

# IP adresy

## Základní pojmy

IP adresa (Internet Protocol address) je numerický identifikátor přiřazený každému zařízení připojenému k počítačové síti, která používá Internet Protocol pro komunikaci. IP adresa slouží ke dvěma hlavním účelům: identifikaci hostitele nebo síťového rozhraní a adresování lokality v síti.

## Verze IP protokolu

### IPv4

IPv4 je čtvrtá verze Internet Protocolu a nejrozšířenější verze používaná v současnosti.

#### Formát

Skládá se ze 32 bitů (4 bajty) Zapisuje se jako čtyři dekadická čísla oddělená tečkami Každé číslo (oktet) může nabývat hodnot 0-255 Příklad: 192 . 168 . 1 . 1

#### Adresní prostor

Celkový počet adres:  $2^{32} = 4\,294\,967\,296$  adres Tento prostor je dnes považován za nedostatečný

#### Struktur IPv4 adresy

IPv4 adresa se skládá ze dvou částí:

Síťová část (Network ID) - identifikuje konkrétní síť Hostitelská část (Host ID) - identifikuje konkrétní zařízení v síti

### IPv6

IPv6 je novější verze Internet Protocolu vyvinutá jako odpověď na vyčerpávání IPv4 adres.

#### Formát

Skládá se ze 128 bitů (16 bajtů) Zapisuje se jako osm skupin po čtyřech hexadecimálních číslicích oddělených dvojtečkami Příklad: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

## Zkrácený zápis

Úvodní nuly ve skupině lze vynechat: 2001:db8:85a3:0:0:8a2e:370:7334 Posloupnost nulových skupin lze nahradit :: 2001:db8:85a3::8a2e:370:7334 :: Lze použít pouze jednou v adrese

## Adresní prostor

Celkový počet adres:  $2^{128} \approx 340$  undecilionů adres Tento prostor je prakticky nevyčerpatelný

## Třídy IPv4 adres

Původní systém dělení IPv4 adres do tříd (dnes již většinou nahrazen CIDR notací):

### Třída A

Rozsah: 1.0.0.0 - 126.255.255.255 První bit: 0 Síťová maska: 255.0.0.0 nebo /8 Počet sítí: 126 Počet hostitelů na síť: 16 777 214

### Třída B

Rozsah: 128.0.0.0 - 191.255.255.255 První dva bity: 10 Síťová maska: 255.255.0.0 nebo /16 Počet sítí: 16 384 Počet hostitelů na síť: 65 534

### Třída C

Rozsah: 192.0.0.0 - 223.255.255.255 První tři bity: 110 Síťová maska: 255.255.255.0 nebo /24 Počet sítí: 2 097 152 Počet hostitelů na síť: 254

### Třída D (Multicast)

Rozsah: 224.0.0.0 - 239.255.255.255 První čtyři bity: 1110 Používá se pro multicastové přenosy

### Třída E (Experimentální)

Rozsah: 240.0.0.0 - 255.255.255.255 První čtyři bity: 1111 Rezervováno pro experimentální účely

# Speciální IP adresy

## Privátní IP adresy (RFC 1918)

Tyto adresy jsou určeny pro použití v lokálních sítích a nejsou routovatelné na veřejném internetu:

Třída A: 10.0.0.0 - 10.255.255.255 (/8) Třída B: 172.16.0.0 - 172.31.255.255 (/12) Třída C: 192.168.0.0 - 192.168.255.255 (/16)

## Loopback adresa

IPv4: 127.0.0.1 (celý rozsah 127.0.0.0/8) IPv6: ::1 Používá se pro komunikaci v rámci stejného zařízení Také známá jako „localhost“

## Adresa nenastaveného rozhraní

IPv4: 0.0.0.0 IPv6: :: Používá se při konfiguraci nebo jako zástupný symbol

## Broadcast adresa

IPv4: 255.255.255.255 (omezený broadcast) Nebo poslední adresa v síti (směřovaný broadcast) Používá se pro zasílání paketů všem zařízením v síti

## Link-Local adresy

IPv4: 169.254.0.0 - 169.254.255.255 (/16) IPv6: fe80::/10 Automaticky přiřazené při nedostupnosti DHCP Platné pouze v lokálním segmentu sítě

## Dokumentační adresy

Vyhrazené pro dokumentaci a příklady:

192.0.2.0/24 (TEST-NET-1) 198.51.100.0/24 (TEST-NET-2) 203.0.113.0/24 (TEST-NET-3)  
2001:db8::/32 (IPv6 dokumentace)

## Carrier-Grade NAT

100.64.0.0 - 100.127.255.255 (/10) RFC 6598 Sdílené adresní prostory pro poskytovatele

# Síťové masky a CIDR

## Síťová maska (Subnet Mask)

Síťová maska určuje, která část IP adresy reprezentuje síť a která hostitele.

### Formát

Zapisuje se stejně jako IP adresa (např. 255.255.255.0) Binárně obsahuje nepřerušenu sekvenci jedniček následovanou nulami Jednička označuje síťovou část, nula hostitelskou část

### Příklady

255.0.0.0 - 8 bitů pro síť 255.255.0.0 - 16 bitů pro síť 255.255.255.0 - 24 bitů pro síť 255.255.255.128 - 25 bitů pro síť

## CIDR notace

CIDR (Classless Inter-Domain Routing) je modernější způsob zápisu síťových masek.

### Formát

Zápis: IP\_adresa/počet\_bitů\_síťové\_části Příklad: 192.168.1.0/24 Číslo za lomítkem udává počet bitů síťové masky

### Převodní tabulka

CIDR	Maska	Počet IP adres	Počet použitelných IP
/8	255.0.0.0	16 777 216	16 777 214
/16	255.255.0.0	65 536	65 534
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	2*
/32	255.255.255.255	1	1

\* RFC 3021 umožňuje použití /31 pro point-to-point spoje

# Subnetting

Subnetting je proces dělení většího síťového segmentu na menší podsítě.

## Důvody pro subnetting

Efektivnější využití adresního prostoru  
Zlepšení výkonu sítě (menší broadcast domény)  
Zvýšení bezpečnosti (izolace segmentů)  
Snadnější správa

## Příklad subnettingu

Mějme síť 192.168.1.0/24 (256 adres) a chceme ji rozdělit na 4 podsítě:

Nová maska: /26 (255.255.255.192) Každá podsít: 64 adres (62 použitelných)

Podsítě:

192.168.1.0/26 (0-63) 192.168.1.64/26 (64-127) 192.168.1.128/26 (128-191)  
192.168.1.192/26 (192-255)

## Síťová a broadcastová adresa

V každé podsíti jsou dvě speciální adresy:

Síťová adresa - první adresa (všechny hostitelské bity = 0)  
Broadcastová adresa - poslední adresa (všechny hostitelské bity = 1)  
Tyto adresy nelze přiřadit hostitelům

## Přidělování IP adres

### Statické přiřazení

Adresa je nakonfigurována ručně administrátorem  
Zůstává stejná po restartu  
Vhodné pro servery, tiskárny, síťové zařízení

### Dynamické přiřazení (DHCP)

DHCP (Dynamic Host Configuration Protocol) automaticky přiřazuje IP adresy zařízením v síti.

### Výhody DHCP

Automatická konfigurace  
Centralizovaná správa  
Efektivní využití adres (recyklace)  
Snadná změna

konfigurace

## **DHCP proces (DORA)**

Discovery - klient hledá DHCP server Offer - server nabídne konfiguraci Request - klient požádá o nabízenou konfiguraci Acknowledgment - server potvrdí přidělení

## **DHCP lease**

IP adresa je přidělena na omezenou dobu (lease time) Klient musí lease obnovovat Po vypršení se adresa vrací do fondu

## **NAT (Network Address Translation)**

NAT umožňuje více zařízením sdílet jednu veřejnou IP adresu.

### **Typy NAT**

#### **Static NAT**

Pevné mapování 1:1 mezi soukromou a veřejnou adresou Používá se pro servery, které musí být dostupné z internetu

#### **Dynamic NAT**

Mapování ze soukromých adres do fondu veřejných adres Přiřazení není pevné

#### **PAT (Port Address Translation) / NAT Overload**

Nejběžnější forma NAT Mnoho soukromých adres → jedna veřejná adresa Rozlišení pomocí portových čísel Používá se v domácích routerech

### **Výhody NAT**

Šetří veřejné IPv4 adresy Poskytuje určitou úroveň zabezpečení (skrývá vnitřní strukturu) Umožňuje změnu ISP bez změny vnitřních adres

### **Nevýhody NAT**

Porušuje end-to-end princip internetu Komplikuje některé aplikace (VoIP, P2P) Přidává latenci Ztěžuje trasování a diagnostiku

## Port Forwarding

Port forwarding umožňuje přístup k zařízení za NATem z internetu.

Mapování specifického portu veřejné IP na interní IP a port Příklad: veřejná\_IP:80 → 192.168.1.10:8080 Nutné pro servery, hry, vzdálený přístup

## DNS (Domain Name System)

DNS překládá doménová jména na IP adresy.

### Základní principy

Hierarchický, distribuovaný databázový systém Převádí lidsky čitelná jména ([www.example.com](http://www.example.com)) na IP adresy Funguje na portu 53 (UDP/TCP)

### DNS záznamy

A záznam - mapování doménového jména na IPv4 adresu AAAA záznam - mapování doménového jména na IPv6 adresu PTR záznam - reverzní DNS (IP → jméno) CNAME - alias (kanonické jméno) MX - mail server pro doménu NS - name server pro doménu TXT - textové informace (SPF, DKIM, atd.)

### DNS hierarchie

Root servery (.) TLD servery (.com, .org, .cz) Autoritativní servery (konkrétní domény) Rekurzivní resolvers (cache, dotazování)

## Routing

Routing je proces výběru cesty pro síťová data od zdroje k cíli.

### Routovací tabulka

Každé síťové zařízení má routovací tabulku obsahující:

Cílovou síť - kam mají pakety směřovat Síťovou masku - maska cílové sítě Gateway - IP adresa dalšího skoku (next hop) Interface - síťové rozhraní pro výstup Metriku - priorita cesty (nižší = lepší)

## Typy routování

### Statické routování

Cesty jsou nakonfigurovány ručně administrátorem Nemění se automaticky Vhodné pro malé, stabilní sítě

### Dynamické routování

Routery si automaticky vyměňují informace o topologii Přizpůsobují se změnám v síti Používají routovací protokoly

## Routovací protokoly

### IGP (Interior Gateway Protocol)

Protokoly pro routing uvnitř autonomního systému:

RIP (Routing Information Protocol) - distance vector, max 15 hopů OSPF (Open Shortest Path First) - link state, rychlejší konvergence EIGRP (Enhanced Interior Gateway Routing Protocol) - Cisco proprietární

### EGP (Exterior Gateway Protocol)

Protokoly pro routing mezi autonomními systémy:

BGP (Border Gateway Protocol) - de facto standard pro internet

## Default Gateway

IP adresa routeru, který odesílá pakety mimo lokální síť Používá se, když není známa specifická cesta k cíli Typicky router připojující lokální síť k internetu

## ARP (Address Resolution Protocol)

ARP překládá IP adresy na MAC adresy (hardwarové adresy) v lokální síti.

## Jak ARP funguje

Zařízení potřebuje komunikovat s IP adresou v lokální síti Odešle ARP request broadcast: „Kdo má IP adresu X.X.X.X?“ Zařízení s danou IP odpoví ARP reply se svou MAC adresou Odesílatel uloží mapování

do ARP cache

## ARP cache

Dočasná tabulka mapování IP → MAC Snižuje množství ARP requestů Záznamy mají omezenou životnost (typicky minuty)

## RARP a další varianty

RARP (Reverse ARP) - MAC → IP (zastaralé) Gratuitous ARP - oznámení vlastní IP/MAC Proxy ARP - router odpovídá za jiné zařízení ARP spoofing - bezpečnostní útok (man-in-the-middle)

## ICMP (Internet Control Message Protocol)

ICMP je používán pro diagnostiku a hlášení chyb v IP sítích.

## ICMP zprávy

### Běžné typy zpráv

Echo Request/Reply (Type 8/0) - ping Destination Unreachable (Type 3) - cíl nedostupný Time Exceeded (Type 11) - TTL vypršelo (traceroute) Redirect (Type 5) - lepší cesta k cíli Source Quench (Type 4) - zpomalení odesílání

## Ping

Nástroj pro testování dosažitelnosti hostitele Odesílá ICMP Echo Request, očekává Echo Reply Měří RTT (Round-Trip Time)

```
ping 8.8.8.8
ping www.example.com
```

## Traceroute

Zobrazuje cestu paketů k cíli Využívá postupně se zvyšující TTL (Time To Live) Každý router snižuje TTL a vrací ICMP Time Exceeded

```
traceroute www.example.com # Linux/Mac
tracert www.example.com # Windows
```

# TTL (Time To Live)

TTL je pole v IP hlavičce omezující životnost paketu v síti.

## Účel

Prevence nekonečných smyček Každý router snižuje TTL o 1 Při dosažení 0 je paket zahozen Router vrací ICMP Time Exceeded

## Typické hodnoty

Linux: 64 Windows: 128 Cisco/síťová zařízení: 255

## Použití

Traceroute/tracert Identifikace operačního systému (OS fingerprinting) Omezení šíření multicastu

# Fragmentace IP paketů

Fragmentace je proces rozdělení velkých IP paketů na menší části.

## MTU (Maximum Transmission Unit)

Maximální velikost paketu, který může síťové rozhraní přenést Ethernet: typicky 1500 bajtů Různé sítě mohou mít různé MTU

## Path MTU Discovery

Proces zjišťování minimálního MTU na cestě k cíli Používá IP flag „Don't Fragment“ (DF) Pokud je paket příliš velký, router vrací ICMP Fragmentation Needed

## Fragmentace

Pokud DF není nastaven, router může paket fragmentovat Každý fragment má vlastní IP hlavičku Defragmentace probíhá až u cílového hostitele Ztráta jednoho fragmentu = ztráta celého paketu

# Bezpečnost IP adres

## IP Spoofing

Falšování zdrojové IP adresy v paketu Používá se při DDoS útocích Obrana: ingress/egress filtering (BCP 38)

## DDoS útoky

SYN flood - zahlcení pololetými TCP spojeními UDP flood - zahlcení UDP pakety ICMP flood (ping flood) - zahlcení ICMP požadavky DNS amplification - zneužití DNS serverů

## Port Scanning

Zjišťování otevřených portů na cílovém systému Nástroje: nmap, masscan Může být přípravou na útok

## Firewall

Síťové zabezpečení kontrolující příchozí a odchozí provoz:

Packet filtering - filtrování na základě IP, portů, protokolů Stateful inspection - sledování stavu spojení Application layer - kontrola na úrovni aplikací

## VPN (Virtual Private Network)

Šifrované tunelové spojení přes veřejnou síť:

Site-to-Site VPN - propojení sítí Remote Access VPN - připojení jednotlivých uživatelů Protokoly: IPsec, OpenVPN, WireGuard, L2TP, PPTP

## Geolokace IP adres

Geolokace umožňuje určit přibližnou fyzickou polohu IP adresy.

## Jak to funguje

Databáze mapující IP rozsahy na lokace Data od RIR (Regional Internet Registries) Data od ISP Crowdsourcované měření

## Přesnost

Země: 95-99% přesnost Město: 50-80% přesnost Přesná adresa: obvykle nemožné Horší přesnost u mobilních sítí a VPN

## Služby

MaxMind GeoIP IP2Location GeoLite2 IPinfo.io

## IPv4 vyčerpání a přechod na IPv6

### IPv4 vyčerpání

IANA přidělila poslední bloky RIR v únoru 2011 Regionální registry postupně vyčerpaly své zásoby RIPE NCC (Evropa) vyčerpána od listopadu 2019 ARIN (Severní Amerika) vyčerpána od září 2015

### Řešení nedostatku IPv4

NAT - sdílení jedné veřejné adresy CIDR - efektivnější přidělování adres Recyklace - zpětné použití nepoužívaných bloků IPv4 trading - obchodování s IPv4 bloky Přechod na IPv6 - dlouhodobé řešení

### Přechod na IPv6

#### Mechanismy přechodu

Dual Stack - zařízení má současně IPv4 i IPv6 Tunneling - zapouzdření IPv6 do IPv4 (6to4, Teredo) Translation - NAT64/DNS64 překlad mezi IPv4 a IPv6

#### Stav adopce

Globální adopce: cca 40-45% (2025) Varies by country: Indie >70%, USA >50%, EU cca 30-40% Velké služby (Google, Facebook) plně podporují IPv6

#### Výhody IPv6

Obrovský adresní prostor Zjednodušená hlavička paketu Zabudovaný IPsec (bezpečnost) Eliminace nutnosti NAT Lepší podpora mobility Autoconfiguration (SLAAC)

## RIR (Regional Internet Registries)

RIR jsou organizace odpovědné za přidělování IP adres v určitých regionech.

### Pět RIR

ARIN - Severní Amerika RIPE NCC - Evropa, Střední východ, část Asie APNIC - Asie a Tichomoří LACNIC - Latinská Amerika a Karibik AFRINIC - Afrika

### Hierarchie přidělování

IANA (Internet Assigned Numbers Authority) - globální koordinace RIR - regionální přidělování LIR (Local Internet Registry) - ISP, velké organizace End users - koneční uživatelé

## WHOIS

WHOIS je protokol pro dotazování na informace o IP adresách a doménách.

### Informace v WHOIS

Vlastník IP bloku nebo domény Kontaktní informace Datum registrace a expirace Name servery Status domény

### Použití

```
whois 8.8.8.8
whois example.com
```

### RDAP (Registration Data Access Protocol)

Modernější alternativa k WHOIS Strukturované JSON odpovědi Lepší internacionalizace Autentizace a autorizace

## Multicast a Anycast

### Unicast

Jeden odesílatel → jeden příjemce Standardní model komunikace Každý paket má jednu cílovou adresu

## Broadcast

Jeden odesílatel → všichni v síti IPv4: broadcastová adresa síť IPv6: broadcast neexistuje (nahrazen multicastem)

## Multicast

Jeden odesílatel → skupina příjemců Efektivní pro streaming, videokonference IPv4: 224.0.0.0/4 (třída D) IPv6: ff00::/8 Vyžaduje podporu v routerech (IGMP, PIM)

## Anycast

Více zařízení sdílí stejnou IP adresu Paket je doručen „nejbližšímu“ zařízení Používá se pro DNS root servery, CDN Zlepšuje redundanci a latenci

## Quality of Service (QoS)

QoS označuje mechanismy pro prioritizaci síťového provozu.

### Důvody pro QoS

Omezená šířka pásma Různé nároky aplikací (VoIP vs. email) Prevence zahlcení sítě

### Metody QoS

Classification - identifikace typu provozu Marking - označení paketů (DSCP, CoS) Queuing - fronty s různými prioritami Policing - omezení přenosové rychlosti Shaping - vyhlazení datového toku

### DSCP (Differentiated Services Code Point)

6-bitové pole v IP hlavičce Umožňuje až 64 různých tříd provozu Běžné hodnoty: EF (Expedited Forwarding), AF (Assured Forwarding)

## IP v kontextu OSI modelu

OSI model je koncepční rámec pro pochopení síťové komunikace.

## Vrstvy OSI modelu

Fyzická vrstva - přenos bitů (kabely, rádiové vlny) Linková vrstva - lokální síťové adresování (MAC, Ethernet) Síťová vrstva - ← IP je zde (routování, logické adresování) Transportní vrstva - TCP, UDP (segmentace, řízení toku) Relační vrstva - správa relací Prezentační vrstva - formátování dat, šifrování Aplikační vrstva - HTTP, FTP, SMTP

## TCP/IP model

Jednodušší, praktičtější model:

Link Layer - fyzická a linková vrstva Internet Layer - ← IP je zde (IP, ICMP, ARP) Transport Layer - TCP, UDP Application Layer - HTTP, DNS, SSH, atd.

From:

<https://serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

[https://serviceit.cz/doku.php?id=ip\\_adresa](https://serviceit.cz/doku.php?id=ip_adresa)

Last update: **2026/01/05 04:54**

