Úvod do počítačových sítí

OSI (*Open Systems Interconnection*) model

Aplikační vrstva (Application)	Komunikační protokoly navržené pro meziprocesní komunikaci po IP síti.		SIP, SSI, DNS, FTP, HTTP, NFS, DHCP, SMTP, SNMP, Telnet,
Prezentační vrstva (Presentation)	Data-translator nebo syntex layer. Kódování a formáty, v nichž je přenášena informace po síti (XML, ASCII, serializace binárních dat)		MIME, TLS, XDR, XML TLS/SSL (enkrypce)
Relační vrstva (Session)	Poskytuje mechanismus pro otevření, správu a ukončení relace (session) mezi aplikačními procesy		RPC, RTP, TLS/SSL (ustavení)
Transportní vrstva (Transport)	Segmenty	Doručování segmentů mezi službami. • Connestion-oriented: spolehlivé, flow control • Connection-less	TCP, UDP
Síťová vrstva (Network)	Packety	Adresace (IP adresy), směrování, (ne nutně spolehlivé) doručení datagramů mezi dvěma počítači.	IP, IPsec, ICMP
Linková vrstva (Data)	Frames	Spolehlivé datové spojení point-to-point. (obálka, MAC adresa)	IEEE 802.3 – Ethernet PPP IEEE 802.11 - WiFi
Fyzická vrstva (Physical)	Proud bitů	Přímé datové spojení (ne nutně spolehlivé) point-to-point.	UTP – RJ45 RS-232 IEEE 802.11 - WiFi

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

- 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

IP protocol (Internet protocol)

- Protokol IPv4 se používá v Internetu od roku 1982.
- IPv5 byl experimentální protokol (nepoužívá se).
- V současnosti se začíná využívat IPv6.

My se zaměříme na IPv4.

IPv4

- Data jsou přenášena v blocích znaků – datagramech/paketech.
- Přenášená data se rozkládají na pakety, po dosažení cíle se pakety skládají zpět.
- Každý paket obsahuje hlavičku, identifikující odesílatele a požadovaného adresáta.
- Za hlavičkou následuje blok dat - obsah paketu.
- Tento proces rozkládání a skládání je pro uživatele obvykle neviditelný.
- Protože z jednoho systému na druhý obvykle existuje několik různých tras, může každy paket od odesílatele k adresátu putovat jinou cestou.

IP paket


Bity
0
4
8
12
16
20
24
28
Objekty
1
Verze
Délka hlavi-čky
Typ služby
Celková délka
5
Identifikace
Příz-naky
Fragmentační offset
7
Životnost
Protokol
Kontrolní součet hlavičky
9
Zdrojová adresa
13
Cílová adresa
17
Parametry
Dorovnání
Hlavička
Data ...
Data

Hlavní způsoby spojení protokolem IP

- Obě stanice jsou připojeny ke stejné lokální síti (dnes obvykle Ethernet, WiFi IEEE 802.11). 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.

Adresace IPv4

- Každé rozhraní připojené na IP síť má přidělenu jednoznačnou 32-bitovou adresu, formálně zapisovanou jako čtveřice hodnot 0-255 (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.
- Proto je obecně nedostatek IP adres – jedna z motivací pro IPv6.

Adresa třídy A

- 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.

Adresa třídy B

- 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.

Adresa třídy C

- Adresy třídy C mají formát N.M.O.a, kde N.M.O je číslo sítě a a je číslo počítače
- Nejvyšší bity čísla N musejí být 110.

Adresa třídy D

- 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, která je asociovaná s danou adresou třídy D.
- Každý z členů skupiny přijímá pakety skupině adresované.

Třídy adres

Třída	Formát	Indikace (bity zleva)	Počet bitů – síť	Počet bitů - host
A	N.a.b.c	0	7	24
B	N.M.a.b	10	14	16
C	N.M.O.a	110	21	8
D	N.M.O.a	1110	20	8

Třídy adres

Třída	Počet sítí	Počet hostů	Rozsah adres	Adresa sítě	Adresa hosta
A	128	16 777 214	1.*.*.* až 127.*.*.*	a	b.c.d
B	16,384	65,534	128.*.*.* až 191.*.*.*	a.b	c.d
C	2,097,152	254	192.*.*.* až 223.*.*.*	a.b.c	d

Speciální adresy

- Adresy Network a Broadcast jsou rezervovány a nepoužívají se jako host adresy.
- Adresa sítě (Network) 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 hostapoužívaný hostem pro zasílání paketů sám sobě. Obvykle je vUnixových systémech značen jako interface lo0.

Maska sítě

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

Maska sítě

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)

Privátní sítě

Existují tři adresy sítí, rezervované pro privátní adresy:

- 10.0.0.0/8, 172.16.0.0/12 a 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.

Jména hostů

$ ping **www.seznam.cz**

PING www.seznam.cz (**77.75.76.3**): 56 data bytes

64 bytes from 77.75.76.3: icmp_seq=0 ttl=244 time=23.527 ms

64 bytes from 77.75.76.3: icmp_seq=1 ttl=244 time=4.210 ms

64 bytes from 77.75.76.3: icmp_seq=2 ttl=244 time=4.081 ms

Jména hostů

- 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 výynamně narostl 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).

Základní protokoly

- **ICMP** Internet Control Message Protocol – zajišťuje nízkoúrovňové operace protokolu IP, např. výměna směrovacích informací apod.

- **TCP** Transmission Control Protocol – slouží k vytvoření obousměrného proudového spojení mezi dvěma počítači. Jedná se o „spojovaný" (connection-based) protokol, ktery implementuje funkce timeoutu a opakování přenosu, aby zajistil spolehlivé doručení informací.

Základní protokoly

- **TCP** Transmission Control Protocol – slouží k vytvoření obousměrného proudového spojení mezi dvěma počítači. Jedná se o „spojovaný” (connection-based) 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" (connection-less) – nezajišťuje doručení.

TCP

- TCP zajišťuje spolehlivý, řízený, obousměrný 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.

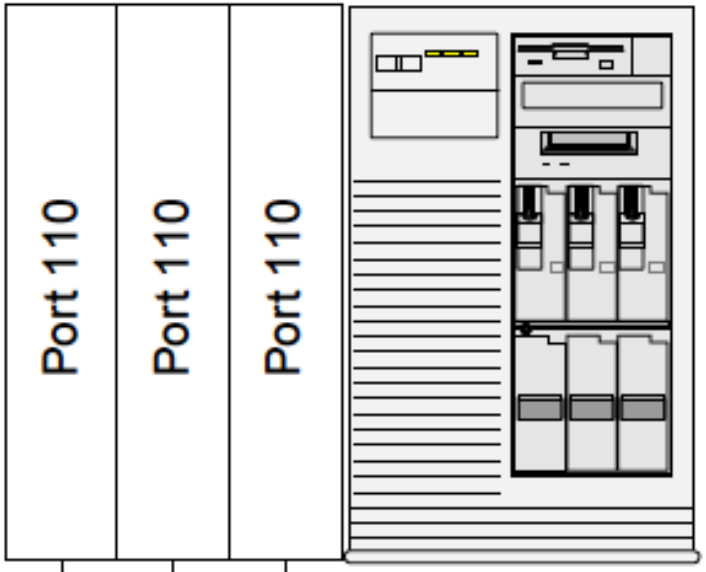
- Pokud dojde k fyzickému přerušení spojení a nepodaří se nalézt alternativní trasu, pak implementace protokolu TCP pošle procesu, který se snaží přijímat nebo odesílat data, chybové hlášení.

TCP

- 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

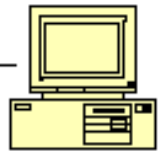
TCP



IP 147.32.81.34

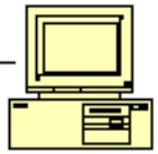
Alice

IP 147.32.81.62
Port 6788



Bob

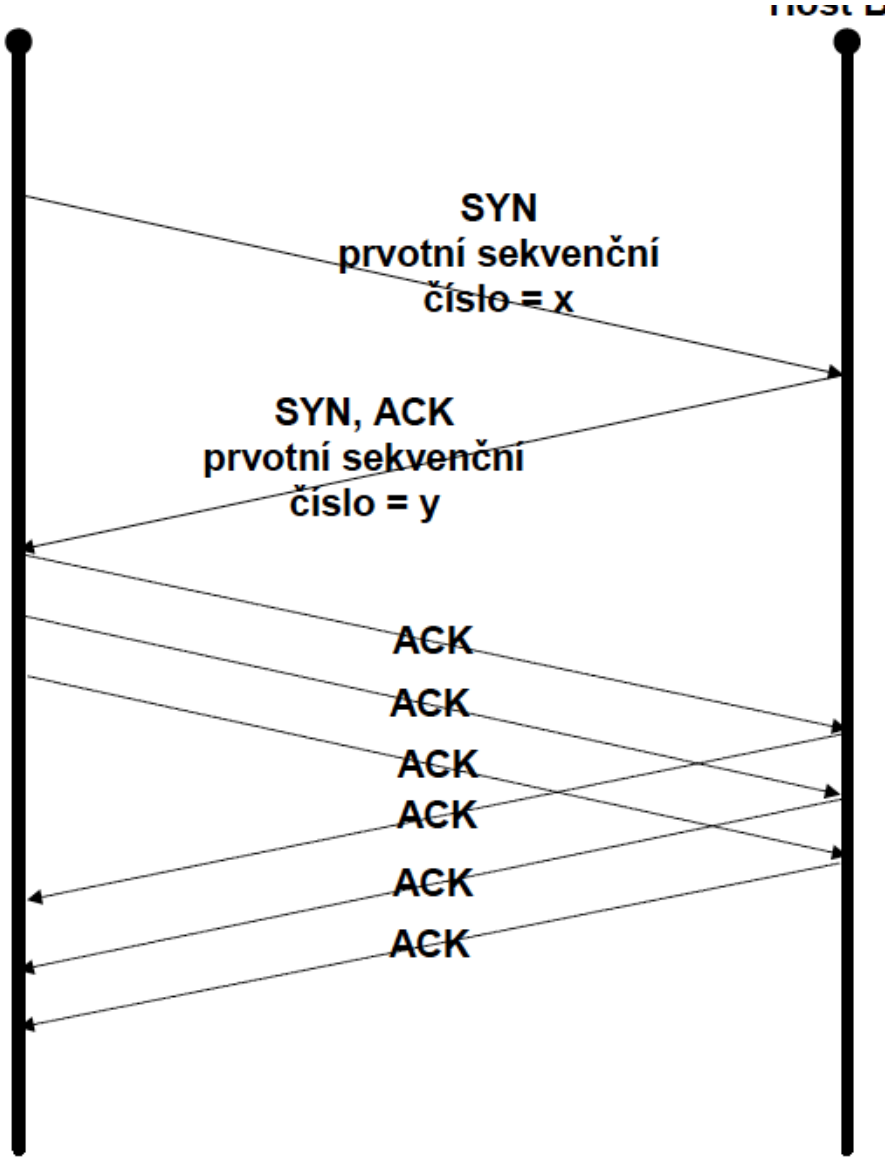
IP 147.32.81.95
Port 9844



Cecille

IP 147.32.81.38
Port 8828

Navazování TCP spojení



Navazování TCP spojení

- 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.

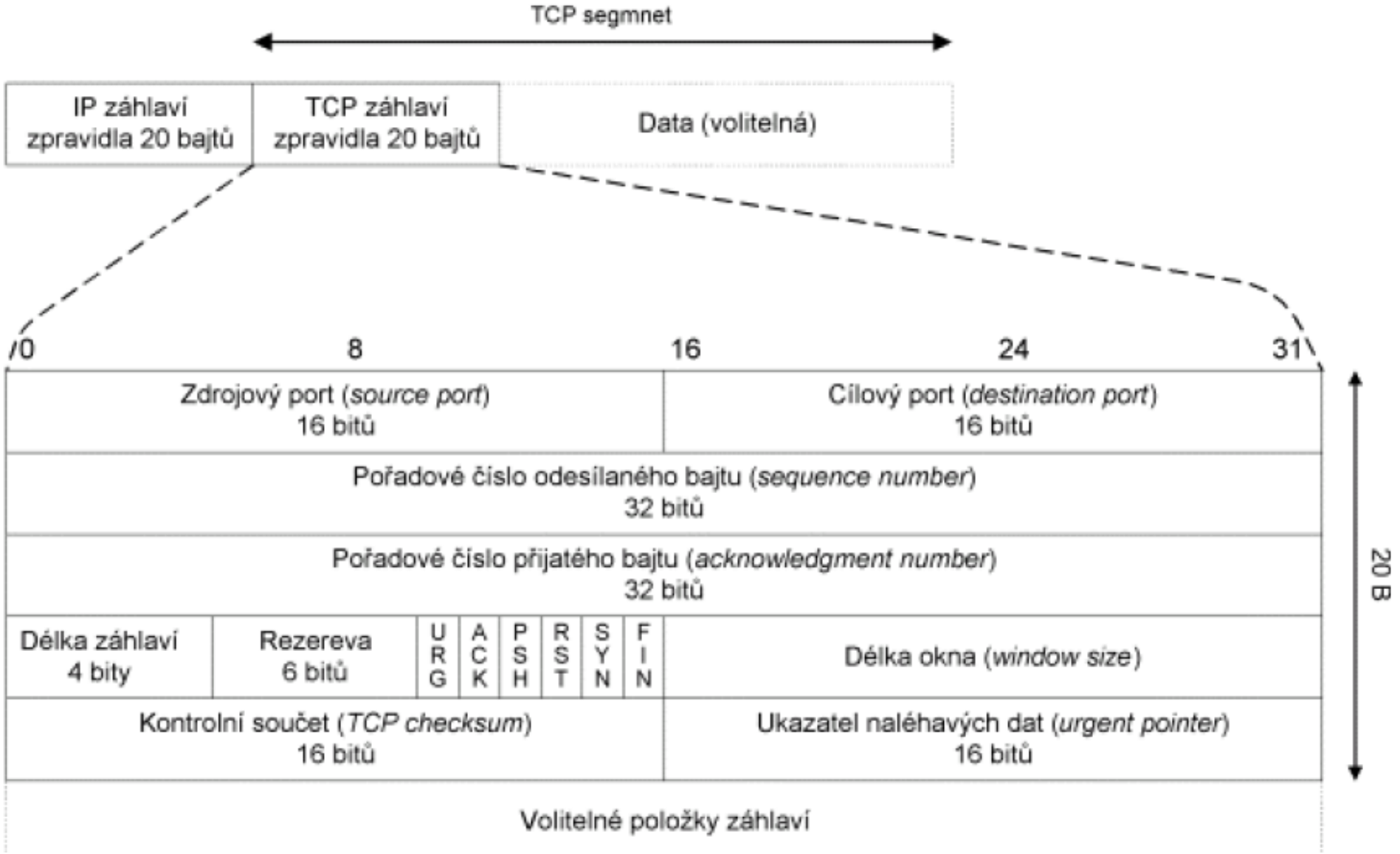
- Druhý host potvrdí navázání spojení paketem, který má
- nastaveny oba bity – SYN i ACK.

- Nakonec žadatel odešle třetí paket, v němž je nastaven
- bit ACK, ale není nastaven bit SYN.

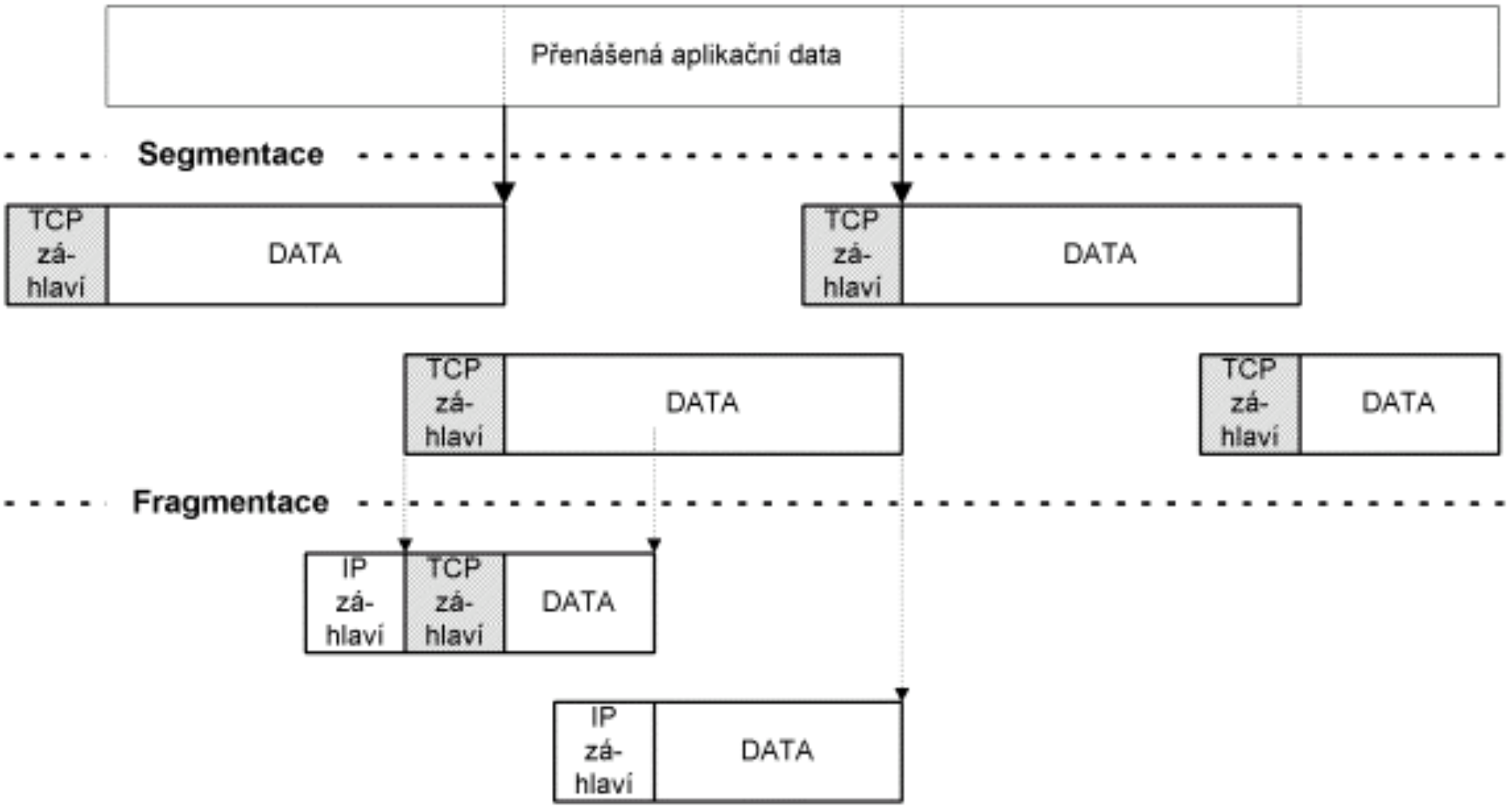
- Tomuto procesu se říká třícestný handshake.

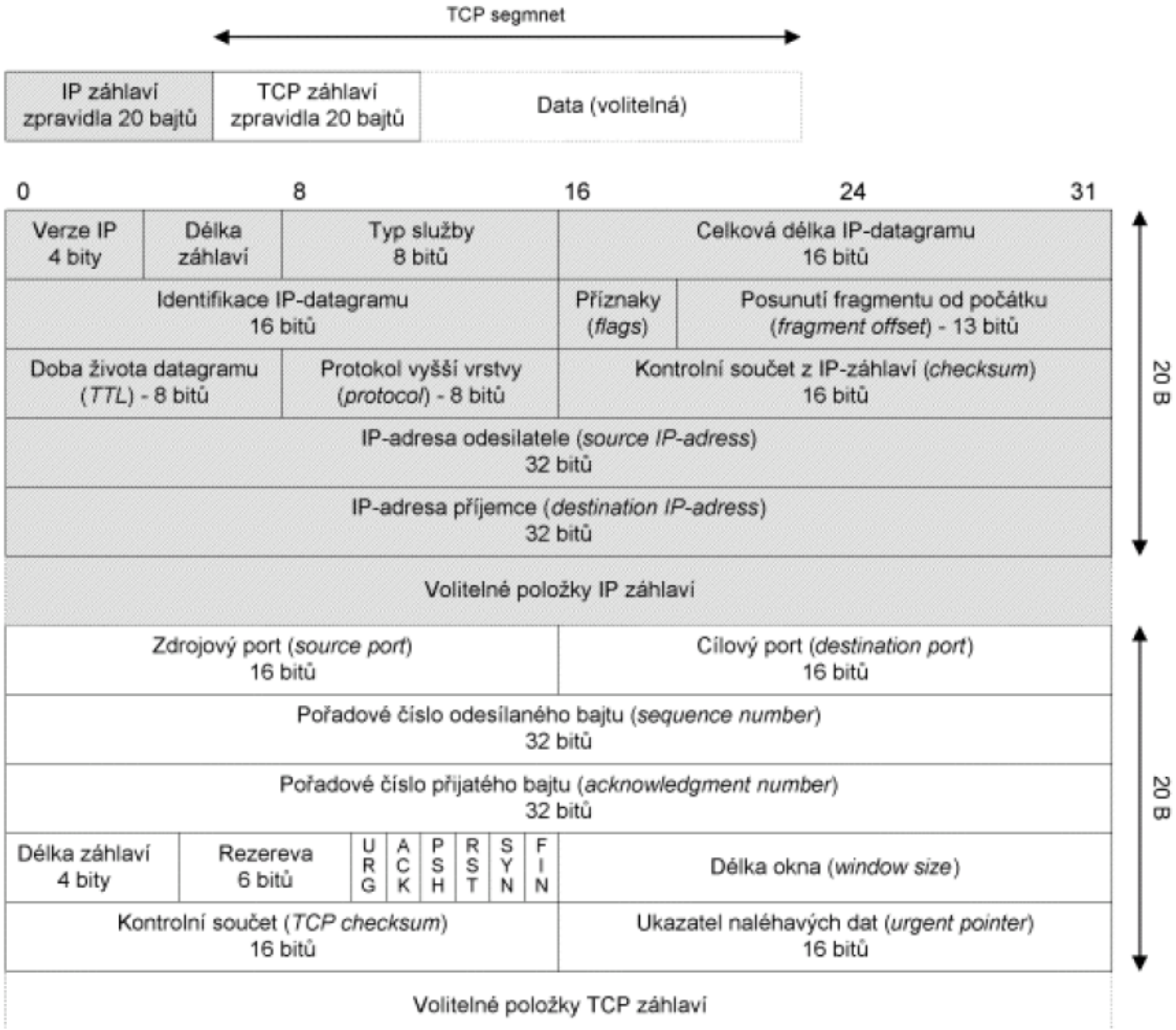
- Když budeme vyhledávat pakety s nenastaveným bitem ACK, můžeme snadno rozeznat požadavky na nove spojení od paketů, které se posílají v rámci již existujícího spojení. Toto rozlišení může být důležité při vytváření fíltračních firewallů.

TCP segment


TCP segmnet
IP záhlaví
zpravidla 20 bajtů
TCP záhlaví
zpravidla 20 bajtů
Data (volitelná)
0
8
16
24
31
Zdrojový port (source port)
16 bitů
Cílový port (destination port)
16 bitů
Pořadové číslo odesílaného bajtu (sequence number)
32 bitů
Pořadové číslo přijatého bajtu (acknowledgment number)
32 bitů
Délka záhlaví
4 bity
Rezereva
6 bitů
URG
ACK
PSH
RST
SYN
FIN
Délka okna (window size)
Kontrolní součet (TCP checksum)
16 bitů
Ukazatel naléhavých dat (urgent pointer)
16 bitů
Volitelné položky záhlaví
20 B

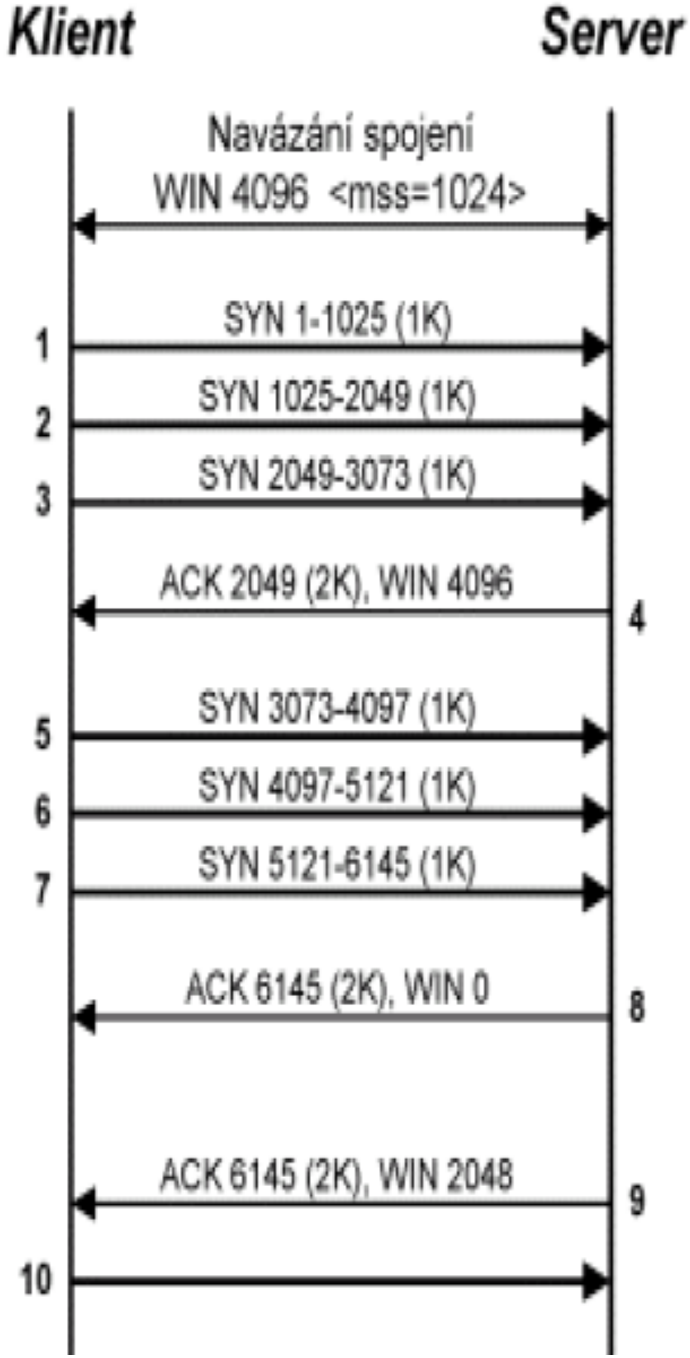
TCP: segmentace, fragmentace




TCP segmnet
IP záhlaví zpravidla 20 bajtů
TCP záhlaví zpravidla 20 bajtů
Data (volitelná)
0
8
16
24
31
Verze IP 4 bity
Délka záhlaví
Typ služby 8 bitů
Celková délka IP-datagramu 16 bitů
Identifikace IP-datagramu 16 bitů
Příznaky (flags)
Posunutí fragmentu od počátku (fragment offset) - 13 bitů
Doba života datagramu (TTL) - 8 bitů
Protokol vyšší vrstvy (protocol) - 8 bitů
Kontrolní součet z IP-záhlaví (checksum) 16 bitů
IP-adresa odesilatele (source IP-adress) 32 bitů
IP-adresa příjemce (destination IP-adress) 32 bitů
20 B
Volitelné položky IP záhlaví
Zdrojový port (source port) 16 bitů
Cílový port (destination port) 16 bitů
Pořadové číslo odesílaného bajtu (sequence number) 32 bitů
Pořadové číslo přijatého bajtu (acknowledgment number) 32 bitů
Délka záhlaví 4 bity
Rezereva 6 bitů
URG
ACK
PSH
RST
SYN
FIN
Délka okna (window size)
Kontrolní součet (TCP checksum) 16 bitů
Ukazatel naléhavých dat (urgent pointer) 16 bitů
20 B
Volitelné položky TCP záhlaví

TCP okno (window)

- Zaměřme se na případ případ, kdy jedna strana (např.klient) potřebuje odeslat druhé straně (serveru) velké množství dat.
- Může odesílat data druhé straně aniž by jejich příjem měl potvrzen až do naplnění tzv. okna.
- Představme si, že klient se serverem navázal spojení a vzájemně se dohodli na maximální velikosti segmentu (MSS) ocvelikosti 1K (tj. 1024 B) a vzájemné velikosti okna 4K (tj. 4096B).



1., 2., 3. 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.

Vybrané služby protokolu TCP

(viz /etc/services na unixových strojích).

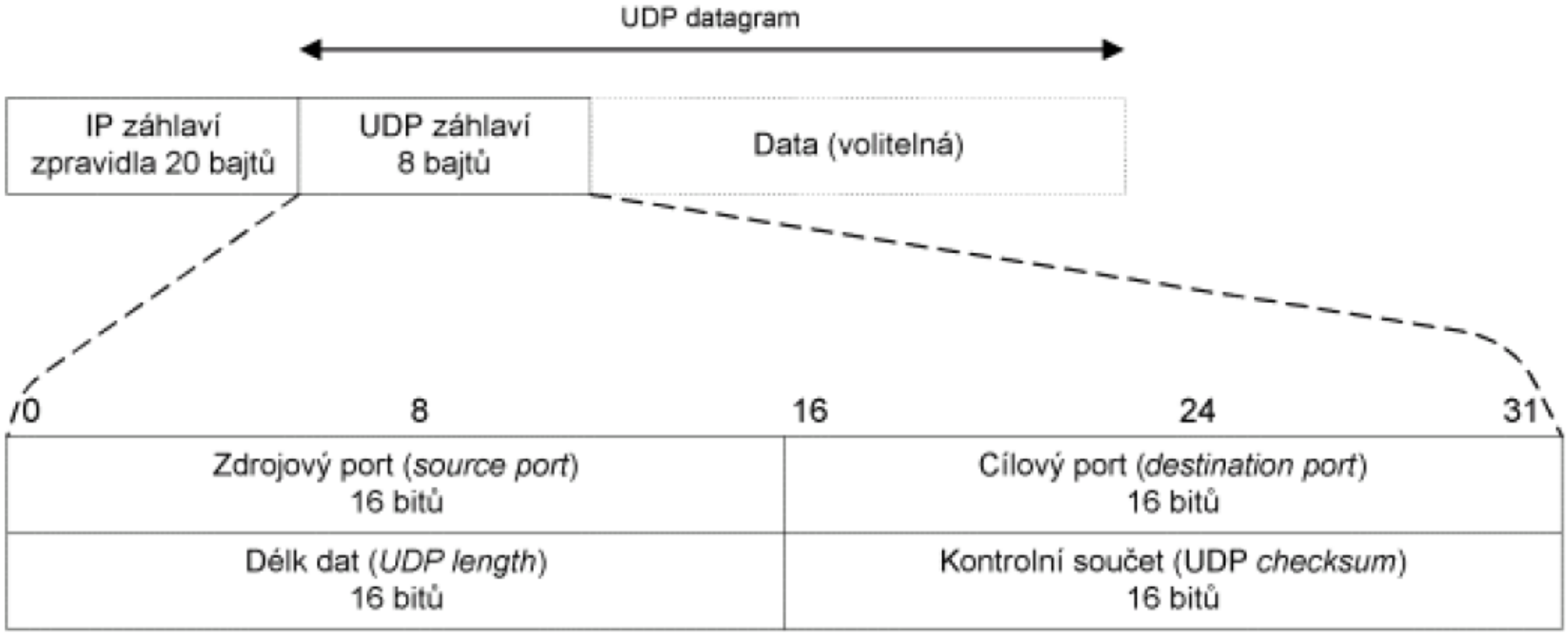
- 21 ftp
- 22 ssh
- 23 telnet
- 25 smtp
- 53 domain
- 110 pop3

UDP

- Protokol UDP nabízí jednoduchý nespolehlivý systém pro přenos paketů.

- Výhodou protokolu UDP je to, že přenosy protokolem UDP jsou až desetkrát rychlejší.

UDP

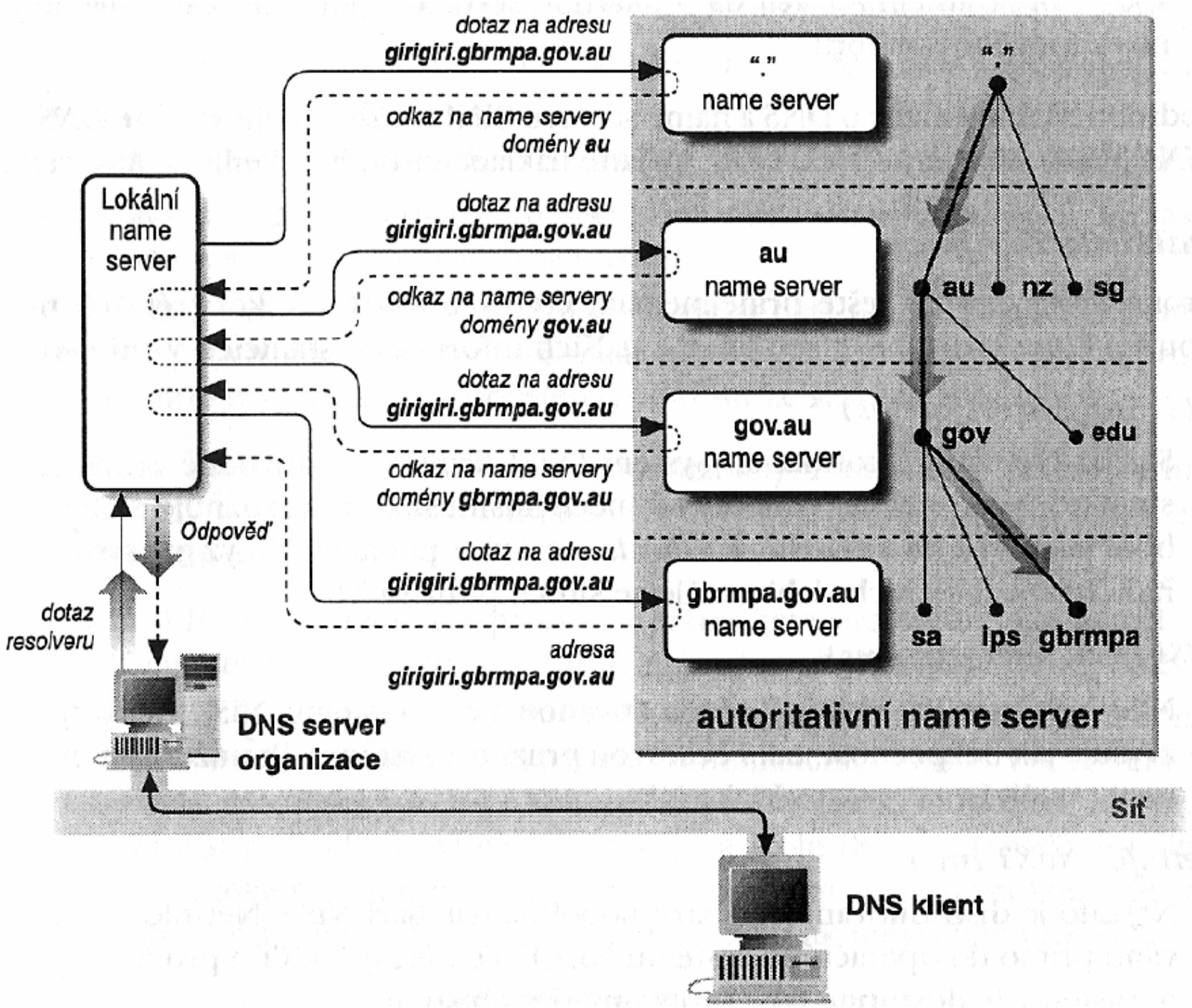

UDP datagram
IP záhlaví
zpravidla 20 bajtů
UDP záhlaví
8 bajtů
Data (volitelná)
0
8
16
24
31
Zdrojový port (source port)
16 bitů
Cílový port (destination port)
16 bitů
Délk dat (UDP length)
16 bitů
Kontrolní součet (UDP checksum)
16 bitů

Příklady UDP služeb

- 53 domain (DNS)
- 123 ntp
- 161 snmp
- 520 route

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.


dotaz na adresu
girigiri.gbrmpa.gov.au
odkaz na name servery
domény au
dotaz na adresu
girigiri.gbrmpa.gov.au
odkaz na name servery
domény gov.au
dotaz na adresu
girigiri.gbrmpa.gov.au
odkaz na name servery
domény gbrmpa.gov.au
dotaz na adresu
girigiri.gbrmpa.gov.au
adresa
girigiri.gbrmpa.gov.au
Lokální
name
server
Odpověď
dotaz
resolveru
" "
name server
au
name server
gov.au
name server
gbrmpa.gov.au
name server
" "
au
nz
sg
gov
edu
sa
ips
gbrmpa
autoritativní name server
DNS server
organizace
Síť
DNS klient

DNS – 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).

DNS – typy name serverů

- **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.