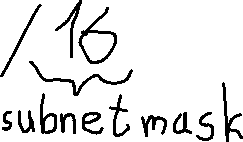
# IPv4, adresování - formát paketu, maska, podsíť. porovnání s IPv6

* je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. Funguje na třetí vrstve OSI modelu.
* 32-bitová dělí se na čtyři políčka(oktety) oddělené tečkou. V každém jenom políčku (oktetu) může bít číslo od 0 do 256 např: 192.168.0.2
* Nejprve historicky se rozsahy ip adres rozdávaly a dělili na třídy A, B, C, (D,E)

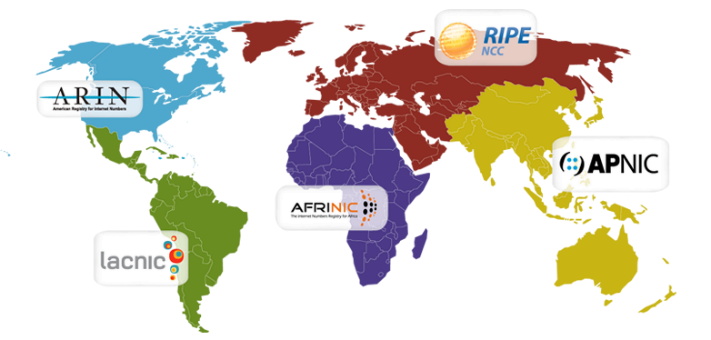
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Class** | **Leading bits** | **Size of *network number* bit field** | **Size of *rest* bit field** | **Number of networks** | **Number of addresses per network** | **Start address** | **End address** |
| **A** | 0 | 8 | 24 | 128 (27) | 16777216 (224) | 0.0.0.0 | 127.255.255.255 |
| **B** | 10 | 16 | 16 | 16384 (214) | 65536 (216) | 128.0.0.0 | 191.255.255.255 |
| **C** | 110 | 24 | 8 | 2097152 (221) | 256 (28) | 192.0.0.0 | 223.255.255.255 |
| **D** |  | 4 | 24 | IP multicast | 268435456 | 224.0.0.0 | 239.255.255.255 |
| **E** | Research & development | = wasted | same |  | 268435456 | 240.0.0.0 | 254.255.255.255 |

* Ip adresa se zkládá z tří částí z network part, host part a subnet mask. Sumbnet mask rozhoduje na jekém bitu končí network part tedy po jakém bitu zační host part. Subnet mask se může psat ve tvaru /16 nebo 255.255.0.0 nebo 11111111.11111111.00000000.00000000



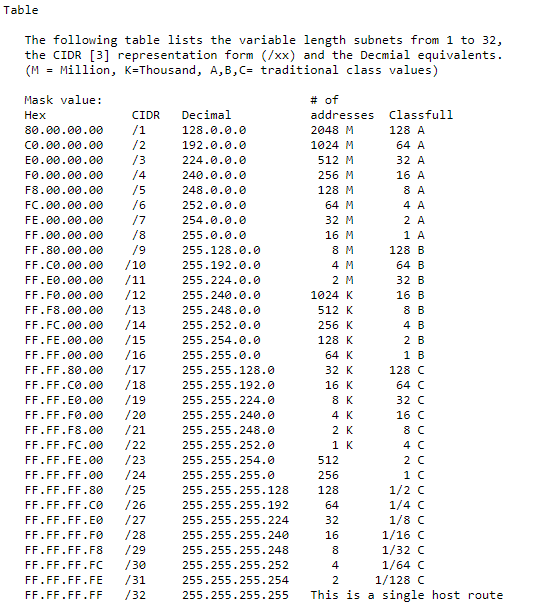


* Ip adressy globálně spravuje Internet Assigned Numbers Authority (IANA), ta své rosahy rozdělí mezi další společnost které následné rosahy operují ned danými světadíly



* Ip adresa má dvě vlastnosti kromě toho že identifikuje hosta (síťový prvek) v komunikaci na třetí vrstvě OSI modelu a poskytuje nám polohu hosta v síti a možnost vytvořit cestu k danému hostu při komunikace s ním.
* Internet Protocol verze 4 byl vyvinut již v roce 1983 v ARPANETU (krom nejznámějších protokolů v4 a v6 existuje taká v1, v2, v3, InternetStream Protocol (v5), v7 (TP/IX: The Next Internet), v8 (PIP — The P Internet Protocol), v9 (TUBA — Tcp & Udp with Big Addresses))
* První adresa se využívá jako adresa sítě a poslední adresa jako broadcast adresa

Nowadays je možné ipv4 rozdělovat po jednotlivých bitech jako je vidět na obrázku:



## Rozsahy rezervované

Ipv4 adressy vyhranili speciální bloky adres pro speciální způsob užití.

### Privátní síť:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **10.0.0.0/8** | **10.0.0.0–10.255.255.255** | **16777216** | **Private network** | **Used for local communications within a private network.** |
| 100.64.0.0/10 | 100.64.0.0–100.127.255.255 | 4194304 | Private network | [Shared address space](https://en.wikipedia.org/wiki/IPv4_shared_address_space) for communications between a service provider and its subscribers when using a [carrier-grade NAT](https://en.wikipedia.org/wiki/Carrier-grade_NAT). |
| **172.16.0.0/12** | **172.16.0.0–172.31.255.255** | **1048576** | **Private network** | **Used for local communications within a private network.** |
| 192.0.0.0/24 | 192.0.0.0–192.0.0.255 | 256 | Private network | IETF Protocol Assignments. |
| **192.168.0.0/16** | **192.168.0.0–192.168.255.255** | **65536** | **Private network** | **Used for local communications within a private network.** |
| 198.18.0.0/15 | 198.18.0.0–198.19.255.255 | 131072 | Private network | Used for benchmark testing of inter-network communications between two separate subnets. |

### Síťe používane pro dokumetaci:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.0.2.0/24 | 192.0.2.0–192.0.2.255 | 256 | Documentation | Assigned as TEST-NET-1, documentation and examples. |
| 198.51.100.0/24 | 198.51.100.0–198.51.100.255 | 256 | Documentation | Assigned as TEST-NET-2, documentation and examples. |
| 203.0.113.0/24 | 203.0.113.0–203.0.113.255 | 256 | Documentation | Assigned as TEST-NET-3, documentation and examples. |
| 233.252.0.0/24 | 233.252.0.0-233.252.0.255 | 256 | Documentation | Assigned as MCAST-TEST-NET, documentation and examples. |

Podsíťová rozsahy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **169.254.0.0/16** | **169.254.0.0–169.254.255.255** | **65536** | **Subnet** | **Used for**[**link-local addresses**](https://en.wikipedia.org/wiki/Link-local_address)**between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a**[**DHCP**](https://en.wikipedia.org/wiki/DHCP)**server. Not routable** |
| **255.255.255.255/32** | **255.255.255.255** | **1** | **Subnet** | **Reserved for the "limited**[**broadcast**](https://en.wikipedia.org/wiki/Broadcast_address)**" destination address.** |

### Loopback rozsah

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **127.0.0.0/8** | **127.0.0.0–127.255.255.255** | **16777216** | **Host** | **Used for**[**loopback addresses**](https://en.wikipedia.org/wiki/Loopback_address)**to the local host.**[**[1]**](https://en.wikipedia.org/wiki/Reserved_IP_addresses#cite_note-rfc6890-1) |

### Aktuální síť

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **0.0.0.0/8** | **0.0.0.0–0.255.255.255** | **16777216** | **Software** | **Current network**[**[1]**](https://en.wikipedia.org/wiki/Reserved_IP_addresses#cite_note-rfc6890-1) |

### Speciální případy využívané na interentu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.88.99.0/24 | 192.88.99.0–192.88.99.255 | 256 | Internet | Reserved.[[7]](https://en.wikipedia.org/wiki/Reserved_IP_addresses#cite_note-rfc7526-7) Formerly used for [IPv6 to IPv4](https://en.wikipedia.org/wiki/6to4) relay[[8]](https://en.wikipedia.org/wiki/Reserved_IP_addresses#cite_note-rfc3068-8) (included [IPv6](https://en.wikipedia.org/wiki/IPv6) address block [2002::/16](https://en.wikipedia.org/wiki/IPv6_address#Special_addresses)). |
| **224.0.0.0/4** | **224.0.0.0–239.255.255.255** | **268435456** | **Internet** | **In use for**[**IP multicast**](https://en.wikipedia.org/wiki/IP_multicast)**. (Former Class D network.)** |
| 240.0.0.0/4 | 240.0.0.0–255.255.255.254 | 268435455 | Internet | Reserved for future use. (Former Class E network.) |

## Paket ipv4

Packet geader se pohybuje s velikostí od 20 do 60 bajtů. Celý packet může mít velikost až 2^16 tedz 65536 bajtů. Tedy payload může mít velikost odpovídající maximální veliskosti packet zmenšené o header (tedy od 65475 do 65515).

Na ipv4 síti můžeme posílat tři druhy paketů:

1. Unicast (one to one) … sending packet to one host.
2. Multicast (one to many of many) … sending packet to group of hosts.
3. Broadcast (one to many) … sending packet to all hosts on subnet.

Obsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automaticky

**Version**

The first header field in an IP [packet](https://en.wikipedia.org/wiki/Packet_(information_technology)) is the four-bit version field. For IPv4, this is always equal to 4.

**Internet Header Length (IHL)**

The IPv4 header is variable in size due to the optional 14th field (options). The IHL field contains the size of the IPv4 header; it has 4 bits that specify the number of 32-bit words in the header. The minimum value for this field is 5,[[35]](https://en.wikipedia.org/wiki/Internet_Protocol_version_4#cite_note-35) which indicates a length of 5 × 32 bits = 160 bits = 20 bytes. As a 4-bit field, the maximum value is 15; this means that the maximum size of the IPv4 header is 15 × 32 bits = 480 bits = 60 bytes.

[**Differentiated Services Code Point**](https://en.wikipedia.org/wiki/Differentiated_Services_Code_Point)**(DSCP)**

Originally defined as the [type of service](https://en.wikipedia.org/wiki/Type_of_service) (ToS), this field specifies [differentiated services](https://en.wikipedia.org/wiki/Differentiated_services) (DiffServ) per RFC 2474.[[a]](https://en.wikipedia.org/wiki/Internet_Protocol_version_4#cite_note-36) Real-time data streaming makes use of the DSCP field. An example is [Voice over IP](https://en.wikipedia.org/wiki/Voice_over_IP) (VoIP), which is used for interactive voice services.

[**Explicit Congestion Notification**](https://en.wikipedia.org/wiki/Explicit_Congestion_Notification)**(ECN)**

This field is defined in RFC 3168 and allows end-to-end notification of [network congestion](https://en.wikipedia.org/wiki/Network_congestion) without [dropping packets](https://en.wikipedia.org/wiki/Packet_loss). ECN is an optional feature available when both endpoints support it and effective when also supported by the underlying network.

**Total Length**

This [16-bit](https://en.wikipedia.org/wiki/16-bit) field defines the entire packet size in bytes, including header and data. The minimum size is 20 bytes (header without data) and the maximum is 65,535 bytes. All hosts are required to be able to reassemble datagrams of size up to 576 bytes, but most modern hosts handle much larger packets. Links may impose further restrictions on the packet size, in which case datagrams must be [fragmented](https://en.wikipedia.org/wiki/IP_fragmentation). Fragmentation in IPv4 is performed in either the sending host or in routers. Reassembly is performed at the receiving host.

**Identification**

This field is an identification field and is primarily used for uniquely identifying the group of fragments of a single IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to help trace datagrams with spoofed source addresses,[[36]](https://en.wikipedia.org/wiki/Internet_Protocol_version_4#cite_note-37) but RFC 6864 now prohibits any such use.

**Flags**

A three-bit field follows and is used to control or identify fragments. They are (in order, from most significant to least significant):

* bit 0: Reserved; must be zero.
* bit 1: Don't Fragment (DF)
* bit 2: More Fragments (MF)

If the DF flag is set, and fragmentation is required to route the packet, then the packet is dropped. This can be used when sending packets to a host that does not have resources to perform reassembly of fragments. It can also be used for [path MTU discovery](https://en.wikipedia.org/wiki/Path_MTU_discovery), either automatically by the host IP software, or manually using diagnostic tools such as [ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)) or [traceroute](https://en.wikipedia.org/wiki/Traceroute).

For unfragmented packets, the MF flag is cleared. For fragmented packets, all fragments except the last have the MF flag set. The last fragment has a non-zero Fragment Offset field, differentiating it from an unfragmented packet.

**Fragment offset**

This field specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The fragmentation offset value for the first fragment is always 0. The field is 13 bits wide, so that the offset can be from 0 to 8191 (from (20  –1) to (213 – 1)). Fragments are specified in units of 8 bytes, which is why fragment length must be a multiple of 8.[[37]](https://en.wikipedia.org/wiki/Internet_Protocol_version_4#cite_note-39) Therefore, the 13-bit field allows a maximum offset of (213 – 1) × 8 = 65,528 bytes, with the header length included (65,528 + 20 = 65,548 bytes), supporting fragmentation of packets exceeding the maximum IP length of 65,535 bytes.

**Time to live (TTL)**

An eight-bit [time to live](https://en.wikipedia.org/wiki/Time_to_live) field limits a datagram's lifetime to prevent network failure in the event of a [routing loop](https://en.wikipedia.org/wiki/Routing_loop). It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In practice, the field is used as a [hop count](https://en.wikipedia.org/wiki/Hop_count)—when the datagram arrives at a [router](https://en.wikipedia.org/wiki/Router_(computing)), the router decrements the TTL field by one. When the TTL field hits zero, the router discards the packet and typically sends an [ICMP time exceeded](https://en.wikipedia.org/wiki/ICMP_time_exceeded) message to the sender.

The program *traceroute* sends messages with adjusted TTL values and uses these ICMP time exceeded messages to identify the routers traversed by packets from the source to the destination.

**Protocol**

This field defines the protocol used in the data portion of the IP datagram. IANA maintains a [list of IP protocol numbers](https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers) as directed by RFC 790.

**Header checksum**

The 16-bit [IPv4 header checksum](https://en.wikipedia.org/wiki/IPv4_header_checksum) field is used for error-checking of the header. When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet. Errors in the data field must be handled by the encapsulated protocol. Both [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) and [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) have separate checksums that apply to their data.

When a packet arrives at a router, the router decreases the TTL field in the header. Consequently, the router must calculate a new header checksum.

The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

**Source address**

This 32-bit field is the [IPv4 address](https://en.wikipedia.org/wiki/IPv4_address) of the sender of the packet. Note that this address may be changed in transit by a [network address translation](https://en.wikipedia.org/wiki/Network_address_translation) device.

**Destination address**

This 32-bit field is the [IPv4 address](https://en.wikipedia.org/wiki/IPv4_address) of the receiver of the packet. As with the source address, this may be changed in transit by a network address translation device.

address translation device.

**Options**

The [options field](https://en.wikipedia.org/wiki/Internet_Protocol_Options) is not often used. Packets containing [some options may be considered as dangerous](https://en.wikipedia.org/wiki/Internet_Protocol_Options_Considerations) by some routers and be blocked.[[38]](https://en.wikipedia.org/wiki/Internet_Protocol_version_4#cite_note-40) Note that the value in the IHL field must include enough extra 32-bit words to hold all the options plus any padding needed to ensure that the header contains an integer number of 32-bit words. If IHL is greater than 5 (i.e., it is from 6 to 15) it means that the options field is present and must be considered. The list of options may be terminated with an EOOL (End of Options List, 0x00) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header. The possible options that can be put in the header are as follows:

|  |  |  |
| --- | --- | --- |
| **Field** | **Size (bits)** | **Description** |
| Copied | 1 | Set to 1 if the options need to be copied into all fragments of a fragmented packet. |
| Option Class | 2 | A general options category. 0 is for *control* options, and 2 is for *debugging and measurement*. 1 and 3 are reserved. |
| Option Number | 5 | Specifies an option. |
| Option Length | 8 | Indicates the size of the entire option (including this field). This field may not exist for simple options. |
| Option Data | Variable | Option-specific data. This field may not exist for simple options. |

**Data**[[edit](https://en.wikipedia.org/w/index.php?title=Internet_Protocol_version_4&action=edit&section=16)]

The packet payload is not included in the checksum. Its contents are interpreted based on the value of the Protocol header field.

[List of IP protocol numbers](https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers) contains a complete list of payload protocol types. Some of the common payload protocols include:

|  |  |  |
| --- | --- | --- |
| **Protocol Number** | **Protocol Name** | **Abbreviation** |
| 1 | [Internet Control Message Protocol](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) | ICMP |
| 2 | [Internet Group Management Protocol](https://en.wikipedia.org/wiki/Internet_Group_Management_Protocol) | IGMP |
| 6 | [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) | TCP |
| 17 | [User Datagram Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) | UDP |
| 41 | [IPv6 encapsulation](https://en.wikipedia.org/wiki/IPv6#Tunneling) | ENCAP |
| 89 | [Open Shortest Path First](https://en.wikipedia.org/wiki/Open_Shortest_Path_First) | OSPF |
| 132 | [Stream Control Transmission Protocol](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) | SCTP |

## Ipv4 vs Ipv6

| **IPv4** | **IPv6** |
| --- | --- |
| Are more expensive (public ip address) because of smaller amount that is available. | Cheaper because of really big address space (everyone can have public ip address) |
| IPv4 has a 32-bit address length | IPv6 has a 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end-to-end, connection integrity is Achievable |
| It can generate 4.29×109 address space. That equals 2^32. | The address space of IPv6 is quite large it can produce 3.4×1038 address space. That equals 2^128. |
| The Security feature is dependent on the application | IPSEC is an inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation is performed only by the sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has a broadcast Message Transmission Scheme | In IPv6 multicast and anycast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has a header of 20-60 bytes. | IPv6 has a header of 40 bytes fixed |
| IPv4 can be converted to IPv6 | Not all IPv6 can be converted to IPv4 |
| IPv4 consists of 4 fields which are separated by addresses dot (.) | IPv6 consists of 8 fields, which are separated by a colon (:) |
| IPv4’s  IP addresses are divided into five different classes. Class A , Class B, Class C, Class Da , Class E. | IPv6 does not have any classes of the IP address. |
| IPv4 supports VLSM(Variable Length subnet mask). | IPv6 does not support VLSM. |
| Example of IPv4:  66.94.29.13 | Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB |

**Benefits of IPv6**

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

* **Larger Address Space:**IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
* **Improved Security:**IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
* **Simplified Header Format:**As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
* **Prioritize:**IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
* **Improved Support for Mobile Devices:**IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.