Počítačové sítě

Technické pozadí online komunikace

První počítače a sítě

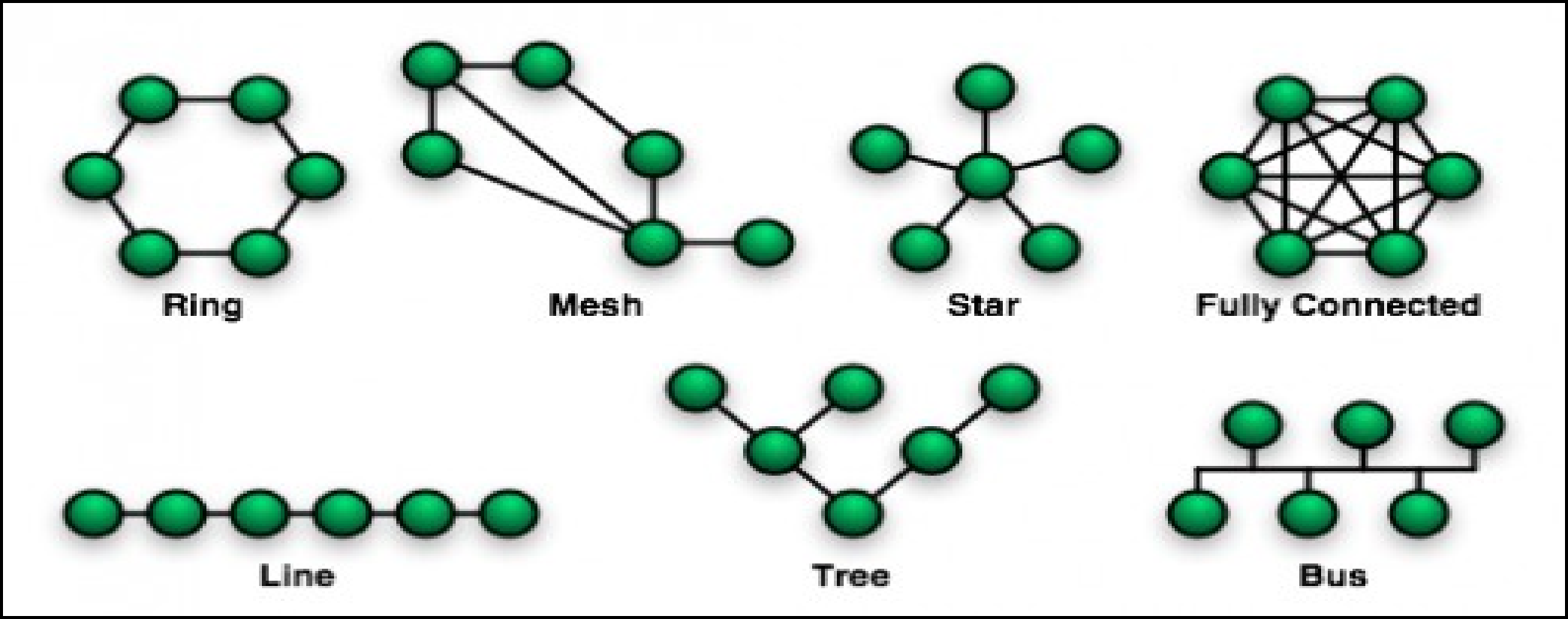
- 1939 John Atansoff – 15 operací/s, elektronkový a binární.
- 1938, 1939, 1941 Konrad Zuse Z1-Z3
- 1943-7 ENIAC

- 1965 paketová síť
- 1969 V USA byla vytvořena experimentální síť ARPANET, která umožní vznik mezinárodní decentralizované sítě – internetu.
- 1980 Bylo vydáno RFC 760, jež popisuje IPv4, a ve stejném roce zahájen experimentální provoz TCP/IP v síti ARPANET.
- 1987 Poprvé se objevuje pojem „internet.“

Dělení sítí

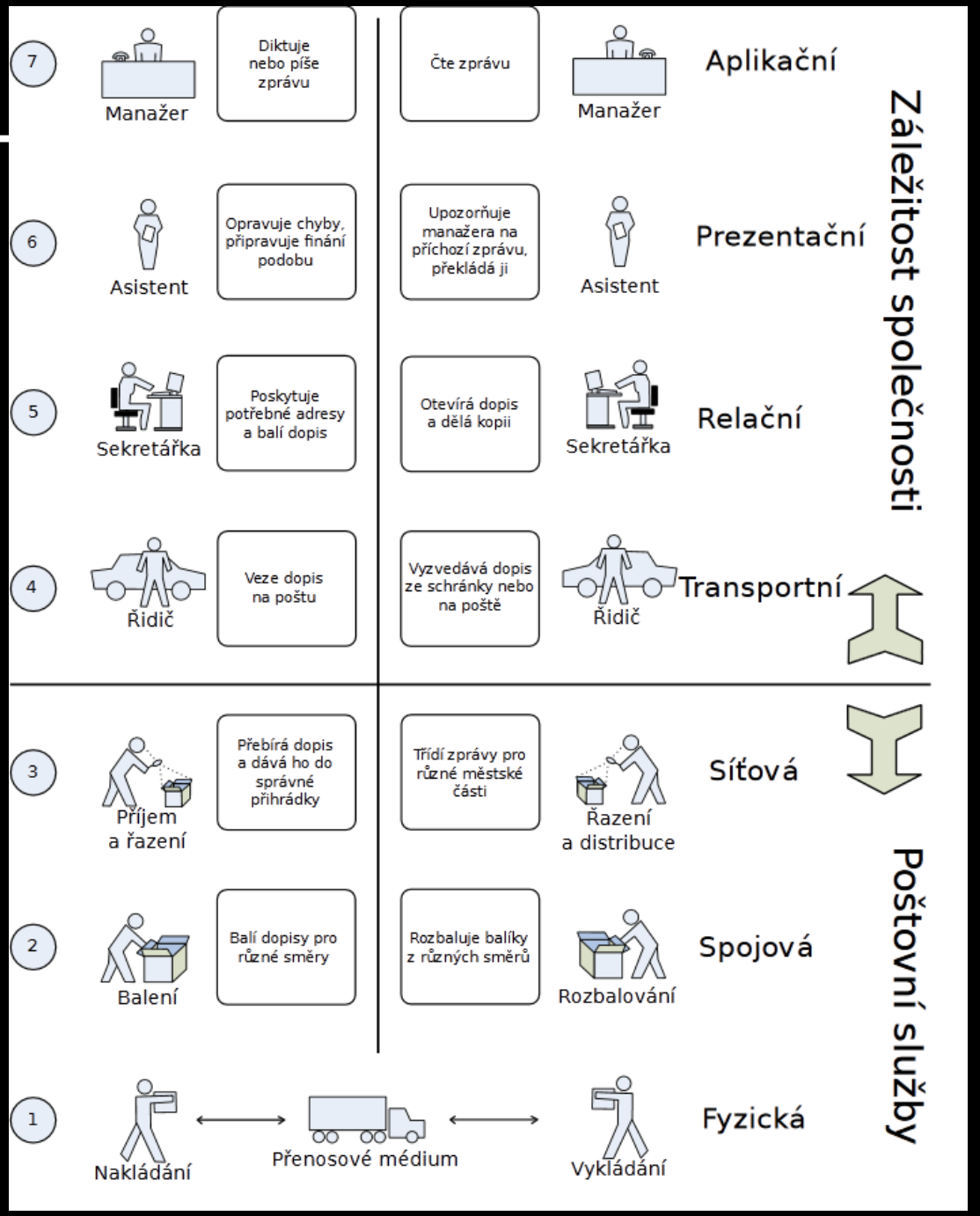
- Podle velikosti: Pan, Lan, Man, Wan
- Podle dynamiky: statické a dynamické
- Podle média: voděné a vlněné
- …

Topologie



ISO-OSI MODEL

ISO-


7
Manažer
Diktuje nebo píše zprávu
Čte zprávu
Manažer
Aplikační
6
Asistent
Opravuje chyby, připravuje finání podobu
Upozorňuje manažera na příchozí zprávu, překládá ji
Asistent
Prezentační
5
Sekretářka
Poskytuje potřebné adresy a balí dopis
Otevírá dopis a dělá kopii
Sekretářka
Relační
4
Řidič
Veze dopis na poštu
Vyzvedává dopis ze schránky nebo na poště
Řidič
Transportní
Záležitost společnosti
3
Příjem a řazení
Přebírá dopis a dává ho do správné přihrádky
Třídí zprávy pro různé městské části
Řazení a distribuce
Síťová
2
Balení
Balí dopisy pro různé směry
Rozbaluje balíky z různých směrů
Rozbalování
Spojová
1
Nakládání
Přenosové médium
Vykládání
Fyzická
Poštovní služby

Aplikační a prezentační vrstva I.

- **POP3** slouží pro stahování emailových zpráv ze vzdáleného serveru na klientský počítač a využívá u toho TCP/IP připojení. Jde o poměrně zastaralou technologii, která je postupně nahrazována IMAP. Nevýhodou je, že stahuje všechnu poštu, i tu kterou si uživatel nepřáli.
- **IMAP4** je protokol pro vzdálený přístup k e-mailové schránce. Na rozdíl od protokolu POP3 umí IMAP pracovat v tzv. on-line i off-line režimu a nabízí pokročilé možnosti vzdálené správy – od práce se složkami, přes pouhé čtení hlaviček až po manipulaci s poštou přímo na serveru.
- **SMTP** slouží pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (jednoduše pro zasílání e-mailů). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky příjemce, odkud si ji může pomocí dalších protokolů (např. IMAP4) stáhnout a přečíst. Pokud má uživatel zájem na používání elektronické pošty, musí ve svém klientovi mít mít nastavenou adresu smtp serveru pro odesílání a imap4 či pop3 pro příjem pošty. Ve webových prostředí je vše zajištěno již provozovatelem služby.
- **FTP** slouží pro přenos souborů prostřednictvím sítě a je založený na modelu klient-server. Přenos je nešifrovaný, server lze chránit heslem. Využívá protokol TCP z rodiny TCP/IP a postupně jej nahrazuje SSH, který nabízí mj. Také šifrovanou komunikaci.

Aplikační a prezentační vrstva II.

- **DNS** (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejnojmeným protokolem sloužícím k výměně informací. Jeho hlavním významem je převod doménových jmen na IP adresu, čímž zajišťují možnost používat URL adresy. Později svoji funkčnost rozšířil o podporu dalších technologií jako je IP telefonie či e-mailová komunikace.
- **HTTP** je bezstavový protokol, který funguje způsobem dotaz-odpověď. Uživatel pošle serveru dotaz ve formě čistého textu, obsahujícího označení požadovaného dokumentu, informace o schopnostech prohlížeče apod. Server následně odpoví taktéž v textové podobě. Jednotlivé dotazy mezi sebou nemají žádnou spojitost. Přenos je primárně nešifrovaný, ale existuje bezpečná varianta HTTPS. Jde o základní protokol internetu, kterou slouží k obsluze hypertextu.
- Snad jediným čistým významnějším zástupcem prezentační vrstvy je **SMB**, který zajišťuje síťovou komunikaci pro sdílený přístup k tiskárnám, souborům, scannerům a dalším zařízením. Nabízí také některé další možnosti pro sdílení zdrojů včetně autorizace.

Transportní vrstva

- **TCP** zajišťuje spolehlivý přenos dat, to znamená, že cílem je dodání všech odeslaných paketů ve správném pořadí. Hlavní kritérium je tedy doručení nikoli rychlost.
- **UDP** je zástupcem klasického nespojovaného přístupu. Používá se tam, kde prim hraje rychlost a nemá smysl kontrolovat doručení – příkladem může být IP telefonie, video stream či online hry.

TCP

Bity	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	zdrojový port																cílový port															
32	číslo sekvence																															
64	potvrzený bajt																															
96	offset dat				rezervováno						příznaky						okénko															
128	kontrolní součet																Urgent Pointer															
160	volby (volitelné)																															
192	volby (pokračování)																								výplň (do 32)							
224	data																															

UDP

+	bity 0 - 15	16 - 31
0	zdrojový port	cílový port
32	délka	kontrolní součet
64	data	

IP

- Zajišťuje doručování paketů na správnou adresu.
- Podrobněji za chvíli.

Linková vrstva

- **Ethernet** je souhrnný název pro v současné době nejrozšířenější technologie pro budování počítačových sítí typu LAN.
- Jako metodu boje proti kolizím se nejčastěji užívá techniky CSMA/CD, která funguje přibližně následujícím způsobem.
  - Naslouchá, zda je médium (klasicky kroucená dvojlinka) volné. Jestliže není, čeká na jeho uvolnění.
  - Pokud je volné, zahájí vysílání. Současně s odesíláním rámce naslouchá, zda nepřichází signál od jiné stanice. Pokud ano, došlo ke kolizi. Stanice ukončí vysílání, odešle signál umožňující rozpoznat kolizi také ostatním stanicím.
  - Vybere náhodné číslo z intervalu a podle něj čeká náhodně dlouhou dobu, než se zase pokusí vysílat. V praxi je omezená doba i nahodilost daného čísla.

Linková vrstva II.

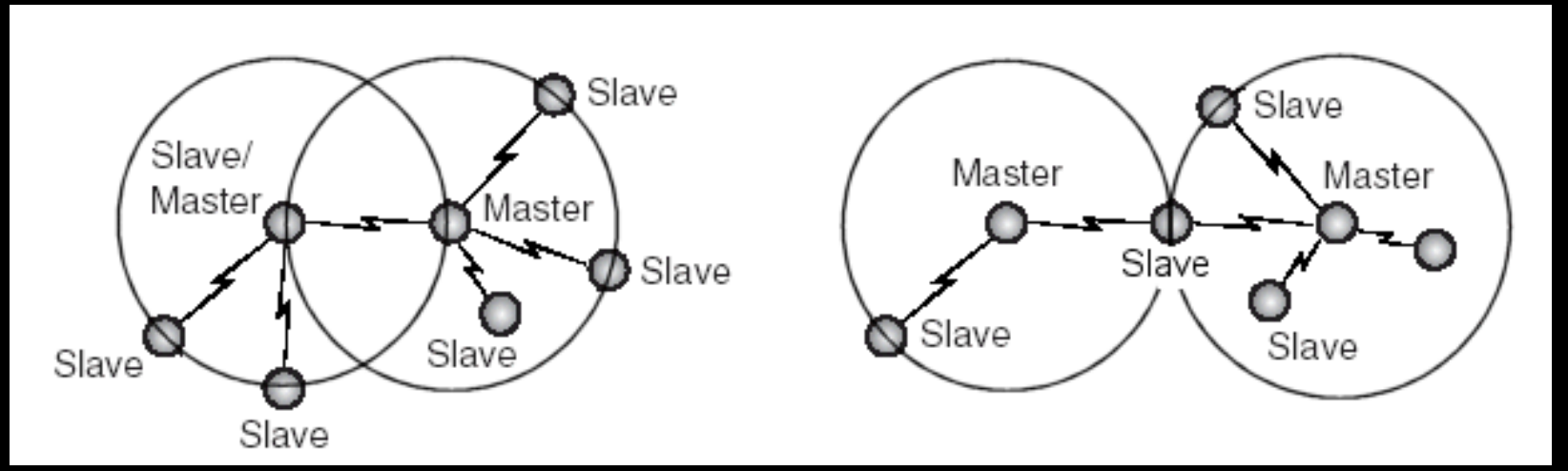
- **WiFi**: Používá bezlicenční pásma, což snižuje její cenu.
- K detekci kolize se používá CDMA/CA, kterou lze opět popsat ve třech krocích:
  - Je-li médium volné po určenou dobu, může stanice zahájit vysílání. Pokud je vysílání neúspěšné, zahájí exponenciální čekání.
  - Pokud je médium obsazeno, počká na jeho uvolnění a následně zahájí exponenciální čekání, stejně jako při neúspěšném odvysílání.
  - Exponenciální čekání znamená odložený pokus o vysílání. Stanice si náhodně vybere dobu z intervalu, jehož velikost se během opakovaných pokusů zdvojnásobuje; to snižuje pravděpodobnost příští kolize.

Linková vrstva III.

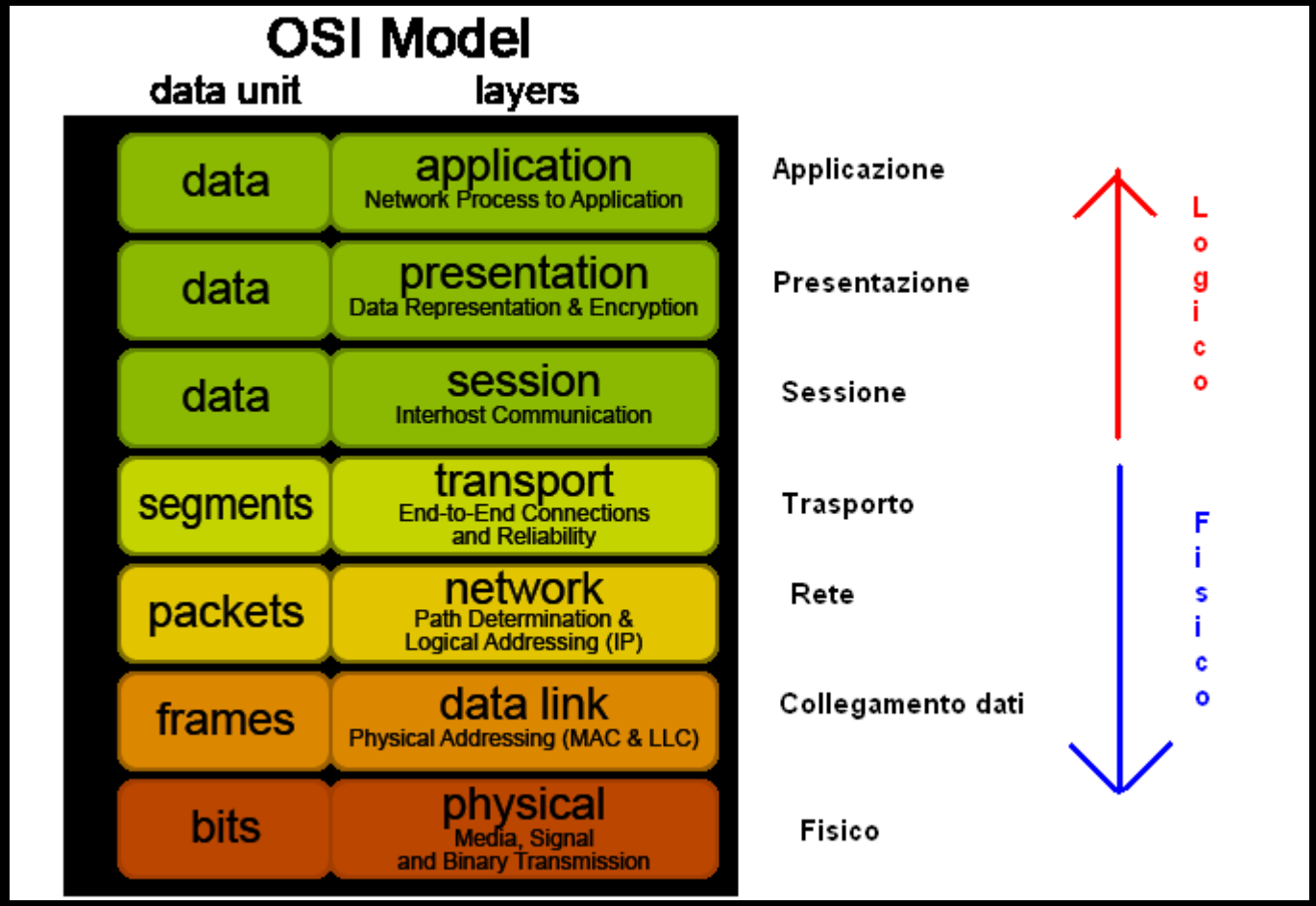
- **Bluetooth**: robustní technologie využívající strategie „Master - Slave“, zasahuje také do všech nižších vrstev.
- Řeší práva, bezpečnost, funkcionalitu.
- Má velice nízkou spotřebu.

Bluetooth


Master
Slave
Point to point
Slave
Master
Slave
Slave
Point to multipoint


Slave/
Master
Master
Slave
Slave
Slave
Slave
Master
Slave
Master
Slave
Slave

IPv6: motivace, funkce, budoucnost


OSI Model
data unit
layers
data
application
Network Process to Application
data
presentation
Data Representation & Encryption
data
session
Interhost Communication
segments
transport
End-to-End Connections and Reliability
packets
network
Path Determination & Logical Addressing (IP)
frames
data link
Physical Addressing (MAC & LLC)
bits
physical
Media, Signal and Binary Transmission
Applicazione
Presentazione
Sessione
Trasporto
Rete
Collegamento dati
Fisico
Logico
Fisico

Internet protocol

- Základní protokol síťové vrstvy
- Poskytuje adresu uzlům v síti
- Umožňuje adresaci a směrování v síti
- Negarantuje doručení

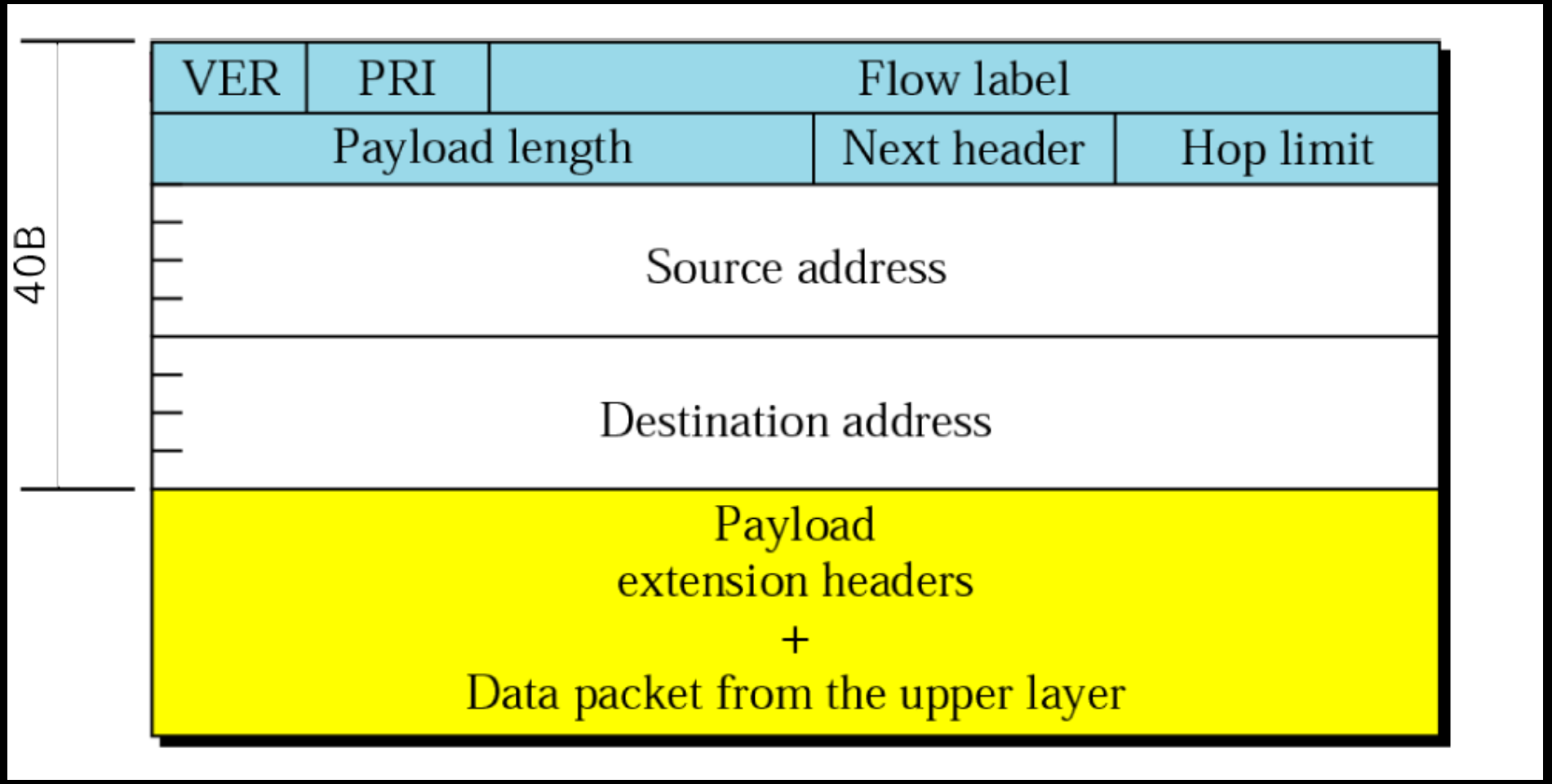
IPv4

- Dominantní na trhu
- Malý adresní rozsah
- Chybí pokročilá funkcionalita:
  - Slabá podpora pro real time aplikace
  - Chybí podpora pro bezpečný přenos dat
  - Chybí podpora pro autokonfiguraci
  - Chybí podpora pro mobilitu
  - …
- Řada funkcí je implementována postupně do IPv4

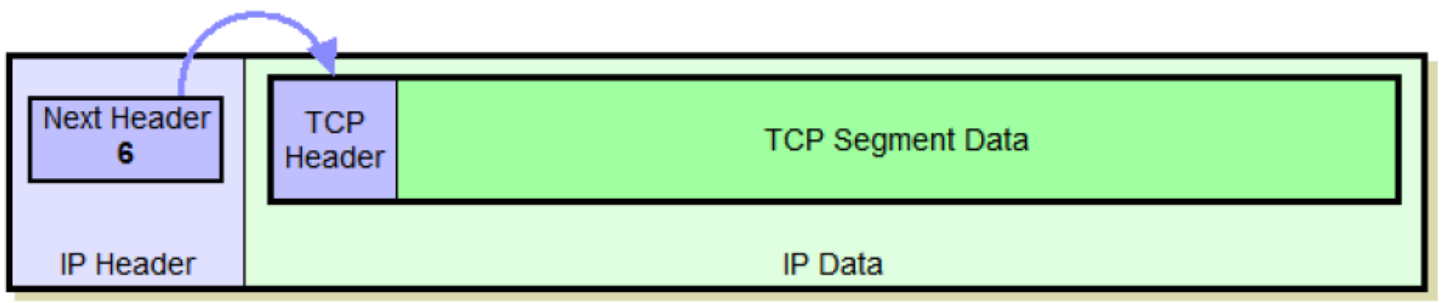
Základní vlastnosti IPv6

- 128 bitová adresa – teoreticky 2^{128} unikátních adres($3{,}4 \ 10^{38}$)
- Jednodušší hlavička s možností rozšíření
- Podpora RT protokolů a přenosu dat.
- Podpora QoS
- Podpora bezpečnosti
- Podpora mobility
- Autokonfigurace

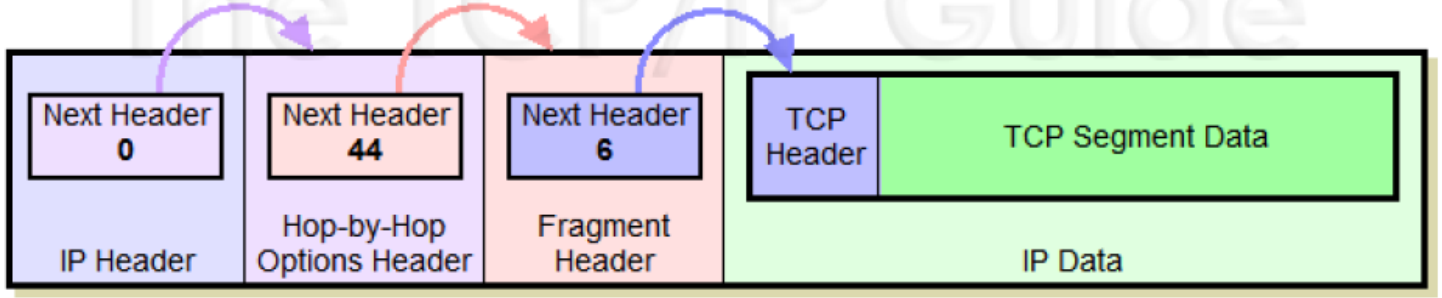
Základní hlavička



Rozšiřující hlavičky



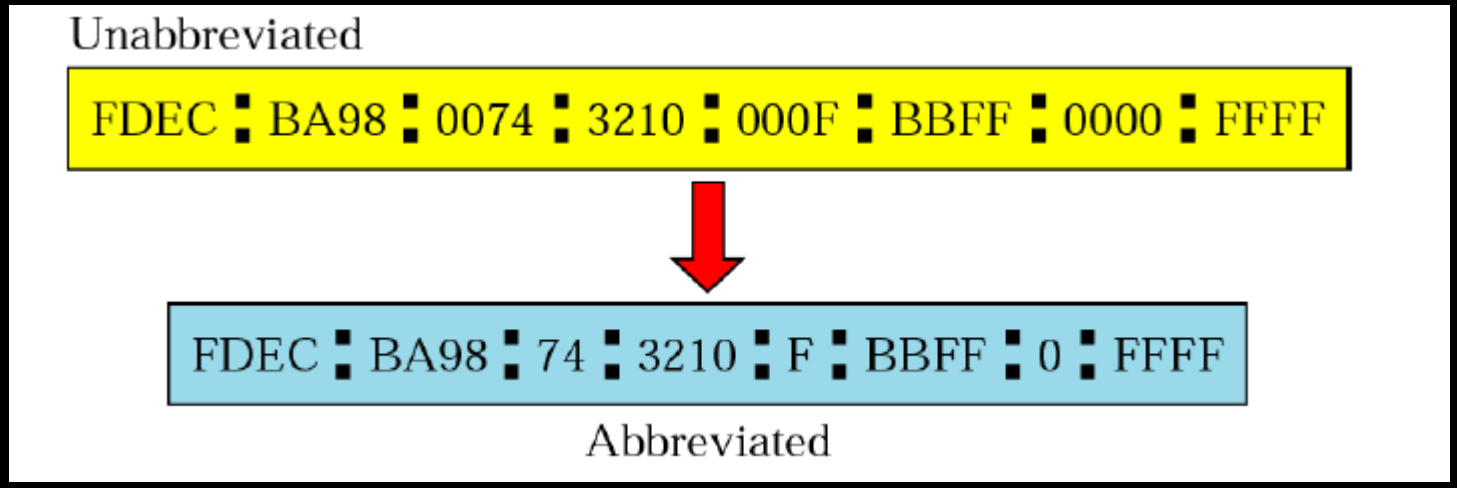
IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment

Zápis adresy

- Je možné zkracování, užívá se hexadecimální číselné soustavy (0..F)
- Není možné si jich pamatovat dostatek (DNS servery).



Typy adres

- Unicast : stejná jako u IPv4, adresuje jedno rozhraní
- Multicast : podobná jako u IPv4, adresuje všechny v adresním prostoru
- Anycast: adresuje rozhraní a požadavek zpracuje vybraný server dle vlastního uvážení daného systému.

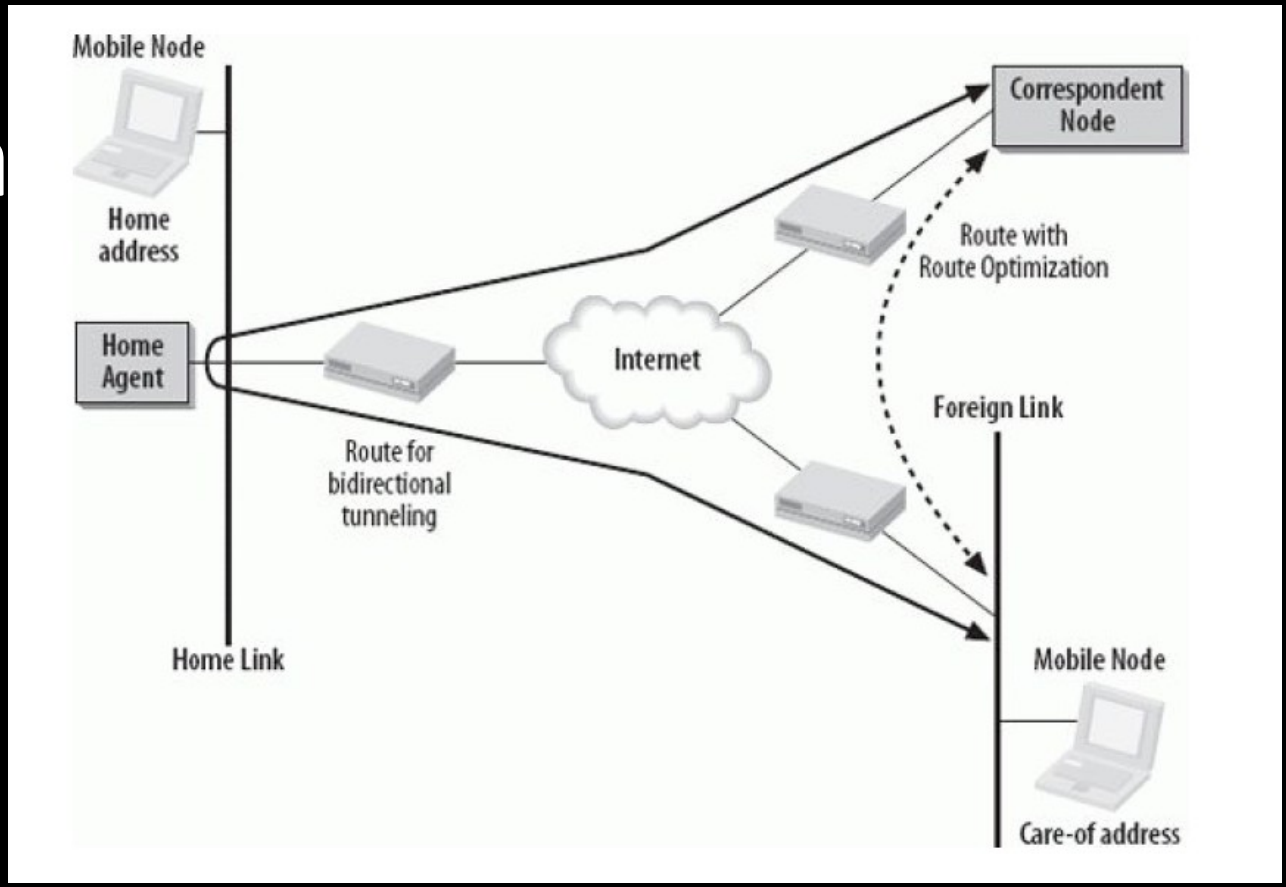
- IPv6 díky anycastovým adresám může dobře podporovat serverové farmy či distribuované výpočty.

Práce se sítí

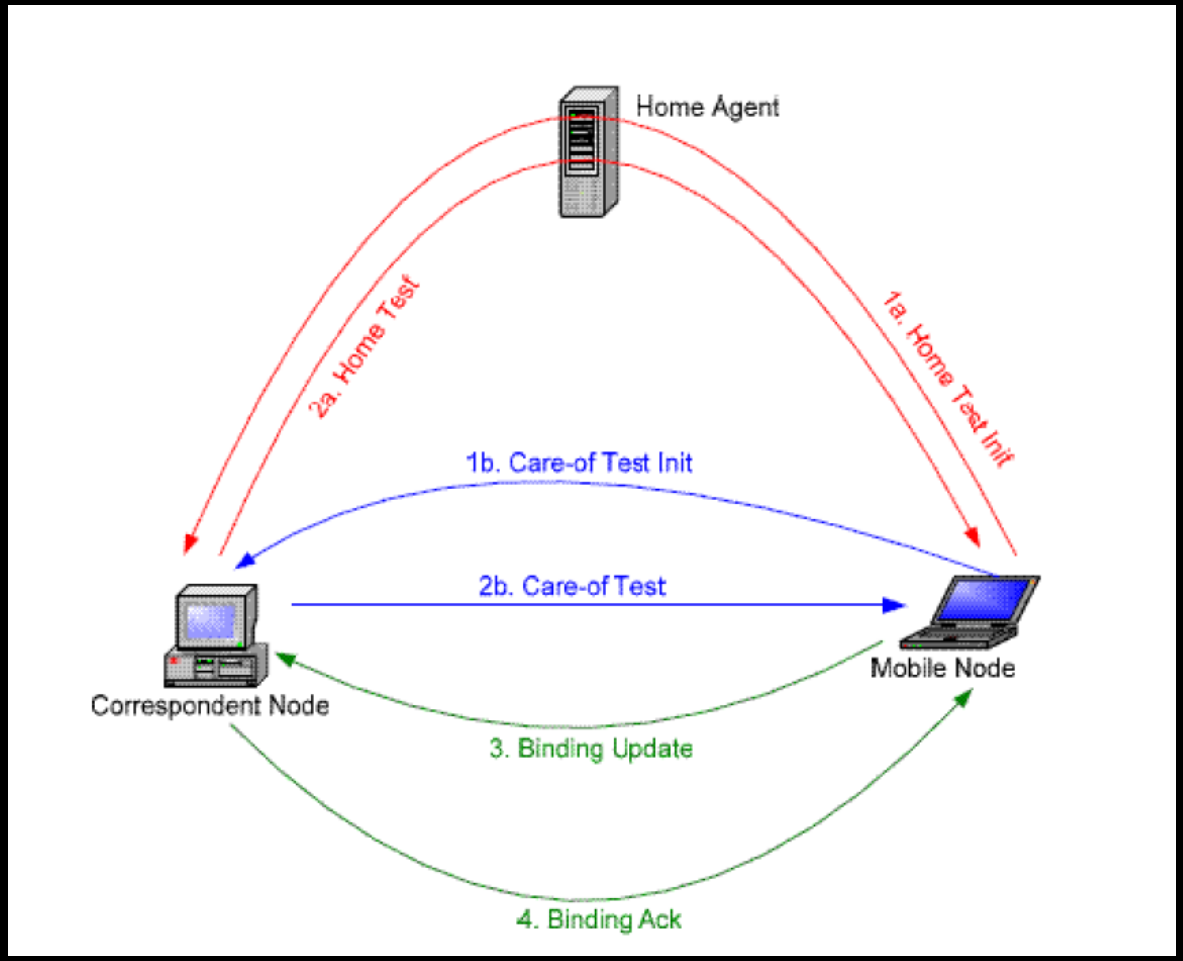
- Podpora stavového a bezstavového připojování se k sítí (objevování sousedů, ohlašování směrovačů).
- IPv6 nepodporuje fragmentaci – MTU si musí hlídat a určovat sama.

Podpora

- Základní myšlenka: každý má svůj domov (totiž směrovač, kterému říká, kde zrovna je a udržuje s ním kontakt).



Podpora mobility

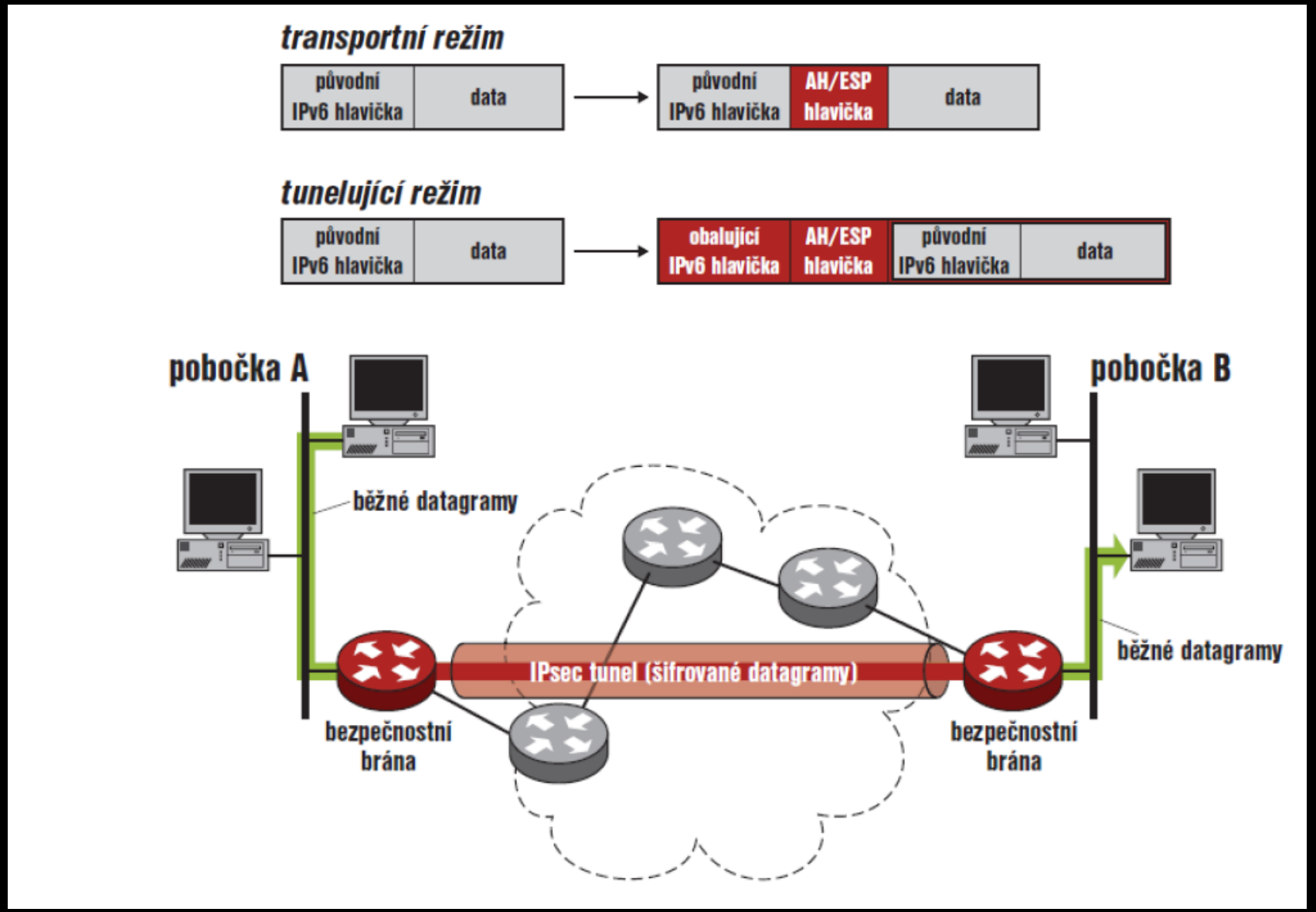


Bezpečnost obecně

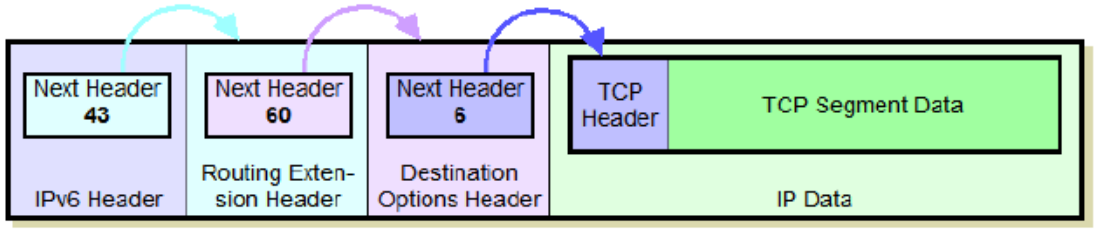
- Pro bezpečnost musíme zajisti CIA
  - Confidentiality – data nesmí přečíst nikdo nepovolaný.
  - Integrity – data nesmí být po cestě změněna či podvržena.
  - Availability – data smí číst jen autorizovaná osoba.
- Či AAA:
  - Autentizace
  - Autorizace
  - Accounting
- V IPv4 řešeno pomocí nepovinného IPSec.

Bezpečnost u IPv6

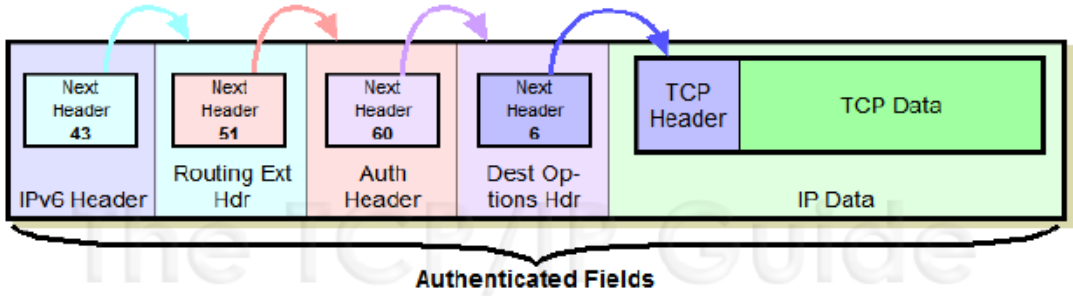
- AH (Authentication Header) – jen hlavička pro potvrzení autenticity vysílajícího
- ESP (Encapsulating Security Payload) – zabalení datagramu do šifrované podoby. Je volitelná.
- Definuje kryptografické metody, bezpečnostní politiku i správu klíčů.
- Dva modely přenosu dat – transportní či tunelující.


transportní režim
původní IPv6 hlavička
data
původní IPv6 hlavička
AH/ESP hlavička
data
tunelující režim
původní IPv6 hlavička
data
obalující IPv6 hlavička
AH/ESP hlavička
původní IPv6 hlavička
data
pobočka A
pobočka B
běžné datagramy
IPsec tunel (šifrované datagramy)
bezpečnostní brána
bezpečnostní brána
běžné datagramy

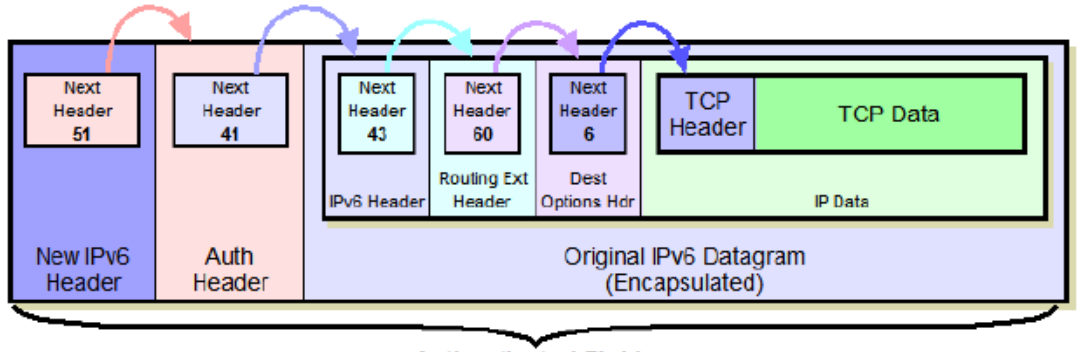
Př



Original IPv6 Datagram Format (Including Routing Extension Header and Destination-Specific Destination Options Extension Header)

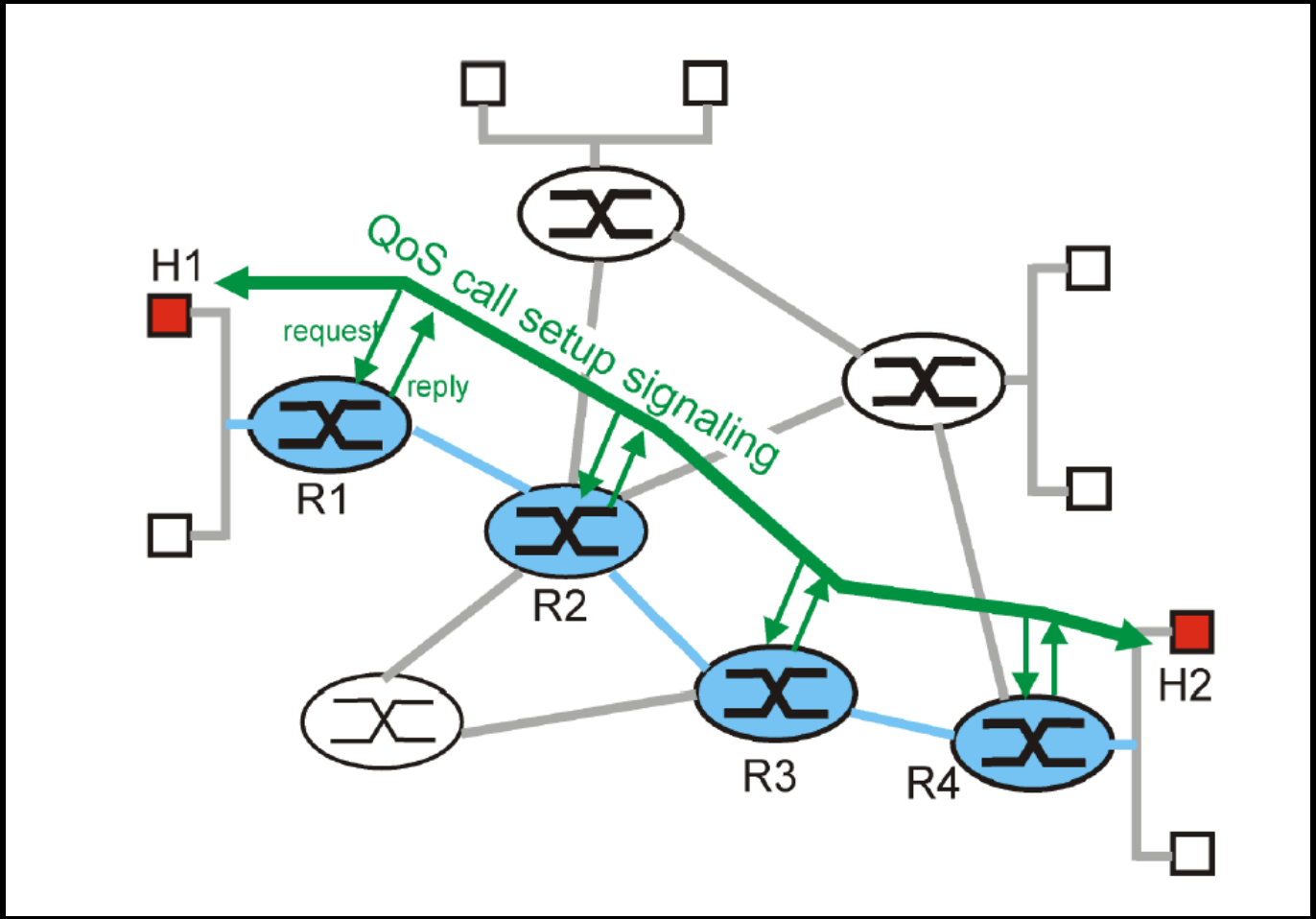


IPv6 AH Datagram Format - IPSec Transport Mode

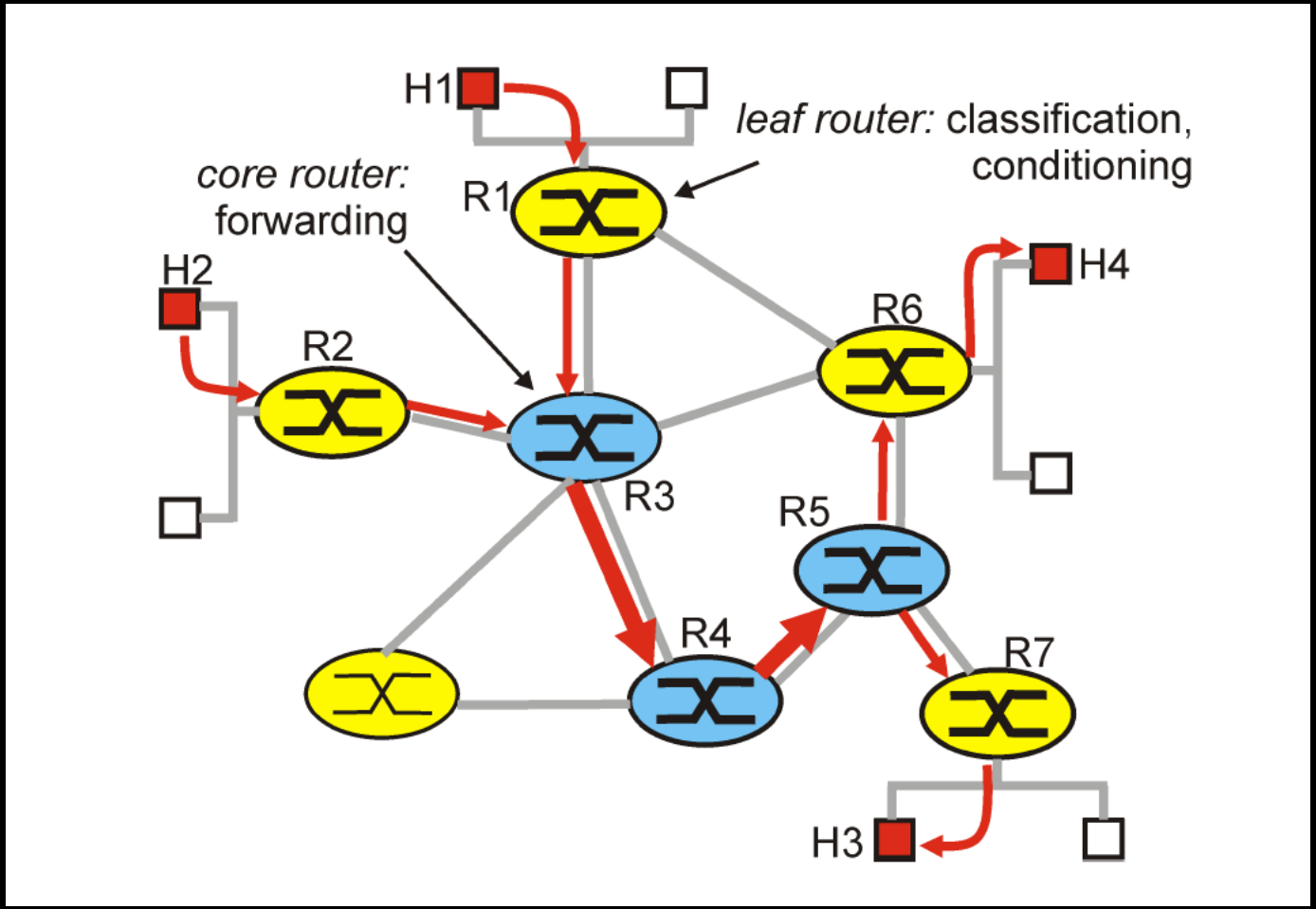


IPv6 AH Datagram Format - IPSec Tunnel Mode

Integrated Services



Dierentiated Services (příklad IPv6)



IPv6 a QoS

- V hlavičce je Treffic Class což je jeden byte => 64 možných úrovní priority.
- Můžeme postavit síť, která bude vysokoprioritní data (RT) odbavovat přednostně před maily atp., ale musíme to dělat rozumným způsobem.
- MPLS sítě umožňují pevné definování stálé cesty a tím pádem garantují QoS a lépe směrují, ale nejsou vždy vhodné pro dynamický provoz.

Přechod na IPv6

- Dvojitý zásobník – uzly podporují oba protokoly
- Tunelování – tunel spojuje dva stejně komunikující „internety“ zabalením do jiného protokolu.
- Translátor – mechanické namapování jedné adresy na druhou.

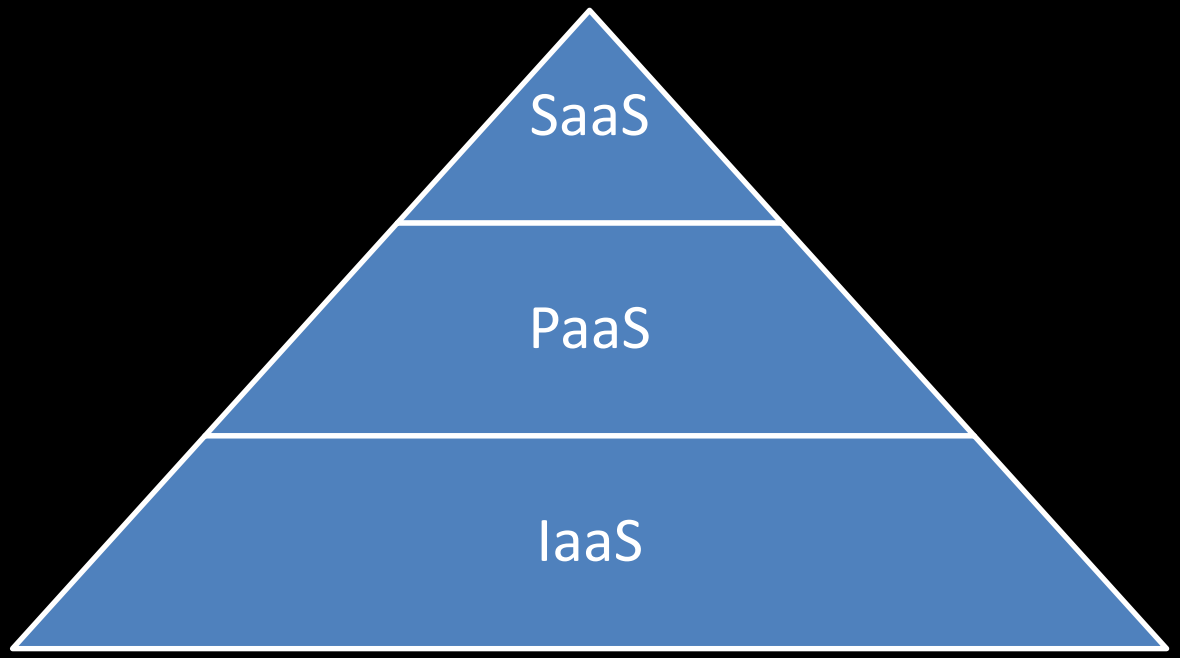
CLOUDCOMPUTING

Definice cloud computingu

- Termín označuje souhrnně technologie a postupy Používané v datových centrech a firmách pro zajištění snadné škálovatelnosti aplikací dodávaných přes Internet.

Taxonomie

- IaaS - pronájem hardwaru
- PaaS - platforma jako služba, hostovaný framework
- SaaS - pronájem aplikace



IaaS - Infrastruktura jako služba

- Jde o pronájem hardwaru na vyžádání. Typicky jde o servery, síťové prvky, zálohování, výpočetní výkon atp.
- Zařízení se objednává přes rozhraní služeb (např. Amazon EC2, Mosso apod.)

- *Výhody* – flexibilní možnosti nastavení hardwaru dle potřeb.
- *Nevýhody* – často vyšší cena, nutné zkušenosti.

PaaS - Platforma jako služba

- Pronájem platformy nad kterou aplikace běží. Velmi podobné tradičnímu hostingu. Nabízí se buď framework (RoR, Django) či prostředí nějakého jazyka (Java, .NET,…)

- *Výhody* – automatické škálování, bez nutností instalací, aktualizací a konfigurací.
- *Nevýhody* – závislost na poskytovateli a často jeho knihovnách, ztráta kontroly nad hardwarem.

SaaS - Software jako služba

- Zákazník nekupuje software, ale pronajímá si ho. Pronájem se
- odvíjí od četnosti využití, tedy zákazník platí jen když software
- využívá. Typicky webová aplikace - Google Apps, Zoho, Salesforce.com, Abakowiki.cz, GoodData.

- *Výhody* – dostupnost přes prohlížeč odkudkoli, rychlá aktualizace, údržba,…
- *Nevýhody* – možné uzamčení dat u poskytovatele, problematická migrace.

Model nasazení

- Veřejný (Public cloud computing): služba pro širokou veřejnost.
- Soukromý (Private cloud computing): jen pro jednu společnost.
- Hybridní (Hybrid cloud computing): propojení výše uvedeného, přes nějaké standardní rozhraní.
- Komunitní (Comunity cloud computing)