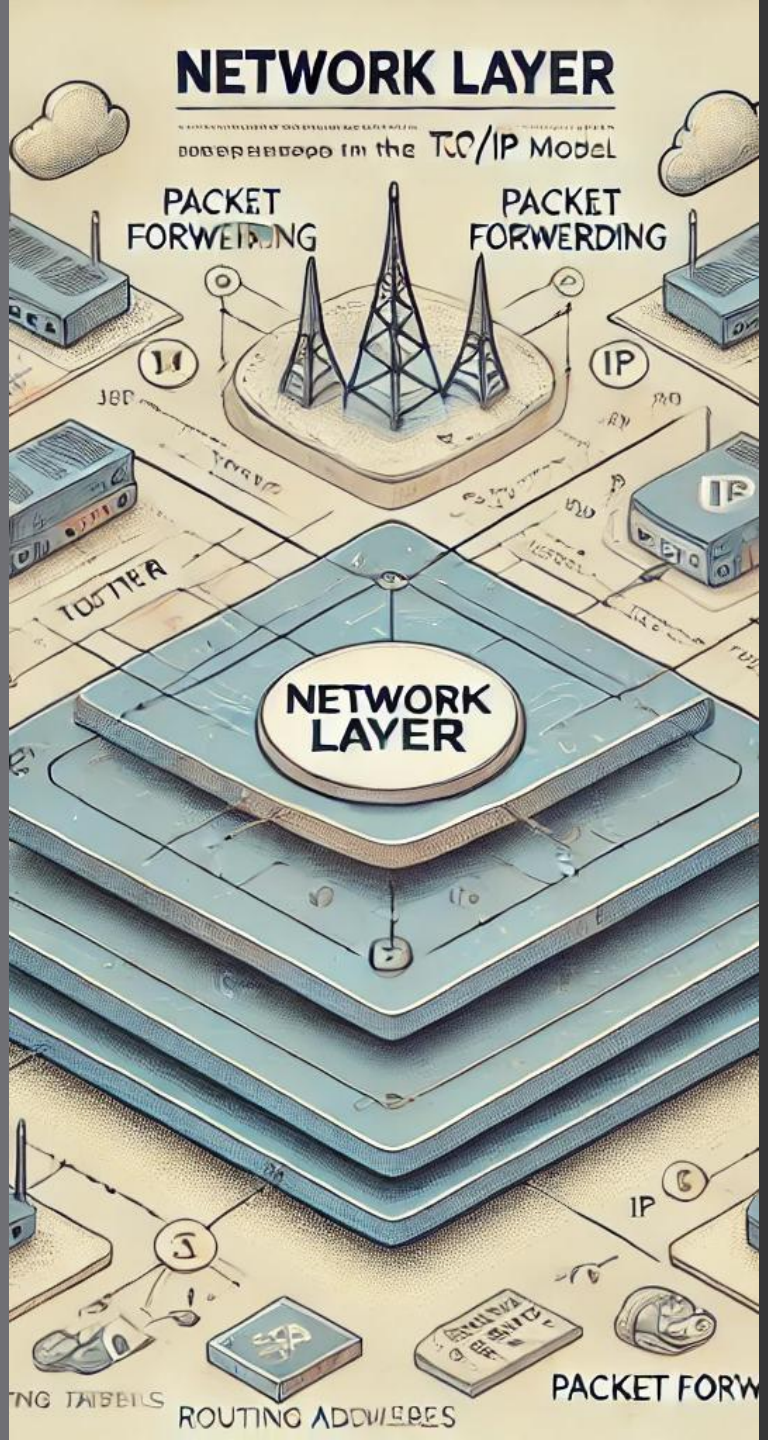


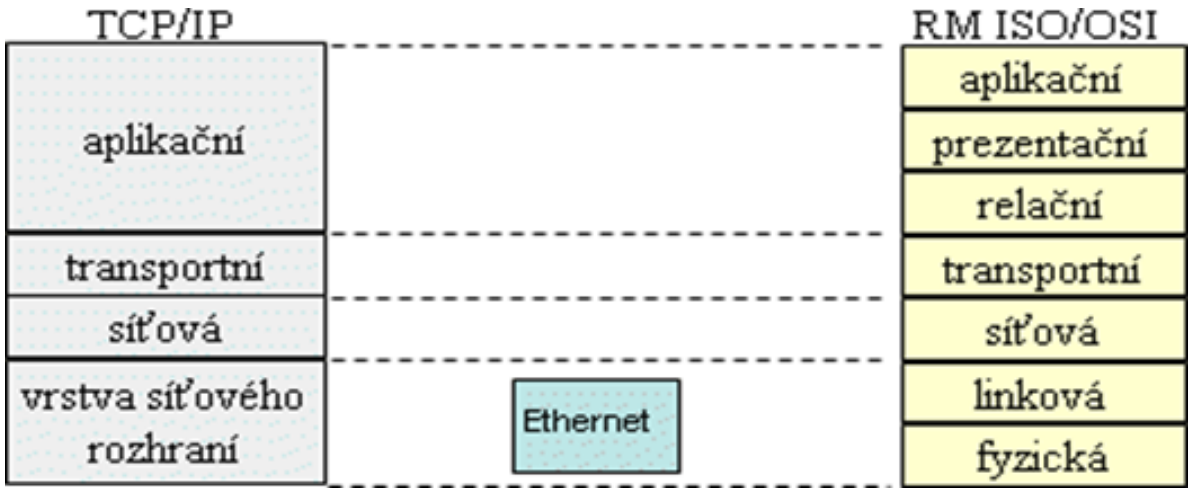
Síťová vrstva a protokol IPv4

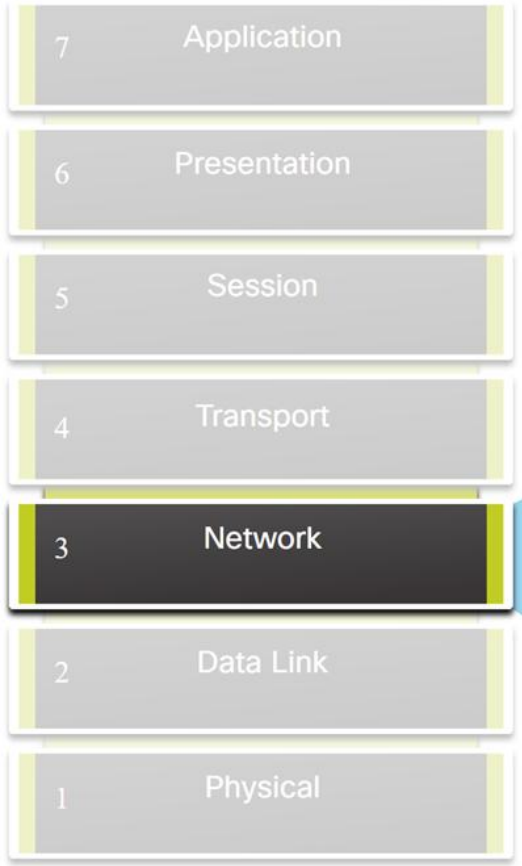
Ing. Petr Orvoš

SOŠ a SOU NERATOVICE

Opakování z předchozí výuky

Síťová vrstva neboli OSI vrstva L3, poskytuje služby, které umožňují koncovým zařízením vyměňovat si data napříč sítěmi.





- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

Datagram vs. paket – v čem je rozdíl?

✅ Datagram - je konkrétní typ paketu používaný u nespojovaného přenosu. IPv4 pracuje s datagramy, a to je správný technický termín.

📦 **Paket (packet) - je obecný výraz pro jednotku dat, která se přenáší po síti.**

„Paket“ může být:

- *datagram (v nespojované síti), paket (ve spojované síti)*
- *frame (na linkové vrstvě),*
- *segment (v TCP),nebo prostě „něco, co nese data“.*

🤷 Proč tedy všichni říkají „paket“?

V běžné praxi se slangově říká "paket" i tehdy, když jde technicky o datagram, podobně jako říkáme „USBčko“, i když myslíme flash disk.

Možné způsoby fungování síťové vrstvy

Přepojování paketů (packet switching)

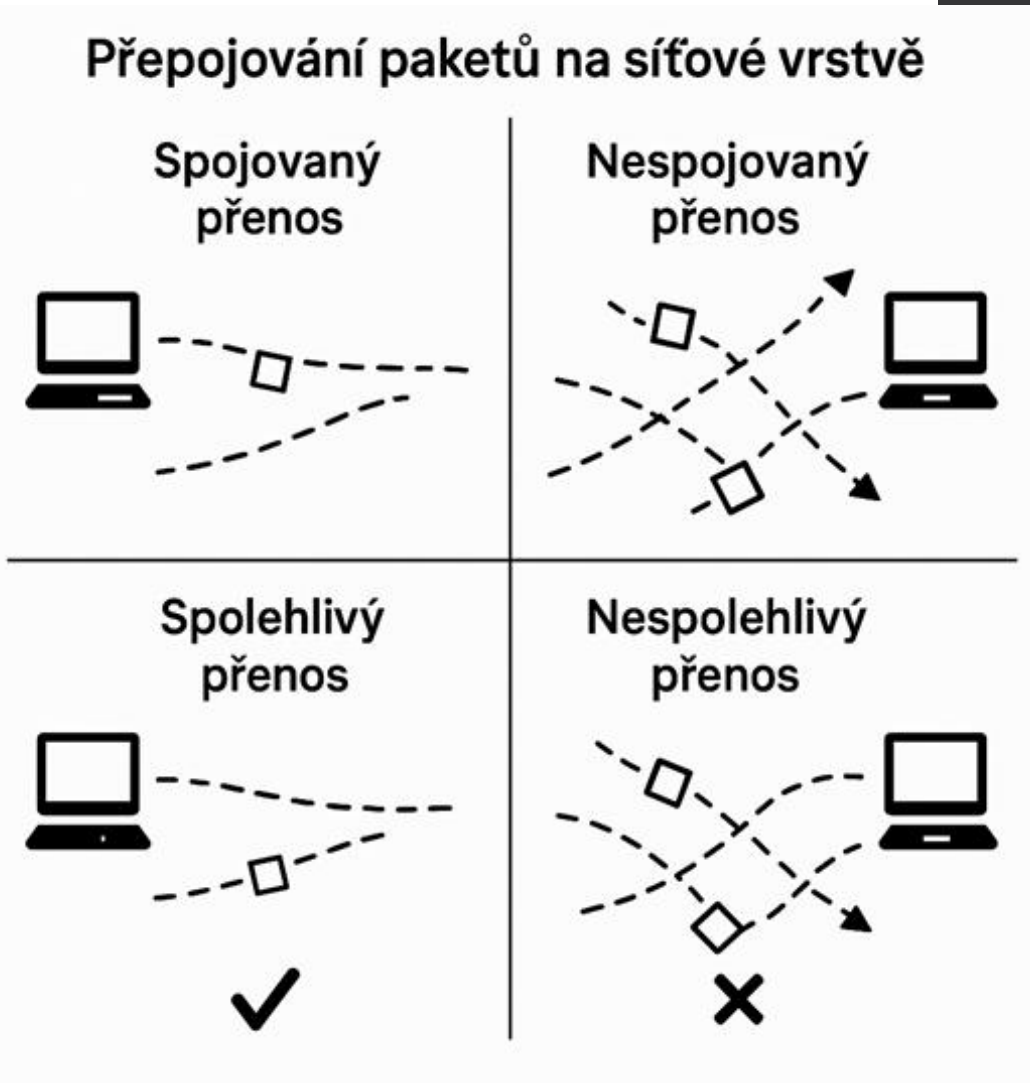
Data jsou rozdělena na **pakety (datagramy)**, které se posílají jednotlivě.

Každý paket obsahuje:

- **adresu odesílatele**
- **adresu příjemce**
- **číslo paketu**
- případně další metadata

Pakety mohou **putovat různými cestami** sítí (na rozdíl od spojového přenosu - okruhy).

Na cílové straně se pakety **znovu složí** (nebo také nemusí – záleží na vyšší vrstvě).



Možné způsoby fungování síťové vrstvy

Spojovaný přenos (connection – oriented)

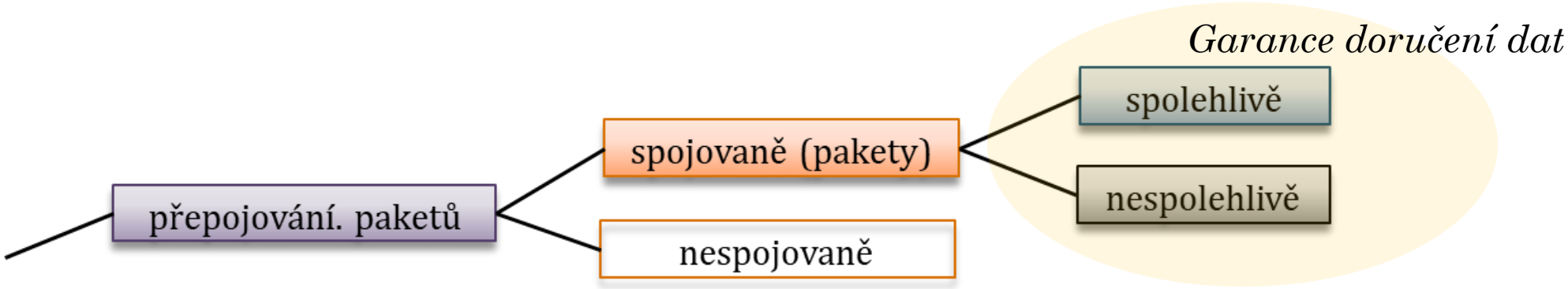
přenášený blok se obecně označuje jako ***paket***

- **před zahájením přenosu** se vytvoří spojení (virtuální cesta) od odesílatele k příjemci
- všechny pakety jdou **stejnou cestou a mají identifikátor cesty**

Výhody:

- větší **kontrola a stabilita**
- méně problémů s pořadím paketů

Spolehlivý přenos znamená, že je kontrolováno doručení, pořadí a integrita dat.



Příklady:

- MPLS (na síťové vrstvě)
- na transportní vrstvě to zajišťuje například TCP (ale to už je vyšší vrstva)

Spojovaný přenos může být nespolehlivý, pokud síť nijak nekontroluje ztrátu nebo chyby v paketech.

Možné způsoby fungování síťové vrstvy

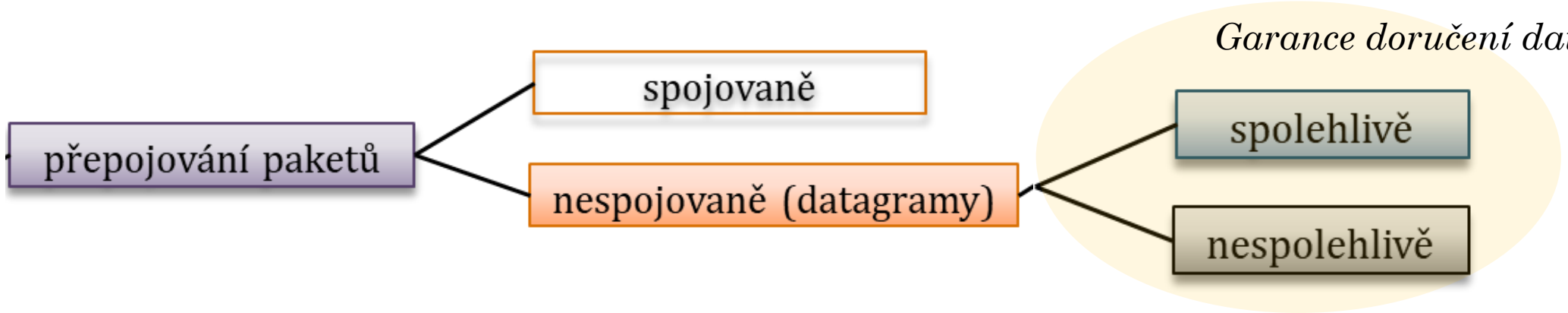
Nespojovaný přenos (connectionless)

přenášený blok se obecně označuje jako ***datagram***

- pakety jsou posílány nezávisle (každý přenášený blok má ve své hlavičce celou adresu svého příjemce)
- každý paket může jít jinou cestou - k hledání cesty dochází pro každý blok znovu (v každém směrovači „po cestě“)
- síť negarantuje doručení, pořadí ani že vůbec dorazí

Výhody: jednodušší, rychlejší, méně režie (overhead)

Příklady: IP (IPv4/IPv6) je nespojovaný protokol a nespolehlivý



Možné způsoby fungování síťové vrstvy

Typ přenosu	Charakteristika	Příklad
Přepojování paketů	Data v blocích, každé může jít jinou cestou	Internet
Spojovaný přenos	Vytvoří se trvalé spojení	MPLS, telefonní síť
Nespojovaný přenos	Každý paket jde samostatně	IP
Spolehlivý přenos	Potvrzení, znovuodeslání, kontrola pořadí	TCP (transportní vrstva)
Nespolehlivý přenos	Žádná garance doručení	IP (síťová vrstva)

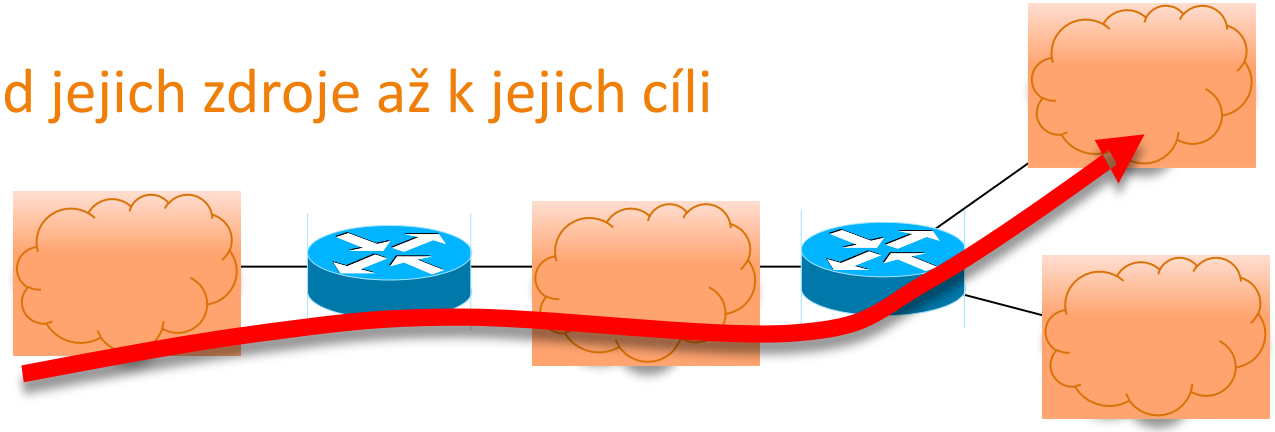
Kombinace přenosů:

Spojení	Spolehlivost	Příklad
Spojovaný	Spolehlivý	Telefonní hovor, TCP přes MPLS
Spojovaný	**Nespolehlivý**	X.25 (bez korekce), některé WAN
Nespojovaný	Spolehlivý	TCP přes IP (běžný internet)
Nespojovaný	Nespolehlivý	IP protokol samotný

Hlavní úkoly síťové vrstvy

hlavní úkol: směrování (routing)

- dopravovat bloky dat (pakety) od jejich zdroje až k jejich cíli
- i přes mezilehlé uzly / celé sítě
- zahrnuje:
- **volbu směru (routing)**
  - směrování v užším slova smyslu: rozhodování o cestě / směru dalšího přenosu
- **cílené předávání (forwarding)**
  - samotná manipulace s jednotlivými pakety („předání dál“ ve zvoleném směru)
- obě tyto funkce jsou obvykle realizovány společně, v zařízení zvaném **směrovač (router)**
  - ale mohou být také oddělené
    - směrování (rozhodování) může být řešeno centrálně, distribuovaný je pak pouze forwarding



Další úkoly síťové vrstvy

- zajištění podpory kvality služeb (QoS, Quality of Service)

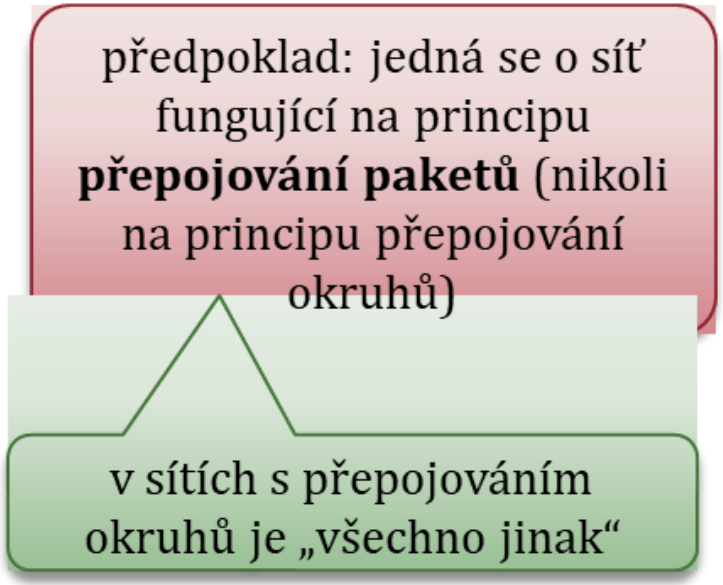
  obvykle: ve spolupráci s dalšími vrstvami, např. transportní

- předcházení zahlcení (congestion control)

  eliminace stavů, kdy je přenosová síť zahlcena a nestíhá přenášet všechny požadované pakety

- řízení toku (flow control)

  předcházení tomu, aby odesilatel zahltil příjemce



Operace protokolů síťové vrstvy

- **Adresování koncových zařízení** – koncová zařízení musí být pro identifikaci v síti nakonfigurována s unikátní IP adresou.
- **Zapouzdření** – síťová vrstva zapouzdřuje datovou jednotku protokolu (PDU) z transportní vrstvy do paketu. Proces zapouzdření je prováděn zdrojem paketu IP.
- **Směrování (routing)** – síťová vrstva poskytuje služby pro směrování paketů na cílového hostitele v jiné síti. **Úlohou směrovače (routeru) je vybrat nejlepší cestu a směrovat pakety směrem k cílovému hostiteli v procesu známém jako směrování.** Každý směrovač, kterým paket projde, aby dosáhl cílového hostitele, se nazývá skok **(hop).**
- **De-encapsulation** – když paket dorazí do síťové vrstvy cílového hostitele, hostitel zkontroluje IP hlavičku paketu. Pokud cílová adresa IP v hlavičce odpovídá její vlastní adrese IP, je hlavička protokolu IP z paketu odstraněna. Poté, co je paket de-encapsulován síťovou vrstvou, je výsledný PDU vrstvy 4 předán příslušné službě na transportní vrstvě.

Proces zrušení zapouzdření je prováděn cílovým hostitelem paketu IP.

Protokoly síťové vrstvy (TCP/IP model)

IPv4 – starší, stále široce používaná verze (32bitové adresy)

IPv6 – novější verze s větším adresním prostorem (128bitové adresy)

ICMP (Internet Control Message Protocol) -používán pro chybová hlášení a diagnostiku (např. ping, traceroute)

IGMP (Internet Group Management Protocol) - správa multicastových skupin v IPv4 sítích

MLD (Multicast Listener Discovery) - ekvivalent IGMP pro IPv6

ARP (Address Resolution Protocol) - převod IP adresy na MAC adresu v lokálních sítích

NDP (Neighbor Discovery Protocol) - nahrazuje ARP v IPv6 sítích, poskytuje i další funkce (např. zjišťování směrovačů)

BGP (Border Gateway Protocol) - používán pro směrování mezi autonomními systémy na internetu (tzv. externí směrovací protokol)

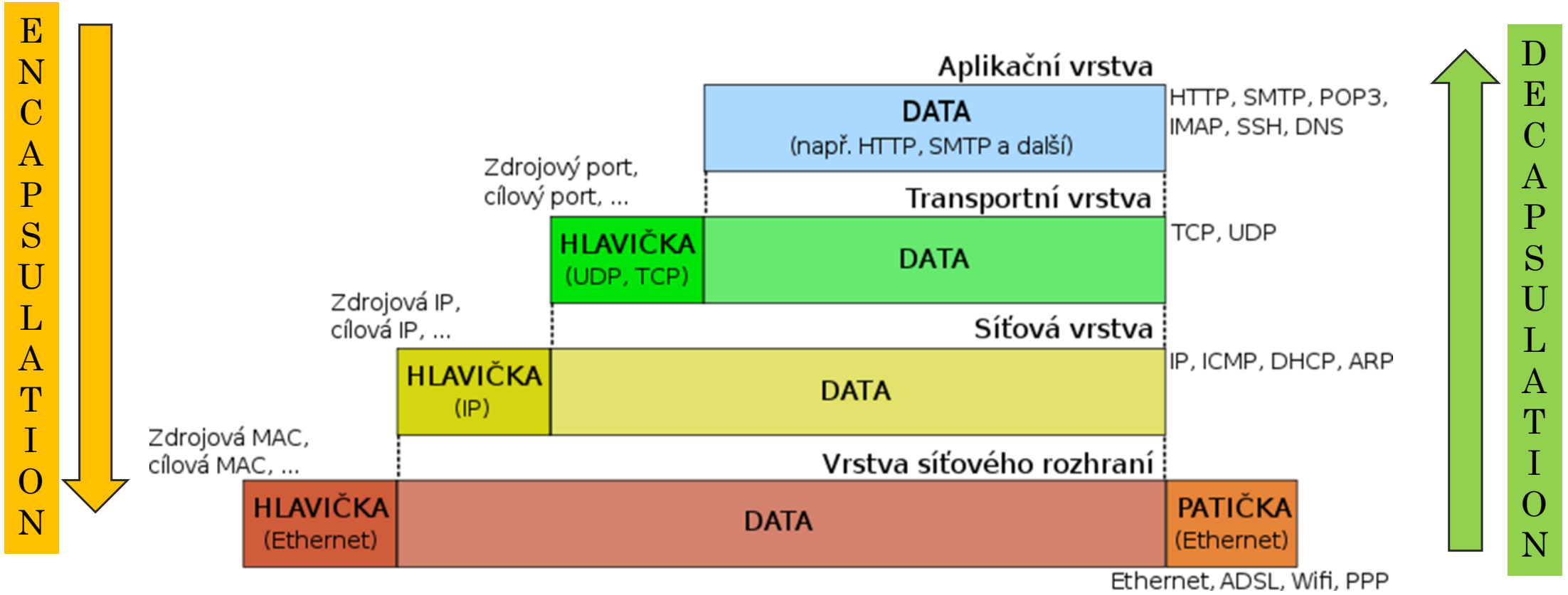
OSPF (Open Shortest Path First) - směrovací protokol pro vnitřní sítě

IGP – (Interior Gateway Protocol), používá Dijkstrův algoritmus

RIP (Routing Information Protocol) - starší směrovací protokol využívající vektor vzdáleností

EIGRP (Enhanced Interior Gateway Routing Protocol) - Cisco proprietární protokol

Zapouzdření dat v síti TCP/IP



VIDEO (zapouzdření dat)

Protokol IP - charakteristika

IP byl navržen jako protokol s nízkou režií. Poskytuje pouze funkce, které jsou nezbytné pro doručení paketu ze zdroje do cíle přes propojenou soustavu sítí. **Protokol nebyl navržen pro sledování a řízení toku paketů.**

Tyto funkce, pokud jsou vyžadovány, jsou prováděny jinými protokoly na jiných vrstvách, především TCP na vrstvě L4.

Základní charakteristiky protokolu IP:

- **je nespojovaný (bez připojení)** – neexistuje žádné spojení s cílem navázaným před odesláním datových paketů;
- **Best Effort (nejlepší snaha > nespolehlivost)** – IP je ze své podstaty nespolehlivý, protože **doručení paketů není zaručeno**;
- **nezávislý na médiu** – provoz je nezávislý na médiu (tj. měděném, optickém nebo bezdrátovém), které přenáší data.

Nespojovanost protokolu IP

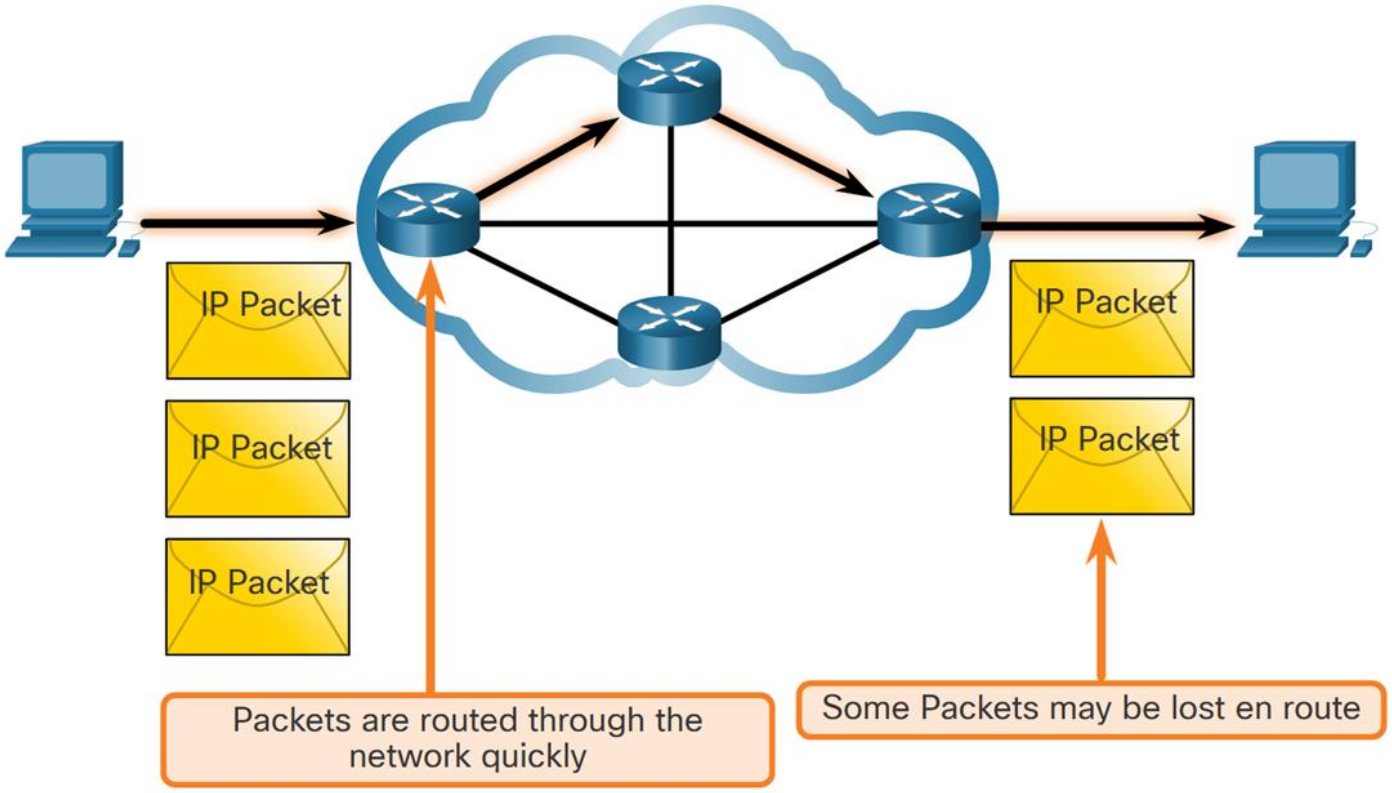
IP je nespojovaný, což znamená, že před odesláním dat nevytváří žádné vyhrazené end-to-end připojení.

- komunikace je koncepčně podobná odeslání dopisu někomu bez předchozího upozornění příjemce.

IP protokol nevyžaduje žádnou počáteční výměnu řídicích informací pro navázání spojení mezi koncovými body před předáním paketů.

Best Effort

- je metoda doručování, síť se pokusí doručit pakety, ale není zaručeno, že doručení bude úspěšné nebo že data nebudou poškozená
- tato metoda neprovádí detekci chyb, opravy chyb ani nezaručuje doručení v určitém čase
- tento způsob se běžně používá u protokolů jako UDP, kde spolehlivost není zaručena a ztracené nebo poškozené pakety se neodesílají znovu



Protokol IP nezaručuje, že všechny doručené pakety budou skutečně přijaty.

Nespolehlivost

- protokol IP nemá schopnost spravovat a obnovovat nedoručené nebo poškozené pakety
- je to proto, že i když jsou pakety IP odesílány s informacemi o místě doručení, neobsahují informace, které by bylo možné zpracovat a informovat odesílatele, zda bylo doručení úspěšné

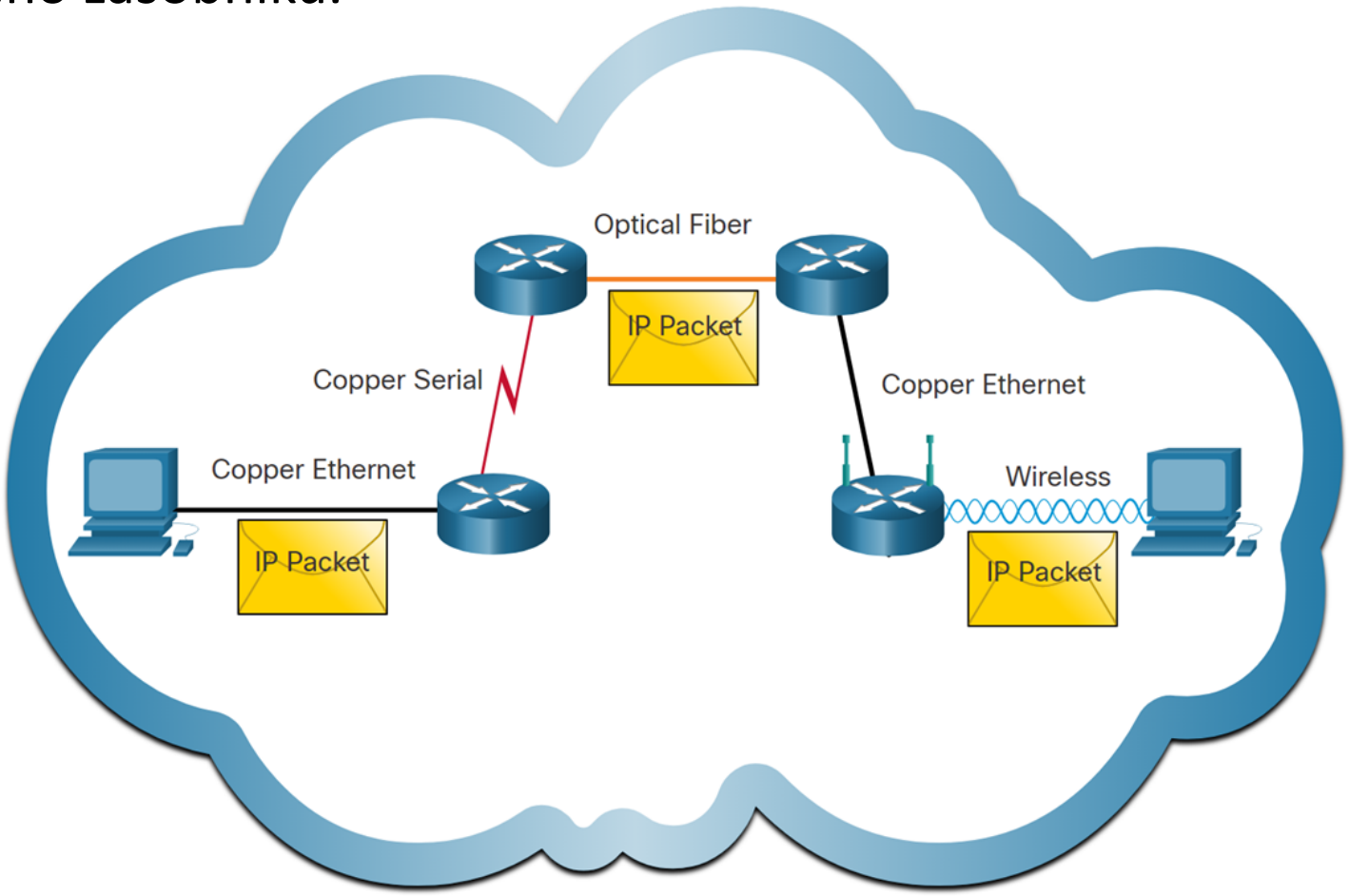
Pakety mohou dorazit na místo určení poškozené, mimo pořadí nebo nemusí dorazit vůbec.

Pokud jsou doručovány pakety mimo pořadí nebo pakety chybí, musí tyto problémy vyřešit aplikace využívající data nebo služby vyšší vrstvy. Díky tomu může IP fungovat velmi efektivně. V sadě protokolů TCP/IP je spolehlivost úlohou protokolu TCP na transportní vrstvě.

IP neposkytuje žádnou možnost opakovaného přenosu paketů, pokud dojde k chybám.

Nezávislost na médiu

- IP pracuje nezávisle na médiích, která přenášejí data v nižších vrstvách protokolového zásobníku.



Jak je znázorněno na obrázku, IP pakety mohou být komunikovány jako elektronické signály po měděném kabelu, jako optické signály po vlákně nebo bezdrátově jako rádiové signály.

MTU (maximální přenosová jednotka)

- **linková vrstva** stanovuje MTU, což je největší možná velikost datového rámce, který může být přenesen přes dané médium (například Ethernet běžně používá **MTU 1500 bajtů**).
- MTU zahrnuje **užitečná data** (payload) a hlavičky protokolů linkové vrstvy, ale **nezahrnuje** hlavičky vyšších vrstev (například IP, TCP nebo UDP)
- záleží na druhu média

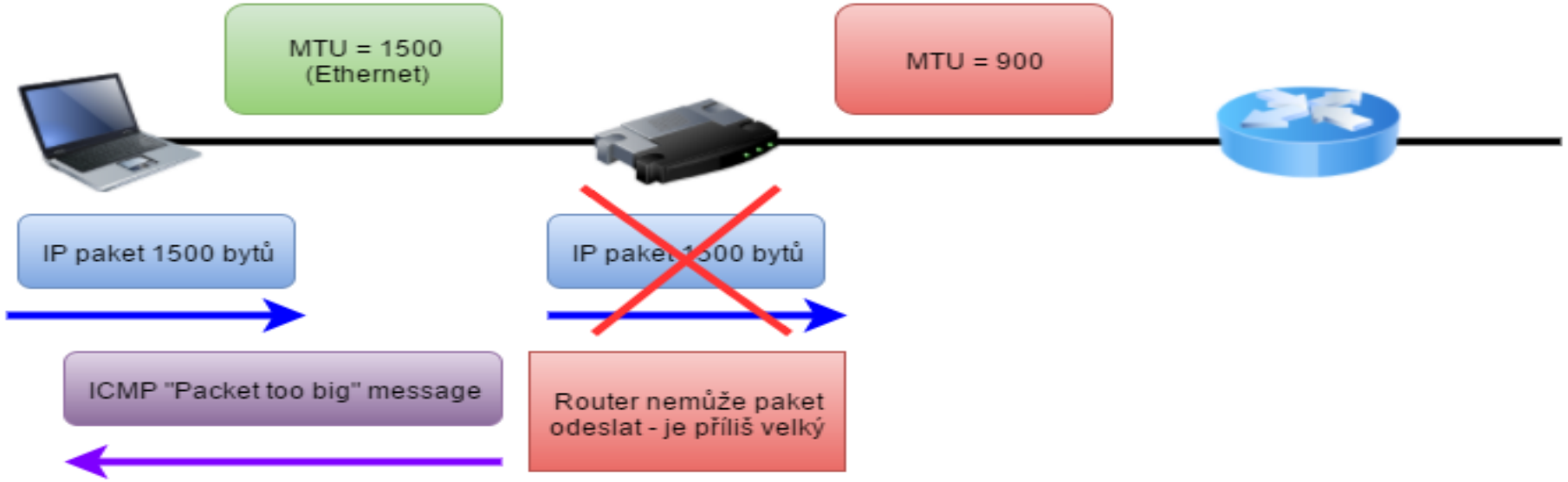
Např. Ethernet má jiný MTU než Wi-Fi nebo optické sítě

Fragmentace

V některých případech musí zprostředkující zařízení, obvykle router, rozdělit paket IPv4 při jeho předávání z jednoho média na druhé médium s menší MTU.

Tento proces se nazývá **fragmentace paketu.**

- fragmentace způsobuje latenci (zdržení) a větší režii
- pakety IPv6 nemohou být směrovačem fragmentovány
- **od fragmentace se již upustilo (nebo upouští), protože má několik nevýhod**



Fragmentace

Původní paket: Délka = 4620 bytů (20 hlavička, 4600 data) , ID = 0x4C02.
Paket se rozdělí na 4 fragmenty:

Identifikace fragmentu [2 byty]	Flagy [3 bity]	Pozice fragmentu [13 bitů]

Zkuste příkaz *ping –f –l 2000 www.seznam.cz*.
Parametr f nastaví flag DF na 1, a l určí, kolik bajtů náhodně vygenerovaných dat se má poslat na server naší oblíbené webové stránky.
Pokud jede vaše LAN na Ethernetu (a nevrtali jste se v nastavení), tak uvidíte chybovou hlášku.

```
Pinging www.seznam.cz [77.75.79.222] with 2000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 77.75.79.222:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\petro>
```

IP hlavička fragmentu	Data [1480 bytů]	ID = 0x4C02 DF flag = 0 MF flag = 1 Fragment offset = 0
IP hlavička fragmentu	Data [1480 bytů]	ID = 0x4C02 DF flag = 0 MF flag = 1 Fragment offset = 185
IP hlavička fragmentu	Data [1480 bytů]	ID = 0x4C02 DF flag = 0 MF flag = 1 Fragment offset = 370
IP hlavička fragmentu	Data [160 bytů]	ID = 0x4C02 DF flag = 0 MF flag = 0 Fragment offset = 555

Fragmentace - příklad

Kolik bude celkem fragmentů a jakých, když je zadáno:

- celková velikost datagramu (vč. hlavičky) je **4000 bajtů**
- velikost hlavičky IPv4: **20 bajtů**
- maximální přenosová jednotka (MTU): **1500 bajtů**

Výpočet fragmentace:

1. Maximální užitečná data na fragment: MTU - IPv4 hlavička = 1500 - 20 = 1480 bajtů
2. Počet fragmentů:

datová část celého paketu je: 4000 – 20 = 3890 bajtů

počet fragmentů: **3** (1. fragment: 1480 B, 2. fragment: 1480 B, 3. fragment: 1020 B (zbytek)

Fragment	Offset (8B jednotky)	Data délka	MF (More Fragments)
1.	0	1480 B	1
2.	185 (1480 ÷ 8)	1480 B	1
3.	370 (1480+1480) ÷ 8)	1020 B	0

MTU - discovery

- je to metoda pro zjištění MTU pro danou cestu

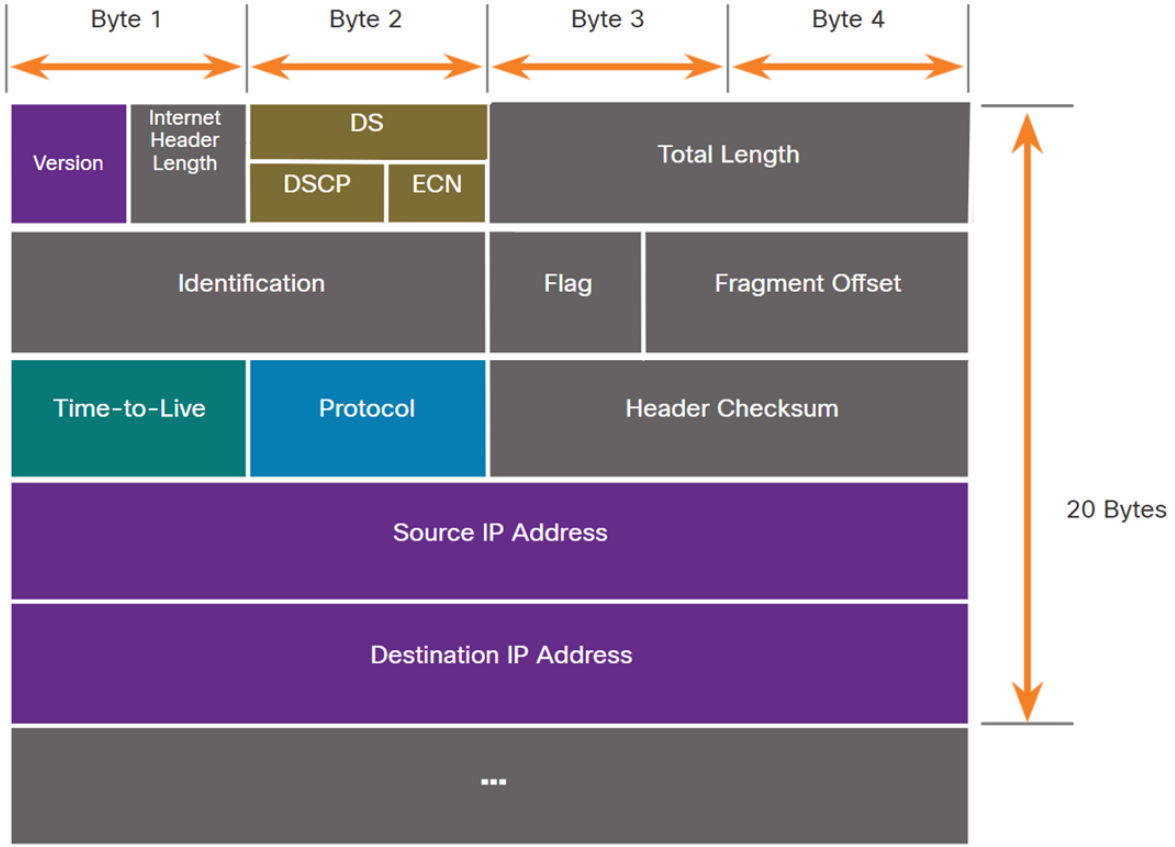
Zjišťování probíhá takto:

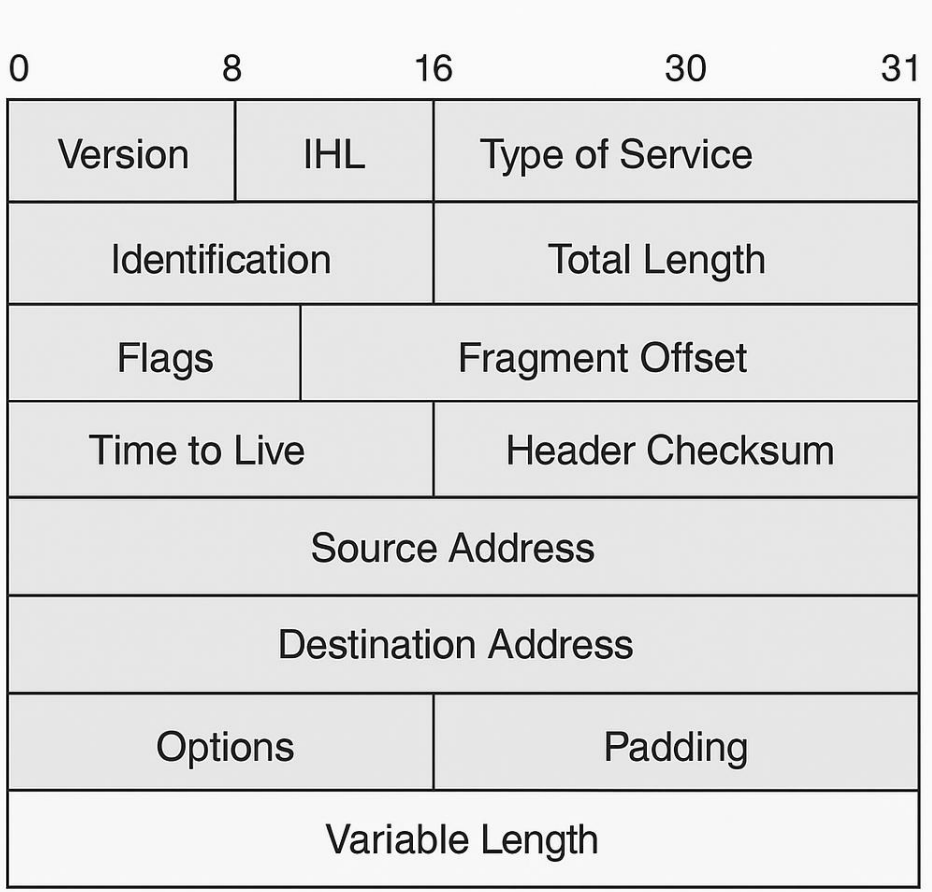
1. Odesilatel (typicky PC) odešle klasický paket s daty tak veliký, jak mu jeho síť dovolí, přičemž nastaví flag Don't fragment (DF) na 1.
2. Pokud se po cestě vyskytne síť s menším MTU, router nemůže paket fragmentovat kvůli DF flagu.
3. Zahodí tedy paket a pošle PC zprávu „Packet too big" – **tato obsahuje i MTU sítě, kterou paket nemohl projít**.
4. PC tedy zmenší paket na danou hodnotu, a odesílá znovu.
5. Postup se opakuje do té doby, než paket projde celou cestou.

U Internetu platí, že jednotlivé pakety pro stejnou destinaci mohou cestovat jinudy – proto je pak ve všech odeslaných paketech nastaven DF flag vždy na 1, aby se PC mohl přizpůsobit i při změně trasy.

Většina spojů v Internetu má MTU stejnou nebo větší než Ethernet (a Ethernet je globální standard pro LAN sítě).

IPv4 paket - header





IPv4 paket

- ***Verze*** *– obsahuje 4bitovou binární hodnotu nastavenou na 0100, která identifikuje tento paket jako paket IPv4*
- ***IHL*** *– délka hlavičky, dnes max. 20 byte (dříve to mohlo být jinak)*
- ***Differentiated Services (DS)*** *– je 8bitové pole používané k určení priority každého paketu, dnes známe spíše jako* ***QoS (Quality of Service)***
- ***Total Lenght*** *– délka datagramu v bytech*
- ***Identification*** *- pokud byl datagram při přepravě fragmentován, pozná se, které fragmenty patří k sobě (mají stejný identifikátor)*
- ***Flag*** *(příznaky) – slouží pro řízení fragmentace, máme DF=1 (nesmí fragmentovat a MF=1 (fragment není poslední)*
- ***Fragment offset*** - udává, na jaké pozici v původním datagramu začíná tento fragment. Důležité k sestavení paketu!
- ***Time to Live (TTL)*** *– obsahuje 8bitovou binární hodnotu, která se používá k omezení životnosti paketu.*
- ***Protokol*** *– toto pole se používá k identifikaci protokolu další úrovně. Mezi běžné hodnoty patří ICMP (1), TCP (6) a UDP (17).*
- ***Header Checksum (kontrolní součet záhlaví)*** *– slouží ke zjištění poškození v hlavičce protokolu IPv4*
- ***Zdrojová IPv4 adresa*** *– obsahuje 32bitovou binární hodnotu, která představuje zdrojovou IPv4 adresu paketu. Zdrojová adresa IPv4 je vždy adresa unicastového vysílání.*
- ***Cílová IPv4 adresa*** *– obsahuje 32bitovou binární hodnotu, která představuje cílovou IPv4 adresu paketu.*

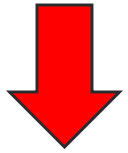
IPv4 paket - TTL

Proč existuje TTL?

- TTL (Time To Live) slouží jako **ochrana proti zacyklení paketů** v síti.
- při každém průchodu routerem se TTL **snižuje o 1**
- pokud by neexistovalo, mohly by se pakety **nekonečně smyčkovat** kvůli chybné konfiguraci

Pokud router obdrží IP paket s hodnotou TTL = 1, provede následující:

TTL se sníží o 1 → výsledná hodnota bude 0



Paket je zahozen – router ho dále nepřepošle.

Router vygeneruje ICMP chybovou zprávu:
Typ: 11 (Time Exceeded)
Kód: 0 (TTL expired in transit)
Tato zpráva je poslána odesílateli paketu. Odesílatel se tak dozví, že paket nedorazil kvůli překročení limitu přeskoků.

TTL – praktické využití Traceroute

Nástroj (příkaz) traceroute právě využívá TTL = 1, 2, 3, ...

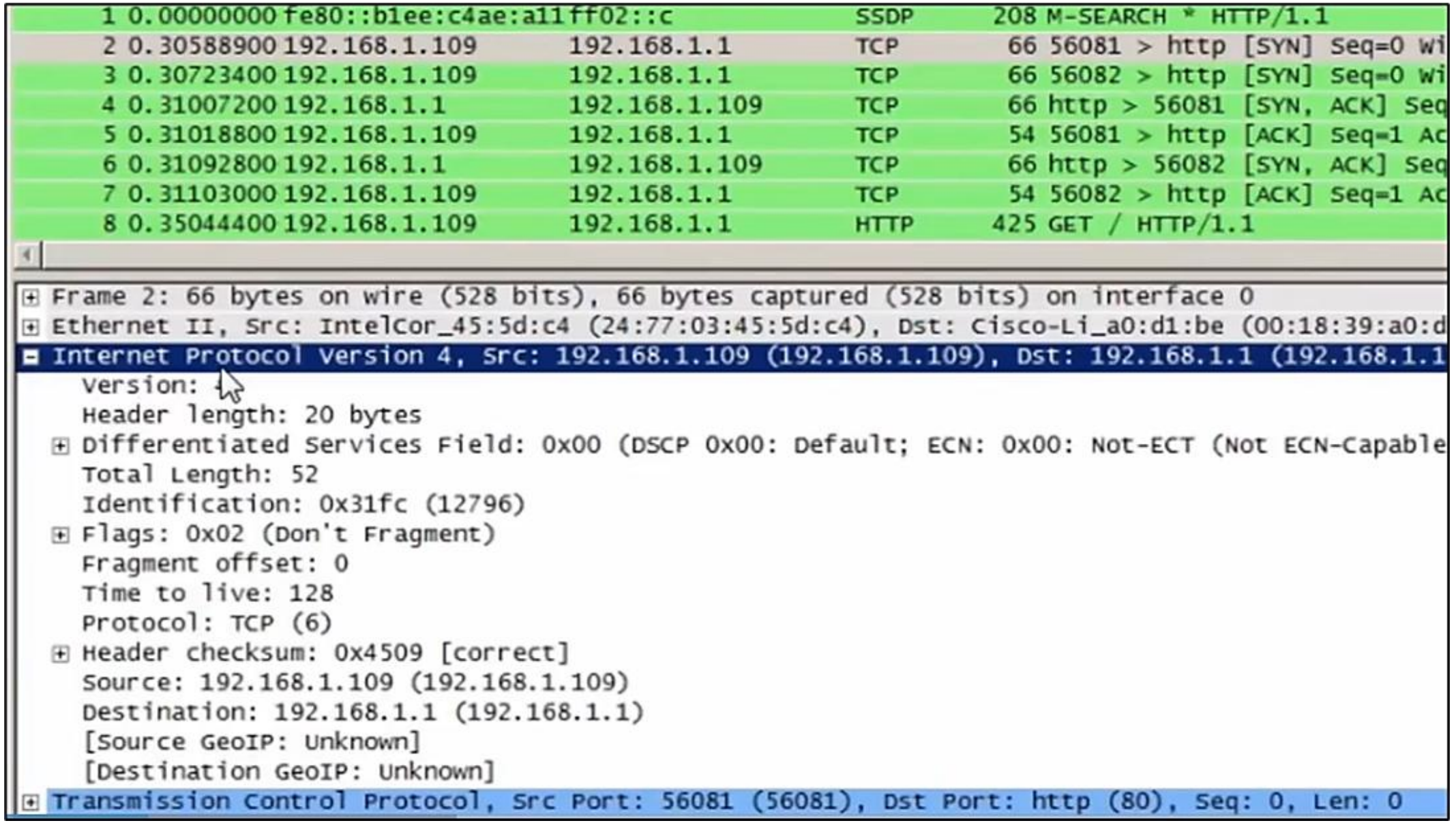
- postupně posílá pakety s rostoucí hodnotou TTL;
- každý router po cestě odpoví ICMP zprávou, když TTL klesne na 0;

Díky tomu lze mapovat trasu paketu přes jednotlivé routery.

```
traceroute to www.google.com (142.250.187.36), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)    1.267 ms  1.179 ms  1.161 ms
 2  10.10.0.1 (10.10.0.1)        2.312 ms  2.290 ms  2.274 ms
 3  81.200.57.1                  5.543 ms  5.617 ms  5.601 ms
 4  89.102.160.49                8.233 ms  8.210 ms  8.189 ms
 5  108.170.251.193              9.012 ms  8.999 ms  8.986 ms
 6  108.170.235.115              9.123 ms  9.087 ms  9.071 ms
 7  fra24s14-in-f36.1e100.net (142.250.187.36)  10.134 ms  10.114 ms  10.092 ms
```

Hodnota 60 bajtů v příkazu traceroute není náhodná – je to velikost výchozího paketu, který se v rámci traceroute testu odesílá (hlavička IPv4, hlavička UDP/ICMP, test data).

IPv4 paket


1 0.00000000 fe80::b1ee:c4ae:a11 ff02::c SSDP 208 M-SEARCH * HTTP/1.1
2 0.30588900 192.168.1.109 192.168.1.1 TCP 66 56081 > http [SYN] Seq=0 Wi
3 0.30723400 192.168.1.109 192.168.1.1 TCP 66 56082 > http [SYN] Seq=0 Wi
4 0.31007200 192.168.1.1 192.168.1.109 TCP 66 http > 56081 [SYN, ACK] Seq
5 0.31018800 192.168.1.109 192.168.1.1 TCP 54 56081 > http [ACK] Seq=1 Ac
6 0.31092800 192.168.1.1 192.168.1.109 TCP 66 http > 56082 [SYN, ACK] Seq
7 0.31103000 192.168.1.109 192.168.1.1 TCP 54 56082 > http [ACK] Seq=1 Ac
8 0.35044400 192.168.1.109 192.168.1.1 HTTP 425 GET / HTTP/1.1
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d
Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Total Length: 52
Identification: 0x31fc (12796)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x4509 [correct]
Source: 192.168.1.109 (192.168.1.109)
Destination: 192.168.1.1 (192.168.1.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 56081 (56081), Dst Port: http (80), Seq: 0, Len: 0

IPv4 paket – Time to Live (TTL)

- zabraňuje nekonečnému cestování paketu v síti *(třeba kvůli chybě v routovací tabulce by paket neustále obíhal kolečko mezi pěti routery).*
- odesílatel ji nastaví na nějakou počáteční hodnotu (doporučená je 64, Windows dává hodnotu 128) a **každý router, který tento IP paket obdrží, tuto hodnotu sníží o 1**.

Pokud se hodnota TTL dostane na nulu (a paket nebyl doručen cílovému zařízení), pak router paket zahodí a odesílateli odešle ICMP zprávu „Time exceeded“.

```
C:\Users\Xenoblade>ping -i 3 www.google.com

Pinging www.google.com [173.194.116.240] with 32 bytes of data:
Reply from 212.111.3.5: TTL expired in transit.
Reply from 212.111.3.5: TTL expired in transit.
Reply from 212.111.3.5: TTL expired in transit.
Reply from 212.111.3.5: TTL expired in transit.

Ping statistics for 173.194.116.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

IPv4 – omezení protokolu

IPv4 se používá dodnes. V průběhu let byly vyvinuty další protokoly a procesy, které řeší nové výzvy. I přes změny má však IPv4 stále tři hlavní problémy:

- **vyčerpání IPv4 adres** – IPv4 má k dispozici omezený počet unikátních veřejných adres. Přestože existují přibližně 4 miliardy adres IPv4, rostoucí počet nových zařízení s podporou IP, připojení always-on a potenciální růst méně rozvinutých regionů zvýšily potřebu dalších adres.
- **nedostatek end-to-end konektivity** – překlad síťových adres (NAT) je technologie běžně implementovaná v sítích IPv4. NAT poskytuje způsob, jak může více zařízení sdílet jednu veřejnou IPv4 adresu. Protože je však veřejná adresa IPv4 sdílená, je adresa IPv4 hostitele interní sítě skrytá. To může být problematické u technologií, které vyžadují end-to-end konektivitu.
- **zvýšená složitost sítě** – i když NAT prodloužil životnost IPv4, byl zamýšlen pouze jako přechodový mechanismus na IPv6. NAT ve své různé implementaci vytváří další složitost v síti, vytváří latenci a ztěžuje řešení problémů.

Zdroje

- https://www.itnetwork.cz/site/zaklady/internet-protokol-hlavicka
- Jiří Peterka – www.e-archiv.cz (sborník přednášek Počítačové sítě II)
- Cisco: výukový portál Netacad.com
- Adresování v IP sítích | SAMURAJ-cz.com dostupné na: https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/

"Části této prezentace byly vytvořeny s využitím generativní umělé inteligence (OpenAI - ChatGPT 4.0, verze z roku 2025) jako podpůrného nástroje pro získávání informací a formulaci textu. Výsledky byly následně editovány a ověřeny autorem."