1 Sítě na bázi IP a jejich bezpečnost(1/2)

1.1 Úvod

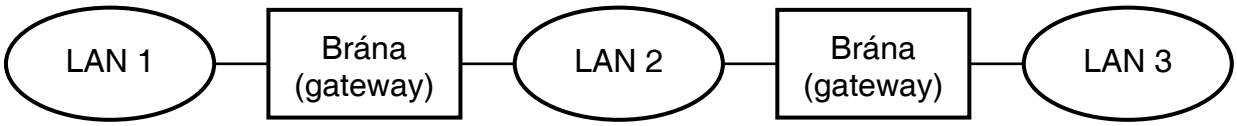
- Služby Internetu - aplikační služby
  - Elektronická pošta, přenos souborů (TFTP, FTP), vzdálené terminály (telnet, ssh), informační služby (HTTP, Gopher, ...) a mnoho dalších.
- Služby komunikační vrstvy - z uživatelského pohledu jsou podstatné:
  - Služba bezkanálového zasílání paketů.
    Protokol UDP (= User Datagram Protocol)
  - Služba spolehlivého spojení.
    Protokol TCP (= Transmission Control Protocol)
- Charakteristiky Internetového TCP/IP
  - Nezávislost na technologii lokálních sítí a jejich propojování, potvrzování mezi koncovými účastníky spojení
  - Standardizované aplikační protokoly nezávislé na hardwarových i softwarových platformách

ISO-OSI síťový model

- OSI = Open System Interconnect, model o 7 vrstvách

Aplikační vrstva	např. FTP nebo TELNET
Prezentační vrstva	Síťové API
Komunikační vrstva	Pravidla pro komunikační spojení mezi dvěma počítači
Transportní vrstva	Pravidla pro zasílání paketů
Síťová vrstva	Pravidla pro HW adresování
Linková vrstva	Pravidla pro časový multiplex paketů
Fyzická vrstva	Kabel

- Základní vlastnosti Internetu
  - Každý stroj má svoji jednoznačnou identifikaci: tzv. IP adresu
  - Chování aplikací a programátorského rozhraní nezávisí na technologii lokální sítě
- Základní architektura Internetu (i internetů)



  - Brány (gateways) a směrovače (routers) propojují fyzické lokální sítě
  - Brány mají informaci o strojích na lokálních sítích, které propojují
  - Směrovače posílají pakety na základě informace o cílové síti, nikoliv o cílovém stroji
  - IP protokoly považují všechny sítě za rovnocenné bez ohledu na jejich fyzickou technologii

Protokol IPv4 se používá v Internetu od roku 1982. IPv5 byl experimentální protokol. Vsoučasnosti se začíná s přípravou na IPv6.

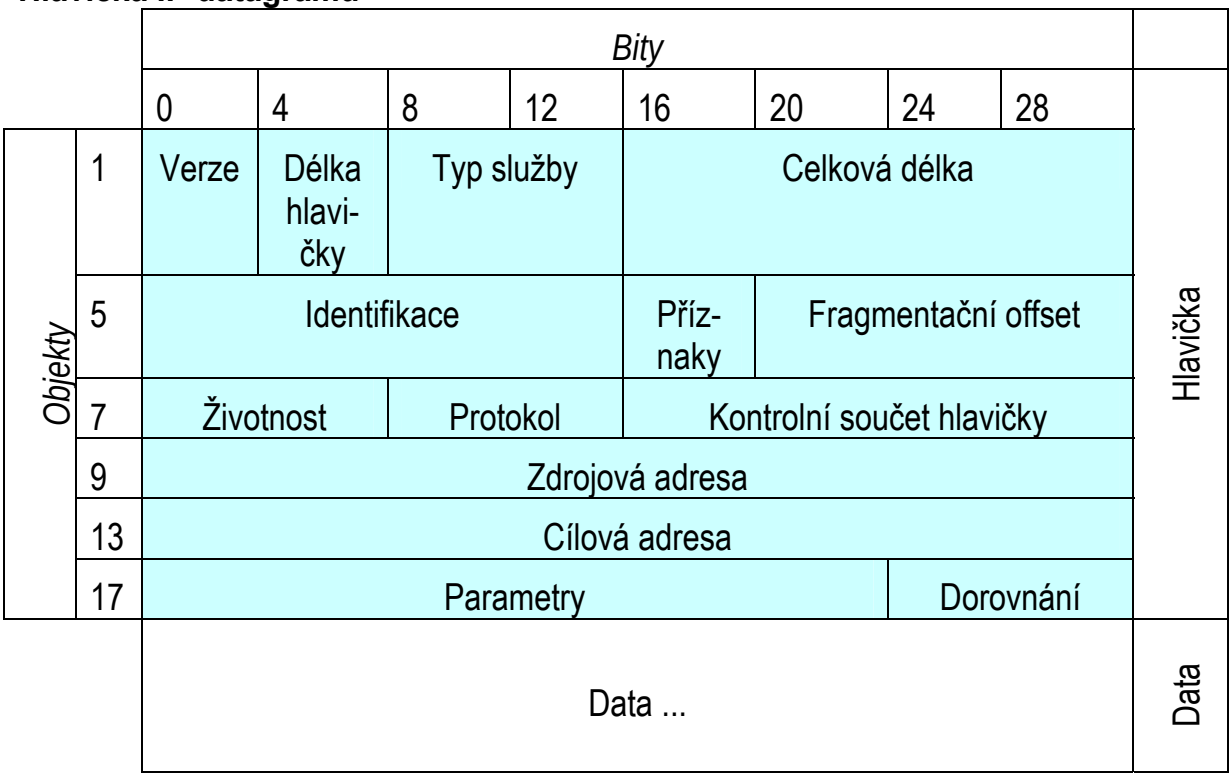
1.2 IPv4 - Internet Protocol Version 4

Data jsou přenášena v blocích znaků - datagramech, nebo paketech. Každý paket obsahuje hlavičku, identifikující odesílatele a požadovaného adresáta. Za hlavičkou následuje blok dat - obsah paketu.

Jakmile pakety dosáhnou cíle, složí se zpět na souvislý blok dat; tento proces rozkládání a skládání je pro uživatele obvykle neviditelný. Protože z jednoho systému na druhý obvykle existuje několik různých tras, může každý paket od odesílatele k

adresátu putovat jinou cestou. Protože Internet přepíná pakety místo vytváření komunikačních okruhů, říká se mu síť s přepínáním paketů.

Hlavička IP datagramu



Hlavnĺ způsoby spojení protokolem IP:

- Obě stanice jsou připojeny ke stejné lokální síti (obvykle Ethernet, dříve i Token Ring). Internetové pakety se zapouzdřují do paketů používaných na lokální síti. Současně s přenosem IP lze přenášet i jiné protokoly (IPX, AppleTalk)
- Dva počítače přímo propojeny sériovou linkou, IP pakety se posílají protokolem SLIP (Serial Line Internet Protocol), CSLIP (CompressedSLIP) nebo PPP (Point-to-Point Protocol). Lze tak propojit i lokální sítě.
- IP pakety zapouzdřeny do paketů jiných síťových protokolů, např. do paketů Frame Relay, ATM (Asynchronous Transfer Mode), aj.

1.3 IPv6 - Internet Protocol Version 6, IPng (Next Generation)

IPv6 vzniklo jako reakce na nedostatky a problémy IPv4. Nejvýznamnější cíle, které si jeho autoři stanovili, byly:

- dostatečně bohatý adresní prostor - pokud možno by už nikdy neměla nastat nouze o adresy
- podpora služeb se zaručenou kvalitou
- design odpovídající vysokorychlostním sítím
- bezpečnostní mechanismy přímo v IP
- podpora mobilních zařízení
- automatická konfigurace
- kooperace s IPv4 a co nejhladší přechod ze stávajícího protokolu na nový

Hlavním motorem IPv6 byl původně nedostatek adres. Jenže jak běžel čas, hledala se (a nacházela) řešení i na bázi klasického IPv4. Vzniklo beztřídní přidělování adres, mechanismy pro nahrazení celé lokální sítě jedinou adresou (NAT, zvaný též IP maškaráda).

Také pro ostatní z výše uvedených cílů se začínají objevovat řešení v IPv4. S postupujícím časem se asi nejzávažnějším argumentem ve prospěch IPv6 stává podpora mobilních počítačů[1], která je zde vyřešena podstatně lépe, než v jeho předchůdci.

IPng rozšiřuje adresu z 32 na 128 bitů, zavádí víceúrovňové adresační hierarchie a jednoduchou autokonfiguraci adres[2].

---

[1] Současně s ní se vrací problém s nedostatkem adres. Počet mobilních zařízení utěšeně roste a berličky pro snížení počtu konzumovaných adres (jako například NAT) se pro ně používají jen obtížně. Právě přenosná zařízení totiž často vyžadují čisté spojení mezi oběma komunikujícími konci.

[2] Mechanismy pro dynamické přečíslování zařízení. Hlavním prvkem tohoto mechanismu je schopnost zařízení mít na jednom interface přiřazeno několik adres. IPv6 adresy, které jsou přiřazeny mohou být označeny jako platné, nedoporučené nebo neplatné. Adresa se stane nedoporučenou, jestliže byla interface přiřazena nová adresa. Po nějakou dobu poté, co byla interface přidělena adresa poračuje příjem a odesílání paketů z nedoporučené adresy, což umožní aby byl dosavadní traffic v pořádku ukončen. Nakonec se z nedoporučené adresy stane neplatná a platná adresa je použita pro veškerý traffic.

Mění se IP hlavička, některá pole se vypuštějí, jiná mění. Zavádí se typ adresy „Cluster address" pro identifikaci topologických regionů.

Přechod z IPv4 na IPv6 bude inkrementální. Existující zařízení budou upgradovány na podporu IPv6 a budou dále používat IPv4 adresu, nova zařízení budou již s podporou IPv6.

Blíže[3] viz http://www.cesnet.cz/ipv6/

1.4 Adresace IPv4

Každé rozhraní připojené na IP síť má přidělenu jednoznačnou 32-bitovou adresu, formálně zapisovanou jako čtveřice 8-bitových oktetů (147.32.80.9).

Teoreticky umožňuje 32-bitová adresa 2^{32} = 4 294 967 296 různých IP adres, prakticky je využitelný počet podstatně nižší vzhledem ke způsobu, jakým se adresy přidělují – po blocích adres.

Internet je tvořen z řady malých lokálních sítí, každá má své číslo:

a) „Klasická" čísla sítí se určovala jako pevně daný bitový prefix IP adresy všech hostů na síti. Tímto řešením se adresový prostor rozpadl na přesně známý počet sítí s různou velikostí, bohužel i se skupinami nevyužívaných IP adres hostů.

b) CIDR (Classless Inter Domain Routing).

c) Protokol IPv6. Tento nový protokol nabízí větší adresový prostor pro čísla sítí a hostů a vyšší úroveň bezpečnosti. V protokolu IPv6 jsou adresy dlouhé 128 bitů.

[3] Sdružení Cesnet propojilo v 11/2002 svou síť Cesnet2 se sítí společnosti 6COM, přičemž toto propojení je jako první na území ČR uskutečněno prostřednictvím protokolu IPv6. Společnost 6Com sídlí na Slovensku a zabývá se vývojem IPv6 aplikací.

1.4.1 Třídy adres IPv4

V „klasickém" adresačním schématu existuje pět základních typů IP adres. Prvních několik bitů adresy (nejvyznamnější btty) urcuje, do které třídy adresa patří. Zbývající bity pak tvoří adresu sítě a adresu hosta.

Adresy třídy A mají podobu *N.a.b.c*, kde *N* je adresa sítě a *a.b.c* adresa počítače; nejvyšší bit *N* musí být nulový. Sítí třídy A není mnoho, jsou neefektivní (16 777 216 adres na síť). Vlastní je průkopníci Internetu, například MIT.

Adresy třídy B mají formát *N.M.a.b*, kde *N.M* je číslo sítě a *a.b* číslo počítače. Dva nejvýznamnější bity čísla N musí být 10.

Adresy třídy C mají formát *N.M.O.a*, kde *N.M.O* je číslo sítě a *a* je číslo počítače; nejvyšší bity čísla /V musejí být 110.

Adresy třídy D mají formát *N.M.O.a*, kde nejvyšší čtyři bity *N* jsou 1110. Nejedná se vlastně o adresy sítí, jsou to takzvané multicast skupiny. Paket zasílán skupině hostů či sítí. Takové skupina adresátů je asociovaná s adresou třídy D a každý z členů skupiny přijímá pakety skupině adresované. Samostatnou otázkou je routování.

Some Common Multicast Group Addresses

Group Address	Description
224.0.0.1	All multicast-aware hosts (including routers) on the local network
224.0.0.2	All multicast routers on the local network
224.0.0.4	DVMR protocol updates
224.0.1.1	Network Time Protocol updates
224.0.1.24	Microsoft's WINS locator service

Adresa třídy E má podobu N.M.O.P, kde nejvyšší čtyři bity N jsou 1111. Tyto adresy jsou rezervovány pro experimentální účely.

IP Classes

Class	First 4 bits	# Network Bits	# Host Bits	Network Number
A	0xxx	7	24	1 to 127
B	10xx	14	16	128 to 191
C	110x	21	8	192 to 223
D	1110	28	Multicast	224 to 239

IP Addresses					
Class	**Maximum # of Networks**	**Maximum # of Hosts**	**Address Range**	**Network Address**	**Host Address**
A	128	16,777,214	1.*.*.* to 127.*.*.*	a	b.c.d
B	16,384	65,534	128.*.*.* to 191.*.*.*	a.b	c.d
C	2,097,152	254	192.*.*.* to 223.*.*.*	a.b.c	d

Adresy **Network** a **Broadcast** jsou rezervovány a nepoužívají se jako host adresy. Adresa sítě má (dle masky) část adresy příslušející hostu nulovou, např. 128.146.116.0. Adresa Broadcast má hodnoty 1 ve všech bitech části adresy příslušející hostu, např. 128.146.116.255. Starší verze SunOS (4.X) používaly pro broadcast adresu s 0, tj. 128.146.116.0. Všechny systémy Sun přijímají broadcasts v obou variantách.

Adresa **loopback**, 127.0.0.1, odkazuje na interní interface hosta používaný hostem pro zasílání paketů sám sobě. Obvykle je v unixových systémech značen jako interface **lo0**.

Příklady adres IPv4

Příklad 1 - Třída C, 256 adres:		
Network address:	192.168.24.0	11000000.10101000.00011000.00000000
Netmask:	255.255.255.0	11111111.11111111.11111111.00000000
Host address od:	192.168.24.0	11000000.10101000.00011000.00000000
do:	192.168.24.255	11000000.10101000.00011000.11111111
Příklad 2 – polovina třídy C, 128 adres:		
Network address:	192.168.24.128	11000000.10101000.00011000.10000000
Netmask:	255.255.255.128	11111111.11111111.11111111.10000000
Host address od:	192.168.24.128	11000000.10101000.00011000.10000000
do:	192.168.24.255	11000000.10101000.00011000.11111111
Příklad 3 – šestnáctina třídy C, 16 adres:		
Network address:	192.168.24.16	11000000.10101000.00011000.00010000
Netmask:	255.255.255.240	11111111.11111111.11111111.11110000
Host address od:	192.168.24.16	11000000.10101000.00011000.00010000
do:	192.168.24.31	11000000.10101000.00011000.00011111
Příklad 4 – šestnáctina třídy C, 16 adres:		
Network address:	192.168.24.0	11000000.10101000.00011000.00000000
Netmask:	255.255.255.240	11111111.11111111.11111111.11110000
Host address od:	192.168.24.0	11000000.10101000.00011000.00000000
do:	192.168.24.15	11000000.10101000.00011000.00001111

Alternativně lze masku zapisovat jako počet bitů adresy platných pro určení sítě, tj. "192.168.0.16/28" je totéž jako "192.168.0.16 netmask 255.255.255.240" (viz počet červených bitů v příkladě tři a čtyři).

Privátní podsítě

Existují tři adresy sítí, rezervované pro privátní adresy:

10.0.0.0/8, **172.16.0.0/12**, and **192.168.0.0/16**.

Jejich využití je pro privátní sítě izolované od Internetu fyzicky či NAT routerem. Internetové routery nikdy neforwardují pakety pocházející z privátních adres.

Blíže viz RFC 1918, např. http://www.faqs.org/rfcs/rfc1918.html

1.4.2 Adresování CIDR – Classlesss InterDomain Routing

CIDR adresy neobsahují třídy, namísto tohojsou sítě defínovány jako *k* nejvýznamnějších bitů každé adresy, zbývajících *32 - k* bitů pak tvoří adresu hosta.

Příklad:

Poskytovatel síťových dostal přidělenu adresu s fixními prvními dvanácti bity (adresa sítě), zbývajících 20 bitů pak tvoří adresu hosta. Poskytovatel tak může svým zákazníkům přidělit 2^{20} různých adres.

Navíc se adresa hosta dále dělí na podsítě. Prvních j bitů adresy hosta má pevnou hodnotu, zbývající bity pak představují adresu hosta na podsíti. I tuto adresu je možno dále dělit na podsítě.

Adresy ve formátu CIDR tedy vypadají takto: k.j.l.(m..n), kde každá část má proměnnou délku. Takže náš poskytovatel může svůj adresový prostor rozdělit na 1024 podsítí, pro každého zákazníka jednu. Každý zákazník pak má k dispozici 2^{10} adres hostů, které může dále dělit na lokální podsítě.

Zavedení mechanismu CIDR současně pomohlo řešit i jeden další naléhavý problém - neúměrně rostoucí objem směrovacích informací, které musí distribuovány po celém Internetu, a které si musí pamatovat každý směrovač. Díky CIDR blokům je možné objem těchto informací velmi významně snížit, ovšem za cenu toho, že IP adresy se stanou závislé na konkrétním poskytovateli připojení (v zásadě si lze představit, že Internet provider, který současně musí být i IP registry), dostane přidělen celý CIDR blok adres. Z něj pak "vykrajuje" menší CIDR bloku a ty přiděluje svým zákazníkům, ovšem detailní informace o tomto "vykrojení" již nemusí šířit do světa, ale ponechává si je pouze u sebe).

1.5 Jména hostů

Informace o jménech hostů viz RFC 1122 a RFC 1123.

Původní unixovské systémy používaly k uložení adres jednotlivých počítačů soubor /etc/hosts. Řada systémů používá tento soubor dodnes k uložení adres počítačů na interní podnikové síti.

```
# /etc/hosts
192.42.0.1 server
192.42.0.2 art
192.42.0.3 science sci
```

Počítač *art* má adresu 192.42.0.2. Jméno *sci* uvedené za jménem *science* znamená, že *sci* je možno použít jako druhé jméno, alias, počítače *science*.

Počátkem 80. let vzrostl počet počítačů na Internetu z tisíců na desítky tisíc a více. Správa jediného souboru s adresami a jmény všech počítačů se brzy ukázala neproveditelná. Namísto toho se na Intemetu zavedl distribuovaný systém jmen, známý jako Domain Name System (DNS).

1.6 Pakety a protokoly

Základní protokoly:

- **ICMP Internet Control Message Protocol.** Tento protokol zajišťuje nízkoúrovňové operace protokolu IP. Těchto operací je několik druhů, příkladem může být výměna směrovacích informací apod.
- **TCP Transmission Control Protocol.** Tento protokol slouží k vytvoření dvousměrného proudového spojení mezi dvěma počítači. Jedná se o „spojovaný" protokol, který implementuje funkce timeoutu a opakování přenosu, aby zajistil spolehlivé doručení informací.

- **UDP User Datagram Protocol**. Tento protokol slouží k posílání paketů z jednoho hosta na druhý a je „nespojovaný" – nezajišťuje doručení.
- **IGMP[4] Internet Group Management Protocol.** Tento protokol slouží k řízení hromadného vysílání - záměrného směrování paketů na více než jeden počítač. Multicast je základem činnosti např. intemetových multimediálních páteří,

1.6.1 ICMP

Protokol ICMP slouží k výměně nízkoúrovňových informací o činnosti sítě mezi hosty a branami. Například pakety ICMP Echo se běžně používají k testování síťového spojení. Typ paketu ICMP je urcen 8-bitovým typovým údajem.

Příklady typů paketů ICMP

Typový údaj	Popis typu ICMP
0	Echo Reply (používáno programem ping)
3	Destination Unreachable
5	Redirect (změna trasy)
8	Echo Request (používáno programem ping)
9	Router Advertisement
10	Router Solicitatíon

Pomocí podvržených paketů ICMP těchto typů může útočník přesměrovat provoz vaší sítě nebo může realizovat útok typu zablokování služby.

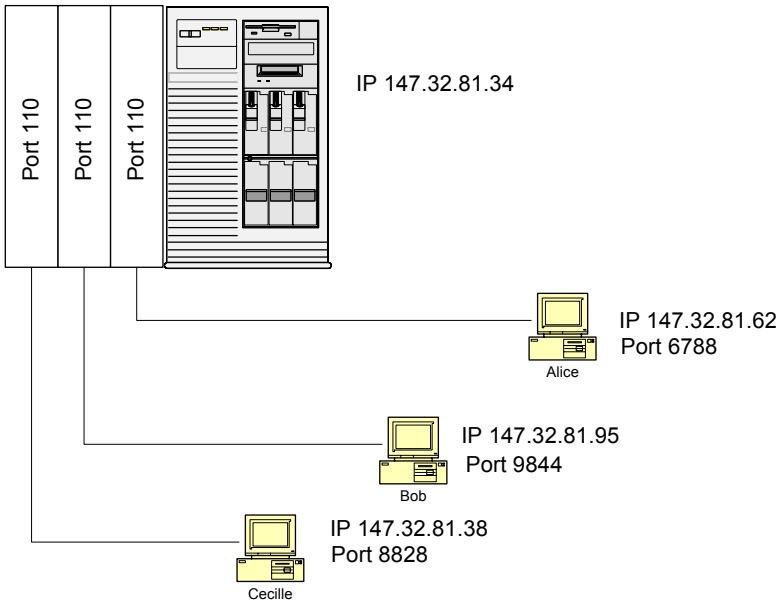
[4] Some networks don't provide any form of group addressing at all (Point-to-point networks). On such networks, a bridge or router must monitor the LAN side of the network for multicast packets and then forward any matching frames to the remote devices. This function is served by **IGMP (Internet Group Management Protocol)** version 2, which provides a set of simple "join" and "leave" messages. Whenever an end system wants to begin watching for specific multicast traffic, it will issue an IGMP join message, which the upstream device will see. Similarly, when the system wants to stop receiving traffic for a specific multicast group address, it can issue a leave message and the gateway will stop forwarding that traffic. In addition, routers will periodically search for active group memberships.

1.6.2 TCP

TCP zajišťuje spolehlivý, řízený, obousměmý datový tok mezi dvěma programy. Je zaručeno, že každý odeslaný bajt bude dopraven k adresátovi (anebo budete uvědoměni, že se přenos nezdařil) a že k cíli dorazi ve stejném pořadí, v jakém byly odeslány.

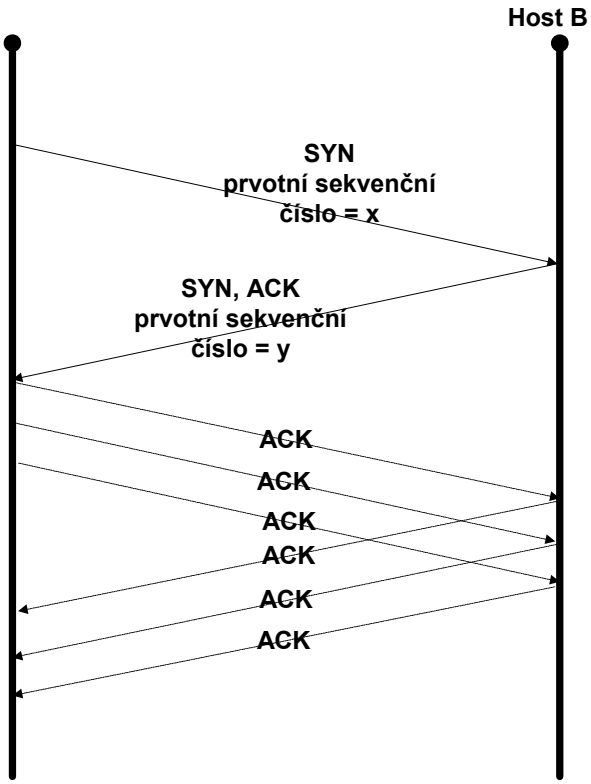
Pokud dojde k fyzickému přerušení spojení a nepodaří se nalézt alternativní trasu, pak implementace protokolu TCP pošle procesu, který se snaží přijímat nebo odesílat data, chybové hlášení.

Každé TCP spojení má na každém konci přidělen jeden port. Porty jsou určeny 16-bitovým číslem. Každé momentální spojení na celém Internetu je tedy vždy jednoznačně popsáno jednou dvojicí 32-bitových čísel a jednou dvojicí 16-bitových čísel:

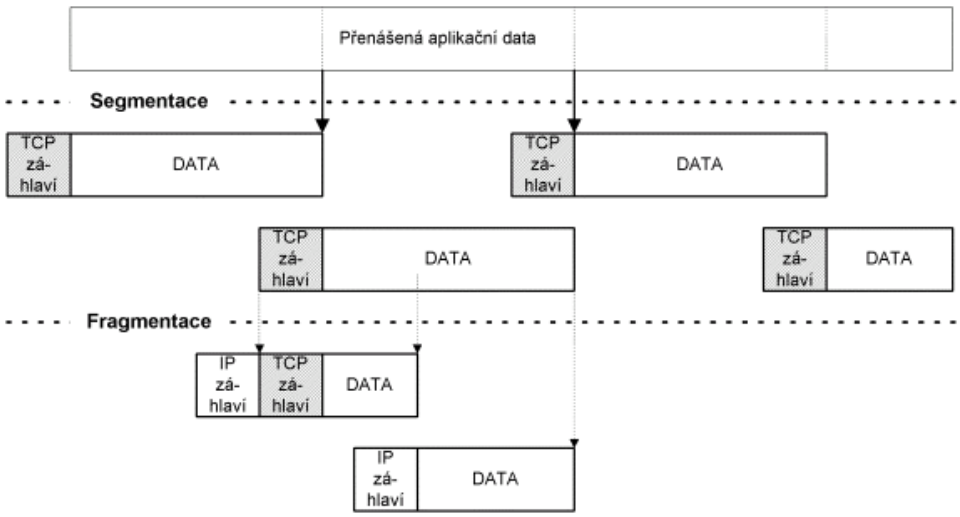


Připojení všech tří stanic na port 110 může být matoucí. Nicméně se stále jedná o tři různá spojení, protože každé z nich vychází z jiného páru host-port a server převede každé spojení na zvláštní port s vyšším číslem.

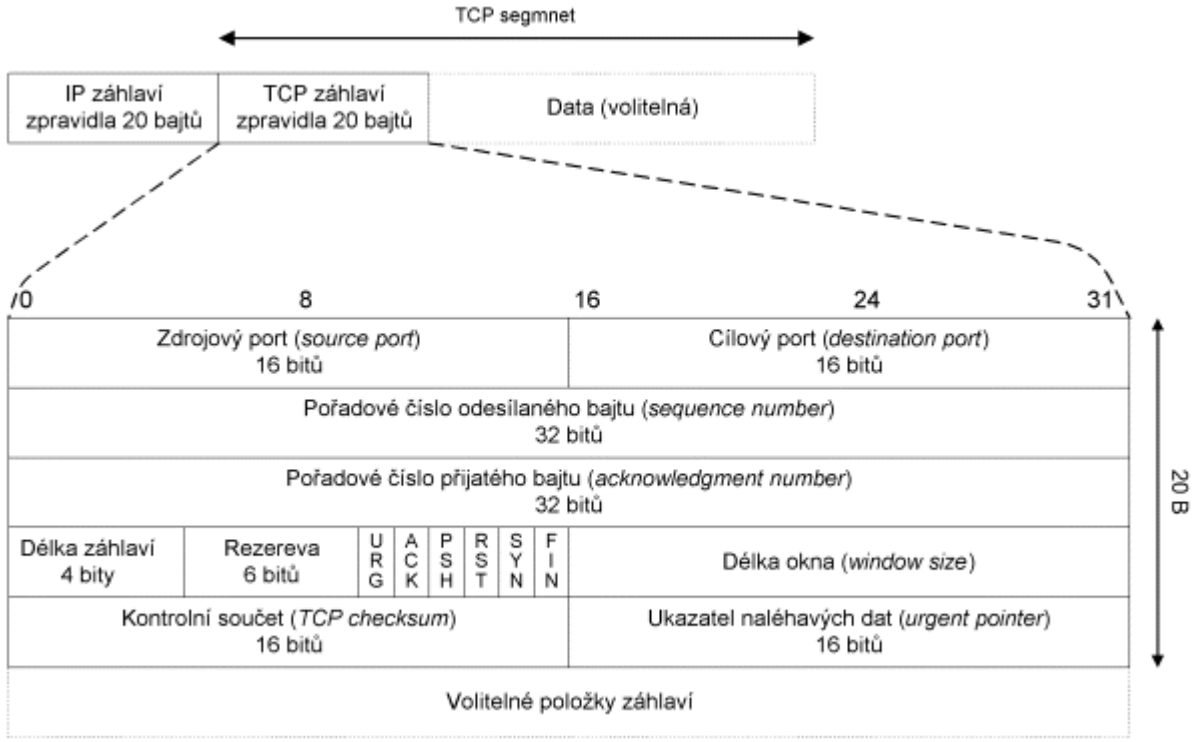
Protokol TCP používá v hlavičce paketu dva speciální bity, SYN a ACK, které slouží k vytváření nového spojení. Pň otevírání TCP spojení odesílá žadatel paket, v němž je nastaven bit SYN, ale není nastaven bit ACK.
Druhý host potvrdí navázání spojení paketem, který má nastaveny oba bity - SYN i ACK. Nakonec žadatel odešle třetí paket, v němž je nastaven bit ACK, ale není nastaven bit SYN. Tomuto procesu se říká třícestný handshake. Když budeme vyhledávat pakety s nenastaveným bitem ACK, můžeme snadno rozeznat požadavky na nove spojení od paketů, které se posílají v rámci již existujícího spojení. Toto rozlišení může být důležité při vytváření fíltračních firewallů.



Základní jednotkou přenosu v protokolu TCP je TCP segment, který se vkládá do IP-datagramu a ten do linkového rámce. Použije-li se příliš velký TCP-segment, který je vetší než maximální velikost přenášeného linkového rámce (MTU), pak IP protokol musí provést fragmentaci IP-datagramu.



TCP segment



Zdrojový port (*source port*) je port odesilatele TCP segmentu

Cílový port (*destination port*) je portem adresáta TCP segmentu.

Pořadové číslo odesílaného bajtu je pořadové číslo prvního bajtu TCP segmentu v toku dat od odesílatele k příjemci (TCP segment nese bajty od **pořadového čísla odesílaného bajtu** až do délky segmentu). Tok dat v opačném směru má samostatné (jiné) číslování svých dat. Jelikož pořadové číslo odesílaného bajtu je 32 bitů dlouhé, tak po dosažení hodnoty 2^{32}-1 nabude cyklicky opět hodnoty 0. Číslování obecně nezačíná od nuly (ani od nějaké určené konstanty), ale číslování by mělo začínat od náhodně zvoleného čísla. Vždy když je nastaven příznak SYN, tak operační systém odesilatele začíná znovu číslovat, tj. vygeneruje startovací pořadové číslo odesílaného bajtu, tzv. ISN (*Initial Sequence Number).*

Naopak **pořadové číslo přijatého bajtu** vyjadřuje číslo následujícího bajtu, který je příjemce připraven přijmout, tj. příjemce potvrzuje, že správně přijal vše až do pořadového čísla přijatého bajtu mínus jedna.

Délka záhlaví vyjadřuje délku záhlaví TCP segmentu v násobcích 32 bitů (4 bajtů) - podobně jako u IP-záhlaví.

Délka okna vyjadřuje přírůstek pořadového čísla přijatého bajtu, který bude příjemcem ještě akceptován (viz kapitola 9.7).

Ukazatel naléhavých dat může být nastaven pouze v případě, že je nastaven příznak URG. Přičte-li se tento ukazatel k pořadovému číslu odesílaného bajtu, pak ukazuje na konec úseku naléhavý dat. Odesilatel si přeje, aby příjemce tato naléhavá data přednostně zpracoval. Tento mechanismus používá např. protokol Telnet.

V poli příznaků mohou být nastaveny následující příznaky:

- **URG** – TCP segment nese naléhavá data.
- **ACK** – TCP segment má platné pole “Pořadové číslo přijatého bajtu” (nastaven ve všech segmentech, kromě prvního segmentu, kterým klient navazuje spojení).
- **PSH** – Zpravidla se používá k signalizaci, že TCP segment nese aplikační data, příjemce má tato data předávat aplikaci. Použití tohoto příznaku není ustáleno.
- **RST – Odmítnutí TCP spojení.**
- **SYN** – Odesílatel začíná s novou sekvencí číslování, tj. TCP segment nese pořadové číslo prvního odesílaného bajtu (ISN).
- **FIN** – odesilatel ukončil odesílání dat. Jelikož protokol TCP vytváří plně duplexní spojení, tak příznak FIN způsobí jen uzavření přenosu dat v jednom směru. V tomto směru už dále nebudou odesílány TCP segmenty obsahující příznak PSH (nepočítaje v to případné opakovaní přenosu).

V dalším textu budeme kombinaci nastavených příznaků zapisovat podle prvních písmen z názvu příznaku. Pokud je příznak nenastaven, pak místo něj napíšeme tečku. Např. skutečnost, že TCP segment má nastaven příznaky ACK a FIN a ostatní příznaky nenastaveny zapíšeme: .A…F .

Kontrolní součet IP-záhlaví se počítá pouze ze samotného IP-záhlaví. Z hlediska zabezpečení integrity přenášených dat je důležitý kontrolní součet v záhlaví TCP-segmentu počítaný i z přenášených dat, i z některých položek IP-záhlaví. Kontrolní součet vyžaduje sudý počet bajtů, proto v případě lichého počtu se data fiktivně doplní jedním bajtem na konci.

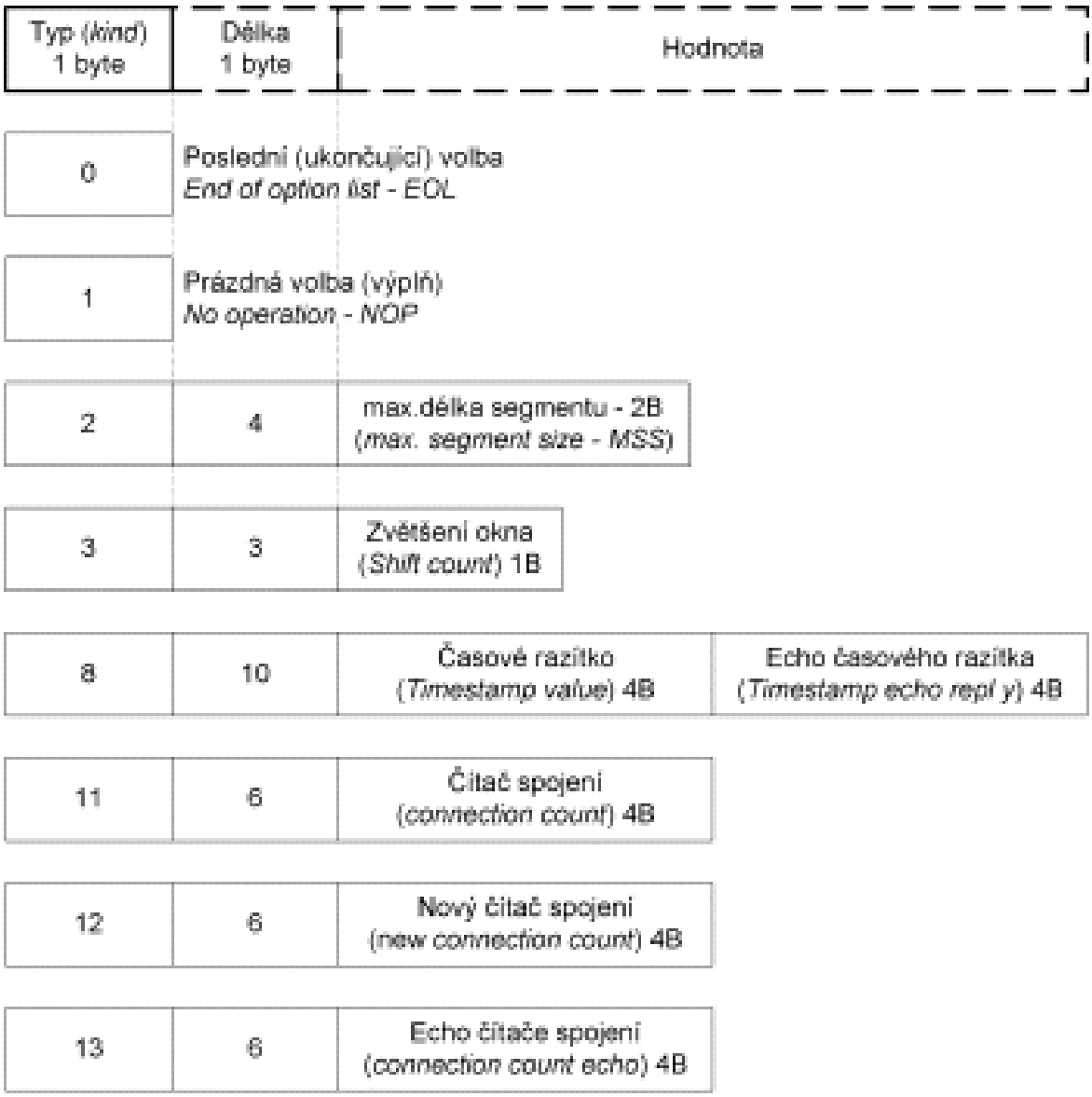
IP a TCP záhlaví

Volitelné položky TCP záhlaví

Povinné položky TCP záhlaví tvoří 20B. Za povinnými položkami následují volitelné položky, nejvýše 40 bajtů.

Volitelná položka se skládá z typu volitelné položky, délky volitelné položky a hodnoty. Délka TCP záhlaví musí být dělitelná čtyřmi. V případě, že délka záhlaví by nebyla dělitelná čtyřmi, pak se záhlaví doplňuje prázdnou volitelnou položkou – NOP.

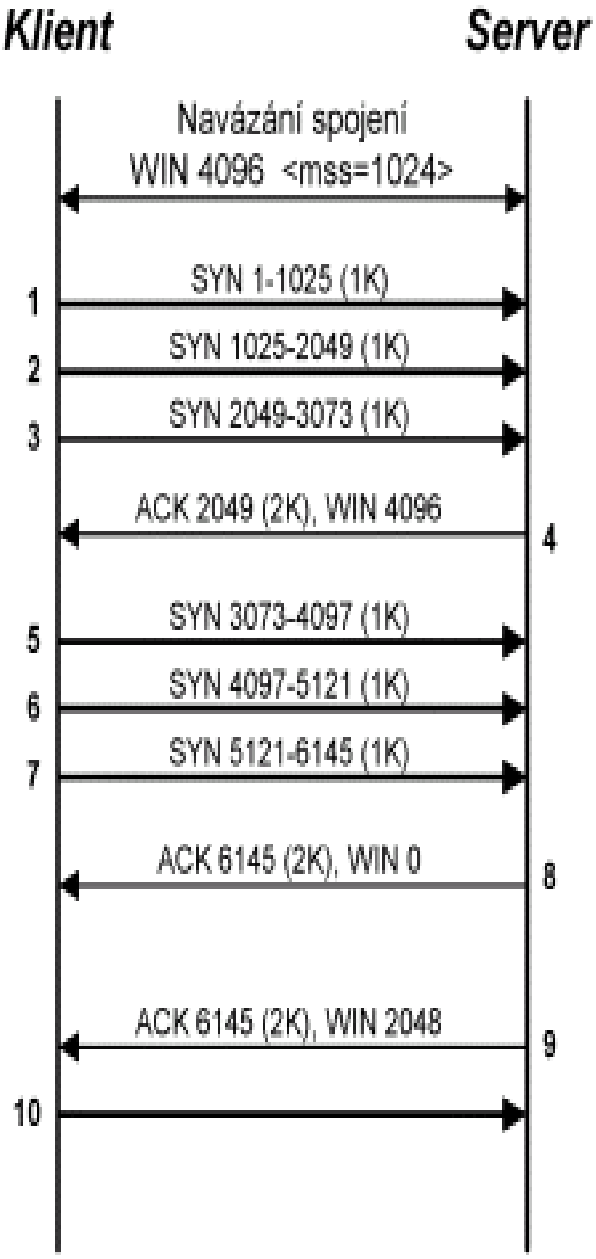
Některé volby TCP záhlaví včetně jejich struktury:



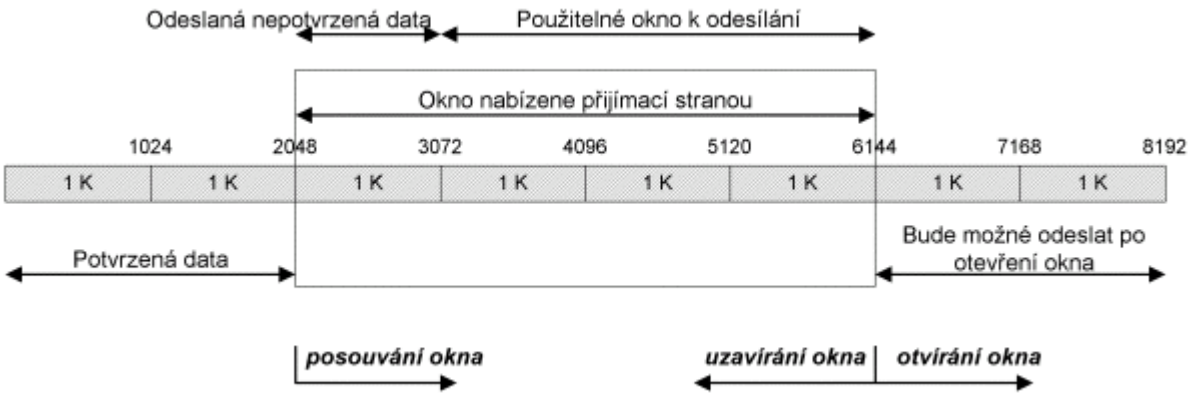
TCP Window

Nyní je naším problémem případ, kdy klient potřebuje odeslat velké množství dat. Klient (resp. Server) může odesílat data druhé straně aniž by jejich příjem měl potvrzen až do tzv. okna (*Window* – zkratkou WIN).

Představme si, že klient se serverem navázal spojení a vzájemně se dohodli na maximální velikosti segmentu (MSS) o velikosti 1K (tj. 1024 B) a vzájemné velikosti okna 4K (tj. 4096B).



- Klient začne s odesíláním dat, odešle segmenty 1, 2, 3.
- Poté obdrží od serveru potvrzení (4), které potvrzuje segmenty 1 a 2.
- Klient v zápětí odesílá segmenty 5, 6 a 7.
- Server data mezitím nedokázal zpracovat a data mu zaplnila vyrovnávací paměť, proto segmentem 8 sice potvrdí příjem segmentů 3, 5, 6 a 7, ale zároveň klientovi uzavře okno, tj. klient nemůže s odesíláním dat pokračovat.
- Poté co server zpracuje část dat (2 KB), umožní klientovi pokračovat v odesílání, ale neotevře mu segmentem 9 okno celé – pouze 2KB, protože všechna data ještě nezpracoval.

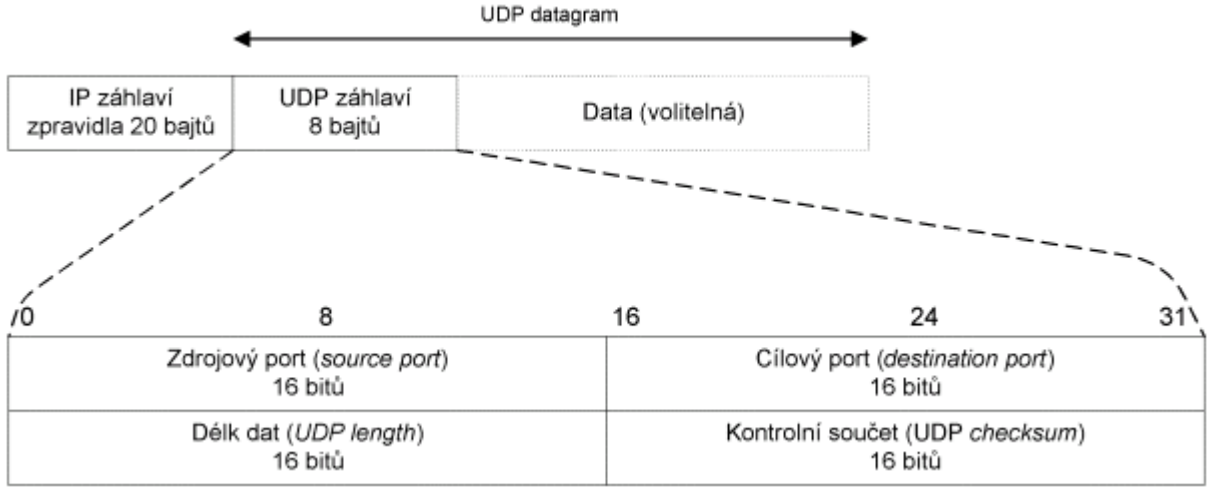


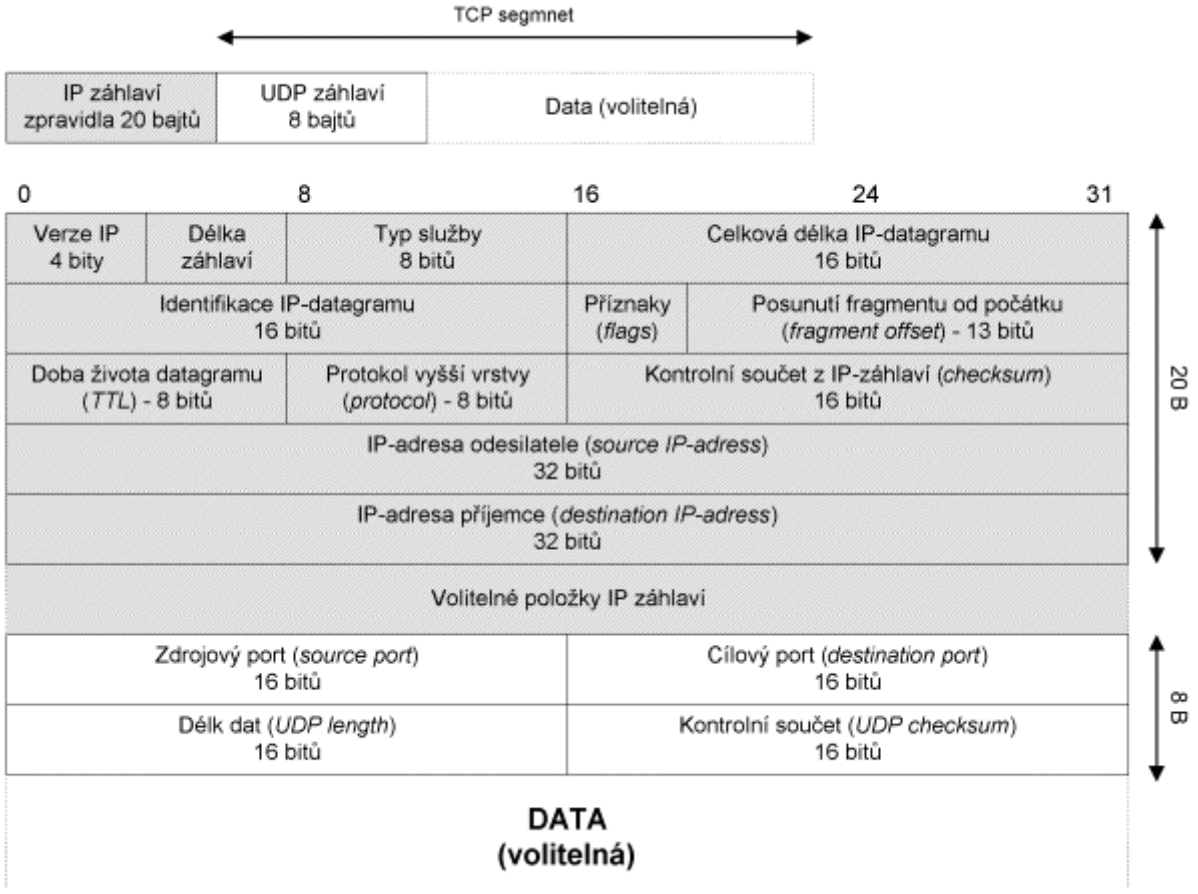
Tabulka uvádí některé běžné služby protokolu TCP (viz /etc/services na unixových strojích).

TCP port	**Jméno služby**
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
110	pop3

1.6.3 UDP

Protokol UDP nabízí jednoduchý nespolehlivý systém pro přenos paketů. Výhodou protokolu UDP je to, že přenosy protokolem UDP jsou až desetkrát rychlejší.



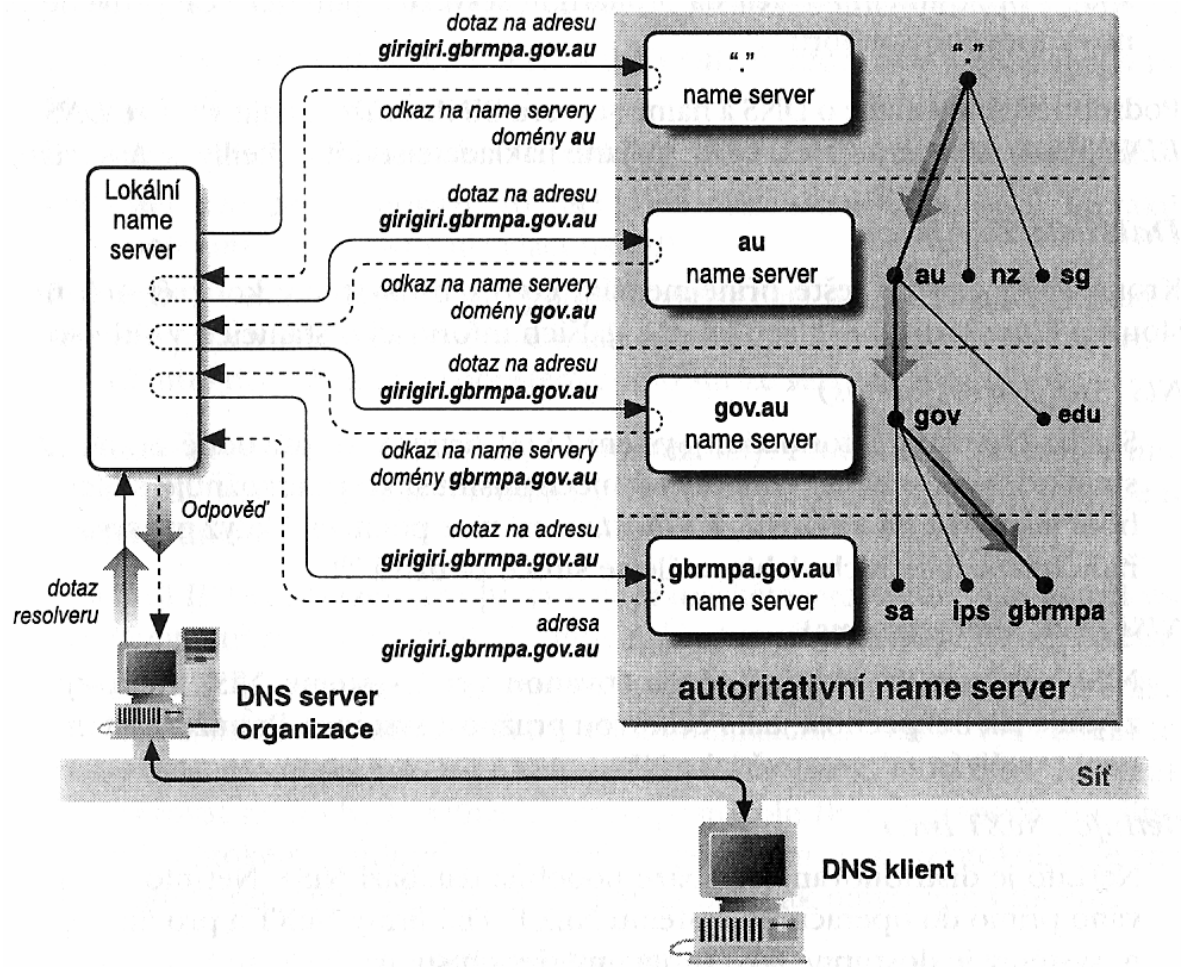


Příklady UDP služeb:

UDP port	Jméno služby
53	domain
123	ntp
161	snmp
520	route

1.7 DNS

DNS implementuje rozsáhlou distribuovanou databázi pro překlad jmen hostů na IP adresy a naopak a zároveň zajišťuje další s tím související služby. Ke snížení celkového zatížení sítě se používá řada různých cacheovacích postupů. DNS je založeno na protokolu UDP, pro některé operace však používá i spojení TCP.



Standardní unixovská implementace DNS se jmenuje *bind* a původně vznikla na University of Carolina v Berkeley. Celá implementace je založena na třech částech:

- ***Resolver*.** Knihovna resolveru slouží k implementaci DNS funkcí *gethosbyname()* a *gethostbyaddress()*
- ***named*** (nebo *in.named*). Démon named je program, který implementuje serverovou stranu DNS systému. Po spuštění načte *named* bootovací soubor (obvykle */etc/named.boot*), který určuje umístění pomocných souborů. Z nich pak *named* načte adresy kořenových doménových serverů. Pokud *named* pracuje jako ns domény, je v konfiguračních souborech uložen rovněž příkaz k načtení tabulek hostů dané domény, nebo příkaz k jejich zjištění od primárního serveru domény.
- ***named-xfer*** slouží k přenosu zónových souborů z primárního serveru na sekundární servery. Spouští jej sekundární server k provedení zónového přenosu. Program *named-xfer* se spojí s *named* na primámím serveru a pomocí TCP provede přenos zónového souboru.

Podle uložení dat rozlišujeme následující typy name serverů:

- **Primární name server** udržuje data o své zóně v databázích na disku. Pouze na primárním name serveru má smysl editovat tyto databáze.
- **Sekundární name server** si kopíruje databáze v pravidelných časových intervalech z primárního name serveru. Tyto databáze nemá smysl na sekundárním name serveru editovat, neboť budou při dalším kopírování přepsány. Primární i sekundární name servery jsou tzv. autoritou pro své domény, tj. jejich data pro příslušnou zónu se považují za nezvratná (autoritativní).
- **Caching only server** není pro žádnou doménu ani primárním ani sekundárním name serverem (není žádnou

autoritou). Avšak využívá obecné vlastnosti name serveru, tj. data, která jím prochází ukládá ve své paměti. Tato data se označují jako neautoritativní. Každý server je caching server, ale slovy caching only zdůrazňujeme, že pro žádnou zónu není ani primárním ani sekundárním name serverem (Pochopitelně i caching only server je primárním name serverem pro zónu 0.0.127.in-addr.arpa, ale to se nepočítá).

- **Root name server** je name server obsluhující root doménu. Každý root name server je primárním serverem, což jej odlišuje od ostatních name serverů.

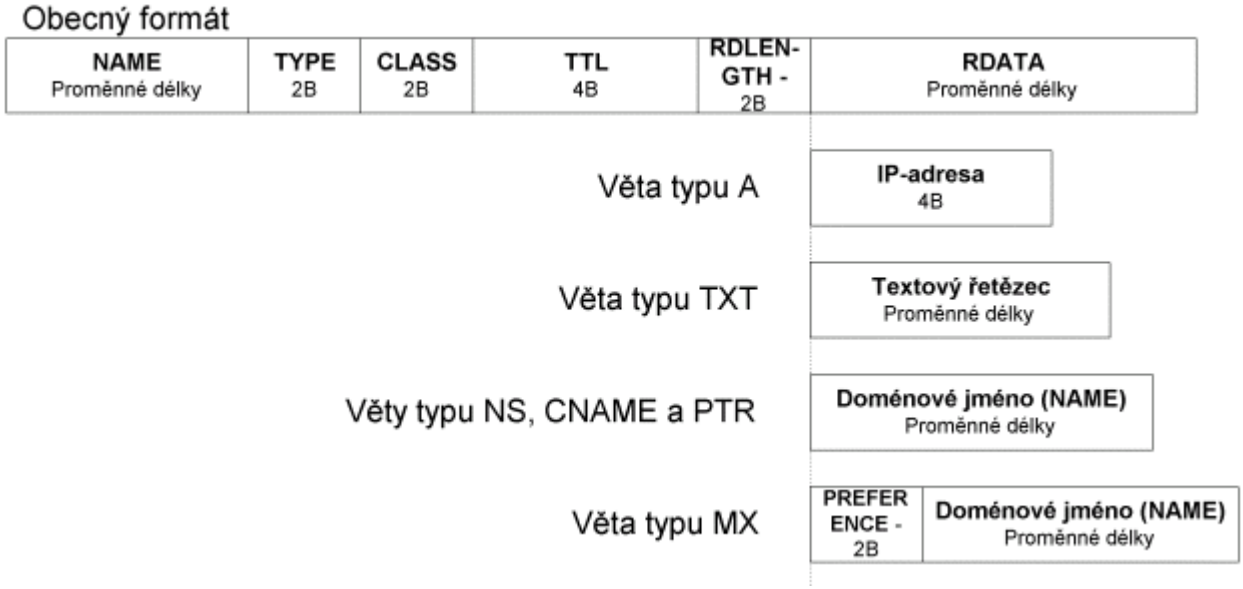
Jeden name server může být pro nějakou zónu primárním serverem, pro jiné sekundárním serverem.

Resource Records – RR

Informace o doménových jménech a jim příslušejících IP adresách, stejně tak jako všechny ostatní informace distrubuované pomocí DNS jsou uloženy v paměti DNS serverů ve tvaru zdrojových vět (***Resource Records – RR***). Name server naplňuje svou paměť několika způsoby. Autoritativní data načte ze souborů na disku, nebo je získá pomocí dotazu *zone transfer* z paměti jiného serveru. Neautoritativní data získává postupně z paměti jiných serverů, tak jak vyřizuje jednotlivé DNS dotazy.

V případě, že DNS klient (resolver) potřebuje získat informace z DNS, pak požaduje po name serveru věty RR podle zadaných požadavků. Klient může např. požadovat po serveru věty RR typu A, které obsahují IP adresy pro dané doménové jméno, apod.

Všechny věty RR mají stejnou strukturu.



Jednotlivá pole vět RR obsahují:

NAME - doménové jméno**.**

TYPE - typ věty.

CLASS - třída věty.

TTL - Time To Live. 32 bitové číslo, udávající dobu, po kterou může být tento RR udržován v cache server jako platný. Po vypršení této doby musí být věta považována za neplatnou. Hodnota 0 zabraňuje neautoritativním serverům uložit RR větu do cache.

RDLENGTH - 16 bitové číslo specifikující délku pole RDATA.

RDATA - Vlastní data ve tvaru řetězce proměnné délky. Formát tohoto pole závisí na typu a třídě RR.

Nejčastější typy vět RR

Typ	Anglický název	Význam pole RDATA
A	A host address	32 bitová IP adresa
NS	Authoritative name server	Doménové jméno name serveru, který je autoritou pro danou doménu.

CNAME	Canonical name for an alias	Doménové jméno specifikující synonymum k NAME
SOA	Start Of Autority.	Právě jedna věta SOA uvozuje každou zónu. Obsahuje 7 polí. přesný popis viz. DNS databáze.
PTR	Domain name pointer	Doménové jméno. Věta se používá pro reverzní překlad.
HINFO	Host information	Obsahuje dva znakové řetězce. První obsahuje popis HW a druhý popis SW, které jsou používané na počítači NAME.
MX	Mail exchange	Obsahuje dvě pole. První 16 bitové pole bez znaménka obsahuje preferenci a druhé obsahuje doménové jméno maillového serveru.
TXT	Text string	Textový řetězec s popisem.
AAAA	IP6 address	128 bitová IP adresa (IP verze 6)
SIG	Security signature	Podpisová věta, používaná při autentizaci v Secure DNS.
KEY	Security key	Veřejný klíč zony používaný pro podepisování při autentizaci
NXT	Next domain	Další doménové jméno. Autentikace neexistence doménového jména a typu.

Template ve FreeBSD:

```
; From: @(#)localhost.rev 5.1 (Berkeley) 6/30/90
; $FreeBSD: src/etc/namedb/PROTO.localhost.rev,v 1.6 2000/01/10
15:31:40 peter Exp $
; This file is automatically edited by the `make-localhost'
; script in the /etc/namedb directory.
;
$TTL    3600
@       IN      SOA     @host@. root.@host@.  (
                                @date@  ; Serial
                                3600    ; Refresh
                                900     ; Retry
                                3600000 ; Expire
                                3600 )  ; Minimum
        IN      NS      @host@.
1       IN      PTR     localhost.@domain@.
```

Příklad:

```
$TTL
@               IN SOA  dns.provider.cz.  root.dns.provider.cz.
                        2001052701      "; Serial"
                        21600           "; Refresh (6 hours)"
                        1800            "; Retry (30 minutes)"
                        172800          "; Expire (2 days)"
                        7200            "; Minimum (2 hours)"
                IN NS   cns.company.cz.
                IN NS   dns.provider.cz.
                IN NS   sns.provider.cz.
                IN MX   0   cns.company.cz.
                IN MX   50  mailx.provider.cz.
c-001   IN      A       195.57.120.1
cns     IN      A       195.57.120.2
c-003   IN      A       195.57.120.3
…
net-1   CNAME   c-000
cisco   CNAME   c-001
…
```

1.7.1 Služby NIS

Network Information System (NIS) firmy Sun, původně zvaná Yellow Pages, představuje jednoduchý mechanismus, který umožňuje sdílení souborů jako */etc/password* a */etc/hosts* mezi více počítači. NIS má řadu bezpečnostních slabin.

NIS+ představuje zásadně přepracovanou verzi systému NIS, která výraznězvyšuje jak bezpečnost, tak i celkovou pružnost systému.