POČÍTAČOVÉ SÍTĚ (2. část)

Přístupové metody

Přístupové metody definují pravidla, podle kterých stanice v síti přistupují ke komunikačnímu kanálu (např. kabelu), který společně sdílejí. Zabezpečují, aby v jednom okamžiku komunikovala prostřednictvím komunikačního kanálu pouze jedna stanice. Při současném vysílání více stanic jedním kanálem (např. vodičem) dojde ke vzájemnému rušení, což znemožní přenos dat. Přístupová metoda je jedním z podstatných znaků síťového standardu.

1. CSMA / CD (Carrier-sense Multiple Access with Collision Detection)

Metoda vícenásobného přístupu ke komunikačnímu kanálu s detekcí kolize. Stanice, která chce vysílat, zkontroluje, zda již nevysílá jiná stanice, připojená do sítě. Pokud tomu tak je, počká až bude komunikační kanál (spojovací vedení) volný. Je-li volno, začne vysílat paket, který se šíří ke všem zbývajícím stanicím připojeným do sítě. Stanice dále pokračuje ve sledování sítě (sleduje, zdali je na síti právě to, co tam poslala). Pokud ve stejném okamžiku začnou vysílat stanice dvě, nastává detekce kolize (CD - Collision Detection). Kolize je detekována tak, že stanice, které vyslaly své pakety a sledují síť, zjistí, že na přenosovém médiu se vyskytují jiné informace, než ty, které tam vyslaly. Stanice se odmlčí a po náhodně stanovené době se pokusí o nové vysílání. Náhodně dlouhá doba (u každé stanice jiná) zaručuje poměrně vysokou pravděpodobnost, že nedojde znovu ke kolizi mezi stejnými stanicemi.

Metodu CSMA/CD používala především sběrnicové topologie sítě standardu Ethernet (koaxiální kabel).

2. CSMA / CA (Carrier-sense Multiple Access with Collision Avoidance)

Metoda vícenásobného přístupu ke komunikačnímu kanálu se zabráněním vzniku kolize. Používá se u bezdrátových sítí standardu Wi-Fi pro zprostředkování komunikace mezi zařízeními. Pokud chce klientská stanice vysílat, poslouchá, je-li v příslušném komunikačním kanálu nějaká aktivita. Pokud ano, počká náhodně dlouhou dobu a poté se pokusí ke kanálu přistoupit znovu. Pokud je kanál volný, musí klientská stanice nejprve požádat přístupový bod (AP) o vysílání. Vyšle signál RTS (Request To Send – požadavek na přenos) a vyčkává, dokud od přístupového bodu nedostane povolení k vysílání ve formě signálu CTS (Clear To Send). Ostatní klientské stanice připojené k AP mají povel nevysílat.

3. Full-Duplex

Využívá se u současných sítí hvězdicové topologie. TP kabel obsahuje 4 páry vodičů. 1 pár vodičů je vyčleněn pro přenos dat z počítače do switche, 1 pár vodičů pro směr opačný. Zbylé páry propojovacího (patch kabelu) nejsou využity. Komunikace prostřednictvím TP kabelu probíhá obousměrně, každé zařízení (např. počítač-switch, počítač-počítač, atd.) má své pevně přidělené vodiče, pomocí nichž může vysílat kdykoliv. Odpadá sdílení média a s ním i důvody pro nasazení algoritmu CSMA/CD.

Odpadají zde prostoje způsobené kolizemi a přenosová rychlost odpovídá maximální možné.

4. Token ring

Používá se především u kruhové topologie sítě. Sítí putuje speciální paket – tzv. token. Vysílat může jen ta stanice, která tento paket vlastní. Vysílat může tedy jen jedna stanice. Token si stanice postupně předávají. Paket putuje v kruhu od jedné stanice ke druhé.

Referenční model počítačové sítě ISO/OSI

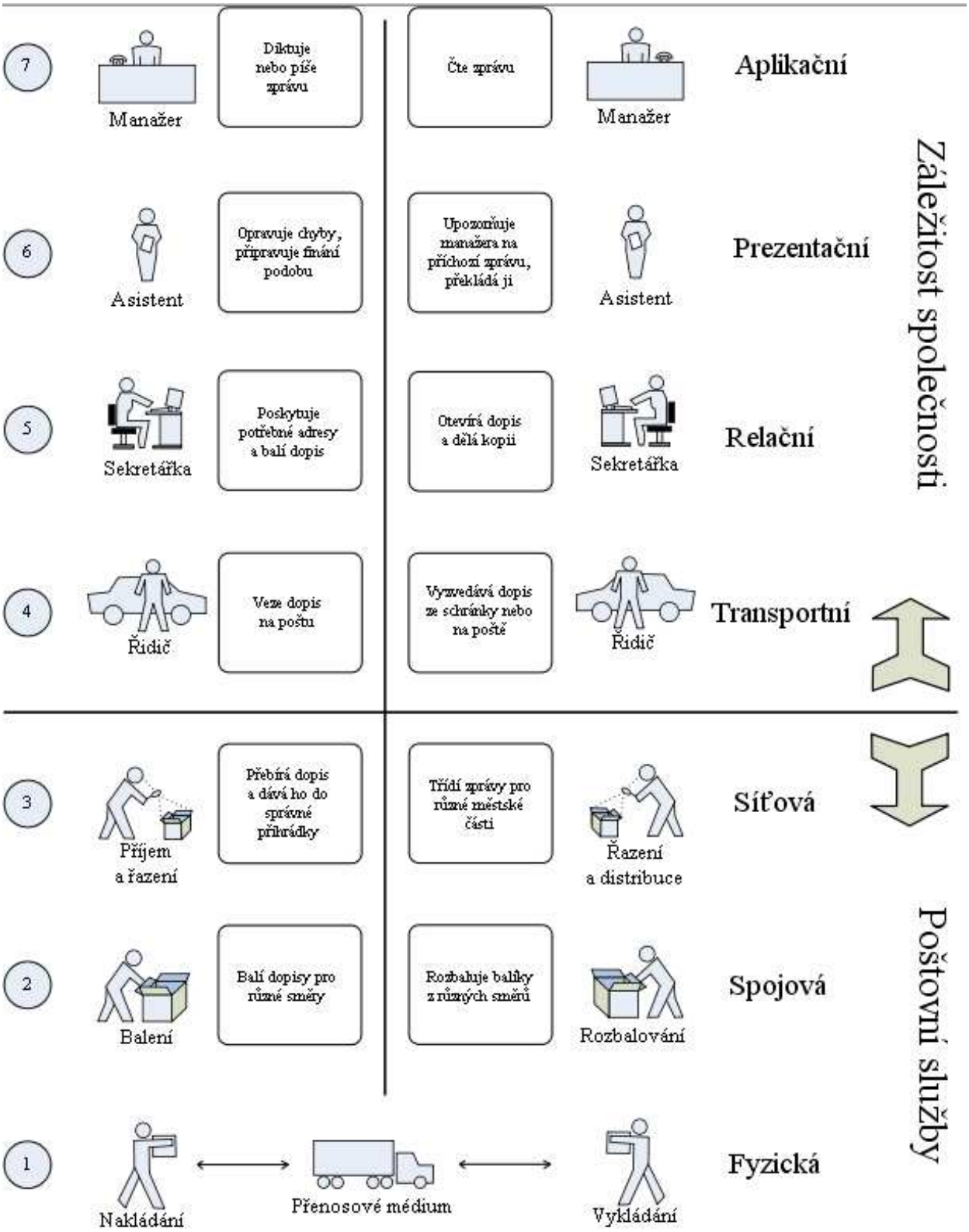
Přenos informací v počítačové síti je obecně považován za složitou úlohu sestávající se z mnoha kroků. Není možné, aby jedno zařízení (např. komunikující počítač) obstarávalo veškeré úkony spojené s přenosem dat. Proto se komunikace rozděluje do několika nezávislých úrovní (vrstev), kdy každá vrstva řeší pouze určité kroky spojené s přenosem dat.

Smyslem obecného referenčního modelu sítě je poskytnout základ pro vypracování norem za účelem propojování jednotlivých zařízení. Jedná se o doporučený model sítě, který rozděluje vzájemnou komunikaci mezi zařízeními do *7 vrstev (úrovní)*. Významný je především pro výrobce síťových prvků. Úkolem každé vrstvy (síťových prvků či programů na dané vrstvě) je poskytovat služby následující vyšší vrstvě a nezatěžovat vyšší vrstvu detaily o tom jak je služba ve skutečnosti realizována. Než se data přesunou z jedné vrstvy do druhé, rozdělí se do *paketů* (datové balíčky). V každé vrstvě se pak k paketu přidávají další doplňkové informace (např. adresy, zabezpečení dat, atd.), které jsou nezbytné pro úspěšný přenos dat po síti.

1. *Fyzická* vrstva - Popisuje fyzické, elektrické, mechanické a funkční parametry technických prostředků pro komunikaci v síti: např. kabely, konektory, ukončovací prvky, dále průběhy a tvar signálů (elektrické, optické), atd. Určuje způsob přenosu binární informace (log.0 a log.1)
2. *Linková* vrstva – Uskutečňuje přenos údajů prostřednictvím komunikačního kanálu, pracuje s fyzickými adresami (MAC) síťových karet, kontroluje jejich zdrojové a cílové adresy, odesílá a přijímá datové pakety podle těchto adres, atd.
3. *Síťová* vrstva - Definuje protokoly pro směrování dat mezi počítači nebo celými sítěmi (tzv. uzly), mezi nimiž není přímé spojení. V lokální síti vůbec nemusí být pokud se nepoužívá směrování. Zajišťuje volbu trasy při spojení (mezi síťovými uzly bývá více možných cest pro přenos paketu). Na této vrstvě pracují směrovače (routery).
4. *Transportní* vrstva - Tato vrstva se již nezabývá samotným přenosem dat, je softwarová. Jejím úkolem je dělení přenášené zprávy na pakety a opětovné skládání paketů do zprávy. Zabezpečuje bezchybnost přenosu (provádí kontroly integrity dat).
5. *Relační* vrstva – Jedná se o softwarovou vrstvu, jejímž úkolem je navázat a ukončit spojení, provádět ověřování uživatelů a zabezpečovat přístup k zařízením.
6. *Prezentační* vrstva - Specifikuje způsob, jakým jsou data formátována (upravena) a kódována, provádí jejich konverzi. Řeší např. háčky a čárky, kontrolní součet, kompresi a dekompresi, šifrování dat. Je softwarová.
7. *Aplikační vrstva* – Je určitou aplikací (např. okno v programu), zpřístupňující uživateli síťové služby. Zabezpečuje přístup k souborům na jiných počítačích, vzdálený přístup k tiskárně, elektronickou poštu, přístup do databáze, atd. Využívá služeb nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků.

Analogie:

Příkladem připomínajícím vrstvový model ISO/OSI může být dopisová komunikace mezi manažery dvou firem. Každý prvek (s výjimkou fyzické vrstvy) má přímý kontakt (pomocí určitého rozhraní) pouze s prvky v sousedních vrstvách. Rozhraním se myslí např. poštovní schránka mezi 4. a 3. vrstvou nebo přihrádka mezi 3. a 2. vrstvou. Každý prvek na straně odesílatele zpracuje zprávu do takového tvaru (dle protokolu), aby jí rozuměl jeho protějšek na straně příjemce. Protokol např. udává, jak má být správně nadepsaná adresa 5. vrstvou, nebo jak správně ve 2. vrstvě seskupit více dopisů jdoucích stejným směrem.



Síťové standardy

Pro vzájemnou kompatibilitu (bezproblémovou spolupráci) síťových zařízení jsou vytvářeny síťové standardy (normy). Normalizaci provádí americká organizace IEEE (Institute of Electrical and Electronics Engineers), proto jednotlivé normy nesou označení této organizace.

Z praktického hlediska nás nejvíce zajímají především tyto standardem definované vlastnosti sítě:

- přístupová metoda ke komunikačnímu kanálu
- topologie sítě
- typy a parametry pasivních prvků sítě (kabely, konektory, popř. ukončovací prvky)
- typy a parametry aktivních prvků sítě
- rychlost přenosu dat
- skladba datového paketu

Základním standardem pro sítě MAN a LAN je **IEEE 802.xx**. Standardy pokrývají fyzickou vrstvu (specifikace hardware) a linkovou vrstvu modelu ISO/OSI. Nejznámější standardy sítí LAN:

Standard Ethernet (IEEE 802.3)

Nejrozšířenější standard sítí LAN. Standard Ethernet lze rozdělit do 6 kategorií podle maximální teoretické přenosové rychlosti. Každá kategorie obsahuje detailnější specifikace tohoto standardu (především typ a parametry kabeláže, aktivních prvků, přístupové metody, atd.).

Mezi nejznámější specifikace standardu Ethernet řadíme:

1. **Ethernet (10 Mb/s)**

   1.1. Specifikace 10Base-2

   Ethernet specifikující jako přenosové médium tenký koaxiální kabel s konektorem BNC o rychlosti 10 Mb/s. Koaxiální kabel tvoří sběrnici, ke které se připojují jednotlivé stanice přímo. Kabel je impedance 50 Ω, nesmí mít žádné odbočky a je na koncích zakončen impedancí 50 Ω (tzv. terminátor). Využívá přístupovou metodu CSMA/CD. Dnes se již tato specifikace Ethernetu v běžné praxi nepoužívá.

   1.2. Specifikace 10Base-T

   Ethernet specifikující jako přenosové médium kroucenou dvoulinku (TP kabel) s rychlostí 10 Mb/s. Využívá dva páry vodičů ze čtyř (přístupová metoda Full Duplex). Dnes již překonaná varianta standardu Ethernet, která byla nahrazena rychlejší variantou 100 Mb/s a 1000 Mb/s.

   1.3. Specifikace 10Base-F

   Specifikace s optickými vlákny o rychlosti 10 Mb/s. Používala se pro spojení na větší vzdálenost nebo pro spojení mezi objekty, kde nelze použít kroucená dvoulinka. Tvořila obvykle tzv. páteřní síť, která propojovala jednotlivé menší celky sítě. Dnes je již nepoužívá.

2. Fast Ethernet (100 Mb/s)

2.1. Specifikace 100Base-T

Ethernet specifikující jako přenosové médium TP kabely pro teoretickou přenosovou rychlost 100 Mb/s. Konektor je typu RJ-45. Specifikace se dále dělí podle konkrétní kategorie TP kabelu. Kategorie TP kabelu (viz tabulka níže) určuje:

- maximální pracovní kmitočet, tedy šířku pásma v MHz (souvisí s max. přenosovou rychlostí)

- maximální délku kabelu

Stručný přehled kategorií

název	šířka pásma	rychlost	jednotka	technologie
Cat.3	16 MHz	10	Mbit/s	10Base-T
Cat.4	20 MHz	16	Mbit/s	TokenRing 16
Cat.5	100 MHz	100	Mbit/s	100Base-Tx
Cat.5E	100 MHz	1	Gb/s	1000Base-T
Cat.6	250 MHz	1	Gb/s	1000Base-TX
Cat.6A	500 MHz	10	Gb/s	10GBase-T
Cat.7	600 MHz	10	Gb/s	10GBase-T
Cat.7A	1000 MHz	40	Gb/s	40GBase-T

2.2. Specifikace 100Base-FX

Ethernet specifikující jako přenosové médium optický kabel s minimálně 2 optickými vlákny (2 směry přenosu).

3. Gigabit Ethernet (1 Gb/s)

3.1. Specifikace 1000Base-T

Specifikace určující jako přenosové médium UTP kabel kategorie 5e (do 100 MHz), je definován do vzdálenosti maximálně 100 metrů.

3.2. Specifikace 1000Base-SX, 1000Base-LX

SX – pro přenos využívá mnohovidové (multi mode) optické vlákno. Je určena pro páteřní sítě do vzdáleností několik set metrů.

LX – pro přenos využívá jednovidové (single mode) optické vlákno. Je určena pro větší vzdáleností až několika desítek kilometrů.

4. 10 Gigabit Ethernet (10 Gb/s)

4.1. Specifikace 10GBase pro optické přenosy

Původní návrhy 10GBase počítaly pouze s optickým přenosem dat. Existuje více standardů pro optické přenosy prostřednictvím jednovidových (single mode) i mnohovidových (multi mode) vláken. Liší se maximální vzdáleností a vlnovou délkou optického signálu.

10GBase-LR, ER, ZR pro jednovidová vlákna

10GBase-SR, LX4 pro mnohovidová vlákna

4.2. Specifikace 10GBase-T a 10GBase-CX

Ethernet s rychlostí 10 Gb/s prostřednictvím metalického vedení. Pro vzdálenost 55 m se používají TP kabely kategorie 6 (šířka pásma 250 MHz), pro vzdálenost 100 m se používají TP kabely kategorie 6a (šířka pásma 500 MHz) a kategorie 7 (šířka pásma 600 MHz). Varianta CX je určena pro spojení do 15 metrů metalickým vedením.

5. 40 a 100 Gigabit Ethernet (40 a 100 Gb/s)

Vysokorychlostní standardy Ethernet přicházející na trh. Přenos informací probíhá především prostřednictvím optických vláken s využitím technologie vlnového multiplexu, specifikovány jsou také přenosy prostřednictvím kvalitně stíněného TP kabelu kategorie 7a (šířka pásma 1000 MHz).

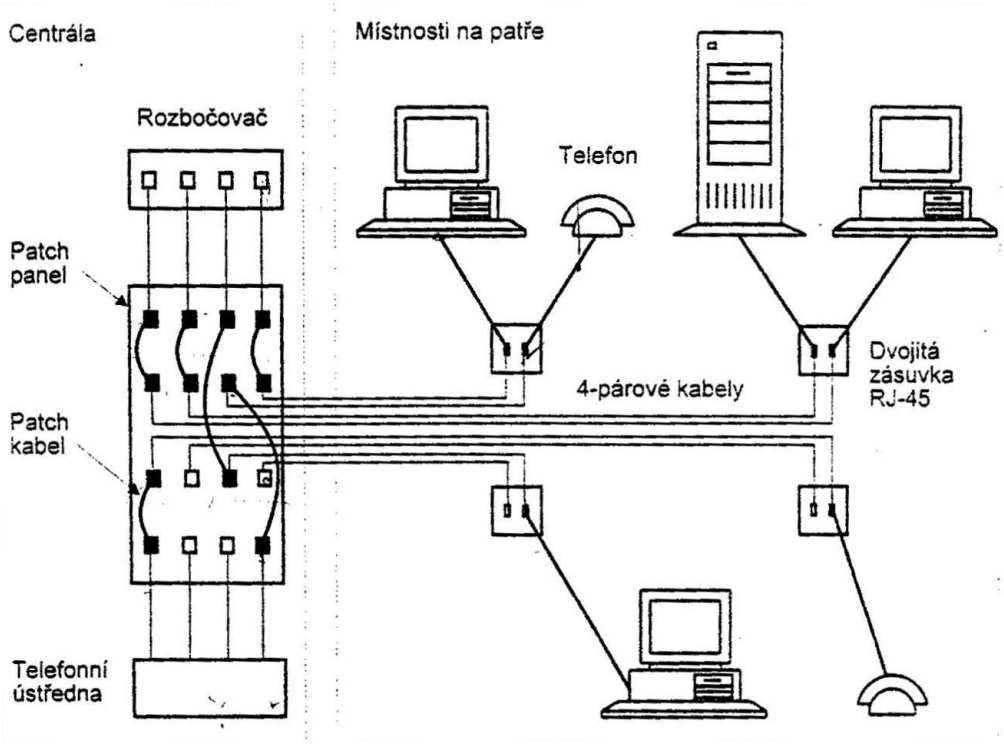
Funkce PoE (Power Over Ethernet)

Tato funkce umožňuje napájení koncových zařízení prostřednictvím TP kabelu bez nutnosti použití přídavných napájecích zdrojů či síťových adaptérů na straně napájeného zařízení, popřípadě vedení samostatného napájecího kabelu souběžně s datovým kabelem. Smyslem funkce PoE je:

- Ušetřit kabely
- Zjednodušit připojování zařízení; zapojuje se jen 1 datový konektor místo 2 (data+napájení)
- Zajistit zálohované napájení i při výpadku napájecí sítě v okolí přístroje, centrální zdroj PoE je obvykle napájen přes záložní zdroj
- Umožnit správci sítě snadný dálkový restart napájeného zařízení na konci kabelu vypnutím a zapnutím napájení

Strukturovaná kabeláž

Strukturovaný kabelážní systém je univerzální systém, který slouží pro potřeby přenosu dat (počítačová síť, internet), hlasu (telefony) a obrazu (kamerové systémy).



Kabely začínají v propojovacím panelu (patch panel) v rozvaděčové skříni (tzv) a končí v dvojité zásuvce na zdi. Do každé dvojité zásuvky vedou dva kabely. Ve skříní je kromě patch panelu ještě switch (resp. v minulosti rozbočovač, tedy HUB) a telefonní ústředna. Nejčastěji bývá jedna rozvaděčová skříň pro více pater budovy a v místnostech vždy jedna telekomunikační zásuvka pro jedno pracovní místo (počítač + IP telefon).

Jednoduchým přepojením patch kabelů v propojovacím panelu lze změnit význam jednotlivých zdířek v telekomunikačních zásuvkách. K jedné zásuvce lze tedy připojit PC + telefon, 2 PC nebo 2 telefony, stačí pouze přepojit patch kabely v propojovacím panelu. Dříve používané samostatné kabelové rozvody jsou tak nahrazeny jediným, univerzálním systémem.

Topologie strukturované kabeláže je hvězdicová. Pro rozvody v rámci budovy se používá kroucená dvoulinka (TP kabel) kategorie 5E (šířka pásma100 MHz) s konektorem RJ 45, postupně se přechází na TP kabely kategorie 6A (šířka pásma 500 MHz) a kategorie 7 (šířka pásma 600 MHz). Fyzická délka kabelu nemá překročit 100 metrů.

Řešení strukturované kabeláže je možné také pomocí optických rozvodů. Jedná se především o instalaci sítí ve venkovním prostředí nebo v náročných provozech (velká vzdálenost, rušení, atd.). Nejčastějším využitím optické sítě je propojení budov, ve kterých je nainstalovaná síť na bázi TP kabelů.

Bezdrátové sítě

Bezdrátová síť je typ počítačové sítě, ve které je spojení mezi jednotlivými zařízeními uskutečňováno pomocí elektromagnetických vln (rádiové vlny, popřípadě světelné záření).

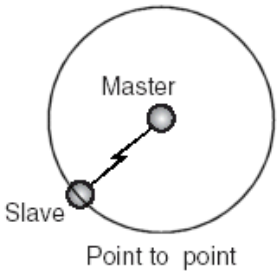
Přehled současných bezdrátových standardů:

1. IEEE 802.15 - Bezdrátové osobní sítě (Wireless Personal Area Network, WPAN)
2. IEEE 802.11 - Bezdrátové lokální sítě (Wireless Local Area Network, WLAN)
3. IEEE 802.16 - Bezdrátové metropolitní sítě (Wireless Metropolitan Area Network, WMAN)
4. Mobilní sítě (WWAN)

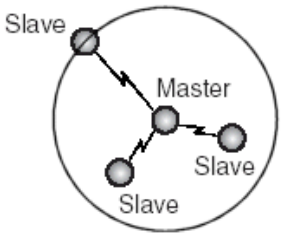
1. Bezdrátové osobní sítě (standard IEEE 802.15)

Mezi bezdrátové osobní sítě standardu 802.15 řadíme rádiové rozhraní *Bluetooth*. Toto rozhraní využívá pro komunikaci rádiové vlny pracující ve frekvenčním pásmu 2400 MHz až 2483,5 MHz, které je rozděleno na 79 kanálů, vždy se vzájemným odstupem 1 MHz.

Bluetooth podporuje jak dvoubodovou, tak mnohabodovou komunikaci.

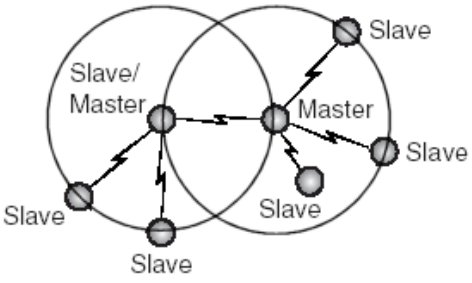


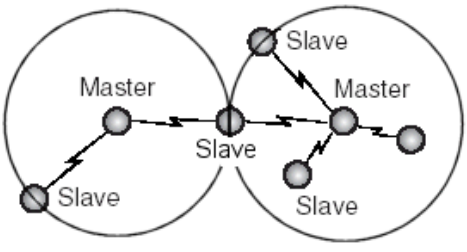
Point to point



Point to multipoint

Pokud je více stanic propojeno do tzv. pikosítě (pikonet), jedna rádiová stanice působí jako hlavní (master) a může simultánně obsloužit až 7 podřízených (slave) zařízení. Všechna zařízení v pikosíti se synchronizují s taktem hlavní stanice. Pikosítě lze sdružovat do tzv. scatternets ("rozprostřených" sítí). V této struktuře jsou některá zařízení obsažena ve více pikosítích a zajišťují tak jejich propojení.





Více informací viz výukový materiál OVT 3. ročník - „Počítačová rozhraní“.

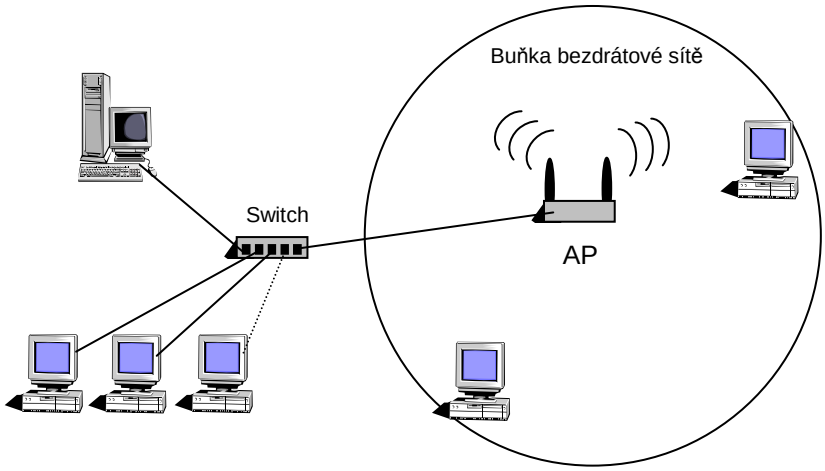
2. Bezdrátové lokální sítě (standard IEEE 802.11)

Bezdrátovou lokální síť standardu IEEE 802.11 označujeme *Wi-Fi*. Pro vzájemnou komunikaci mezi zařízeními využívá rádiové vlny v kmitočtovém pásmu 2,4 GHz a 5 GHz (bezlicenční pásmo) s přístupovou metodou ke komunikačnímu kanálu CSMA/CA. V současnosti existuje několik specifikací standardu 802.11, které se vzájemné liší především teoretickou přenosovou rychlostí. Mezi nejpoužívanější specifikace řadíme:

standard	**teoretická rychlost**	**kmitočet**
802.11a	do 54 Mb/s	5 GHz
802.11b	do 11 Mb/s	2,4 GHz
802.11g	do 54 Mb/s	2,4 GHz
802.11n	do 600 Mb/s	2,4 i 5 GHz

Základním prvkem Wi-Fi sítí je přístupový bod (AP - Access Point), kolem kterého se vytvoří buňka bezdrátové sítě. Přístupový bod komunikuje s klientskými adaptéry (bezdrátové síťové karty v počítačích) ve svém dosahu a stará se o směřování komunikace mezi nimi a zpravidla také pevnou kabelovou sítí.

Druhou část tvoří klientské adaptéry. Klientský adaptér je bezdrátová síťová karta s anténou. Může být v provedení PCI, PCCard, ExpressCard, externí adaptér pro USB rozhraní nebo je součástí přenosných počítačů (anténka pak bývá zabudována v rámu displeje notebooku).



Oba základní prvky jsou schopny rádiové signály přijímat i vysílat. AP má funkci switche, umožňuje tedy filtraci paketů, dále má funkci bezdrátového mostu (propojení segmentů sítě bezdrátově).

Původním cílem Wi-Fi sítí bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě.

S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit. Wi-Fi adaptéry jsou dnes prakticky ve všech přenosných počítačích a také v mobilních telefonech, PDA či tiskárnách. Úspěch Wi-Fi přineslo využívání bezlicenčního pásma, což má však negativní dopad ve formě silného zarušení příslušného frekvenčního spektra v dané lokalitě a dále časté bezpečnostní incidenty.

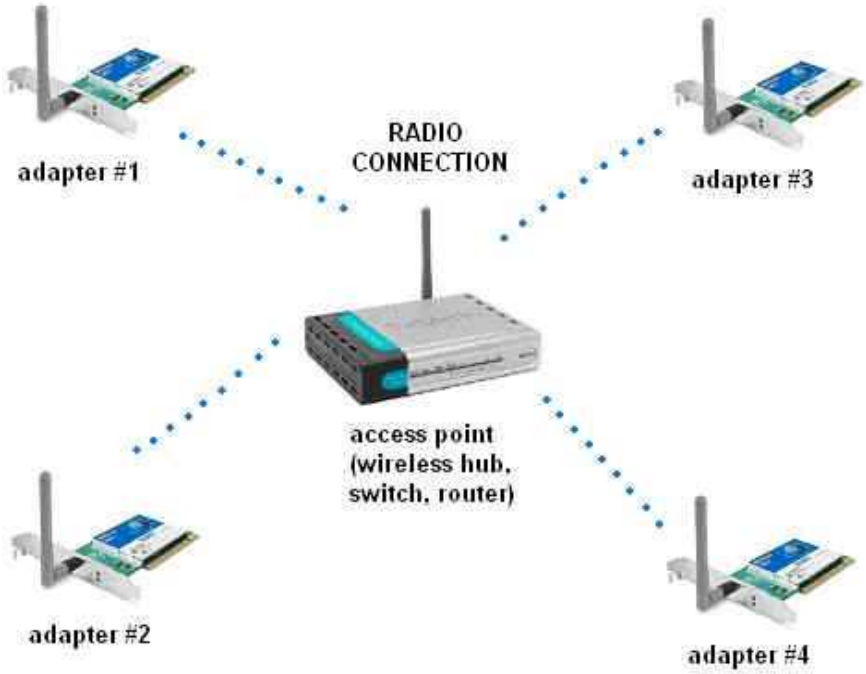
2.1 Struktura Wi-Fi sítě

a. Ad-Hoc síť (peer to peer)

Jedná se o přímé spojení jednotlivých počítačů vybavených Wi-Fi adaptérem bez potřeby přístupového bodu. Nevýhodou je, že všechny Wi-Fi zařízení musí být v rádiovém dosahu jeden druhého.

b. Infrastrukturní síť

*Z*ákladním rozdílem mezi sítěmi ad-hoc a infrastrukturními sítěmi je použití přístupového bodu (AP neboli Access Point), přes který probíhá veškerá komunikace. Přístupový bod plní funkce switche v běžných sítích LAN. Jednotlivá koncová zařízení nemusí být v dosahu jeden druhého, ale stačí být v dosahu alespoň jednoho přístupového bodu a ten již komunikaci předá dále. Další výhodou je fakt, že AP umožňuje propojení s "drátovou" sítí LAN či přístup k síti WAN (typicky Internet).



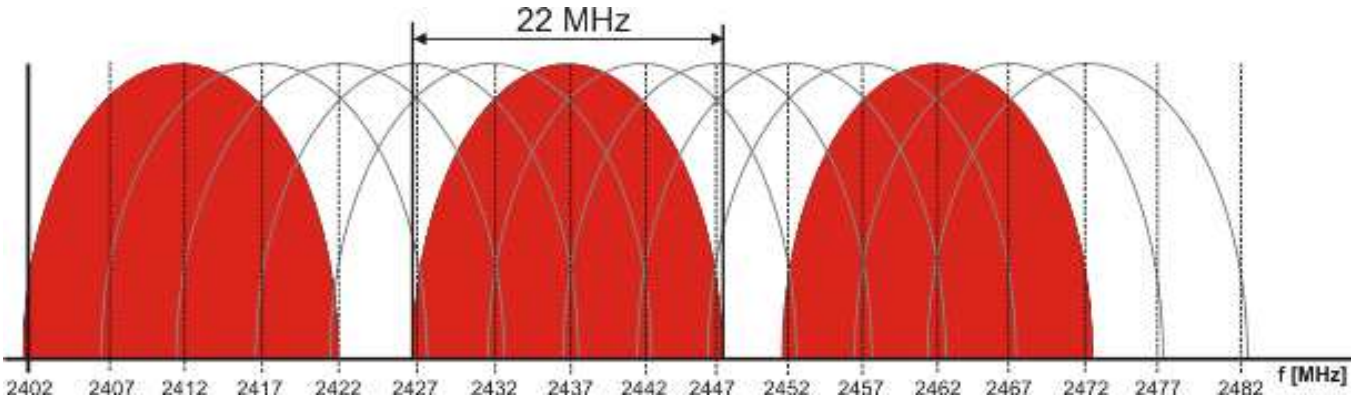
Veřejné přístupové body (veřejné hotspoty)

Lze se s nimi setkat na letištích, na větších vlakových nádražích, kavárnách, nákupní centra (např. AVION shopping park v Ostravě) atd. Tyto hotspoty nebývají zabezpečeny a zajišťují přístup k síti Internet libovolnému uživateli vybavenému přenosným zařízením s Wi-Fi adaptérem.

2.2 Komunikační kanály

Standard 802.11 b/g pro Evropu definuje v pásmu 2,4GHz 13 komunikačních kanálů o šířce 5 MHz. Povolený vyzářený výkon je 100 mW.

Frekvenční pásma jednotlivých kanálů se vzájemně překrývají. V rámci určitého prostoru může vysílat i několik bezdrátových sítí. Aby nedocházelo k rušení, musí každá síť vysílat na jiném kanále. Bezdrátová síť by měla vysílat na kanále, jehož číslo je alespoň ± 3 vzdáleno od kanálu sousední sítě. Pro pásmo 2,4 GHz existují pouze 3 nepřekrývající se kanály (viz obrázek níže).



Standard popisující frekvenční pásmo 5 GHz pro Evropu definuje šířku jednoho komunikačního kanálu 20 MHz. Z hlediska regulačních pravidel se pásmo 5 GHz dělí do 3 skupin:

A. *5150 - 5250 MHz* (zkráceně 5,1 GHz): použití pouze uvnitř jedné budovy, maximální hodnota vyzářeného výkonu je 200 mW
B. *5250 – 5350 MHz* (zkráceně 5,2 GHz): použití pouze uvnitř jedné budovy. Zařízení v tomto pásmu musí být vybaveny automatickou regulací výkonu, která může snížit podle podmínek výstupní výkon zařízení na polovinu. Tato regulace ale nemusí být zapnuta, potom je však maximální vyzářený výkon poloviční, tj. 100 mW. Zařízení musí být schopno automatického přelaďování.
C. *5470 - 5725 MHz* (zkráceně 5,4 GHz): použití uvnitř i vně budov, maximální vyzářený výkon 1 W. Zařízení musí být vybaveno automatickou regulací výkonu, není-li zapnuta, je max. vyzářený výkon poloviční, tj. 0,5 W. I zde musí být zařízení schopno automatického přelaďování. Na rozdíl od pásma 2,4 GHz nabízí 11 vzájemně se nepřekrývajících kanálů (11 navzájem se nerušících sítí v rámci jednoho prostoru).

2.3 Zabezpečení Wi-Fi sítě

2.3.1 Skrytí SSID (Service Set Identifier)

SSID neboli název bezdrátové sítě (název přístupového bodu) je možné veřejně vysílat, popřípadě jej schovat, takže se připojí automaticky pouze stanice, která jej zná. Nejedná se ve skutečnosti o žádné seriózní zabezpečení, neboť SSID se dá odhalit velice rychle (např. program NetStumbler)

2.3.2 Filtrace MAC adres

MAC adresa je jedinečný identifikátor každého síťového zařízení, tedy i bezdrátového síťového adaptéru. Prostřednictvím konfiguračního rozhraní přístupového bodu lze uložit MAC adresy síťových zařízení, které mají povolenou (resp. zakázanou) komunikaci v rámci dané bezdrátové sítě.

Doporučována je první možnost, tedy seznam MAC adres s povolenou komunikací. Ostatním zařízením bude komunikace prostřednictvím přístupového bodu zamítnuta.

2.3.3 Regulace výstupního výkon AP

Snížení výstupního výkonu vysílaného signálu tak, aby pokryl, pokud možno, pouze prostory, v nichž se nachází síťová zařízení s oprávněním komunikovat v dané síti. Výstupní výkon se volí v nastavení konfiguračního prostředí přístupového bodu.

2.2.4 Nastavení šifrování komunikace

a. **WEP** (Wired Equivalent Privacy) je protokol sloužící k šifrování a dešifrování přenášených dat v bezdrátové síti. Zároveň slouží k zabezpečení přístupu do bezdrátové sítě. Ověřování je pouze jednostranné (pouze klientské zařízení vůči přístupovému bodu).

   Pro šifrování a dešifrování používá stejný, dnes již překonaný algoritmus i totožný statický klíč (všechna zařízení v síti sdílejí stejný klíč). Šifrování přenášených dat se provádí 64 bitovým (WEP 64) nebo 128 bitovým (WEP 128) klíčem.

   Reálná délka 64 bitového klíče je 40 bitů a 128 bitového klíče 104 bitů. Druhou část tvoří tzv. inicializační vektor (24 bitů), který je zasílán v hlavičce každého paketu a neustále se mění (šifrování je jedinečné pro každý paket). Nevýhodou je, že se tato dynamická část klíče v reálném čase opakuje.

   V současnosti se jedná o nejslabší a snadno prolomitelné zabezpečení sítě (na internetu existuje mnoho návodů a programů k prolomení tohoto zabezpečení). Dnes se používá výhradně ve spojitosti se starými Wi-Fi klientskými adaptéry, které podporují pouze WEP protokol.

b. **WPA** (WiFi Protected Access) je zpětně kompatibilní s WEP, používá stejný šifrovací algoritmus, ale se 128 bitovým klíčem a 48 bitovým inicializačním vektorem.

   Zásadní vylepšení oproti WEP zabezpečení spočívá v použití TKIP (Temporal Key Integrity Protocol), což je protokol dynamicky měnící klíče. Byla také vylepšena metoda kontroly integrity (celistvosti, správnosti) dat.

   WPA nabízí více možností zabezpečení sítě:

   RADIUS - autentizační server RADIUS (Remote Authentication Dial-In User Service), jehož úkolem je po úspěšné autentizaci vzdálené stanice (login+heslo) zaslat této stanici klíč. Každá stanice obdrží od serveru RADIUS jiný klíč. Jedná se o nákladné řešení zabezpečení, vhodné pouze pro větší podnikové sítě.

   PSK – zabezpečení PSK (Pre-Shared Key) je řešení, kdy má každá klientská stanice stejný přístupový klíč. Každý uživatel musí před vstupem do sítě zadat heslo obsahující 8 až 63 tisknutelných znaků. Většina operačních systémů umožňuje uložení hesla na uživatelském počítači, aby nebylo nutné jej opakovaně zadávat. Heslo musí být uloženo na všech přístupových bodech Wi-Fi sítě. Vhodné spíše pro kanceláře a domácí sítě.

   WPA je dnes považováno podobně jako WEP za překonanou techniku zabezpečení bezdrátové sítě.

c. **WPA 2** je také označován jako standard IEEE 802.11i. Klíč již neobsahuje inicializační vektor a zavádí se číslování paketů (PN – Packet Number). Každý paket, obsahující číslo stejné nebo nižší než předchozí, je zahozen (ochrana proti útokům, které se snaží zopakovat předchozí odposlouchanou komunikaci). Nabízí silnější šifrování AES (Advanced Encryption Standard),

které však vyžaduje výkonnější hardware. Možnosti zabezpečení sítě jsou shodné s WPA, tedy buď použití serveru pro vzdálenou autentizaci klientských stanic (RADIUS) nebo pomocí sdíleného klíče (PSK).

2.3.5 Zabezpečení přístupu ke konfiguraci AP

Pro přístup ke konfiguračnímu rozhraní přístupového bodu je vhodné nastavit přihlašovací jméno a heslo, které je jiné než u továrního nastavení. Pokud se útočník nějakým způsobem dostane do bezdrátové sítě, není pro něj problém dostat se do konfiguračního rozhraní AP a získat nad sítí plnou kontrolu.

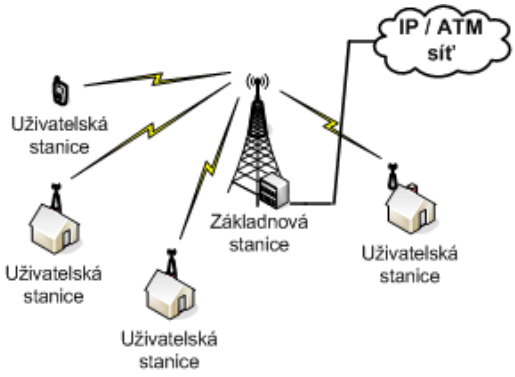
Pozn.: V praxi je vhodné výše zmíněné možnosti zabezpečení využívat v maximální možné míře společně. Přehled metod zabezpečení bezdrátové sítě není kompletní (dále je vhodné např. vypnutí DHCP serveru, používání silných hesel, která jsou odolná vůči „slovníkovým“ útokům, zamezení fyzického přístupu neoprávněných osob k přístupovému bodu, apod.)

3. Bezdrátové metropolitní sítě (standard IEEE 802.16)

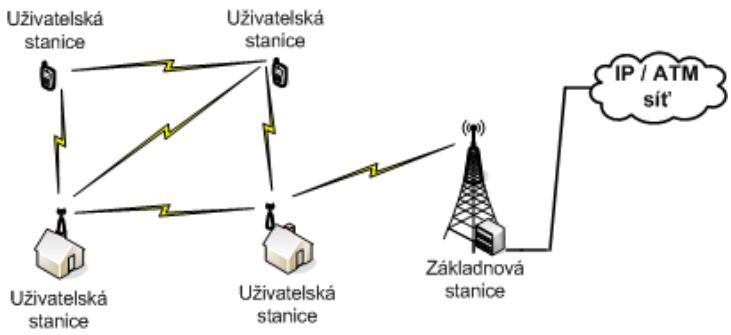
Jde o standard pro bezdrátový vysokorychlostní přenos dat zaměřený na relativně dlouhé vzdálenosti (venkovní sítě). Tato bezdrátová technologie nese označení *WiMAX*. Jedná se o doplněk k Wi-Fi, které je chápáno jako standard pro vnitřní sítě. Díky použití směrových antén a signálu o vyšším výkonu je dosah komunikace počítán v řádu desítek kilometrů při přímé viditelnosti (LOS - Line Of Sight) a několika kilometrů bez přímé viditelnosti (NLOS - Non Line Of Sight).

Jedná se o technologii určenou pro poskytovatele připojení k internetu a proto klade větší důraz na podporu kvality služeb QoS (Quality of Service), rychlost, velký dosah a možnost řízení a správy sítě. Z tohoto důvodu se využívají především licencovaná (placená) frekvenční pásma.

3.1 Struktura sítě



a) PMP (Point to MultiPoint)



b) MESH

PMP struktura je založena na klasické buňkové topologii sítě, kdy se jednotlivé uživatelské stanice připojují přímo k základnové stanici. U MESH topologie v porovnání s PMP je umožněna i přímá komunikace mezi stanicemi.

3.2 Specifikace WiMAX

IEEE 802.16

- Specifikace navržena v roce 2001 pro kmitočty 10 – 66 GHz
- Nutná přímá viditelnost zařízení (LOS)

IEEE 802.16a

- Rozšíření o kmitočty 2 - 11 GHz
- Není nutná přímá viditelnost (NLOS)

IEEE 802.16e (Mobile WiMAX)

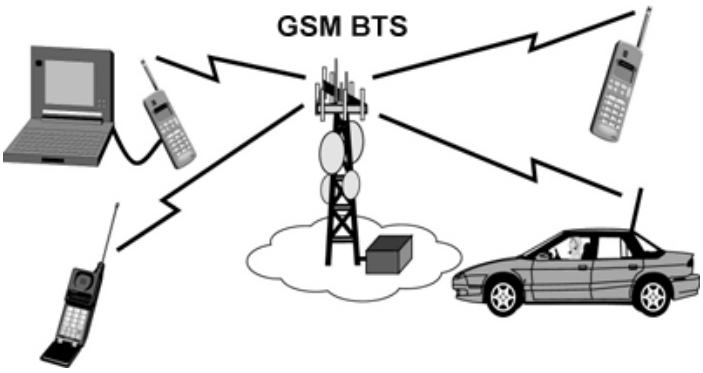
- Rozšíření o podporu mobilních, tedy pohybujících se zařízení
- Rozšíření o kmitočty 2 - 6 GHz

IEEE 802.16m

- Připravovaný standard, možnost komunikace mobilních zařízení
- Přenosové rychlosti 100 Mb/s až 1 Gb/s

4. Mobilní sítě (WWAN)

Využití veřejných mobilních sítí NMT (analogové mobilní sítě 1. generace), GSM (digitální mobilní sítě 2. generace) a UMTS (digitální mobilní sítě 3. generace), které jsou primárně určeny pro hlasovou komunikaci, také pro přenos dat a přístup k internetu.



Komunikaci prostřednictvím mobilních sítí zprostředkovávají mobilní telefony se zabudovaným modemem, popř. samostatné modemy, které se připojují k počítači (notebooku) přes USB rozhraní. Přenos dat v mobilní síti se uskutečňuje stejně jako hovory přes základnové vysílací stanice (BTS, Base Transceiver Station), které pokrývají celé území. Připojení k Internetu je tedy dostupné všude tam, kde je signál alespoň jednoho mobilního operátora.

Pro datové služby v rámci mobilních sítí bylo vytvořeno několik technologií:

a. GPRS (General Packet Radio Service) – technologie pro datové služby určená uživatelům GSM mobilních telefonů. Uživatelé platí za objem odeslaných a přijatých dat. U technologie GPRS není nikdy garantována rychlost spojení, protože GPRS jednoduše využívá volné místo (místo=slot) v síti GSM. Každý slot je dimenzován pro potřeby jednoho hlasového hovoru. V GSM síti mají přednost nejprve hovory a až poté požadavky GPRS přenosů.

b. EDGE – je rozšířením technologie GPRS (zpětně kompatibilní). Nabízí vyšší přenosové rychlosti

c. HSCSD (High Speed Circuit Switched Data) - Jde o technologii, která se snaží zrychlovat datové přenosy v mobilních sítích GSM tím, že pro přenos dat využívá více slotů najednou.

d. CDMA - umožňuje současnou komunikaci více uživatelů v rámci jednoho frekvenčního pásma. Využívá frekvenční pásmo 450 MHz (v minulosti určeno pro analogové mobilní sítě NMT 1. generace). V ČR tuto technologii nabízí pouze společnost O2 Telefonica výhradně pro datové služby – připojení uživatelů k internetu.

Síťové protokoly

Jsou nedílnou součástí síťového hardware i software. Protokoly definují komunikační pravidla, jimiž se řídí přenos dat v rámci počítačové sítě. Pro správnou funkci sítě je nutné, aby všechny stanice používaly stejný síťový protokol. V současnosti existují tyto síťové protokoly:

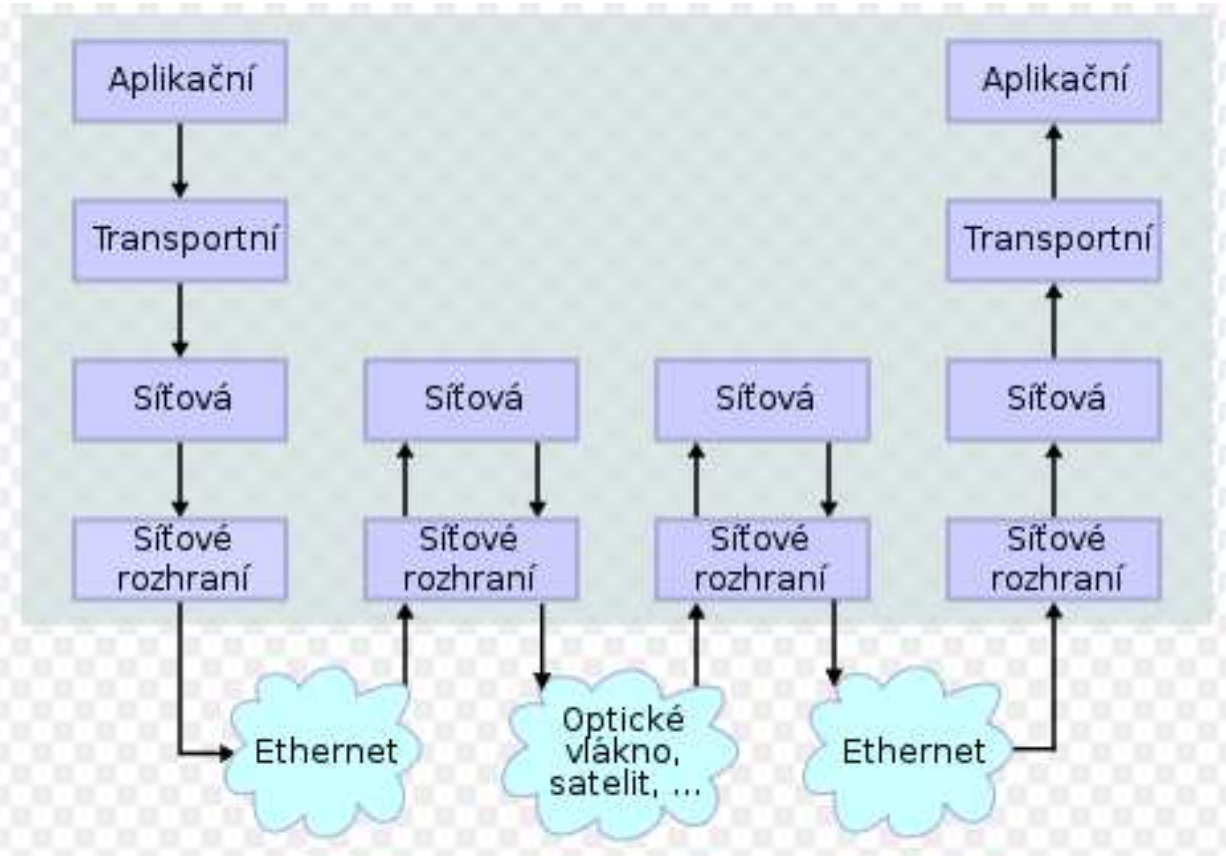
1. NetBEUI

NetBEUI (NetBIOS Extended User Interface) je starším protokolem vyvinutým firmou IBM. Protokol je od počátku vzniku určen především pro komunikaci v malých lokálních sítích, protože jeho způsob adresování nepodporuje směrování

Protokol byl ve své době velmi oblíben pro jeho vysokou přenosovou rychlost a jednoduchost konfigurace. Ta se skládala pouze ze zadání názvu připojené stanice a pracovní skupiny nebo domény jíž eventuálně náleží. Dnes se tento protokol v podstatě nevyužívá.

2. TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) sdružuje sadu protokolů pro komunikaci v počítačové síti. Model takovéto sítě se odlišuje od původního referenčního ISO/OSI modelu. Síťová komunikace je rozdělena pouze do 4 vrstev (ISO/OSI model definoval 7 vrstev):



2.1 IP protokol

IP (Internet Protocol) je základní protokol síťové vrstvy a celého Internetu. Provádí vysílání paketů na základě síťových IP adres obsažených v záhlaví paketu.

IP adresa jednoznačně identifikuje zařízení v síti využívající IP protokol. V současné době je nejrozšířenější verze IPv4, která používá 32 bitové adresy. Adresa je zapsaná jako čtveřice čísel 0 až 255 (každé číslo 8 bitů) oddělených tečkou, např.:

zápis pomocí dekadických čísel: *192 . 168 . 10 . 1*

zápis pomocí binárních čísel: *11000000 . 10101000 . 00001010 . 00000001*

Z důvodu nedostatku IP adres verze 4 je tento protokol postupně doplňován protokolem IPv6, který používá 128 bitové IP adresy. IPv6 adresa se obvykle zapisuje jako osm skupin, kdy každá skupina obsahuje čtyři hexadecimálních číslice, např.:

2001 : 0db8 : 85a3 : 08d3 : 1319 : 8a2e : 0370 : 7334

2.2 TCP protokol

Zatímco protokol IP zajišťuje přenos dat mezi libovolnými počítači v síti (např. lokální síť popřípadě internet), protokol TCP (Transmission Control Protocol) přenáší data mezi dvěma konkrétními aplikacemi běžícími na těchto počítačích. Na počítači uživatele běží více aplikací (programů), které komunikují se stejnou aplikací na jiném počítači. Např. emailový klient, ICQ klient, Skype, Internetový prohlížeč, atd. Aby bylo jednoznačné, které aplikaci je paket určen, mají jednotlivé aplikace přidělenou adresu v rámci TCP protokolu – tzv. číslo portu (číslo v rozmezí 0-65535). Podle čísla cílového portu operační systém pozná, které aplikaci má TCP protokol data doručit.

Analogie: Pokud použijeme přirovnání k běžnému poštovnímu styku:

IP adresa = adresa domu

Port = jméno konkrétního obyvatele domu

Příklady používaných portů:

Port 80: služba HTTP (přenos dat mezi webovým serverem a internetovým prohlížečem)

Port 25: služba SMTP (služba pro odesílání elektronické pošty)

Port 110: služba POP3 (služba pro příjem elektronické pošty)

Port 5190: komunikace prostřednictvím klientů sítě ICQ

TCP protokol je považován za tzv. spolehlivý (na rozdíl od IP protokolu), což znamená, že v případě přijetí poškozených dat se pokouší o nápravu, nejčastěji si vyžádá nový přenos poškozených dat.

2.3 UDP protokol

UDP (User Datagram Protocol) protokol je podobný protokolu TCP. Výrazně se liší především tím, že se jedná o protokol „nespolehlivý“ (nezatěžuje se potvrzováním přijatých dat), což je v jistých aplikacích s velkým objemem přenášených dat (např. streamování videa, poslouchání internetových rádií, apod.) jeho velká výhoda. V případě ztráty nějakého paketu například uživateli pouze blikne obrazovka, popřípadě na malý okamžik neslyší zvuk. Naopak, v případě přenosu elektronické pošty je vhodnější použít spolehlivého protokolu TCP.

2.4 Aplikační protokoly TCP/IP

TCP/IP sdružují velké množství protokolů, které byly vyvinuty pro různé aplikace. Jedná se např. o:

- HTTP (HyperText Transfer Protocol) - protokol pro komunikaci mezi webovými servery a jejich klienty (internetové prohlížeče)
- SMTP (Simple Mail Transfer Protocol) a POP3 (Post Office Protocol ver. 3) – protokoly umožňující komunikaci mezi poštovními servery a poštovními klienty (odesílání, příjem elektronické pošty).
- FTP (File Transfer Protocol) – protokol pro přenos souborů mezi počítači sítě. Předpokládá existenci FTP serverů a klientů. FTP server je aplikace běžící na počítači umožňující zabezpečený, řízený přístup do jeho systému souborů na dálku prostřednictvím aplikace FTP klienta.
- DHCP (Dynamic Host Configuration Protocol) – protokol se používá pro automatické přidělování IP adres prostřednictvím aktivních prvků sítě (např. přístupový bod) jednotlivým zařízením v počítačových sítích (počítače, PDA, tiskárny, IP telefony, apod.), čímž zjednodušuje jejich správu.
- DNS (Domain Name Server) – DNS protokol umožňuje překlad IP adresy (např. 77.75.72.3) na srozumitelnější doménové jméno počítače (www.seznam.cz), což je pro koncového uživatele přijatelnější označení koncového počítače, resp. serveru. Vyžaduje existenci tzv. DNS serveru, který sdružuje databázi IP adres a jim přidělených doménových jmen počítačů v síti.
- a další…

3. IPX/SPX

Síťový protokol vyvinutý firmou Xerox, který se používá v operačním systému Novell NetWare.

3.1 Protokol IPX (Internetwork Packet Exchange)

Síťový protokol používaný ke směrování paketů v síti. IPX pracuje podobně jako IP protokol a vyžaduje použití schématu adres, které rozlišují jednotlivé uzly sítě. Adresa IPX je zapsaná v hexadecimálním kódu a skládá ze dvou částí:

- Síťová adresa (32 bitů)
- MAC adresa síťové karty uzlu (48 bitů)

Příklad IPX adresy: BC-3D-15-A1 . 00-18-DE-C0-25-ED

Administrátor sítě definuje pouze síťovou část adresy. Směrování v této síti je velice přímočaré, protože IPX adresa již obsahuje fyzikou (MAC) adresu uzlu, na který paket směřuje.

3.2 Protokol SPX (Sequenced Packet Exchange)

Protokol, který je určen k řízení toku dat mezi komunikujícími aplikacemi v rámci sítě IPX. Je tedy podobný protokolu TCP. Protokol zabezpečuje výměnu paketů s potvrzováním příjmu a opakováním přenosu při jejich ztrátě nebo poškození. Protokol SPX je tedy spojově orientovaný - mezi uzly komunikujících aplikací je vytvořena spolehlivá potvrzovaná služba.