Rodina protokolů IPv4

Síťové protokoly musí zajistit univerzální

- Adresaci – logické adresy (probráno dříve)
- Prostředí a služby – parametry „rodiny“ IP protokolů

Do rodiny IP patří

- IP – Internet Protocol
- ICMP – Internet Control Message Protocol
- IGMP – Internet Group Management Protocol

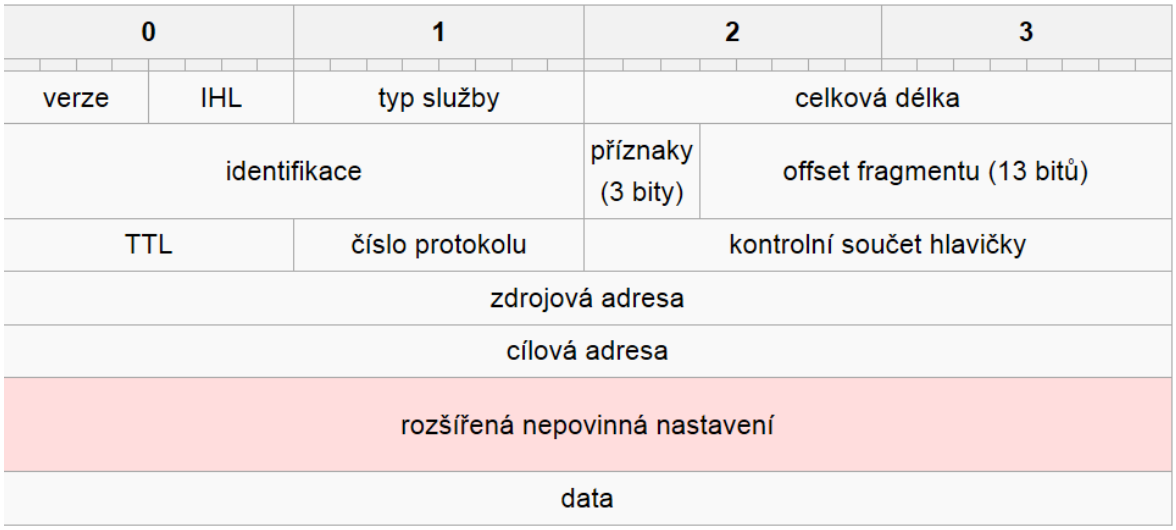
Internet Protokol

Na síťové vrstvě je datovou jednotkou – paket (packet). V případě IP proto IP paket. Univerzálnějším vyjádřením datové jednotky, přenášené v síti (internet) samostatně, je datagram. Paket je současně i datagram, protože každý paket je přenášen samostatně bez vazby na ostatní (na síťové vrstvě se nevytváří „spoj“). Na síťové vrstvě lze použít pro označení datové jednotky IP paket nebo IP datagram. IP paket je přesnější výraz, proto je dále používán.

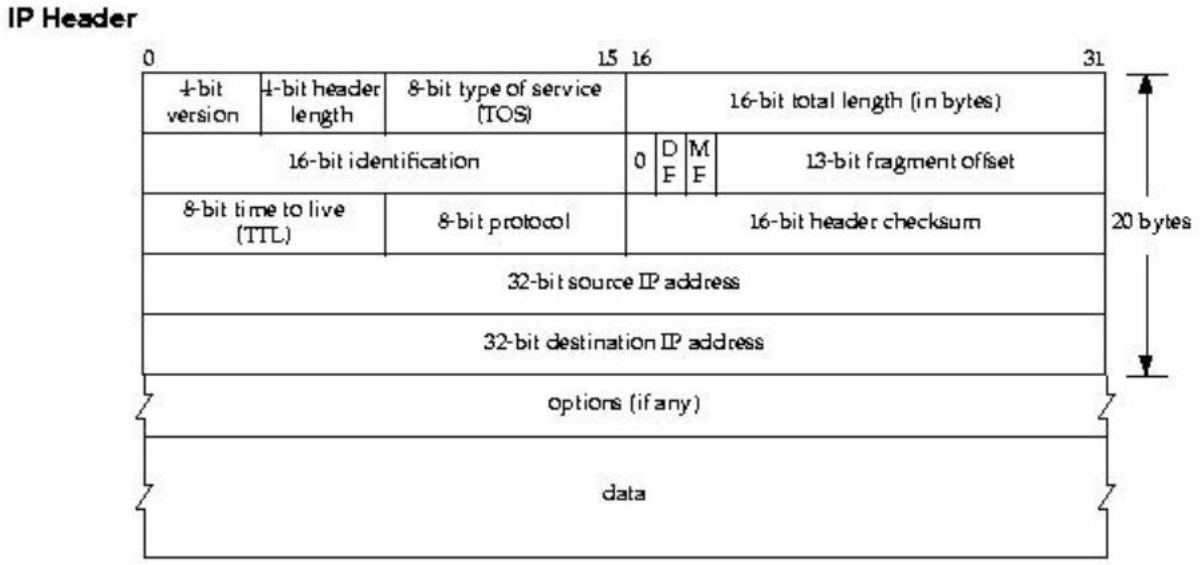
IPv4 paket

Paket se sestává z datové části a hlavičky. Datová část může být různé délky. Režijní část paketu se sestává z hlavičky a záhlaví (délka 20Bhlavička + max.40Bvolitelné záhlaví). Šířka zpracovávaného slova je dána použitým HW a bývá většinou 4B = 32bitů (viz. 32bitovéOS). Hlavička IPv4 je proto členěna do 5slov po 4B. Každé slovo obsahuje určité parametry (tento rozměr hlavičky je použit u TCP protokolu).

Hlavička s českým popisem:



Hlavička (Header) s anglickým popisem (paketové analyzátory nepřekládají…):



Popis polí hlavičky:

1 slovo – obecná část

- **Verze (Version)**: verze protokolu (0x4) – např. IPv4 – verze 4
- **IHL(Internet Header Length)**: délka hlavičky ve slovech (4B).Typická a minimální je (0x5) tj. 5*4B a maximální (0xF)tj. 15*4 = 60B.
- **Typ služby (TOS, Type of Service)**: podle původních představ měla tato položka umožnit odesilateli, aby zvolil charakter přepravní služby ideální pro dotyčný paket. Jednotlivé bity znamenaly - požadavek na nejmenší zpoždění, největší šířku pásma či nejrychlejší cestu v síti. Směrování mělo brát ohled na hodnotu TOS a volit z alternativních tras tu, která nejlépe odpovídala požadavkům. V praxi k realizaci nedošlo. V současnosti se položka zřídka používá k účelům QoS (Quality of Services) a nese příznak pro mechanismy zajišťující služby s definovanou kvalitou.
- **Celková délka (Total Length)**: celková délka paketu v bajtech. Vyjádření 16 bity umožňuje maximální délku paketu „FFFF“ = 65536 B. Jedná se o „SW“ údaj bez vazby na prostředí. To je realizováno většinou Ethernetem, který má maximální datovou část rámce 1500B (MTU 1500 – Maximum Transmission Unit). Tímto je limitována délka běžných IP paketů.

2 slovo – zajištění fragmentace

Fragmentace

- **Identifikace (Identification)**: odesilatel přidělí každému odeslanému paketu jednoznačný identifikátor. Pokud byl datagram při přepravě fragmentován, pozná se podle této položky, které fragmenty patří k sobě (mají stejný identifikátor).
- **Příznaky (Flags)**: 3 bity, které slouží k řízení fragmentace.
  - První bit - je vždy nulový a nevyužit
  - Druhý bit - ***Don't fragment*** „1" - zakazující tento paket fragmentovat „0" - OK
  - Třetí bit - ***More fragments*** „1" - následuje fragment, „0" – poslední fragment
- **Offset fragmentu (Fragment Offset)**: 13 bitové číslo udává pozici fragmentu vzhledem k začátku původního paketu. Jednotkou je oktet – 8B. Podle offsetu defragmentuje cílové KZ paket do původní podoby.

3 slovo – „zabezpečení" služby

- **TTL (Time To Live)**: představuje ochranu proti zacyklení. Každý směrovač zmenší tuto hodnotu o jedničku (případně o počet sekund, které datagram ve směrovači strávil, pokud zde čeká déle). Pokud tím TTL nabude hodnotu nula, datagram zahodí, protože vypršela jeho životnost.
- **Protokol (Protocol)**: určuje, kterému protokolu vyšší vrstvy se mají data předat při doručení. Čísla protokolů definována v RFC 1700 (TCP: 6, UDP: 17, ICMP: 1, EGP: 8, …). RFC 1700 je již překonáno novým standardem RFC 3232, jež odkazuje na databáze organizace IANA a její stránky: http://www.iana.org .
- **Kontrolní součet hlavičky (Header Checksum)**: slouží k ověření, zda nedošlo k poškození paketu. Počítá se pouze z hlavičky. Pokud nesouhlasí, paket je zahozen. V žádném případě se tímto nekontrolují data.

4 slovo – IP adresa odesílatele

- **Adresa odesílatele**: IPv4 adresa síťového rozhraní, které datagram vyslalo.

5 slovo – IP adresa příjemce

- **Adresa cíle**: IP adresa síťového rozhraní, kterému je datagram určen.

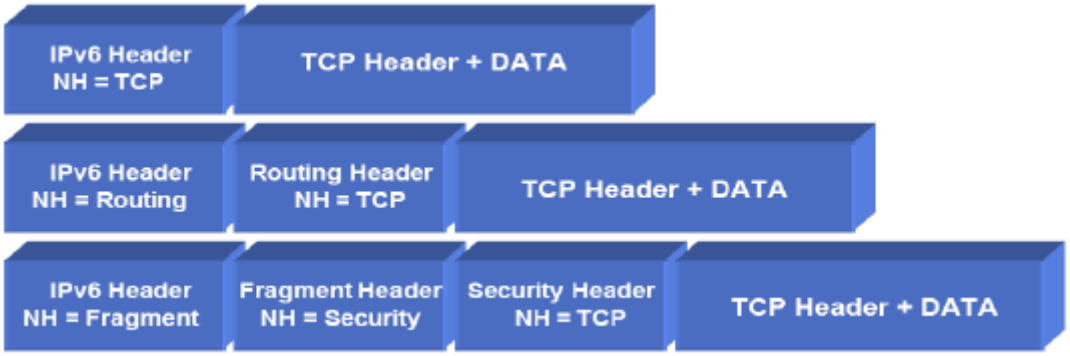
Záhlaví – volitelná část

- **Volby**: různé rozšiřující informace či požadavky. Například lze předepsat sérii adres, kterými má paket projít. Volby obvykle nejsou v paketu použity
- **Data**: obsahuje další zapouzdřené protokoly.

Zdroj: wikipedie

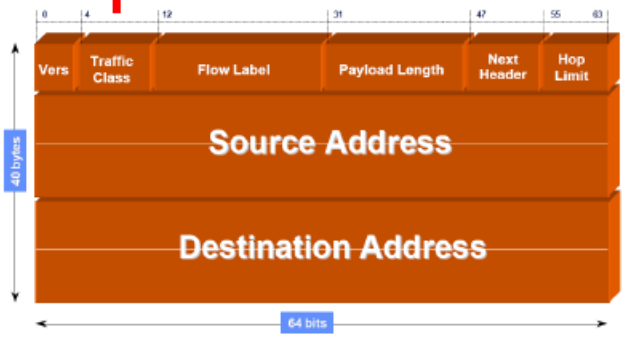
Hlavička IPv6

IPv6 zajišťuje další služby a to hlavně – bezpečnost, mobilitu. I proto je nově rozšířen o dodatečné (rozšiřující) hlavičky. Ty jsou řazeny za základní a vytvářejí tzv. vláček.



- Struktura hlavičky se skládá ze 40B záhlaví následovaného rozšířeními
  - pole Verze (4b) obsahuje 6 (u IPv4 4)
  - pole třída dat specifikuje naléhavost dat
    - jinak řečeno, která data budou zahazována v případě zahlcení sítě

- 0 - nespecifikovaná data
- 1 - provoz na pozadí (např. news)
- 2 - automatický provoz (např. mail)
- 4 - uživatelské velké přenosy (ftp. ...)
- 6 - interaktivní přenos (VNC, telnet...)
- 7 - management sítě (RIP, SNMP...)
- 8 - 15 přenosy v reálném čase
  - multimediální data
  - realtime řízení technolog. procesů
  - data s vyšším číslem (≥8) mají vyšší prioritu



- Další položky tvoří:
  - délka dat (2B = 65535B), bez základní hlavičky
    - s použitím příznaku „ohromný datagram“ v další hlavičce i více
  - typ další hlavičky
    - TCP, UDP, IPv4, rozšíření hlavičky IPv6
  - identifikace toku dat — nová myšlenka
    - slouží ke dvěma účelům
      - **snížení zátěže směrovačů**
    - datagramy jednoho toku dostanou shodný identifikátor
    - směrovače pak řeší úlohu směrování pouze pro první datagram
    - další datagramy odesílá stále do stejného rozhraní (max. 6s)
      - **další možností je zajištění QoS**
    - směrovače se nakonfigurují tak, aby pro pakety s určitým FL upřednostňovaly jejich směrování
    - směrovače pak neobsluhují datagramy jako sekvenční frontu ale vybírají pakety s vhodným FL

- Pole „Next Header“
  - ukazuje jaký typ hlavičky následuje (TCP, UDP, IPv4 nebo další IPv6)
    - v další hlavičce je za polem *Next Header* pole specifikující posunutí k další hlavičce
    - základní hlavička toto pole nemá, má vždy 40B

Pole – HOP LIMIT – je funkčně stejné jako TTL u IPv4 , počet skoků k cíli.

Dodatečné hlavičky

První tři jsou z IPv4, další dvě ohledně bezpečnosti (převzato z IPsec) a další dvě jsou ohledně zajištění mobility.

- *Volby pro všechny*
  - informace zajímavé pro každého po cestě (např. **upozornění pro směrovače**, že paket nese data, která by jej mohla zajímat)
- *Explicitní směrování*
  - datagram musí projít předepsanou cestou

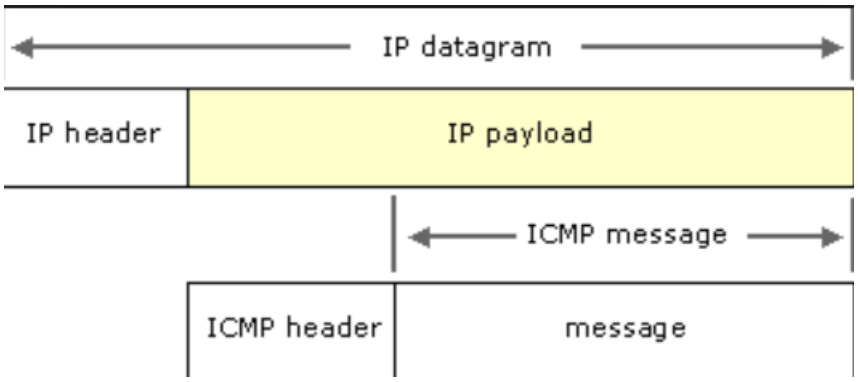
Patrně stejně „nestravitelné“ jako u IPv4

- *Fragmentace*
  - při fragmentaci paketu nese informace nutné pro jeho složení do původní podoby
- *Šifrování obsahu (ESP)*
  - obsah datagramu je zašifrován, ESP hlavička nese odkaz na parametry pro dešifrování
- *Autentizace (AH)*
  - data pro ověření totožnosti odesilatele a původnosti obsahu
- *Volby pro cíl*
  - informace určené příjemci datagramu (např. domácí adresa mobilního uzlu)
- *Mobilita*
  - hlavička pro potřeby komunikace s mobilními zařízeními
  - v podstatě explicitní směrování →pevná IP (domácí) + mobilní IP (přesměrování)

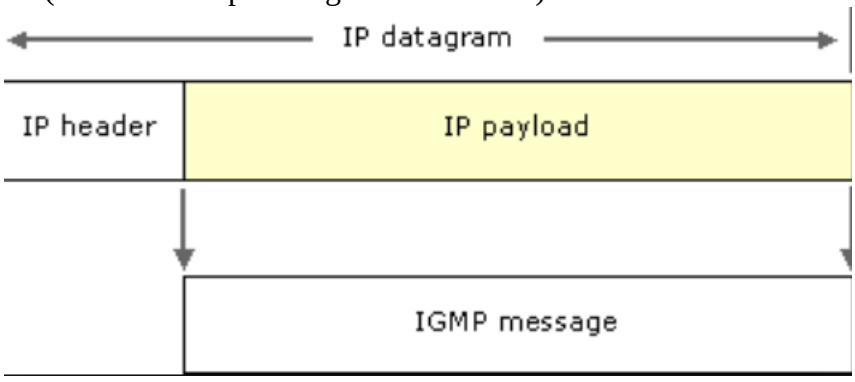
IP protokol přepravuje data bez záruky, tj. negarantuje ani doručení ani zachování pořadí ani vyloučení duplicit. Zajištění těchto záruk je ponecháno na vyšší vrstvě, kterou například představuje protokol TCP. Hlavním cílem je nalezení ideální cesty internetem.

Protokoly ICMP a IGMP

IP protokol by k zajištění služeb síťové vrstvy nestačil. Musí být ošetřeny nestandardní stavy (chyby apod.) vznikající při přenosu paketu sítí. To je úkolem protokolu ICMP (Internet Control Message Protocol).



IP protokol je orientován především pro zajištění „unicast“ adresace (komunikace 1:1). To opět nestačí a musí být zajištěny všechny typy adresací tj. multicast a broadcast. To je úkolem protokolu IGMP (Internet Group Management Protocol).



Oba protokoly jsou realizovány na transportní vrstvě (L4). K přenosu dat tedy využívají IP paketů, do kterých jsou „encapsulovány“ (zapouzdřeny). Patří mezi protokoly transportní vrstvy, které se označují jako pseudoprotokoly transportní vrstvy nebo také RAW (znamená to, že mají specifický formát a neposkytují běžné služby transportní vrstvy). Využití vyšší vrstvy k zajištění služeb nižší vrstvy je běžnou záležitostí.

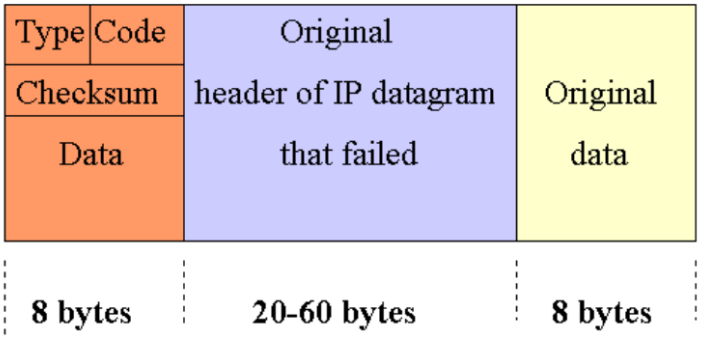
Internet Control Message Protocol

Ošetření nestandardních stavů většinou musí provádět směrovač. Zprávy ICMP se vysílají například v těchto případech:

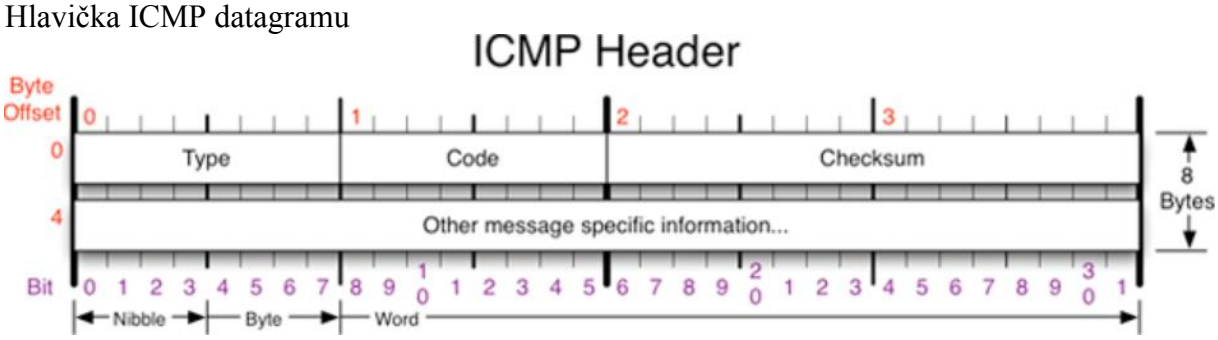
- Adresa cílové sítě není ve směrovací tabulce
- Koncový uzel je nedostupný
- Hodnota TTL klesla na nulu
- Potřeba fragmentovat paket s příznakem „nefragmentovat“

ICMP protokol definovaný v RFC 792. ICMP dále používají obslužné programy „ping“ a „traceroute“ (síťové diagnostické utility).

Formát ICMP datagramu obsahuje – hlavičku, IP hlavičku původního paketu a doplňující data.



Hlavička ICMP datagramu



Type (typ zprávy) – (1 B) specifikuje typ ICMP zprávy. Teoretický prostor je pro 256 typů zpráv. Využita je pouze část a navíc „ na přeskáčku“(např. 0 a potom 3 apod.). Nejznámějšími typy ICMP zpráv jsou

Type		Popis
8	Echo request (Ozvěna)	Slouží ke zjištění, zda je v síti stále přítomen určitý uzel IP (hostitel nebo směrovač).
0	Echo reply (Odpověď na ozvěnu)	Odpověď na požadavek odezvy ICMP.
3	Destination unreachable (Nedosažitelný cíl)	Informuje hostitele o tom, že datagram nelze doručit.
4	Source quench (Zpomalení toku dat ze zdroje)	Žádá hostitele o snížení rychlosti, jakou jsou odesílány datagramy, z důvodů zahlcení přenosové cesty.
5	Redirect (Přesměrování)	Informuje hostitele o upřednostňované trase.
11	Time exceeded (Překročení času)	Informuje o tom, že platnost hodnoty TTL (Time-to-Live) datagramu IP vypršela.

Code („ podtyp“ zprávy) - (1B) “Subtype” pro určitý typ zprávy. Detailnější specifikace je u některých typů zpráv nutná. Níže je uveden jako příklad podtyp „nedosažitelného cíle“.

3 – Destination Unreachable[3]:4	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Destination host unknown
	8	Source host isolated
	9	Network administratively prohibited
	10	Host administratively prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication administratively prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect

- 0 - Destination network unreachable … nedostupná cílová síť, reakce směrovače na požadavek komunikovat se sítí, do které nezná cestu
- 1 - Destination host unreachable … nedostupný cílový stroj
- 2 – Destination protocol unreachable … informace o nemožnosti použít vybraný protokol
- 3 – Destination port unreachable … informace o nemožnosti připojit se na vybraný port

Checksum (2B)– Error checking data. Kontrolní součet je vypočítán z ICMP header+data, (with value 0 for this field).

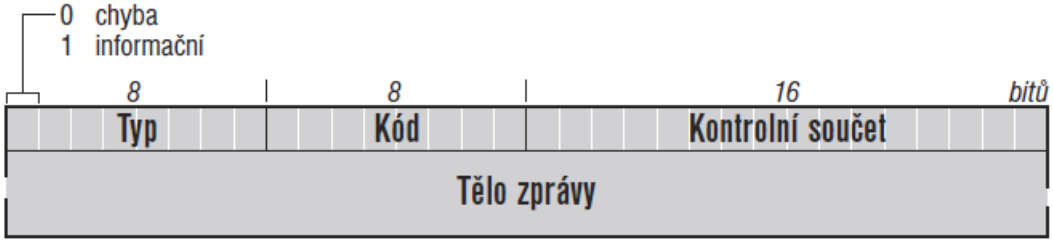
Rest of Header – (4B – druhé slovo hlavičky). Obsahuje eventuální doplňující informace dle typu zprávy.

Někdy je používání ICMP znemožněno špatným nastavením firewallu.

ICMPv6

V IPv6 přebírá ICMP další role. Zajišťuje funkce ARP v IPv4 , zajišťuje informace ohledně fragmentace a předává další režijní informace (podpora skupinových adres).

IP datagram nesoucí ICMPv6 zprávu, signalizuje hodnota 58 v položce *Další hlavička*.



Všechny ICMP zprávy mají jednotný základ.

***Typ (Type)* určuje základní druh zprávy.**

Typy zprávy jsou rozděleny do **dvou tříd: na chybové (jejichž *Typ* leží v intervalu od 0 do 127) a informační (*Typ* 128 až 255).**

chyby

1	cíl je nedosažitelný
2	příliš velký paket
3	vypršela životnost paketu
4	problém s parametry

echo

128	požadavek na echo
129	odpověď na echo

MLD (skupinové adresování)

130	dotaz na členství ve skupině
131	ohlášení členství ve skupině
132	ukončení členství ve skupině
143	ohlášení členství ve skupině (MLDv2)

objevování sousedů

133	výzva směrovači
134	ohlášení směrovače
135	výzva sousedovi
136	ohlášení souseda
137	přesměrování
148	žádost o certifikační cestu
149	ohlášení certifikační cesty

informace o uzlu

139	dotaz na informace
140	odpověď s informacemi

inverzní objevování sousedů

141	IND výzva
142	IND ohlášení

mobilita

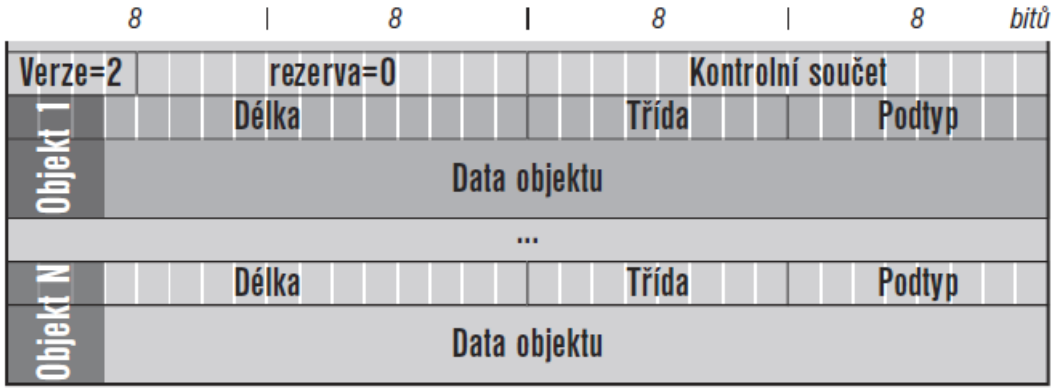
144	žádost o adresy domácích agentů
145	odpověď s adresami domácích agentů
146	žádost o mobilní prefix
147	ohlášení mobilního prefixu
154	rychlé předávání

objevování skupinových směrovačů

151	ohlášení skupinového směrovače
152	výzva skupinovému směrovači
153	ukončení skupinového směrovače

Rozšířené ICMP

RFC 4884: *Extended ICMP to Support Multi-Part Messages d*efinuje **rozšíření, kterými lze do těla zprávy přidávat další informace.**



Rozšíření se přidává na konec těla ICMP zprávy.

Za úvodní hlavičkou poskytující jen číslo verze a kontrolní součet se nachází **libovolný počet rozšiřujících objektů.**

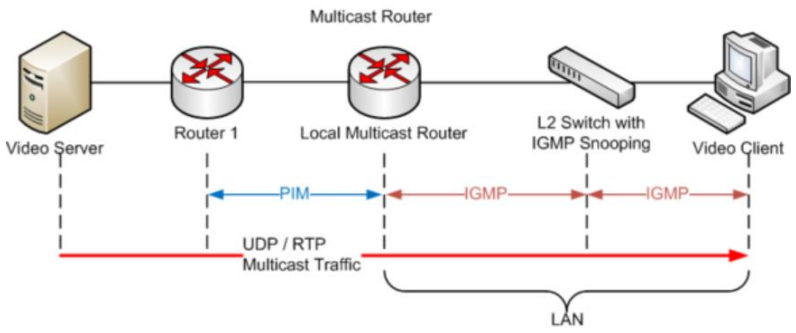
Každý z nich má svou vlastní hlavičku, obsahující jeho *Délku (Length)*, *Třídu (Class-Num)* a *Podtyp (C-Type)*. Za ní pak následují vlastní data rozšiřujícího objektu

Internet Group Management Protocol

Protokol IGMP slouží k zajištění možnosti šíření tzv. lokálního multicastu (skupinového vysílání) v rámci LAN. Řízení skupinového vysílání má opět na starosti pověřený směrovač (multicastový).

Skupinové vysílání

Data skupinového (multicast) vysílání IP jsou odesílána na jedinou adresu, ale zpracovává je více hostitelů (více KZ). Princip skupinového vysílání IP je podobný principu novinového předplatného. Podobně jako právě vydané noviny obdrží pouze jejich předplatitelé, data protokolu IP odeslaná na adresu IP rezervovanou pro skupinu skupinového vysílání přijmou a zpracují pouze hostitelské počítače, které patří do této skupiny. Skupina hostitelů, kteří přijímají zprávy odeslané na určitou adresu IP pro skupinové vysílání, se nazývá multicast group.



Velikost skupin není omezena a jejich členové mohou být rozptýleni ve více sítích IP (pokud směrovače, kterými jsou tyto sítě propojeny, podporují šíření dat skupinového vysílání IP a

informací o členství ve skupinách). Navíc hostitel, který odesílá data protokolu IP na adresu IP skupiny, nemusí do této skupiny patřit.

Pro správnou funkci musí být zajištěno dynamické přihlašování a odhlašování ze skupiny. Více směrovačů v síti si musí rozdělit role – jeden je „posluchač“(pasivní) a druhý „dotazovač“(aktivní). Ten zasílá dotazy.

Příklad přidělených skupinových (multicast) adres:

IP multicast address range	Description	Routable
224.0.0.0 to 224.0.0.255	Local subnetwork[1]	No
224.0.1.0 to 224.0.1.255	Internetwork control	Yes
224.0.2.0 to 224.0.255.255	AD-HOC block 1[2]	Yes
224.3.0.0 to 224.4.255.255	AD-HOC block 2[3]	Yes
232.0.0.0 to 232.255.255.255	Source-specific multicast[1]	Yes
233.0.0.0 to 233.255.255.255	GLOP addressing[1]	Yes
233.252.0.0 to 233.255.255.255	AD-HOC block 3[4]	Yes
234.0.0.0 to 234.255.255.255	Unicast-prefix-based	Yes
239.0.0.0 to 239.255.255.255	Administratively scoped[1]	Yes

Adresa vícesměrového vysílání IP	Popis
224.0.0.0	Základní adresa (rezervováno).
224.0.0.1	Skupina vícesměrového vysílání All Hosts (všichni hostitelé), do které patří všechny systémy v daném síťovém segmentu.
224.0.0.2	Skupina vícesměrového vysílání All Routers (všechny směrovače), do které patří všechny směrovače v daném síťovém segmentu.
224.0.0.5	Adresa AllSPFRouters (všechny směrovače) protokolu OSPF (Open Shortest Path First). Používá se k odesílání informací o trasách OSPF všem směrovačům OSPF v daném síťovém segmentu.
224.0.0.6	Adresa AllDRouters (všechny vyhrazené směrovače) protokolu OSPF. Používá se k odesílání informací o trasách OSPF vyhrazeným směrovačům OSPF v daném síťovém segmentu.
224.0.0.9	Adresa skupiny RIP verze 2. Používá se k odesílání informací o trasách RIP všem směrovačům RIP 2 v daném síťovém segmentu.
224.0.1.24	Adresa skupiny serverů WINS. Zajišťuje podporu automatického vyhledávání a dynamického konfigurování replikace u serverů WINS.

The following table is a list of notable well-known IPv4 addresses that are reserved for IP multicasting and that are registered with the Internet Assigned Numbers Authority (IANA).[7]

IP multicast address	Description	Routable
224.0.0.0	Base address (reserved)	No
224.0.0.1	The *All Hosts* multicast group addresses all hosts on the same network segment.	No
224.0.0.2	The *All Routers* multicast group addresses all routers on the same network segment.	No
224.0.0.4	This address is used in the Distance Vector Multicast Routing Protocol (DVMRP) to address multicast routers.	No
224.0.0.5	The Open Shortest Path First (OSPF) *All OSPF Routers* address is used to send Hello packets to all OSPF routers on a network segment.	No
224.0.0.6	The OSPF *All Designated Routers* ""(DR)"" address is used to send OSPF routing information to designated routers on a network segment.	No
224.0.0.9	The Routing Information Protocol (RIP) version 2 group address is used to send routing information to all RIP2-aware routers on a network segment.	No
224.0.0.10	The Enhanced Interior Gateway Routing Protocol (EIGRP) group address is used to send routing information to all EIGRP routers on a network segment.	No
224.0.0.13	Protocol Independent Multicast (PIM) Version 2	No
224.0.0.18	Virtual Router Redundancy Protocol (VRRP)	No
224.0.0.19–21	IS-IS over IP	No
224.0.0.22	Internet Group Management Protocol (IGMP) version 3[8]	No
224.0.0.102	Hot Standby Router Protocol version 2 (HSRPv2) / Gateway Load Balancing Protocol (GLBP)	No
224.0.0.107	Precision Time Protocol (PTP) version 2 peer delay measurement messaging	No
224.0.0.251	Multicast DNS (mDNS) address	No
224.0.0.252	Link-local Multicast Name Resolution (LLMNR) address	No
224.0.0.253	Teredo tunneling client discovery address[9]	No
224.0.1.1	Network Time Protocol clients listen on this address for protocol messages when operating in multicast mode.	Yes
224.0.1.22	Service Location Protocol version 1 general	Yes
224.0.1.35	Service Location Protocol version 1 directory agent	Yes
224.0.1.39	The Cisco multicast router *AUTO-RP-ANNOUNCE* address is used by RP mapping agents to listen for candidate announcements.	Yes
224.0.1.40	The Cisco multicast router *AUTO-RP-DISCOVERY* address is the destination address for messages from the RP mapping agent to discover candidates.	Yes
224.0.1.41	H.323 Gatekeeper discovery address	Yes
224.0.1.129–132	Precision Time Protocol (PTP) version 1 messages (Sync, Announce, etc.) except peer delay measurement	Yes
224.0.1.129	Precision Time Protocol (PTP) version 2 messages (Sync, Announce, etc.) except peer delay measurement	Yes
239.255.255.250	Simple Service Discovery Protocol address	Yes
239.255.255.253	Service Location Protocol version 2 address	Yes

Zdroj Wikipedie

Připojování hostitelů ke skupinám skupinového vysílání se provádí prostřednictvím zpráv IGMP.

Funkce a formát IGMP zprávy

Aby se stanice přihlásila do skupiny, musí zaslat přes protokol IGMP zprávu „Membership report“ s IP adresou třídy D. Tato zpráva dorazí k směrovači lokální sítě a ten si ji zapíše do tabulky. K odhlášení ze skupiny použije stanice typ zprávy „Leave group“ pokud v tabulce neexistuje žádná stanice, která by chtěla z této adresy informace odebírat, směrovač záznam z tabulky zruší.

Směrovač zasílá také periodický dotaz „General query“ ke stanicím v lokální sítí, jestli je v ní alespoň jedna stanice, která chce ze skupiny informace odebírat. Pokud mu žádná do 10 sekund neodpoví, vymaže z tabulky záznam o skupině. Tento dotaz řeší problém, kdy se nějaká stanice, např. před vypnutím, nestihne z odběru skupiny odhlásit.

IMGP protokol má tři verze. Protokoly IGMPv1 a IGMPv2 jsou svou strukturou velmi podobné.

Formát IGMPv2

Bity	0–7	8–15	16–31
0	typ	max. čas odpovědi	kontrolní součet
32	skupinová adresa		

Formát IGMPv3

Bity	0–7	8–15	16–31
0	typ	rezervované	kontrolní součet
32	rezervované		počet záznamů skupin
64	záznam skupiny [1]		
...	záznam skupiny [n]		

Typ (1B)- typ dotazu

- Membership Query (0x11)
- Membership Report (IGMPv1: 0x12, IGMPv2: 0x16)
- Leave Group (0x17)
- IGMPv3 adds type Membership Report (0x22)

Verze 2 **Maximum Response Time (1B)**- max. čas na odpověď. Krok je 100msec.
Verze 3 **Max Resp Code** - podobné

Checksum (2B) - kontrolní součet hlavičky

Verze 2 – **Skupinová adresa** (4B)
Verze3 - **Počet záznamů skupin** (2B)

A dále ve verzi 3 následují slova se záznamem skupiny (ten obsahuje i skupinovou adresu)

Zdroj: MS Technet a Wikipedie