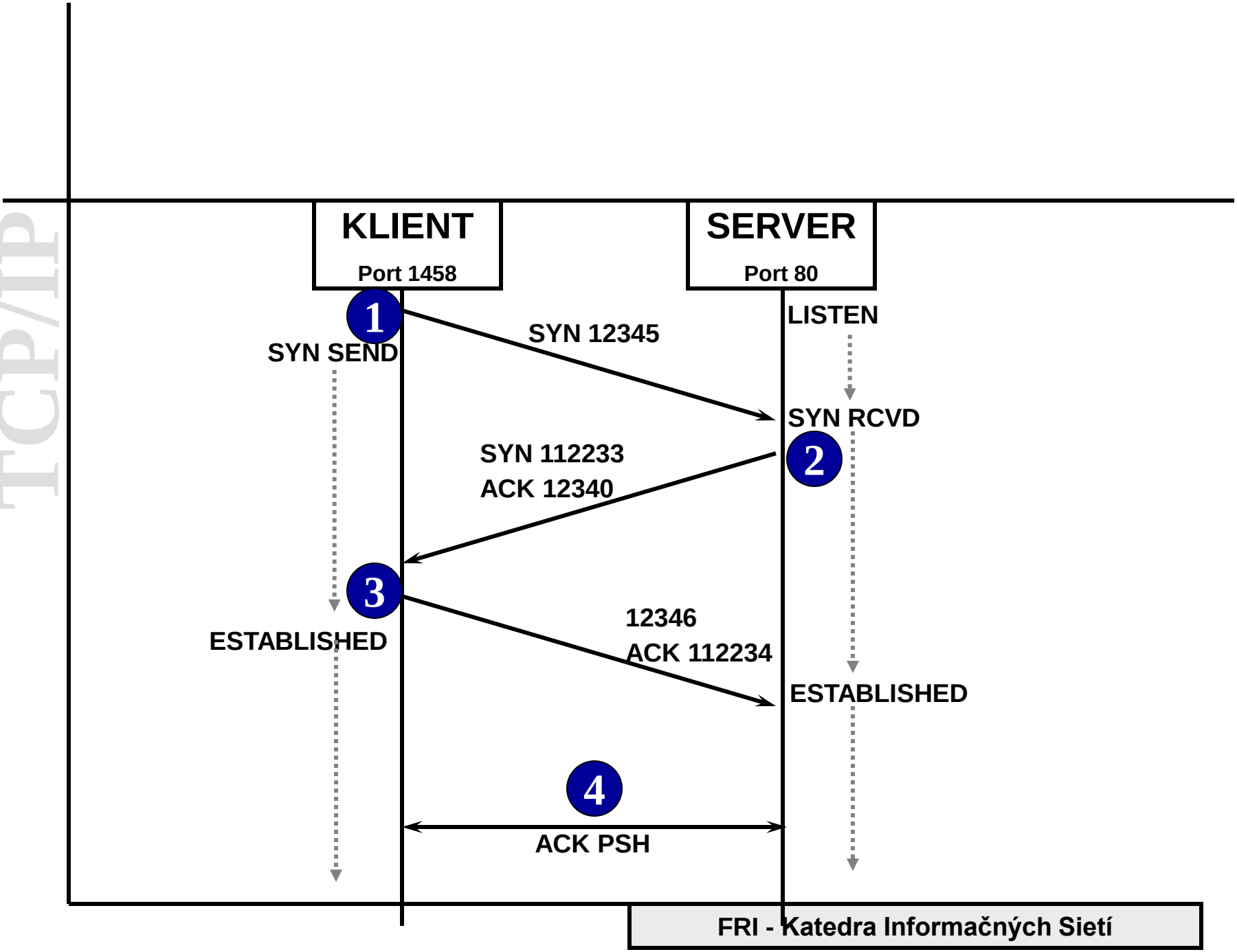


TCP Sliding Window

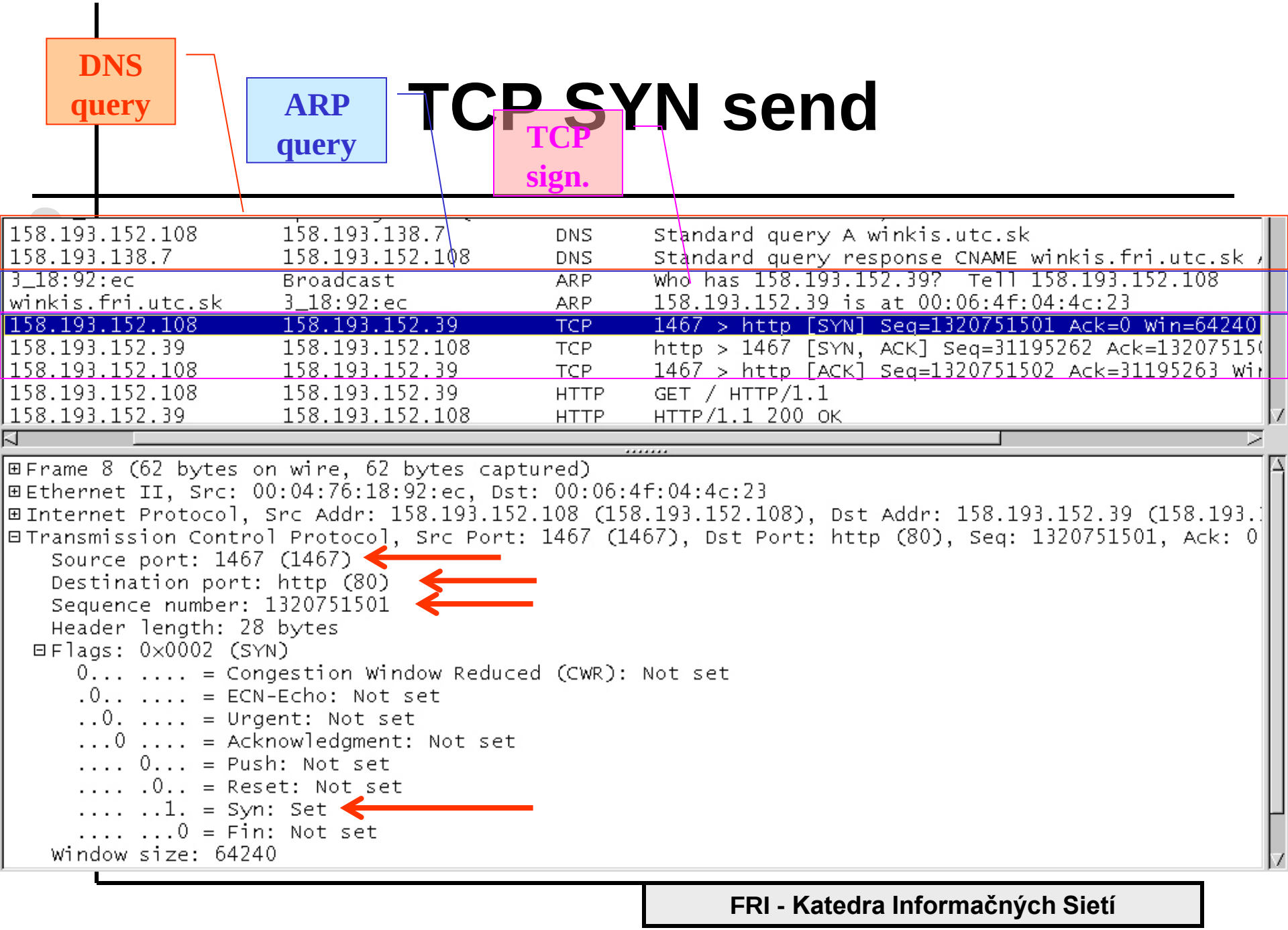


TCP Sliding window (2)

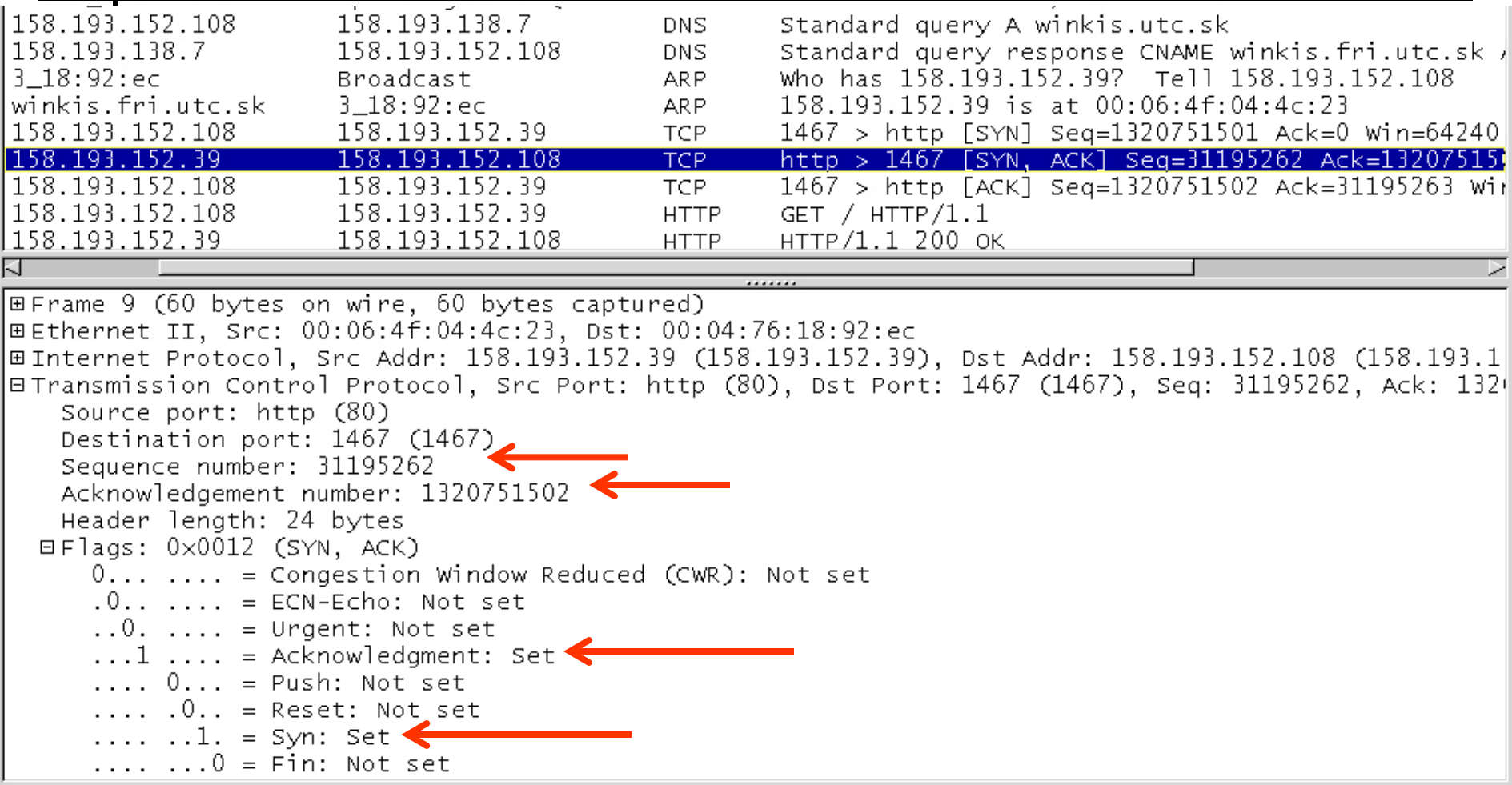



KLIENT
Port 1458
SERVER
Port 80
1
SYN SEND
SYN 12345
LISTEN
SYN RCVD
SYN 112233
ACK 12340
2
3
ESTABLISHED
12346
ACK 112234
ESTABLISHED
4
ACK PSH

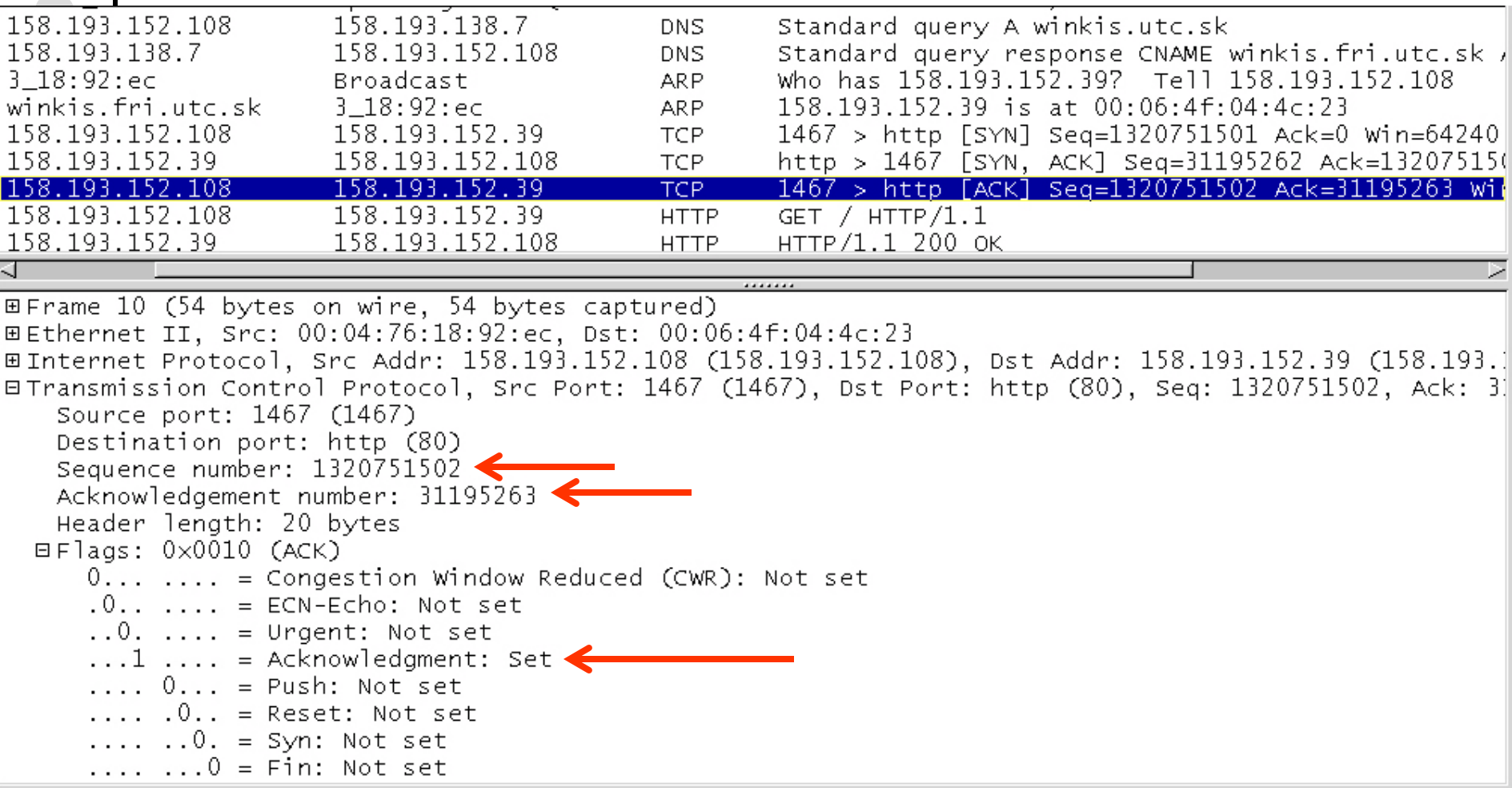
TCP SYN send


DNS query
ARP query
TCP sign.
158.193.152.108 158.193.138.7 DNS Standard query A winkis.utc.sk
158.193.138.7 158.193.152.108 DNS Standard query response CNAME winkis.fri.utc.sk
3_18:92:ec Broadcast ARP Who has 158.193.152.39? Tell 158.193.152.108
winkis.fri.utc.sk 3_18:92:ec ARP 158.193.152.39 is at 00:06:4f:04:4c:23
158.193.152.108 158.193.152.39 TCP 1467 > http [SYN] Seq=1320751501 Ack=0 Win=64240
158.193.152.39 158.193.152.108 TCP http > 1467 [SYN, ACK] Seq=31195262 Ack=13207515
158.193.152.108 158.193.152.39 TCP 1467 > http [ACK] Seq=1320751502 Ack=31195263 Wi
158.193.152.108 158.193.152.39 HTTP GET / HTTP/1.1
158.193.152.39 158.193.152.108 HTTP HTTP/1.1 200 OK
Frame 8 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:04:76:18:92:ec, Dst: 00:06:4f:04:4c:23
Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 158.193.152.39 (158.193.
Transmission Control Protocol, Src Port: 1467 (1467), Dst Port: http (80), Seq: 1320751501, Ack: 0
Source port: 1467 (1467)
Destination port: http (80)
Sequence number: 1320751501
Header length: 28 bytes
Flags: 0x0002 (SYN)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 64240

TCP SYN, ACK send



TCP ACK send back



Stavy spojení

Netstat –a (linux, win)

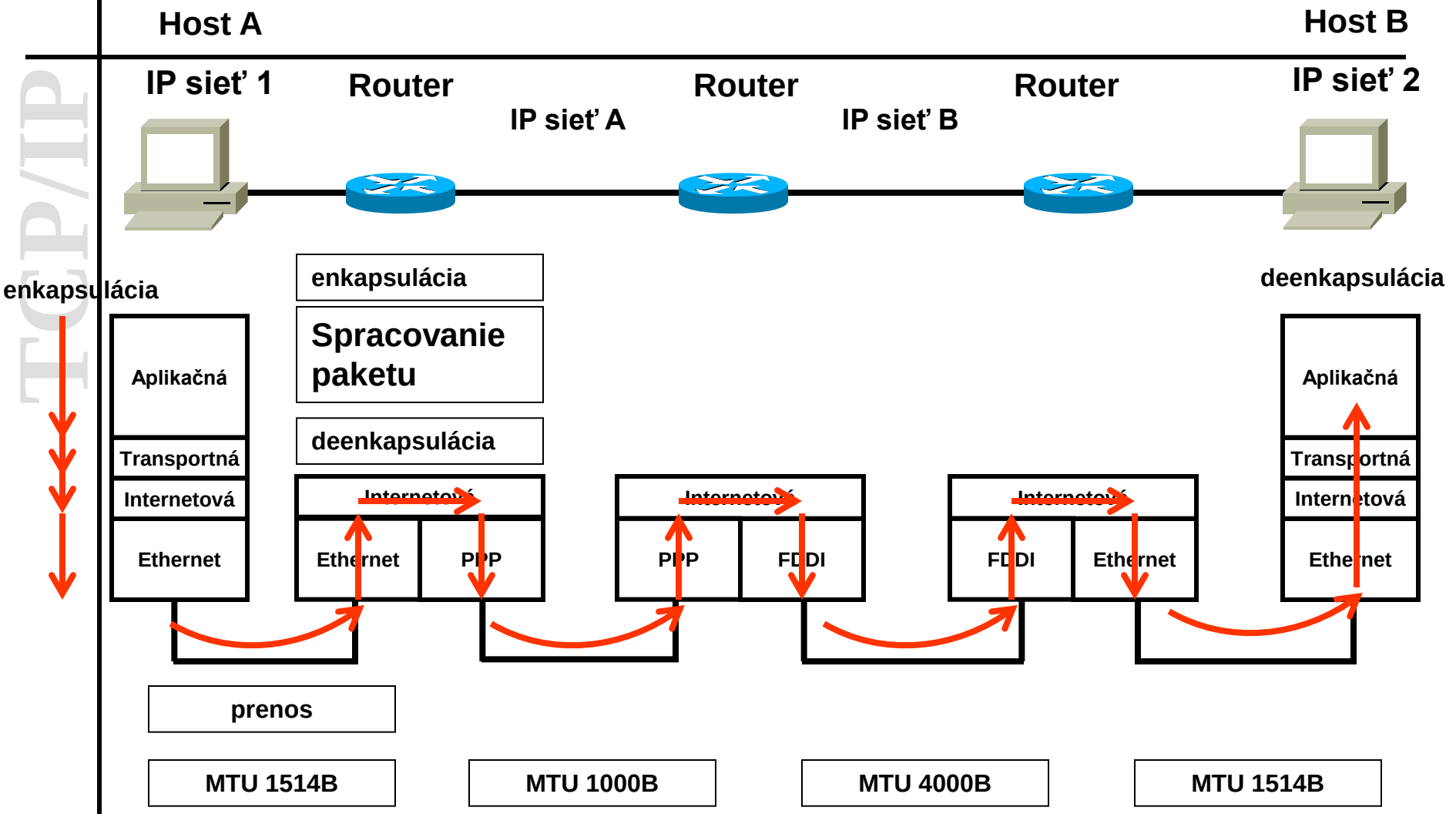
Aktivní připojení

Místní adresa	Protokol	Cizí adresa	Stav cizí adresy
TCP	segi:epmap	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:microsoft-ds	egi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:1027	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:2413	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:2415	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:2417	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:2914	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:10500	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:51025	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:51034	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:netbios-ssn	segi.fri.utc.sk:0	NASLOUCHÁNÍ
TCP	segi:2914	winkis.fri.utc.sk:5900	NAVÁZÁNO
UDP	segi:microsoft-ds	*:*	
UDP	segi:1058	*:*	
UDP	segi:2630	*:*	
UDP	segi:2911	*:*	
UDP	segi:netbios-ns	*:*	
UDP	segi:netbios-dgm	*:*	
UDP	segi:isakmp	*:*	

Zdroje

- Internet
  - http://winkis.utc.sk/Slov/html/pracovnici/segec_s.html
- Knihy:
  - Dostálek, Kabelová: Velký prúvodce protokoly TCP/IP a systémem DNS (Computer Press)
  - Šmtrha: Internetworking pomocí TCP/IP (Kopp)
  - Douglas E. Comer: Internetworking with TCP/IP (Prentice-Hall)
- Voľne šíriteľné materiály IETF (www.ietf.org)
  - Internet drafty
  - Request for Comments (oficiálne dokumenty):
    - INFORMAČNÉ (background info k danej téme)
    - EXPERIMENTÁLNE: (popis skúšaného protokolu or systému)
    - ŠTANDARDY (Standards Track):
      - Proposed standard, Draft standard, Standard

Fragmentácia(1)



TCP/IP

Fragmentácia(2)

- Ak MTU IP vrstvy (max. môže byť 65535) väčšie MTU linkovej vrstvy (Ethernet 1514 B)

```
  2 0.177036 158.193.152.108 158.193.152.39  ICMP Echo (ping) request
  3 0.177073 158.193.152.108 158.193.152.39  IP   Fragmented IP protocol (proto=ICMP
  4 0.177095 158.193.152.108 158.193.152.39  IP   Fragmented IP protocol (proto=ICMP
  5 0.178131 158.193.152.39  158.193.152.108 ICMP Echo (ping) reply
  6 0.178250 158.193.152.39  158.193.152.108 IP   Fragmented IP protocol (proto=ICMP
  7 0.178332 158.193.152.39  158.193.152.108 IP   Fragmented IP protocol (proto=ICMP
  8 0.370726 158.193.152.108 158.193.152.39  ICMP Echo (ping) request
  9 0.370765 158.193.152.108 158.193.152.39  IP   Fragmented IP protocol (proto=ICMP
 10 0.370787 158.193.152.108 158.193.152.39  IP   Fragmented IP protocol (proto=ICMP
```

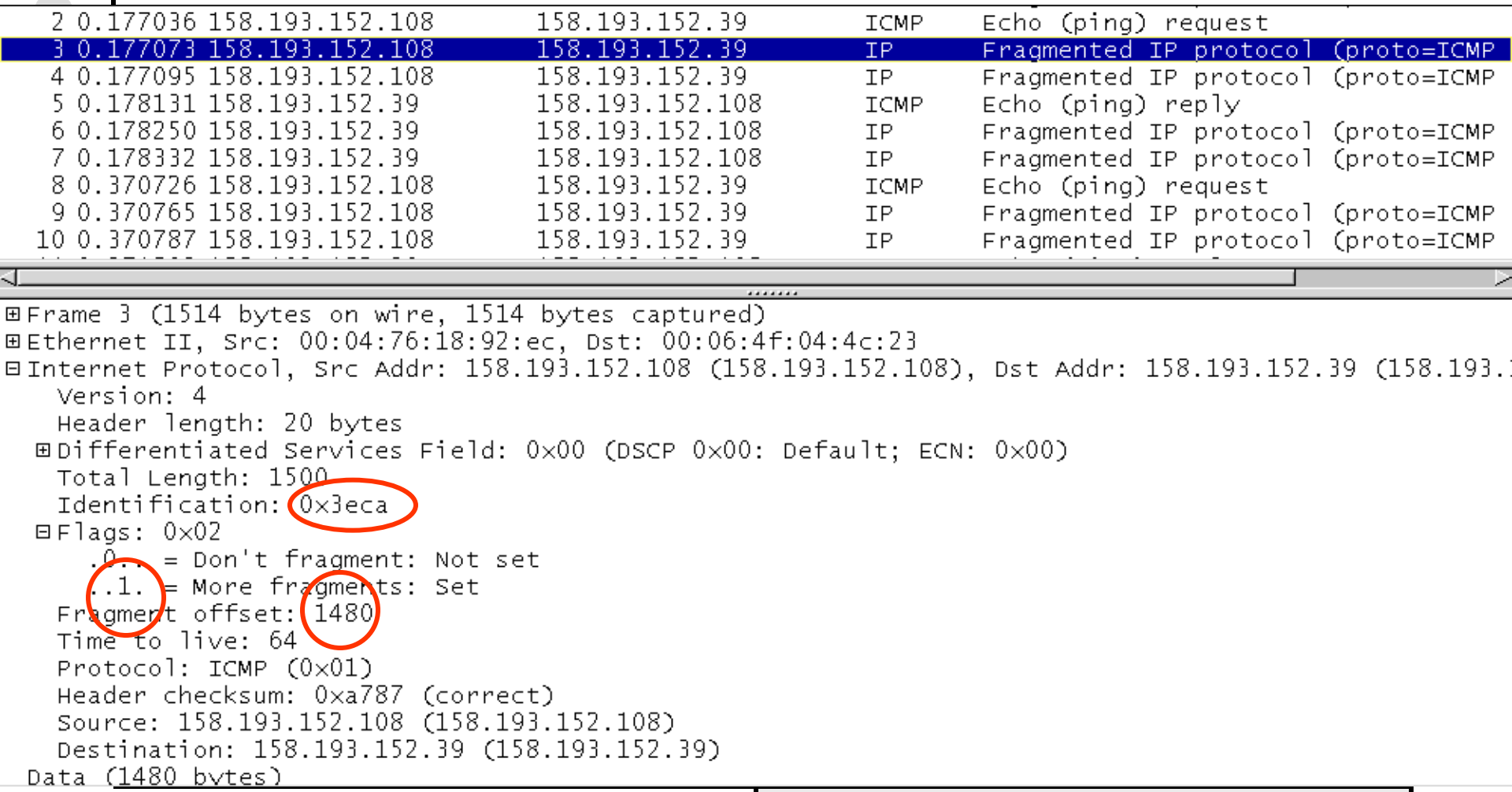
```
⊞Frame 2 (1514 bytes on wire, 1514 bytes captured)
⊞Ethernet II, Src: 00:04:76:18:92:ec, Dst: 00:06:4f:04:4c:23
⊟Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 158.193.152.39 (158.193.
   Version: 4
   Header length: 20 bytes
 ⊞Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 1500
   Identification: 0x3eca
 ⊟Flags: 0x02
     0.. = Don't fragment: Not set
     .1. = More fragments: Set
   Fragment offset: 0
   Time to live: 64
   Protocol: ICMP (0x01)
   Header checksum: 0xa840 (correct)
   Source: 158.193.152.108 (158.193.152.108)
   Destination: 158.193.152.39 (158.193.152.39)
⊞Internet Control Message Protocol
```

Ping, 4000B

Max MTU Eth. 1514B

Hlavička fragmentovaných paketov rovnaká

Fragmentácia(3)



Fragmentácia(4)

```
  2 0.177036 158.193.152.108      158.193.152.39       ICMP    Echo (ping) request
  3 0.177073 158.193.152.108      158.193.152.39       IP      Fragmented IP protocol (proto=ICMP
  4 0.177095 158.193.152.108      158.193.152.39       IP      Fragmented IP protocol (proto=ICMP
  5 0.178131 158.193.152.39       158.193.152.108      ICMP    Echo (ping) reply
  6 0.178250 158.193.152.39       158.193.152.108      IP      Fragmented IP protocol (proto=ICMP
  7 0.178332 158.193.152.39       158.193.152.108      IP      Fragmented IP protocol (proto=ICMP
  8 0.370726 158.193.152.108      158.193.152.39       ICMP    Echo (ping) request
  9 0.370765 158.193.152.108      158.193.152.39       IP      Fragmented IP protocol (proto=ICMP
 10 0.370787 158.193.152.108      158.193.152.39       IP      Fragmented IP protocol (proto=ICMP
```

```
⊞Frame 4 (1082 bytes on wire, 1082 bytes captured)
⊞Ethernet II, Src: 00:04:76:18:92:ec, Dst: 00:06:4f:04:4c:23
⊟Internet Protocol, Src Addr: 158.193.152.108 (158.193.152.108), Dst Addr: 158.193.152.39 (158.193.
   Version: 4
   Header length: 20 bytes
  ⊞Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 1068
   Identification: 0x3eca
  ⊟Flags: 0x00
     0.. = Don't fragment: Not set
     .0. = More fragments: Not set
   Fragment offset: 2960
   Time to live: 64
   Protocol: ICMP (0x01)
   Header checksum: 0xc87e (correct)
   Source: 158.193.152.108 (158.193.152.108)
   Destination: 158.193.152.39 (158.193.152.39)
 Data (1048 bytes)
```