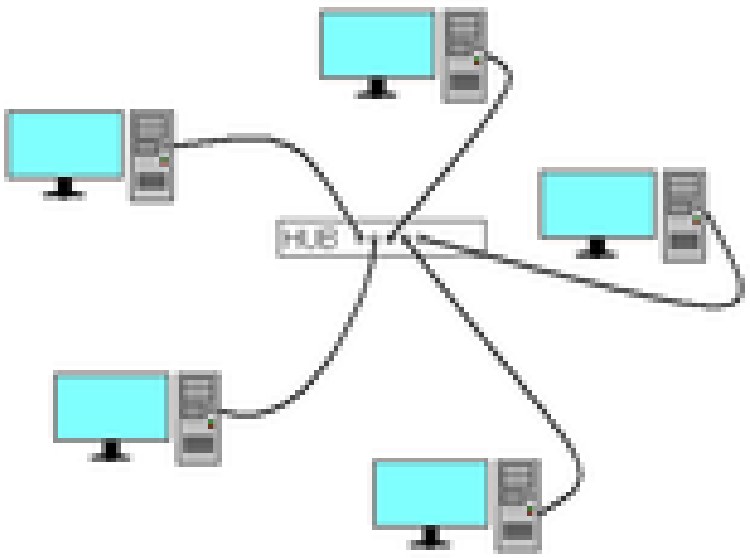
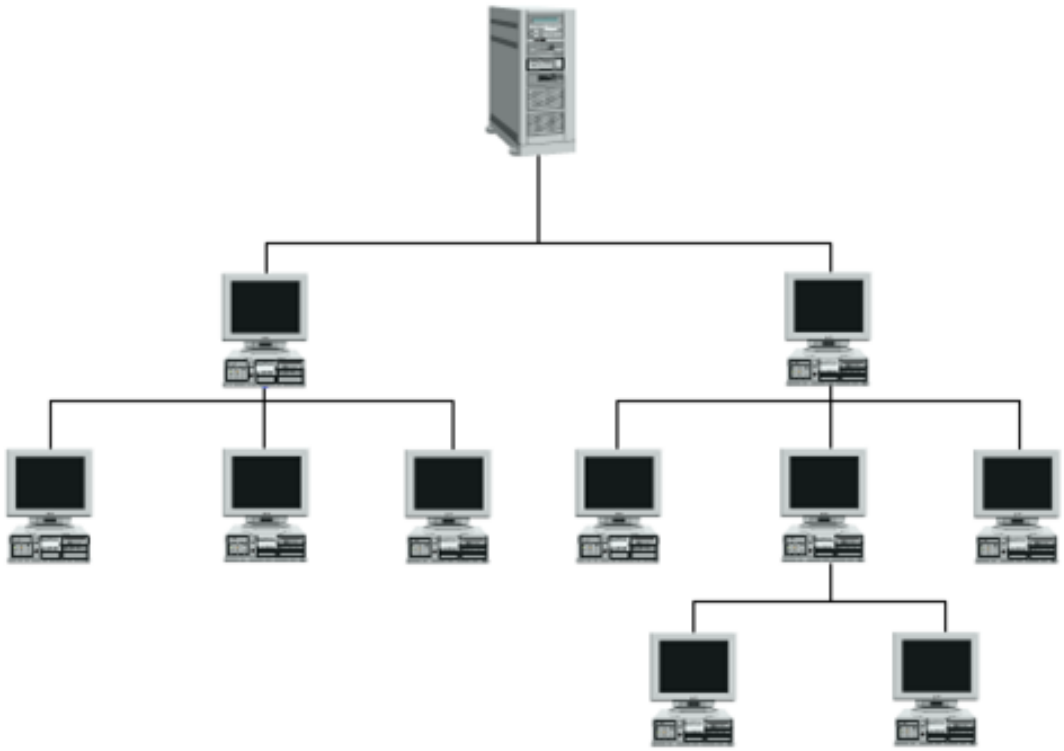
Základní pojmy sítě

Topologie

- Hvězdicová
    - Propojení PC ve tvaru hvězdy
    - Toto je nejčastější zapojení PC v PC sítích
    - Každý PC je připojen kabelem (UTP, STP) k centrálnímu prvku – hubu nebo switchi
    - Když vypadne hub nebo switch tak vypadne celá síť
    - Výhody
        - Pokud selže PC či kabel, tak vypadne jen daná stanice
        - 1 kabel pro 1 přenos dat
        - Snadno se zavádí a rozšiřuje
        - Snadno se nachází a řeší závady
    - Nevýhody
        - Potřeba mnoho kabelů – 1 pro každý počítač
        - Potřeba centrálního prvku – př.: switch
        - Když selže centrální prvek, vypadne celá síť



- Stromová
    - Připojení PC do útvaru ve tvaru stromu
    - Vychází z hvězdicové topologie – prvky ve větvích stromu mají na sebe napojené další prvky, tyto prvky jsou centry jednotlivých hvězd
    - Využívá se ve velkých firmách
    - Výhody
        - Když selže prvek v nižší části sítě, zbytek sítě může stále fungovat
        - Potřeba méně kabelů než na mesh – propojení všeho se vším
        - Zvýšení bezpečnosti – hůře se odposlouchávají data
    - Nevýhody
        - Selháním prvku ze sítě vypadnou i prvky pod ním



- Kruhová
    - Propojení ve tvaru kruhu
    - Data tečou kruhem v jednom směru
    - Stanice si posílají ve směru toku dat paket token – kdo ho má, může vysílat, po určitém čase vysílání ho pošle dál (bez vysílání pošle paket dál okamžitě)

    - Výhody
        - Celkem levné zapojení
        - Netřeba řešit kolizi dat, protože data tečou v jednom směru
        - Netřeba ukončovat terminátory (zařízení, co brání odrazu signálu zpět)
    - Nevýhody
        - Data musí projít celou cestu v kruhu – zdržuje se přenos
        - Při selhání jednoho uzlu selže celá síť
        - Není snadné najít závadu
        - Pro zapojení nového zařízení se musí odstavit celá síť
- Sběrnicová
    - Pomocí jednoho souvislého kabelu
    - Stanice zapojeny za sebou do kabelu
    - Ukončeno terminátory
    - Výhody
        - Jednoduchá levná realizace
        - Vhodná pro malé a dočasné sítě
    - Nevýhody
        - Při problému s kabelem výpadek celé sítě
        - Jen jedna informace naráz
        - Malá přenosová rychlost, s každým dalším zařízením klesá výkon
        - Vyslanou informaci dostávají všechny počítače

Taxonomie sítí = dělení sítí

- Existuje mnoho dělení sítí, mezi nejzákladnější patří:
    - Dělení dle dosahu
        - PAN – ta nejmenší, třeba připojení myši k PC
        - BAN – ve zdravotnictví, týká se těla
        - LAN – místní síť, male zpoždění
        - MAN – oblast města, propojení LANek
        - WAN – Propojení států, kontinentů
        - CAN – oblast kampusu

    - Dělení dle přenosového média
        - Metalické
        - Optické
        - Bezdrátové
        - Satelitní
    - Dělení dle vlastnictví
        - Veřejná – pro přenos dat přes internet, slouží ke komunikaci s ostatními
        - Privátní – slouží ke komunikaci doma, v kanceláři, v podniku
        - VPN – soukromé zabezpečené propojení vzdálených počítačů přes veřejnou síť, počítače spolu komunikují jako kdyby byly propojeny do privátní sítě

Vývoj internetu

- ARPANET
    - V roce 1969
    - Vznik v USA, síť měla umožnit robustní vzdálenou komunikaci
    - Myšlenka pro vznik přišla kvůli studené válce
    - Měla ověřit myšlenku komunikace na základě přepojování paketů
    - Také měla na dálku propojit superpočítače, první uzly byly tedy na univerzitách
    - Po úspěchu se začala šířit dále
- Komercializace internetu
    - Internet zpočátku nebyl navrhnut pro komerční účely, byl navrhnut pro univerzity a výzkum, komerčním účelům bylo bráněno
    - Proto vznikaly vedle internetu různé jiné sítě, které byly spíše pro omezené množství služeb, př.: email, tyto sítě byly regionální
    - V roce 1991 zlom – umožněno propojování sítí v rámci světa, začátek podoby internetu tak, jak je dnes
    - V ČR internet poprvé 1992 (Československo)
    - V ČR první sítí byl CESNET
    - V roce 1995 začala liberalizace českého internetu a začaly vznikat různí soukromí ISP
- IANA

- Za úkol má celosvětové přidělování IP adres a zprávu adres a domén nejvyššího řádu (TLD)
- Komunikuje se správci domén nejvyššího řádu
- Také definuje MIME a dohlíží na internetové protokoly
- Přiděluje IP adresy jen velkým regionům (Severní Amerika, Evropa, …)
- Přiděluje bloky s prefixem 8

ISO/OSI, TCP/IP

<table>
<tr><th>TCP/IP</th><th>Model ISO/OSI</th></tr>
<tr><td rowspan="3">Aplikační vrstva</td><td>Aplikační vrstva</td></tr>
<tr><td>Prezentační vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová (IP) vrstva</td><td>Síťová vrstva</td></tr>
<tr><td rowspan="2">Vrstva síťového rozhraní</td><td>Linková vrstva</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

- Bylo nutné standardizovat pravidla pro komunikaci v počítačových sítích
- Modely byly zavedeny, aby spolu mohly komunikovat počítače s různými OS a přes jiné síťové technologie
- TCP/IP má 4 vrstvy:
  - Vrstva síťového rozhraní – slouží k řízení fyzického přenosového média – linky
  - Síťová vrstva – zajišťuje především síťovou adresaci, směrování a předávání datagramů
  - Transportní vrstva – stará se o celistvost dat, řídí spojení, kontroluje, zda data dorazila, protokoly TPC a UDP, je implementována pouze v koncových zařízení

    - Aplikační vrstva – protokoly a aplikace, přenášejí určitá data pomocí protokolů transportní vrstvy a ostatních vrstev, třeba DHCP
- ISO/OSI má 7 vrstev
    - Fyzická vrstva – přenos bitů
    - Linková vrstva – přenos rámců, CRC, sdružování bitů do rámců
    - Síťová vrstva – přenos dat v síti, přenáší pakety
    - Transportní vrstva – v koncových zař., řídí spojení, kontroluje, zda data dorazila
    - Relační vrstva – koordinuje a udržuje komunikaci, stará se o přihlašování a správu
    - Prezentační vrstva – formát dat, kompresi, dekompresi, šifrování
    - Aplikační vrstva – protokoly, přenášejí určitá data pomocí protokolů ostatních vrstev, třeba DHCP
- ISO/OSI je zbytečně moc složitý, v praxi se používá spíše TCP/IP

standardy používané v počítačových sítích

- RFC
    - Dokumenty napsané experty, je to spíše doporučení pro řešení nějakých problémů, popisuje internetové protokoly
    - RFC 2046 – definuje text/plain MIME
- IEEE
    - Organizace, formuluje různé standardy pro komunikaci v počítačových sítích a podobu počítačových sítí
    - Třeba IEEE 802.11 – Wi-Fi

Fyzická vrstva

binary transmision – bezpečný přenos jednotky informace

Je první vrstva modelu vrstvové síťové architektury (ISO).

Zajišťuje převod proudu bitů na signál (nejčastěji elektrický) a opačný převod ze signálu na proud bitů.

Může provádět aktivaci, udržování a rušení fyzického spoje

Realizace

Z průběhu signálu je potřeba zajistit správné parametry pro „rozhodovací okna“

Amplitudové okno – oblast nad a pod prahovými úrovněmi signálu, mimo oblast „nejistoty“ – úroveň signálu

Časové okno- oblast validity signálu

1. Přenosová média - amplitudové okno – elektrické a fyzické parametry přenosových médií.
2. Kódování – validita signálu – zajištění vložení synchronizace, není k dispozici speciální hodinový signál.

Pojmy

Reálné vlastnosti přenosového média vždy negativně ovlivňují přenos. Hlavně se jedná o následující:

- **Útlum** (atenuation) - zeslabení signálu, jednotka dB
- **Přeslech** (crosstalk)– deformace působením okolních signálu (např. ze sousedních párů vedení) – jednotka dB
- **Zkreslení** – deformace signálu (přeslechem nebo rušení*) – jednotka %
- **Šum** – deformace signálu (vliv parametrů součástek zařízení)- jednotka dB

Obecné vlastnosti média

Přenosová rychlost - vyjadřuje objem dat, přenesených za jednotku času [b/s]

Modulační rychlost - modulační rychlost udává, s jakou frekvencí se mění signál

Koaxiální kabel

Koaxiální kabel (zkráceně koax) je souosý elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým nebo trubkovým vodičem vnitřním

Použití:

- napáječ vysílacích nebo přijímacích antén
- svod od televizní antény, televizní rozvody
- kabelová televize
- svod od parabolické antény pro družicový přijímač
- počítačové sítě
- telefonie

Kroucená dvoulinka

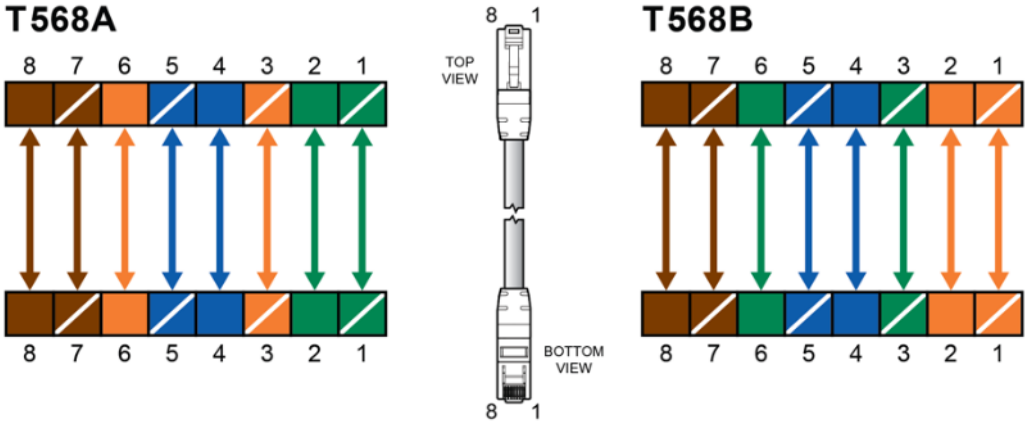
Kroucená dvojlinka je tvořena páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny a následně jsou do sebe zakrouceny i samy výsledné páry

Kategorie kroucených dvojlinek:

- Kategorie (Level) 1 - přenos hlasu
- Kategorie (Level) 2 - data do 4 Mb/s
- Kategorie (Level) 3 - data do 10 Mb/s, Ethernet
- Kategorie (Level) 4 - data do 20 Mb/s, Token Ring
- Kategorie (Level) 5 - data do 100 (155) Mb/s, Fast Ethernet, ATM 155
- Kategorie (Level) 5e - data do 1 Gb/s (test. 100 MHz), Ethernet
- Kategorie (Level) 6 - data do 10 Gb/s (test. 200 MHz), Ethernet
- Kategorie (Level) 7 - data do 10 Gb/s, Ethernet

Konektory

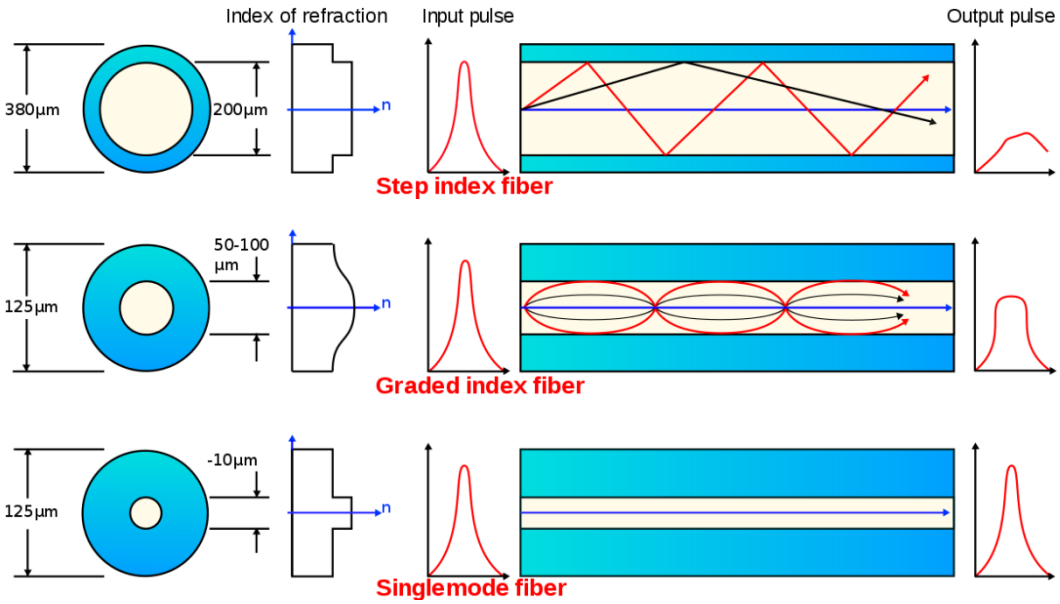
- 2 standarty – RJ45a a RJ45b
- V sítích se častěji používá B



Optická vlákna

Typy:

- Mnohavidové optické vlákno
- Jednovidové optické vlákno
- Vlákna pro speciální účely



Parametry:

Multimode (MMF)

- průměr vlákna (jádra) – 62,5 µm, 50 µm
- útlum - 1.5 dB/km - 3.5 dB/km
- dosah – cca 1 km

Singlemode (SMF)

- průměr vlákna (jádra) – 9 µm
- útlum - 0.4 dB/km - 1 dB/km
- dosah – 50km +

Konektory:

SC, ST, FC, SMA 905 a 906, LC, E2000/LX.5, MTRJ

Kódování, modulace

Baseband

jde o takový druh přenosu, při kterém je vstupní signál okamžitě převáděn na přenosové médium – bez činnosti modulačního prvku

Boardband

Data k přenosu se naloží na nosný signál

Naloží se na něj pomocí modulace – ta mění pomocí signálu s daty parametry nosného signálu

Kódování

NRZI

Používá ho Ethernet na optických vláknech

Jednička = změna úrovně signálu, nula = žádná změna

Modulace

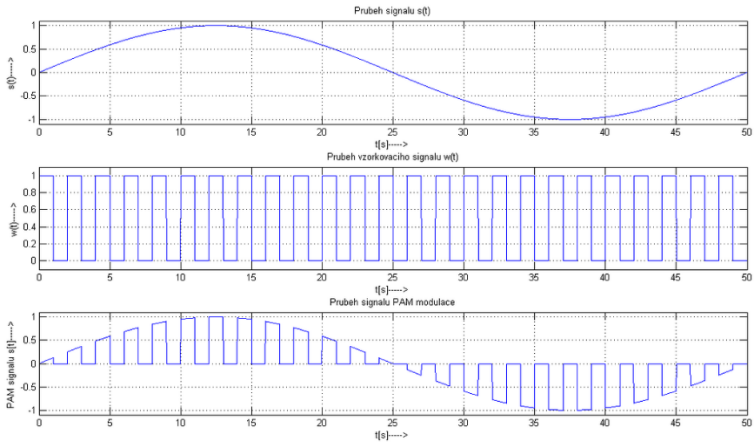
Modulace vznikla pro posílení signálu na delší vzdálenosti přenosu

Druhy:

- amplitudová modulace - amplitude modulation (AM)
- frekvenční modulace - frequency modulation (FM)
- fázová modulace - phase modulation (PM)

Pulzně amplitudová modulace

je diskrétní modulace v základním pásmu



Media konvertor

Media konvertor je převodník mezi různými druhy sítí

Používají se, když potřebujeme změnit optický signál na elektrický

optické a metalické ethernetové linky

PoE

PoE (Power over Ethernet) je napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem

K napájení se využívají 3 a 5 + 7 a 8 kabely

Způsoby PoE:

- Napájení po volných nevyužitých párech v datovém kabelu (režim B). Napájecí páry jsou 4-5 a 7-8.
- Napájení „fantómovým“ napětím mezi dvojicí aktivních párů vodičů, po kterých se současně přenášejí i data (režim A). Napájecí (a datové) páry jsou zde 1-2 a 3-6.

Vlastnosti PoE:

- napětí 44 – 57 V;
- maximální proud 550 mA;
- maximální zapínací proud 500 mA;
- Typický proud 10 – 350 mA;
- detekce přetížení 350 – 500 mA;
- odběr v klidovém stavu maximálně 5 mA.

Aktivní / pasivní

Pasivní PoE na straně u zdroje jednoduše přivede napájení na nevyužité vodiče v síťovém kabelu

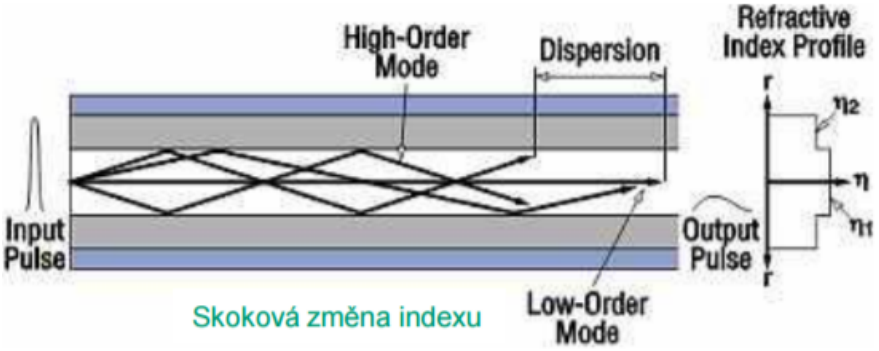
Aktivní PoE je narozdíl od pasivního PoE jej pomocí tzv. fantomového napětí injektují na datové linky, lze tedy využít gigabitovou rychlost

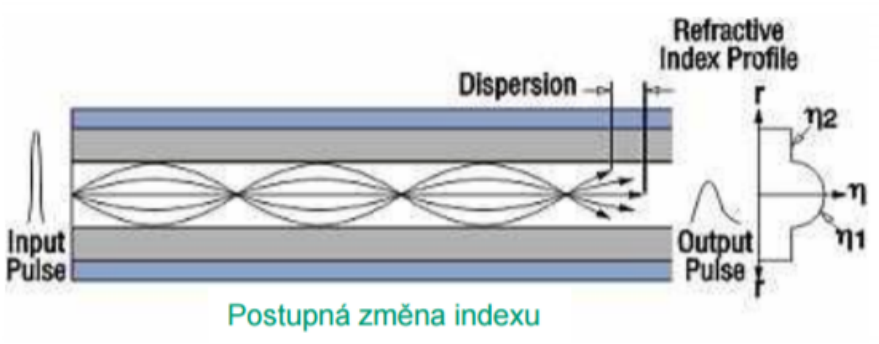
Optická vlákna

Optické vlákno je tenké vlákno ze skla nebo ve speciálních případech z průhledného plastu, které je schopné přenášet po své délce světelné záření, a to i na značné vzdálenosti. V dnešní době nachází optická vlákna využití zejména v telekomunikacích (tvoří naprostou většinu dálkových telekomunikačních sítí a brzy se rozšíří i do místních sítí) a v medicíně, ale jejich využití se rychle rozšiřuje i do jiných oblastí lidské činnosti.
Umožnují vyšší přenosové rychlosti - 10, 40, 100 Gbit

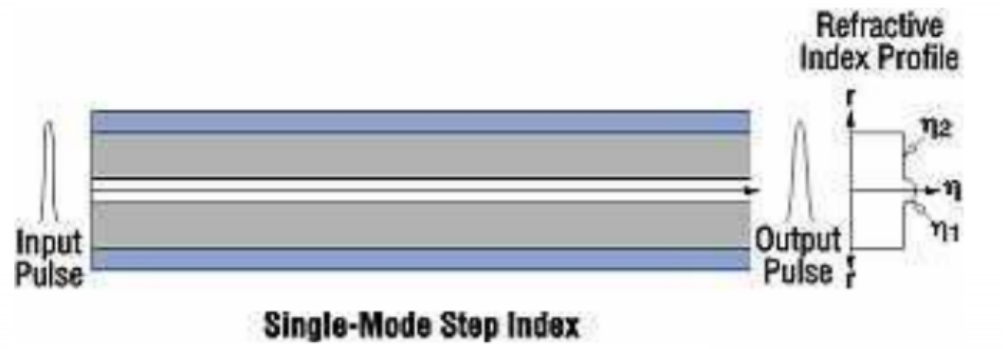
Typy vláken

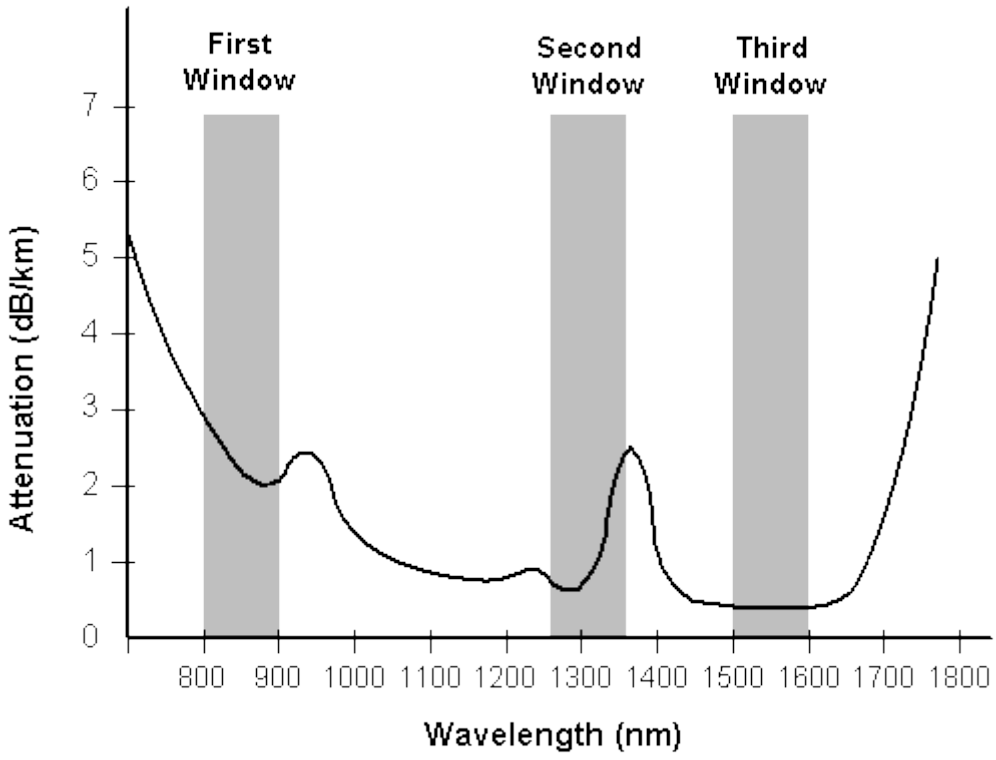
Mnohovidové optické vlákno (Multimode)





Jednovidové optické vlákno (Singlemod)


Refractive
Index Profile
r
η2
η
η1
Input
Pulse
Output
Pulse
Single-Mode Step Index

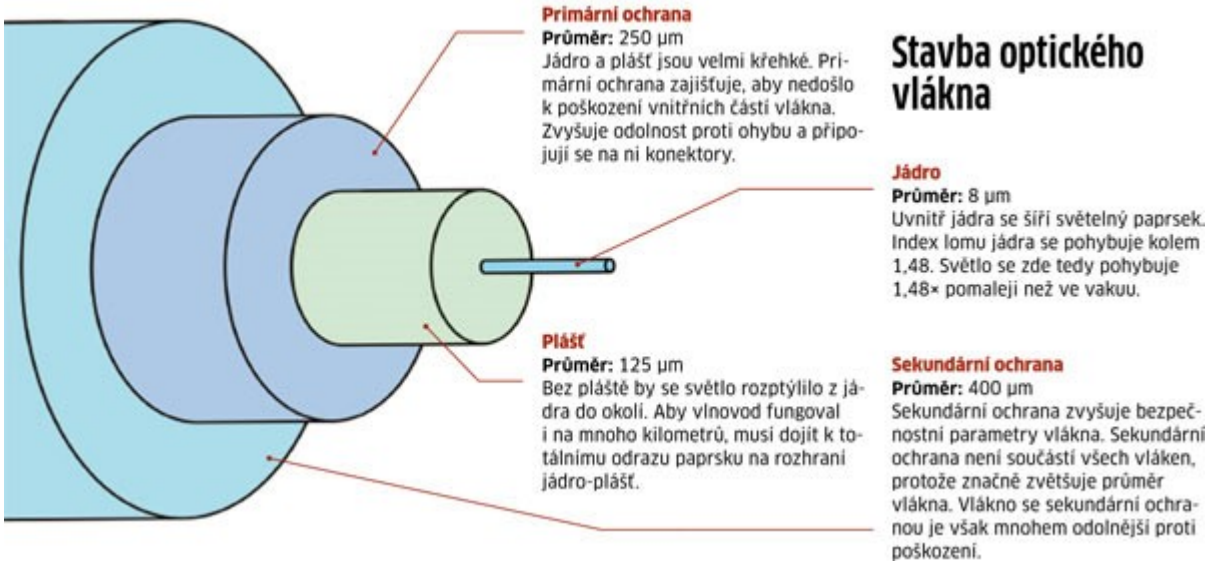

First
Window
Second
Window
Third
Window
Attenuation (dB/km)
0
1
2
3
4
5
6
7
800
900
1000
1100
1200
1300
1400
1500
1600
1700
1800
Wavelength (nm)

MM – 850nm,1310nm

SM – 1310nm,1550nm

Stavba optického vlákna

- Optická vlákna jsou obalena Primární ochranou zajišťující pružnost vlákna, bez ní je velmi křehké.
- Sekundární ochrana značně zvyšuje tloušťku vlákna, ale zajišťuje dobrou ochranu. Její odstranění je běžné u propojovacích kabelů



Spojování optických vláken

- Permanentní spojení
  - Tavné svařování
  - Mechanické spojování - čelní spoje s přímým stykem spojovaných ploch
- Semipermanentní spojení
  - Mechanické (spojky, rychlokonektory)

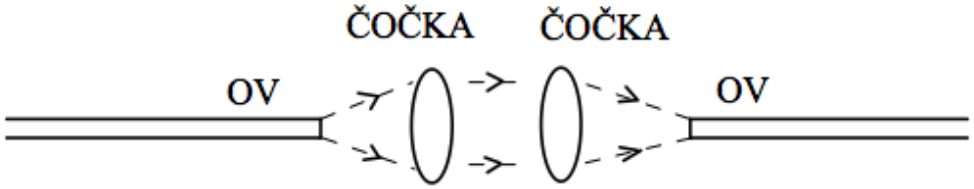
Tavné svařování

Nejnižší útlum, dlouhá životnost, obtížné, zejména kvůli malé velikosti jádra, úspěšnost se posuzuje podle optického útlumu a mechanické pevnosti (útlum okolo 0,2dB).

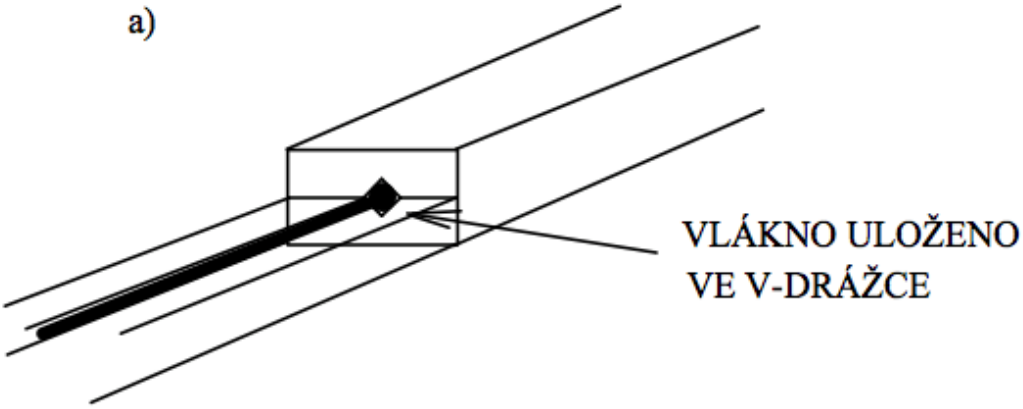
Rozebíratelné spoje – konektory

Rozebíratelné spoje (konektory) požadují, aby se mechanické spoje nedotýkaly kvůli opotřebení ploch. Zároveň je nutné, aby mezi nimi byla minimální vzdálenost (maximálně

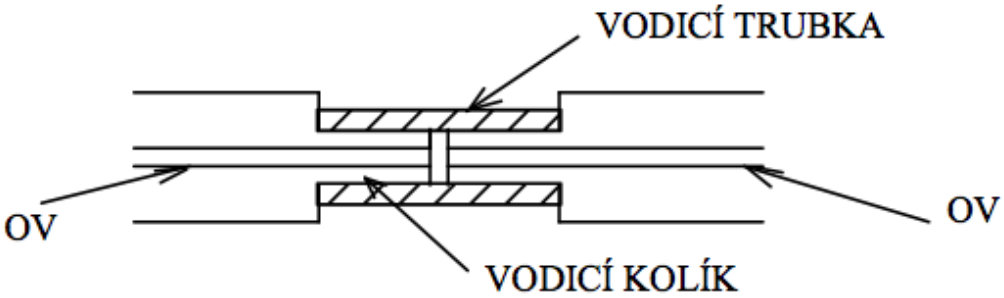
10% průměru jádra). Používají se pro spojování vláken u kterých se předpokládá opakované rozpojování a spojování.
Vzácně se využívá spojování pomocí čoček. Tyto čočky jsou neúměrně drahé a složité na výrobu, zároveň ale dosahují minimálních útlumů – až 0,2 dB, podobné jako u svarů. (obrázek A).
Druhá skupina využívá mechanické vedení vlákna – pomocí v-drážky (obrázek B) nebo pomocí vodícího kolíku a trubky (obrázek C). Typický útlum jsou menší než 1 dB
Konektory SC, LC a ST



a)



b)



c)

Transreceiver

- síťový prvek, který umožňuje překlad toku informací z jednoho typu sítě na typ jiný
- TRANSmitter a reCEIVER - vysílač a přijímač.
- využívají se nejčastěji při převodu metalické sítě na optickou, z bezdrátové na metalickou apod.
- dnes už funkce transceiveru nebývá řešena jako samostatný hardwarový prvek, ale integruje se dnes do inteligentnějších zařízení (směrovač, access point).
- TRANSMITTER + RECEIVER = Media converter

Druhy :

GBIC

- (Gigabit Interface Converter) - Hlavní rozdíl oproti předcházejícím dvěma byl ten,

že GBIC modul se zasunuje dovnitř zařízení (GBIC slot).

SFP

- označované také jako Mini-GBIC, jsou k dispozici ve dvouvláknovém, jednovláknovém (WDM, Bidi, Single Fiber), CWDM a DWDM verzi.
- Narozdíl od GBIC modulu má SFP přibližně poloviční velikost - menší rozměry umožňují osazení aktivních prvků v hustotě až 24 portů SFP.

SFP+

- Oproti SFP má rychlejší datovou sběrnici i lepší stínění proti elektromagnetickým rušením a je tak určen hlavně pro vysokorychlostní aplikace.
- Je optimalizovaný pro 10Gbps Ethernet a 2x/4x/8x Fiber Channel
- Dostupné jsou varianty pro přenos po jednom vlákně (WDM) či CWDM pro vlnový multiplex.

Jednotlivé vlnové délky tvoří logické kanály – WDM (2 CH), CWDM (16 CH), DWDM (40 CH)

WDM (Wavelength Division Multiplexing)

- vlnový multiplex představuje technologii, kterou se při přenosu multiplexuje více optických signálů v jednom optickém vlákně s použitím rozdílných vlnových délek (barev) LED nebo laserů
    - je tak umožněno rozšířit kapacitu média nebo provést obousměrnou komunikaci na jednom optickém vlákně.
    - nejčastěji se používá při přenosu informace optickým způsobem (signál bývá popsán svojí vlnovou délkou)
    - používá multiplexer ve vysílači pro spojení signálů dohromady a demultiplexer v přijímači pro následné rozděleni
    - pouze 2 kanály

CWDM (Cable Wavelength-division multiplexing)

- Rozdíl oproti DWDM je ve větším odstupu jednotlivých kanálů, což snižuje celkovou kapacitu vlákna
    - Kvůli většímu odstupu je CWDM vhodnější na krátké vzdálenosti (cca 50 km po jednovidovém vlákně).
    - ITU standardizovala 20 nm kanálové rozteče pro použití s CWDM za použití vlnových délek mezi 1270 nm a 1610 nm
    - 16 kanálů
    - nevyžaduje perfektní zdroj
    - lokální sítě

DWDM (Dense Wavelength Division Multiplexing)

- Hustý vlnový multiplex je efektivní metoda, kde je několik kanálů,
- každý o jiné vlnové délce, přenášeno jedním optickým vláknem, využívající více z dostupné šířky pásma, bez zvyšování efektu disperze.
- Každý kanál může být nezávislý na protokolu, rychlosti a směru komunikace.

    - Technologie DWDM je použitá nejvíce na dálkových optických trasách.
    - 40 kanálů
    - páteřní sítě a dlouhé trasy

24. Linková vrstva

také „spojová vrstva“, „vrstva datového spoje“
je druhá nejnižší vrstva v referenčním modelu ISO/OSI.

Zajišťuje komunikaci mezi dvěma nebo více uzly propojenými tímtéž datovým spojem, který může být dvoubodový (např. sériová linka) nebo mnohabodový (lokální sítě, např. Ethernet); specifickým uspořádáním je point-to-multipoint, při kterém jedna řídicí stanice komunikuje s větším počtem stanic podřízených.

typická struktura ethernet rámce

Struktura ethernetového paketu a rámce podle IEEE 802.3

Layer	Preambule	Oddělovač začátku rámce	MAC cíle	MAC zdroje	802.1Q tag (volitelný)	Délka/Typ	Datové pole	Kontrolní posloupnost rámce (32bitový CRC)	Mezera mezi pakety
	7 oktetů	1 oktet	6 oktetů	6 oktetů	(4 oktety)	2 oktety	46(42)[3]–1500 oktetů	4 oktety	12 oktetů
Ethernetový rámec (linková vrstva)			← 64–1518(1522) oktetů →						
Ethernetový paket (fyzická vrstva)	← 72–1526(1530) oktetů →								

- typy rámce
    - Rámce Ethernet II nebo Ethernet Version 2, neboli DIX rámce je nejobvyklejší dnes používaný typ rámců v sítích Ethernet, protože se často používá pro Internet Protocol.
    - Nestandardní rámce Novell raw IEEE 802.3
    - Rámce IEEE 802.2 Logical Link Control (LLC)
    - Rámce IEEE 802.2 Subnetwork Access Protocol (SNAP)
- popis hlavičky
    - Hlavička obsahuje cílovou a zdrojovou MAC adresu (každá o délce šest oktetů), pole Délka/Typ a volitelně IEEE 802.1Q tag.
    - Pole Délka/Typ je dlouhé dva oktety a může být použito dvěma způsoby. Hodnoty 1500 a menší znamenají, že se jedná o délku datového pole v oktetech, zatímco hodnoty 1536 a větší znamenají, že se jedná o EtherType, který indikuje, jaký protokol je zapouzdřený v datovém poli rámce. Pokud je pole používáno jako EtherType, délka rámce se zjistí podle mezery mezi pakety a podle správné hodnoty kontrolní posloupnosti rámce (FCS).
    - Nepovinný IEEE 802.1Q tag je čtyřbytové pole, které indikuje příslušnost k Vlan a prioritu podle IEEE 802.1Q
    -
- min. a max. velikost rámce

- Rozlišování typů ethernetových rámců

Typ rámce	Délka/Typ	První 2 byty datového pole
Ethernet II	≥ 1536	Libovolné
Novell IEEE 802.3	≤ 1500	0xFFFF
IEEE 802.2 SNAP	≤ 1500	0xAAAA
IEEE 802.2 LLC	≤ 1500	Jiné

chybovost, efektivita přenosu adresování

- spolehlivou nebo nespolehlivou komunikaci
- spojovanou nebo nespojovanou

• MAC adresa ◦ složení

- **MAC zajišťuje**
- fyzické adresování,
- řízení přístupu k médiu

◦ speciální adresy

typy vysílání

- unicast ◦ popis
  - Unicast označuje v počítačové síti zasílání paketů pouze jedinému cíli (uzlu, stanici).
- broadcast ◦ popis
  - Broadcast je v informatice zpráva, kterou v počítačové síti přijmou všechna připojená síťová rozhraní.

  V ethernet síti MAC adresa FF.FF.FF.FF.FF.FF
- multicast
  - IP multicast je metoda přeposílání IP datagramů z jednoho zdroje skupině více koncových stanic.

  V ethernet síti MAC adresa 01.xx.xx.xx.xx.xx

kolizní a bezkolizní přístupové metody

- TDMA
  - Time Division Multiple Access (TDMA), je deterministická metoda přístupu k médiu pro sdílené sítě. Umožňuje více uživatelům sdílet stejný frekvenční kanál dělením signálu do různých časových slotů.

- CSMA/CA ◦ princip
    - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) – vyhýbá se kolizím, ale nedetekuje je. Patří v počítačových sítích do třídy protokolů označovaných jako metody s vícenásobným přístupem a naslouchánim nosné (CSMA). Čeká dokud nezmizí nosná, pak chvilku počká (náhodně dlouho) a pak začne vysílat ale nedetekuje kolize.

- CSMA/CD - ethernet
    - Carrier Sense Multiple Access with Collision Detection CSMA/CD) je protokol pro přístup k přenosovému médiu v počítačových sítích. Patří do třídy CSMA, tedy metod s vícenásobným kolizním přístupem a naslouchánim nosné.

  Detekuje kolize. Používá se v ethernet sítích. Pokud dojde ke kolizi, počká náhodně dlouhou dobu a začne znovu vysílat.

Ethernet

základní typy:

Ethernet I – již se nepoužívá

IEEE 802.3x – používá se

Ethernet II – používá se, velmi podobný IEEE 802.3x

přenosová média:

TP kabel, optika (100Base-Tx, 1000Base-Fx)

25. Aktivní prvky fyzické a linkové vrstvy

Popis a jejich funkce

MOST

- **Popis** – vytváří „most“ mezi dvěma segmenty sítě (má pouze dva porty, víceportový bridge je switch). Přenosovým médiem je většinou tenký koaxiální kabel (topologie BUS) nebo nověji se používá bridge pro přepínání mezi různými typy přenosových médií.
- **Na které vrstvě pracuje** – L2 – Linková vrstva

SWITCH

- **Popis** – Jedná se víceportový bridge. Obsahuje část hardwarového řešení portů, část řízení a jádrem je přepínací matice (propojovací pole). Přepínač je optimalizován na výkon, tj. rychlost přepínání. Cílem je co nejvyšší datová propustnost sítě. Je to v současnosti základní aktivní prvek LAN.
- **Na které vrstvě pracuje** – L2 – Linková vrstva
- **Příklad parametrů** – Rychlost přepínání, Propustnost, přenosová kapacita

OPAKOVAČ

- **Popis** – Aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále
- **Na které vrstvě pracuje** – Fyzická vrstva

HUB/ROZBOČOVAČ

- **Popis** – Hub, je aktivní prvek počítačové sítě, který umožňuje její větvení a je základem sítí s hvězdicovou topologií. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů, zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena.
- **Na které vrstvě pracuje** – Fyzická vrstva

Řízení přístupu k médiu

- **Kolizní doména** – je část počítačové sítě, která je sdílena více síťovými zařízeními. Kolizní doménu tvoří stanice, které jsou umístěny ve stejném síťovém segmentu, tj. komunikují navzájem na fyzické vrstvě
- **Broadcast doména** – je v informatice část počítačové sítě, ve které může na linkové vrstvě ISO/OSI modelu každý síťový uzel komunikovat s každým

pomocí broadcastu. Broadcastovou doménu tvoří jeden segment sítě (propojení pomocí hubů a switchů) nebo ve více segmentech pomocí mostu (bridge). Broadcastovou doménu rozděluje router nebo gateway.

- **Mikrosegmentace** – na porty switche je připojeno pouze jedno KZ. V segmentech sítě nejsou víceportové opakovače, ani sběrnice. Každý počítač tvoří samostatnou kolizní doménu.
- **Plně duplexní provoz** – zařízení komunikují naráz oběma směry

Management přepínačů

- **Nastavitelné parametry** –
- **Rozhraní pro správu** – sériové (RS232) a ethernetové

VLAN

- **Důvod použití**
    1. Cíl učinit logickou organizaci sítě nezávislou na fyzické vrstvě
    2. Usnadnění správy sítě
    3. Zvýšení výkonu a bezpečnosti
- **Identifikace** – IEEE 802.1q
- **Začlenění do Ethernetového rámce** – IEEE 802.1q

ACCESS PORT

- **Použití** – Veškerý trafic z tohoto portu je součástí defaultní vlan 1.
- **Vlastnosti** – Patří do jediné sítě VLAN, přenášejí provoz pouze této sítě

TRUNK PORT

- **Použití** – Zajišťuje přenášení čísel a názvů VLAN mezi přepínači zařazených do jedné domény, což usnadňuje jejich správu.
    - Konfiguraci provedeme pouze na jednom přepínači (server)
- **Vlastnosti** – Dvoubodové spojení mezi přepínači, přepínačem a směrovačem nebo přepínačem a serverem, které přenáší provoz do více různých sítí VLAN

Paměti CAM/TCAM

• **Princip** – Chová se jako asociativní pole (hodnoty uloženy pod klíčem, podle kterého se vyhledává). Porovnává vstupní data (index, značka) s tabulkou uložených dat a vrací adresu uložených dat

• **Použití** – Ukládání MAC adres a portů v dražších switchích

• **Vlastnosti** –

ACL

• **Princip** – Seznam oprávnění připojený k nějakému objektu (např. souboru)

• **Použití** – Určení, kdo nebo co má povolení přistupovat k objektu a jaké operace s ním může provádět

27. IP adresa a způsoby řešení nedostatku IP adres

složení, syntaxe zápisu (IPv4, IPv6), rozdělení do tříd

• způsob zápisu –

IPv4 = čtyři desítková čísla -> např. 192.168.48.36, IPv6 = osm skupin po čtyřech hexadecimálních číslicích, např. 2001: 0718: 1c01: 0016: 0214: 22ff: fec9: 0ca5

• třídy IPv4 adres –

A (10.0.0.0 až 10.255.255.255),

B (172.16.0.0 až 172.31.255.255),
C (192.168.0.0 až 192.168.255.255),

100.64.0.0/10 - IPv4 Prefix for Shared Address Space podle specifikace RFC 6598

• max. hodnoty jednotlivých čísel u IPv4 + důvod

• zkracování zápisu IPv6 adres –

Klasický tvar: 2001: 0718: 1c01: 0016: 0214: 22ff: fec9: 0ca5

Úvodní nuly v každé skupině lze ze zápisu vynechat. Výše uvedenou adresu tedy lze psát ve tvaru: 2001: 718: 1c01: 16: 0214: 22ff: fec9: ca5

rozdíly mezi IPv4 a IPv6

• délka adresy –

IPv4 = čtyři desítková čísla

IPv6 = osm skupin po čtyřech hexadecimálních číslicích

• velikosti adresního prostoru u IPv4 a IPv6

IPv4 = 2^{32}

IPv6 = 2^{128}

• min. přidělovaná velikost IPv6 sítě

Minimální délka prefixu je 64

• broadcast a multicast na IPv4 a IPv6

IPv4 broadcast – broadcast adresa se získává z masky sítě. Změnou všech nul v masce sítě na jedničku dostaneme broadcast adresu.

IPv6 broadcast – Ipv6 nepoužívá metodu broadcast. Místo toho využívá Multicast.

IPv4 multicast – pro multicast je rezervováno místo s tímto rozsahem: 232.0.0.0-232.255.255.255

IPv6 multicast – používá se pro optimalizaci dodatkových služeb, přenosu zařízení, bezpečnost a konfiguraci

• veřejné, privátní a link-local adresy

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

IPv4 – používá 24bitové, 20bitové a 16bitové bloky pro jejich udělení

IPv6 – používá náhodné 40bitové číslo v prefixu -> předchází tím kolizím.

Veřejné adresy využívají ostatní bloky pro jejich adresaci.

• **ARP a NDP**

Protokol ARP je používán protokolem IPv4 k vyhledání fyzické adresy (například adresy MAC nebo adresy linky) přidružené k adrese IPv4.

IPv6 vkládá tyto funkce do samotného protokolu IP jako součást algoritmu automatické bezstavové konfigurace a zjišťování sousedních uzlů pomocí protokolu ICMPv6 (Internet Control Message Protocol, verze 6). Něco jako ARP6 proto neexistuje.

způsoby získání adresy (DHCP, RA)

• **DHCP**

IPv4 - Tento protokol se používá k dynamickému získávání adres IP a jiných informací o konfiguraci. IBM i podporuje server DHCP pro IPv4.

IPv6 - Implementace IBM i protokolu DHCP nepodporuje IPv6. Je však možné použít implementaci serveru ISC DHCP.

◦ **základní předávané parametry**

Používá sadu protokolů TCP/IP

◦ **identifikace koncového zařízení**

K ověřování dochází pomocí vlastní části síťové a cílové IP adresy.

◦ **komunikace s DHCP serverem (vrstva, cílové adresy)**

Aplikační vrstva, prezentační vrstva, relační vrstva, transportní vrstva, síťová vrstva, linková vrstva, fyzická vrstva,

◦ **obnova IP adresy**

- Klient dostane tzv. DHCPACK kdy může používat ip adresu a její zbylá nastavení. Pokud jí v době zapůjčení neobnoví musí ji přestat používat.

◦ **příklad DHCP serveru**

◦ **dynamická a statická alokace**

Statická:

DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.

Dynamická:

Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu.

• **SLAAC (RA)**

Host v IPv6 může být konfigurován automaticky, pokud je připojen na směrovanou IPv6 síť, za použití zpráv směrem k ICMP v6 směrovači. Při prvním připojení k síti host vyšle 'router solicitation' multicast žádost o konfigurační parametry na místní linku. Odpovídajícím způsobem nastavený ICMPv6 směrovač odpoví na tuto žádost paketem 'router advertisement', který obsahuje konfigurační parametry síťové vrstvy.[10] Pokud není IPv6 autokonfigurace použitelná, host může využít stavové konfigurace (DHCPv6) nebo být nastaven ručně či jiným způsobem.

SLAAC počítá s 64bitovým prefixem sítě, pro jinou velikost síťového prefixu není chování implementací IPv6 definováno.

◦ **předávané parametry**

DNS – systém doménových jmen

DHCP – dynamické přidělování síťových informací jako například: výchozí brána, maska sítě, IP adresa

FTP – přenos souborů po síti

TFTP - jednoduchý protokol pro přenos souborů

HTTP – přenos hypertextových dokumentů (WWW)

WebDAV – rozšíření HTTP o práci se soubory

IMAP (Internet Message Access Protocol) umožňuje manipulovat s jednotlivými e-mail zprávami na poštovním serveru.

IRC (Internet Relay Chat) – jednoduchý chat po internetu.

NNTP (Network News Transfer Protocol) umožňuje číst a umísťovat do sítě zprávy typu news.

NFS (Network File System) – síťový systém souborů, který umožňuje transparentní sdílení vzdálených souborů jakoby byly lokální.

NTLM Autentizační protokol Windows

NTP – synchronizace času (šíření přesného času)

POP3 (Post Office Protocol) – protokol pro získání pošty z poštovního serveru.

SMB (Server Message Block) - sdílení souborů a tiskáren v sítích Windows

SMTP – zasílání elektronické pošty

SNMP Simple Network Management Protokol je určen pro správu síťových uzlů.

Telnet – protokol virtuálního terminálu.

SSH – bezpečný shell

X11 – zobrazování oken grafických programů v Unixových systémech

XMPP – rozšiřitelný protokol pro zasílání zpráv a sledování přítomnosti (protokol Jabber)

◦ **předávání adres DNS serverů**

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, který se na ni ptal. 666

◦ **komunikace routeru s koncovými zařízeními a opačně (vrstva, cílové adresy)**

Routování probíhá pomocí referenčního modelu ISO/OSI

Cílové adresy se zde překládají pomocí techniky NAT

• **DHCPv6**

DHCPv6 je síťový protokol, který umožňuje počítačům získat IPv6 adresu, případně jiné parametry sítě jako adresy DNS serverů. Princip je podobný DHCP, existuje ale několik zásadních rozdílů, např. DHCPv6:

- umí spravovat více IP adres pro jedno rozhraní
- je jednodušší, protože klient využívá automatické konfigurace lokální linkové IPv6 adresy
- klient posílá zprávy na skupinové adresy, nikoliv všesměrovým vysíláním
- klient je identifikován prostřednictvím jedinečného identifikátoru DUID (DHCP unique identifier)

- zprávy pro počáteční přidělení adresy se jmenují: Solicit, Advertise, Request, Reply
- nedokáže poskytnout informaci o výchozí bráně (default route, default gateway) – tu klient obdrží pomocí oznámení směrovače (Router Advertisment).

◦ **předávané parametry**

◦ **identifikace koncového zařízení**

K ověřování dochází pomocí vlastní části síťové a cílové IP adresy.

◦ **spolupráce s RA**

• statická konfigurace IP adres

neboli pevná IP adresa. Pevnou IP adresu můžeme od poskytovatele připojení získat většinou za příplatek, ale dostáváme tím garanci, že IP adresa koncového zařízení, které se připojuje do internetu zůstane stále stejná.

základní údaje nutné pro směrování, maska a její použití

• určení adresy sítě a broadcastu (IPv4)

broadcast adresa se získává z masky sítě. Změnou všech nul v masce sítě na jedničku dostaneme broadcast adresu.

• vliv masky, resp. délky prefixu na velikost sítě

• rozpoznání rozdílných sítí

řešení nedostatku IPv4 adres (CIDR, subnetting, privátní adresy, NAT, proxy)

• CIDR

Classless Inter-Domain Routing (CIDR, tj. „beztřídní směrování“) je v počítačových sítích metoda směrování, která v roce 1993 umožnila v IPv4 používat jemnější dělení větších sítí na podsítě tím, že maska sítě byla určena počtem bitů a nikoliv příslušností IP adresy ke třídě IP adres. CIDR byl zaveden IETF a jeho cílem bylo zpomalit vyčerpání IPv4 adres a též omezit růst směrovacích tabulek na směrovačích v Internetu.

◦ **důvod zavedení**

Před zavedením CIDR byly adresy rozděleny do tříd a koncovým sítím připojeným k Internetu se v závislosti na jejich velikosti přidělovala adresa sítě třídy A, B nebo C. To způsobovalo dva problémy, jejichž závažnost postupně narůstala:

- Špatnou efektivitu využití adresního prostoru a v jejím důsledku rychle ubývající zásobu volných adres. Jako první začaly docházet adresy třídy B, protože sítí příliš velkých pro třídu C (256 místních adres) bylo mnoho a adres třídy B jen 16 tisíc (16384).
- Velké směrovací tabulky. Adresy sítí se přidělovaly tak, jak byly postupně vyžadovány, bez respektování jejich geografické či jiné souvstažnosti. To znamenalo, že v páteřních částech Internetu musely směrovače uchovávat ve svých směrovacích tabulkách pro každou koncovou síť

samostatný záznam. Tím směrovací tabulky nabývaly značné velikosti, takže jejich procházení bylo pomalé a mohlo nastat až vyčerpání dostupné kapacity operační paměti směrovačů.

◦ **způsob použití**

Zavedením CIDR bylo možné určit masku na hranici jednotlivých bitů IP adresy, místo po výše zmíněných osmicích bitů (resp. po jednotlivých bajtech).

• dělení sítě na podsítě (subnetting)

Podsíť (anglicky subnet, subnetwork) je v informatice označení pro samostatnou část počítačové sítě. Označením podsíť je obvykle míněna konkrétní (menší) vyčleněná část větší IP sítě. Pro určení rozsahu IP adres v dané podsíti slouží maska sítě.

◦ **způsob rozdělení**

Počítače, které jsou umístěny v jedné síti (resp. podsíti), mají ve svých IP adresách shodné nejvýznamnější bity této IP adresy. Tím je IP adresa rozdělena na dvě části, které označujeme jako „číslo sítě“ a „číslo počítače“. Místo označení „číslo počítače“ by mělo být uvedeno „číslo síťového rozhraní“, protože některé počítače mohou mít více síťových karet a tím i více síťových rozhraní s více IP adresami.

Velikost významnější části IP adresy (tj. velikost části, která vyjadřuje „číslo sítě“) je definována pomocí CIDR notace počtem bitů zleva (tzv. prefix) nebo pomocí masky sítě.

◦ **VLSM**

VLSM umožňuje síťovým inženýrům rozdělit prostor adres IP do hierarchie podsítí různých velikostí, což umožňuje vytvářet podsítě s velmi odlišnými počty hostitelů, aniž by došlo ke ztrátě velkého počtu adres.

• privátní adresy

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

IPv4 – používá 24bitové, 20bitové a 16bitové bloky pro jejich udělení

◦ **důvod použití a vlastnosti**

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

◦ **příklady privátních rozsahů**

- ve třídě A: 10.0.0.0 až 10.255.255.255 (celkem 1× 16 777 216 adres; tj. 16 777 216 adres, z nichž je použitelných jen 16 777 214)
- ve třídě B: 172.16.0.0 až 172.31.255.255 (celkem 16× 65 536 adres; tj. 1 048 576 adres, z nichž je použitelných jen 1 048 544)

- ve třídě C: 192.168.0.0 až 192.168.255.255 (celkem 256× 256 adres; tj. 65 536 adres, z nichž je použitelných jen 65 024)

• NAT

◦ **účel použití, princip, vrstva**

NAT se většinou používá pro přístup více počítačů z lokální sítě do Internetu prostřednictvím jediné veřejné IP adresy (viz gateway).

◦ **omezení komunikace do vnitřní sítě**

NAT však znemožňuje přímou komunikaci mezi klienty (end–to–end spojení) a může snížit rychlost přenosu.

◦ **přesměrování portů**

Pro obcházení problémů, které NAT způsobuje, jsou k dispozici různé techniky umožňující (přímou) komunikaci mezi zařízeními za NAT – viz NAT traversal[16] nebo Hole punching.
Protokol UPnP (anglicky Universal Plug and Play) umožňuje automatickou konfiguraci přesměrování portů na routeru, avšak vyžaduje vysokou úroveň důvěry mezi ovládající stanicí a routerem, což například v případě Carrier-grade NAT není možné.

• proxy

◦ **účel použití, princip, vrstva**

Proxy server funguje jako prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Přijatou odpověď následně odesílá zpět na klienta. Může se jednat jak o specializovaný hardware, tak o software provozovaný na běžném počítači. Proxy server odděluje lokální počítačovou síť (intranet) od Internetu.

Linková vrstva

◦ **porovnání s NAT**

NAT-device změní adresu počítače, který vysílá paket do Internetu, aby vaše (nebo registrovány v nastavení), aniž by se změnila strukturu dotazu a poté, co obdrží balíček z online serveru, který ji doručí na místo určení i nezměněné

proxy- Server obdrží žádost od počítače, který vysílá paket do Internetu, předá jej on-line serveru prostřednictvím zavedené IP adresy, a poté, co obdrží balíček, dodává, že na místo určení bez úprav nebo opraveny filtrem (je-li to nutné - zkontrolujte antivirový modul) Technologie nevyžaduje předpis dalších síťových nastavení na jednotlivých počítačích v síti LAN

◦ **reverzní proxy**

Reverzní proxy je proxy server, který se zobrazí klientům jako obyčejný server. Žádosti jsou přesměrovány na jeden nebo více serverů, které je zpracují. Odpovědi jsou navráceny, jakoby přišly přímo z webového serveru.

IP datagram (hlavička, TTL...) , fragmentace

• popis základních částí IPv4 a IPv6 hlavičky, velikost hlavičky

IPv4 - Datagram IPv4 obsahuje hlavičku se služebními údaji nutnými pro přepravu a za ní následují data. Konec hlavičky je zarovnán na násobek čtveřice bajtů pomocí výplně (anglicky padding). Strukturu IP datagramu vystihuje tabulka uvedená nahoře.

délka hlavičky jako počet 32bitových slov (pro získání délky v bajtech je potřeba vynásobit čtyřmi, tzn. typická a minimální délka (0x5 × 4) = 20 bajtů, a maximální (0xF ×* 4) = 60 bajtů.

IPv6 –

Byty	0		1	2	3
0–3	Verze	Třída provozu		Značka toku	
4–7	Délka dat			Další hlavička	Max. skoků
8–11	Zdrojová adresa				
12–15					
16–19					
20–23					
24–27	Cílová adresa				
28–31					
32–35					
36–39					

◦ **verze**

Verze protokolu, zde 6.

◦ **adresy**

Adresa odesílatele, cílová adresa

◦ **TTL, hop limit**

Životnost datagramu. Stejně jako u TTL v IPv4 zde každý směrovač zmenší hodnotu o jedničku a dojde-li do nuly, datagram zahodí.

◦ **délka**

Délka datagramu, ovšem nepočítá se do ní úvodní 20B hlavička.

◦ **protokol, next header**

Rozšiřující prvky jsou v IPv6 přesunuty do rozšiřujících hlaviček, které se v případě potřeby připojují za základní hlavičku. Jsou zřetězeny položkami Další hlavička, které vždy identifikují typ následující hlavičky. Poslední hlavička pak v této položce nese informaci o protokolu vyšší vrstvy, kterému mají být data předána při doručení. Pokud tedy datagram žádné rozšiřující hlavičky nemá, hned základní hlavička v této položce stanoví protokol vyšší vrstvy.

• fragmentace

◦ **důvod**

IP datagram je rozdělen na menší části, aby mohly být přeneseny další části počítačové sítě

◦ **parametr fragment offset**

pozice fragmentu v originálním paketu (počet osmic bytů dat od počátku původního datagramu k počátku tohoto fragmentu)

29. Bezdrátové sítě

bezdrátové spoje a jejch vlastnosti

Wi Fi

původně bez významu nyní (wireless fidelity)

principu rozprostřeného spektra, první pokusy už v roce 1942 (armáda)
co je to rozpr. Spektrum?

v roce 1997 standard 802.11 -> hromada modulací nekompatibilita, v r. 2002 vznik WiFi aliance, pokud má zařízení označeníWiFi tak umí komunikovat s dalšími WiFi zař.

Bezdrátová Wi Fi sí může pracovat na několika standardech IEEE, které postupně vznikaly od roku 1997, kdy přišel základní 802.11 s datovou propustností maximálně 2 Mb/s (reálně› 120 kB/s).
O dva roky později byly schváleny standardy 802.11a (5 GHz, maximálně› 54 Mb/s, reálně 3,1 MB/s) a 802.11b (2,4 GHz, maximálně› 11 Mb/s, reálně› 700 kB/s). Až standard 802.11g přinesl v roce 2003 rychlost 54 Mb/s i do 2,4GHz pásma, a Wi Fi síť se tak stala jak cenově dostupnou, tak i použitelnou pro plnohodnotné surfování.

Skutečně vysoké rychlosti přenosu ale přinesl standard 802.11n v roce 2009 s maximální fyzickou rychlostí 600 Mb/s
(reálně až 25 MB/s).

Má to však pár háčků:

Zatímco u předchozích standardů se pro komunikaci používala zpravidla jediná anténa jak na vysílači, tak na přijímači (tzv. SISO – Single-Input Single-Output), standard 802.11n používá k razantnímu navýšení rychlosti vícecestné šíření signálu, tzv. MIMO (Multiple- Input Multiple-Output).

MIMO využívají např. i sítě 4G.

Vícenásobné antény pracují na principu vysílání několika signálu různými, na sobě nezávislými cestami, každá anténa má svůj přijímač/vysílač bezdrátového signálu. Pro správný provoz těchto prvků je nutné použití vyhodnocovacích algoritmů v čipových sadách, které řídí vysílání informace jednotlivými anténami (přijímači) v závislosti na jejich momentálním vytížení. Navíc se signály bezdrátové sítě od překážky v prostoru odrážejí a může dojít k rušení signálu, jeho útlumům, což mají tyto algoritmy také odstranit, nebo aspoň výrazně zmírnit.

P2P spoje na >10 Ghz

Pro profesionální PtP spoje jsou v České republice definována licencovaná pásma, mezi která patří **4, 6, 7, 8, 11, 13, 15, 18, 23, 26, 32, 38 a 42 GHz.** Hlavní výhody licencovaných pásem jsou:

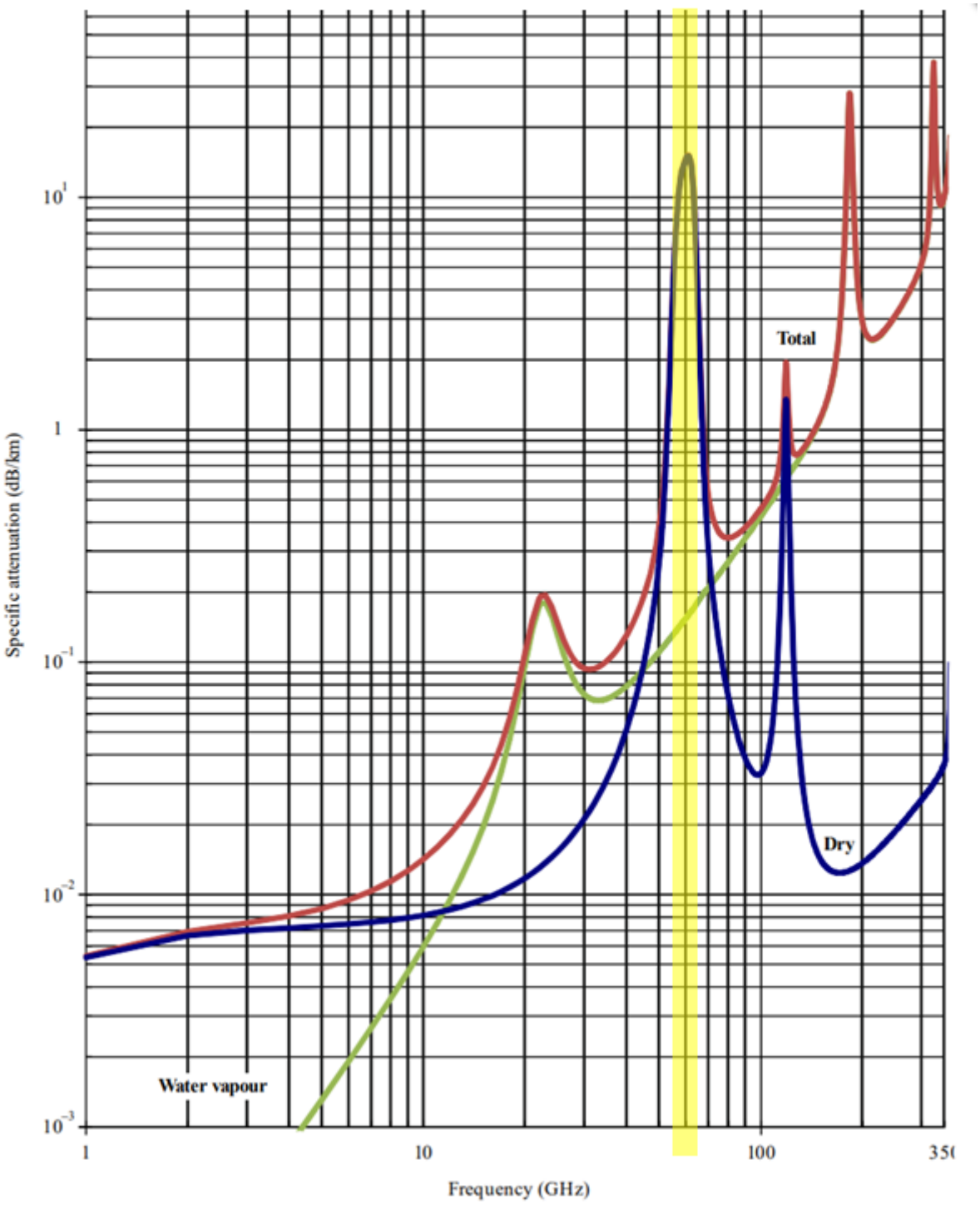
- ochrana proti rušení
- použitelnost i na extrémně dlouhé skoky, případně použití menších parabol na dlouhé skoky
- možnost přenosu vysokých kapacit

Nevýhoda: ja to placené

Bezlicenční bezdrátové spoje v pásmu 60 Ghz

(přesněji 57–66 GHz) přináší řadu výhod. Jeho využití je tedy pro uživatele (ať již operátora, nebo koncového zákazníka) bezplatné. (standard 802.11ad)

Při přímém porovnání s technologií Wi-Fi v pásmu 2,4, resp. 5 GHz vynikne hlavní rozdíl, který předurčuje pásmo 60 GHz pro poskytování vysokorychlostního bezdrátového internetu – zatímco v současných Wi-Fi sítích se šířka používaného kanálu pohybuje v řádu desítek megahertzů (20/40/80 MHz), v pásmu 60 GHz se prozatím jedná o 2,16 GHz, tedy šířku o dva řády vyšší. Tato skutečnost umožňuje dosahovat přenosových kapacit až několika Gb/s bez použití pokročilých technologií. Užv současné době, tedy na začátku masového nasazení, jsou běžně dostupná zařízení v cenové relaci několika tisícikorun, která dokáží přenést 1 Gb/s na vzdálenost stovek metrů.


Specific attenuation (dB/km)
10^{1}
1
10^{-1}
10^{-2}
10^{-3}
Total
Dry
Water vapour
1
10
100
350
Frequency (GHz)

Optická pojítka

Je přenos dat s pomocí laserového spoje (FSO) bezpečný?

Bezdrátové laserové spojení je jedno z nejefektivnějších a nejbezpečnějších systémů komunikace, který umoňuje přenos dat o vysoké rychlosti s požadavkem vysoké bezpečnosti přenosu bez možnosti odposlechu.

Je světlo viditelné?

Spojení na přímou viditelnost (LOS) používá neviditelné paprsky, které zajišťují optické spojení s propustností dat, videa a hlasu o velikosti až 10 312,5 Mbps (u ECSYSTEM zařízení) a to simultánně vzduchem - pro zajištění optického spojení nepotřebuje fyzicky optický kabel.

Je potřebný optický kabel nebo licence?

Bezdrátové optické spojení prostřednictvím laserového - optického pojítka nevyžaduje fyzické položení optického kabelu nebo licenci pro vydělené radiové pásmo. Technologie optického pojítka potřebuje světlo. Toto světlo je podobné tomu, které je používáno při optickém přenosu prostřednictvím optického kabelu, rozdíl je jen v médiu, kterým prochází. U optického kabelu je to sklo, u optického pojítka je to vzduch, kterým světlo prochází rychleji než sklem.

Jak funguje technologie optického spoje?

Je založení na bezdrátovém propojení optických hlavic, z nichž každá obsahuje optický vysílač a přijímač k zajištění full duplex kapacity. Optické vysílače vysílají světlo vzduchem a jiná přijímací čočka přijímá informaci

Jaké jsou výhody EC SYSTEM laserového pojítka?

- Rychlá a snadná instalace, žádné zdržení, žádné kopání
- Není nutná žádná licence
- Čistá kapacita přenosu 10 Gbps Full Duplex, nízká latence, možné navýšení kapacity dokoupením modulu
- Nejbezpečnější přenos dat, nemožnost odposlechu, nabourání
- Pokrokový reálný automatický autotracking a automatická kontrola výkonu
- Konkurenční výhoda nabídnout big data přenos zákazníkům dřív než konkurence

Proč dát přednost bezdrátové optické technologii (FSO- free space optics) před radiovou technologií nebo optickým kabelem?

Optická bezdrátová technologie založená na technologii bezdrátového optického spoje, je technologie pro venkovní použití zajišťující rychlost vyrovnající se rychlosti prostřednictvím optického kabelu až do 40 Gps Full Duplex. To neumožní žádná bezdrátová radiová technologie. Optické bezdrátové spojení také eliminuje potřebu kupovat drahé spektrum, žádat státní orgány povolení pro umístění mikrovlnného zařízení nebo položení optického kabelu. FSO technologie používá paprsky a umoňuje rychlejší a snadnější integraci do stávající sítě. Poskytovateli internetu šetří čas a peníze a dává mu tím konkurenční výhodu.

Jak instalovat laserové pojítko?

Laserové - optické pojítko je používáno pro spojení přímé viditelnosti, tzn., že spojované body musí mít přímou viditelnost bez fyzických překážek, ale narozdíl od spojení založeném na radiu nepotřebuje Fresnelovu zónu.

Jaký vliv má počasí na spolehlivost spojení?

Déš´t a sníh mohou částečně ovlivnit optické bezdrátové spojení, ale nemají takový vliv, jaký mají na mikrovlnné spojení. Mlha může ovlivnit světelné charakteristiky a průchod paprsku v závislosti na kombinaci absorbce,rozptylu, odrazu. Pro tento případ doporučujeme při návrhu sítě a instalaci laserového pojítka počítat s kratším linkem a případně použít zálohu -backup,v závislosti na frekvenci výskytu

mlhy v oblasti, kam je laserové pojítko instalováno.Nicméně EC SYSTEM optická pojítka byla instalována v oblastech s výskytem mlhy a dosáhly vysoké spolehlivosti. EC SYSTEM laserová pojítka mají vstavěný AGC modul (automatc gain control), který v reálném čase reguluje optický vysílací výkon laseru v závislosti na kvalitě linku (spojení), který je nepřetržitě monitorován. Takovým způsobem je zajiš´těna vysoká dostupnost spoje i v případě horších klimatických podmínek

Mohou přerušit letící ptáci spojení?

Letící ptáci mohou dočasně přerušit jeden paprsek optického zařízení, ale toto přerušení je jen velmi krátké a spojení je jednoduše a automaticky znovu navázáno. Některé modely ECSYSTEM mají několik paprsků, které tyto dočasné překážky odstraní.

Jaký vliv má na spolehlivost bezdrátového optického spoje pohyb budov, stožárů nebo zemětřesení?

Pohyb budov nebo stožárů způsobený větrem, zemětřesením nebo tepelnou roztažitelností může dočasně narušit nastavení přijímače a vysílače, ale ECSYSTEM optická pojítka používají z toho důvodu reálný autotracking systém, který tyto výchylky v reálném čase kompenzuje a zajišťuje tak vysokou spolehlivost spojení.

Je technologie laserového pojítka bezpečná pro oči?

EC SYSTEM laserové pojítko používávlnovou délku 1550nm, narozdíl od laserových pojítek jiných výrobců. Tato vlnová délka je bezpečná pro oči i při vyšším výkonu Zařízení, které je používáno striktně s návodem k použití je bezpečné. EC SYSTEM optické pojítko splňuje požadované standarty.

Jaký je provozní rozsah optického pojítka?

Provozní rozsah laserového pojítka závisí na modelu. EC SYSTEM optické pojítko může být použito na vzdálenosti až **7000m**. Na konkrétní vzdálenosti se podívejte do specifikací jednotlivých modelů. Please refer to the product specifications for each product or to our Models overview for more information.

Jaká je přenosová rychlost bezdrátového optického spoje EC SYSTEM?

Přenosová rychlost EC SYSTEM optických pojítke v závislosti od modelu je 10Gbps, 1Gbps , 100 Mbps a může být navýšena přidáním dodatečného IDU například +10 Gbps,+10 bps or +1 Gbps,+1Gbps up to 8 Gbps or up to 30 Gbps.

Jaká příslouženství má EC SYSTEM optické pojítko?

EC SYSTEM laserová pojítka obsahují autotracking a indikátor úrovně signálu. Pojítka jsou dodávána s montážní sadou, nebudete potřebovat dodatečná zařízení. To vše urychluje a usnadňuje montáž.

Jaký vliv mají vibrace na fungování laserového pojítka?

EC SYSTEM laserové pojítko bylo navrženo a je konstruováno tak, že vibrace nemají vliv na jeho fungování a spolehlivost. Autotracking je zabudován v každém ECSYSTEM pojítku.

Je seřizování - nastavení optického pojítka automatické?

EC SYSTEM optická pojítka mají v každém modelu zabudovaný autotracking a indikátor úrovně signálu, to vše usnadňuje a umoňuje automatické nastavení pojítek.

Je potřeba čistit a jak často je potřeba čistit laserové pojítka?

ECSYSTEM optická pojítka obvykle není potřeba periodicky čistit.

Cena optických pojítek : mezi 50 – 100tis. kč

Vlastnosti Wi Fi

Používané frekvence

Rozsah 2,4GHz (standardy 802.11b/g/n) je dán mezi 2,412 a 2,484 GHz, což dává dohromady 13 (14 např. Japonsko) nezávislých kanálů
po 5MHz krocích, výjimkou je čtrnáctý kanál vzdálený o 12 MHz od třináctého.
Podstatný je však fakt, že si každá Wi Fi síť obsad šířku pásma o velikosti 20 MHz okolo používaného kanálu.
Aby se tedy sítě vůbec nerušily (podotýkám, pouze v místě› vysíání), mohou běžet souběžně jen tři (čtyři), a to na kanálech 1, 5, 9 a (13).

Rozsah 5GHz pásma (standardy 802.11a/n) je značně› vě›tší, a to 5,180 (36. kanál) až 5,700 GHz (140. kanál).
V Evropě› je dostupných 19 kanálů, ze kterých je prvních osm (kanály 48â€“64, 5,180 až 5,240 GHz) určeno pouze pro použití
uvnitř budov (maximální vysílací výkon omezen do 200 mW). Zbylých jedenáct (kanály 100 až 140, 5,500 až 5,700 GHz)
už lze použít i mimo budovy (vysílací výkon do 1 W), vysílací zařízení ale musí být vybavena dynamickým výběrem frekvencí a regulací výstupního výkonu.

Max. Rychlost

Standard	Označení	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	-	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	Wi-Fi 1	1999	5	54	OFDM
IEEE 802.11b	Wi-Fi 2	1999	2,4	11	DSSS
IEEE 802.11g	Wi-Fi 3	2003	2,4	54	OFDM
IEEE 802.11n	Wi-Fi 4	2009	2,4/5	600	MIMO OFDM
IEEE 802.11y	-	2008	3,7	54	
IEEE 802.11ac	Wi-Fi 5	2013	5	3466.8	MU-MIMO OFDM
IEEE 802.11ad	-	2012	60	6757	
IEEE 802.11ax	Wi-Fi 6	2019	2,4/5/6	10530	MIMO-OFDM

Režimy provozu

infrastruktura ad hoc – decentralizovaná bezdr. Sít, každý se může spojit s každým
AP – Acess Point
Client
Repeater – pouze opakuje data, zvětšení dosahu
Bridge – pro PtP spoje

Zabezpečení

WEP (Wired Equivalent Privacy)
WPA (WiFi Protected Access)
WPA2
802.1x – ověření user/password, RADIUS server,.... (klient se připojí k uzlu, data nejdou ale funuje pouze EAP (**Extensible Authentication Protocol**)protokol pro autentikaci uživatele)

Řízení přístupu k médiu u Wi Fi

U WiFi (Wireless Fidelity) se používa přístupová metoda **CSMA/CA (Carrier Sense Multiple Access /with Collision Avoidance)**. Kolize lze v bezdrátových sítích težko detekovat a proto se nepoužívá CSMA/CD. I když je pásmo v okolí stanice volné, neznamená to, že je volné i v okolí příjemce, kterým je většinou Access Point (AP - přístupový bod). Na AP totiž mohla vyslat požadavek jiná stanice, která není v dosahu první. Proto vysílací stanice nejdříve pošle paket RTS (Request To Send) ve kterém je kromě zdroje uvedena i doba trvání přenosu. Pokud následně přijme **CTS (Clear To Send)** paket, tak zahájí přenos. Okolní stanice, které jsou v dosahu a slyší pakety RST a CTS tím pádem vědí jak dlouho bude médium obsazené a nepokoušejí se vysílat. Jak již všem logicky došlo tak komunikace probíhá **half-duplexem**.

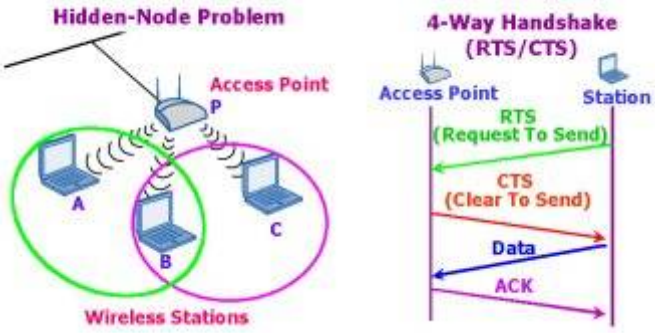
Problém skrytého uzlu

Standard 802.11 není určený pro venkovní sítě. Při jeho návrhu se počítalo s tím, že půjde o náhradu pro vnitřní ethernetové sítě a tedy také s tím, že všechny WiFi prvky na sebe „uvidí". Tomu odpovídá i způsob, jakým se WiFi sítě brání kolizím – velmi nedokonale. 802.11 standard definuje CSMA/CA jakožto systém předcházení kolizím, kde se kvůli problému „skrytého uzlu" používá RTS/CTS potvrzování.

Právě proto, že WiFi je optimalizováno pro nasazení, kde na sebe všichni klienti vidí a kde neexistuje problém skrytého uzlu, je třeba v případě venkovních sítí provést patřičné úpravy, které odstraní potenciální problémy s kvalitou datového přenosu. Je tedy dobré rovnou zdůraznit, že touto optimalizací nezískáte signál tam, kde není, ale můžete i výrazně zvýšit propustnost v síti.
Při používání WiFi ve venkovním prostředí je "skrytý uzel", jak zní terminus technicus, velkým problémem. Skrytý uzel se prakticky vždy objevuje tam, kde se WiFi používá ve venkovním prostředí pro distribuci signálu způsobem Point – Multipoint. Příčinou je fakt, že zatímco přípojný bod vidí všechny stanice, protože používá všesměrovou nebo alespoň sektorovou anténu, klientské stanice (tedy uzly) se navzájem nevidí, protože je s přípojným bodem pojí směrová anténa.

To má za následek, že se klientské stanice snaží vysílat najednou domnívaje se, že „éter je volný" a přípojný bod je jejich vysíláním zahlušen. Ačkoliv standard 802.11 definuje kombinaci CSMA/CA a RTS/CTS pro předcházení kolizím a potvrzování přístupu k médiu, znamená skrytý uzel snížení propustnosti sítě a nárůst chybovosti, ztrátovosti packetů. Taková síť se stává podstatně méně komfortní k používání – právě tak vznikají ona nejrůznější „zamrzání", kdy sice detekujete dostatečný signál, ale data se nepřenáší, nebo přenáší pomalu.

RTS, CTS



Legislativní omezení provozu Wi Fi

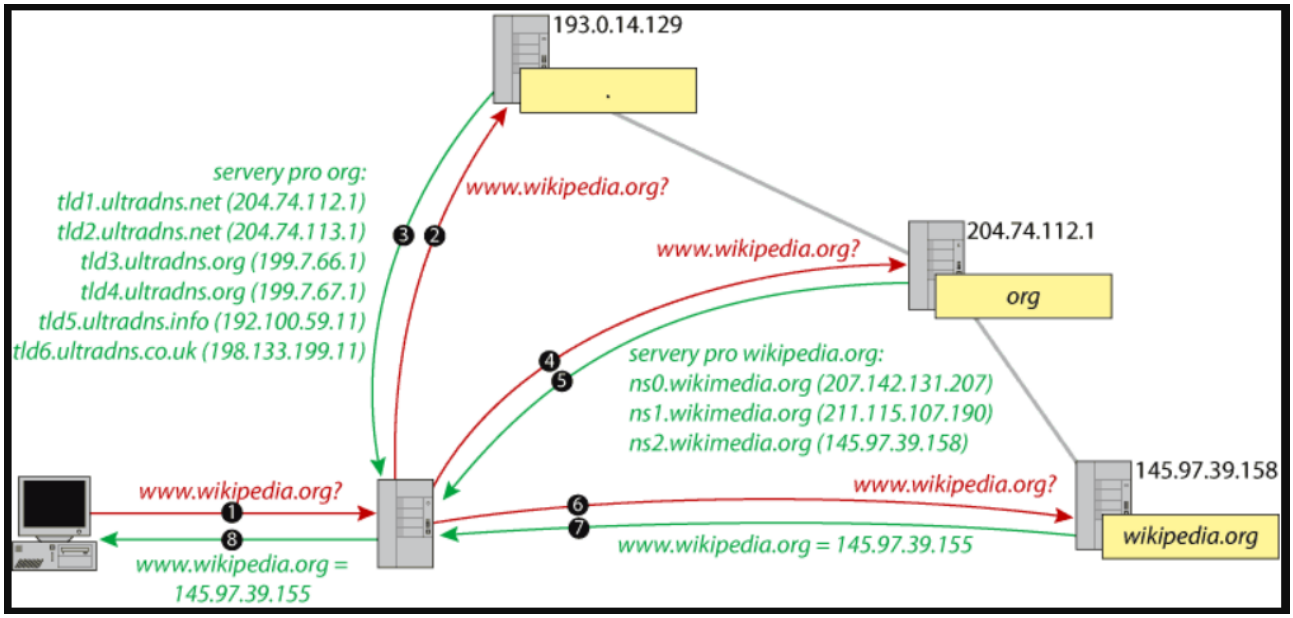
b) technické parametry stanic jsou:

Ozn.	Kmitočtové pásmo	Vyzářený výkon	Maximální spektrální hustota e.i.r.p.	Další podmínky
a	2400,0–2483,5 MHz	100 mW e.i.r.p.[2])	10 mW/1 MHz	systémy s technikou DSSS[5]) nebo OFDM[3])
			100 mW/100 kHz	systémy s technikou FHSS[6])
b	5150–5250 MHz	200 mW střední e.i.r.p.[2]), [7])	10 mW/MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz)	pouze pro použití uvnitř budovy[8])

Výkon + zisk antény – ztráty

30. DNS a zabezpečení

http://www.jakfungujedns.cz/



DNS – Domain Name System překlad URL na IP adresu

Reverse DNS překlad IP adresy na URL

funguje naprosto stejně jako DNS, rozdíl je v tom, kdo spravuje reversní záznamy – většinou to je váš ISP.

Doména 1. řádu (nebo také Top Level Domain – TLD) – IP adresy DNS serverů pro TLD jsou uloženy v tzv. Root serverech. Je jich 13 a značí se písmeny abecedy A-M. Jsou spravovány 12-ti nezávislými organizacemi po celám světě.

DNS – Primární a sekundární DNS servery

Množina autoritativních DNS serverů pro konkrétní doménu se často dělí na jeden **primární** a na jeden nebo více **sekundárních**. **Primární server** je hlavním nositelem informace, je to tedy místo, kde je hlavní úložiště dat a kde jeho administrátor provádí úpravy DNS. Jakmile se na tomto serveru provedou změny v nastavení nějaké domény, **sekundární servery** si tyto změny synchronizují speciálními mechanismy protokolu DNS (notifikace a AXFR přenos). Tyto mechanismy nejsou povinné – záleží na administrátorovi, jak zajistí, aby všechny servery měly aktuální údaje.

Protokol DNS – Autoritativní a neautoritativní odpověď

V souvislosti s cachováním DNS záznamů na serverech je nutné klienty informovat, zda odpověď, která je jim zasílána, pochází od cachovacího serveru anebo zda odpověď přichází přímo od autoritativního DNS serveru. K tomu slouží příznak v hlavičce zprávy protokolu DNS. Jako **neautoritativní** je označena i ta odpověď, kterou právě v tento okamžik cachovací DNS server, který nám dotaz zprostředkovává, přijal z příslušného autoritativního serveru.

Jako **autoritativní** je tedy označena pouze ta, kterou jsme získali přímo bez jakéhokoliv prostředníka.

DNS – Cachovací DNS servery

Mimo autoritativních DNS serverů, které jsou hlavními nositeli informací o doménách, existuje ještě další typ DNS serverů – tzv. **cachovací**. Jakýkoliv klient, který potřebuje pracovat s doménovými názvy, by v běžném případě musel pro překlad každého doménového názvu vždy obeslat množství DNS serverů s dotazy na záznamy pro každou část domény. To je však nešetrné a zbytečné, protože DNS záznamy se tak často nemění. Navíc čím více se ve stromě blížíme kořeni, tím je pravděpodobnost změny v záznamech nižší a nižší. Například je zřejmé, že seznam DNS serverů pro TLD se bude měnit jen jednou za velmi dlouhou dobu a je zbytečné se neustále dokola na to ptát kořenových DNS serverů a zatěžovat je i sebe.

Zde přichází na řadu cachovací DNS servery, které jednotlivým klientům (klienty jsou zde myšleni koncoví uživatelé Internetu – pracovní stanice, jednotlivé aplikační servery apod.) zprostředkovávají celý mechanismus překladů názvů a IP adres a průběžně získávaná data si **ukládají do paměti**. Průběžně zde znamená, že si neukládají nejenom výsledné údaje (např. IP adresy pro požadované doménové názvy), ale také veškeré mezivýsledky, tj. zjištěné autoritativní servery pro všechny uzly na cestě ve stromu od kořeni až k cíli.

SPF – ochrana proti spamu s pomocí DNS

Prakticky to vypadá tak, že majitel domény zanese do zóny speciální záznam **TXT**, ve kterém je uveden seznam IP adres počítačů, ze kterých mohou pocházet e-maily s danou doménou. Typicky to bude seznam IP adres firemních počítačů, serverů, firemní SMTP brány apod. Tento systém musí být samozřejmě podporován ostatními servery. Pokud SMTP server obdrží e-mail a k doméně odesílatele získá dotazem do DNS záznam typu TXT, který obsahuje SPF pravidla, provede kontrolu. E-mail pak propustí jen pokud pravidlům vyhovuje. Jinak jej odmítne. Kontrola se provádí ještě před zasláním těla zprávy (po odeslání příkazu MAIL FROM). SMTP server, který SPF nepodporuje, jej nezkontroluje a e-mail propustí dál.

Příklad obsahu zónového souboru pro doménu *example.com*

```
$ORIGIN example.com.     ; designates the start of this zone file in the namespace
$TTL 1h                  ; default expiration time of all resource records without their own TTL value
example.com.  IN  SOA   ns.example.com. username.example.com. ( 2007120710 1d 2h 4w 1h )
example.com.  IN  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  IN  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for example.com
example.com.  IN  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             IN  MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             IN  MX    50 mail3              ; equivalent to above line, but using a relative host name
example.com.  IN  A     192.0.2.1             ; IPv4 address for example.com
              IN  AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            IN  A     192.0.2.2             ; IPv4 address for ns.example.com
              IN  AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           IN  CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       IN  CNAME www                   ; wwwtest.example.com is another alias for www.example.com
mail          IN  A     192.0.2.3             ; IPv4 address for mail.example.com
mail2         IN  A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         IN  A     192.0.2.5             ; IPv4 address for mail3.example.com
```

Příklad obsahu zónového souboru pro reversní záznam IP 192.168.0.x

```
$TTL    86400 ; 24 hours, could have been written as 24h or 1d
$ORIGIN 0.168.192.IN-ADDR.ARPA.
@  1D  IN        SOA ns1.example.com.   hostmaster.example.com. (
                              2002022401 ; serial
                              3H ; refresh
                              15 ; retry
                              1w ; expire
                              3h ; minimum
                             )
; Name servers for the zone - both out-of-zone - no A RRs required
       IN  NS ns1.example.com.
       IN  NS ns2.smokeyjoe.com.
; server host definitions
1      IN  PTR    ns1.example.com.
2      IN  PTR    www.example.com.
; non server domain hosts
3      IN  PTR    bill.example.com.
4      IN  PTR    fred.example.com.
```

Některé typy záznamů:

A – Address record
AAAA – IPv6 Address record
CNAME – Canonical name record (slouží k přesměrování na jinou doménu)
MX – Mail exchanger record (přesměrování na mail server pro tuto doménu)
TTL – Time to live (jak dlouho je záznam z tohoto serveru platný, pokud je záznam umístěn např. V cache serveru)

kontrola DNS:

http://www.intodns.com/

http://mxtoolbox.com/

DNSSEC

DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS.

DNSSEC používá asymetrické šifrování (jeden klíč pro zašifrování, druhý klíč na dešifrování). Držitel domény vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče je pak možné ověřit pravost tohoto podpisu. Aby byl tento klíč dostupný všem, publikuje jej držitel ke své doméně u nadřazené autority (v případě domén .CZ je to CZ.NIC).

https://www.dnssec.cz/page/444/jak-funguje-dnssec/