POČÍTAČOVÉ SÍTĚ

1. Základní komunikační funkce – synchronizace, adresace, detekce a oprava chyb, řízení přístupu, řízení toku, taxonomie sítí.

Synchronní, asynchronní přenos

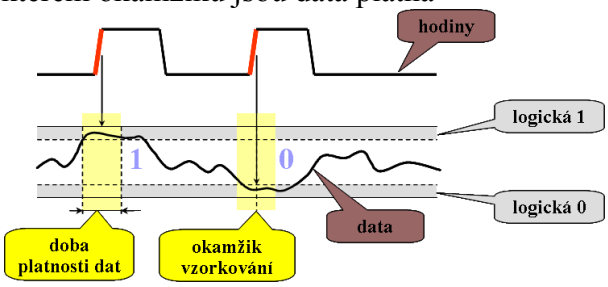
Synchronní = informace se přenášejí po jednotlivých bitech, vzdálenosti mezi nimi jsou pevně určeny

Asynchronní = okamžiky přechodu od přenosu jednoho bitu k přenosu dalšího bitu nejsou stejně vzdáleny, arytmický přenos.

Časová synchronizace

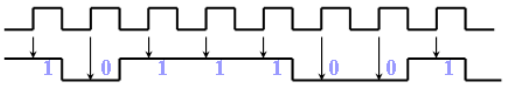
Hodinový signál-hodinový signál je v časovém vztahu s daty

- určuje, ve kterém okamžiku jsou data platná

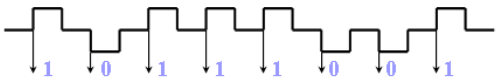


Metody odvození hodinového signálu

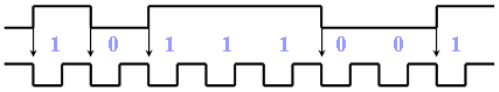
- hodinový signál se přenáší po samostatném vodiči



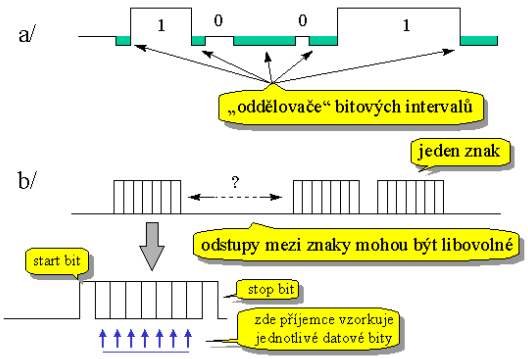
- hodinový signál se přenáší současně s daty



- hodinový signál lze také nějak zakódovat do přenášených dat



- **asynchronní arytmický přenos** – přenos slov je asynchronní, ale přenos jednotlivých bitů v rámci slova je již synchronní



Synchronizace přijímače a vysílače

v přijímači je nutné rozpoznat hranice jednotlivých symbolů bitů, znaků, bloků, zpráv…
přímá synchronizace – synchronizační informace je obsažena v přijímaném signálu

PŘEDPOKLAD:
časová základna přijímače se liší od časové základny vysílače jen málo a synchronizaci proto není nutné obnovovat v každém bitu
nepřímá synchronizace – synchronizační informace se odvozuje z přijímaného signálu
nepřímo – start-stopní (arytmický) přenos, fázový závěs (PLL)…

Adresace

- Každý paket v síti je adresován na jednu unikátní adresu.
- V sítích IP se adresuje pomocí adresy IP.
- Pomocí IP adresy dochází ke směrování
- Data uvnitř jedné sítě jsou doručována podle MAC adresy
- Protokoly ARP, RARP, DNS

Vznik a detekce chyb

mezi vysílačem a přijímačem dojde ke změně, např. vlivem rušení, přenášeného signálu, který se pak demoduluje a dekóduje na jiný znak, než byl původně vyslán – vysláno 1111, přijato 1101

Možnosti detekce:

- **parita (příčná a podélná)**
- **kontrolní součty**
- **cyklické redundantní kódy CRC (zdaleka nejlepší účinnost)**

Kódová (Hammingova) vzdálenost

je počet pozic, na kterých se řetězce stejné délky liší, neboli počet záměn, které je potřeba provést pro změnu jednoho z řetězců na druhý.
1010101010
1100110010
0+1+1+0+0+1+1+0+0+0 = 4 - Hammingova vzdálenost je 4.

PARITA

– jednoduchá metoda zabezpečení proti chybám
– ke kódu se přidá další bit, jehož hodnota udává počet jedniček MODULO 2
– parita zvyšuje kódovou oblast o 1

7bitová data	1byte s paritním bitem	
	sudá parita	lichá parita
0000000	**0**0000000	**1**0000000
1010001	**1**1010001	**0**1010001
1101001	**0**1101001	**1**1101001
1111111	**1**1111111	**0**1111111

např. **seriova linka**

Samoopravný kód umožňuje následnou opravu chyby v jediném bitu, přidává ke každému 8 bitovému bytu navíc pět bitů (resp. 6 bitů ke každému 16-bitovému slovu).

Kódová krychle

– symboly A, B jsou zakódovány pomocí 3 bitů tak, že při změně A na B nebo opačně se musí změnit hodnota všech 3 bitů

symbol	kód
A	0 0 0
B	1 1 1

kódová vzdálenost = 3
– je-li kódová vzdálenost větší nebo rovna 2n+1, umožňuje kód detekci 2n chyb a automatickou opravu n chyb

Zabezpečovací kódy

– větší kódové vzdálenosti lze dosáhnout speciálními kódy
  – Hammingovy a cyklické kódy využívají vlastnosti polynomů
  – zákrytové (Orchad) kódy využívají geometrické principy
– ve fyzikálním prostředí se chyby často vyskytují ve shlucích
  – rušivý impuls potlačí několik přenášených bitů za sebou
  – poškození povrchu optického či magnetického paměťového media zasáhne několik bitů za sebou
– důležitou vlastností zabezpečovacích kódů je odolnost proti shlukům chyb

BSC
Binary synchronous communication (bisync). Znakově orientovaný protokol spojové vrstvy.

HDSL
High-data-rate digital subscriber line. Jedna ze čtyř DSL technologií s přenosovým pásmem 1,544 Mb/s v obou směrech, využívající dva kroucené dvoupáry. Bez použití opakovačů je vzdálenost omezena na 3658,5 m.

Řízení přístupu
v době, kdy uzel nevysílá, zůstává část přenosové cesty přidělená uzlu zcela nevyužitá
výhodnější je **dynamické přidělování** (alokování) přenosového kanálu přenosové médium je přidělováno (typicky celé) dynamicky, na základě skutečné potřeby (**požadavku**)

Možné varianty řízení přístupu:
- **řízené metody** (deterministické) např. Token Passing (Token Ring, FDDI)
- **neřízené metody** (stochastické) – CSMA/CD
  - jejich pravidla obsahují „**náhodný**“ prvek – např. „počkej náhodně zvolenou dobu“
  - vedou k výsledku jen s určitou **pravděpodobností**
- **centralizované metody**
  - většinou jde o řízené (deterministické) metody – např. HDLC
- **distribuované metody**
  - metodu realizují jednotlivé uzly ve vzájemné součinnosti např. **CSMA/CD** (Ethernet)

Řízené centralizované metody
- počítají s existencí centrálního arbitra
- arbitr se musí dozvědět, kdo a kdy chce vysílat (získat přístup)
  - **metodou výzev** (polling) – centrální arbitr se pravidelně (cyklicky) dotazuje všech potenciálních zájemců o vysílání
  - **z explicitních žádostí uzlů** o právo na vysílání

Řízené distribuované metody
- nemají centrálního arbitra
- algoritmus přidělování „běží“ na všech uzlech
- počítají s důslednou disciplínou všech uzlů – že každý dodrží stanovená „pravidla hry“

varianty:
- **rezervační metody** – distribuovaná obdoba přidělování na žádost
- **prioritní přístup** – existuje způsob, jak žadatelé mohou ze svého středu vybrat jednoho, a ten může vysílat
- **metody s předáváním pověření** (token)
  - vysílá pouze držitel oprávnění
  - kruh je pouze logický
  - lze garantovat přístup do doby x

Neřízené distribuované metody
Metoda **Aloha** odešli, když potřebuješ (na nikoho se neohlížej), pokud nedostaneš včas potvrzení, opakuj
- dochází často ke kolizím, efektivnost do 18%

Metoda CSMA
- poslouchej nosnou, a pokud nikdo nevysílá, můžeš začít vysílat sám
- kdy může dojít ke kolizi:
  - více uzlů (zájemců o vysílání) současně zjistí, že nikdo nevysílá, a začne vysílat
  - více uzlů čeká, až někdo jiný přestane vysílat, a pak začnou všichni najednou

nenaléhající CSMA
- podívá se, jestli někdo vysílá, pokud ano, odmlčí se na náhodnou dobu

naléhající CSMA
- jakmile je volno, začne vysílat

Metody CD
- snaží se detekovat výskyt kolizí
- metody „bez CD“ pokračují ve vysílání, i když ke kolizi došlo
- metody s CD využívají schopnost detekce k (téměř) okamžitému ukončení vysílání
- uzel, který detekoval kolizi, vyšle zvláštní „rušení“ (jam), aby ostatní uzly určitě detekovaly kolizi také

Algoritmus CSMA/CD
- pokud nikdo právě nevysílá (CS), můžeš začít vysílat sám
- pokud někdo vysílá, čekej až skončí
- pokud začneš vysílat a dojde ke kolizi, přestaň, a odmlč se na náhodně zvolenou dobu
- při vyšší zátěži vykazují nestabilitu

Řízení toku

- Řízení toku je umožňují aktivní prvky
- *Routery*
- *Switche*

Rozdělení počítačových sítí (taxonomie)

Počítačové sítě můžeme rozdělit do různých skupin podle kritérii, které nemusí být přesně definována a můžou se vzájemně prolínat. To znamená, že výsledné skupiny nemají pevně určeny hranice a jedna síť může patřit do více skupin současně.
Nejzákladnější dělení je podle:
- Velikosti
- Topologie
- Přenosové rychlosti
- Typu uzlu
- Vztahu mezi uzly
- Architektury
- Mobility

2. Spojovaný a nespojovaný přenos, síťové modely a architektury, referenční model ISO/OSI, architektura TCP/IP

Přepojování okruhů (spojovaný přenos)

- pochází ze „světa spojů“
- obdoba telefonní sítě
- mezi příjemcem a odesilatelem **vzniká přímá, souvislá cesta**
- komunikace probíhá v reálném čase
- představa: od odesilatele vede až k příjemci jednolitá „roura“, kterou protékají data
- data nemusí být příjemci explicitně adresována

Přepojování paketů (nespojovaný přenos)

- pochází ze „světa počítačů“
- fungují tak prakticky všechny sítě **LAN a WAN**
- obdoba listovní pošty
- mezi příjemcem a odesilatelem **nevzniká** žádná souvislá **vyhrazená cesta**
- data se přenášejí po blocích (paketech, datagramech, buňkách, …)
- přenos neprobíhá v reálném čase – přestupní uzel nejprve přijme celý přenášený blok dat a teprve pak jej předá dál
- přenášená data musí být explicitně adresována

čím jsou bloky větší

- tím je přenos dat efektivnější klesá režie
- tím více rychlost přenosu závisí na kvalitě přenosové cesty, při chybě se musí opakovat přenos celého bloku
- tím větší je rozdíl mezi přepojováním paketů a přepojováním okruhů
  - důležité např. pro přenos zvuku a obrazu

při extrémně malých blocích (buňkách) se rozdíl téměř ztrácí – toho využívá technologie ATM – přenos dat je založen na přepojování velmi krátkých bloků dat (buněk), vyhovuje potřebám „světa spojů“ i „světa počítačů“

Síťový model a síťová architektura

síťový model je ucelená představa o tom, jak mají být sítě řešeny zahrnuje:

- **představu o počtu vrstev**
- **představu o tom, co má mít která vrstva na starosti**

nezahrnuje:

- konkrétní představu o tom, jak má která vrstva své úkoly plnit tedy **konkrétní protokoly**

síťová architektura obsahuje navíc také:

- konkrétní **představu o způsobu fungování jednotlivých vrstev** (tj. **obsahuje konkrétní protokoly**)

příklad síťového **modelu**: referenční model ISO/OSI

příklad síťové **architektury**: TCP/IP

switching = přepínání

- přepojování na nižší úrovni (linková vrstva)
- bere v úvahu jen nejbližší okolí uzlu
- lze řešit HW

routing = směrování

- přepojování na vyšší úrovni (síťová vrstva)
- bere v úvahu topologii celé sítě
- řeší se SW

ISO/OSI

- pokus o vytvoření univerzální síťové architektury
- pochází ze světa spojů
- používá se pro srovnávací účely

fyzická vrstva – zabývá se přenosem bitů

- neinterpretuje, co přenáší
- rozlišuje se paralelní a sériový přenos
- přenos v základní a přeloženém pásmu

linková vrstva – přenáší celé bloky (frames)

- zajišťuje přenos pouze v dosahu přímého spojení
- funguje spolehlivě, nespolehlivě, spojovaně, nespojovaně
- synchronizace na úrovni rámců
- zajištění spolehlivosti – detekce chyb
- řízení toku
- přístup ke sdílenému médiu

síťová vrstva

- přenáší bloky dat jako datagramy či pakety
- zajišťuje doručení paketů až ke koncovému adresátovi
- v prostředí, kde není přímé spojení, hledá vhodnou cestu až k cíli
  - zajišťuje tzv. směrování (routing)
- musí si uvědomovat skutečnou topologii celé sítě (obecně)
- může používat různé algoritmy směrování: adaptivní, neadaptivní, izolované, distribuované
- data v přestupních uzlech se nedostanou výš než na úroveň síťové vrstvy

transportní vrstva – s vlastnostmi a funkcemi nižších vrstev nelze „hýbat“

- vyšší vrstvy mohou chtít něco jiného, než co nabízí nižší vrstvy
- je úkolem transportní vrstvy zajistit potřebné přizpůsobení!
- může měnit:
  - **nespolehlivý charakter přenosu na spolehlivý**
  - **méně spolehlivý přenos na více spolehlivý**
  - **nespojovaný přenos na spojovaný**

relační vrstva – zajišťuje vedení relací

- může zajišťovat: **synchronizaci, šifrování**, podporu transakcí

prezentační vrstva – nižší vrstvy se snaží doručit každý bit přesně tak, jak byl odeslán

- stejná posloupnost bitů může však mít pro příjemce jiný význam než pro odesilatele,
- např. pro rozdíly:
  - **v kódování znaků (ASCII, EBCDIC,…)**
- **prezentační vrstva má na starosti potřebné konverze**

aplikační vrstva – původně měl obsahovat aplikace

- problém: aplikací je moc, musely by být všechny standardizovány
- později:
  - aplikační vrstva měla obsahovat pouze „jádro“ aplikací, které má smysl standardizovat
  - například přenosové mechanismy elektronické pošty

TCP/IP

- obsahuje ucelenou představu o počtu a úloze vrstev
- síťová architektura – obsahuje konkrétní protokoly
- nejdříve vznikají protokoly a později vrstvy

TCP/IP	ISO/OSI
Aplikační	Aplikační
	Prezentační
	Relační
Transportní	Transportní
Síťová	Síťová
Vrstva síťového rozhranní	Linková
	Fyzická

vrstva síťového rozhraní

- zahrnuje vše, co se nachází „pod síťovou vrstvou“
- předpokládá se, že bude používat to, co vznikne někde jinde

síťová vrstva

- zajišťuje pouze nespojovaný a nespolehlivý přenos
- protokol IP snaží se **zakrývat specifika přenosových technologií** nižších vrstev a fungovat nad nimi optimálně

transportní vrstva

- sama využívá **nespojovaný a nespolehlivý přenos na úrovni síťové vrstvy**
- sama **nabízí spojovaný a spolehlivý přenos**
- protokol **TCP** /transmission control protocol/
  - zajišťuje spolehlivý přenos a spojovaný
  - tváří se jako proud /stream/
- protokol **UDP** /User Datagram Protocol/
  - zajišťuje nespojovaný a nespolehlivý přenos

aplikační vrstva

- koncepce obdobná modelu ISO/OSI
- původní – elektronická pošta, přenos souborů – později vznikají další, sdílení souborů, správa sítě…

3. Přístupové metody ke sdílenému médiu na 2. vrstvě. Technologie Ethernet, typy a vlastnosti aktivních síťových prvků.

První komerčně dostupná verze Ethernetu byla společným projektem firem DEC, Intel a XEROX (Ethernet II, DIX Ethernet), dnešní podoba je standardizována organizací IEEE – existuje celá řadaverzí (včetně Wireless)

Ethernet
- *přenosové cesty:* optické, drátové
- *rychlosti*: 10,100,1000 Mb/s
- *paket:* hlavička a datová část (adresa odesilatele, příjemce, opravny crc kod)
- *adresace:* pevně alokovaná adresa 48 bitů (světově unikátní)
- *zabezpečení:* 32-bitový cyklický kód (CRC)
- *řízení přístupu:* adaptivní CSMA/CD

Ethernet 10Mb/s

- 10BASE-T hvězdicová topologie (společné medium tvoří opakovač nebo port přepínače),
- MAU (Samostatné jednotky, ke kterým lze připojit až 8 uzlových počítačů.) na desce, připojení
- k rozbočovači nebo přepínači konektorem RJ45 a dvojicí kroucených dvoulinky
- 10BASE-F verze používající optické kabely (FL, FB, FP)

Ethernet 100Mb/s je 10x rychlejší

- všechny časy jsou 10x kratší, ve stejném poměru se však zmenšily maximální vzdálenosti
- 100BASE-TX hvězdicová topologie, populární díky kompatibilitě s 10BASE-T, připojení konektorem RJ45 a dvojicí kroucených dvojvodičů; některé síťové prvky se dokáží automaticky přizpůsobit provozu rychlostí 10 i 100 Mb/s
- 100BASE-FX varianta pro připojení optickým kabelem
- 10BROAD36 verze 10Mb/s používající technologii kabelové televize

Wireless Ethernet

- bezdrátová verze Ethernetu, používá kódový multiplex

Ethernet 1Gb/s

- nová verze Ethernetu, opět 10x rychlejší než Ethernet 100Mb/s (max.délka přípojky 25m)

Aktivní prvky:

- fyzická vrstva: opakovač (repeater), rozbočovač (hub)
- linková vrstva: most(bridge), přepínač (switch)
- síťová vrstva: směrovač (router)
- aplikační vrstva: brána (gateway)

Opakovač:

- je to pouze digitální zesilovač, zesilující a znovu tvarující přenášený signál
- funguje v reálném čase až na malé zpoždění způsobené elektronickými prvky
- kompenzuje zkreslení, útlum a další vady reálných přenosových cest
- vše, co přijímá, rozesílá („opakuje“) do všech připojených segmentů
- šíří i kolize a poškozené pakety
- uzly v jiných segmentech musí poznat, že k ní došlo
- propojené segmenty tvoří jednu kolizní doménu tj. oblast, ve které současné zahájení vysílání kterýchkoliv dvou uzlů způsobí kolizi
- kolizní doména končí až na nejbližším mostu, přepínači nebo směrovači
- Mosty, přepínače a směrovače se nezajímají o datový obsah rámců resp. Paketů mohou propojovat jen takové systémy, které do rámců/paketů „balí“ stejná data, tj. stejné systémy,
- ev. systémy lišící se v přenosových technologiích nižších vrstev

Switche:

Princip fungování

- Jako opakovač
- Naplnění směrovací tabulky MAC adresami
- Další přenos už je analyzovaný
- Switch vždy pracuje plnou rychlostí sítě
- Propustnost přepínače je dána CPU
- store and forward – celý rámec do paměti (možná detekce poškozeného rámce, větší latence)
- cut throught – z bufferu se přečte jen hlavička a poté okamžité odeslání, jednodušší algoritmus, větší propustnost
- přepínání přepojování na úrovni linkové vrstvy
- bere v úvahu jen nejbližší okolí uzlu
- rozhodování o dalším směru přenosu je jednoduché
- obecně jednodušší a rychlejší
- lze „zadrátovat“ (tj. řešit přímo v HW)

Routry:

- směrování přepojování na úrovni síťové vrstvy
- bere v úvahu topologii celé sítě
- vyžaduje náročnější rozhodování o dalším směru přenosu dat
- obecně složitější a pomalejší
- řeší se v SW, nelze snadno řešit pomocí HW

Brány:

- pro spolupráci odlišných systémů je nutné rozumět přenášeným datům a provádět jejich konverzi
- brány jsou vždy aplikačně orientované, rozumí jen datům určité aplikace (aplikací)

Přístupové metody ke sdílenému médiu

Řízené centralizované metody

- počítají s existencí centrálního arbitra
- arbitr se musí dozvědět, kdo a kdy chce vysílat (získat přístup)
- jinak by muselo jít o statické přidělování
- *jak se to arbitr může dozvědět?*
    - metodou výzev (polling) – centrální arbitr se pravidelně (cyklicky) dotazuje všech potenciálních zájemců o vysílání
    - z explicitních žádostí uzlů
    - zájemce musí „explicitně požádat“ o právo na vysílání
    - musí existovat možnost vyslání dotazu k arbitru
    - výhody-nezdržují se přenosy-nevýhody – velká režie

Řízené distribuované metody

- nemají centrálního arbitra
- mají plně deterministická “pravidla hry“
- algoritmus přidělování „běží“ na všech uzlech
- počítají s důslednou disciplínou všech uzlů – že každý dodrží stanovená „pravidla hry“
- *varianty:*
    - rezervační metody – distribuovaná obdoba přidělování na žádost
    - prioritní přístup – existuje způsob, jak žadatelé mohou ze svého středu vybrat (koordinovaným, deterministickým způsobem) jednoho, a ten může vysílat
    - metody s předáváním pověření (token) logický kruh
        - vysílá pouze držitel oprávnění
        - token – pešek – speciální balíček dat

- kruh je pouze logický
- lze garantovat přístup do doby x

Neřízené distribuované metody

- Metoda Aloha (tzv. „čistá“)
  - vznikla na univerzitě na Havajských ostrovech
  - potřebovali přenášet data mezi ostrovy, neměli vhodnou infrastrukturu
  - využívá rádiového přenosu
  - přenosu „éterem“, jedním společným kanálem se všesměrovým šířením
  - strategie: odešli když potřebuješ (na nikoho se neohlížej) pokud nedostaneš včas potvrzení, opakuj
  - dochází často ke kolizím
  - efektivnost do 18%
- Metoda CSMA
  - „čistá“ Aloha nemonitorovala provoz na kanále – nerozpoznala, že už někdo vysílá
  - metody CS (Carrier Sense) využívají možnosti „odposlechu nosné“ a díky tomu dokáží zmenšit počet kolizí, ale nedokáží je odstranit zcela
  - princip (chování uzlu): poslouchej nosnou, a pokud nikdo nevysílá, můžeš začít vysílat sám
  - *kdy může dojít ke kolizi:*
    - více uzlů (zájemců o vysílání) současně zjistí, že nikdo nevysílá, a začne vysílat
    - více uzlů čeká, až někdo jiný přestane vysílat, a pak začnou všichni najednou
- Nenaléhající CSMA
  - podívá se, jestli někdo vysílá – pokud anoo odmlčí se na náhodnou dobu
- p-naléhající
  - podívá se, jestli někdo vysílá – pokud ano odmlčí se na 1/p zvloneou náhodnou dobu
- naléhající CSMA
  - jakmile je volno, začne vysílat

Metody CD

- snaží se detekovat výskyt kolizí
- metody „bez CD“ pokračují ve vysílání, i když ke kolizi došlo
- metody s CD využívají schopnost detekce k (téměř) okamžitému ukončení vysílání
- některé uzly nemusí kolizi správně detekovat
- uzel, který detekoval kolizi, vyšle zvláštní „rušení“ (jam), aby ostatní uzly určitě detekovaly kolizi také

Algoritmus CSMA/CD

- pokud nikdo právě nevysílá (CS), můžeš začít vysílat sám
- pokud někdo vysílá, čekej, až skončí
- pokud začneš vysílat a dojde ke kolizi, přestaň, a odmlč se na náhodně zvolenou dobu
- při vyšší zátěži vykazují nestabilitu

4. Adresování ve 2. a 3. vrstvě, MAC-adresa, IP-adresa, protokoly ARP a RARP, třídy IP-adres, podsítě a supersítě. Princip všesměrového adresování, šíření kolizí a všesměrového vysílání, kolizní doména, broadcast doména.

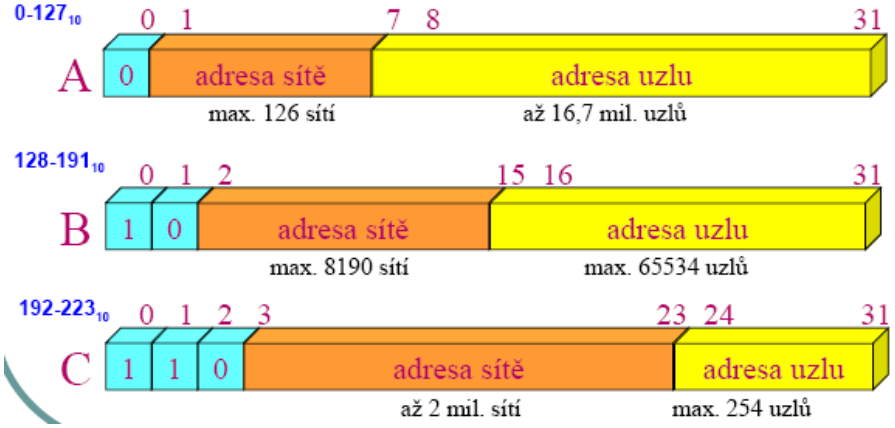
MAC – jednoznačná identifikace na LV **48 bit** (první tři oktety = výrobce, další 3 identifikace karty v rámci výrobce). např. 00-00-64-65-73-74

IP adresa je jednoznačná identifikace konkrétního zařízení v prostředí Internetu. Veškerá data (ve formě datagramů), která jsou posílána z daného zařízení přes počítačovou síť, obsahují IP adresu odesilatele i příjemce. Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. Dnes nejčastěji používaná je jeho IPv4, postupně se však bude přecházet na novější verzi IPv6. V jiných protokolech se adresování jednotlivých zařízení může provádět jinak (viz např. MAC adresa)

Třídy IP adres

- **A** 126 sítí 16,7 mil. uzlů [intranet – 10.0.0.0/8] /8 = počet bitů masky
- **B** 8190 sítí 65. 534 uzlů [intranet – 172.16.0.0/12]
- **C** 2 mil. sítí max 254 uzlů [intranet – 192.168.0.0/16]
- InterNIC přiděluje IP adresy po skupinách národním distributorům ty je přidělí po skupinách providerům

Třídy adres:
proměnný formát adresy spočívá v různém nastavení "předělu" mezi adresou sítě a adresou uzlu v rámci sítě



Podsítě:

- velký počet adres třídy C způsobuje komplikace
  - každé adrese C odpovídá ve směrovacích tabulkách jedna položka
  - ... směrovací tabulky se tím stávají neúnosně velké!
- možné řešení: použít adresy třídy B, ale těch je málo

Využijeme techniku podsítí (subneting)
technika, umožňující efektivněji využívat adresový prostor IP adres
umožňuje zavést jiné jemnější dělení adresy na dvě logické složky
umožňuje vytvářet „logické podsítě"
Supersíť: spojení podsítí jednou maskou 255.255.0.0
Kolizní doména je oblast kde dochází ke kolizím na úrovni linkové vrstvy (vysílá moc lidí).

IP: 130.75.27.11192.168.32.34
Maska: 255.255.0.0

M and IP130.75.0.0	adr. sítě	Využívá se u směrování
M' and IP0.0.27.11	adr. hosta	

M‘ or IP130.75.255.255 broadcast Data jsou doručeny všem uzlům v síti

Kódování tříd adres

- Iterativní
- A - 0xxx
- B - 10xxx
- C - 110xxx

Kolize

– při časovém multiplexu obvykle nesmí vysílat více uzlů najednou
  – „technicky“ to většinou moc nevadí - obvykle nedojde k poškození přenosové cesty
  – vadí to však „logicky“
    – dochází k nežádoucímu „smísení“ signálů
    – jeden zdroj signálu ruší druhý
    – pokud k takové situaci dojde, hovoříme o kolizi
– frekvenční a kódový multiplex obvykle připouští současné vysílání více uzlů

ARP je jedním možným mechanismem dynamického **překladu IP adres na fyzické adresy** nikoli jediným možným řešením!

- využívá možnosti všesměrového vysílání (broadcastingu) např. v Ethernetu
- ARP dotaz obsahuje IP adresu, ke které se hledá fyzická adresa. Tento paket se rozešle všem uzlům dané sítě (směrovače nesmí šíření paketu omezit)
- ARP odpověď posílá uzel, který rozpoznal svoji IP adresu.
  K odpovědi připojí i svou fyzickou adresu

důsledek:
tázající se dozví potřebnou fyzickou adresu

Jednotlivé uzly si své IP adresy mohou pamatovat samy (na svých pevných discích)

- ne vždy je to možné (např. u bezdiskových stanic)
- ne vždy je to vhodné (zejména pro správu sítě a správu konfigurací)

Každý uzel musí znát svou IP adresu ještě dříve, než vyšle či přijme svůj první IP paket!

RARP se v počítačových sítích s IP protokolem používá k **získání vlastní IP adresy počítače při znalosti MAC adresy**

Vysílající vyšle RARP dotaz obsahující vlastní MAC adresu. Dotaz se posílá na MAC broadcast, tedy všem počítačům v dané fyzické síti. V ní by se měl nacházet RARP server opatřený tabulkou obsahující IP adresy příslušející jednotlivým MAC adresám. Server prohlédne tabulku, a pokud v ní najde MAC adresu tazatele, pošle mu zpět RARP odpověď (RARP reply) s IP adresou, kterou si má nastavit.

- RARP pakety se vkládají přímo do linkových rámců
- RARP se používá především v Ethernetu (využívá broadcasting)
- RARP neprojde přes směrovače,
  tj. jeho působnost je omezena na lokální síť

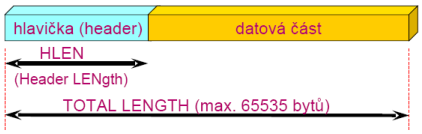
5. Protokol IP, formát paketu a záhlaví, doba života paketu (TTL), maximální velikost paketu (MTU). Průchod IP-paketu sítí, fragmentace a defragmentace, úloha protokolu ICMP.

Protokol IP

- Stará se o doručení dat z jednoho uzlu na druhý
- Směrování IP paketů v síti
- Definuje formát IP paketů
- Implemetuje jednotné adresování IP
- Ošetřuje nestandartní situace

IP Datagram (paket)

- Zapouzdřuje data z vyšších vrstev
- Skládá se z hlavičky (20 B) a datové části
- Max 65535 B



Hlavička IP paketu

- Verze – první položka, verze IP, pro IPv4 obsahuje 4
- Délka záhlaví
  - v násobcích „čtyřbajtů“ (32bitů) – např. pro délku 20B obsahuje 5
  - záhlaví se proto vždy doplňuje na velikost dělitelnou 4B
  - maximální velikost záhlaví je tedy 11112 x 4B=1510 x 4B = **60B**
  - povinné položky zabírají **20B** – na volitelné tedy zbývá 40B
- Typ služby
  - dlouho nevyužitá položka
  - dnes se používá maximálně jako jednoduché QoS
- Celková délka
  - celková délka IP datagramu (včetně hlavičky) v B
  - 2B → 65536 - nulová velikost = **65536B**
- Identifikace IP datagramu
  - základní identifikátor datagramu
  - datagramy mohou do cíle přijít v různém pořadí – je třeba je pak podle něčeho seřadit
- Fragmentační příznaky
  - popisují možnost fragmentace datagramu
- Offset fragmentu
  - použije se v momentě vytváření fragmentovaného datagramu
- Tyto položky úzce souvisejí s možností fragmentace (rozdělováním) datagramů při průchodu některými cestami
- Doba životnosti datagramu - Time to live (TTL)
  - slouží k zamezení nekonečného toulání datagramu po směrovačích
  - každý směrovač snižuje např. o 1
  - při TTL=0 se datagram zahazuje
    - odesilateli je odeslán ICMP
- Protokol vyšší vrstvy
  - číselná identifikace vloženého protokolu
  - málokdy se komunikuje přímo IP protokolem
  - proto je vkládán další vyšší protokol (např.: 6-TCP, 17-UDP...)
- Kontrolní součet z IP záhlaví
  - pouze ze záhlaví

- problémem je, že pokud se něco změní v hlavičce (např. TTL) musí se CRC znovu dopočítat

Fragmentace IP Paketu

- Přenos je nejefektivnější když můžeme celý paket vložit do linkového rámce bez dělení. – IP protokol se o to snaží
- parametr **MTU Maximum Transfer Unit** – je definován v konfiguraci PC
- IP protokol má nástroje pro (de)**fragmentaci** paketů
- Defragmentaci provádí příjemce
- Není rozumné přizpůsobovat velikost **minimu** ze všech síťových prvků
- Každý fragment zatíží sít novou hlavičkou.
- Identifikace – podleni se zjisti které pakety patri k sobe
- Offset – podleni se zjisti na jako pozici patri paket, offset = 0 první paket

MTU

Maximum transmission unit, zkráceně MTU (česky maximální přenosová jednotka). V sadě protokolů internetu se jedná o označení maximální velikosti IP paketu, který je možné přenést z jednoho síťového zařízení na druhé. Obvyklá hodnota MTU v případě Ethernetu je 1500 bajtů, nicméně mezi některými místy počítačové sítě (spojených například modemem nebo sériovou linkou) může být maximální délka přeneseného paketu nižší.

Maximální možnou velikost MTU na trase lze zjistit metodou Path MTU discovery, kdy je vyslán datagram s nastaveným příznakem *Do not fragment* (nefragmentovat). Pokud některý router potřebuje provést fragmentaci (která je zakázána), je pomocí protokolu ICMP oznámena odesílateli chyba.

Servisní protokoly a diagnostika

ICMP - Internet Control Message Protocol

- Povinná součást všech realizací IP protokolů
- Mechanizmus **pro hlášení chyb** a **nestandartních situací**
- ICMP pakety jsou přenášeny **v datové části IP paketů**
- ICMP pakety mohou být filtrovány

Složení ICMP

- Typ - hrubé dělení zpráv
- Kód - Jemné dělení
- Podle těchto polí se odlišuje hlavička i tělo zprávy

Použití ICMP

- **Echo** - dosažitelnost uzlů
- **Nedoručitelný paket** - informování adresáta pomocí ICMP
- Čas vypršel - TTL = 0 **Tracert**

6. Směrování, směrovací tabulky, směrovací protokoly.

Směrování Routing – hledání cest **v počítačových sítích**. Úkolem je dopravit datový paket určenému adresátovi, pokud možno co **nejefektivnější cestou**.

Směrovací tabulka – sadu ukazatelů, podle kterých se rozhoduje, co udělat s kterým paketem.

Adresa cílové sítě: "IP + Maska" Příští adresa Síťové rozhraní Metrika

1. Procházení po řádcích – Vyhodnocení Maska x uzel
2. pro více vyhovujících rozhoduje Metrika
3. Pro žádný záznam se použije default s maskou 0.0.0.0

Konstrukce směrovacích tabulek

- **Manuálně**
- **Dynamicky** pomocí **ICMP**
- Dynamicky pomocí **směrovacích protokolů**
- Příme směrování se využívá na stejné dílčí síti – je snadné
- Nepřímé směrování – paket putuje přes více sítí
- Routery na každém TCP/IP segmentu tvoří vzájemně spolupracující soustavu

Hostitelská PC se od Routerů *"učí"*
Směrovače upozorňují PC pomocí ICMP o existenci jiných routerů **ICMP redirect**

ICMP a směrování

- Reakci na **zahlcení**
- Informaci o **zacyklení** cest
- Testuje **dosažitelnost** uzlů **"ICMP echo"**

Dřívější představa Internetu

- Core gateways
- NonCore gateways

Dnešní routování

- Soustava **autonomních systémů**
- Stromovitá struktura
- Soustava Core gateways kořen stromu

IGP Interior Gateway Protocols – napr. RIP, OSPF, EGRP

- Automatické směrovací protokoly dynamicky vytvářejí *směrovací tabulky*
- Snadná *adaptace* na změny v topologii
- Hledání **optimální cesty** – různými metodami
- **Centralizované směrování – (distribuce** směrovací tabulky centrálem)
- **Izolované směrování** – pouze znalost okolí (záplavové vs horká brambora)

Algoritmy pro výpočet směrovacích cest

- **DVA** – Distance Vector Alghoritm (**RIP**, IGRP, E-IGRP) – ohodnocení cesty (délky) HopCount
- **LSA** – Link State Alghoritm (NLSP, **EGP, OSPF**, IS-IS) – kvality cesty

Interní protokoly

RIP Routing Information protocol

- DVA
- Metrika – počet směrovačů = 15
- Broadcast požadavek do všech sítí na směrovací informace
- Podle odpovědí se sestaví směrovací tabulka

IGRP Interior gateway routing protocol

- Cisco standard
- 5 metrik

1. počet přeskoků
2. zpoždění přenosu
3. šířka pásma
4. spolehlivost
5. zatížení

- 1994 → **EIGRP**
- Aktualizace řízené událostmi

OSPF Open Shortest path First

- Periodická aktualizace
- limit 15 routerů
- Volitelná metrika
- Distribuovaný výpočet ST = **LSA**

Externí protokoly

EGP Exterior Gateway Protocol

- **Stromová** struktura
- **bez metriky**
- **Zjisti** každému routeru **sousední router,** se kterým bude komunikovat

BGP Border Gateway Protocol

- novější na bázi **hvězdicové** struktury
- Na poprvé vysílá celé **směrovací mapy**
- vysílá periodicky jen **aktualizuje**

7. Transportní protokoly TCP a UDP, rozdílné a společné vlastnosti, porty. Potvrzovací mechanizmus v TCP, třícestné navazování spojení, technika zpožděné odpovědi.

- služby transportní vrstvy používají entity aplikační vrstvy
- **zajišťuje komunikaci koncových účastníků**
- **rozlišuje zdrojovou a cílovou aplikaci**
- rodina protokolů TCP/IP nabízí v transportní vrstvě dva alternativní protokoly:
  TCP = Transmission Control Protocol
  UDP = User Datagram Protocol
- oba využívají **nespolehlivý a nespojovaný přenos** (IP), zajišťovaný síťovou vrstvou

Protokol TCP
- **spojovanou** službou, TCP segment
- přidává **spolehlivost** kontroluje **integritu paketů**, zajišťuje **opakování přenosu** poškozených a ztracených paketů, kontroluje a opravuje pořadí došlých paketů, vyřazuje zdvojené pakety, funguje na spojovaném principu, mezi odesilatelem a příjemcem vytváří **virtuální spoj, plne duplexni,** Přenášené **bajty jsou číslovány**. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena **kontrolním součtem.**

Protokol UDP
- nespojová služba, UDP datagram
- nezajišťuje spolehlivost
- nenavazuje spojení
- maximálně jednoduchou "obálkou" nad protokolem IP nabízí prakticky tytéž přenosové služby jako IP
- odesilatel odešle data a více se o ně nestará, o to se musí postarat až aplikace na aplikační vrstvě

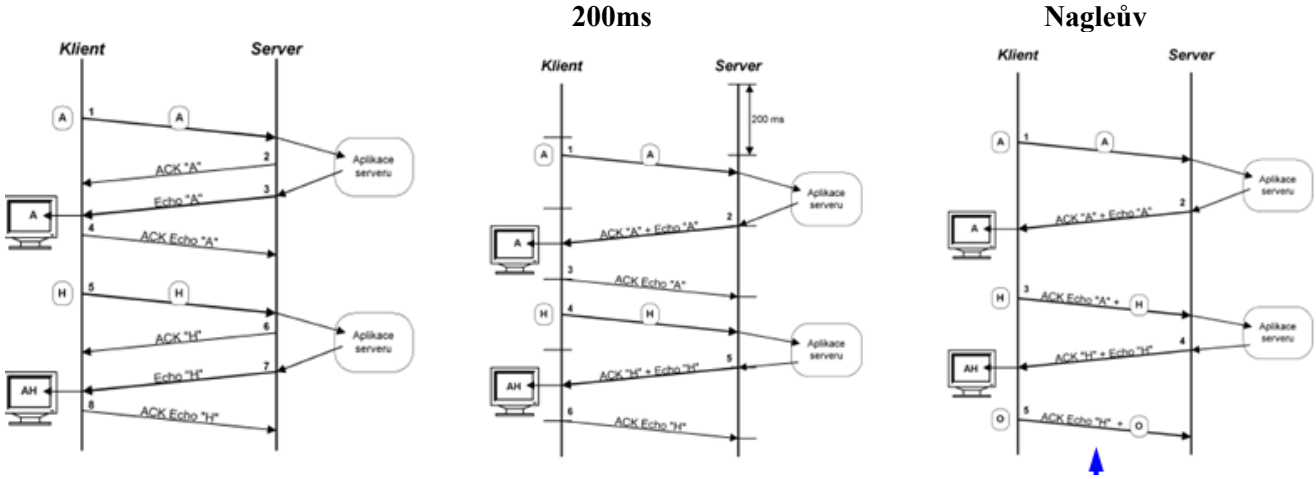
Porty – číselná označení programů (služeb) běžících na jednom stroji.
- transportní protokoly (UDP i TCP) musí přebírat data k přenosu od více odesilatelů a přijatá data rozdělovat mezi více potenciálních příjemců.
- k **rozlišení aplikace** v rámci počítače.
- Čísla portů mohou být přidělena **staticky** – předem dohodnutá (a všem známá)
  - servery pak budou dostupné na portech s předem dohodnutými (známými) čísly
  - Všeobecně známé porty – dokumentech RFC
  - 21 = FTP, 23 = telnet, 42 = name server, 80 = www server, 110 = POP3 server
- mohou vznikat **dynamicky** – přidělována až v okamžiku **jejich vzniku** (generovaná čísla portů)
  - server číslo portu klienta předem nemusí znát, dozví se ho z žádosti klienta o službu

kompletní adresace v Internetu tedy je: IP adresa + číslo portu + použitý protokol

třícestné navazování spojení
- **Klient začíná navazovat spojení – 1**
  - TCP paket 1, připojuje se na port 4433, nastaven SYN, vygeneruje startovací pořadové č. odesílaného bajtu ISN
  - 1 je prvním segmentem – nemůže potvrzovat žádná data, není nastaven ACK
- **Server potvrzuje spojení, navazuje 2. – 2**
  - nastaven ACK (zadost o potvrzeni), nastaven SYN
- **Klient potvrzuje 2. spojení – 3**
  - nastaven ACK

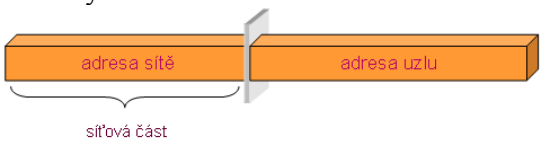
Technika zpožděné odpovědi

- snaha objem přenášených dat zmenšit, čímž se snažíme zabránit ucpání přenosových cest. Myšlenka spočívá v tom, že potvrzování přijatých dat nebude probíhat okamžitě, ale se zpožděním. Během tohoto zpoždění se pak mohou objevit i další data k přenosu.
- **Zpoždění 200 ms** – operační systém spustí pro tento účel hodiny zpravidla s tikem 200 ms (pod 500 ms). Po každém tiku systém zkontroluje, zda-li není něco k odeslání (potvrzení přijatých dat či odeslání dat). Pokud je třeba něco odeslat, pak vše odešle najednou. Jenže je již málo pravděpodobné, že klient stiskne další klávesu H, tak aby software klienta byl schopen znak H odeslat společně s potvrzením přijetí echa klávesy A. Proto jak je z následujícího obrázku patrné klient provede potvrzení echa klávesy A pomocí segmentu a stisk klávesy H způsobí vyslání dalšího TCP segmentu.
- **Nagleův algoritmus** - čeká až dojdou nějaká data od protistrany ⇨ vyrovnává dobu odezvy vůči kapacitě linky



8. IP verze 4 a řešení nedostatku adres, privátní rozsahy, NAT.

stav v IP verze 4 – teoreticky 4 miliardy adres



Řešení nedostatku adres:
podsítě

- velký počet adres třídy C způsobuje komplikace.
- každé adrese C odpovídá ve směrovacích tabulkách jedna položka. ST se tím stávají neúnosně velké!
- možné řešení: použít adresy třídy B, ale těch je málo
- jak adresu rozdělit, aby mohla být využita pro více sítí?
- **podsíť** = technika, umožňující efektivněji využívat adresový prostor IP adres – zavádí jiné **dělení** 32-bitové IP adresy na dvě logické složky, než je definováno třídami A, B a C
- umožňuje vytvářet „**logické podsítě**"

- Idea dělení na podsítě (subnettingu):
  - hranice (bitová pozice) se posune směrem k nižším bitům
    - **adresy uzlů se rozdělí na několik skupin**
      - velikosti mocniny 2, aby to byl posun o celé bitové pozice
    - **použijí se masky**
    - **vše se udělá někde "izolovaně" (v rámci jedné soustavy dílčích sítí)**
      - **a informace o tomto rozdělení není šířena "do světa„**
- Subnetting hodně pomohl
  - byl okamžitým řešením, které šlo použít "lokálně"
  - zpomalil úbytek IP adres, ale neřešil jej z principu

NAT – Network Address Translation – překlad síťových adres

- převádí IP-adresy **přímo na routeru**
- překládá lokální (privátní, vícenásobně použitelné) adresy na veřejné (unikátní) adresy
- poskytuje zabezpečení-lokální adresy "nejsou vidět"
- šetří IP adresy – pokud jen část lokálních uzlů potřebuje komunikovat s vnějším světem!

neveřejné (privátní) IP adresy

- Co brání vícenásobnému použití IP adres? – to, že by směr. Alg. nevěděly, kam doručovat IP pakety
- nebude existovat přímá komunikace, aby se adresy mohly opakovat
  - tato situace nastává v sítích bez přímé IP konektivity ("privátních sítích"), které jsou odděleny od "ostatního světa" vhodnou bránou (**firewallem**)
    - která **zajišťuje přestup na úrovni vyšší, než je síťová!!**
- Podmínka fungování:
  - na hranicích privátních sítí je třeba **zastavit šíření směrovacích informací**
    - "ohlašujících" existenci uzlů uvnitř privátních sítí
- Důsledek:
  - v privátních sítích lze **použít v zásadě libovolné IP adresy**
    - uvnitř jedné privátní sítě musí být jednoznačně
    - v různých privátních sítích mohou být použity stejné IP adresy
- Doporučení:
  - nepoužívat úplně libovolné IP adresy, ale takové, které byly k tomuto účelu vyhrazeny (RFC 1597)
  - jsou to adresy:
    - 1síťová adresa třídy A: 10.0.0.0 – 10.255.255.255
    - 16 adres třídy B: 172.16.0.0 – 172.31.255.255
    - 256 adres třídy C: 192.168.0.0 – 192.168.255.255

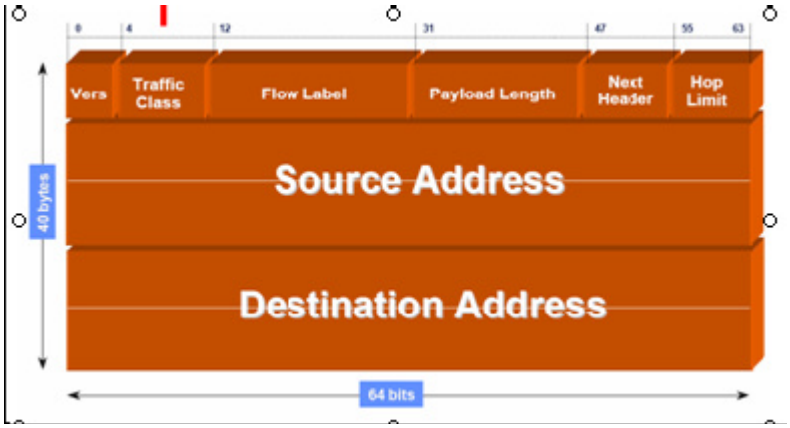
9. IP verze 6

Úvod

S rozvojem Internetu se objevily nové požadavky na přenosové služby.
IP verze 4 neřeší například tyto problémy:
· již zmíněný nedostatek dres
· nedostatečná podpora služeb se zaručenou kvalitou (QoS)
· design neodpovídající vysokorychlostním sítím
· bezpečnostní mechanismy nejsou obsaženy přímo v IP
· nedostatečná podpora mobilních zařízení
· neexistující automatická konfigurace
Nový protokol je označován:
· nejprve jako protokol příští generace IP next generation (IPng)
· později se vžilo označení IPv6 (IP verze 5 exp. proudový protokol)
Nový protokol byl vyvíjen s cílem postupně nahradit protokol IPv4, podmínkou nového protokolu tedy byl co nejsnazší přechod na novou verzi.

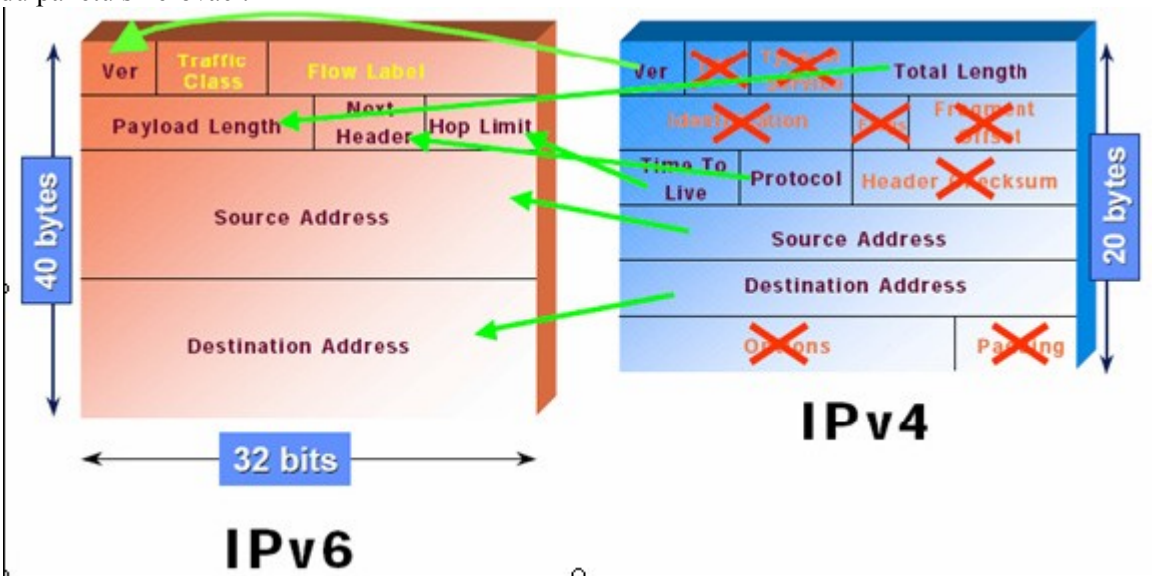
Struktura hlavičky IPv6

Struktura hlavičky IPv6 se skládá ze 40B záhlaví následovaného rozšířeními
· pole Verze (4b) obsahuje 6 (u IPv4 4)
· pole třída dat specifikuje naléhavost dat, jinak řečeno, která data budou zahazována v případě zahlcení sítě



· délka dat (2B = 65535B), bez základní hlavičky, s použitím příznaku „ohromný datagram“ v další hlavičce i více
· typ další hlavičky – TCP, UDP, IPv4, rozšíření hlavičky IPv6
· identifikace toku dat, nová myšlenka, slouží ke dvěma účelům:
– snížení zátěže směrovačů
– datagramy jednoho toku dostanou shodný identifikátor
– směrovače pak řeší úlohu směrování pouze pro první datagram
– další datagramy odesílá stále do stejného rozhraní (max. 6s)
– další možností je zajištění QoS
– směrovače se nakonfigurují tak, aby pro pakety s určitým FL upřednostňovaly jejich směrování
– směrovače pak neobsluhují datagramy jako sekvenční frontu ale vybírají pakety s vhodným FL

Porovnání hlavičky IPv4, IPv6
V hlavičce IPv6 zůstaly pouze nejdůležitější informace, zejména takové, které se uplatňují při průchodu paketu směrovači.



Pole „Next Header“
· ukazuje jaký typ hlavičky následuje (TCP, UDP, IPv4 nebo další IPv6)
· v další hlavičce je za polem Next Header pole specifikující posunutí k další hlavičce
· základní hlavička toto pole nemá, má vždy 40B
· v dodatečných hlavičkách IPv6 se vyskytují méně často používané údaje
Dodatečné hlavičky IPv6
· Volby pro všechny – informace zajímavé pro každého po cestě (např. upozornění směrovače, že paket nese data, která by jej mohla zajímat)
· Směrování – datagram musí projít předepsanou cestou
· Fragmentace – při fragmentaci paketu nese informace nutné pro jeho složení do původní podoby
· Šifrování obsahu (ESP) – obsah datagramu je zašifrován, ESP hlavička nese odkaz na parametry pro dešifrování
· Autentizace (AH) – data pro ověření totožnosti odesilatele a původnosti obsahu
· Volby pro cíl - informace určené příjemci datagramu (např. domácí adresa mobilního uzlu)
· Mobilita – hlavička pro potřeby komunikace s mobilními zařízeními
Šifrovací a autentizační hlavička
IPv6 nativně podporuje autentizaci a šifrování.
Autentizace je zajišťována vypočítáním CRC za pomocí MD-5 a šifrovacího 128bit. klíče → ten musí mít odesilatel i příjemce.
Formát adresy
Pro adresy zdroje a cíle je v IPv6 vyhrazeno 2 x 128b (2 x 16B) = 3.4 x 1038*
Rozeznáváme tři typy adres
Unicast jednoznačná adresa síťového rozhraní
Anycast adresa skupiny síťových rozhraní - dresována je skupina uzlů, ale paket je doručen pouze jednomu (nejbližšímu z hlediska topologie), typicky: hledám nejbližší přístupový bod
Multicast – oběžník, adresována je skupina uzlů, paket je doručen všem
Datagramy typu všeobecného oběžníku (Broadcat) v IPv6 neexistují.

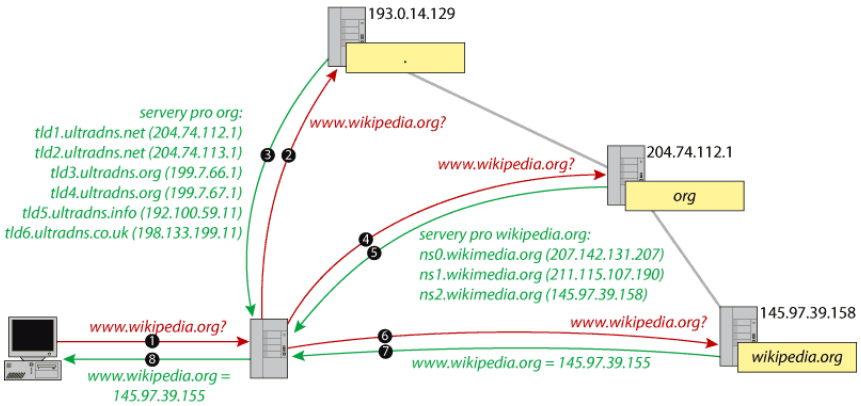
10. Princip doménového adresování, protokol DNS.

DNS je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
Zóna: oblast sítě spravovaná jedním name serverem
Name servery – úkol: převod HOSTNAME (doménového jména) na IP adresu
Doména – jednoznačné jméno počítače nebo počítačové sítě, které jsou připojené do internetu. Př. doménového jména je www.example.com
DNS protokol – pracuje způsobem dotaz – odpověď. Klient pošle dotaz serveru a server na dotaz odpoví.
DNS protokol je protokol aplikační vrstvy, neřeší tedy otázku vlastního přenosu paketů.
využívá DNS jako transportní protokoly UDP i TCP.
DNS servery (name servery)
DNS server může hrát vůči doméně jednu ze tří rolí:

- **Primární server** je ten, na němž data vznikají. Pokud je třeba provést v doméně změnu, musí se editovat data na jejím primárním serveru. Každá doména má právě jeden primární server.
- **Sekundární server** je automatickou kopií primárního. Průběžně si aktualizuje data a slouží jednak jako záloha pro případ výpadku primárního serveru, jednak pro rozkládání zátěže u frekventovaných domén. Každá doména musí mít alespoň jeden sekundární server.
- **Pomocný (caching only) server** slouží jako vyrovnávací paměť pro snížení zátěže celého systému. Uchovává si odpovědi a poskytuje je při opakování dotazů, dokud nevyprší jejich životnost.

Příklad: Podívejme se, jak by postupovalo hledání IP adresy ke jménu *www.wikipedia.org*:
Postup hledání www.wikipedia.org

1. Uživatel zadal do svého WWW klienta doménové jméno *www.wikipedia.org*. Resolver v počítači se obrátil na lokální DNS server s dotazem na IP adresu pro *www.wikipedia.org*.
2. Lokální DNS server tuto informaci nezná. Má však k dispozici adresy kořenových serverů. Na jeden z nich se obrátí (řekněme na 193.0.14.129) a dotaz mu přepošle.
3. Kořenový server také nezná odpověď. Ví však, že existuje doména nejvyšší úrovně *org*, a jaké jsou její autoritativní servery, jejichž adresy tazateli poskytne.
4. Lokální server jeden z nich vybere (řekněme, že zvolí *tld1.ultradns.net* s IP adresou 204.74.112.1) a pošle mu dotaz na IP adresu ke jménu *www.wikipedia.org*.
5. Oslovený server informaci opět nezná, ale poskytne IP adresy autoritativních serverů pro doménu *wikipedia.org*. Jsou to *ns0.wikimedia.org* (207.142.131.207), *ns1.wikimedia.org* (211.115.107.190) a *ns2.wikimedia.org* (145.97.39.158).
6. Lokální server opět jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu *www.wikipedia.org*.
7. Jelikož toto jméno se již nachází v doméně *wikipedia.org*, dostane od jejího serveru nepochybně autoritativní odpověď, že hledaná IP adresa zní 145.97.39.155
8. Lokální DNS server tuto odpověď předá uživatelskému počítači.



11. WiFi, AP, rizika odposlechu, šifrování WEP a jeho slabiny, WPA, WPA2.

WiFi (Standard 802.11) standard pro doplňky pro lokální bezdrátové sítě.
Dobré si uvědomit: přenosová rychlost není nijak garantována, v prostoru nejsme sami, přenos je **poloduplexní**

Přehled standardů IEEE 802.11

Standard	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	2,4	2	DSSS
IEEE 802.11a	5	55	OFDM
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM
IEEE 802.11n zatim neni standardizován	2,4 nebo 5	540	OFDM, MIMO

Techniky přenosu

- **FHSS – Frequency Hopping Spread Spektrum –** frekvenčně rozprostřené spektrum
  - základní metoda, pouze pro nižší přenosové rychlosti do 1–2 Mb/s
  - frekvenční modulace, 78 kanalu po 1Mhz
  - vyšší režie na přeskoky → nižší rychlost
- **DSSS – Direct Sequence Spread Spektrum** – kódově rozprostřené spektrum
  - nejpoužívanější v 802.11
  - frekvenční pásmo 2,412GHz – 2,484 GHz je rozděleno na 14 kanálů po 22Mhz
  - vysílač komunikuje s přijímačem na jedné zvolené frekvenci
  - **signál** je rozprostřen do větší šíře spektra – je **méně citlivý** vůči úzkopásmovému rušení
- **Protokol 802.11a již nepoužívá DSSS ale OFDM –** rozprostřeným spektrem
  - pásmo 2,412 až 2,484 rozděleno na 4 nepřekrývající se pásma
  - v každém pásmu 52 podkanálů (nosných odstupňovaných o 300 kHz)
  - přenášená data jsou zabezpečena kódováním s možností rozsáhlé rekonstrukce chyb
  - modulaci 64QAM (54Mbit/s)

AP = přístupový bod – Základní prvek protokolu rodiny 802.11
Klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu

- **BSA** (Basic Service Area) – oblast, kterou pokrývá přístupový bod.
- **BSS** (Basic Service Set)-Dva a více uzlů, které navzájem navázaly komunikaci.
- **SSID** (Service Set Identifier) – jedinečný identifikátor každé bezdrátové (WiFi) počítačové sítě.
- **2 hlavní varianty SSID:**

  AD-HOC – je bezdrátové připojení, které se skládá z klientských zařízení bez přístupového bodu (AP).
  - nevýhodou je obecně nižší dosah
  - výhodou je vyšší propustnost
  - vyšší globální spolehlivost

  Infrastrukturní sítě obsahuje přístupové body (AP)
  - nevýhodou je nižší propustnost
  - v topologii se dále používají: Klienti, opakovače

Mechanismy zabezpečení dat
Autentizace
Pro připojení stanice se používají dvě metody:

1. **metoda otevřeného systému (Open-system)**
   - klient je autentizován na základě informací jím zaslaných, které nejsou nikde ověřovány
   - AP tedy vždy autentizuje klienta
2. **metoda sdíleného klíče (Shared Key)**
   - je vyžadována pro všechna zařízení s podporou **WEP**
   - klient usilující o připojení musí správně zašifrovat (**RC4**) zaslaný klíč (náhodně vygenerované číslo)
   - velkou nevýhodou je **zasílání textu v nezašifrované a následně zašifrované podobě**
   - je tak možné díky slabinám šifry RC4 získat odposlechem šifrovací klíč

Další metody řízení přístupu

1. **SSID** – nejnižší stupeň zabezpečení

- SSID je logický identifikaci konkrétní sítě (nastaven na AP)
- AP své SSID pravidelně prezentuje

2. Filtrování MAC adres

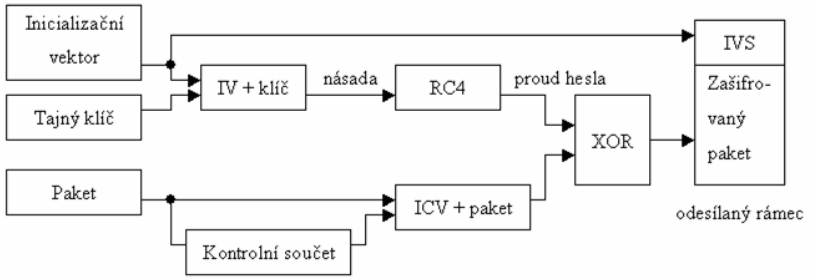
- asociovány budou pouze stanice z platného seznamu MAC adres
- útočník si může snadno změnit svou MAC adresu
- předpokládá se ale, že útočník neví, za jakou
- **nevýhody:**
  - seznam MAC adres je nutné vytvářet ručně (administrátor)
  - filtrování MAC adres neumožňuje dynamickou změnu klientů
- **mnohem větší nevýhodou je ale:**
  - přítomnost MAC adres klientů ve vysílaných paketech a to i v případě použití šifrování v nezašifrované podobě

WEP-ochrana ekvivalentní kabelovému vedení

- volitelný doplněk k 802.11b
- pro řízení přístupu k síti a zabezpečení přenášených dat pomocí **sdíleného klíče** – je nutné ho nastavit **na klientských stanicích**
- data jsou šifrována a dešifrována pomocí šifrovacího klíče:
  - 40bit. WEP klíč (10 x hex znak) + 24 bit. inicializační vektor (IV)
  - nebo 104bit. WEP (26 x hex znak) klíč + 24 bit. inicializační vektor (IV)
- IV – **inicializační vektor** – mění se v každém paketu, *bohužel pouze z* 2^{24} ***možností***

Dalším problémem WEPu je **existence statických klíčů**

- není nijak řešena redistribuce nových klíčů a posílání IV v nezašifrované podobě



WEP - zjevné nevýhody WEPu:

- v takovém případě je vhodné dodržet několik pravidel:

1. používejte tabulku validních MAC adres
2. zapněte WEP na 128bit.
3. pravidelně WEP klíče měňte
4. používejte statické přidělování IP adres
5. nastavte uzký rozsah IP, nebo povolené IP
6. zakažte prezentaci SSID
7. znemožněte fyzický přístup k AP
8. pravidelně kontrolujte síť i logy z AP
9. omezte výkon na nejnižší akceptovatelný
10. používejte VPN

WPA

- je zpětně slučitelné s WEP a předně slučitelné s 802.11i/WPA2
- pokud se v síti sejdou produkty s podporou WPA a WEP, použije se slabší WEP
- pro autentizaci a management klíčů se používá 802.1x
- pro utajení dat protokol **TKIP**
    - používající dynamicky se měnící klíč pro každý paket
    - prodlouženou délku vektoru IV (na 48 bitů)
    - pro kontrolu integrity zpráv – mechanizmus **MIC** (*Message-Integrity Check*).

Přednosti WPA jsou:

- **dynamické klíče**
- autentizace se serverem **RADIUS**
- v domácích sítích lze použít předem nastavené sdílené klíč.

WPA2

- komerční název standardu 802.11i (2004)
- architektura označovaná jako **RSN** (Robust Security Network)
- podarchitektura 802.1X určená pro bezdrátové sítě
- vlastnosti:
    - používá nový standard **AES**
    - velikost šifrovacího klíče **128b, 192b, 256b**
    - **šifrovací** klíče se **mění automaticky**

Postup autentizace:

- stanice se autentizuje otevřenou metodou a domluví se na bezp. zásadách
- následuje fáze komunikace s ověřovacím serverem, je vygenerován společný hlavní klíč