ftp-21, ssh-22, telnet 23, smtp-25, dns-53, dhpc-bootp-server-67 klient 68, http-80, pop3-110,

sftp-115, https-443, smtps ssl- 465, imaps ssl-993, pop3s ssl-995,

Internetové protokoly	[skrýt]
Aplikační vrstva	BitTorrent • DNS • BOOTP • DHCP • FTP • HTTP • HTTPS • IMAP • IRC • Ident • NNTP • NFS • NTP • POP3 • RTP • SIP • SMB • SMTP • SNMP • SSH • STUN • Telnet • Websphere MQ • XMPP
Relační vrstva	SPDY • SSL • NetBIOS • RPC • SMB • NFS
Transportní vrstva	DCCP • IL • RUDP • SCTP • TCP • UDP
Síťová vrstva	IPv4 • IPv6 • ICMP • IGMP • ARP • Proxy ARP • RARP
Linková vrstva	Ethernet • FDDI • PPP • Token ring • Wi-Fi
Fyzická vrstva	10Base2 • 10Base-T • EIA-422 • EIA-485 • RS-232 • RS-449

$192.168.0.1_{10}$ desitkova-dekadická , $11000000\ 10101000\ 00000000\ 00000001_2$ dvojková-binární

4 oktávy oddělené tečkami

192_{10} - odspodu 11000000_2 . 168_{10} - 10101000_2 . 0_{10} - 00000000_2 . 1_{10} - 00000001

192/2=96	0	168/2=84	0
92/2=48	0	84/2=42	0
48/2=24	0	42/2=21	0
24/2=12	0	21/2=10	1
12/2=6	0	10/2=5	0
6/2=3	0	5/2=2	1
3/2=1	1	2/2=1	0
1/2=0	1	1/2=0	1

z desitkove do dvojkove

$1^7 1^6 0^5 0^4 0^3 0^2 0^1 0^0$	$1x2^7 + 1x2^6$	128+64=192
$1^7 0^6 1^5 0^4 1^3 0^2 0^1 0^0$	$1x2^7 + 1x2^5 + 1x2^3$	128+32+8=168
$0^7 0^6 0^5 0^4 0^3 0^2 0^1 0^0$	$0x2^7=0$	0
$0^7 0^6 0^5 0^4 0^3 0^2 0^1 1^0$	$1x2^0=1$	1

z dvojkove do desitkove

255_{10} - 11111111_2 , 0_{10} – 00000000_2 , 1_{10} - 00000001_2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

2^8 – 256 max 255 u IP a prakticky 254, 255 je broadcast pro všechny,

Určení třídy IP adresy vezmu první číslo IP např. 192, převedu na 2kovou a zapíšu si počet 1ček v prvních 4 bitech, tudíž 192 je 1100000000, 4 bity 1100, mam 110 třída C.

c	určující bity	rozsah adres	maska	CIDR maska	poznámka
class A	0xxx	0 - 127.x.x.x	255.0.0.0	/8	hlavní
class B	10xx	128 - 191.x.x.x	255.255.0.0	/16	hlavní
class C	110x	192 - 223.x.x.x	255.255.255.0	/24	hlavní
class D	1110	224 - 239.x.x.x			multicast
class E	1111	240 - 255.x.x.x			rezervováno

Fyzická vrstva
Vrstva č. 1, anglicky physical layer. Specifikuje fyzickou komunikaci. Aktivuje, udržuje a deaktivuje fyzické spoje (např. komutovaný spoj) mezi koncovými systémy. Fyzické spojení může být dvoubodové (sériová linka) nebo mnohobodové (Ethernet). Fyzická vrstva definuje všechny elektrické a fyzikální vlastnosti zařízení. Obsahuje rozložení pinů, napěťové úrovně a specifikuje vlastnosti kabelů; stanovuje způsob přenosu "jedniček a nul". Huby, opakovače, síťové adaptéry a hostitelské adaptéry (Host Bus Adapters používané v síťových úložištích SAN) jsou právě zařízení pracující na této vrstvě. Hlavní funkce poskytované fyzickou vrstvou jsou: Navazování a ukončování spojení s komunikačním médiem. Spolupráce na efektivním rozložení všech zdrojů mezi všechny uživatele. Modulace neboli konverze digitálních dat na signály používané přenosovým médiem (a zpět) (A/D, D/A převodníky).

Linková (spojová)
Vrstva č. 2, anglicky data link layer. Poskytuje spojení mezi dvěma sousedními systémy. Uspořádává data z fyzické vrstvy do logických celků známých jako rámce (frames). Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby. Formátuje fyzické rámce, opatřuje je fyzickou adresou a poskytuje synchronizaci pro fyzickou vrstvu. Datová vrstva poskytuje funkce k přenosu dat mezi jednotlivými síťovými jednotkami a detekuje případně opravuje chyby vzniklé na fyzické vrstvě. Nejlepším příkladem je Ethernet. Na lokálních sítích založených na IEEE 802 a některých na IEEE 802 sítích jako je FDDI, by tato vrstva měla být rozdělena na vrstvu řízení přístupu k médiu (Medium Access Control, MAC) a vrstvu IEEE 802.2 logické řízení linek (Logical Link Control, LLC). Na této vrstvě pracují veškeré mosty a přepínače. Poskytuje propojení pouze mezi místně připojenými zařízeními a tak vytváří doménu na druhé vrstvě pro směrové a všesměrové vysílání.

Síťová vrstva
Vrstva č. 3, anglicky network layer. Tato vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Síťová vrstva poskytuje funkce k zajištění přenosu dat různé délky od zdroje k příjemci skrze jednu případně několik vzájemně propojených sítí při zachování kvality služby, kterou požaduje přenosová vrstva. Síťová vrstva poskytuje směrovací funkce a také reportuje o problémech při doručování dat. Veškeré směrovače pracují na této vrstvě a posílají data do jiných sítí. Zde se již pracuje s hierarchickou strukturou adres. Nejznámější protokol pracující na 3. vrstvě je Internetový Protokol (IP). Jednotkou informace je paket.

Transportní vrstva
Vrstva č. 4, anglicky transport layer. Tato vrstva zajišťuje přenos dat mezi koncovými uzly. Jejím účelem je poskytnout takovou kvalitu přenosu, jakou požadují vyšší vrstvy. Vrstva nabízí spojově (TCP) a nespojově orientované (UDP) protokoly. TCP – Zajišťuje přenos dat se zárukami, který vyžadují aplikace, kde nesmí „chybět ani paket“. Jedná se o přenosy souborů, e-mailů, WWW stránek atd. Záruka se vztahuje na řešení ztrát přenášených paketů, zachování jejich pořadí a odstranění duplikace. Jednotkou posílané informace je na této vrstvě TCP segment. UDP – Zajišťuje přenos dat bez záruk, který využívají aplikace, u kterých by bylo na obtíž zdržení (delay) v síti způsobené čekáním na přenos všech paketů a ztráty se dají řešit jiným způsobem (např. snížení kvality, opakování dotazu). Využívá se pro DNS, VoIP, streamované video, internetová rádia, vyhledávání sdílených souborů v rámci sítě DC++, on-line hry atp.

Relační vrstva
Vrstva č. 5, anglicky session layer. Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamovaní výjimečných stavů. Do této vrstvy se řadí: NetBIOS, RPC. K paketům přiřazuje synchronizační značky, které využije v případě vrácení paket (např. z důvodu, že se během přenosu dat poškodí síť) k poskládání původního pořadí.

Prezentační vrstva
Vrstva č. 6, anglicky presentation layer. Funkcí vrstvy je transformovat data do tvaru, který používají aplikace (šifrování, konvertování, komprimace). Formát dat (datové struktury) se může lišit na obou komunikujících systémech, navíc dochází k transformaci pro účel přenosu dat nižšími vrstvami. Mezi funkce patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů a pod. Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační. Příklady protokolů: SMB (Samba).

Aplikační vrstva
Související informace naleznete také v článku Aplikační vrstva.
Vrstva č. 7, anglicky application layer. Účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci. Do této vrstvy se řadí například tyto služby a protokoly: FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP.

OSI Model

vrstva	jméno	jednotka	funkce vrstvy	příklad
L7	Application	Data	Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikaci.	HTTP, DNS
L6	Presentation	Data	Reprezentace dat a šifrování. Řeší rozdíly v reprezentaci dat mezi aplikací a síťovým formátem - kóduje data pro přenos.	SSL, MPEG
L5	Session	Data	Spojení mezi aplikacemi, správa session. Komunikace jedné aplikace s druhou, posílání více dat po sobě. Udržuje celé spojení mezi dvěma počítači.	NetBIOS
L4	Transport	Segments	End-to-end spojení systémů, spolehlivost - zajišťuje kompletní přenos dat, kvalita služby. Řeší spolehlivé odeslání všech dat ze zdroje do cíle pomocí segmentace a potvrzování.	TCP, UDP
L3	Network	Packets	Logická adresace - routování - určení cesty paketu, přenos dat z bodu do bodu, používá IP adresy, fragmentace. Komunikace mezi zdrojovým a cílovým zařízením pomocí IP adresy.	IP, ICMP, OSPF
L2	Data Link	Frames	Fyzická adresace, MAC - media access control a LLC - logical link control, datový tok, synchronizace rámců, komunikace 1 hop, používá MAC adresy. Detekce chyb, řízení toku a přístupu na médium. Komunikace mezi dvěma zařízeními v jednom subnetu (nebo na bránu) pomocí MAC adresy. Vytváří rámce (hlavička + data + zápatí).	Ethernet, 802.1q, PPP, ARP
L1	Physical	Bits	Fyzické parametry linky - média (kabely, rádio, světlo), signály a binární přenos. Řeší fyzické poslání dat (přenášeným bitům nepřiřazuje žádný význam).	100BaseT, 802.11g

TCP/IP Model

vrstva	jméno	příklad
L4	Application	SSL, HTTP, DNS
L3	Transport	TCP, UDP
L2	Internet	IP, ICMP, OSPF
L1	Link	Ethernet, ARP

síť	adresa sítě	broadcast adresa	adresy uzlů
10.0.0.0/8	10.0.0.0	10.255.255.255	10.0.0.1 - 10.255.255.254
192.168.0.0/16	192.168.0.0	192.168.255.255	192.168.0.1 - 192.168.255.254
172.16.0.0/12	172.16.0.0	172.31.255.255	172.16.0.1 - 172.31.255.254

Některé adresy z veřejných i privátních mají od začátku plánovaný speciální význam. Z těch důležitějších se jedná o rozsah 127.0.0.0/8 , což jsou localhost loopback adresy či 169.254.0.0/16 , to jsou adresy pro autokonfiguraci (APIPA).

c	určující bity	rozsah adres	maska	CIDR maska	poznámka
class A	0xxx	0 - 127.x.x.x	255.0.0.0	/8	hlavní
class B	10xx	128 - 191.x.x.x	255.255.0.0	/16	hlavní
class C	110x	192 - 223.x.x.x	255.255.255.0	/24	hlavní
class D	1110	224 - 239.x.x.x			multicast
class E	1111	240 - 255.x.x.x			rezervováno

Později se ukázalo, že toto pevné rozdělení sítí je neefektivní a velice plýtvá adresami, které začaly ubývat.
Tak vznikl síťový design označovaný jako ***classless***. Ten využívá ***Variable Length Subnet Mask*** (VLSM), které povoluje proměnnou délku síťové masky. Na VLSM je založen ***Classless Inter-Domain Routing*** (CIDR), který dovoluje libovolně dlouhou masku a používá zkrácený zápis pomocí počtu jedničkových bitů v masce (délka masky). CIDR zápis adresy vypadá například 10.5.0.2/28 , tomu odpovídá tradiční maska 255.255.255.240 , kterou zapíšeme binárně

11111111.11111111.11111111.11110000 .

CIDR také obsahuje mechanismus agregace, který dovoluje spojit několik spojitých síťových rozsahů do jednoho supernetu. Použití agregace šetří místo a prostředky při routování. Použitím agregace můžeme spojit subnety 192.168.0.0/24 a 192.168.1.0/24 do 192.168.0.0/23 .

Výpočet maximálního počtu uzlů a podsítí

Maximální počet uzlů a subnetů v určité síti je určen pomocí masky podsítě. Určení, která část IP adresy je částí sítě a která částí hostů, je jednoduché. Když si IP adresu i masku zapíšeme binárně pod sebe, tak tam, kde jsou v masce jedničky, je část síťová a kde nuly část adresy uzlu v rámci subnetu. Jednoduché je to u nejběžnějších masek, kdy v oktetu jsou buď jen jedničky, tedy hodnota 255, nebo nuly.

IP adresa	10.240.5.8	**00001010.11110000.00000101**.00001000
maska	255.255.255.0	**11111111.11111111.11111111**.00000000

Když máme masku v CIDR zápisu, tak rovnou víme počet jedniček a počet nul můžeme dopočítat 32 – CIDR hodnota . Síťová část je dána jedničkami v masce sítě, pokud v této části IP adresy změníme nějakou hodnotu, dostaneme jiný subnet. Takže počet kombinací v této části adresy se rovná maximálnímu **počtu subnetů**. Počet kombinací spočítáme jako $2^{\text{počet jedniček}}$.

Ve starších dobách se nesměli používat subnety, které měli v adrese samé jedničky nebo nuly (to určovalo staré RFC 950), takže podle této normy by počet subnetů byl $2^{\text{počet jedniček}} - 2$. Již dlouho ale platí novější RFC 1812, kde můžeme využít všechny adresy. Celkový počet subnetů také záleží na tom, jestli přihlížíme k síťovým třídám, potom počítám počet subnetů v dané síťové třídě, tedy $2^{\text{počet jedniček v masce – počet jedniček ve třídě}}$.

Maximální počet **adres pro uzly** spočítáme obdobně pomocí vzorce $2^{\text{počet nul}} - 2$. Dvojku odečítáme, protože jako adresu uzlu nemůžeme použít network id a broadcast adresu.

Uvedeme si nyní jednoduchý konkrétní příklad, na kterém snad bude dřívější obecný popis jasně pochopitelný. Máme síťovou adresu zapsanou pomocí CIDR 148.25.3.5/22 . Takže počet jedniček v masce je 22 a počet nul je 32 - 22 = 10 . Pokud budeme uvažovat třídy, tak tato adresa spadá do třídy B (podle prvních dvou bitů IP adresy, první oktet je binárně 10010100) a její maska je /16. Počet subnetů v rámci třídy B s maskou /22 je $2^{22-16} = 2^6 = 64$. Pokud bychom brali veškeré subnety, tak je to $2^{22} = 4\ 194\ 304$. Počet hostů, který může být v každém subnetu s touto maskou sítě, je $2^{10} - 2 = 1024 - 2 = 1022$.

Jsou dvě adresy ze stejného subnetu?

Občas potřebujeme určit, zda se dvě adresy (které známe včetně masky) nachází ve stejném subnetu (podle toho probíhá komunikace apod.). Pokud máme jednoduchou masku, tak to poznáme na první pohled, ale u některých složitějších musíme použít základní matematiku. Stačí porovnat síťové části adres a pokud jsou stejné, patří adresy do stejné podsítě. Nejjednodušší je převést všechny adresy do binární formy a vše je hned patrné. Důležitým předpokladem je, aby masky podsítí byly shodné.

Příklad si ukážeme na adresách 192.168.5.13/22 a 192.168.7.128/22 , hned vidíme, že masky jsou stejné.

dekadicky	binárně
192.168.5.13	**11000000.10101000.00000**101.00001101
192.168.7.128	**11000000.10101000.00000**111.10000000
255.255.252.0	**11111111.11111111.111111**00.00000000

Ze zápisu vidíme části IP adres určených jedničkami v masce a jednoduše porovnáme, že jsou obě stejné, tudíž patří obě adresy do stejné sítě.

Nalezení Network ID

Nalezení první adresy podsítě se může zdát jednoduché, ale někdy to na první pohled vidět není. Pak musíme použít logiku nebo matematiku. Network ID se dá vypočítat z binárního zápisu adresy a masky, kdy se provede bitové AND, networ-ID = IP-adresa AND subnet-mask.

Příklad pro adresu 10.217.123.7/20

IP binárně	00001010.11011001.01111011.00000111
maska binárně	11111111.11111111.11110000.00000000
operace AND	00001010.11011001.01110000.00000000
dekadicky	10.217.112.0

Funkce AND znamená násobení 0*1 je 0, 1*1 je 1, zapíšu jako operace AND

Nalezení broadcast adresy

Broadcastovou adresu subnetu nalezneme podobně jako network ID. Matematicky můžeme použít bitové OR mezi IP adresou a negovanou maskou, tedy broadcast-adresa = IP-adresa OR NOT(subnet-mask). Příklad pro stejnou adresu jako minule 10.217.123.7/20 .

IP binárně	00001010.11011001.01111011.00000111
maska binárně	11111111.11111111.11110000.00000000
negace masky	00000000.00000000.00001111.11111111
operace OR	00001010.11011001.01111111.11111111
dekadicky	**10.217.127.255**

Jiná možnost výpočtu je, když známe network ID, pak stačí do části uzlů v binárním tvaru zadat samé jedničky.

Tzn. Spočítám network ID a do řádku operace AND vložím jedničky podle počtu nul v masce, tzn. v /20 bude posledních 12 bitů 1.

Jiné výpočty

Otázky na to, co chceme spočítat mohou být různé, ale vše vychází z předchozích úvah. Například chceme najít masku podsítě, aby se v ní nacházel zadaný počet adres. Převedeme počet adres na binární hodnotu, z toho dostaneme jak dlouhá je část uzlů a doplněk je maska podsítě. Tedy například subnet pro 4000 klientů, binárně 1111.10100000 , to je délka 12 , maska je dlouhá 32 – 12 = 20 . Subnet /20 může obsahovat až 4094 adres uzlů.

Jiný příklad může být, když chceme rozdělit síť na určitý počet stejných subnetů. Vezmeme hodnotu počtu subnetů, odečteme 1 (protože nabývá hodnot 0 až n-1), převedeme na binární hodnotu, ta musí obsahovat samé jedničky, jinak není možno dosáhnout tohoto počtu subnetů. Pokud počítáme v rámci nějaké třídy, tak připočteme masku třídy a máme cílovou masku jednoho subnetu, kterých může vzniknout zadaný počet.

Například síť 192.168.100.0/24 v rámci třídy C rozdělit na 8 stejných podsítí. 8 – 1 = 7 binárně 111 , v rámci třídy C máme masku 24 + 3 = 27 , takže možné subnety jsou 192.168.100.0/27, 192.168.100.32/27, 192.168.100.64/27, 192.168.100.96/27, 192.168.100.128/27, 192.168.100.160/27, 192.168.100.192/27, 192.168.100.224/27.

Kalkulačky
Pro výpočty různých hodnot okolo adresování se používají kalkulačky IP podsítí (IP subnet calculator). Takových aplikací nalezneme celou řadu a velká část jich je online na internetu. Příkladem je ***subnet-calculator.samuraj-cz.com*** .