INVESTICE DO ROZVOJE VZDĚLÁNÍ
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky

IP adresy

Tato kapitola navazuje na kapitoly Síťová komunikace a TCP/IP protokoly a podrobněji rozebírá problematiku adresování v počítačových sítích. Po jejím prostudování bude čtenář schopen vysvětlit jak vypadá síťová IP adresa verze 4 i verze 6, vysvětlit principy členění adres do tříd, mechanismy sloužící pro vyřešení nedostatku IP adres, znát základní odlišnosti v IPv4 a IPv6.

Klíčové pojmy:
IPv4, IPv6, maska sítě, třídy adres, privátní adresy, vyhrazené adresy, loopback, broadcast, multicast, CIDR, subnetting, supernetting, NAT, PAT, unicast, anycast, dosah, objevování sousedů, IPv4 překládaná adresa, IPv4 kompatibilní adresa, bezpečnostní asociace.

IP protokol – shrnutí poznatků

IP protokol je přenosový protokol síťové vrstvy v architektuře TCP/IP. Protokol slouží k nespolehlivému, nespojovanému přenosu dat mezi zdrojovým počítačem a příjemcem. Protokol je implementován v koncových uzlech i ve směrovačích.
V současnosti jsou paralelně používány dvě verze protokolu, dominuje stále verze IPv4, současně je používána i novější verze IPv6 tam, kde je to možné.

IP adresa (IPv4)

IP protokol pro identifikaci komunikujících partnerů používá IP adresy. IP adresa je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti. Starší variantou je IP adresa verze 4, která je tvořena čtyřmi osmibitovými čísly, oddělenými tečkou (celkem 32 bitů). IP adresa může být zapsána v desítkové soustavě nebo ve dvojkoé soustavě. V binární soustavě může být na každé pozici nula nebo jednička, v desítkové soustavě mohou jednotlivá čísla nabývat hodnot 0 - 255.
Tvar IPv4 adresy v binární podobě: xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx, např. `11011100.11110000.11000010.10000001`
Tvar IPv4 adresy v desítkové soustavě: ddd.ddd.ddd.ddd, např. `220.240.194.129`.
Adresní prostor tvořený takto vzniklými adresami nedostačuje celosvětovým potřebám, proto je protokol IP verze 4 postupně nahrazován novější variantou protokolu IP verze 6, která počítá se 128 bitovými adresami.

Struktura IP adresy verze 4:

Správa IP adres

Přidělování a správu IP adres mají celosvětově na starosti organizace ICANN a IANA, které provádí registraci generických domén a také zastřešují regionální organizace, které mají na starosti přidělování IP adres na jednotlivých kontinentech. Kromě toho agentura IANA spravuje kořenové DNS servery a vytváří pravidla pro ICANN.
Regionální organizace dále přidělené bloky adres rozdělují jednotlivým oblastním providerům a dalším organizacím. V České republice je to sdružení CZ.NIC, které má na starosti provozování registru doménových jmen, zabezpečení provozu domény nejvyšší úrovně .cz a další úkoly.

Strukturu lokální části sítě, tj. zda bude rozdělena na podsítě, jaká část adresy bude věnována na rozdělení do podsítí, přidělování IP adres jednotlivým zařízením v podsítích řídí správce lokální sítě.

Maska sítě

Hranice mezi adresou sítě a počítače určuje tzv. *maska sítě*. Maska sítě je opět 32 bitová hodnota, která v bitovém tvaru obsahuje jedničky tam, kde se nachází adresa sítě a nuly na místech, kde je adresa počítače. Maska sítě je součástí konfigurace síťového rozhraní, předává se protokolem DHCP.

```
Příklad masky: 11111111.11111111.11111111.00000000
```

Třídy adres

Autoři protokolů TCP/IP stáli před problémem, jaké adresy zvolit pro adresování v sítích s TCP/IP architekturou. Nerozhodli se pro použití fyzických adres, ale zvolili zcela nové, abstraktní adresy, nemající se skutečnou fyzickou (hw) adresou zařízení žádnou spojitost. Jako velikost IP adresy zvolili kompromis mezi největšími a nejmenšími fyzickými adresami a vybrali velikost 32 bitů. Již v počátcích autoři předpokládali vnitřní rozdělení adresy na dvě části, kdy první část bude specifikovat lokální síť a druhá konkrétní zařízení v této síti. Toto rozdělení je použito například pro směrování, kdy je pro výběr další trasy důležitá pouze síťová část IP adresy, teprve v síti, do které příjemce spadá se bere v úvahu část adresy specifikující zařízení.
Vzhledem k tomu, že od počátku existoval předpoklad, že v internetu budou připojeny jak sítě rozsáhlé, tak sítě relativně malé, nebylo možné rozdělit IP adresu na část síťovou a lokální staticky (např. prvních 16 b síť, druhých 16 b uzel). Vznikly tedy tzv. *třídy adres*, označované A, B, C a speciální třídy D, E. Jednotlivé třídy se liší počtem bitů vyhrazených pro síťovou část adresy.

Adresy třídy A
Třída A má pro síťovou část vyhrazený první byte (7 bitů, první bit slouží k identifikaci, že jde o adresu třídy A – má hodnotu vždy 0). Ve třídě může existovat až 2^7 velkých sítí, každá z nich může mít až 2^{24} koncových uzlů. Maska sítě třídy A je dekadicky 255.0.0.0

Adresy třídy B
Třída B má pro síťovou část vyhrazeny první dva byte (první dva bity identifikují třídu adres B, zbývajících 14 bitů je použito pro adresování sítě). Ve třídě může existovat až 2^{14} sítí, každá z nich může mít až 2^{16} koncových uzlů. Maska třídy B je dekadicky 255.255.0.0

Adresy třídy C
Třída C má pro síťovou část vyhrazeny první tři byte (první tři bity identifikují třídu adres C, zbývajících 21 bitů je použito pro adresování sítě). Pro adresování uzlů pak zbývá jediný byte. Ve třídě může existovat až 2^{21} sítí, každá z nich může mít nicméně maximálně 256 koncových uzlů. Maska třídy C je dekadicky 255.255.255.0

Ne všechny z výše uvedených adres tříd A-C je možné použít pro identifikaci nějakého síťového rozhraní, v každé třídě existuje vždy skupina tzv. *vyhrazených adres*, které mají speciální účel, např. adresy tvořené samými nulami nebo samými jedničkami které nelze použít pro adresaci konkrétního síťového rozhraní.

IP adresa, tvořená v lokální části samými jedničkami vyjadřuje *broadcastovou* adresu pro všesměrové vysílání v síti (vysílání je doručeno všem uzlům sítě), adresa tvořená samými nulami identifikuje síť jako celek.

Dále je v každé třídě vyhrazena skupina *privátních adres*, které se používají pro adresování uvnitř lokálních sítí (*neveřejné adresy*).

- ve třídě A jsou to adresy: **10.0.0.0 až 10.255.255.255**
- ve třídě B: **172.16.0.0 až 172.31.255.255**
- ve třídě C: **192.168.0.0 až 192.168.255.255**

Adresa **127.x.x.x** (např. 127.0.0.1) je vyhrazena pro *localhost* (*loopback*), umožňuje posílat pakety sám sobě.

Kromě tříd A-C existují **třídy** se speciálním účelem, **D a E**.

- Třída D se používá jako *multicast*, její adresy začínají 1110
- Třída E je vyhrazena pro budoucí použití, adresy začínají 1111.

Rostoucí nedostatek IP adres ukázal i toto řešení jako příliš hrubé a nepružné, hledají se mechanismy umožňující lépe využít adresní prostor, případně jej zvětšit.
Jedním z prvních řešení, které mělo vyřešit plýtvání při přidělování adres bylo přidělování více adres z nižší třídy namísto jedné adresy vyšší třídy. Např. při požadavku o přidělení IP adres pro síť s 1000 uzly bylo namísto jedné adresy třídy B přiděleno několik adres třídy C a tím se výrazně ušetřil adresní prostor, který zůstane nevyužitý. Toto řešení nicméně má také podstatnou nevýhodu, kterou je nárůst složitosti směrování, tj. nárůst objemu informací, které se při směrování musí zpracovat. Roste složitost směrovacích tabulek (místo jednořádkové informace o jedné přidělené síti třídy B je např. 8 řádků s informacemi o přidělených sítích třídy C) a tím se prodlužuje čas na každém směrovači, po který probíhá vyhodnocování směrování.

Oba tyto problémy lze řešit pomocí různých mechanismů:

- dynamický a statický NAT
- subnetting
- supernettin
- CIDR
- protokol vyšší verze (IPv6)

NAT (Network Address Translation), PAT (Port Address Translation)

Využívá faktu, že některé adresy jsou vyhrazeny jako privátní (neveřejné) a mohou být v různých sítích použity vícekrát. Toto řešení je použitelné v těch lokálních sítích, které mají koncové uzly bez přímé konektivity (využívají pro spojení navenek bránu, např, firewall), např. v privátních sítích.
Mechanismus NAT je implementován na rozhraní, které odděluje danou lokální síť od veřejné sítě (Internetu) a slouží k překladu lokálních privátních adres na adresu veřejnou (tato již musí být jedinečná).
Přiřazování veřejných adres lokálním privátním uzlům může být dynamické – *dynamický NAT* - pouze pokud to uzel potřebuje, nebo statické – *statický NAT* – vztah mezi vnitřními a vnějšími adresami je pevně dán.
Rozšířením NATU je *PAT*, který všechny vnitřní adresy mapuje na jednu vnější adresu, přitom rozlišení, o kterou vnitřní adresu se jedná, zajišťují čísla portů.

Subnetting

Technika subnettingu umožňuje rozdělit jednu síťovou adresu na více menších síťových adres. Používá se zejména v oddělených oblastech, ve kterých je potřeba lépe využít přidělený adresní prostor. Typicky toto řešení využívají firmy, které mají několik menších oddělených sítí s relativně malým počtem uzlů v každé síti. Takováto firma pak místo více adres třídy C (pro každou lokální síť jedna) vystačí s jedinou adresou třídy C, kde prvních několik bitů z lokální části adresy použije pro adresaci podsítě.

adresa sítě	adresa podsítě	adresa uzlu

Př. adresu 192.44.118.192 třídy C firma použije pro vytvoření 4 lokálních firemních podsítí takto:

Původní IP adresa:

síťová část adresy	lokální část adresy

Pro adresaci podsítí budou použity první 2 bity lokální části adresy, mohou vzniknout 4 podsítě s různými adresami:

adresa sítě	00	adresa uzlu
adresa sítě	01	adresa uzlu
adresa sítě	10	adresa uzlu
adresa sítě	11	adresa uzlu

Rozdělení jedné síťové adresy na několik adres se děje posunutím hranice mezi oběma logickými složkami adresy směrem k nižším bitům (doprava). Posunutí je definováno maskou sítě (podsítě).

Důležitý je fakt, že toto rozdělení na několik podsítí je záležitostí lokální, nikoli globální, navenek se tedy všechny adresy podsítí jeví stále jako jediná síťová adresa (např. třídy C). Z toho důvodu je nutné, aby sítě, které subnetting využívají měly jediný společný vstupní bod.

Supernetting

Princip supernettingu je opačný než u subnettingu. Původně samostatné síťové dresy spojuje do jedné společné adresy. Pro použití supernettingu nejsou vhodné libovolné adresy, musí jít o adresy "sousední", tj. adresy, které se shodují v určitém počtu vyšších bitů své síťové části, a vyčerpávají všechny bitové kombinace v příslušném počtu nižších bitů své síťové části. Supernetting se používá pro zjednodušení

směrovacích tabulek. Informace o "splynutí" více adres v jednu musí mít na rozdíl od subnettingu globální charakter, aby ji pro směrování bylo možné použít. Praktickou implementací supernettingu je mechanismus CIDR.

CIDR (Classless Inter-Domain Routing)

Mechanismus CIDR umožňuje vést dělicí čáru mezi síťovou a lokální částí síťové adresy v libovolném místě, nejen tam, kde to dovoluje příslušná adresní třída. Součástí každé IP adresy pak musí být také informace, na pozici kterého bitu se nachází předěl mezi oběma částmi adresy. IP adresa využívající mechanicmu CIDR na konci adresy obsahuje lomítko, za kterým je uveden počet bitů vyhrazených pro síťovou část (maska sítě).

```
Př.: 192.168.24.0/21
```

Tato síť je určena prvními 21 bity, zbývajících 11 bitů je určeno pro vnitřní členění sítě a adresy koncových uzlů.

V současné době se adresy přidělují po CIDR blocích, jejichž velikost je dána síťovou maskou, toto řešení umožňuje pružné přidělování skutečně potřebných počtů adres a tak oddálit vyčerpání IP adres.

Rozdíly mezi IPv4 a IPv6

Jediným koncepčním řešením, které může odvrátit hrozbu vyčerpání IP adres za adresního prostoru je nová verze protokolu, která bude počítat s větší velikostí síťové adresy. Touto novou verzí je IPv6, kterou fanoušci Star Tracku nazývají IpnG (IP new Generation). Kromě zvětšení velikosti má nová verze protokolu řešit také další problémy, které se během doby fungování protokolu IP nashromáždily, zejména minimalizovat zátěž směrovačů, minimalizovat plýtvání adresním prostorem a umožnit přenos multimediálních dat.

Požadavky na IPv6

1. **adresní prostor navždy** – zajistit dostatečný počet adres pro budoucí použití (předpokládá se, že v síti budou zapojena v budoucnu i jiná elektronická zařízení, než je počítač, např. lednička, pračka, televizor apod.)
2. **skupinová komunikace** – umožnit vysílání dat určité skupině adresátů, např. pro radiové vysílání, konference apod.

3. **zefektivnit překlad IP adres na MAC adresy** – v IPv4 to bylo pomocí protokolu ARP, který používal všesměrové vysílání, IPv6 přichází s efektivnější metodou *objevování sousedů*
4. **bezpečnost** – doplnit protokol o šifrovací a autentizační procedury
5. **zefektivnit směrování** – přidělování adres pomocí autokonfiguračních mechanismů dynamicky, toto řešení navíc podporuje mobilitu (např. pro připojení přenosných zařízení). Každému mobilnímu zařízení jsou přiřazeny dvě adresy, jedna v mateřské síti, druhá dynamická (v hostující síti), firewall na domácí síti pak vytvoří tunel k danému zařízení
6. **lépe využít přenosové možnosti** – pomocí toků (posloupností paketů), které mají stejnou zdrojovou i cílovou adresu, autentizaci, bezpečnost
7. **podpora priorit** – různé priority pro různých požadavků na přenos, např. pro přenos v reálném čase apod.
8. **snadný přechod od IPv4 k IPv6** – po několik let je nutná koexistence a paralelní fugování obou verzí protokolů, přitom oba protokoly musí využívat vzájemně nezávislé zásobníky (dual stack)

IPv6 počítá se 128 bitovou velikostí adresy, adresa je složena ze dvou částí, prvních 64 bitů (prefix) je vyhrazeno pro identifikaci sítě, druhých 64 bitů pro identifikaci zařízení. Část pro identifikaci zařízení je buď vytvořena automaticky z HW (MAC) adresy rozhraní nebo je přiřazena následně. IPv6 adresy se s časem mění, aby byla zajištěna anonymita uživatele (MAC adresy jsou celosvětově unikátní).

IPv6 adresa se zapisuje jako osm skupin čtyř hexadecimálních číslic. Pokud je některá ze skupin 0000, je možné nuly vynechat a nahradit tuto skupinu zápisem ::. Také je-li více skupin za sebou složeno ze samých nul, je možné tyto skupiny nahradit zápisem ::

```
Př.:  fe80:0000:0000:0000:211:d8ff:fe50:f8cd je adresa identická s:
       fe80::211:d8ff:fe50:f8cd
```

V praxi se můžeme setkat i se smíšeným zápisem, kdy poslední 4 Byty jsou zapisovány dekadicky a odděleny tečkou. Tato forma zápisu není schválena RFC a řada aplikací ji nepodporuje. Prefix adresy můžeme podobně jako v mechanismu CIDR IPv4 zapsat za lomítko na konec adresy, např. 1080:0:0:0:8::/80.

Typy adres IPv6

- **unicast** (jedinečná adresa) – identifikuje právě jedno síťové rozhraní
- **multicast** (skupinová adresa) – identifikuje skupinu síťových zařízení, jimž se má zpráva dopravit
- **anycast** (výběrová adresa) – identifikuje skupinu síťových zařízení, zpráva se doručí nejbližšímu zařízení ze skupiny (měřeno počtem skoků)

IPv6 neobsahuje všesměrové (broadcast) adresy, které byly nahrazeny multicastem, pro potřeby odeslání zprávy všem uzlům dané lokální sítě je v každé lokální síti vyhrazena speciální skupinová adresa.

IPv6 zavádí tzv. *dosah* (scope) adresy, který určuje oblast, ve které je daná adresa jednoznačná. Největší dosah je globální, dosah může být omezen např. jen na konkrétní lokální síť, např. Ethernet.

Jedinečné (unicast) adresy

Obecná struktura unicast adresy:

n bitů	64 – n bitů	64 bitů
globální směrovací prefix	adresa sítě	adresa rozhraní

Dělí se do skupin:

- globální individuální adresy - prefix **001**
- linkové adresy – používají se pro automatickou konfiguraci síťového zařízení a pro objevování sousedů, prefix **1111:1110:10**
- nespecifikované adresy – adresa **::** , nesmí být přiřazena žádnému rozhraní, lze ji použít jako zdrojovou adresu při konfiguraci zařízení, snažícího se získat IPv6 adresy
- smyčka (loopback) – adresa **::1**, používá se k posílání paketů sám sobě, nesmí být přiřazena žádnému rozhraní

Speciálním případem IPv6 adresy je *IPv4 kompatibilní adresa* (IPv6 s vloženou IPv4 adresou). Přechodový mechanismus mezi IPv4 a IPv6 obsahuje metodu dynamického tunelování IPv6 paketů přes IPv4 oblasti. Uzlům používajícím tuto metodu jsou přiřazeny speciální IPv6 adresy, které obsahují na nejnižších 32 bitech IPv4 adresu, prvních 12 B nabývá nulových hodnot (např. ::130.170.234.24).
Dalším speciálním typem IPv6 obsahujícím IPv4 adresu je *IPv4 překládaná adresa*. Tyto adresy se používají pro zařízení podporující pouze IPv4, na prvních 10 B mají nulové hodnoty, další 2B obsahují binární jedničky, posledních 32 bitů je opět IPv4 adresa (např. ::FFFF:130.170.234.24).

Výběrové (anycast) adresy
Tyto adresy jsou přiřazeny většímu počtu rozhraní, nelze přitom rozlišit, zda jde o adresu výběrovou nebo individuální, tuto skutečnost je třeba v konfiguraci zařízení zadat. Výběrové adresy nemohou být přiděleny koncovým zařízením, pouze směrovačům a nesmí být užity jako zdrojová adresa.

Skupinové (multicast) adresy
Význam těchto adres spočívá zejména v možnosti přenášet multimediální aplikace do více (mnoha) zařízení současně, slouží tedy k přenosu videokonferencí, televizního a rozhlasového vysílání, telefonních hovorů apod.

8b	4b	4b	112b
ff	příznaky	dosah	Identifikátor skupiny

Prefix skupinových adres je ff (binární prefix je 11111111), následuje položka příznaky, dosah a skupinový identifikátor (group ID). Položka příznaky upřesňuje typ skupinové adresy (např. dočasné nebo trvalé adresy), položka dosah specifikuje dosah šíření skupinově adresovaných dat (jediné rozhraní, linka, organizace).

Formát IPv6 paketu

IPv6 se snaží minimalizovat hlavičku, která bude zpracovávána směrovači, méně důležité části hlavičky tedy přesouvá do rozšiřujících hlaviček.

verze	Třída provozu	Značka toku dat
Délka dat	Další hlavička	Max. skoků
Adresa zdroje		
Adresa cíle		

Položky hlavičky:

- verze – verze protokolu, zde 6
- třída provozu – hodnoty v položce určují priority (uplatní se v případě zahlcení), např. přenos videa, telefonní hovor
- značka toku – označení paketů stejného toku, tok je identifikován kombinací zdrojové adresy a čísla toku. Toky mohou být individuální nebo skupinové, všechny pakety jednoho toku musí být směrovačem zpracovány stejně. O zařazení paketu do toku rozhoduje odesilatel, během přepravy musí být značka toku zachována.
- Délka dat – délka datové části paketu, délka položky je 16b => maximální velikost datové části paketu je 64KB. Pro přenos většího objemu dat musíme použít rozšiřující hlavičku Jumbo
- Další hlavička – určuje typ rozšiřující hlavičky, ty se nacházejí na začátku datové části paketu
- Dosah – obdoba TTL u IPv4, na každém směrovači klesne o jedničku, dosáhne-li hodnoty 0 je paket zahozen. Položka má velikost 8b => maximální

počet směrovačů na cestě mezi dvěma koncovými IPv6 zařízeními může být 254.

Pro správné fugování protokolu IPv6 je doporučováno MTU přenosové linky minimálně 576 B, dále je doporučeno na všech směrovačích, kde je IPv6 používán implementovat algoritmus objevování MTU cesty, který hledá maximální velikost paketu, který se dá poslat danému cíli.

Bezpečnost v IPv6

Orientuje se na ochranu síťových spojení a je realizována pomocí rozšiřujících hlaviček, tedy se dá snadno aktivovat nebo deaktivovat. Je zajištěna zejména dvěma hlavičkami – autentizace a šifrování.
Autentizační hlavička zabezpečuje neporušenost (nelegální modifikaci) paketu
Hlavička šifrování zajišťuje šifrování datové části paketu, data paketu může číst pouze koncové zařízení. Obě hlavičky se používají současně.
Bezpečnostní asociace je virtuální spojení dvou zařízení pro bezpečný přenos dat, součástí této asociace jsou šifrovací algoritmy, klíče a další prvky. Bezpečnostní asociace jsou jednosměrné a navazují se po dvojicích, jedna pro vysílání, druhá pro příjem (pro každý směr se mohou použít jiné klíče).

Protokoly související s použitím IPv6

Služební protokol ICMP je nahrazen protokolem **ICMPv6**, tento protokol přitom v sobě kombinuje dříve používané protokoly ICMP, IGMP a ARP. Používá se pro diagnostiku a ohlašování chyb vzniklých při přenosu paketů a při objevování sousedů. Jeho funkce jsou rozděleny do dvou oblastí – oblast chybová a oblast informační.
Chybové zprávy ICMP spadají do kategorií:

- Nedosažitelný cíl (destination unreacheable)
- Příliš velký paket (packet too big)
- Vypršela životnost paketu (time exceeded)
- Problémy s parametry (parameter problems)

Informační zprávy jsou rozděleny do kategorií:

- Diagnostické zprávy (echo request, echo reply)
- Zprávy objevování sousedů (výzva směrovači, ohlášení směrovače, výzva sousedovi, ohlášení souseda, přesměrování)
- Zprávy o zacházení se skupinovými adresami (dotaz na členství, ohlášení členství, vystoupení ze skupiny)

Adresy linkové vrstvy jsou rozpoznávány pomocí zpráv výzva a ohlášení sousedovi (řeší protokol ICMP namísto původního protokolu ARP).

Pro **směrování** jsou používány směrovací protokoly RIPng, OSPFv6, IDRPv2, může být použit i EIGRP a Dual IS-IS.

Shrnutí:

Pro identifikaci jednotlivých zařízení v počítačových sítích je používána tzv. IP adresa. Její původní verze (IPv4) má velikost 32 bitů, zapisuje se binárně nebo dekadicky. Každá IP adresa je logicky členěna do dvou částí, část identifikující síť a část lokální, identifikující konkrétní zařízení. Původní členění IPv4 adres na tyto dvě logické složky vycházelo z konceptu adresních tříd, kde hranice mezi síťovou a lokální částí adresy mohla být vedena vždy za každým Bytem (osmi bity) adresy. Toto rozdělení adresního prostoru nebylo dostatečně jemné a vedlo k velkému plýtvání adresami, které nemohly být využity. Vzhledem k hrozícímu nedostatku IP adres vznikaly mechanismy, které měly úbytek adres oddálit.
Mezi tyto mechanismy patří zejména koncepce privátních adres, které mohou být v sítích použity vícekrát a také supernetting a z něj vycházející CIDR, jež umožnily vést dělicí čáru mezi lokální a síťovou částí adresy na libovolném místě. Tyto mechanismy zároveň řeší problémy vzrůstající složitosti směrování a nárůst velikosti směrovacích tabulek.
Jediným koncepčním řešením je přechod na novou verzi protokolu IP (IPv6), která kromě zvětšení adresního prostoru řeší i další nedostatky a slabá místa protokolu IPv4, např. problematiku bezpečnosti, mobility, požadavků na garanci kvality přenosu. Přesto, že koncepce protokolu IPv6 je hotova již asi 10 let, dosud se více využívá protokol IPv4.

Kontrolní otázky:

1. Na jaké vrstvě funguje, jak principiálně pracuje a k čemu slouží protokol IP?
2. Jak vypadá IP adresa verze 4? Jakou má logickou strukturu?
3. Popište koncept rozdělení adres IPv4 do adresních tříd.
4. Co jsou to privátní adresy a k čemu se používají? Uveďte příklad privátní adresy z každé adresní třídy.
5. Co je maska sítě, jak se zapisuje?
6. Jmenujte mechanismy, které umožnily oddálit hrozbu vyčerpání adresního prostoru.
7. Popište princip subnettingu. Za jakých podmínek se dá subnetting použít?
8. V čem spočítá supernetting? Co je jeho výhodou?

9. Vysvětlete mechanismus CIDR. Co je největší výhodou tohoto řešení?
10. Z jakých předpokladů (požadavků) vycházeli tvůrci nové verze protokolu IP (IPv6)?
11. Jak vypadá adresa IPv6?
12. Jmenujte typy adres v IPv6.
13. Popište strukturu unicastové adresy. Znáte nějaké speciální unicast adresy?
14. Co jsou multicastové adresy? Jak je poznáme?
15. K čemu slouží adresy anycast?
16. Jak je řešena bezpečnost v IPv6?
17. Popište formát IPv6 paketu.
18. Kterým protokolem je v IPv6 nahrazen protokol ARP?

Použité informační zdroje:

Sochor Tomáš: Počítačové sítě II, skripta pro distanční studium, vydala Ostravská univerzita v Ostravě, Přírodovědecká fakulta, Ostrava 2009

RFC 4291: IP Version 6 Addressing Architecture [online], vydáno 02/2006, dostupné z: http://tools.ietf.org/html/rfc4291, [cit. 03/2012]

IP adresa – Wikipedie [online], poslední editace 02/2012, dostupné z: http://cs.wikipedia.org/wiki/IP_adresa#Vyhrazen.C3.A9_adresy, [cit. 03/2012]

Peterka Jiří: Subnetting, supernetting a CIDR [online], dostupné z: http://www.earchiv.cz/anovinky/ai1681.php3, [cit. 03/2012]