

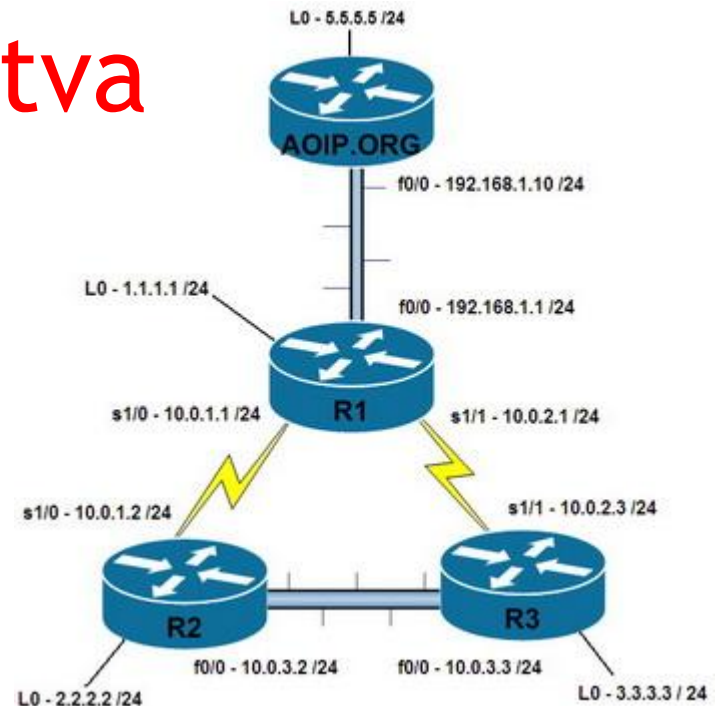
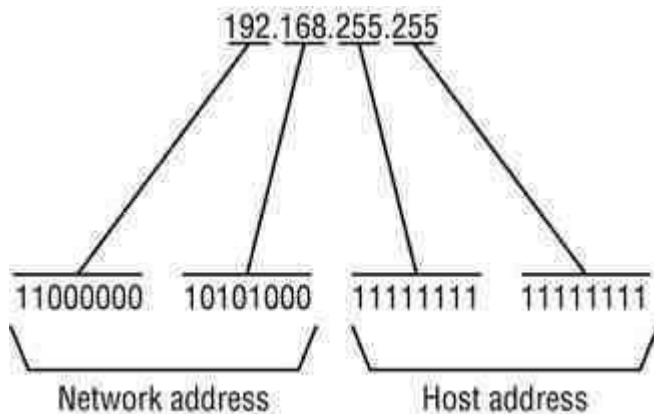
7. prednáška

4-bit	8-bit	16-bit	32-bit	
Ver.	Header Length	Type of Service	Total Length	
Identification			Flags	Offset
Time To Live	Protocol	Checksum		
Source Address				
Destination Address				
Options and Padding				

158.197.31.4/24

fe80::221:9bff:fe64:db91/64

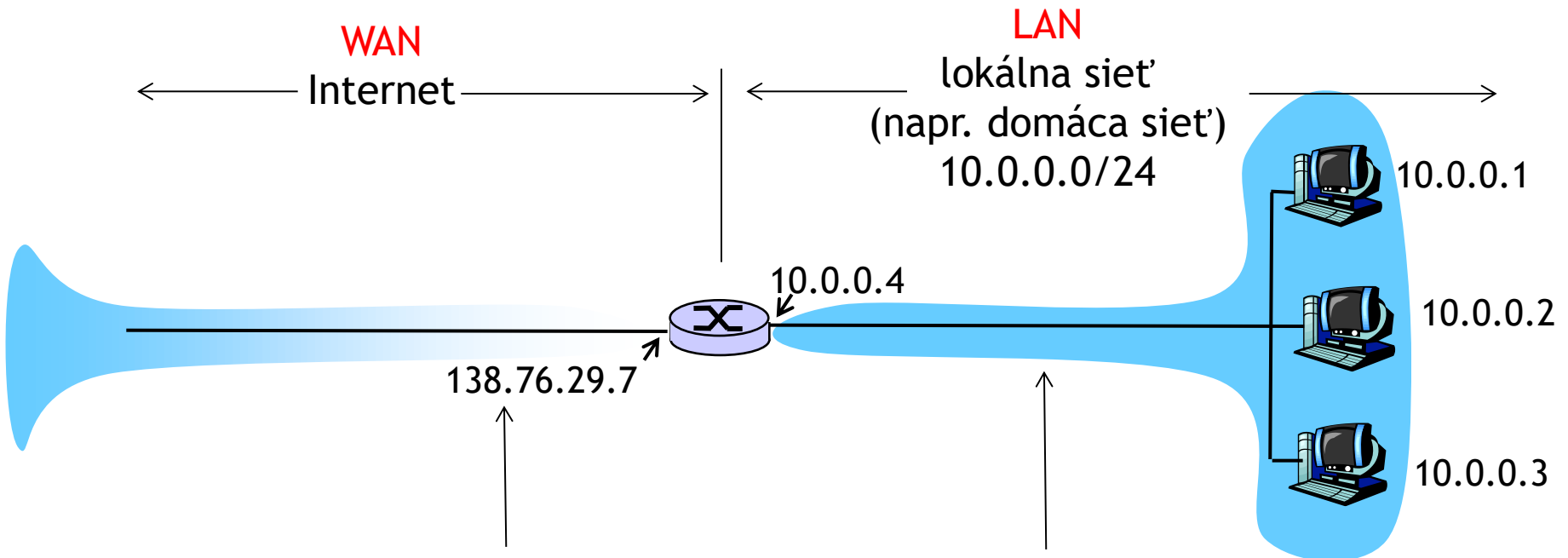
Siet'ová vrstva 2.časť



Prehľad prednášky

- NAT - network address translation
- ICMP
- IPv6

NAT: Network Address Translation



Všetky datagramy *odchádzajúce* z lokálnej siete majú *rovnakú* zdrojovú WAN IPv4 adresu: 138.76.29.7, rôzne môžu byť zdrojové porty

Pakety so zdrojovou a zároveň cieľovou IPv4 adresou z vnútra siete 10.0.0.0/24 fungujú tak, ako obvykle

NAT: Network Address Translation

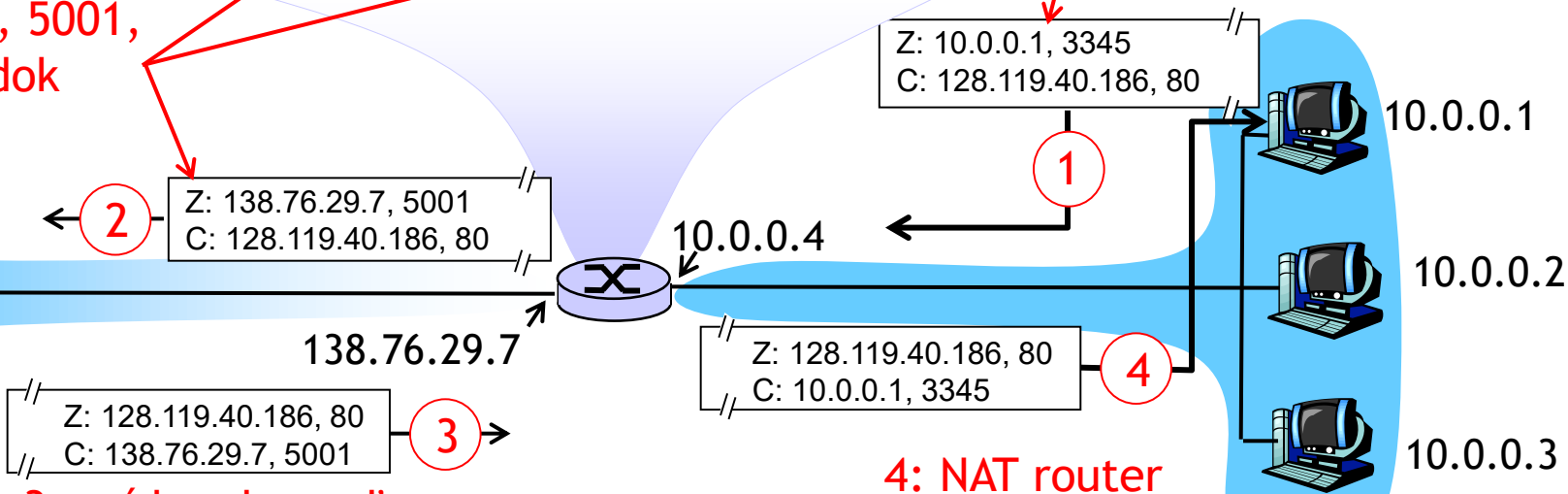
- ❑ **Motivácia:** lokálna sieť sa javí navonok (z internetu) ako jeden počítač s jedinou IPv4 adresou
 - ❖ stačí, ak nám provider (napr. Antik) prideli jednu IPv4 adresu a môžeme pripájať viac počítačov
 - ❖ môžeme meniť IPv4 adresy vo vnútri lokálnej sieti bez účasti providera, aj klientov pre naše servery
 - ❖ môžeme zmeniť ISP bez zmeny vnútornej adresácie v lokálnej sieti
 - ❖ zariadenia vo vnútornej sieti nie sú explicitne adresovateľné a viditeľné z vonku - nevieme ich priamo napadnúť (vylepšenie bezpečnosti).

NAT: postup

NAT prekladová tabuľka	
WAN adresa	LAN adresa
138.76.29.7, 5001	10.0.0.1, 3345
.....

1: stanica 10.0.0.1 pošle paket na 128.119.40.186, 80

2: NAT router zmení zdrojovú adresu paketu z 10.0.0.1, 3345 na 138.76.29.7, 5001, a doplní riadok



3: príde odpoveď
cieľová adresa:
138.76.29.7, 5001

4: NAT router zmení cieľovú adresu paketu z 138.76.29.7, 5001 na 10.0.0.1, 3345

NAT: Network Address Translation

- čísla portov môžu byť 0 - 65535
- ❖ S jedinou IPv4 adresou vieme robiť naraz vyše 65000 spojení!
- NAT je kontroverzný:
 - ❖ obvykle ako doplnková služba routrov, ktoré by inak mali rozbaľovať iba po tretiu vrstvu
 - ❖ dva počítače, každý za iným NATom, nevedia za normálnych okolností priamo komunikovať
 - možnosť, že klient je za NATom, musí byť braná do úvahy pri tvorbe sieťových aplikácií, napr. pri P2P
 - ❖ zánik by mal priniesť protokol IPv6

NAT traversal problem

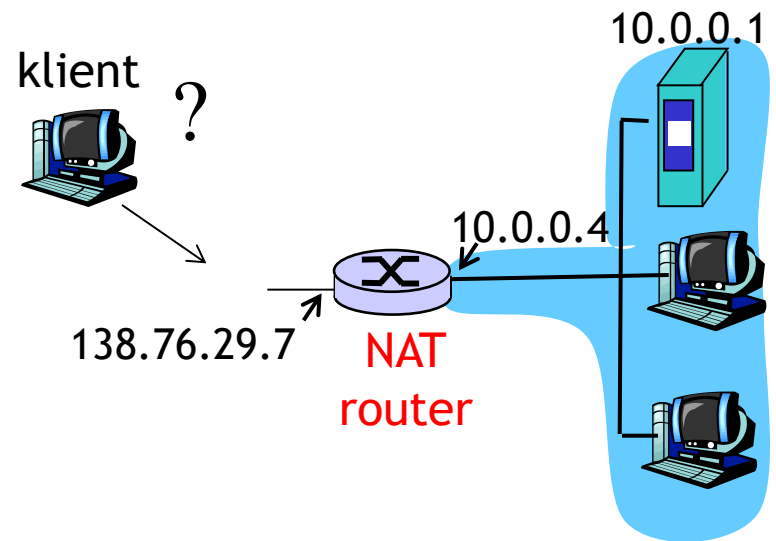
❑ klient sa chce napojiť na server na adrese 10.0.0.1

❖ 10.0.0.1 je lokálna adresa neexistujúca na internete (klient ju nemôže použiť ako cieľovú adresu)

❖ jediný viditeľný je WAN port NAT routera: 138.76.29.7

❑ **riešenie 1:** statická konfigurácia NATu na preposielanie všetkých požiadaviek na určený port priamo na správny server

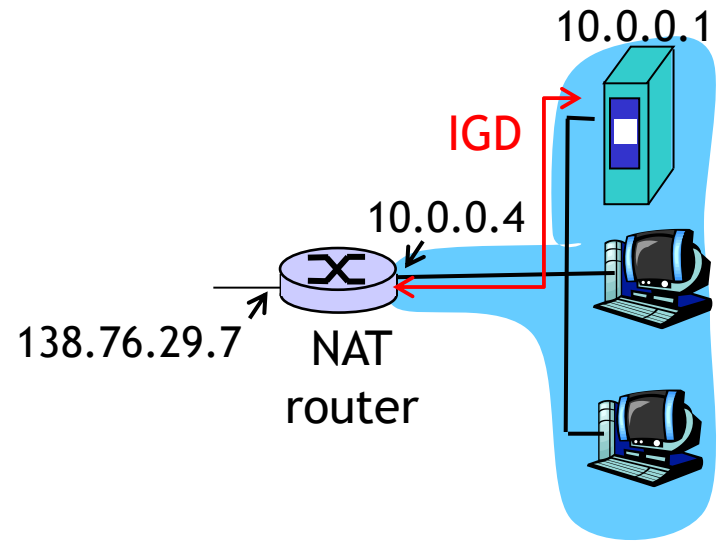
❖ napr. (138.76.29.7, port 2500) preposielame na (10.0.0.1, port 25000)



NAT traversal problem

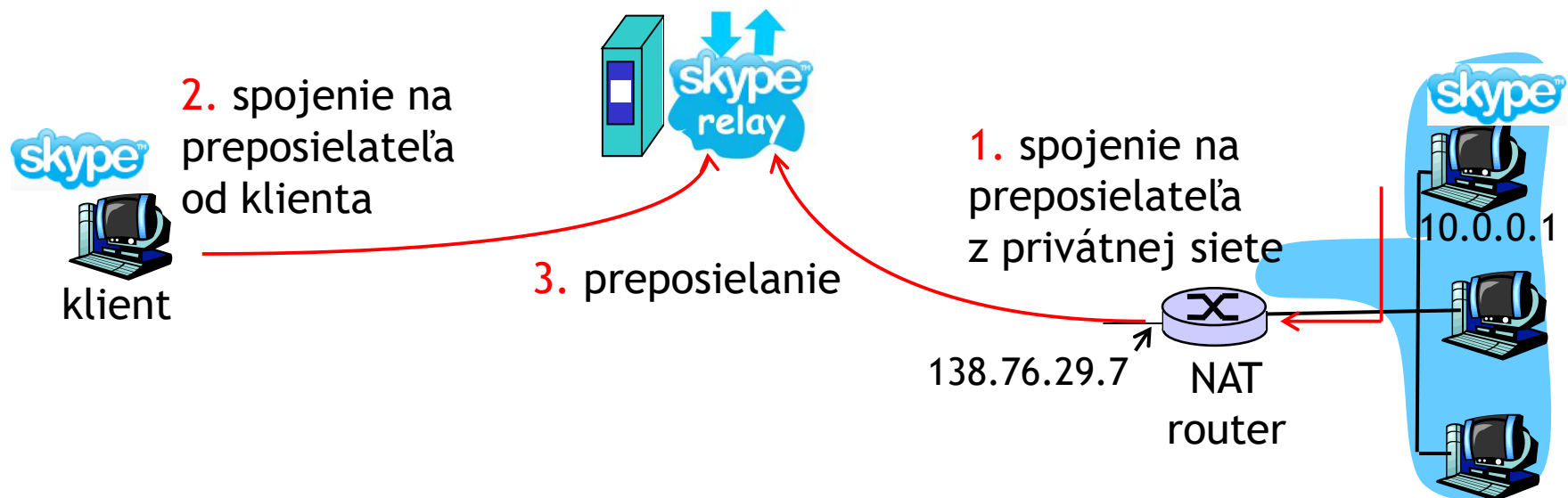
❑ **riešenie 2:** Univerzálny Plug and Play (UPnP) Internet Gateway Device (IGD) protokol. Umožňuje stanici v lokálnej sieti:

- ❖ zistiť verejnú IP adresu NAT routra (138.76.29.7)
- ❖ zistiť existujúce mapovania portov
- ❖ pridávať/odoberať mapovania portov (na daný čas)



NAT traversal problem

- ❑ **riešenie 3:** relaying/preposielanie (napr. v Skype)
- ❖ príjemca hovoru vytvorí spojenie na preposielateľa
- ❖ externý klient sa tiež napojí na preposielateľa
- ❖ preposielateľ preposiela pakety komunikácie



Prehľad prednášky

- NAT - network address translation
- ICMP
- IPv6

ICMP: Internet Control Message Protocol

□ používaný stanicami a routrami na výmenu sieťových informácií

❖ hlásenie chýb: nedostupná stanica, sieť, port, protokol

❖ echo request/reply (používané programom ping)

□ sieťová vrstva “nad” IP:

❖ ICMP správy vo vnútri IPv4 paketov

□ ICMP správa: typ, kód, plus prvých 8 bajtov IP paketu, ktorý spôsobil vytvorenie správy

<u>Typ</u>	<u>Kód</u>	<u>popis</u>
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest. host unreachable
3	2	dest. protocol unreachable
3	3	dest. port unreachable
3	6	dest. network unknown
3	7	dest. host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Skúste si ping

❑ ping -t 3 adresa (unix), -i (windows)

❖ Time To Live = 3

❑ ping -b broadcastováAdresa (unix)

❖ pingujeme všetkých v našej sieti

❑ ping -s veľkosť adresa, -l (windows)

nastavíme veľkosť ICMP paketu (bez hlavičky)
(keď je výsledný paket väčší ako MTU, nastáva
IP fragmentácia)

Traceroute a ICMP

❑ Pošleme sériu UDP datagramov k cieľu (alebo TCP či ICMP)

❖ prvé 3 majú TTL =1

❖ druhé 3 majú TTL=2, atď.

❖ nepravdepodobné číslo portu

❑ Keď paket vyslaný s TTL=n dôjde k n-tému routru:

❖ router zahodí paket

❖ pošle na zdrojovú adresu ICMP správu “TTL expired” (type 11, code 0)

❖ IP paket s ICMP správou má zdrojovú adresu routra, ktorý ju posielal

❑ Keď príde ICMP správa, vypočítame RTT

Ukončenie

❑ UDP datagram môže dôjsť až k cieľu

❑ Cieľová stanica vráti ICMP správu “port unreachable” (type 3, code 3)

❑ Keď odosielateľ dostane túto správu, končí

Prehľad prednášky

- NAT - network address translation
- ICMP
- IPv6

IPv6

□ **úvodná motivácia (1992-1995):** 32-bitové adresy budú čoskoro všetky vyčerpané

❖ prišiel však CIDR a presadil sa NAT

□ **d'alšia motivácia:**

❖ formát hlavičky umožňuje rýchlejšie spracovanie a smerovanie

❖ hierarchické pridelenie adries

❖ podpora anycastu a lepšia podpora multicastu

❖ autokonfigurácia koncových zariadení

❖ lepšie riešenie mobility

□ **formát hlavičky datagramu IPv6:**

❖ presne 40 bajtová hlavička (žiadne voliteľné časti hlavičky), ale možnosť ďalších doplnujúcich hlavičiek

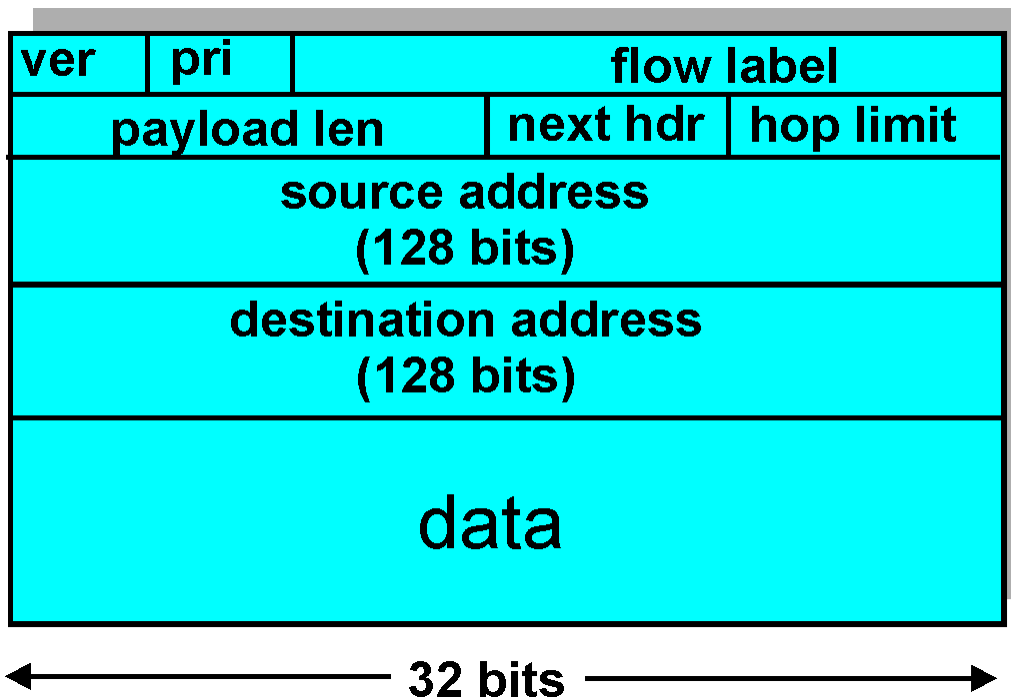
❖ fragmentácia už len vo voliteľnej hlavičke vytvorenej odosielateľom (nie routrami)

IPv6 hlavička

Priorita (traffic class): identifikuje prioritu datagramu

Flow label: identifikácia toku dát

Next header: identifikácia rozširujúcej hlavičky alebo protokolu “vyššej vrstvy” v dátach



Niektoré zmeny oproti IPv4

- ❑ **Kontrolný súčet** : zrušený ako redundantný
 - ❖ kontrolné súčty sa robia v transportnej aj spojovej vrstve
 - ❖ netreba kontrolovať na routoch (šetríme čas)
- ❑ **Options**: nahradené ďalšími hlavičkami.
 - ❖ V časti “Next Header” sa môže namiesto identifikácie transportného protokolu dať identifikácia “ďalšej špeciálnej IP hlavičky”
- ❑ **ICMPv6**: nová verzia ICMP
 - ❖ nové typy správ, napr. “Packet Too Big”
 - ❖ funkcie na riadenie multicastu (namiesto IGMP)
 - ❖ riadenie autokonfigurácie

IPv6 adresy

□ úplný výpis všetkých bitov (hexadecimálne po dvoch bajtoch v slove)

❖ fe80:0000:0000:0000:0221:5cff:fe64:d39a

□ s odstránenými úvodnými nulami slov

❖ fe80:0:0:0:221:5cff:fe64:d39a

□ vynechané nulové sekvencie

❖ fe80::221:5cff:fe64:d39a

□ mixovaná notácia

❖ fe80::221:5cff:254.100.211.154

Niektoré špeciálne IPv6 adresy

□ nešpecifikovaná lokálna IP adresa

❖ `::/128` resp. `0:0:0:0:0:0:0:0/128` (analógia 0.0.0.0 z IPv4)

□ loopback, localhost

❖ `::1/128` resp. `0:0:0:0:0:0:0:1/128` (analógia 127.0.0.1 z IPv4)

□ reprezentácia IPv4 adres v IPv6 notácii (IPv4-mapované adresy v SIIT [RFC 2765]) - **v praxi sa nepoužíva**

❖ napr. `::ffff:158.197.31.4/128`

□ lokálne adresy `fe80::/10` - **novinka!**

❖ fe8X, fe9X, feaX, febX - IPv6 adresy v lokálnej sieti

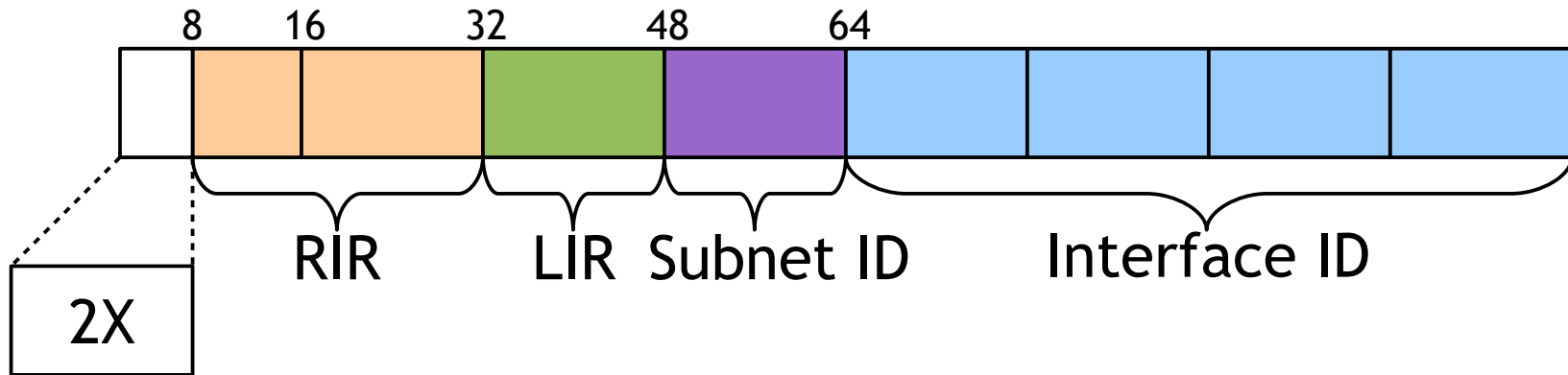
❖ IPv4 analógia nie je

□ site-local (lokálna sieť sídla/organizácie) `fec0::/10` - **zrušené!**

Niektoré špeciálne IPv6 adresy

- ❑ unique-local (unikátne privátne adresy) **fc00::/7** (fcXX, fdXX)
 - ❖ takmer analógia sietí 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
 - ❖ sieťový prefix tvorený z MAC adresy a dátumu - **vysoká pravdepodobnosť unikátnosti!** (RFC 4193)
- ❑ broadcast - **zrušený!**
 - ❖ analógia 255.255.255.255/32 a broadcastových adries sietí napr. 158.197.35.255/24
- ❑ multicastové adresy **ff00::/8** (ffXX:hocičo)
 - ❖ analógia triedy D: 224.0.0.0/4
- ❑ globálne (celosvetové adresy) **2000::/3**
 - ❖ 2XXX:hocičo a 3XXX:hocičo
 - ❖ najčastejšie 2001:hocičo
 - ❖ UPJŠ IPv4: 158.197.0.0/16
 - ❖ UPJŠ IPv6: 2001:4118:400/48

Štruktúra globálnych unicastových IPv6 adres



❑ **RIR** - IANA + regionálni registrátori (RIPE NCC, ARIN, APNIC, AFRINIC, LACNIC)

❑ **LIR** - lokálni registrátori pridelujú siete s prefixom dlhým 48-56 bitov

❑ **Subnet ID** - podsieť organizácie (65 535 alebo 256 možných podsietí)

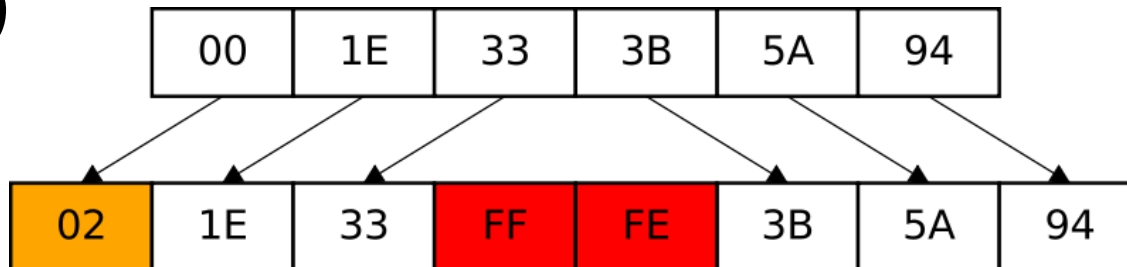
❑ **Interface ID** - identifikátor rozhrania (siet'ovej karty)

Interface ID

□ máme k dispozícii $2^{64} \sim 10^{18}$ adries zariadení v jednej podsieti

□ IPv6 EUI-64

❖ odvodenie z MAC adresy (48 bitov na 64 bitov)



□ Privacy extensions for stateless address autoconfiguration in IPv6

❖ náhodné koncovky pravidelne menené

Nastavovanie IPv6 adresy

- ❑ ručne (hlavne servery s DNS AAAA záznamami)
- ❑ automatizovane
 - ❖ informácia o adrese default routra
 - SLAAC (stateless address autoconfiguration) (RFC 2462)
 - ❖ pridelovanie sieťovej časti
 - SLAAC
 - ❖ pridelovanie rekurzívnych lokálnych DNS serverov
 - DHCPv6 alebo DHCP(v4) ak máme dual-stack
 - od novembra 2010 aj cez SLAAC (RFC 6106)
 - ❖ pridelovanie identifikátora rozhrania
 - stanica si ho prideluje sama (EUI 64 alebo privacy extensions)
 - a/alebo ho dostane od stavového DHCPv6 (nebráni to stanici dodat' si ďalšie identifikátory podľa ľubovôle)

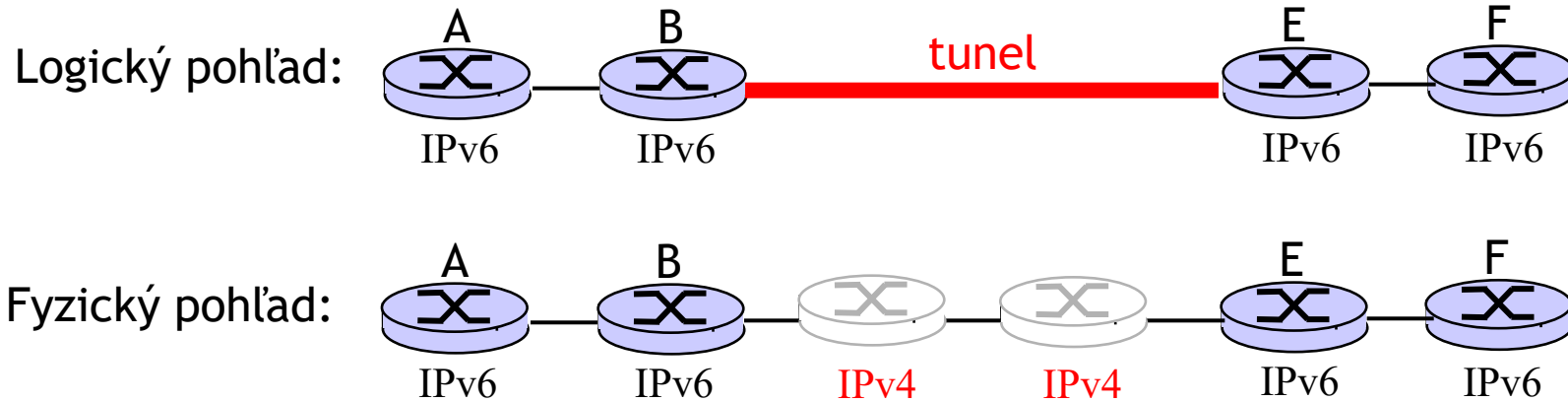
SLAAC + DHCPv6

- ❑ stanica si nastaví lokálnu adresu fe80::niečo
- ❑ stanica si overí unikátnosť cez detekciu duplicitných adries (typ paketu ICMPv6 na fe02::1:ffxx:xxxx) a prípadne nastaví inú
- ❑ stanica vyšle “router solicitation” (typ paketu ICMPv6)
- ❑ router mu zašle “router advertisement“ (typ paketu ICMPv6) s adresou brány a prípadnými ďalšími parametrami
 - ❖ ak príznak M=1 a O=0, má sa ešte použiť stavové DHCPv6
 - ❖ ak príznak M=0 a O=1, má sa ešte použiť bezstavové DHCPv6
 - ❖ ak príznak M=0 a O=0, v sieti sa nenachádza DHCPv6
- ❑ stavové DHCPv6 : stanica požiada o celú IPv6 adresu a ostatné parametre
- ❑ bezstavové DHCPv6 : stanica má sieťový prefix z “router advertisement” paketu a ďalšie parametre, hlavne lokálne rekurzívne DNS servery má získať z DHCPv6 serveru

Prechod od IPv4 k IPv6

- ❑ Nemôžeme všetky zariadenia vymeniť naraz
 - ❖ žiaden “flag day” = “deň D”
 - ❖ Ako má sieť fungovať s pomiešanými IPv4 a IPv6 routrami?
- ❑ riešenia:
 - ❖ **dual-stack**: zariadenia zvládajú IPv4 aj IPv6
 - ❖ **bezstavový preklad**: SIIT, NAT64, TRT, BIH, SOCKS64
 - ❖ **tunelovanie**: IPv6 prenášaný ako telo IPv4 paketu cez IPv4 routr: server/broker, 6to4, 6rd, 6over4, ISATAP, Teredo

Tunelovanie

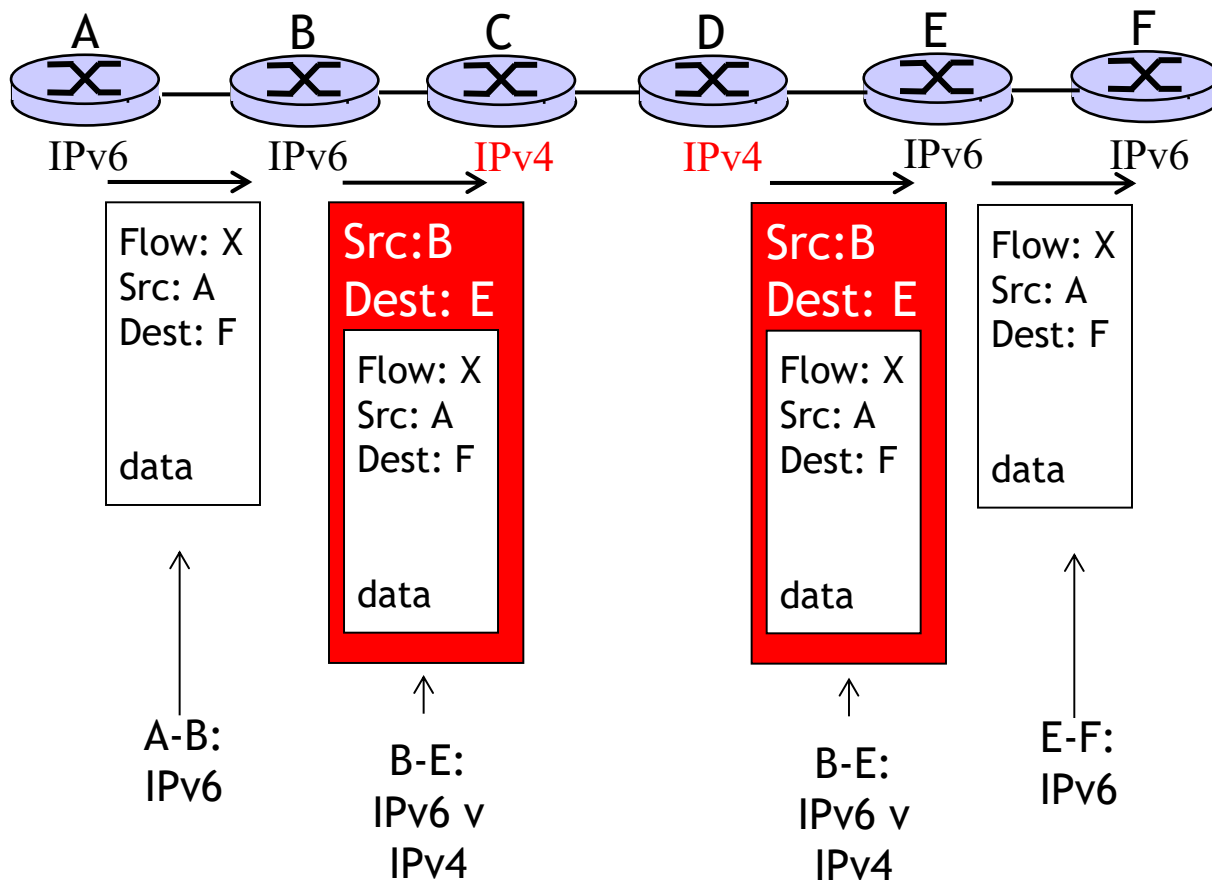


Tunelovanie (cez konfigurovaný tunel)

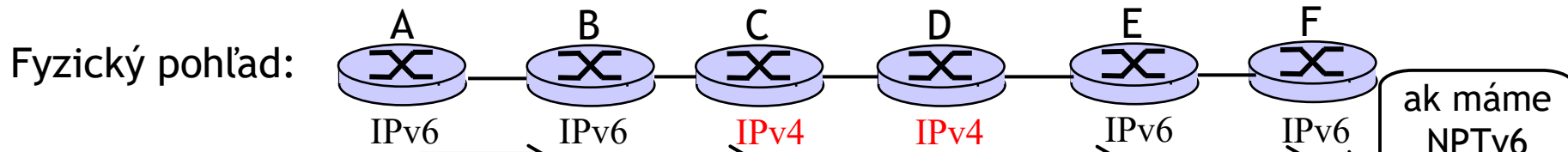
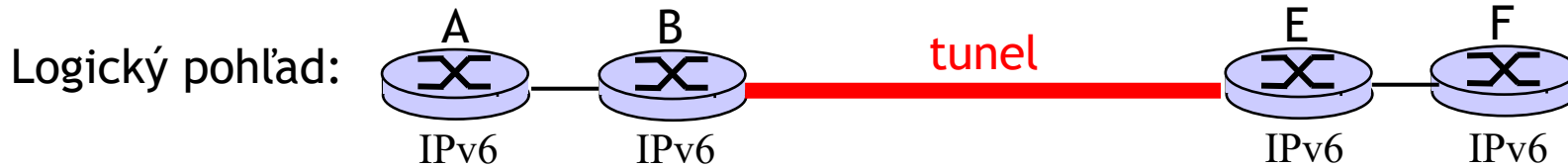
Logický pohľad:



Fyzický pohľad:



Tunelovanie [RFC 3056] (6to4)



2002:c001:0203:abcd:
pppp:pppp:pppp:pppp

Flow: X
Src: A
Dest: EF
data

Src: B⁴
Dest: E⁴
Flow: X
Src: A
Dest: EF
data

Src: B⁴
Dest: E⁴
Flow: X
Src: A
Dest: EF
data

Flow: X
Src: A
Dest: EF
alebo
Dest: F
data

IPv4^E: 192.1.2.3

ak máme
NPTv6

IPv6^F (EF):
2002:c001:0203:abcd:
pppp:pppp:pppp:pppp
alebo (F):
2001:98:542:abcd:
pppp:pppp:pppp:pppp



Zhrnutie

- NAT
- ICMP
- IPv6

Ďakujem za pozornosť

Modifikované slajdy z knihy:

Computer Networking: A Top Down Approach ,
4th edition.

Jim Kurose, Keith Ross
Addison-Wesley, July 2007.