Příklad materiálů pro kurz

Základy počítačových sítí (TCCN-IP1)

Modul 5, kapitoly 2 – 4
http://www.ictlogic.eu/cs/course-TCCN-IP1-Zaklady-internetworkingu
learning@ictlogic.cz

20110428M5K2-4

5.2 Představení IPv4 protokolu

IPv4 byl vytvořen jako protokol s co *nejmenší režií síťových zdrojů* (*low overhead*), hlavně *šířky pásma* (*bandwidth*). Jeho základní charakteristiky jsou:

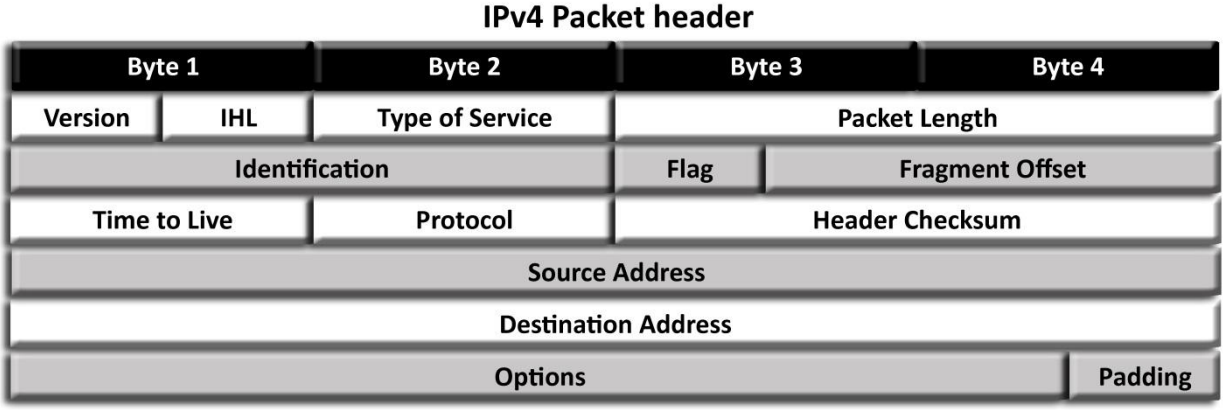
- *Connectionless* – žádné sestavování relací či okruhů před posíláním paketů
- *Nespolehlivost (Best Effort, unreliable)* – žádná režie navíc pro garantování doručení paketů a žádné garantování doručení paketů ve správném pořadí
- *Nezávislost na síťovém médiu (media independent)* – funguje nezávisle na tom, zda jsou data posílána přes měděné kabely, optiku, vzduch atd.

Výhoda spočívá v relativně malé síťové hlavičce (standardně 20 bytů), a tím úspoře kapacity pásma. Nicméně v případě prvních dvou bodů se musí tyto problémy vyřešit na vyšších vrstvách OSI modelu, pokud je pro danou síťovou službu vyžadována větší spolehlivost přenosu či mechanizmus pro poskládání paketů do správného pořadí.

Maximální velikost paketů a jejich fragmentace (MTU and packets fragmentation)
IPv4 podobně jako IPv6 sice fungují nezávisle na síťových médiích, nicméně různá média mohou umět přenášet různě veliká PDU. Maximální velikost jednoho PDU se nazývá *MTU (Maximum Transmission Unit).* Proto linková vrstva poskytuje síťové vrstvě informaci o maximálním MTU na daném médiu, což umožňuje síťové vrstvě rozhodnout, jak velký paket pošle o vrstvu níž.
Někdy může nastat případ, že směrovač (router), který spojuje různé segmenty sítí, musí přeposlat příliš velké pakety do média, jež má menší MTU. Tehdy je třeba, aby směrovač paket rozdělil. Tento proces se nazývá *fragmentace* (*packets fragmentation*).

IPv4 hlavička
Podobně jako hlavička segmentu na transportní vrstvě, i hlavička na síťové vrstvě obsahuje mnoho binárních polí. Klíčová z nich jsou:

- *IP Source Address*
- *IP Destination Address*
- *Time-to-Live (TTL)*
- *Type-of-Service (ToS)*
- *Protocol*
- *Fragment Offset*
- *Flag*



IP Source Address
32bitová (4bytová) adresa odesílatele

IP Destination Address
32bitová (4bytová) adresa příjemce

Time-to-Live
Značí zbývající „život“ paketu. Vzhledem k tomu, že pole má velikost 8 bitů, maximální velikost hodnoty může být 255. Nicméně pokaždé, když směrovač zpracovává paket, odečte číslo 1 ze zbývající hodnoty. Jinak řečeno, každým skokem (hop) se Time-to-Live snižuje. Jakmile se sníží na nulu, směrovač již paket nepřepošle dál, ale tzv. jej „*zahodí*“ (*drop, discard*). Tento mechanizmus brání paketům, které nemohou dosáhnout svého cíle z důvodu chybného směrování v síti, aby cyklicky donekonečna chodily mezi stejnými směrovači. Zacyklení paketů z důvodu chybného směrování se říká *směrovací smyčky* (*routing loops*).

Protocol
Hodnota o velikosti 8 bitů, značící *typ datového obsahu* (*data payload type*) paketu. Toto pole identifikuje druh protokolu na vyšších vrstvách. Běžné hodnoty jsou:
- 01 ICMP (*Internet Control Message Protocol*)
- 06 TCP (Transmition Control Protocol)
- 11 UDP (User Datagram Protocol)

Type-of-Service
Obsahuje 8bitovou hodnotu, která určuje prioritu každého paketu. Díky ní se dají aplikovat na každý paket QoS mechanizmy. Např. pro VoIP provoz bývá pole typicky na hodnotě 5, u obyčejného provozu na 0.

Fragment Offset
V případě, že směrovač chce přeposlat dál větší paket, než je dané médium schopno přenést, musí paket rozdělit na menší části neboli fragmenty. Pole *Fragment Offset* ukazuje pořadí každé části v původním paketu, a umožní tak přijímající straně paket znovu správně sestavit.

Flag
Může mít hodnoty „More Fragments“ nebo „Don’t Fragment”.
- *More Fragments flag (MF)* – 1bitová hodnota, která se využívá v kombinaci s Fragment Offset.
  - Jestliže MF = 1, jde o fragment a směrovač musí z pole Fragment Offset zjistit pořadí tohoto fragmentu v původním paketu.
  - Pokud MF = 0 a ve Fragment Offset je jiná než nulová hodnota, jde o poslední fragment z paketu.
  - V případě, že v obou polích jsou samé nuly, nejedná se o fragmentovaný paket.
- *Don’t Fragment flag (DF)* – 1bitová hodnota, která indikuje, že paket nesmí být rozdělen. Pokud směrovač potřebuje takovýto paket rozdělit a poslat do média, podporujícího jen menší MTU, s DF = 1 toto nebude povoleno a směrovač musí takový paket zahodit.

Další pole v hlavičce IPv4
Version – verze IP protokolu (4)
Internet Header Length (IHL) – specifikuje velikost hlavičky paketu (obvykle 20 bytů)
Packet Length – celková velikost paketu vč. hlavičky a dat
Identification – slouží pro identifikaci, k jakému paketu patří daný fragment. Toto pole je vyplněno i u nefragmentovaných paketů.
Header Checksum – kontrolní součet, který ukazuje, zda hlavička paketu dorazila nepoškozena. Je vypočítán pouze z polí hlavičky, nikoli z celého paketu.
Option – zřídka používané pole. Slouží pro případné další IPv4 služby.

5.3 Základy IP architektury

V dřívějších dobách byly jednotlivé hosty připojeny do jedné sítě. Z důvodu neustálého nárůstu počtu hostů bylo potřeba začít více plánovat síťovou architekturu, a tudíž lépe navrhovat a řídit architekturu logických adres. Jeden z prvních důležitých kroků je sdružování jednotlivých hostů do síťových skupin, nazývaných *podsítě (subnets).*
IP architekti zpravidla sdružují hosty do daných podsítí na základě následujících faktorů či jejich kombinací:

- *Geografická poloha* – hosty z jedné lokality spadají do jedné podsítě
- *Povaha a cíle hostů a jejich pracovníků* – např. jedna podsíť je určena pro počítače běžných úředníků, druhá pro IT administrátory, další pro IP telefony, pro servery atd.
- *Vztah pracovníků k dané organizaci* – počítače zaměstnanců organizace bývají zařazovány do jiné podsítě než počítače externích pracovníků, tzv. *„třetích stran“*
- *Privátní či veřejný host* – záleží na tom, zda host má napřímo komunikovat s veřejnými sítěmi, či ne

U všech těchto bodů hraje často významnou roli datová bezpečnost.

Výkonnost sítě
Dalším důvodem pro rozdělení sítě na menší segmenty je degradace její výkonnosti ve chvíli, kdy se v ní rozroste počet hostů na stovky až tisíce. Většina protokolů na linkové a síťové vrstvě funguje tak, že každý host před tím, než začne komunikaci s jiným hostem, musí zjistit jeho adresu. Provádí to pomocí zprávy, která se nazývá *„broadcast“.* Protože se tato zpráva posílá všem hostům v jedné síti, náročnost distribuce takové zprávy narůstá s počtem připojených stanic. Všechny tyto stanice musí danou zprávu také zpracovat a vyhodnotit, zda se jich týká.
Proto je lepší rozdělit hosty podle nějaké logiky do menších skupin a tyto skupiny propojit směrovači.

Bezpečnost
Na rozdělení do skupin mají významný vliv i bezpečnostní pravidla organizace. Různé podsítě tak bývají zařazovány do *bezpečnostních tříd* (*security levels*). Mnohé skupiny pak mají např. omezený přístup k jiným. Omezení mezi podsítěmi se může provádět na směrovačích, nicméně specializované zařízení pro filtrování či zamezení provozu se nazývá *firewall* (*firewall*).
Zařazení do jednotlivých bezpečnostních skupin může fungovat např. na základě:

- fyzického zabezpečení lokality (pobočka bez řádného zabezpečení versus centrála s ostrahou)
- pracovní povahy stanic a jejich pracovníků (na rozdíl od IT administrátora nemá většinou běžný zaměstnanec přístup do administrace IT a síťových prvků)
- na základě vztahu pracovníka k organizaci (zaměstnanci např. mají přístup do zón, do kterých externí partneři mít přístup nesmí)

5.4 Adresování v IPv4 sítích

V IPv4 musí každý paket obsahovat ve své hlavičce 32bitovou zdrojovou i cílovou IP adresu zapsanou v binární soustavě. Protože každých *8 bitů (b) = 1 byte (B),* je IPv4 adresa velká 4 byty. Takovéhle adresy by se ovšem lidem špatně pamatovaly, proto se přepisují do čtyř čísel v decimální soustavě, oddělených tečkami.

Příklad 32bitové adresy v binární podobě:
10101100000100000000010000010100

Zápis téže adresy rozdělené do čtyř částí po osmi bitech, tzv. *oktetů*, oddělených tečkami:
172.16.4.20

Adresa sítě a číslo hostu
Každá IP adresa v IPv4 sítích obsahuje první část bitů, reprezentujících adresu sítě (podsítě) neboli skupinu hostů. Všechny hosty v této skupině tak mají první část řetězce bitů stejnou. Druhá část adresy pak určuje číslo hostu v dané podsíti.
První i druhá část mohou být různě velké, ale dohromady musí mít vždy délku 32 bitů. Počet bitů v druhé části nám jednoznačně určuje maximální počet hostů, které se v dané podsíti mohou nacházet. Např. pokud prvních 24 bitů označuje podsíť, zbývajících 8 bitů nám dává maximální počet kombinací 256, což je i maximální teoretický počet hostů v dané síti. Matematický vyjádřeno, $8^2 = 256$, neboli 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 = 256.

Konverze mezi binární (dvojkovou) a decimální (desítkovou) soustavou

binární	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
(x)	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

decimální	**255**

* První hodnota je nula, proto výsledek v tabulce je 255, což je poslední 256. hodnota

binární	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
(x)	0^7	0^6	0^5	0^4	0^3	0^2	0^1	0^0
	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**

decimální	**0**

binární	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
(x)	2^7	0^6	0^5	0^4	0^3	0^2	0^1	0^0
	128	**0**	**0**	**0**	**0**	**0**	**0**	**0**

decimální	**128**

Podrobnější vysvětlení převodů čísel mezi dvojkovou a desítkovou soustavou najdete např. na www.matweb.cz/prevod

Typy adres v IPv4
V každém rozsahu sítě či podsítě rozlišujeme tři druhy adres:
- *Adresa sítě (Network Address)*
- *Broadcastová adresa (Broadcast Address)*
- *Adresa hostu (Host Address)*

Adresa sítě (Network Address)
Označuje začátek rozsahu sítě či podsítě (např. 10.0.0.0). Nesmí být přiřazena žádnému hostu!

Broadcastová adresa (Broadcast Address)
Označuje konec rozsahu sítě či podsítě (např. 10.0.0.255). Nesmí být přiřazena žádnému hostu! Používá se k oslovení všech zařízení z daného rozsahu. Pro poslání zprávy všem hostům v síti tak stačí odesílajícímu zařízení poslat pouze jeden tok dat. Ve všech hlavičkách paketů v tomto toku dat bude jako cílová adresa uvedena broadcastová adresa.

Adresa hostu (Host Address)
Adresa koncového hostu v síti, např. 10.0.0.1

Maska a délka prefixu sítě (Network Mask and Network Prefix Length)
Počet hostů, které patří do dané sítě či podsítě, vyjádříme buď její maskou, nebo délkou prefixu.
Masku sítě (network mask) zapíšeme podobně jako síťovou adresu, tedy pomocí čtyř oktetů, oddělených tečkami. Každý bit, který označuje síťovou část, bude mít hodnotu 1 a každý bit označující číslo hostu, bude mít hodnotu 0. Pokud bude např. počet bitů označujících síť 24, pak maska bude v binární podobě vypadat takto: 11111111.11111111.11111111.00000000

V decimálním tvaru ji zapíšeme tímto způsobem:
255.255.255.0

Délka prefixu sítě (network prefix length) vyjadřuje také počet bitů, označujících síť. Píše se za lomítkem, jež se nachází za adresou sítě či hostu v decimálním tvaru. Tedy např. síť 10.0.0.0, kde počet bitů označujících podsíť je 24, vyjádříme tímto způsobem:
10.0.0.0/24

Porovnání počtu hostů stejné sítě s různou délkou prefixu či různou maskou

172.20.0.0/24
172.20.0.0 255.255.255.0
Tato podsíť má 24 bitů vyjadřujících číslo sítě a 8 bitů vyjadřujících čísla hostů. Počet IP adres v podsíti tedy bude 256 (2^8) v rozsahu 172.20.0.0 – 172.20.0.255.

172.20.0.0/23
172.20.0.0 255.255.254.0
Tato podsíť má 23 bitů vyjadřujících číslo sítě a 9 bitů vyjadřujících čísla hostů. Počet IP adres v podsíti tedy bude 512 (2^9) v rozsahu 172.20.0.0 – 172.20.1.255.

172.20.0.0/28
172.20.0.0 255.255.255.240
Tato podsíť má 28 bitů vyjadřujících číslo sítě a 4 bity vyjadřující čísla hostů. Počet IP adres v podsíti tedy bude 16 (2^4) v rozsahu 172.20.0.0 – 172.20.0.15.

Konfigurace IPv4 adres

Aby jakékoliv zařízení mohlo správně komunikovat v lokální IPv4 síti, musí mít přidělenu alespoň jednu IPv4 adresu a masku ke svému *síťovému interfacu* (rozhraní, připojení). Aktivní síťové prvky, např. směrovače, mají na každém aktivním interfacu nakonfigurovanou alespoň jednu adresu s maskou. Tyto parametry je možné do každého zařízení nastavit ručně (tzv. staticky), nebo dynamicky, nejčastěji přes *DHCP* prokol (viz níže).

Typy komunikací v IPv4 sítích
Zařízení fungující na IPv4 protokolu může komunikovat s ostatními zařízeními třemi způsoby, a to pomocí *unicastu, broadcastu a multicastu.*

Unicast
Je určen pro běžnou komunikaci typu klient/server nebo peer-to-peer. Unicastová adresa označuje vždy jeden konkrétní host. Při této komunikaci je v hlavičce IP paketu v poli „IP Source Address" IP adresa odesílajícího zařízení a v poli „IP Destination Address" IP adresa koncového zařízení.
Tento typ provozu funguje jak v lokální síti, tak může být směrován mimo lokální síť.

Broadcast
Používá se pro spárování logických adres s fyzickými (viz kapitola 6 – OSI linková vrstva), pro vyžádání dynamicky přidělované adresy (typicky DHCP) nebo pro výměnu informací dynamických směrovacích protokolů. Jakmile zařízení v síti obdrží paket s destinační broadcastovou adresou, zpracuje ji stejně jako unicastový paket. Prověří, zda patří jemu, a následně buď odpoví odesílateli, nebo paket „zahodí".
Rozlišujeme dva druhy broadcastů, *přímý* (*Directed broadcast*) a *limitovaný* (*Limited broadcast*)

Directed Broadcast
Je zaslán na všechny hosty mimo lokální síť. V případě sítě 172.20.10.0/24 by byla destinační broadcastová adresa 172.20.10.255. Takový broadcast musí do cílové sítě přeposlat směrovače, ovšem v základním nastavení bývá zpravidla tato funkce vypnuta, aby sítě nebyly těmito cílenými broadcasty zahlcovány.

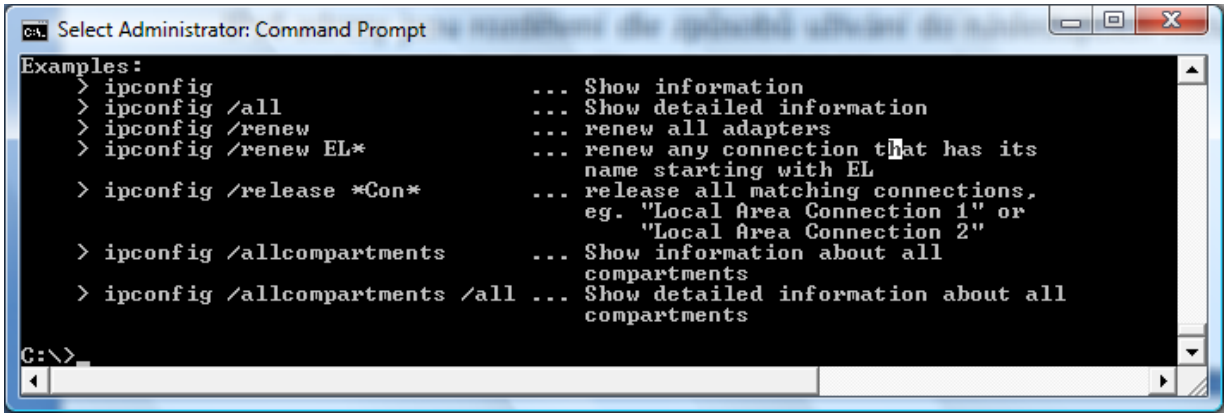
Limited Broadcast
Je rozesílán jen v rámci lokální sítě, není tedy přeposílán směrovači dále. Nejčastěji se s ním setkáme právě při DHCP protokolu. Destinační adresa je vždy ve tvaru 255.255.255.255. Lokální síť v IPv4 je obecně brána jako tzv. „broadcastová doména", přičemž tyto domény jsou od sebe odděleny směrovači.

Multicast
Multicastový provoz byl vytvořen pro snížení nároků na šířku datového pásma ve chvíli, kdy zdrojové zařízení potřebuje poslat datový paket vícero koncovým hostům najednou. V případě unicastu by bylo nutné poslat datový provoz každému hostu zvlášť, takto stačí poslat jediný datový tok se speciální destinační multicastovou IPv4 adresou. Koncová zařízení, která chtějí pakety s touto destinační adresou zpracovávat stejně, jako by se jednalo o unicast paket, mířený na ně, se nazývají *multicastoví klienti* (*multicast clients*). Na nich běží klientský program, jenž zařídí zapsání daného klienta do konkrétní *multicastové skupiny* (*multicast group*). Každé zařízení z takové multicastové skupiny pak zpracovává stejnou předem určenou IPv4 destinační multicastovou adresu.
V IPv4 světě je pro multicastové adresy vymezen rozsah od 224.0.0.0 do 239.255.255.255.
Typické příklady pro multicastový provoz:

- video (TV) a audio (rádio) přes intranet/internet
- výměna informací dynamických směrovacích protokolů
- hromadné SW instalace v síti

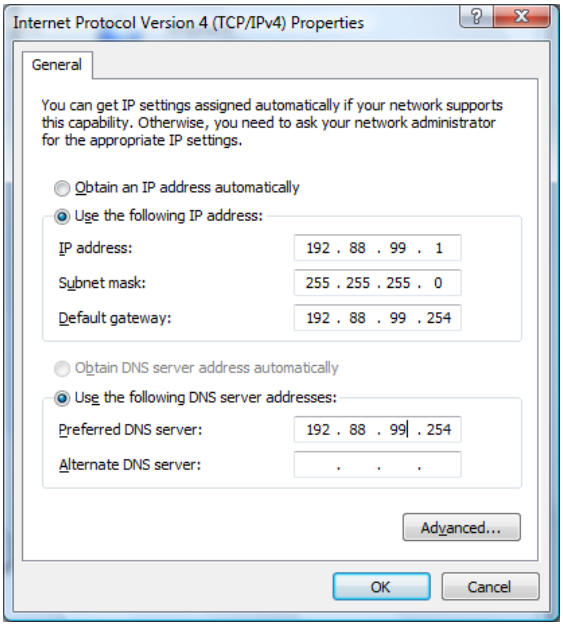
DHCP (Dynamic Host Configuration Protocol)
Slouží k dynamickému přidělování IPv4 adres. Vznikl v roce 1993 (RFC 1531), v roce 1997 pak byl aktualizován do dnešní podoby. Postupně nahradil starší *BOOTP* (*Bootstrap Protocol*).

Zařízení (klient), které potřebuje získat přes DHCP síťové nastavení, nejprve pošle pomocí limitovaného broadcastu tzv. „DHCPDISCOVER paket“. Jedná se o UDP se zdrojovým portem 68 a destinačním 67.
Zdrojová IPv4 adresa je ve tvaru 0.0.0.0. Všechna zařízení v lokální síti, na nichž běží DHCP server (poslouchá právě na portu 67), na tento požadavek odpoví pomocí zprávy DHCPOFFER, ve které nabídnou IP adresu, masku, *výchozí bránu* (*default gateway*) a další síťová nastavení. V případě, že klientovi dorazí nabídky od více serverů, vybere dle své naprogramované logiky jednu z nabídek a danému DHCP serveru odpoví zprávou DHCPREQUEST. Na tuto zprávu DHCP server pošle DHCPACK, a pokud toto potvrzení klient přijme, začne tato síťová nastavení používat. Všechny tyto zprávy obsahují v poli „Destinační IPv4 adresa“ adresu limitovaného broadcastu 255.255.255.255.



Přehled příkazů pro vypsání či aktualizaci síťového nastavení (ipconfig nebo ipconfig /all pro aktuální výpis síťového nastavení, ipconfig /renew pro vyslání zprávy DHCPDISCOVER)

Tato nastavení však bývají zpravidla časově omezená, takže před uplynutím doby „zapůjčení adresy“ je nutné, aby klient potvrdil zájem o její používání pomocí dalšího DHCPREQUEST a následně přijal opět DHCPACK od serveru.
Další ze známých typů zpráv je např. DHCPDECLINE. Je vyslán klientem v případě, že se mu přidělené síťové parametry nezdají korektní. Pokud klient již nechce nadále používat správně přidělenou adresu, pošle serveru DHCPRELEASE.



Pokud není DHCP server k dispozici, je nutné nastavit IP adresu, masku, default gateway (výchozí bránu) a DNS servery ručně

Rozdělení adresních rozsahů v IPv4 sítích
IPv4 adresy jsou rozděleny podle způsobu užívání do následujících rozsahů:

- *experimentální adresy (Experimental Addresses)*
- *multicastové adresy (Multicast Addresses)*
- *adresy hostů (Host Addresses)*

Na přidělování adresních rozsahů a na jejich správné používání dohlíží organizace *IANA (Internet Assigned Numbers Autority)*

Experimentální adresy (RFC 1700 a 3330)
V současnosti se v IPv4 sítích nevyužívají, jsou oficiálně rezervovány pro vývoj a budoucí využití.
Rozsah adres: 240.0.0.0 – 255.255.255.255

Multicastové adresy (RFC 1700)
Využívají se k multicastovému provozu.
Rozsah adres: 224.0.0.0 – 239.255.255.255.255

Tento rozsah se dále dělí do mnoha dalších skupin, spravovaných opět organizací IANA, např. *Local Network Control Block* s rozsahem 224.0.0.0 – 224.0.0.255. TTL jejich paketů je vždy 1, proto je směrovače nikdy nepřesměrují dál. Typicky slouží směrovacím protokolům k výměně směrovacích informací, např. ve směrovacím protokolu *OSPF* (*Open Shortest Path First*) k vyslání tzv. *„Hello packets“* s destinační adresou 224.0.0.5.
Další důležitou skupinou multicastových adres je *Internetwork Control Block* v rozsahu 224.0.1.0 - 224.0.1.255, jenž je využíván pro šíření multicastového provozu internetem. Typickým příkladem je zde *Network Time Protocol (NTP)*, pomocí kterého si síťová zařízení seřizují správný čas. Destinační multicastová adresa pro NTP je 224.0.1.1.
Multicastových skupin je celá řada a všechny jsou popsány např. v RFC 3171.

Adresy Hostů (RFC 790)
Jsou určeny pro adresaci (opatřování adresou) síťových interfaců hostů v IPv4 síti, pro označení sítí a broadcastů. Celý tento velký blok adres je striktně spravován organizací IANA.
Rozsah adres: 0.0.0.0 – 223.255.255.255

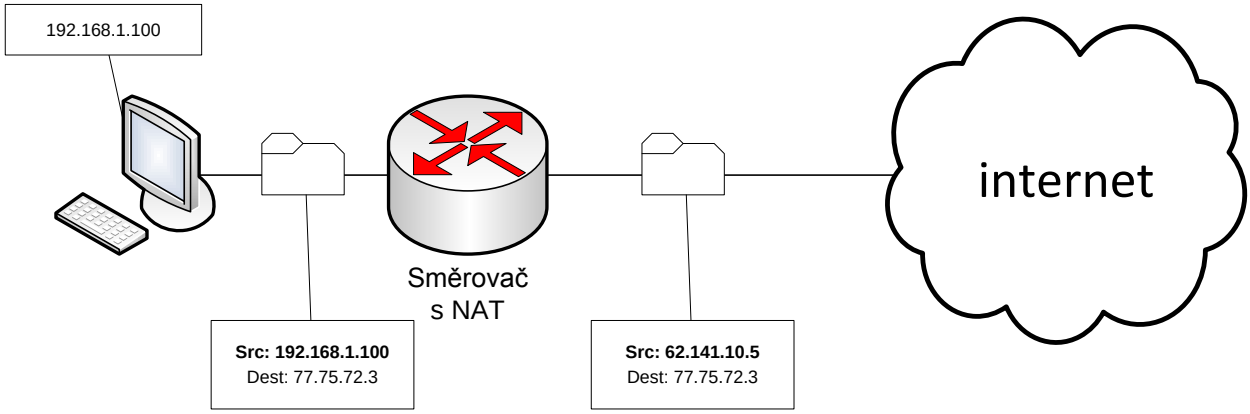
Většina adres z tohoto velkého bloku se používá pro veřejnou internetovou komunikaci, nicméně tři rozsahy jsou určeny pouze pro adresaci hostů v privátních sítích a nejsou ve veřejném internetu dosažitelné. Jsou to:

- 10.0.0.0 – 10.255.255.255 (10.0.0./8, 16 777 216 adres)
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12, 1 048 576 adres)
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16, 65 536 adres)

Běžně se používají pro adresování zařízení v nezávislých izolovaných sítích, např. intranetových hostů, počítačů v domácnostech apod. Z tohoto důvodu není nutné celosvětově řídit adresní prostor v těchto třech skupinách. Společnost A tak může používat IP adresu 192.168.1.100 stejně tak jako domácnost s malým WIFI směrovačem. S těmito adresními rozsahy tak může každý správce privátní sítě nakládat, jak uzná za vhodné. Pro správné a bezproblémové používání každé větší privátní sítě se však doporučuje každému hostu dávat unikátní IPv4 adresu a vést si řádnou a aktuální adresní dokumentaci. Tím zajistíme, že se v síti neobjeví dvě zařízení se stejnou IPv4 adresou, což by vedlo k problémům se síťovým připojením těchto hostů.

Překlady IPv4 adres a sítí (*NAT)*
Aby zařízení s privátní IPv4 adresou mohlo komunikovat s ostatními hosty v internetu, byla stvořena funkce pro překlad IPv4 adres (*NAT – Network Address Translation*). NAT je konfigurován typicky na směrovačích a firewallích, jež se nacházejí na hranici privátní sítě s internetem. Jakmile dorazí paket z vnitřní privátní sítě na toto zařízení, pomocí funkce NAT se změní zdrojová IPv4 adresa odesílatele na veřejnou adresu, kterou má směrovač či firewall pro tuto funkci přidělenu. Jakmile dorazí paket k destinačnímu zařízení, odešle odpověď na veřejnou adresu. Návratový paket tak dorazí na ten samý směrovač (event. firewall), jenž udržuje v paměti aktuální tabulku s aktivními překlady. Díky této tabulce je pak paket doručen do vnitřní sítě tomu správnému zařízení.
Pomocí NAT se dá překládat zdrojová i cílová adresa, privátní i veřejná. Jedna lokální adresa tak může být přeložena za jednu veřejnou adresu, další lokální adresa za druhou veřejnou atd. Pokud ale nastane případ, že např. vícero hostů z privátní sítě potřebuje komunikovat na veřejné služby přes stejnou překladovou

veřejnou IP adresu (např. z nedostatku přidělených veřejných IP adres), je nutné kromě síťové adresy překládat i zdrojový port paketu. To je jediná možnost, jak může směrovač vytvořit správný překlad a nasměrovat zpáteční pakety správnému zařízení. Tato rozšířená funkce se jmenuje *PAT* (*Port Address Translation*).



Speciální adresy z rozsahu hostů

Ne všechny adresy z RFC 790 lze přidělit a nakonfigurovat síťovému portu koncových či síťových zařízení. Patří mezi ně např. již výše zmíněné síťové a broadcastové adresy.

Default-route address

Dalším rozsahem, který nelze hostům přidělovat, je 0.0.0.0 – 0.255.255.255 (0.0.0.0/8), který je organizací IANA rezervován pro zvláštní účely. Např. adresa 0.0.0.0/32 označuje ve směrovací tabulce každého síťového zařízení tzv. *výchozí bránu* (*default route*), tedy směrovací záznam pro výběr cesty, jenž se uplatní tehdy, když zařízení nezná specifičtější cestu pro směrování paketu.

Loopback

Dalším speciálním rozsahem je 127.0.0.0 – 127.255.255.255 (127.0.0.0/8). Je určen pro tzv. *Loopback*, tedy adresu, kterou každý host používá pro řízení komunikací TCP/IP služeb, jež běží na tom stejném zařízení. Pokud spolu chtějí dvě TCP/IP služby komunikovat v rámci jednoho zařízení, komunikují přes Loopback, čímž obejdou zbytečnou cestu přes nižší vrstvy OSI modelu.
I přes to, že v současné době se v systémech prakticky používá jen adresa 127.0.0.1, je celý tento rozsah nedostupný pro adresaci hostů v IPv4 sítích.

Link-Local Addresses

Jedná se o IPv4 adresy z rozsahu 169.254.0.0 – 169.254.255.255 (169.254.0.0/16), jež se automaticky přidělí lokálnímu hostu operačním systémem v případě, že není možné staticky či dynamicky nastavit korektní IPv4 adresu. Velmi záleží na konkrétní implementaci výrobce systému, nicméně běžně se používají jen pro komunikaci v lokální podsíti s pakety, v kterých je pole TTL nastaveno na 1, takže provoz není směrován mimo lokální síť.

TEST-NET Addresses

Další z rezervovaných bloků, které se nepoužívají pro internetové účely, i když se do konfigurace síťových portů různých systému dají nakonfigurovat. Obecně se užívají pro vyučovací či dokumentační účely, v různých technických dokumentacích a dalších materiálech.

V IPv4 sítích existují i další speciální bloky adres. Všechny jsou přesně popsány např. na stránkách organizace IANA www.iana.com.

Historické rozdělení adres na třídy
V RFC 1700 byly adresní bloky rozděleny do tříd A, B, C (všechny pro hosty), D (pro multicast) a E (experimentální adresy).

Rozsahy adres dle tříd
A 1.0.0.0/8 – 127.0.0.0/8
B 128.0.0.0/16 – 191.0.0.0/16
C 192.0.0.0/24 – 223.0.0.0/24
D 224.0.0.0 – 239.255.255.255
E 240.0.0.0 – 255.255.255.255

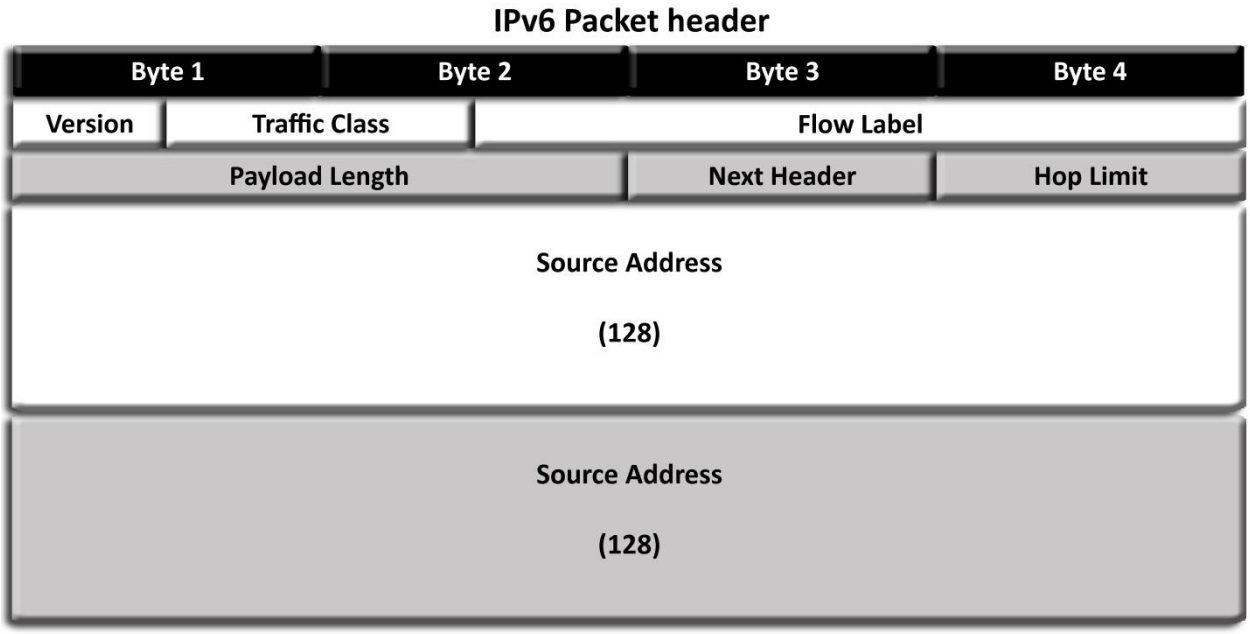
Sítě z *třídy A (Class A blocks)* měly být užívány se síťovým prefixem /8 a přidělovány obrovským organizacím s počtem hostů v řádech milionů. V praxi by tak bylo možné přidělit tyto velké adresy jen asi cca 120 organizacím.
Sítě z *třídy B (Class B blocks)* měly být užívány se síťovým prefixem /16, čímž by vzniklo zhruba přes 16 000 sítí, z nichž každá by poskytla adresní prostor pro více než 65 000 hostů.
Konečně třída C *(Class C block)* s prefixem /24 měla být určena pro zhruba 2 miliony malých organizací s maximálním počtem 254 hostů.

Toto striktní rozdělení rozsahů s pevně danými prefixy (*Classfull Addressing*) však nesplňovalo technické požadavky na využívání síťových zdrojů (např. u ethernetu a IPv4 z důvodu obrovského množství broadcastových požadavků zejména ve třídě A a B) ani požadavky na efektivní využívání síťových adres. Proto se v praxi setkáváme spíš s různě dlouhými prefixy v jakémkoliv síťovém rozsahu (*Classless Addresing*).
I tak se v IP světě pro prefixy /8, /16 a /24 vžilo označení dle tříd.

Přidělování veřejných adres
Jednotlivé adresní rozsahy bylo možno dříve získat přímo od organizace IANA, nicméně mnoho dalších rozsahů svěřila IANA dalším organizacím zabývajícím se registrací veřejných adres (např. RIPE, ARIN). Tito registrátoři obvykle poskytují adresy internetovým providerům, kteří je pak používají pro své vlastní účely nebo pronajímají svým zákazníkům.

IPv6 – náhrada za IPv4
Z důvodu postupného ubývání volných veřejných IPv4 adres vytvořila počátkem 90. let organizace IETF nový IPv6 protokol, který by měl vyřešit nedostatek volných IPv4 adres a některé slabiny IPv4 protokolu. Zvláštní důraz byl kladen např. na:
- zrychlení zpracování paketů
- zvýšenou škálovatelnost sítí a dlouhověkost nového protokolu
- integraci QoS mechanizmů
- integraci bezpečnostních prvků

Výsledky vývoje IPv6:
- 128bitové hierarchické adresování zajišťující prakticky nevyčerpatelné rozsahy adres
- zjednodušení síťové hlavičky umožňující rychlé zpracování paketů
- zvýšená podpora pro možnou integraci dalších nových možností a služeb
- zajištění QoS mechanizmů formou označení jednotlivých toků dat
- ověřovací a ochranné možnosti



Vzhledem k některým zásadním změnám bylo třeba krom nového síťového protokolu vyvinout celou sadu nových protokolů na dalších vrstvách OSI modelu, např. ICMPv6.

Výhled do budoucna

Protože se v posledních letech podařilo vyvinout mnoho nových efektivnějších způsobů využívání IPv4 protokolu a hlavně jeho síťových adres, je implementace IPv6 protokolu zatím velice pomalá. Nicméně dříve nebo později se IPv6 stane dominantní sadou internetových protokolů.