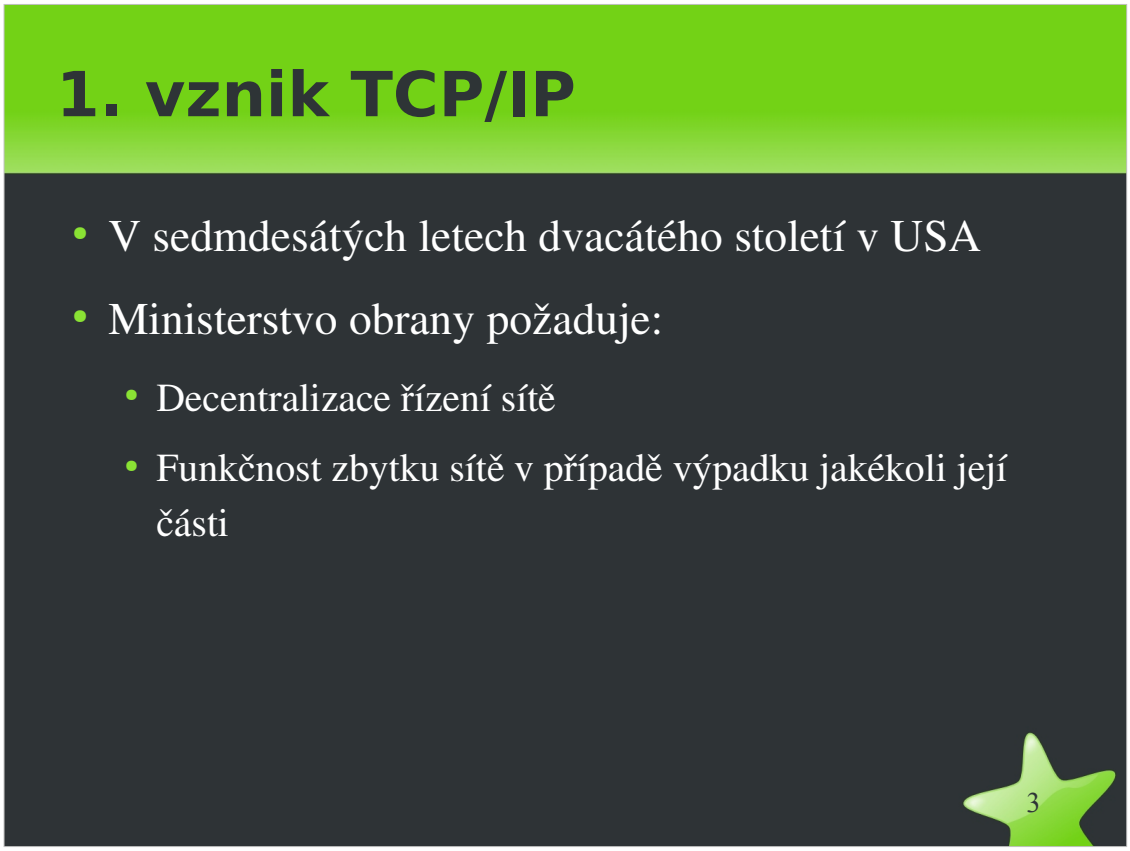
Protokol TCP/IP

- KAREL FATURA
- 17.03.2008

Obsah



existují tři druhy způsobu přenosu dat v síti

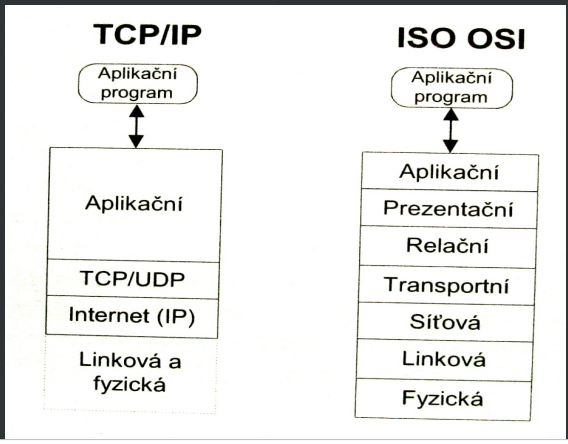
1. spojování okruhů – v síti jsou napevno vytvořena fyzická spojení po kterých se přenášejí data, tento způsob se často využíval v minulých letech pro etlefonní sítě.

2. paketový přenos – data se opatří záhlavím, kde je adresa příjemce a taková struktura, kterou nazýváme paket se pošle do sítě a ona dorazí k adresátovi. V praxi se v zahlaví musí přenášet mnohem více údajů ale pro vysvětlení principu stačí adresa příjemce.

3. hybrid mezi dvěma předchozími přístupy – spojování paketů. V síti se vytvoří tzv. virtuální okruh a ten má identifikátor. Hodnota identifikátoru se připojí k přenášeným datům a ta pak vesele cestují sítí. Jejich cestu řídí nějaká inteligence sítě, která ví, že příslušný virtuální okruj je spojením jistých bodů v síti (ta inteligence ví jaké body to jsou)

2. Srovnání s ISO-OSI

- Soustavy protokolů TCP/IP a ISO OSI se od sebe liší a jsou vzájemně neporovnaelné.
- Jsou si blízké na síťové a transportní vrstvě



3. Protokol IP

- Vlastní protokol IP
- Služební protokol ICMP
  - signaliazce mimořádných stavů
- Služební protokol IGMP
  - doprava adresových oběžníků
- Služební protokoly ARP a RARP
  - často se považují za nezávislé na IP, jejich rámce totiž nepředchází IP záhlaví

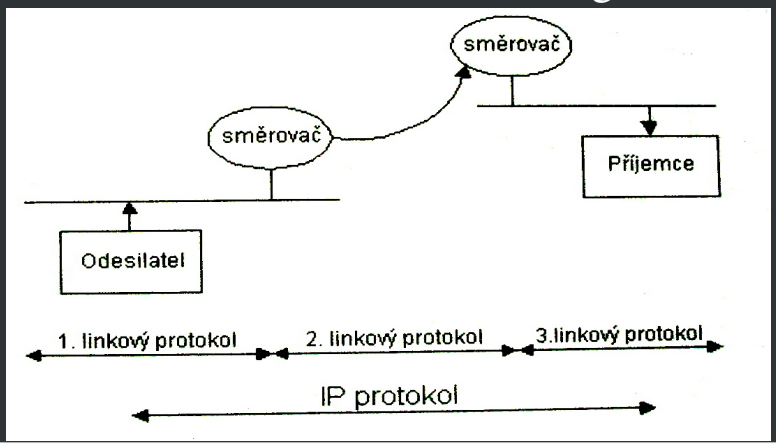
Některé linkové protokoly jsou určeny pro přenos v rámci lokální sítě, jiné slouží k přenosu dat mezi sousedími směrovači rozsáhlé sítě. IP narozdíl od linkových protokolů dopravuje data mezi dvěma počítači v internetu = tedy přes mnohé LAN.

Od odesilatele k příjemci jsou data směrována pomocí směrovačů (router). Přičemž těchto směrovačů je na cestě zpravidla několik několik. Každý směrovač řeší směrování jen na další směrovač = *next hop*

U linkových protokolů má každé síťové rozhraní zpravidla 6B-ovou adresu, protokol IP pracuje s 4B- (IP v4) nebo 16B- (IP v6) -ovou adresou. Každé rozhraní má alespoň jednu IP adresu. Žádná dvě rozhraní nemohou používat stejnou IP adresu. Pokud toto není zajištěno dalsími technologiemi (NAT atp.)

3. Protokol IP
Proč nestačí linkové adresy

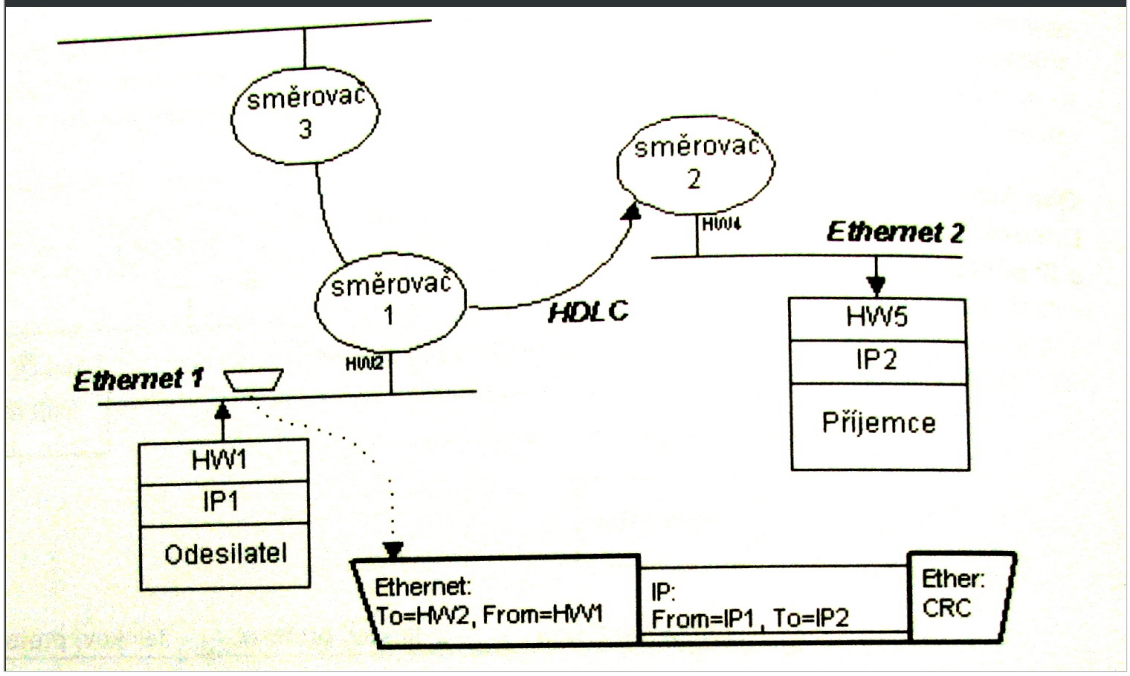
- Linkový protokol = doprava v rámci LAN = k nejbližšímu směrovači
- Směrovač nemění obsah IP datagramu krom TLL



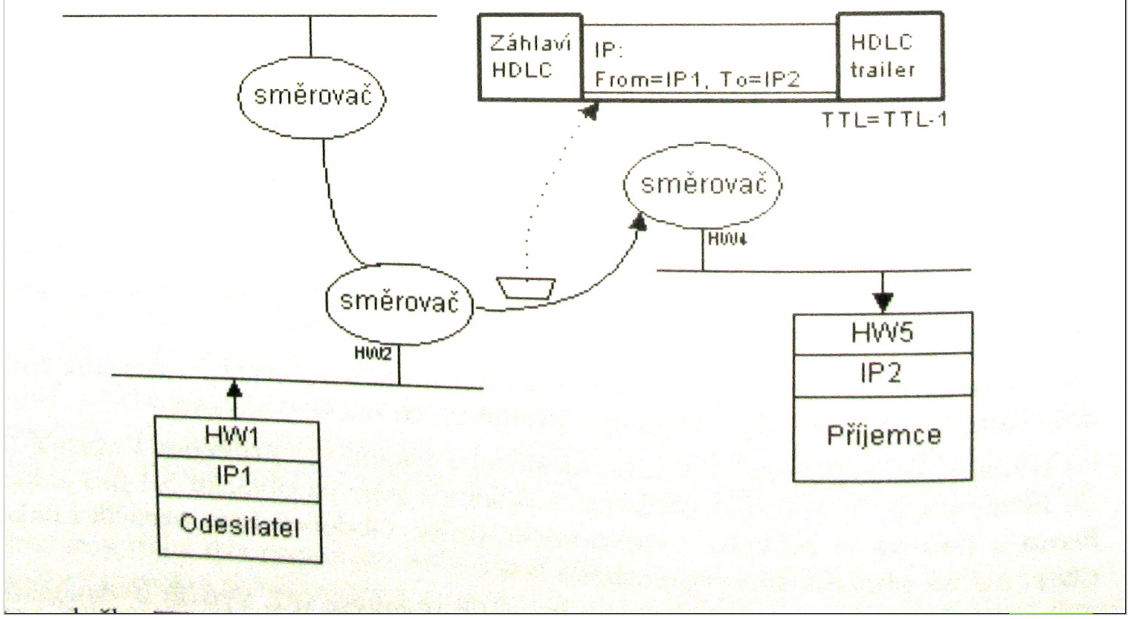
Nejbližší směrovač data vybalí a přebalí je do jiného linkového rámce. Na druhé straně směrovače může být nasazen jiný, nebo i stejný linkový protokol. Přebalení proběhne vždy.

Položka TLL v IP datagramu určuje jak dlouho bude datagram v síti ”žít”. Každý směrovač, kterým datagram prochází má povinnost snížit tuto hodnotu aspoň o jedničku. Směrovač, který dostane datagram s TLL 1, jej už dálě neposílá ale zahodí. Tím se v internetu zajišťuje ochrana před zbloudilými pakety, které by se donekonečna toulaly. Existují i další výjimky (fragmentace).

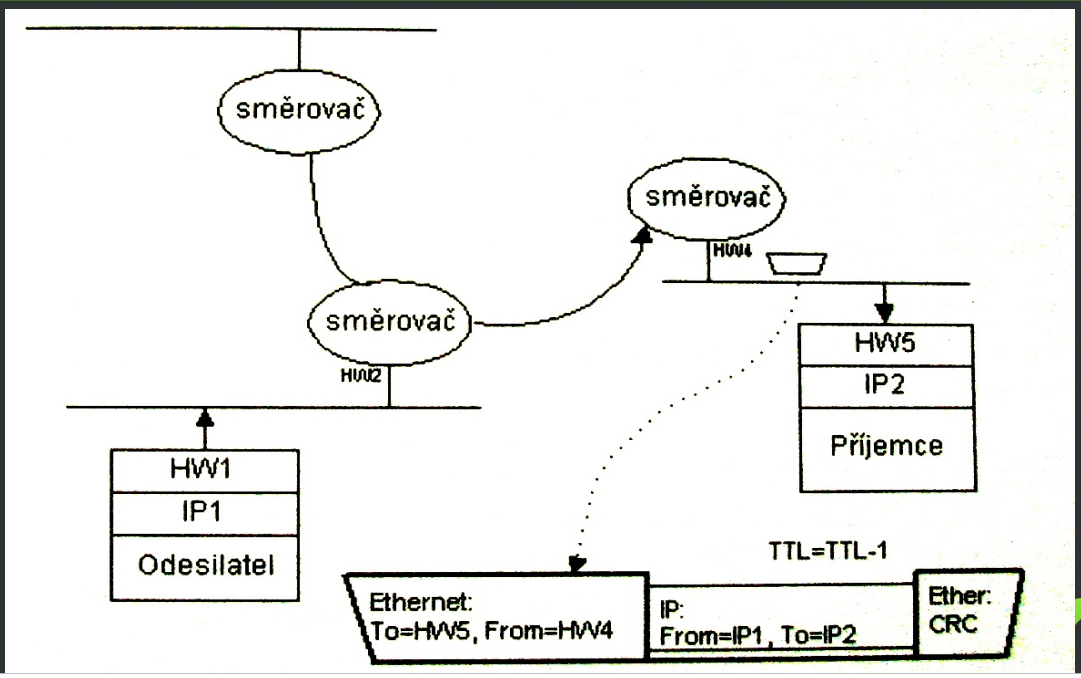
3. Protokol IP
Příklad odesílání IP datagr.



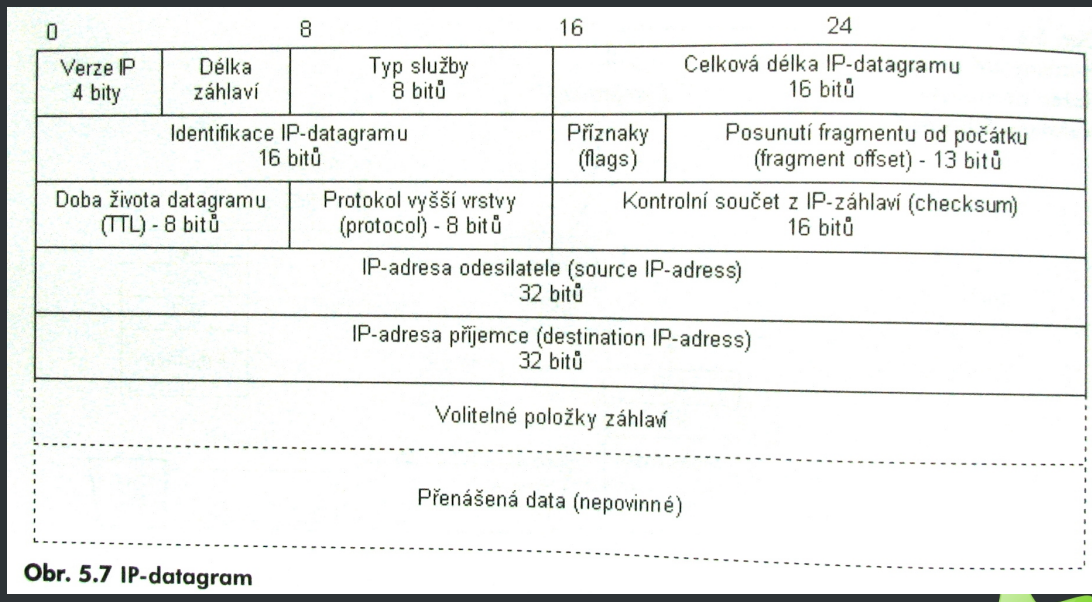
3. Protokol IP
Příklad odesílání IP datagr.



3. Protokol IP
Příklad odesílání IP datagr.



3. Protokol IP
IP - datagram



Obr. 5.7 IP-datagram

Verze – délka 4b, hodnota 4 pro Ipv4 nebo 6 pro Ipv6

Délka záhlaví – délka záhlaví se neuvádí v Bytech ale ve čtyřBytech, když délka záhlaví není dělitelná 4 dopní se záhlaví bezvýznamným obsahem. Maximální délka záhlaví je 60 B, z toho povinné položky zabírají 20B a na nepovinné tedy zbývá až 40B.

Typ služby – Dlouho neměla uplatnění, význam nabývá až s požadavkem přenosu videa zvuku přes internet

Celková délka IP datagramu – tato položke je dvouBytová a pro může být největší délka přenášeného paketu max 65 535 bitů.

Identifikace IP datagramu – vkládá operační systém odelilatele, společně s
Příznaky (0, Dont Fragment, More Fragments) a s
Posunutí fragmentu je využívána mechanismem fragmentace ip datagramu.

Doba života IP datagramu – každý směrovač ji sníží alespoň o jednicku, když už dekrementace není proveditelná, datagram se zahodí a odesilateli se toto signalizuje pomocí ICMP protokolu. TLL bývá parametrem operačního systému.

Protokol vyšší vrstvy – identifikace protokolu vyšší vrstvy (TCP nebo UDP) nebo nějaký služební protokol ICMP nebo IGMP. Služební protokoly jsou formálně součástí IP, ale za hlavičkou IP se přenáší hlavička ICMP nebo IGMP a proto se na ně dá dívat i tímto způsobem.

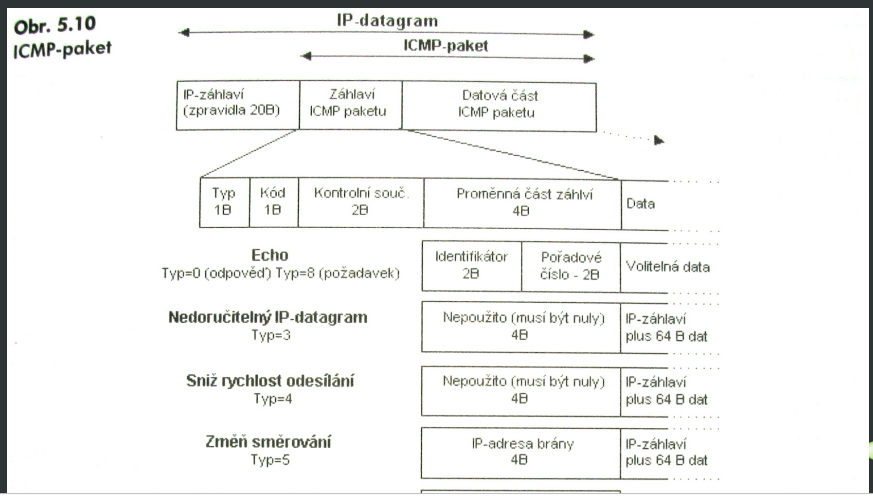
Kontrolní součet záhlaví – poze součet záhlaví nikoli celého datagramu. Směrovač tento součet musí přepočítat, protože v záhlaví mění TLL.

IP adresa odesilatele a
IP adresa příjemce

Volitelné položky – používají se ojediněle

3. Protokol IP
Služební protokol ICMP

- typ – hrubé dělení ICMP paketů
- kód – konkrétní problém (*jemné dělení*)



Vlastní formát ICMP zprávy se dovíjí od tohjo o jaký typ zprávy se jedná.

Echo – jednoduchý nástroj pro kontrolu dozažitelnosti bodu v síti. Tazatel vyšle paket žádost o echo na který je tázaný prvek odpovědět paketem ICMP *echo* viz program ping

Nedoručitelný IP datagram – nelze doručit.

Sniž rychlost odesílání – v případě, že směrovač je zahlcen a není schopen předávat všechny pakety, vysílá odesilatelům zprávy sniž rychlost odesílání. Jestli se odesílá na TCP, odesilatel sníží rychlost, v případě UDP je tato zpráva odesilatelem ignorována.

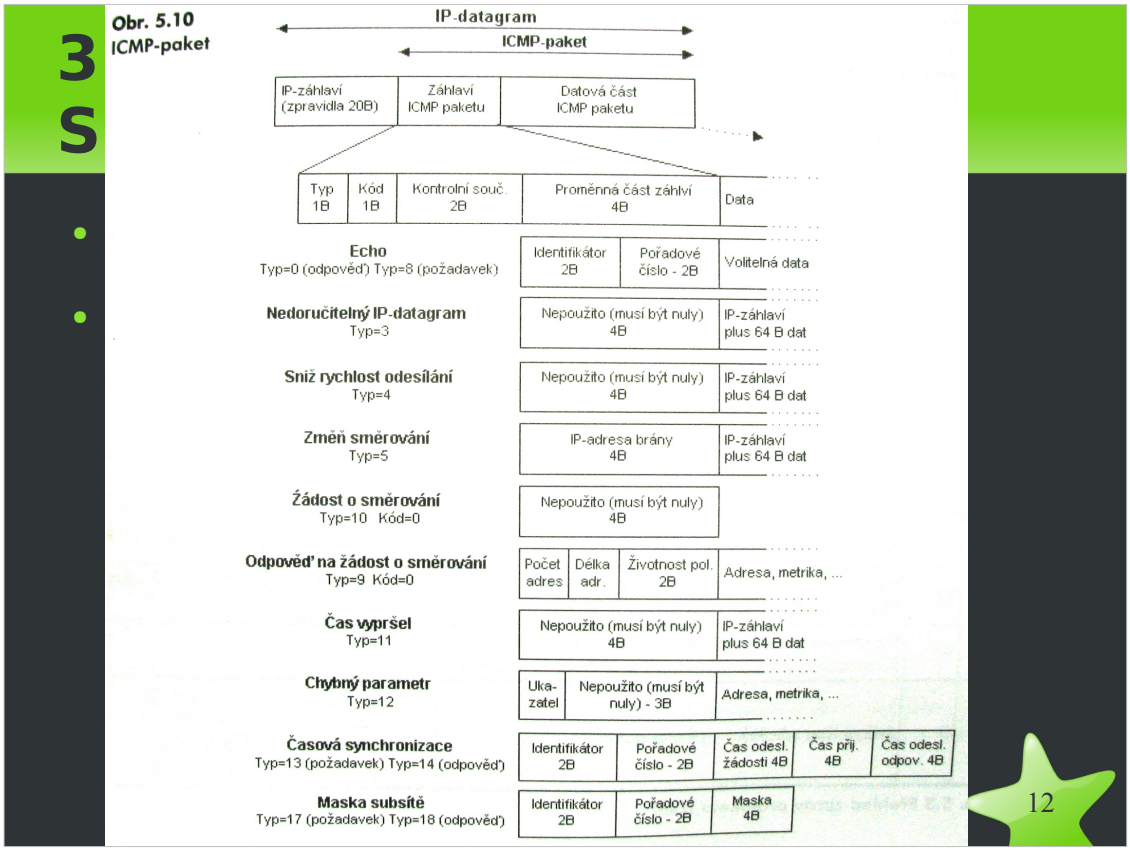
Změň směrování - když má směrovač poslat paket do stejné části sítě ze které přišel, tak jej odešle a současně pošle ICMP zprávu *změň směrování*. To může nastat když se počítače propojují do sítě, kde je více směrovačů, s položkou *default* = je nastaven jeden z těchto směrovačů nezávisle na tom, zda je tento optimální.

Žádost o směrování – počítač pošle oběžníkem žádost o směrování, a směrovač mu odpoví Odpovědí na žádost o směrování. Současně tuto odpověď vysílá náhodně v intervalu 450 až 600 sekund.

Čas vypršel – zahrnuje dva odlišné případy
kód 0 = TLL sníženo na 0, paker zřejmě zabloudil a bude zlikvidován
kód 1 = směrovač nemůže z fragmentů sestavic celý IP datagram
na tomto principu funguje windowsacky *tracert* nejdříve vyšle paket s TLL=1, příjde mu odpověď Čas vypršel, on si zapamatuje informace o směrovači. To provede třikrát a zprůměruje časy. Potom vyšle paket s TLL=2 a tak pokračuje dokud není paket doručen k cíli.

Žádost o masku – bezdisková stanice, která zná svou IP adresu (dostane ji přeba pomocí RARP) může požádat o masku sítě

Časová synchronizace – zdroj vyšle žádost a zapamatuje si kdy jí odeslal, až mu přijde odpověď, zjistí si čas (přijetí odpovědi) a z toho lze spočítat RTT (Roud Trip Time)



Vlastní formát ICMP zprávy se dovíjí od tohjo o jaký typ zprávy se jedná.

Echo – jednoduchý nástroj pro kontrolu dozažitelnosti bodu v síti. Tazatel vyšle paket žádost o echo na který je tázaný prvek odpovědět paketem ICMP *echo* viz program ping

Nedoručitelný IP datagram – nelze doručit.

Sniž rychlost odesílání – v případě, že směrovač je zahlcen a není schopen předávat všechny pakety, vysílá odesilatelům zprávy sniž rychlost odesílání. Jestli se odesílá na TCP, odesilatel sníží rychlost, v případě UDP je tato zpráva odesilatelem ignorována.

Změň směrování - když má směrovač poslat paket do stejné části sítě ze které přišel, tak jej odešle a současně pošle ICMP zprávu *změň směrování*. To může nastat když se počítače propojují do sítě, kde je více směrovačů, s položkou *default* = je nastaven jeden z těchto směrovačů nezávisle na tom, zda je tento optimální.

Žádost o směrování – počítač pošle oběžníkem žádost o směrování, a směrovač mu odpoví Odpovědí na žádost o směrování. Současně tuto odpověď vysílá náhodně v intervalu 450 až 600 sekund.

Čas vypršel – zahrnuje dva odlišné případy

kód 0 = TLL sníženo na 0, paker zřejmě zabloudil a bude zlikvidován

kód 1 = směrovač nemůže z fragmentů sestavic celý IP datagram

na tomto principu funguje windowsacky *tracert* nejdříve vyšle paket s TLL=1, příjde mu odpověď Čas vypršel, on si zapamatuje informace o směrovači. To provede třikrát a zprůměruje časy. Potom vyšle paket s TLL=2 a tak pokračuje dokud není paket doručen k cíli.

Žádost o masku – bezdisková stanice, která zná svou IP adresu (dostane ji přeba pomocí RARP) může požádat o masku sítě

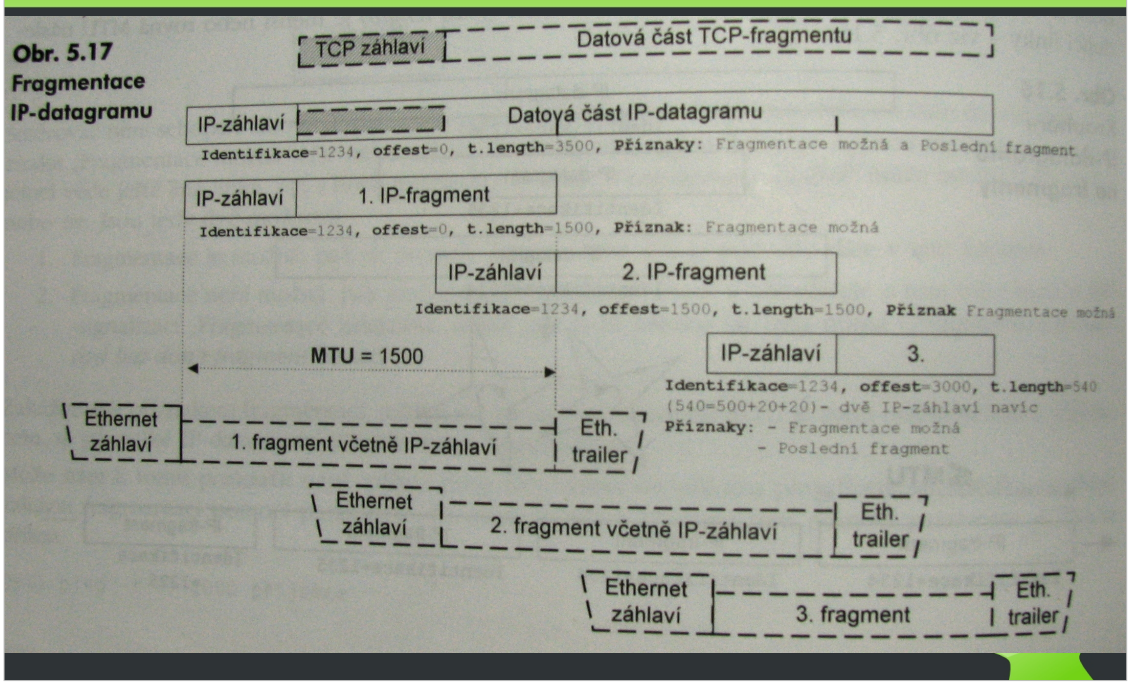
Časová synchronizace – zdroj vyšle žádost a zapamatuje si kdy jí odeslal, až mu přijde odpověď, zjistí si čas (přijetí odpovědi) a z toho lze spočítat RTT (Roud Trip Time)

3. Protokol IP Fragmentace

- Délka IP datagramu může být větší než délka linkového rámce
- Fragmentaci lze zakázat
  - je-li bit fragmentace nastaven, proběhne
  - bit není nastaven, odesilatel obdrží zprávu ”Fragmentation needed but don't fragment bit set”
- Datová část IP datagramu se rozseká a po kouskách se přenáší

to, zda k fragmentaci na jistém úseku dojde či nikoli lze jsistit windowsackym prikazem
PING -f -l delka_datagramu

3. Protokol IP
Fragmentace (2)



Každý fragment dědí identifikaci původního datagramu. U vyšších fragmentů je nastavován bit offset. Poslední fragment ná navíc aktivní příznak, že se jedná o poslední fragment.

Původní datagram smí sestavit pouze příjemce. Technicky by bylo možné aby jej sestavoval i následující router, ale to koliduje z koncepcí TCP/IP protokolu která dovoluje posílat každý paket jinou cestou.

Kazdý fragment nese původní IP záhlaví, hodnota fragment offset znamená kolik Bytů původního datagramu bylo již odesláno v předchozích fragmentech.

V principu lze fragmentovat i fragmenty.

Bezpečné aplikace fragmentaci zakazují. Router, který filtruje pakety na základě TCP totiž zahodí jen první fragment. V tom je přenášeno záhlaví TCP. V osatních fragmentch už není a proto jsou routerem propuštěny. Cílový počítač obdrží vše krom prvního paketu a vygenetuze zprávu, že z famentů nelze sestavit původní paket, kterou odesílá zpět. Pokud tuto zprávu router nezahodí, dozví se potenciální útočník, že na routeru probíhá filtrování na úrovni TCP.

3. Protokol IP
Volitelné položky IP záhlaví

- 1. Zaznamenávej směrovače
- 2. Zaznamenávej čas
- 3. Explicitní směrování
- 4. Striktní explicitní směrování
- 5. Upozormění pro směrovač
- 6. Bezpečnostní omezneí podle normy RFC-1108

Zaznamenávej směrovače – zaznamenávají se odchozí ip adresy všech uzlů, kterými IP datagram cestuje. To je rozdíl oproti třeba příkazu tracert, kdy se dozvím jen adresy routerů z mojí strany.

Zaznamenávej čas – obdoba zaznamenávej směrovače s tim rozdíelm, že každý směrovač do záhlaví zapíše časové razítko

Explicitní směrování – umožňuje zadat přes jaké routery má paket jít. To je dobré pro hackery.

Upozornění pro směrovač – Když je třeba upozornit směrovač, třeba na nejakou změnu v síti, tak se mu tato informace posílá IP datagramem. Směrovače na cestě s tím zachazejí jako s normálním datagramem a vůbec netuší, že jsou v tom informace, které by se jim taky mohly hodit. Proto se nastavuje tento příznak a směrovače se, když to umějí, do datové části datagramu také podívají a v případě, že se jim přenášená informace hodí, zařídí se podle toho a datagram posílají dál (next hop)

3. Protokol IP
Protokoly ARP a RARP

- Stanice na síti zná svou IP adresu, zná i IP adresu příjemce a je tedy schopna sestavit IP datagram, kam ho ale poslat?
- Řešení je ARP
- RARP – opačný problém

Sestavený IP datagram musí být zabalen do linkového rámce. Aby bylo možné tento rámec vytvořit, je třeba znát linkovou adresu příjemce i odesilatele. Odesilatel jsem já, to je v pohodě, ale jakou linkovou adresu má příjemce (znám jeho IP adresu)

ARP – Do LAN se vyšle oběžník ”já stanice A s Ipa hledám linkovou adresu stanice B s Ipb kdo mi s tím pomůže”, na to zareaguje stanice B a v odpovědi mi sdělí svou HW adresu. Na tu potom linkový rámec pošlu.

Filtrace ARP – není to filtrace ale tváří se to tak, jde o to, že jedna LAN se tváří jako dvě oddělené sítě. Například síť v budouvě využívá nekolik firem. Aby se počítač z firmy B netvářil jako počítač firmy A docílíme tím, že naplníme ARP-cache statickými adresami. Server potom odpovídá pouze na linkovou adresu pc firmy A.

proxy ARP- když je v cestě mezi stroji A a B směrovač, tedy počítače A a B jsou v různých segmentech sítě, nelze pomocí ARP získat adresu B. Proto se na směrovači pouští proxy ARP, a směrovač potom na takový dotaz odpoví svou HW adresou.

RARP – reverzní ARP jeho využití není příliš časté, může ho být potřeba třeba v případě, že bezdisková stanice se připojí do sítě a nezná svou IP adresu. V současnosti je ale nahrazován komplexnějším DHCP

3. Protokol IP
Protokol IGMP

- Podobně jako ICMP je služebním protokolem
- Řeší problémy oběžníků na LAN
  - Skupiny, jejich členové
  - Dva pracovní režimy směrovače
    - Dotazovač
    - Posluchač

Pokud přijde na směrovač oběžník, není nutné aby jej směrovač vpustil do LAN, pokud tam ovšem nemá nějaké příjemce. Na jejich počtu nezáleží, důležité je, zda tam jsou či nikoli. Příjemci se směrovači nahlasí. Například stanice A chce poslouchat muziku z rozhlasové stanice 266.1.1.1, vyšle počítač požadavek na členství ve skupině 266.1.1.1

Když je v síti více směrovačů, usporádávají se do hiearchije takovým způsobem, že jeden je v režimu dotazovač = posíla na LAN dotazy ohledně členství ve skupinách a ostatní jsou v režimu posluchčů = jen poslouchá a když j v síti aktivní dotazovač tak tento nevstupuje do hry.

Každý router se spouští jako dotazovač, když ale zjistí, že v síti již dotazovač je, přepne se do módu posluchače. Dotazovač pravidelně kontroluje členství ve skupinách. Tím se docílí toho, že když někdo vytáhle počítač, který byl jediným členem nějaké skupiny, ze zásuvky a on tedy nectihne odeslat IGMP paket se žádostí o zrušení členství, tak se jeho členství po určité době zruší automaticky (nikdo neodpoví na dotaz ”kdo je clenem skupiny XXX?”)

3. Protokol IP
IPv6

- 16 Byte na IP adresu místo původních 4
- Filozoficky nový pohled na stavbu IP datagramu
- V záhlaví už není kontrolní součet
- Některé údaje hlavičky se přesouvají do nepovinných
- Definován v roce 1995 (cca 15 let po IPv4)

4. IP adresa

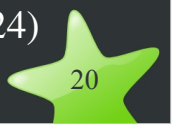
- velikost: 4 Byte
- interpretace:
  - dvojková 10101010.01010101.11111111.00000000
  - desítková 170.85.255.248
  - šestnáctková aa.55.ff.f8

IP adresa se skládá ze dvou částí:
adresa sítě a
adresa počítače

Historie se dělí na dvě etapy. Nejdříve se IP adresy dělily do tříd
A – 0s ss ss ss ~ 126 sítí po 2^24 -2 počítačích
B – 10 ss ss ss ~ 2^14 sítí po 2^16 -2 počítačích
C – 11 0s ss ss ~ 2^22 sítí po 128 -2 počítačích
D – 11 10 ss ss ~ zbytek adresy se už nedělí, tvoří oběžníkový multitask
E – Zbytek adres je rezerva

4. IP adresa

- v roce 1993 vyšly normy RFC-1517 až 1520
- na sítě se přestalo dívat přes třídy ale dívá se na ně výhradně přes síťové masky
- jaká je adresa sítě, ve které je zapojen počítač 10.0.0.239, maska je 255.255.255.240?
  - 00001010.00000000.00000000.11101111 (10.0.0.239)
  - 11111111.11111111.11111111.11110000 (255.255.255.240)
  - 00001010.00000000.00000000.11100000 (10.0.0.224)



Síťová maska – určuje jaké bity IP adresy jsou bity identifikace sítě a kde jsou nuly, tak to znamená že to jsou bity identifikující počítač.

Masky pro jednotlivé typy sítí

A 255.0.0.0
B 255.255.0.0
C 255.255.255.0

podle masky lze určit adresu sítě tak, že se IP adresa počítače vynásobí (bitově) maskou sítě

Je dobrým zvykem, že maska je složena z jedné strany z jedniček a dokončena nulami. V principu je možné aby jedničky a nuly byly přeházené ale nedělá se to, potom by interval IP adres nebyl intervalem ale jakousi vybranou posloupností a to by znesnadnilo práci správci sítě a neslo by to s sebou další negativa... Směrovače by ale s takovou síťovou maskou problém neměly.

4. IP adresa

- speciální IP adresy
  - 0.0.0.0 = tento počítač na této síti
  - 00...0.počítač = počítač na této síti
  - síť.00...0 = adresa sítě jako takové
  - síť.11...1 = všeobecný oběžník zaslaný do sítě
  - 1.1.1.1 = všeobecný oběžník na lokální síti
  - 127.cokoli = programová smyčka, nikdy neopouští počítač

4. IP adresa

- Autonomní systémy a supersítě
  - internet = poskytovatelé, kteří si předávají data mezi sebou
  - poskytovatelé žádají o intervaly IP adres
  - poskytovatelé jsou správci autonomních systémů
- Proč používat intervaly adres?

V rámci autonomních systémů se používají intervaly adres. To je výhodné proto, že interval adres lze snadno agregovat do jedné adresy supersítě a ta potom ve vzdáleném směrovači vystupuje jako jedna položka.

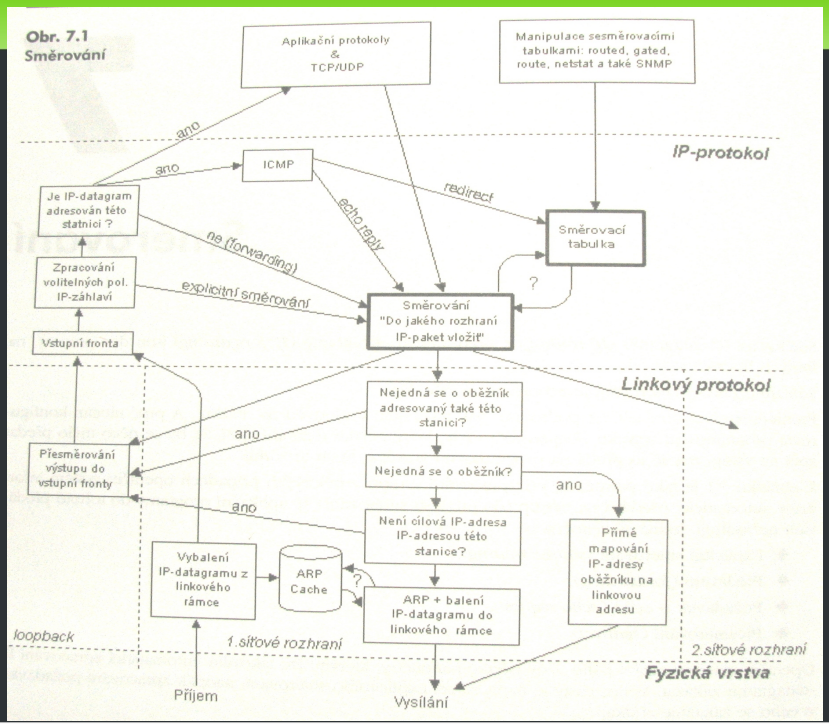
Agregace je snadná:
máme interval 194.149.96.0 až 194.149.128.0, potom se adresa supersítě agreguje na 194.149.96.0 s maskou 255.255.224.0 (resp. 194.149.96.0/19)

4. IP adresa

- Nečíslované sítě
- OBR 6.7

Nečíslované sítě – pokud jsou směrovače propojeny např. seriovým rozhraním, není třeba plýtvat IP adresou ale dva směrovače a jejich spojení považujeme za jeden virtuální směrovač.

5. Směrování



Směrování je velice podobné třídění dopisů na poště. Tam je třídící stůl, v něm jsou díry a u každé díry je napsáno jméno města a pod stolem je přidělaný pytel, do kterého díra ústí. Úředník bere dopis po dopisu přečte si město, kam je tento určen a hodí jej do patřičné díry.

Směrovač je analogie. Zjednodušeně jde říci, že směrovač předává IP datagramy z jednoho síťového rozhraní do jiného. Do jakého – to určují směrovací tabulky

5. Směrování

- příklad směrovací tabulky

Síť	Maska	Next Hop	Síťové rozhraní	Metrika
192.168.1.0	255.255.255.0	192.168.254.5	Seriál 1	4
10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0
10.5.1.0	255.255.255.0	10.10.10.2	Seriál 2	3
10.5.0.0	255.255.0.0	10.5.5.5	Seriál 1	2
…				
0.0.0.0	0.0.0.0	10.10.10.2	Seriál 2	1

V prvním sloupci je IP adresa cílové sítě, dále následuje maska, IP kam se to má poslat (next hop) a síťové rozhraní (jaká díra ve stole z předchozího slide) Metrika ta prijde na řadu v případě, že do cílové sítě existuje několik spojení.

Jak to teda probíhá?

1. 192.168.1.0 – 255.255.255.0 – 192.168.254.5 – serial 1 – 4
vynasobenim vznikne 10.5.2.0 to je jiné než 192.168.1.0 takže se jde na další řádek

2. 10.1.2.0 – 255.255.255.0 – lokalni rozhrani – ethernet – 0
vynasobenim vznikne 10.5.2.0 to je jiné než 10.1.2.0 takže se jde na další řádek

3. 10.5.1.0 – 255.255.255.0 – 10.10.10.2 – serial 2 – 3
vynasobenim vznikne 10.5.2.0 to je jiné než 10.5.2.0 takže se jde na další řádek

4. 10.5.0.0 – 255.255.0.0 – 10.5.5.5 – serial 1 – 2
vynasobenim vznikne 10.5.0.0 a proto se to pošle do serial 1, pokud by se nejednalo o seriovou linku, potom se protokolem ARP se zjisti HW adresa zarizeni s IP 10.5.5.5

Více specifické adresy mají přednost

na konci se uvadi sit 0.0.0.0 s maskou 0.0.0.0 což vyhovuje vždy tam se datagram posílá pokud nevyhovuje žádné z předchozích podmínek. Tento řádek tam nemusí být.

6. TCP a UDP

- TCP je spojovaný protokol
- Oproti IP je na vyšší vrstvě
- IP přepravuje data mezi dvěma počítači libovolně umístěnými v síti, TCP mezi aplikacemi na těchto počítačích

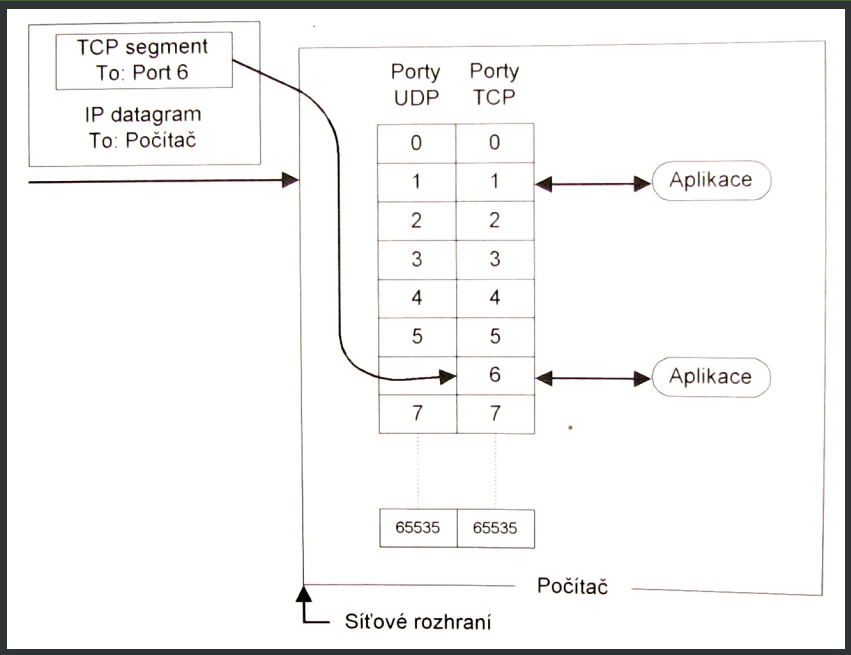
Protokoly TCP a UDP odpovídají transportní vrstvě. TCP dopravuje data pomocí tzv. TCP segmentů, které jsou adresovány jednotlivým aplikacím. UDP k tomu používá UDP datagramy.

TCP je spojovný, příjemce potvrzuje přijímaná data. V případě ztráty dat si příjemce vyžádá zopakování přenosu.

Jako adresa je použit port. Rozdíl mezi IP adresou a portem je obdobný jako rozdíl mezi poštovní adresou (Město, ulice, dům) ~ IP adresa, a jménem osoby, jíž má být zásilka doručena ~ port. Porty nabývají hodnot 0 – 65 535, pričemž 0 až 1023 jsou vyhrazeny pro systém, normální uživatelská aplikace je nikdy přidělené nedostane.

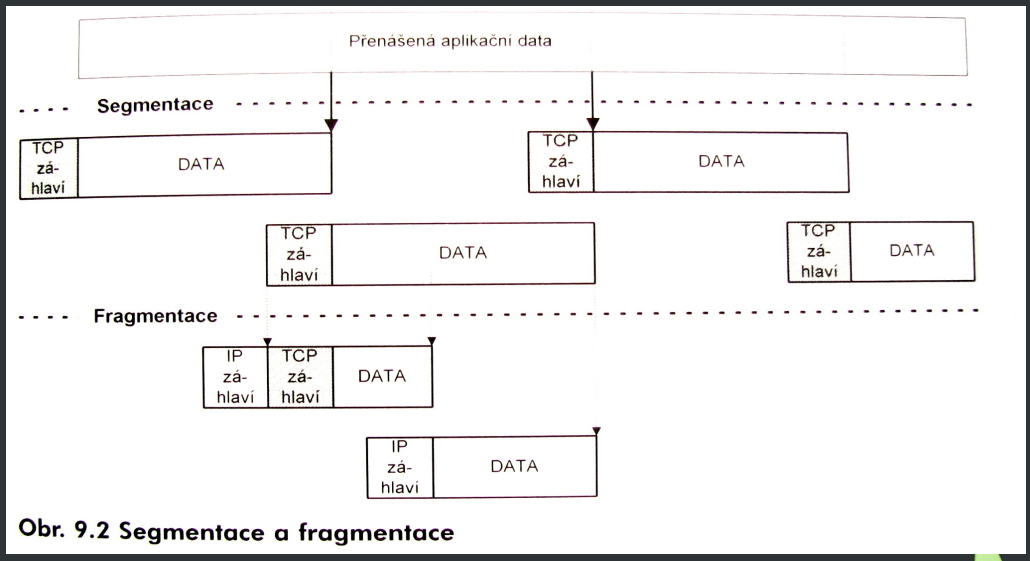
TCP navazuje plně duplexní spojení

6. TCP a UDP porty



Porty TCP a UDP jsou na sobě nezávislé – port 80UDP je jiným portem než 80TCP

6. TCP a UDP
Segmentace

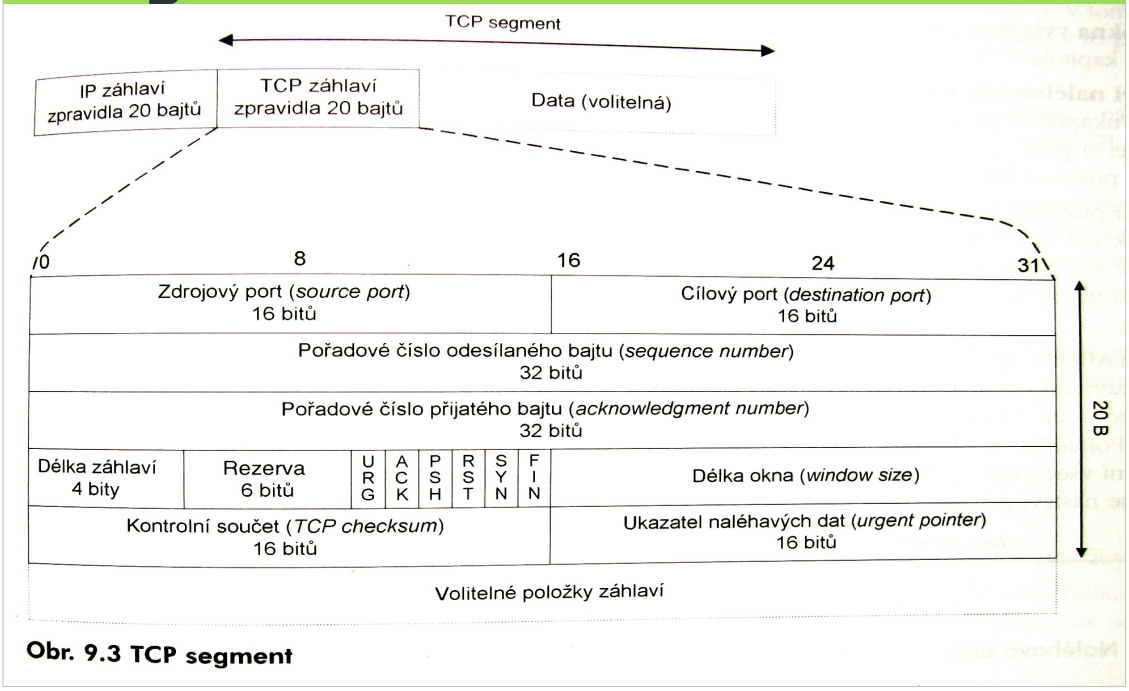


Obr. 9.2 Segmentace a fragmentace

Základní jednotkou v přenosu TCP je segment. Chceme=li např. přenést soubor o velikosti třeba 2GB, je třeba jej rozdělit. Velikost IP paketu může být max 64kb. Dada se tedy rozdělí do patřičných kousků a ty se postupně odesílají.

Jednotlivé segmenty se číslují (32bit), po přetečení indexu segmentu se začíná znovu od nuly. Při navazování spojení nemá první segment identifikátor 0 ale libovolné náhodné číslo z daného intervalu.

6. TCP a UDP
Segment TCP



Obr. 9.3 TCP segment

Zrdojový port – port odesilatele segmenu
Cílový port – port příjemce segmentu, zdrojový a cílový port nemusí být stejné hodnoty

Pořadové číslo odesilaného segmentu – nese pořadové číslo prvního Bytu TCP segmentu v toku dat od odesilatele k příjemci. V opačném směru je číslování jiné, začíná od náhodně zvoleného čísla.

Pořadové číslo přijímaného Bytu – číslo následujícího Bytu, který je příjemce ochoten přijmout = přijal jsem vše až po tuto hodnotu-1.

Délka záhlaví – podobně jako u IP, záhlaví může obsahovat nepovinné položky

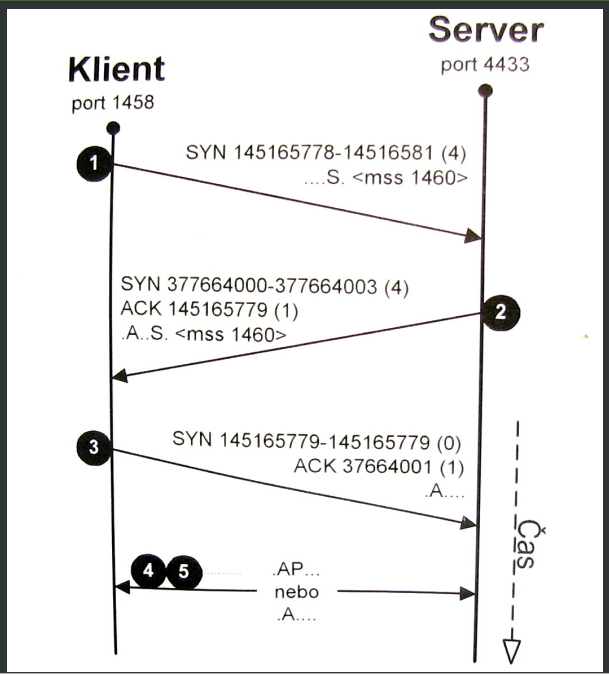
Delka okna – Přírůstek přijímaného Bytu, který bude příjemcem ještě akceptován viz dále

Ukazatel naléhavých dat – ukazuje na konec dat, které se mají přednostně zpracovat. Například zrušení odesílání souboru. Normálně by se v sekvenci celý soubor přijal a na konci by se zjistilo, že se má smazat.

Příznaky:
URG = segment nese naléhavá data (souvisí s ukazatelem naléhavých dat)
ACK = je 0 pouze u prvního segmentu, kde odesilatel navazuje spojení
PSH = signalizace, že segment nese aplikační data
RST = odmítnutí TCP spojení
SYN = odesilatel začíná novou sekvenci číslování
FIN = Odesilatel ukončil odesílání dat

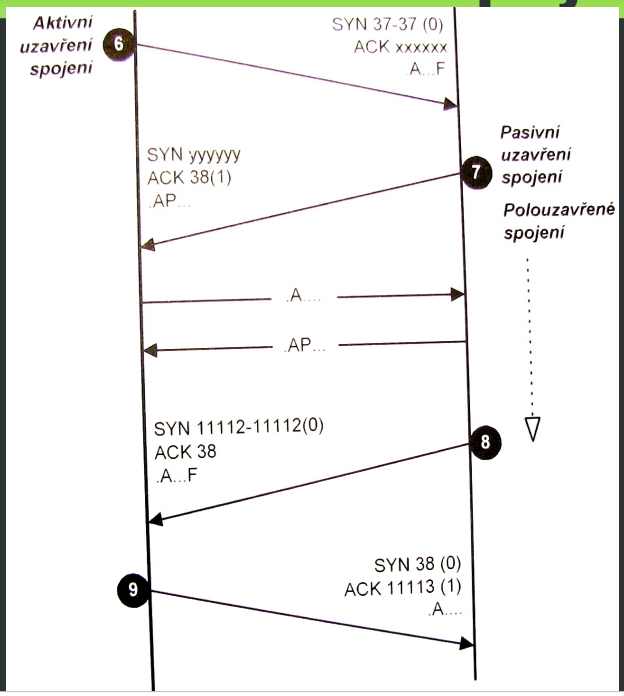
Kontrolní součet – počítá se nejen z celého TCP segmentu ale i s některých položek IP záhlaví

6. TCP a UDP
Navázání spojení



Součástí při navazování spojení je i MSS = maximum segment size klient a server se na zacatku domluví na maximální velikosti TCP segmentu.

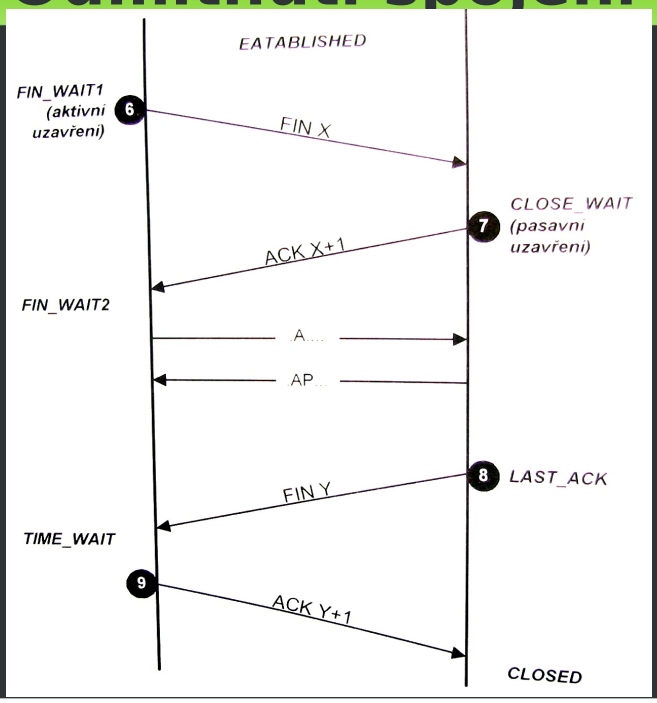
6. TCP a UDP
Ukončování spojení



Ukončit spojení může server i klient.

Rozlišujeme aktivní a pasivní uzavírání spojení. Aktiní znamená, že jedna strana vyšle segment s příznakem FIN. Druhá ale může s odesílaním pokračovat, tomu se říká polouzavřené spojení (již není duplexní). To trvá až do doby, kdy už nemá co zbývající aktivní počítač co odeslat. Ukončí tedy také polouzavřené spojení a tuto činnost nazýváme pasivním ukončováním spojení.

6. TCP a UDP
Odmítnutí spojení



nastává když

1. klient požaduje spojení na portu, kde žádný server neběží. (UDP je toto oznámeno ICMP protokolem)
2. Již navázané spojení je odmítnuto
    a. Řádné ukončení je poměrně dlouhé a proto se někdy používá to, že poté co se přenesou všechna data se poslední potvrzení odečle s příznakem RST
    b. Pokud jedna strana zjistí, že protějšek je nedůvěryhodný např. při komunikaci přes SSL

6. TCP a UDP
Technika zpoždění odpovědi

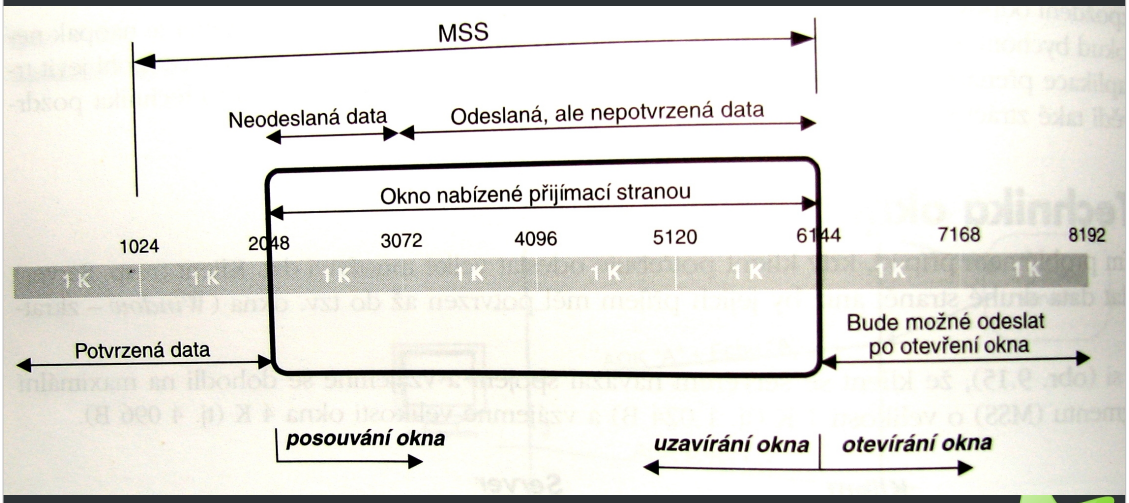
- Telnet: uživatel píše příkazy, jení třeba odesílat po znacích, stačí v jistých kvantech
- Operační systém sustí hodiny s taktem < 500 ms
- Nagleův algoritmus
- Nevhodné pro X-server (trhání myši)

nastává když

1. klient požaduje spojení na portu, kde žádný server neběží. (UDP je toto oznámeno ICMP protokolem)
2. Již navázané spojení je odmítnuto
    a. Řádné ukončení je poměrně dlouhé a proto se někdy používá to, že poté co se přenesou všechna data se poslední potvrzení odečle s příznakem RST
    b. Pokud jedna strana zjistí, že protějšek je nedůvěryhodný např. při komunikaci přes SSL

6. TCP a UDP
Technika okna

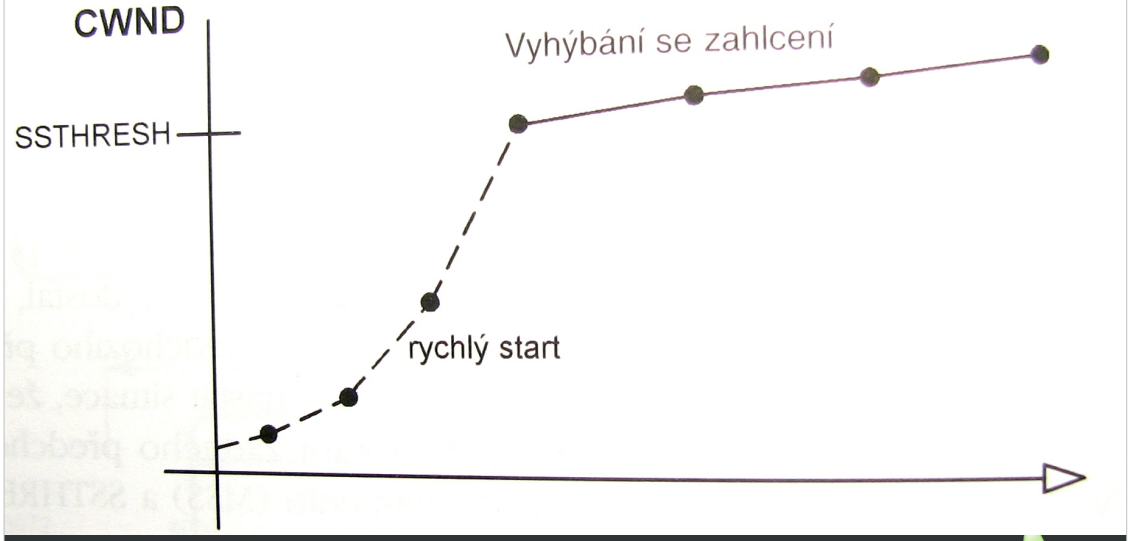
- Pro přenos velkého množství dat



Pri navazování spojení se obě strany nedohadují pouze na max velikosti TCP segmentu ale dohodnou se i na maximální velikosti okna. To udává kolik nepotvrzených segmentů může odesilatel do sítě vyslat.

Příklad okno je 4K, velikost MSS je 1K
pokud klient nekdostane potvrzení dorušených segmentů a již odeslal počet segmentů velikosti okna, vyčkává na potvrzení.

6. TCP a UDP
Zahlcení sítě



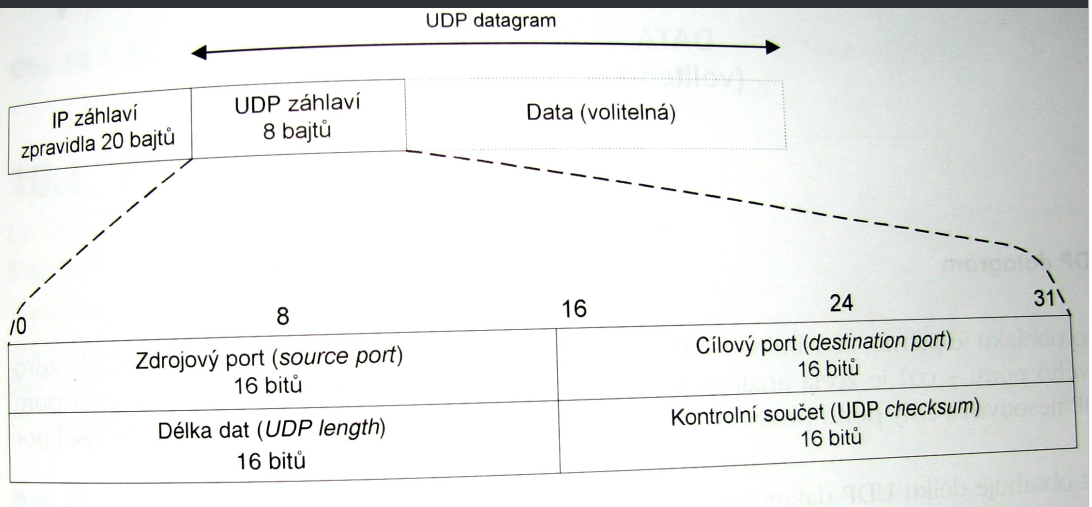
Velikost okna se v průběhu spojení může měnit.

Rychlý start znamená, že se okno zvětšuje podle řady 2^n až dokud nedojde k zahlcení sítě (to se pozná podle toho, že se segmenty začnou ztrácet). Poté se nastaví hodnota SSTHRESH která má velikost prvku n-1 ve zmíněné řadě.

Okno je ale možná přeci jen malé – chci okno co největší protože ovlivňuje rychlost přenášení dat. Proto ho z hodnoty SSTRESH ještě zkusím pomalu zvětšovat o hodnotu MSSxMSS/CWND + MSS/8

Když se TCP segmenty v síti ztrácejí, resp. když předběhme jeden segment druhý, dojde k zopakování potvrzení podledního v řadě správně přijatého segmentu. Odesílací strana si toho nevšímá (v internetu se to stává, protože každý paket může jít jinou cestou) až do doby, kdy se jeden segment potvrdí 3x, pak odesílací strana zopakuje odeslání segmentu, o kterém se přijímací strana domnívá, že se ztratil.

6. UDP



Obr. 10.1 Záhlaví UDP datagramu

Je to jednodušší obdoba TCP.

Oproti TCP není spojovanou službou

Jednodušší záhlaví, nepovinný výpočet kontrolního součtu.

Fragmentace se nedoporučuje ale je možná:
například v komunikaci DNS-klient, se nejdříve klient dotáže pomocí UDP. Dostane odpověď a pokud se tato nevejde do IP protokolu, odečle server DNS jen část a označí ji jako neúplnou informaci. Pokud ta informece klientovi nestačí, naváže s DNS spojení pomocí TCP.

UDP vhodný pro přenos hlasu a RLT audio nebo video.

8. Přehled nejdůležitějších aktivních prvků

- Opakovač (*repeater*)
  - pracuje na fyzické vrstvě
  - zesilovač
- Most (*bridge*)
  - má představu o topoligii sítě = pracije na linkové vrstvě
  - komunikaci v rámci segmentu ponechává, mimo segmet šíří do všech zbývajících segmentů sítě
- Směrovač (*router*)
  - pracuje na síťové vrstvě, zná topologii sítě
  - umí rozhodnout kam paket poslat
  - viditelná kompinenta sítě

poznamka

Informační zdroje

- *Libor Dostálek, Alena Kabelová:* Velký průvodce protokoly TCP/IP a systémem DNS (*computer press, Praha, 2002*)
- *Jiří Peterka: WWW.EARCHIV.CZ*

poznamka