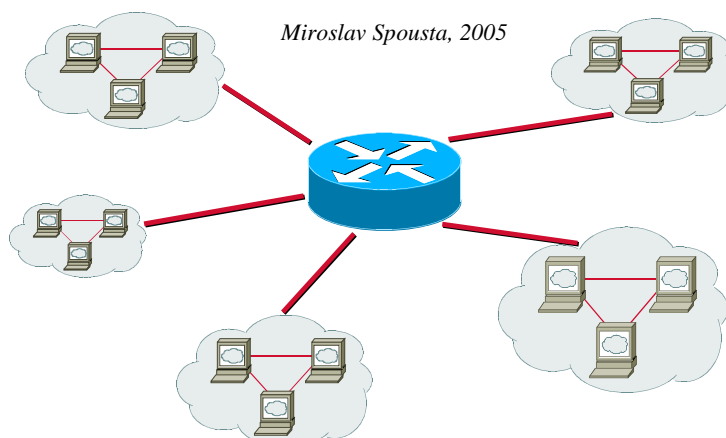


Poítařové sítě II

12. pomocné protokoly, IPv6



1

ICMP

- Internet Control Message Protocol
 - doslova protokol řídicích hlášení
 - RFC 792
- pomocný protokol IP, vlastně součástí IP protokolu
 - přenáší se v IP datagramech
 - problémy s ICMP datagramy se nehlásí
- používá se v síťce pro informování o nějakém nestandardním stavu při doručování IP datagramu
- generují se například při zahození datagramu
 - IP se nestará o nápravu
 - ale informuje odesílatele, že se tak stalo
- ICMP zprávy se zpracovávají v IP stacku odesílatele

2

ICMP

8b	8b	16b
typ zprávy (TYPE)	kód (CODE)	kontrolní součet
...		

- typ vyjadřuje o jakou zprávu jde
 - echo request, echo reply, redirect, ...
- kód udává parametry konkrétní zprávy
 - například z jakého důvodu se nepodařilo datagram doručit
- další formát zprávy závisí na typu
- často následuje předvodní IP hlavička + 64 bit dat z předvodního datagramu

3

ICMP Destination Unreachable

8b	8b	16b
TYPE = 3	CODE	kontrolní součet
nepoužito		
IP hlavička + vodního datagramu + 64 bit dat		

- CODE
 - 0: síť nedostupná (net unreachable) – směrování nenašel cestu k síti
 - 1: stanice nedostupná (host unreachable) – nelze se spojit se stanicí
 - 2: protokol nedostupný (protocol unreachable)
 - 3: port nedostupný (port unreachable)
 - 4: fragmentace nutná, ale byl nastavený příznak DF (Don't fragment)
 - 5: špatné zdrojové směrování (source route failed)
- 2, 3 od cílové stanice, 0, 1, 4, 5 od směrování

4

ICMP Time Exceeded

8b	8b	16b
TYPE = 11	CODE	kontrolní součet
nepoužito		
IP hlavička + vodního datagramu + 64 bit dat		

- CODE
 - 0: Time to Live Exceeded – TTL kleslo na nulu (příliš mnoho směrování po cestě)
 - 1: Fragment Reassembly Time Exceeded – vypršel čas na sestavení datagramu z fragmentů; pokud nedošel fragment 0, nic se neposílá
- TTL brání zacyklení
 - je nutné vždy při skoku ve směrování připočítat kontrolní součet IP hlavičky
- kód 0: od směrování, kód 1: od stanice

5

traceroute, tracepath

- zasílání zpráv od směrování, pokud TTL klesne na 0 se dá využít pro stopování cesty datagramu sítí
- nastavíme TTL na 1 a vyšleme datagram k cíli
- vrátí se nám od prvního směrování => zjistíme adresu prvního směrování
- nastavíme TTL na 2, ...
- běžně se používá TTL kolem 64
- počet přeskoků („hop“) z ČR do USA běžně kolem dvaceti
- traceroute a tracepath jsou programy, které zjišťují cestu k cíli
- traceroute používá UDP pakety, případně může používat ICMP echo request datagramy

6

traceroute, tracepath

```
traceroute to 195.113.31.123 (195.113.31.123), 30 hops max, 38 byte packets
 1 s1.chello.upc.cz (62.24.84.1) 86.565 ms 48.663 ms 21.908 ms
 2 cz-prg01a-ra2-ge0-0-0-v20.aorta.net (213.46.172.9) 17.375 ms 14.643 ms 5.852 ms
 3 at-vie01a-rd1-pos-1-0-0.aorta.net (213.46.160.53) 10.940 ms 25.298 ms 11.238 ms
 4 at-vie02a-ri1-pos-4-0.aorta.net (213.46.173.6) 12.161 ms 27.251 ms 11.681 ms
 5 Wien1.ACO.net (193.171.16.162) 24.182 ms 12.473 ms 12.142 ms
 6 195.113.179.149 (195.113.179.149) 13.623 ms 15.295 ms 11.803 ms
 7 r92-r41-oc48.cesnet.cz (195.113.156.126) 14.339 ms 13.646 ms 13.179 ms
 8 geovc-cesnet.pasnet.cz (195.113.69.53) 12.408 ms 35.663 ms 41.404 ms
 9 geruk-geovc.pasnet.cz (195.113.68.237) 12.076 ms 13.161 ms 13.301 ms
10 flor-ruk.pasnet.cz (195.113.69.118) 12.803 ms 13.360 ms 12.571 ms
11 karlingw-c.karlin.mff.cuni.cz (195.113.31.130) 12.472 ms 12.701 ms 12.412 ms
12 k5gw.karlin.mff.cuni.cz (195.113.31.137) 12.682 ms 12.995 ms 12.428 ms
13 atrey.karlin.mff.cuni.cz (195.113.31.123) 13.067 ms 12.311 ms 19.759 ms
```

7

ICMP Parameter Problem

8b	8b	16b
TYPE = 12	CODE	kontrolní sou et
pointer	nepoužito	
IP hlavi ka p vodního datagramu + 64 bit dat		

- nastala „jiná chyba“ a datagram byl zahozen
 - nap . chybná data v hlavi ce
- pokud je CODE = 0, pointer ukazuje do p vodního datagramu, kde nastala chyba

8

ICMP Source Quench

8b	8b	16b
TYPE = 4	CODE = 0	kontrolní sou et
nepoužito		
IP hlavi ka p vodního datagramu + 64 bit dat		

- sm rova je zahlcen a musí zahazovat datagramy
- za každý zahozený datagram vygeneruje tuto zprávu
- m že generovat zprávy i d íve (datagramy mohou být doru eny, i když pro n byla vygenerovaná zpráva Source Quench
- jedná se vlastn o žádost o snížení toku dat, které generuje zdrojová stanice
- neexistuje inverzní zpráva (zahlčení pominulo)

9

ICMP Redirect

8b	8b	16b
TYPE = 5	CODE	kontrolní součet
adresa nové brány (gateway)		
IP hlavička + vodního datagramu + 64 bit dat		

- CODE
 - 0: problém s datagramy pro síť
 - 1: problém s datagramy pro stanici
 - 2: problém s datagramy pro TOS a síť
 - 3: problém s datagramy pro TOS a stanici
- pokud první směr zjistí, že stanice má lepší cestu k danému cíli, pošle tuto zprávu
- filtrovat na vnějších rozhraních sítě!

10

ICMP Echo Request/Echo Reply

8b	8b	16b
TYPE = 8/0	CODE = 0	kontrolní součet
identifikátor		sequence number
data...		

- žádost o odpověď (TYPE = 8) je vyslána k cíli
- cílový uzel změnil adresy, například TYPE na 0 odešle zprávu (data zůstávají stejná)
- umožňuje detekovat:
 - funkčnost IP stacku cílové stanice
 - počet hopů, MTU po cestě (nastavením velikosti dat)
 - RTT (Round Time Trip) – doba přenosu dat tam a zpět

11

ping

```
qi@bug:~$ ping -s 5000 195.113.31.123
PING 195.113.31.123 (195.113.31.123) 5000(5028) bytes of data.
5008 bytes from 195.113.31.123: icmp_seq=1 ttl=53 time=892 ms
5008 bytes from 195.113.31.123: icmp_seq=3 ttl=53 time=114 ms
5008 bytes from 195.113.31.123: icmp_seq=4 ttl=53 time=578 ms
5008 bytes from 195.113.31.123: icmp_seq=5 ttl=53 time=154 ms
5008 bytes from 195.113.31.123: icmp_seq=6 ttl=53 time=133 ms
5008 bytes from 195.113.31.123: icmp_seq=7 ttl=53 time=122 ms
5008 bytes from 195.113.31.123: icmp_seq=8 ttl=53 time=103 ms
5008 bytes from 195.113.31.123: icmp_seq=9 ttl=53 time=100 ms
5008 bytes from 195.113.31.123: icmp_seq=10 ttl=53 time=99.3 ms
5008 bytes from 195.113.31.123: icmp_seq=11 ttl=53 time=103 ms
5008 bytes from 195.113.31.123: icmp_seq=12 ttl=53 time=105 ms
--- 195.113.31.123 ping statistics ---
12 packets transmitted, 11 received, 8% packet loss, time 11010ms
rtt min/avg/max/mdev = 99.376/227.984/892.493/248.939 ms
```

12

ICMP Timestamp

8b	8b	16b
TYPE = 13/14	CODE = 0	kontrolní součet
identifikátor		sequence number
as odeslání (zdroj)		
as příjemce (cíl)		
as odeslání (cíl)		

- odesílatel zaznamená čas odeslání
- příjemce čas přijetí a čas odeslání zpět
- slouží k zjištění doby přenosu dat k cílové stanici

13

ICMP Router Discovery Protocol

8b	8b	16b
TYPE = 9	CODE = 0	kontrolní součet
počet adres	velikost adresy (2)	životnost (s)
Router address 1		
Preference 1		
Router address 2		
Preference 2		

- RFC 1256
- 9: Router Advertisement
 - inzerování adresy směrovače, směrovač periodicky (nebo na žádost) inzeruje svoji adresu v síti a posílá ji na broadcast/multicast adresu všem připojeným uzlům
- 10: Router Solicitation
 - žádost stanice o adresu směrovače
 - jednoduchý datagram s TYPE = 10

14

ICMP

- další zprávy ICMP:
 - v dnešní době zastaralé, nahrazené RARP, BOOTP, DHCP
- 17/18: Address Mask Request/Reply
 - žádost o masku sítě
- 14/15: Information Request/Reply
 - žádost o adresu sítě

15

Příklad adres

symbolické jméno

DNS

IP adresa

ARP

MAC adresa

- MAC adresy jsou používány za účelem řízení, používají se k adresaci na linkové úrovni, jsou závislé na zařazení, slouží k rozlišení uzlu v rámci *lokální sítě*
- IP adresy jsou *univerzální v celé síti*, nezávislé na použité síťové technologii
- komunikující uzel má obě adresy, je potřeba mít mechanismus, jak zajistit převod mezi adresami
- Address Resolution (IP => MAC)
- Reverse Address Resolution (MAC => IP)

16

ARP

- Address Resolution Protocol
- protokol, který dokáže zjistit MAC adresu uzlu, pokud známe IP adresu
- kdy se to hodí? Směřujeme datagramy na určitý uzel (koncovou stanicí nebo směrovačem) v lokální síti, neznáme její linkovou (MAC) adresu
- dynamický, distribuovaný protokol, schopný reagovat na změny v síti
 - informace se podle potřeby obnovují
 - příkladová tabulka obsahuje v tabulce pouze dočasné položky
- pokud chce stanice znát MAC adresu jiného počítače v dané síti, vyšle linkový broadcast – ARP dotaz
- stanice, která rozpozná svoji IP adresu odpoví linkovým unicastem – ARP odpověď

17

ARP

- ARP pracuje na vrstvě „mezi“ linkovou a síťovou
 - používá rámce linkové (tedy nikoli IP), ale přenáší IP adresu
 - v Ethernetu používá typ rámce 0x0806 (IP používá 0x0800)
- žádost vyšle IP vrstva když zjistí, že je potřeba odeslat rámec a není známá MAC adresa příjemce
 - vyšle se jen jeden ARP dotaz, i když rámec při vyslání je víc

6B	6B	2B	28B
cílová MAC	zdrojová MAC	typ	ARP žádost/odpověď

18

ARP

- typ média: Ethernet: 1, ATM: 16
- protokol: pro IP 0x0800
- délka MAC adresy: 6
- délka IP adresy: 4
- operace: request: 1, response: 2
- zdrojová MAC a IP adresa
 - adresa odesílatele žádosti nebo toho, kdo odpovídá
- cílová MAC a IP adresa
 - adresa příjemce (v případě žádosti je MAC adresa broadcast (všechny 1))

Typ média	
Protokol	
Délka MAC adresy	Délka IP adresy
operace	
Zdrojová MAC adresa	
Zdrojová IP adresa	
Cílová MAC adresa	
Cílová IP adresa	

19

ARP algoritmus

- počítač chce poslat data (IP datagram) jinému počítači v síti
 - potřebuje zjistit MAC adresu příjemce
 - podívá se do cache, je-li tam položka => OK
 - není, musí se použít ARP protokol
- vyšle rámec s broadcast cílovou MAC adresou (a s vyplněnými ostatními)
- příjemce zkontroluje, jedná-li se o jeho IP adresu, ne => rámec zahodí
- vyplní svoji MAC adresu a prohodí páry adres, aby odpovídaly odesílateli/příjemci
- odešle rámec zpět (unicastem)
- do ARP tabulky si přidá adresu tazatele (pravděpodobně s ním bude komunikovat)

20

Proxy ARP

- node, který v síti (směrová) odpovídá na ARP dotazy za uzel, který je „skrytý“ za ním
- odpovídá svojí adresou (a datagramy poté směruje správným směrem)
- vlastně rozšiřuje lokální síť přes směrová
- směrová v síti „nevidí“

21

RARP

- Reverse Address Resolution Protocol
- IP adresa bývá na uložena v konfiguracním souboru na disku
 - MAC bývá v ROM na síťové kartě (nebo ekvivalentu)
 - vzniká problém s bezdiskovými stanicemi – znají MAC, ale ne IP adresu
- formát rámce stejný jako u ARP, ale operace je 3 pro request, 4 pro response
- typ v ethernetovém rámci je 0x8035

Typ média	
Protokol	
Délka MAC adresy	Délka IP adresy
operace	
Zdrojová MAC adresa	
Zdrojová IP adresa	
Cílová MAC adresa	
Cílová IP adresa	

22

IPv6

- nejnovější protokol, ve fázi testování
- eš:
 - vyerpání adres
 - zabezpečení (povinně implementované)
 - mobilitu
- adresy IPv4: 2^{32} (několik desítek miliard)
 - reálně použitelné jen asi dvě miliardy
 - počet přístrojů (mobilní telefony, PDA, mnoho zařízení, které by bylo vhodné?) připojit k Internetu (lednice, ...), auta)
 - dohodnuté řešení způsobují komplikace (NAT)
 - Asie dostala málo adres IPv4
 - bylo nutno rozšířit adresy
 - rozhodovalo se, zda budou 64bitové nebo 128 bitové

23

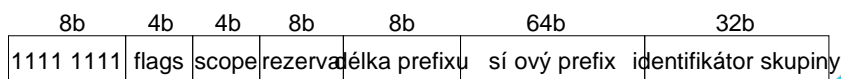
Adresy IPv6

- 128 bitů dlouhé
 - to je hodnota: každý člověk na zemi by jich mohl mít 4 miliardy
 - mohl by vystit na dlouhou dobu (nebude-li se plýtvat)
- zapisují se jako osm šestnáctibitových číslic
 - například: 2001:0700:0230:0003:0000:0000:0000:0001
- adresa se může zkrátit vynecháním spojitého úseku nul (jen jedenkrát v adrese)
 - 2001:700:230:3::1
- IPv6 nemá broadcast adresy, používají se
 - unicasty (jednomu příjemci)
 - multicasty (více příjemcům)
 - anycasty (jednomu, nejbližšímu příjemci)

24

Tídy adres IPv6

- multicast a anycast adresy mají definován dosah (scope):
 - link-local: platí v jednom subnetu
 - site-local: platí v jedné privátní síti
 - global: platí v Internetu
- prefixy se používají podobně jako u CIDR IPv4
- loopback adresa ::1/128
- nedefinovaná adresa (uzel nemá přidělenou adresu) ::/128
- multicast (skupinová) adresa
 - FF00::/8

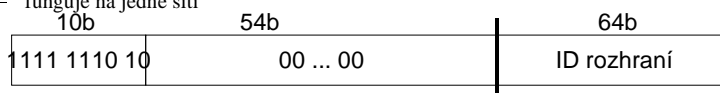


25

Tídy adres IPv6

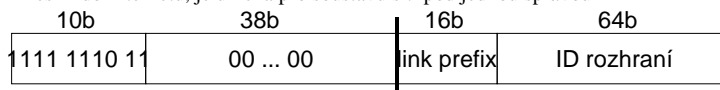
- individuální lokální adresa segmentu: FE80::/10

- funguje na jedné síti



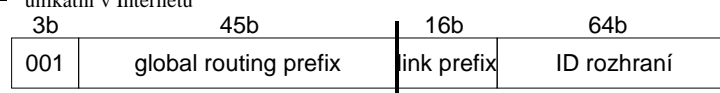
- individuální lokální adresa místní: FEC0::/10

- nesmí do Internetu, je určena pro soustavu sítí pod jednou správou



- individuální globální adresa: 001/3

- unikátní v Internetu



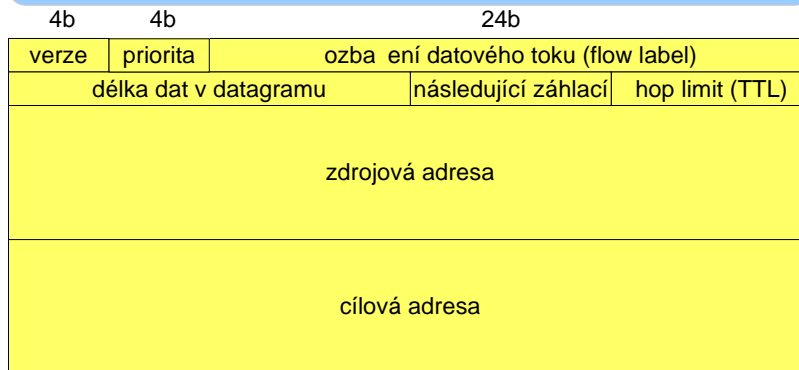
26

Autokonfigurace adres IPv6

- použije se síťová část adresy
 - ta se zjistí pomocí odposlechu, router solicitation, router advertisement
- k ní se připojí unikátní část (ID rozhraní)
 - musí být unikátní na dané podsíti
 - většinou se získá z MAC adresy
- EUI-64: Extended Unique Identifier
 - do MAC adresy se vloží 0xFFFE

27

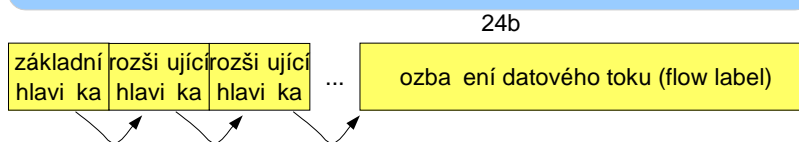
Formát datagramu IPv6



- verze: 6, priorita+flow label: pro QoS, délka dat: doplňkové hlavičky a data
- následující záhlaví: typ následující za povinným záhlavím, případně číslo transportního protokolu, hop limit: jako TTL v IPv4

28

Formát datagramu IPv6



- základní hlavička je co nejjednodušší
 - je pevné délky
 - neobsahuje kontrolní součet
 - neobsahuje pole umožňující fragmentaci (označení a sestavení fragmentů)
- rozšířující hlavičky (záhlaví)
 - šifrování
 - informace pro směrování a po cestě
 - možnosti pro cílovou stanici
-

29

IPv6 a fragmentace

- minimální MTU je 1280B
 - v IPv4 to bylo 576
- k fragmentaci po cestě nedochází
 - fragmentuje pouze vysílající stanice
 - pokud je potřeba po cestě fragmentovat, pošle se ICMPv6 zpráva (Packet Too Big) vysílající stanici a datagram se zmenší
 - jako kdyby všechny datagramy byly nastaveny flag DF
- „plně“ implementace mají používat Path MTU discovery
- jednoduché implementace mají generovat datagramy max. velikosti 1280B

30