

Směrování, směrovací algoritmy a protokoly

Přepínání okruhů:

- explicitní žádost sítě o vytvoření /zrušení okruhu koncovým zařízením
- rezervovaná kapacita po celou dobu
- garance kvality služby
- (neekonomické pro síť)
- Při výpadku se vyhledává nová cesta

Přepínání paketů:

- ARPA
- Rychlé zotavení při výpadku
- Do dnešního Internetu
- Redundantní spoje
- D. jednotka – paket
 - Id příjemce
 - Každý paket může jít jinou cestou
 - Může být pozdržen
- „Hop by hop“

Virtuální kanál:

- Vytvoření logického okruhu s přepínáním paketů
- Řízen koncovým zařízením
- Hledání cesty při vytvoření
- Id Okruhu

- Pakety jdou stejnou cestou nemůžou se předbhat

Směrování

- Hledání cesty sítí
- S O sítě při vytváření spojení
- S přepínáním pkt při přenosu jednotlévého pkt

Směrovací Algoritmy

- 3.vrstva RM OSI
- Požadujeme
 - Jednoduchost
 - Robustnost
 - Stabilitu
 - Férovost
 - Optimalitu

Směrovací tabulka

- <cílová adresa(+maska), výstupní rozhraní|next hop, metrika>
- Nutno vždy projít celou tabulku

Implicitní cesta (default route)

- Pro síť připojení k vyšším sítím
- Pro pakety které nemají cílovou adresu ... default route
- Snížení počtu záznamů v tabulce

Typy a přístupy ke směrování

Přístupy – centralizované distribuované (každý směrovač zná vzdálenost), izolované (BW learning, Hor. Br., Flooding)

Typy – Statické a dynamické

...

...

...

Dělení algoritmů

- Distance Vector
- Link State

DVA – problém počítání do nekonečna (Nekonečno nahrazeno průměrem sítě + 1, Split horizon směrovač neposílá info do používaného rozhraní)

- Trigger update – po výpadku/náběhu se nečeká na periodu časovače a rovnou se rozesílá směrovací tabulka
- Poisson reverse – jako split horizont
- Hold down – po ztrátě nejlepší cesty po holddown dobu nepřijímáme cesty od jiných směrovačů
- DVA – RIP, IGRP

LSA – Na základě stavu linky (funkčnost, cena)

- Neustálé sledováním, okamžitý update
- LSA – OSPF. IS-IS

Dijkstra(OSPF), Floyd, Ford-Fulkerson(RIP)

Směrování v TCP/IP

- Vnitřní – Otevřené :RIP, OSPF, Firemní: IGRP, EIGRP(cisco), NLSP(Novell)
- Vnější – (Mezi autonomními systémy) BGP – path vector

- Beztrždní adresy sm. Protokoly:
 - Vyžadují konstantní masku podsítě
 - Spojitost podsítí
 - Problémy s DV (RIP, IGRP)
- VLSM: Variable length subnet mask

Bezpečnost v počítačových sítích

- Firemní politika, Viry
- Utajení (posluchač na kanále datům nerozumí), Autentizace (ověření uživatele), Integrita (nemodifikovaná data), Nepopiratelnost – Zdroj dat nemůže popřít odeslání

Možnosti implementace:

- Utajit algoritmus
- Zavést klíče parametrizující algoritmus

Symetrický systém

- Sdílený klíč
- DES, 3DES, AES

- Problém distribuce klíčů
- Zakódování a odkódování stejným klíčem + test smysluplnosti (hash)
- Integrita: Zpráva+ sdílený klíč = hash
- Klíče se generují jako doplňující se pár(šifra, dešifra)
- Pomalé

Asymetrický systém

- Digitální podpisy
- Využívá se pro předávání klíčů pro symetrický systém

Cert. Autorita

- Je jí důvěřováno
- Vytváří dvojice klíčů
- Alice -> Data+K_{pub}->Hash+K_{pub} -----
Data+K_{priv}->Hash+K_{priv} -: Bob

L2 – Hop by hop, L2TP (tunneling)

L3 – Nezávislé na médiu, IPSec

L4 – Secure Socket Layers, Jen TCP

L7- Jednotlivé aplikace, např MIME

Filtrace provozu

- Bezstavová (paketové filtry)
- Výsledkem propuštění nebo zahození paketu
- Pouze na základě dat obsažených v paketu
- Problém s inspekcí 4. a vyšší vrstvy při použití

fragmentace

- Stavová (transparentní nebo proxy server)
- Rekonstrukce datových toků
- Potřeba udržovat stav pro každý tok
- omezená škálovatelnost

Paketové filtry

AccessControl Lists – ACL

- Na rozhraních směrovačů
- Sekvence položek zakazujících nebo povolujících
- Na konci implicitně zákaz veškerého provozu

Návrh

- Rozhraní
- Vstupní/výstupní
- Kritéria

access-list <acl_number> {permit | deny}

<PROTOCOL>

<source-IP-addr> <source-addr-wildcard>

[<source-port>] <destination-IP-addr>

<destination-addr-wildcard> [<destinationport>]

[protocol-dependent-options]

access-list 101 deny ip 158.196.135.0 0.0.0.255 any

access-list 101 permit tcp any host 158.196.135.103 eq
25

access-list 101 permit tcp any host 158.196.135.102 eq
80

access-list 101 permit tcp any host 158.196.135.102 eq
443

access-list 101 permit tcp any host 158.196.135.102 eq
22


```
access-list 101 permit udp host 200.1.1.100 eq 53  
158.196.135.0 0.0.0.255
```

```
access-list 101 permit icmp any 158.196.135.0  
0.0.0.255 echo-reply
```

```
access-list 101 permit tcp any eq 80 host  
158.196.135.101 established
```

```
access-list 101 permit tcp any eq 443 host  
158.196.135.101 established
```

```
access-list 101 permit tcp any eq 22 158.196.135.101  
0.0.0.255 established
```

```
interface s0
```

```
ip access-group 101 in
```

FireWally

- Oddělení důvěryhodné a nedůvěryhodné části
- Transparentní chování, proxy server
- HW/SW

Bezpečnost a NAT

- Skrytí vnitřní struktury
- Dyn. NAT, komunikace dovnitř povolena jen v době spojení ven

VPN

- Provátní síť na sdílené infrastruktuře
- Tunelování – virtuální dvoubodové spojení
- IPSec – architektura pro technickou realizaci tunelů

Bezpečnost technologií LAN WAN

- ARP – možnost neregulární odpovědi, řešení v cache směrovče
- Směrování – ochrana proti generování falešné směrovací informace (RIPv2, OSPF, EIGRP, BGP)
- Přepínané sítě - omezení počtu připojených stanic
- Bezpečnost DNS – falešné mapování doménových jmen, falešní mx záznamy, řešení DNSSec

Zabezpečení managementu síťových prvků

- Jmeno a heslo
- Idle timeout

- Specifikace povolené adresy pro management
- Oddělený management VLAN

Útoky

- SYN Flood, Ping FLOOD

Služby internetu

Emulace terminálu

- Telnet (tcp/23)
- NVT – virtuální znakové zařízení s klávesnicí
- SSH – secure shell, podobný telnetu

Přenos souborů

- FTP obousměrný přenos souborů mezi dvěma systémy
 - USER, PASS
 - LIST
 - PORT
 - TYPE
 - RETR,STOR
 - ABORT

- PASV
- QUIT
- Volitelně pasivní/aktivní režim, spojení navazuje server,
- TFTP – nad UDP

Elektronická pošta

- UA-User agent
- MTA Message Transfer Agent
- Mailbox
- Textově orientované protokoly
- SMTP bez autentizace
- POP IMAP pomocí cleartext hesla nebo MD5
- POP3S, IMAPS – šifrované
- Struktura zprávy
 - Obálka (odesílatel, příjemce)
 - Hlavička (seznam dvojic jmeno:hodnota)
 - Tělo
 - NVT ASCII
 - MIME Multimedia Internet Mail extension
- Předávání zpráv
 - Z klienta přímo na poštovní server příjemce
 - Z klienta na poštovní server
 - Z poštovního klienta na bránu do jiných sítí

- SMTP (Od poštovního klienta d serveru a mezi servery)
 - TCP/25(Nešifrováno neautentizováno)
 - Textové příkazy
 - HELO – klient
 - MAIL FROM: Odesílatel
 - RCPT TO: příjemce
 - DATA: uvozuje samotnou zprávu
 - TURN: Výměna rolí
 - QUIT: Ukončení spojení
 - VRFY: existence mail listu(Kvui bezpečnosti zakázáno)
 - EXPN: rozvinutí listu(Kvui bezpečnosti zakázáno)
- MIME
 - Strukturovat tělo zprávy
 - Určení interpretace souborů
 - Způsob kódování dat bin souborů
 - MIME-Version:
 - Content-Type: text, multipart, message, application, image, audio,video
 - Content-Transfer-Encoding: 7bit (NVT ASCII, default), quoted-printable, base64,binary
 - Content- Description
- POP3
 - Nad TCP port 110

- Nešifrováno
- USER PASS
- listopad RETR
- DELE
- RSET
- QUIT
- UIDL (identifikátor)
- TOP Výpis prvních n řádků
- IMAP
 - Dokonalejší POP3
 - TCP/143
 - Pro mobilní klienty
 - Selektivn načítání zpráv
 - Možnost vyhledávání ve zprávách přímo na serveru
 - Autentizační mechanismy
 - Podpora složek

World Wide Web

- CERN
- protokol://uživatel:heslo@stroj:port/cesta

http – hypertext transfer protocol

- TCP/port 80
- Návaznost na URL

- Požadavek: Příkaz, hlavička, prázdný řádek, data-obsah formuláře
- Odpověď: Odpověď, hlavička, prázdný řádek, data-obsah WWW stránky
- GET, HEAD, POST/PUT, DELETE, LINK, UNLINK, OPTIONS, TRACE
- Hlavičky požadavku: Accept (Charset, encoding, language), Authorization, IF Modified Since. Referer, User Agent
- Hlavičky odpovědi: Allow, Content encoding, content language, length, type, MIME-version, Date, Expires, Last Modified, Location, . Retry after, Server, WWW authenticvate, Refresh
- HTTP 1.0 (RFC 1945) – spojení iniciuje klient, každý dokument po zvlášť TCP spojení
- HTTP 1.1 (RFC 2068) – Virtual hosts, podržení spojení, Přenost části dokumentu, Komprese dat
- HTTPS – Secure

Cookies

- Podpora stavové transakce
- Využívá hlavičku (set-cookie serverklient, cookie klientserver)
- Obsah

- Jméno hodnota
- Server, path
- Flag secure
- Comment
- Max age

BootstrapProtocol (BOOTP)

- Konfigurace TCP/IP na základě MAC
- Poskytuje IP adresu, masku, default gateway, boot TFTP server, Boot image
- Šíření v UDP broadcastech

DHCP

- Dočasné přiřazení adres klientům na žádost z poolu volných adres
- Lze přidělovat stejné vždy parametry
- Žádost UDP broadcastem
- Oproti BOOTP umí přidělit více parametrů
 - DHCP Discover- vyhledání serveru
 - DHCP Offer – Nanízí parametry
 - DHCP Request – klient žádá o zarezervování jedné znabídek
 - DHCP Ack – žádaný server potvrzuje rezervaci

Domain Name Systém DNS

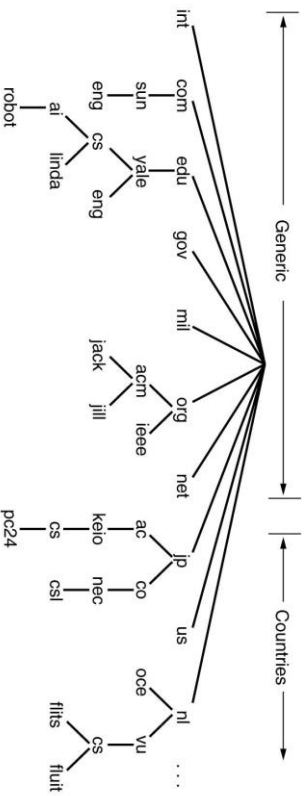
- Mapování doménových jmen(logických) na IP adresy
- RFC 1034, 1035, koncepce, jmenný prostor
- Využívá distribuovanou databázi
- („name servery“, „jmenné servery“)

Doménová jména

- Stromová struktura
- Spojením uzlu stromu se všemi jmény uzlů na cestě ke kořeni (oddělovačem je tečka)
- Komponenta 63 znaků
- Jméno 256 znaků

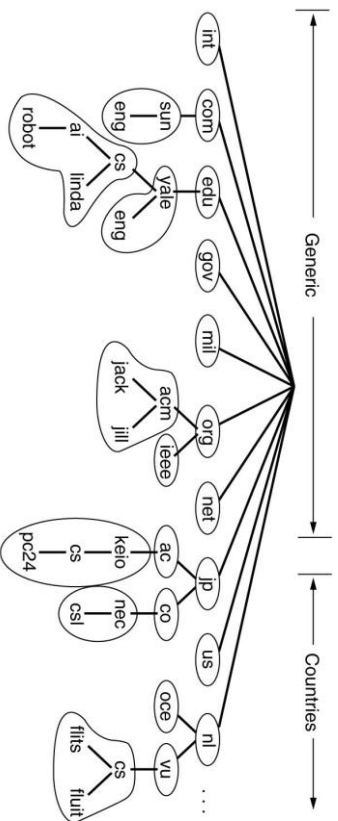
Generické domény nejvyšší úrovně:

- Edu, com, mil, gov. Net, org,
- Označení států, cz uk at



Zóna

- Část stromu uložená na jednom DNS serveru
- DNS server je autoritativní pro domény obsažené v jím spravované zóně



Vyhledávání v databázi DNS

- Provádí SW klienta
- Začíná se od rootu serverů a pokračuje po komponentech
- Při datu na nespravované jméno
 - o Odmítnutí dotazu, rekurzivní vyhledávání

Primární a sekundární name servery

- Data zóny permanentně uložena v souborech na primárním serveru
- Caching only DNS servery nejsou autoritou pro žádnou doménu, jen provádějí překlad a caching

Resolver

Část SW klienta která provádí komunikaci s DNS serverem

Konfigurace:

- default domain pro relativní jména
- první a záložní (rekurzivní) jmenné servery
- u některých systému, které provádějí vyhledání samy, konfigurace seznamu kořenových jmenných serverů

Komunikační protokol DNS

- Resolver – jmenný server
- Jmenný server – Jmenný server
- Běžné dotazy – UDP (53)
- Dlouhá data –TCP (53)

Záznamy databáze DNS (Resource Records)

Univerzální formát

- Doménové jméno
- Typ záznamu
- Data proměnné délky
- Time to live

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

; Authoritative data for cs.vu.nl

cs.vu.nl.	86400	IN	SOA	star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.	86400	IN	TXT	"Divisie Wiskunde en Informatica."
cs.vu.nl.	86400	IN	TXT	"Vrije Universiteit Amsterdam."
cs.vu.nl.	86400	IN	MX	1 zephyr.cs.vu.nl.
cs.vu.nl.	86400	IN	MX	2 top.cs.vu.nl.

flits.cs.vu.nl.	86400	IN	HINFO	Sun Unix
flits.cs.vu.nl.	86400	IN	A	130.37.16.112
flits.cs.vu.nl.	86400	IN	A	192.31.231.165
flits.cs.vu.nl.	86400	IN	MX	1 flits.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	2 zephyr.cs.vu.nl.
flits.cs.vu.nl.	86400	IN	MX	3 top.cs.vu.nl.
www.cs.vu.nl.	86400	IN	CNAME	star.cs.vu.nl
ftp.cs.vu.nl.	86400	IN	CNAME	zephyr.cs.vu.nl

rowboat		IN	A	130.37.56.201
		IN	MX	1 rowboat
		IN	MX	2 zephyr
		IN	HINFO	Sun Unix

little-sister		IN	A	130.37.62.23
		IN	HINFO	Mac MacOS

laserjet		IN	A	192.31.231.216
		IN	HINFO	"HP Laserjet IIISi" Proprietary

Konverze zónového souboru

- @ implicitní adresa
- Pokud v levé části není jméno, bere se z předchozího řádku
- Jména neukončení tečkou jsou relativní, doplňují se \$ORIGIN
- Direktivou \$TTL lze stanovit impl. hodnotu pro TTL

V databázi DNS (všech) root serverů:

cz. NS dns-server.eunet.cz.

dns-server.eunet.cz. A 120.0.1.2

V databázi DNS serveru dns-server.eunet.cz:

vsb.cz. NS dns.vsb.cz.

dns.vsb.cz. A 158.196.1.100

V databázi DNS serveru dns.vsb.cz:

www.vsb.cz. A 158.196.1.200

Reverzní domény

- Mapování IP na doménová jména
- Doména in-addr.arpa., pak rozdělení na NS nižších úrovní po bajtech IP adresy

Příklad:

Doménové jméno pro záznam k reverznímu překladu

adresy 158.196.146.10 je 10.146.196.158.in-addr.arpa.

Delegace reverzních domén u beztrždních adres

- RFS 2317 (1998)
- Při změně PTR záznamu kontaktuje poskytovatele DNS
- Řeší odkazy Alias – CNAME z DNS serveru reverzní domény poskytovatele pro všechny adresy podsítě na speciální jméno domény na DNS serveru zákazníka

Dynamická DNS (DDNS)

- RFC 2136
- Dynamické registrování IP adres
- DHCP
- Problém s autentizací,

IPv6

- Adresní prostor - 128bitů ($3,4 * 10^{E38}$)
- Uni, multi, any část
- Jednotné adresní schéma (no NAT)
- Podpora QoS
- Snadný přechod z IPv4
- Bezpečnost, šifrování

Datagram IPv6

- RFC 2460
- Verze 4b
- Třída provozu 8b
- Značka toku 20b
- Délka dat za hlavičkou 16b
- Další hlavička 8b
- Dosah 8b
- Odesílatel a příjemce (2x128b)

0	3	7	15	23	31
Ver	HL	ToS	Total length		
Identification		F	Fragment offset		
TTL	Protocol	Header checksum			
Source address (32 bits)					
Destination address (32 bits)					
Options				Padding	

IPv4 header

0	3	11	15	23	31
Ver	Traffic class	Flow label			
Payload length		Next header	Hop limit		
Source address (128 bits)					
Destination address (128 bits)					

Basic IPv6 header

Pole identifikace toku dat

- Jednoznačná identifikace dílčího toku
 - IP odesilatele
 - IP cíle
 - Značka toku (určuje odesílatel libovolně)
- Možnost rychlejšího směřování
- Možnost zajištění šířky pásma
- Životnost položky v paměti směrovače max 6s
- Dosah
 - Náhrada TTP
 - Hop sníží hodnotu

Ztracené položky IPv4

- Délka hlavičky, Identifikace, Kontrolní součet (nejsou již třeba)
- Rozšiřující volby, fragmentace (nahrazeny mechanismem zřetěžením rozšiřujících hlaviček)

Zřetězení rozš. Hlaviček

- Každá r. hlavička je samostatný blok
- Propojení pomocí položky „Další hlavička)

- Poslední r. hlavička ukazuje na typ dat paketu (Zastupuje položku „Protokol“ z IPv4)
- Řetěz obsahuje pouze hlavičky které jsou nutné

Vybrané hodnoty položky „další hlavička“

Ro z š i ř u j í c í h l a v i č k y

- 0 volby pro všechny
- 43 směrování
- 44 fragmentace
- 50 šifrování obsahu (ESP)
- 51 autentizace (AH)
- 59 poslední hlavička
- 60 volby pro cíl
- 62 mobilita
- Typ nesených dat
- 6 TCP
- 8 EGP
- 9 IGP
- 17 UDP
- 46 RSVP
- 47 GRE
- 58 ICMP

Doporučené pořadí rozšiřujících hlaviček

1. základní hlavička IPv6
2. volby pro všechny
3. volby pro cíl (pro první cílovou adresu)
4. směrování
5. fragmentace
6. autentizace
7. šifrování obsahu
8. volby pro cíl (pro konečného příjemce)

Rozšiřující hlavička Volby

- Pro všechny (typ 0), pro cíl (typ 60)
- Délka 16 B

8b	8b	8b	8b
Další hlavička	Délka dat	Volby	

Struktura Volby

- ● Samotná volba má části
 - typ (1 B)

- délka (1 B)
 - data
- ● 2 nejvyšší bity typu určují co s neznámou volbou
 - 00 – přeskočit a pokračovat dalšími volbami
 - 01 – zahodit datagram a nepokračovat dalšími volbami
 - 10 – zahodit datagram a odesilatel poslat ICMP zprávu
 - 11 – zahodit datagram a ICMP poslat jen pokud cílová adresa nebyla
 - multicastová
- ● třetí nejvyšší bit určuje možnost změny volby po cestě
 - 0 – volba se nesmí změnit
 - 1 – volba se může změnit

Definované typy Voleb

- ● Pro všechny
 - 0 – Pad1
 - 1 – PadN

- 5 – Upozornění směrovače
- 194 – Jumbo obsah (začíná bity 11)
- ● Pro cíl
 - 0 – Pad1
 - 1 – PadN
 - 201 – Domácí adresa

Rozšiřující hlavička Směrování

8 b	8 b	8 b	8 b
Další hlavička	Délka dat	Typ směrování = 0	Zbývá segmentů
Rezerva = 0			
Adresa [1]			
Adresa [2]			
.			
Adresa [n]			

Rozšiřující hlavička Fragmentace

- ● IPv6 nedovoluje fragmentovat na cestě
 - fragmentuje tedy výlučně odesílatel
- ● Vyžaduje min. délku MTU 1280 B (IPv4 576 B)
- ● Posun fragmentu je v osmicích bajtů od začátku fragmentované
 - části dat
- ● Příznak M určuje, zda-li jsou další fragmenty

<i>8 b</i>	<i>8 b</i>	<i>13 b</i>	<i>2b</i>	<i>1 b</i>
Další hlavička	Rezerva = 0	Posun fragmentu	R ez.	M
Identifikace				

Jumbogramy

- Použití oznámeno volbou
- Délka dat je určena 32 bity
 - Velikost je tedy 64 kB až 4 GB
- Délka dat v základní hlavičce se vynuluje

8 b	8 b	8 b	8 b
		Typ volby = 194	Délka volby = 4
Délka jumbo dat			

Adresy IPv6 (128b)

- ● Typy
 - Individuální (unicast)
 - Skupinové (multicast)
 - Výběrové (anycast) – “nejbližší” člen skupiny
- ● Rozsah platnosti
 - Globální
- ●
 - <http://www.iana.org/assignments/ipv6-unicast-address-assignments>
 - Linkové (fe80::/10) – zahrnují EUI64
- ● pro servisní protokoly, směrovací protokoly, autokonfiguraci
 - Unique local address (fc00::/7)
- ● pro sítě nepřipojené k Internetu (obdoba privátních adres IPv4)

- ● směrovatelné jen mezi skupinou spolupracujících sítí
- ● nahrazují původní “site-scope” adresy

Zápis IPv6 adres

- ● Standardní zápis
- FEDC:BA98:7654:1230:FECD:BACD:7546:3210
- ● Zkrácené zápisy
- – Mějme adresu
- 2001:0718:1001:0000:0000:69ff:fe06:e407
- – Zkrácení počátečních nul
- 2001:718:1001:0:0:69ff:fe06:e407
- – Vynechání nul
- 2001:718:1001::69ff:fe06:e407

Prefixy sítí

- ● Příslušnost k dané síti je dána prefixem
 - všechna rozhraní na jedné síti mají stejný prefix
 - podobné jako CIDR
- ● IPv6_adresa / délka_prefixu

Speciální IPv6 adresy

- ● `::/128` – unspecified address
- ● `::1/128` - loopback
- ● `::ffff:0:0/96`
- – IPv4 mapped addresses
- – Poslední 4 bajty jsou IPv4 adresou
- ● Příklad zápisu:
`0:0:0:ffff:0:0:158.196.158.77`
- ● Adresy pro mechanismy přechodu
- – `2001::/32`
- ● Teredo tunneling
- – `2002::/16`
- ● 6to4 tunneling

Skupinové adresy (`FF00::/8`)

- ● Význam bitu T
- 1 – trvalé přiřazení
- 0 – dočasné přiřazení
- ● Význam rozsahu
- 1 – lokální uzel
- 2 – LAN
- 5 – místo
- 8 – organizace

- E – globální

Vyhrazené skupinové adresy

- ● FFxx::1 – všechny stanice (počítače i směrovače)
- ● FFxx::2 – všechny směrovače
- ● FFxx::9 – všechny směrovače provozující RIP
- ● a další...

Identifikátor rozhraní- modifikované EUI-64

- ● pro Ethernet (a varianty)
- mezi 3. a 4. bajt MAC adresy se vloží 16 bitů FFFE

Povinné adresy rozhraní

- ● Koncová stanice
 - lokální linková adresa (FE80::....)
 - všechny individuální adresy
 - lokální smyčka (::1)
 - skupinová adresa pro všechny uzly (FF01::1)

- skupinová adresa pro vyzývaný uzel pro všechny přidělené
- individuální (a příp. výběrové) adresy
 - všechny skupinové adresy
- ● Směrovač
 - výběrová adresa pro směrovače v podsíti
 - všechny výběrové adresy, které byly přiděleny
 - skupinová adresa pro všechny směrovače (FF05::2)

ICMPv6

- ● nejvyšší bit typu
- 0 – chyba
- 1 – informační

8 b	8 b	16 b
Typ	Kód	Kontrolní součet
Tělo zprávy		

ICMPv6 typy a kódy I

- typ kód popis
- 1 nedoručitelný datagram
- 1 0 ve směrovací tabulce neex. směr pro adresu
- 1 1 spojení s cílem je administrativně uzavřeno
- 1 3 nedosažitelná adresa
- 2 0 příliš velký datagram
- 3 čas vypršel
- 3 0 dosažen max. počet hopů
- 3 1 vypršel čas na sestavení datagramu z fragmentů
- 4 chybný parametr
- 4 0 chybné pole v záhlaví
- 4 1 nepodporovaný typ v poli
- typ kód popis
- 128 0 žádost o echo
- 129 0 echo
- 133 0 žádost o směrování
- 134 0 oznámení o směrování
- 135 0 žádost o linkovou adresu (náhrada ARP)

- 136 0 oznámení o linkové adrese
- adrese (náhrada ARP)
- 137 0 změň směrování

DNS a IPv6

- ● RFC 3596 (vychází z RFC 1886)
- ● adresy typu AAAA
 - konstrukce se záznamy typu A6 zrušeny
- ● reverzní dotazy do domény ip6.arpa
- ● named.conf
- zone "1.0.0.1.8.1.7.0.1.0.0.2.IP6.ARPA" {
type master; file
- "pri/vsb6.rev"; };
- ● příklad pro host.db
- michelle IN AAAA
2001:718:1001:9e:a00:69ff:fe06:e407

- ● příklad pro reverzní záznam
- 7.0.4.e.6.0.e.f.f.f.9.6.0.0.a.0.e.9.0.0 IN PTR michelle.vsb.cz.

Podpora v OS

- ● *BSD
- KAME Project – www.kame.net
- ● Linux
- standardní jádro
- USAGI Project – www.linux-ipv6.org
- ● Microsoft Windows
- starší než 2000 – podpora IPv6 není a nebude
- 2000 – stáhnout a instalovat záplatu
- XP, Vista – již obsaženo

Další

- ● Hledání linkových adres (náhrada ARP)
- ● Podpora vícenásobných adres
- ● Automatická konfigurace
- ● Směrování

- RIPNG, OSPFv6, ISIS, EIGRP, BGP4+
- ● IPv6 Multicasting
- ● Mobile IP
- ● Bezpečnost IPv6
- ● Připojení/propojení IPv6 sítí a izolovaných IPv6 strojů
 - dual-stack hosts, IPv4-kompatibilní adresy
 - statické tunely
 - dynamické tunely – 6to4, Teredo, ISATA