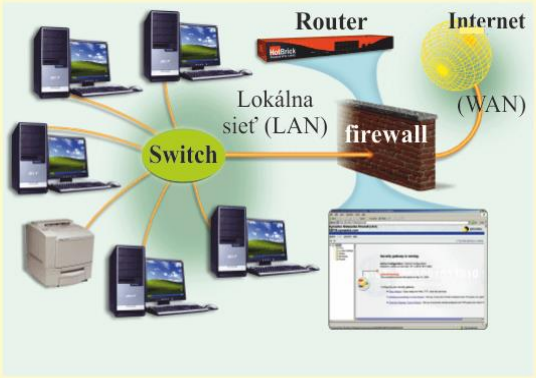
POČÍTAČOVÁ SIEŤ

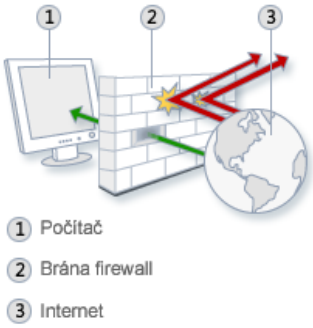
Počítačová sieť je súhrn: 1.technických prostriedkov (sieťové karty, switche, routre, konektory, káble, apod.), pomocou ktorých je realizované prepojenie a výmena dát medzi aspoň dvomi počítačmi ale aj inými zariadeniami v sieti (napr. router, server, tlačiareň), ktoré môžu navzájom komunikovať, zdieľať údaje, softvér ale aj hardvér a 2.softvérových prostriedkov (z OS a aplikácií schopných využívať prostriedky systému, určené k sieťovej komunikácii – napr. web prehliadač). Vzájomná komunikácia prebieha podľa sieťových protokolov (**protokoly TCP/IP** je súbor pravidiel, ktoré definujú formu, poradie odoslaných a prijatých správ medzi sieťovými prvkami a akcie pri posielaní, prenášaní a prijímaní správ; známe protokoly sú napr. HTTP – na prenos webových stránok, SMTP – na prenos e-mailových správ, FTP – na prenos súborov medzi počítačmi pripojenými na internet, DHCP – slúži na prideľovanie IP adries zariadeniam v sieti, DNS – slúži na preklad doménových mien na IP adresu a opačne, IMAP – slúži na nahrávanie, sťahovanie, vymazávanie e-mailových správ, ...).

Čo je to firewall ("protipožiarna stena") ?

Firewall (internetová brána) je softvér alebo hardvér, ktorý pomáha chrániť našu vnútornú sieť (počítač) pred hackerom alebo škodlivým softvérom (napr. červami) tým, že kontroluje informácie prichádzajúce z Internetu alebo zo siete a v závislosti od nastavenia brány firewall ich buď zablokuje, alebo im umožní vstup do počítača. Firewall je už súčasťou OS v našom počítači, ale často je už i súčasťou nášho routera.



Firewall slúži tiež na zamedzenie nevyžiadaného prijatia a odoslania dát z PC. Určuje, ktorá komunikácia je povolená a ktorá nie, a tým chráni ostatné zariadenia v našej sieti pred únikom dát alebo iným zneužitím. Firewall kontroluje tok dát, ktoré cez neho prechádzajú. Táto kontrola údajov prebieha na základe aplikovania **pravidiel**, ktoré určujú **podmienky** a **akcie**. Podmienky sa stanovujú pre údaje (napr. zdrojová, resp. cieľová IP adresa, zdrojový alebo cieľový port a rôzne iné). Úlohou firewallu je vyhodnotiť podmienky a ak je podmienka splnená, vykoná sa akcia napríklad povolenie alebo zamietnutie komunikácie. Napr. firewall je vhodný i na filtrovanie prístupu z rôznych IP adries, t.z. je možné zakázať prístup z jednej siete do druhej.



Význam a výhody počítačových sietí (všetky nasledovné výhody znamenajú úsporu finančných prostriedkov):

- komunikácia medzi počítačmi (napr. internet, e-maily, elektronický obchod, VOIP (voice over internet protocol) - telefonovanie cez internet, ftp-protokol na prenos súborov, chat („pokec"), zasielanie rôznych správ – sociálne siete (Facebook), atď.)
- prenos dát, výmena dát medzi stanicami (netreba ako v minulosti prenášať dáta osobne prostredníctvom diskiet a CD média) ale i prístup k informáciám cez internet
- zdieľanie dát viacerými stanicami – centralizovaná správa dát (napr. prepojenie bánk, poisťovní, cestovných kancelárií, železnice, letiská - predaj cestovných lístkov, zdieľanie fotiek, videí na serveri, atď.)
- zdieľanie hardvéru (napr. zdieľanie veľkého disku na serveri, alebo na pracovisku stačí mať napr. jednu sieťovú tlačiareň, plotter, atď.)
- zdieľanie softvéru – sieťové inštalácie, ktoré nemusia byť iba na miestnom serveri, ľahšia administrácia napr. vo firmách , školách a štátnych úradoch a taktiež zdieľanie pripojenia k internetu
- administrácia (správa) počítačov na diaľku (údržbu operačného systému, inštaláciu nových programov, zmenu konfigurácií a pod.), monitorovanie – riadenie výroby, sledovanie stavov na počítačoch na diaľku
- bezpečnosť uložených dát (dáta môžu byť v sieti uložené duplicitne), resp. zálohovanie dôležitých dát a ich následná obnova

Riziká a problémy (nevýhody) počítačových sietí

- **bezpečnosť** – a) každý počítač sa môže stať terčom útoku cudzieho narušiteľa - hackera, preto je potrebné venovať zvýšenú pozornosť bezpečnosti dát; b) možnosť infikovania svojho počítača malwarom (počítačovými vírusmi, červami, trojskými koňmi a pod.)

- **strata sociálnych kontaktov, strata cítenia, život mimo reality** - práca, platenie účtov, nakupovanie, komunikácia s priateľmi, kolegami, spolužiakmi cez internet - prakticky sa nemusíme so živým človekom vôbec stretnúť. To vedie k strate medziľudských kontaktov, k strate schopnosti komunikovať tvárou v tvár. Strácame cit, schopnosť empatie k človeku. Žijeme vo virtuálnom, neexistujúcom svete.
- **presýtenosť informáciami** - množstvo informácií, ktoré je schopný ľudský mozog prijímať, filtrovať a spracúvať je obmedzené. Pri surfovaní po internetových stránkach, pri četovaní sa k nám dostáva obrovské množstvo informácií. Spam, nevyžiadaná pošta, reklama, poplašné správy, pyramídové hry. To sú informácie, ktoré zbytočne zahlcujú náš mozog. Ich spracovanie, filtrácia nás oberá o čas a peniaze.
- **závislosť na Internete, sieti, službách Internetu, nových technológiách** - stále viac ľudí prepadáva závislosti na počítačoch, hrách, on-line komunikácií. Je to závislosť ako každá iná a predstavuje veľké riziko, ak sa neodhalí včas.
- **(ne)pravdivosť informácií** - nie vždy si dokážeme dostatočne overiť pravdivosť informácií, ktoré nájdeme na sieti. V podstate hocikto môže zverejniť nepravdivú informáciu.

Na vytvorenie spojenia sa používajú:

- metalické (kovové) káble - prenos el. signálu (najmä krútená dvojlinka zakončená konektormi RJ-45 alebo telefónna sieť, elektrická sieť) - **metalické spojenie**
- optické káble – prenos svetelného lúča - **optické spojenie**
- rádiové vlny, elektromagnetické vlnenie – prenos signálu **bezdrôtovým spojením** (napr. wi-fi, bluetooth, mobilné telekomunikačné siete, satelitné siete)

} prenosové média (fyzická cesta medzi vysielačom a prijímačom)

Každá z technológií má svoje presne určené možnosti nasadenia a použitia. Káblom sa prepájajú počítače v budovách, budovy sa prepájajú medzi sebou optickým káblom alebo vzduchom a telefónna linka prepája geograficky najvzdialenejšie počítače a objekty (príkladom použitia telefónnej linky je technológia ADSL).

Počítačová sieť sa skladá z aktívnych a pasívnych prvkov. Aktívne prvky sú napájané zo siete a aktívne nejakým spôsobom reagujú na signál, ktorý cez ne prechádza. Patrí medzi nich napríklad switch, router, sieťová karta a pod. Pasívne prvky sú súčasťou, ktoré sa na komunikácii podieľajú iba pasívne (tj. nevyžadujú napájanie, pasívne signál prenášajú bez jeho akejkoľvek modifikácie, alebo sledovania) – prepojovací kábel (napr. krútená dvojlinka, optický kábel, koaxiálny kábel sa už takmer nepoužíva), konektory.

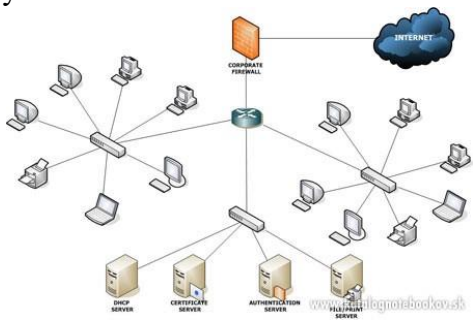
Delenie sieti podľa geografickej rozlohy:

- Osobné – PAN
- Lokálne – LAN
- Metropolitné - MAN
- Rozsiahle alebo globálne – WAN

PAN →

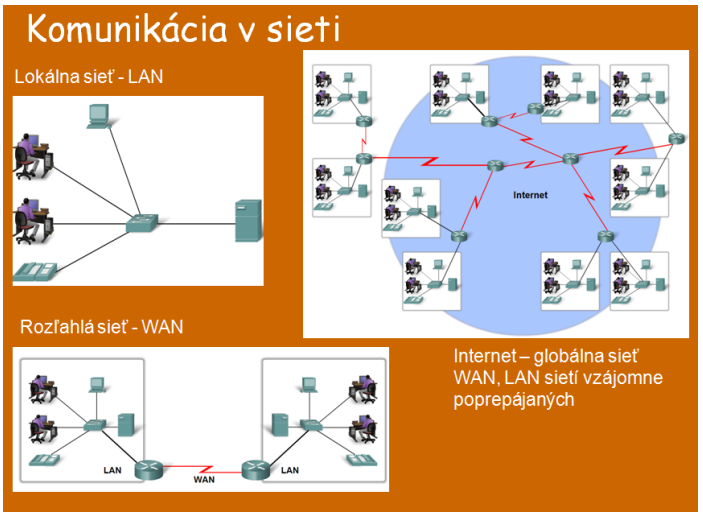
Osobná PAN sieť (personal area network) spája zariadenia rádovo v jednotkách metrov. Spolupracujúce zariadenia obvykle slúžia len jednej osobe (typicky prepojenie počítača s tlačiarňou, mobilom, PDA, notebookom ...). Na prepojenie zariadení v PAN sieti sa obvykle používajú väčšinou bezdrôtové technológie Bluetooth (skôr IrDA).

Lokálna sieť - Local Area Network, **LAN** - je to sieť v rámci jedného poschodia až budovy v rámci firmy, školy, ale i domácnosti, spájajúca hlavne počítače, tlačiarne a iné zariadenia. Súčasné LAN bývajú najčastejšie založené na technológii Ethernet - s prepojením metalickým alebo optickým káblom alebo bezdrôtovou technológiou Wi-Fi. Najrozšírenejšou používanou technológiou v LAN sieti je dnes Ethernet - vďaka jednoduchosti protokolu, cene a pomerne jednoduchej implementácii a inštalácii (najrozšírenejším druhom Ethernetovej kabeláže je krútená dvojlinka).



Metropolitné (mestské) siete - Metropolitan Area Network, **MAN** - tieto siete vznikajú prepájaním jednotlivých LAN sietí v rozsahu od niekoľko blokov budov až po celé mesto (rozsah v kilometroch). Prepojenie se deje taktiež väčšinou technológiou Ethernet, prevažne cez optický kábel alebo Wi-Fi.

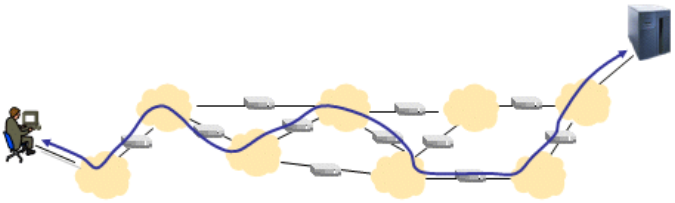
Globálne (resp. rozsiahle) siete - Wide Area Network, **WAN** - umožňujú komunikáciu medzi jednotlivými LAN a MAN sieťami, spravidla na vzdialenosť v stovkách kilometrov, resp. pokrývajú kontinenty, využívajú podmorské káble a družicové spoje.



WAN siete prostredníctvom routrov (smerovačov) prepájajú verejné telekomunikačné linky – fungujúcimi na technológii s prepojovaním okruhov (napr. siete ISDN, DSL, ...- digitálny prenos údajov po existujúcich metalických vedeniach) a a sieťami s prepojovaním paketov ako napr. Frame Relay, ATM (ešte sa používajú, ale kvôli rýchlosti sa od nich upúšťa) a technológiami ako napr.bezdrôtová WiMax (IEEE 802.16d). Najväčším a najznámejším príkladom siete WAN je sieť **Internet**.

Pri metóde prepojovania okruhov je najprv pomocou prepínačov vytvorená fyzická cesta (prepojený okruh) na prenos správy medzi odosielateľom a adresátom, až potom môže byť správa odoslaná. Po jej odoslaní je spojenie opäť zrušené, (napr. bežné telefónne siete, kde je komunikačný kanál neustále vyhradený pre jedného užívateľa a ten sa oň s nikým nedelí. Vyhradenie prenosového kanála je zrušené až v okamžiku ukončenia hovoru a až potom môže byť kanál použitý pre ďalšieho užívateľa – čiže nevýhodou je neefektívne využitie prenosového média, výhodou je zase garantovanie kvality a prenosovej rýchlosti – vhodné najmä napr. pre videokonferencie.

Metóda prepojovania paketov - Princíp prenosu dát v počítačových sieťach je založený na tzv. **paketovom prenose** (každá správa sa rozdelí na drobné časti - balíčky dát (aj dáta na Internete sa prenášajú paketami). V jednotlivých spojovacích uzloch (switche, resp. routre) sa stále hľadá najvhodnejšia cesta putovania paketov. V okamihu odoslania paketu zdrojovým uzlom k cieľovému uzlu nie je známa jeho presná cesta sieťou. Každý paket v rámci danej komunikácie teda putuje nezávisle, teoreticky rôznou cestou – podľa topológie siete, jej priechodnosti a výpadkom na trase. Všetky tieto záležitosti ovplyvňujú voľbu jeho ďalšej cesty v sieťových uzloch (hlavne routroch), ktoré musia dynamicky reagovať na každú zmenu. Musia zisťovať aktuálny stav spojov vo svojom okolí a podľa toho budovať a upravovať svoje smerovacie tabuľky (databáza IP adries okolitých uzlov), aby čo najlepšie odpovedali v každom okamihu aktuálnej situácii v sieti.



Pakety sú malé fragmenty dát (32-bitové postupnosti slov), majú svoju štruktúru, obsahujú hlavičku, adresy odosielateľa a prijímateľa, kontrolný súčet hlavičky (ochrana pred chybami pri prenose) a dáta

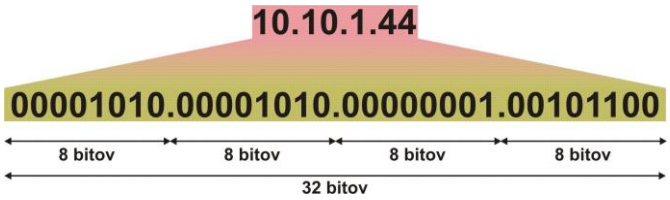
Štruktúra IP paketu:

4b	4b	8b	16b
Verzia	Dĺž hlavič	Typ služby	Dĺžka IP paketu (max. 65535 B)
Identifikácia		Flags	Fragment offset
TTL	Číslo protokolu	Kontrolný súčet hlavičky	
Zdrojová IP adresa			
Cieľová IP adresa			
Options			
Dáta ...			

rozsah 32 bitov

Pri prezeraní web stránky sú dáta prenášané vo viacerých paketoch, ktoré môžu prichádzať v rôznom poradí a môžu mať rozličné cesty, na konci svojej cesty sa však opäť zoradia podľa poradia. Protokol, ktorým sa celý tento proces riadi, sa nazýva **TCP/IP** (transmission control protocol/Internet protocol) je sada (približne 100) protokolov vyvinutá pre Internet (v roku 1970) na prenos dát medzi počítačovými sieťami.

Aby sa pakety mohli dostať k presne určenému počítaču, každý počítač v sieti má svoju unikátnu adresu. Nazýva sa **IP adresa.** a je zložená zo štvorice čísel oddelených bodkou (spolu ide o 32 bitové číslo). Tieto štvorice čísel môžu nadobúdať hodnoty od 0 – 255, napr.:



V počítačovej sieti ľubovoľného typu sa **nemôžu** vyskytovať **dva počítače s rovnakou IP adresou**.
Pomocou súčasnej verzie IPv4 s 32 bitovými adresami možno zaadresovať 2^{32}=cca 4 miliardy rôznych IP adries zariadení a tento počet dnes už pomaly nepostačuje, (pre porovnanie na zemi žije viac ako 6 miliárd ľudí). Preto je pripravená nová verzia IPv6 so 128 bitovými adresami, ktorá rieši nedostatok unikátnych sieťových adries v IPv4 a rieši tiež niektoré bezpečnostné a výkonnostné problémy (hierarchické smerovanie). Tvar IPv6: **0000:0000:0000:0000:0000:0000:9EC5:24A5**
IP adresa je presnejšie logický číselný identifikátor fyzického sieťového rozhrania (napr. sieťovej karty) daného uzla (počítača alebo routra) v sieti. Uzol môže mať aj viac IP adries, podľa toho koľko má sieťových rozhraní.

Doménové mená

Ak si chceme zobraziť nejakú internetovú stránku, potrebujeme sa spojiť s počítačom – serverom, na ktorom je uložená. Pamätanie si IP adresy je však pre človeka ľahko mýliteľné a nepohodlné, preto sa adresa nahradzuje doménovým menom, (to sa ešte delí na *názov počítača. doména).*

Doménové meno	**IP adresa**
.markiza.sk	85.248.10.2
.azet.sk	213.215.107.244

Preklad medzi IP adresami a doménovými menami zabezpečujú **DNS servery** (Domain Name System). Tie obsahujú rozsiahlu tabuľku, v ktorej sa nachádza zoznam IP adries s prislúchajúcimi doménovými menami. IP adresa a maska sa dajú nastaviť manuálne cez príslušné konfiguračné nastavenia v operačnom systéme.

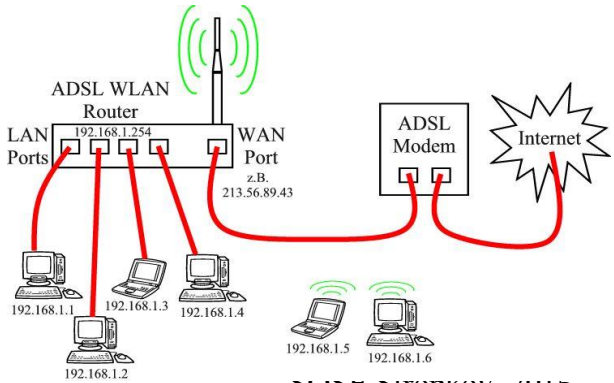
Verejné a neverejné (privátne-súkromné) IP adresy

Verejné IP adresy sú jedinečné na svete (ináč smerovač by nevedel kam má smerovať dáta). Pod takouto adresou sa javíme okolitému svetu. Aby nenastali duplicity, IP adresy prideľuje jedna organizácia v každom štáte (SK-NIC na Slovensku).
Neverejné IP adresy sú IP adresy používané vo vnútorných LAN sieťach (aj doma) a používajú sa adresy z nasledovných dohodnutých intervalov:

Privátne IP adresy

trieda A	10.0.0.0 - 10.255.255.255
trieda B	172.16.0.0 - 172.31.255.255
trieda C	192.168.0.0 - 192.168.255.255

Napr. IP adresa jedného z našich počítačov doma môže byť 192.168.1.4, ale pritom musí byť tiež jedinečná v našej LAN sieti. Avšak Takúto IP adresu môžu mať aj počítače v iných súkromných LAN sieťach. Tieto neverejné IP adresy však nie sú viditeľné zvonku na Internete. Takto sa čiastočne rieši nedostatok IPv4 adries, ktorých počet sa blíži k 4 miliardám (čo je max. v IPv4).
Avšak ak chceme, aby počítače v našej LAN sieti so svojimi neverejnými IP adresami boli pripojené na internet, tak sa pripoja najčastejšie cez router k jeho LAN portom (pozri obr.) a cez jeho WAN port, ktorý má svoju verejnú IP adresu, napr. 213.56.89.43 smerujú dáta na Internet. Preto smerovač vykonáva funkciu - **NAT** (Network Address Translation) - preklad neverejných IP adries na verejné a opačne.



Výhody verejných IP adries oproti neverejným: 1.) zariadenie je dostupné priamo z Internetu, môže teda pracovať ako server (web server, mail server a pod.); 2.)niektoré programy (napr. niektoré hry) dokážu korektne pracovať len ak má počítač verejnú IP adresu, ale aj priama komunikácia medzi programami (napr. prenos súborov - FTP). Nevýhody: 1.)

zariadenie je dostupné priamo z Internetu, môže teda byť ľahšie napadnuté škodlivým programom, zahltené a pod. čo znamená vyššie nároky na zabezpečenie takéhoto zariadenia (počítača); 2.) vyššia cena za pripojenie, vďaka obmedzenému počtu verejných IP adries; 3.) určitá strata anonymity
IP adresy sa v počítačoch môžu prideľovať ručne (napr. administrátorom príslušnej siete) alebo sú pridelené automaticky. Tento druhý spôsob je už väčšinou implicitne nastavený v operačnom systéme.

Najskôr je však potrebné mať pripojený router (smerovač) k internetu a ten aj nakonfigurovať - router sa spravidla konfiguruje cez webové rozhranie – pozrieť v manuáli daného routera (okrem prístupového mena a hesla je potrebné zadať aj napr. spôsob zabezpečenia) a v OS Windows softvérovo zapnúť **DHCP server** pre automatické pridelenie IP adries pre všetky pripojené počítače v lokálnej sieti. **Ako ?** - Otvoriť vlastnosti protokolu TCP/IP v nastavení sieťovej karty, nasledovne: – *„Štart“* > *„Ovládacie panely“* > *„Sieťové pripojenia“* > po kliknutí na ikonu pravým tlačidlom myši vybrať *„Vlastnosti“* a vybrať *„Internet Protokol (TCP/IP)“* a kliknúť na *„Vlastnosti“*. V otvorenom okne zvoliť *„získať adresu IP zo serveru DHCP automaticky“*, taktiež pri nastavení DNS zvoliť *„získať adresu serveru DNS automaticky“*.

DHCP (angl. Dynamic Host Configuration Protocol – môže byť súčasťou aj routra) ponúka možnosť nastaviť si nielen IP adresu, ale aj masku siete, adresu predvolenej brány a a adresy používaných DNS serverov dynamicky, bez nutnosti manuálneho nastavovania. DHCP je veľmi obľúbený protokol najmä súvislosti s masovým rozšírením notebookov, ktoré sa bežne pripájajú do rôznych sietí (doma, v škole, v práci, v kaviarni, na stanici, …) a všade sa nastavia IP adresy dynamicky, bez potreby ručného nastavovania. „DHCP pôžička“ sa dá chápať ako dohoda medzi serverom a klientom, ktorá platí obmedzený čas. Napr. pri každom vypnutí a zapnutí nášho routera (resp. modemu), alebo pri každom reštarte DHCP serverov na strane nášho poskytovateľa internet. služby **ISP** (Internet Service Provider, napr.T-com), **nám bude pridelená zakaždým iná vonkajšia IP adresa,** (je ju možné zistiť viacerými spôsobmi, napr. aj na web-stránke: ***http://whatismyip.com***).

Zjednodušene: **DNS** je systém pre preklad doménových mien na IP adresy a opačne.
DHCP je protokol pre automatické prideľovanie IP adries jednotlivým osobným počítačom.

Každá sieťová IP adresa obsahuje dve časti – predčíslie (adresu) siete a číslo uzla (počítača, routra). Veľkosť predčíslia siete v IP adrese je premenlivá a je určované **maskou siete** (napr. často je: 255.255.255.0). Predčíslie siete má veľký význam pri smerovaní paketov prostredníctvom routrov – pretože cieľ prenosu paketov sa najprv smeruje práve podľa adresy (predčíslia) siete.

Postup výpočtu:

Napr. IP adresa:	200. 5.189.68	11001000.00000101.10111101.01000100
AND Sieťová maska:	255.255.255. 0	AND 11111111.11111111.11111111.00000000
Výsledná adresa siete:	**200. 5.189. 0**	11001000.00000101.10111101.00000000

MAC adresa (Media Access Control) – je fyzická adresa je vypálená do čipu ROM na sieťovej karte počítača. Je to šesť bajtové číslo, pričom prvé tri bajty identifikujú výrobcu sieťovej karty a u sieťových kariet od toho istého výrobcu môžu byť tie 3 bajty zhodné, na rozdiel od ďalších troch bajtov, ktoré musia byť jedinečné (pozri na obr.). T. z. každá sieťová karta vo svete má jedinečnú MAC adresu. Táto adresa je nemenná a identifikuje počítač v sieti. Zobrazuje sa v šestnástkovej číselnej sústave a zodpovedá napr. rodnému číslu človeka - ktoré sa počas jeho života nemení. IP adresa zodpovedá logickej adrese zariadenia, napr. v reálnom živote poštovej adrese určitého človeka. MAC adresa je na rozdiel od IP adresy prenositeľná, t.z. sieťovú kartu je možné presunúť z jednej siete do druhej.

Postup pre zistenie MAC adresy je jednoduchý - otvoríte príkazový riadok (*„Štart“* > *„Spustiť“*, do poľa napíšte: ***cmd*** a stlačte *„OK“*). Do príkazového riadku napíšte príkaz: ***IPconfig /all*** a na obrazovke sa vypíšu

vlastnosti všetkých sieťových adaptérov v počítači aj IP adresa vášho počítača. Vašu MAC adresu nájdete v riadku *Fyzická adresa* = MAC adresa (pozri obr.).

FTP – **F**ile **T**ransfer **P**rotocol (protokol prenosu súboru). Táto služba umožňuje zdieľanie a prenos súborov cez Internet ale aj po lokálnej sieti. Je typu klient – server. Ako úložný priestor slúži jeden hlavný počítač – ftp server a jednotliví klienti sa k nemu pripájajú napr. aj cez Total Commander → Sieť → FTP Spojenie zadaním IP adresy servera alebo FTP adresy v tvare: ftp.meno_servera.pripona, napr. ftp.szm.sk. Pripojenie je možné zabezpečiť prístupovým menom a heslom.

Delenie sieti podľa typov pripojených počítačov (ako a kým sú zdieľané zdroje spravované):

a) Klient - Klient (alebo **peer to peer** - rovný s rovným) všetky prepojené počítače **(klienti)**, sú medzi sebou navzájom rovnocenné. To znamená, že si medzi sebou môžu ľubovoľne vymieňať informácie, sledovať prevádzku po celej sieti a byť navzájom nezávislé. Typ siete peer to peer nachádza uplatnenie predovšetkým v prevádzke malých sietí do cca 10 počítačov napr. v našej školskej učebni, v malej firme, domácnosti a pod. Každý počítač chvíľu môže slúžiť ako server (v okamihu keď poskytuje súbor) a chvíľu ako klient (keď sťahuje súbor). Pre sieť P2P nepotrebujeme mať žiadny špeciálny software – stačí operačný systém Windows..

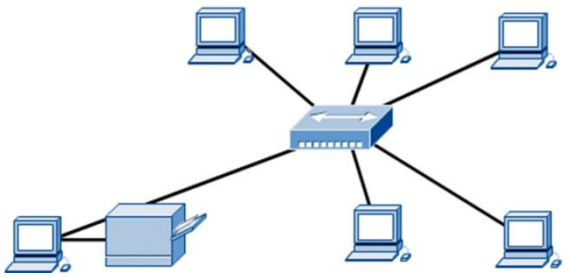


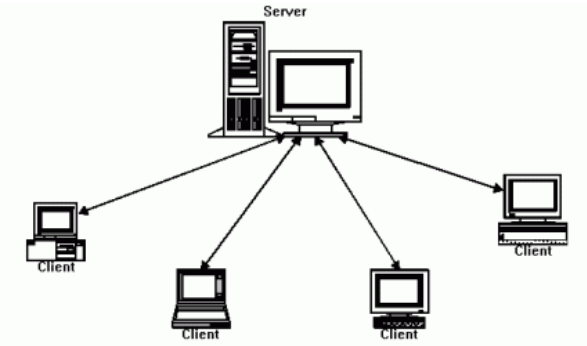
Schéma zapojenia siete - topológia "hviezda" uprostred je "prepínač" (switch)

Výhody počítačovej siete peer to peer:

1. je relatívne lacná, nie je nutné kupovať náročný hardvér pre server; potrebný softvér je súčasťou operačného systému; 2.počítače sa ľahko konfigurujú; 3. počítače nie sú závislé od centrálneho počítača, t. z., že môžu pracovať nezávisle od ostatných počítačov v sieti

Nevýhody: nie sú vhodné pre siete väčšieho rozsahu a pre väčší počet užívateľov, neposkytujú žiadne centralizované zabezpečenie, neumožňujú centrálne zálohovanie dát, užívatelia si sami riadia prístup ku zdrojom a prostriedkom

Klient - Server - tento spôsob je založený na existencii výkonného počítača - **servera**, ktorý poskytuje služby, sprístupňuje svoje zdroje (dáta, softvér, pripojené zariadenia) ostatným počítačom - **klientom** v sieti. Klient - pracovná stanica (napr. aj PC) s relatívne menším výkonom, posiela žiadosti na služby, musí byť autorizovaný na serveri (meno, heslo). Staníc môže byť niekoľko desiatok aj stoviek a v súčasnosti je tento typ siete rozšírený aj vo firmách. Práve na architektúre klient - server je postavená aj štruktúra Internetu. Svet obopína sieť hlavných serverov, ktoré sú medzi sebou prepojené najrýchlejšími optickými spojmi a vytvárajú tzv. **chrbticovú sieť**. K tejto sieti sa pripájajú ďalšie a ďalšie menšie servery, a celý tento proces pripájania končí u koncového používateľa na jeho domácom alebo kancelárskom počítači.



Výhody siete klient/server:
užívatelia používajú k prístupu k sieťovým zdrojom jedno používateľské meno a heslo, jednoduchá možnosť centralizovaného zálohovania dát, servery s vysokým výkonom umožňujú užívateľom rýchlejší prístup k zdrojom, poskytujú možnosť vyššej bezpečnosti

Nevýhody siete klient/server:
vysoké náklady spojené s hardvérom a sieťovým operačným systémom, vyžaduje správcu (administrátora) siete, v prípade výpadku servera nefunguje prístup k sieťovým zdrojom

Typy serverov:

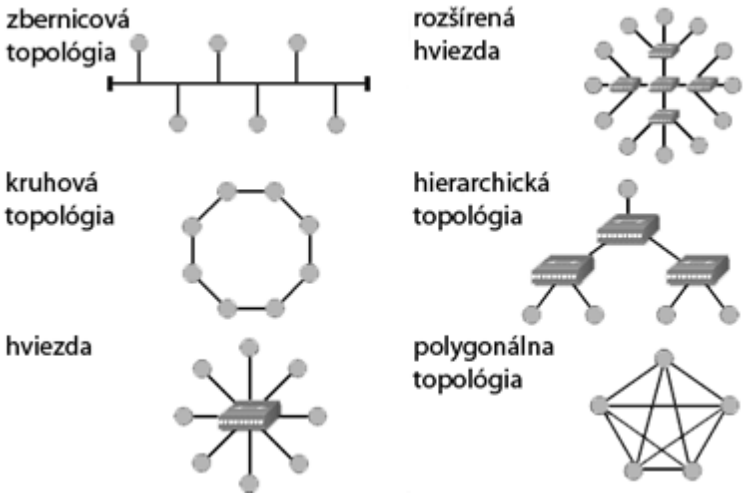
- Webový Server – poskytuje nám webové stránky stránky (WWW/World Wide Web)
- Databázový Server – poskytuje nám v podstate úložisko/miesto kde si môžeme uložiť svoje súbory dokumenty a pod.

- DNS Server – DNS Server prekladá odkaz (www.niečo.niečo) do IP adresy.
- *DHCP* server - automaticky konfiguruje TCP/IP protokol na pracovných staniciach, čím je zabezpečené pridelenie jedinečných IP adries počítačov v sieti
- Mail Server – služba e-mailu (e-mail/enthernetová pošta) pomocou.
- Proxy Server – v podstate nám riadi prístup do inej siete.
- Tlačiarensky Server – umožňuje tlačiť dokumenty počítačom/počítaču.
- Herný Server – umožňuje hráčom hrať multiplayer (hráč+hráč).

Delenie sieti podľa topológie (vzájomného usporiadania zariadení v sieti - rozloženie káblov alebo iného média)

Sieť môže byť prepojená priamo z počítača do počítača, alebo s využitím týchto aktívnych prvkov.

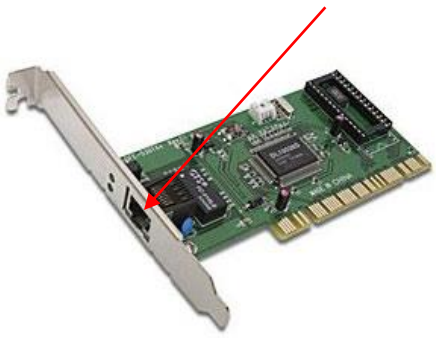
- Zbernicová topológia siete - Táto topológia sa používa v sieťach s koaxiálnym káblom. Prenosové médium je spoločné, dáta sa šíria ku všetkým staniciam. Výhodou je to, že kábel vedie od stanice k stanici, s čím súvisí pomerne malá spotreba kábla a nízka cena kabeláže. Nevýhodou je nespoľahlivosť topológie. Akékoľvek prerušenie zbernice znamená haváriu celej siete - prerušenie komunikácie medzi všetkými stanicami. Problémom je tiež obtiažná lokalizácia poruchy.
- Hviezdicová topológia siete - Každá stanica je pripojená vlastným káblom k centrálnemu bodu siete. Prenosovým médiom je krútená dvojlinka (UTP alebo STP). Výhodou je nízka náchylnosť k chybe. Porucha jedného kábla vyradí z činnosti len jednu sieťovú stanicu. Lokalizácia poruchy je podstatne jednoduchšia ako pri zbernicovej topológii. Nevýhodou je vyššia spotreba káblov a nutnosť použiť switch (prepínač). Topológia hviezda je najpoužívanejšou metódou prepojenia v sieťach LAN.
- Kruhová topológia siete - Počítače sú spojené navzájom do kruhu, dáta sa pohybujú medzi stanicami v jednom definovanom smere. Výhodou je predpovedateľnosť oneskorení v sieti a lepšia priepustnosť pri veľkom počte staníc. Nevýhodou je to, že pri malej záťaži je táto sieť spravidla menej výkonná než iná topológia a je tiež citlivá na prerušenie kábla.

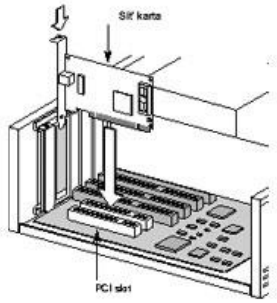


Základné sieťové prvky: A) aktívne (sú napájané zo siete a aktívne nejakým spôsobom reagujú na signál, ktorý cez ne prechádza, napr. sieťová karta, modem, switch, router, ...)

Sieťová karta je počítačový hardvér, ktorý zabezpečuje komunikáciu počítača s ďalšími zariadeniami v počítačovej sieti. Do sieťového média (napr. kábla) vysiela údaje podľa príkazov procesora alebo zo sieťového média prijíma správy určené pre ňu a odovzdáva ich procesoru na spracovanie.

Integrovaná sieťová karta je dnes bežnou súčasťou základnej dosky. Konektor RJ-45 siete **Ethernet**, sa najčastejšie nachádza na zadnom paneli základnej dosky. **Ethernet** je sieťová technológia umožňujúca prenos signálov medzi počítačmi LAN siete, ktorá je nezávislá na architektúre sieti (klient/server alebo peer-to-peer), či použitom operačnom systéme (Novell, Windows, Unix...) a má jednoduchý protokol i samotnú inštaláciu



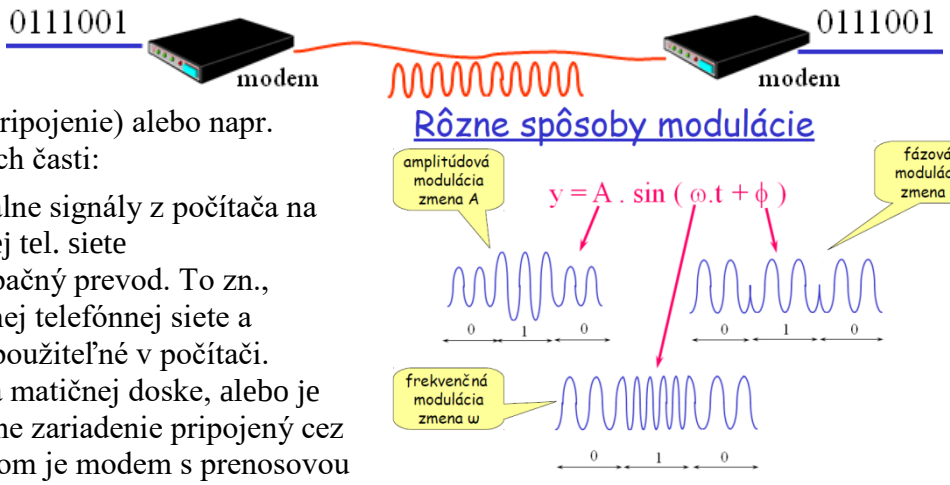


Pokiaľ na vašej základnej doske sieťová karta predsa len chýba, je ju možné dokúpiť ako externú sieťovú karu za cca 6 €. Karta sa zasunie do PCI alebo PCIe slotu a po naštartovaní počítača by ju mal operačný systém detekovať a nainštalovať. Sieťové karty pracujú na 2.linkovej vrstve OSI modelu

Windows XP pozná väčšinu sieťových kariet, a tak by si ju mal sám automaticky nainštalovať - pokiaľ sa tak nestane, použijete ovládač dodávaný v balení na CD. Sieťové karty pracujú na rýchlosti 10/100Mbps a dnes už aj

1Gbit (pre domáce použitie však stačí 100Mbps sieť). Každá sieťová karta má vo svojej pamäti uloženú jedinečnú 48-bitovú MAC adresu (fyzickú), napr. 00-11-09-95-26-FE, ktorú možno zistiť ak v príkazovom riadku v danom počítači zadáme príkaz „ipconfig /all“.

Modem (**mo**dulátor a **dem**odulátor) - slúži na premenu digitálneho signálu počítača na analógový signál, vhodný na prenos po telefónnej linke a na opačný proces pri príjmu signálu na druhej strane linky - premenu analógového signálu na digitálny.



Je niekoľko druhov modemov ako napr. dial-up (vytáčané pripojenie cez telefon), ADSL (širokopásmové pripojenie) alebo napr. ISDN. Každý modem sa skladá z dvoch časti:

- MOdulátor - ktorý prevádza digitálne signály z počítača na analógové a vysiela ich do verejnej tel. siete
- DEModulátor - ktorý vykonáva opačný prevod. To zn., prijíma analógové signály z verejnej telefónnej siete a prevádza ich na digitálne signály použiteľné v počítači.

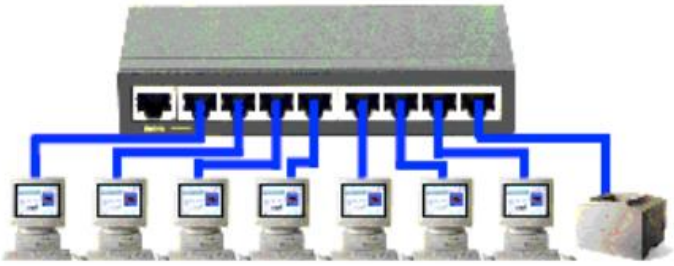
Modem je buď integrovaný priamo na matičnej doske, alebo je ako rozšírujúca karta, alebo ako extérne zariadenie pripojený cez COM alebo USB k počítaču.Štandardom je modem s prenosovou rýchlosťou 56 kb/s

interný modem

externý USB

Opakovač (**Repeater**) je aktívne sieťové zariadenie, ktorého úlohou je zosilniť a zregenerovať signál. Používa sa na zväčšenie vzdialenosti medzi dvoma sieťovými zariadeniami. Pokiaľ je vzdialenosť medzi miestami, ktoré chceme prepájať väčšia ako maximálny dosah média, dochádza k *degradácii signálu.* Degradácia znamená, že v istom bode nie sme schopný rozlíšiť, či prenášaný signál reprezentuje logickú nulu alebo logickú jednotku. Pri koaxiálnej kabeláži musíme opakovač použiť približne po 185 metroch, pri TP kabeláži po 100 metroch Opakovač pracuje 1.fyzickej vrstve OSI modelu.

Prepínač (angl. **switch**) je aktívny prvok v lokálnej (LAN) počítačovej siete, ktorý spája jej jednotlivé časti (počítače, tlačiareň). Prepínač slúži ako centrálny prvok v sieťach hviezdicovej topológie.

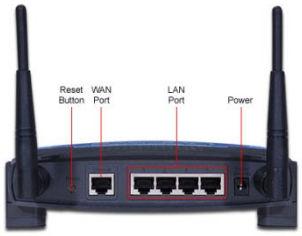


Meno prepínač je odvodené od intuitívnej predstavy, že pri prenose dát (rámcov) prepínačom sa dočasne prepojí vstupný port s výstupným, a že na prepínači teda dochádza k prepínaniu vstupných a výstupných portov. Prepínač v skutočnosti pracuje na princípe uloženia rámcov vo vyrovnávacej pamäti, určení výstupného portu a odoslaní príslušných rámcov výstupným portom. Prepínač si vedie *tabuľku* svojich portov a MAC adries jednotlivých pripojených staníc. Túto tabuľku si prepínač vytvára z prijatých rámcov a používa ju na doručovanie rámcov k ich príjemcom. Keď niektorým portom vojde rámec, prepínač z tohto rámca prečíta MAC adresu odosielateľa a zaznačí si ju do tabuľky k portu, ktorým rámec vošiel. Týmto spôsobom sa prepínač *učí*, aké adresy majú stanice na jednotlivých jeho portoch.

Ďalej prepínač z rámca prečíta MAC adresu príjemcu a pokúsi sa v tabuľke nájsť port, na ktorom je príjemca pripojený. Ak sa prepínaču podarí vo svojej tabuľke taký port nájsť, odošle rámec von iba týmto portom, inak

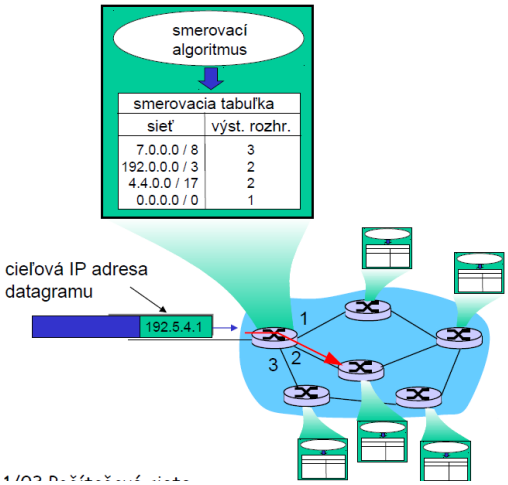
rozpošle rámec na všetky porty okrem toho, ktorým rámec vošiel. Prepínače pracujú na 2.linkovej vrstve OSI modelu.
V minulosti sa ako centrálny prvok v týchto sieťach používal **rozbočovač** (angl. **hub**). Ten pracuje na 1.fyzickej vrstve OSI modelu.

Prepínače sú v porovnaní s rozbočovačom inteligentnejšie, podľa MAC adresy dokážu rozpoznať, kam majú byť dáta doručené a tak prepínač dáta nepreposiela na všetky porty súčasne. Vďaka tomu dokáže prepínač radikálne znížiť tok zbytočných dát na sieti a je omnoho efektívnejší ako rozbočovače. Ďalší veľký rozdiel je, že switch v prípade kolízie v časti počítačovej siete (t.z. dva počítače začnú v jednom okamžiku vysielať dáta → výsledkom potom bude znehodnotený signál) nezablokuje celú sieť všetkých počítačov pripojených na switch (ako by sa stalo v prípade hubu), ale len v daných 2 portoch (vstupov), t.z. switch delí „kolíznu doménu“.

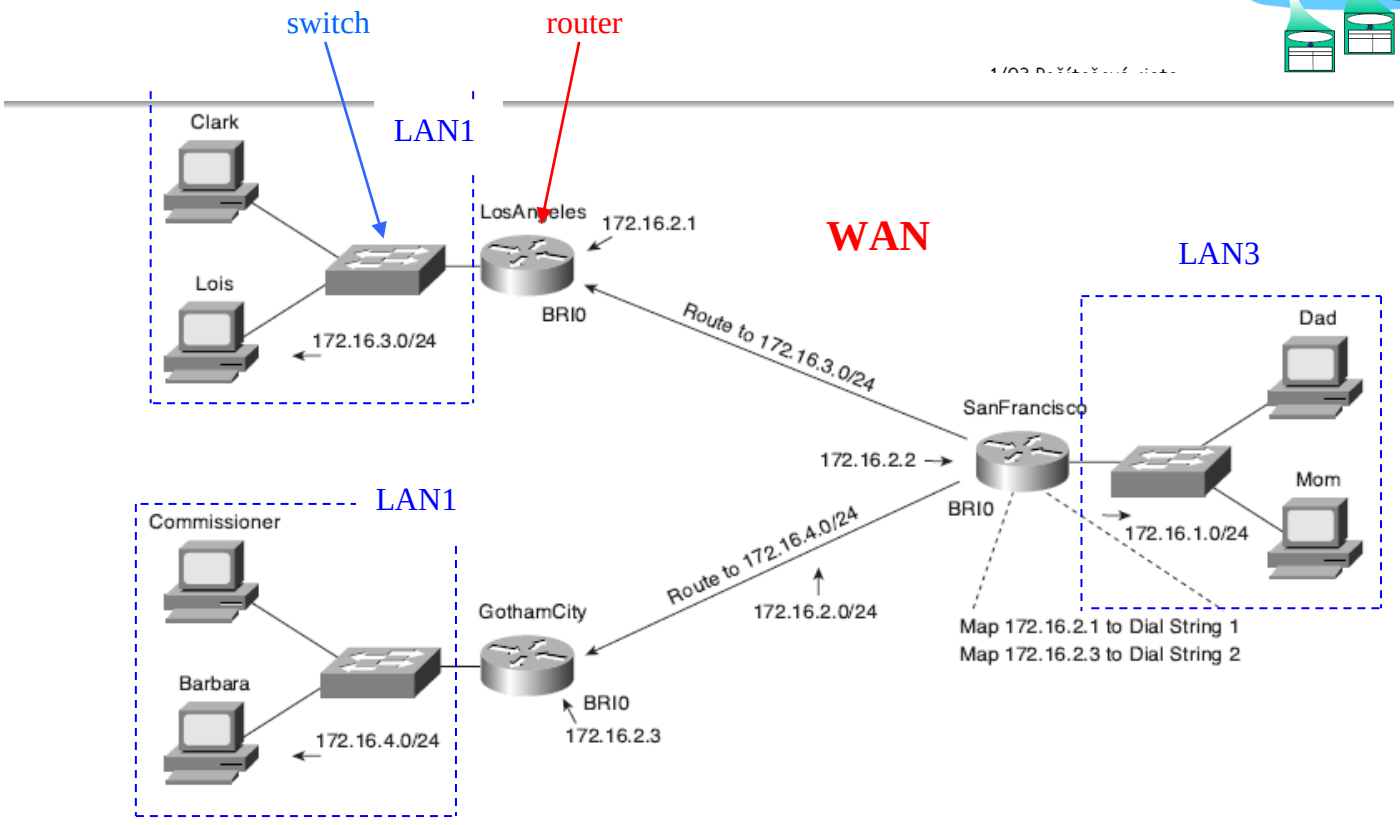


Smerovač (Router) – sa väčšinou používa pre spojenie lokálnej siete (LAN) s vonkajšou (WAN) – najčastejšie s Internetom, tým sa líši od switcha, ktorý spája iba počítače v LAN sieti. Jeho hlavnou úlohou je smerovať dáta v Internete a lokálnych sieťach. Jednotlivé dáta (pakety) smeruje na základe analýzy ich hlavičiek (napr. cieľovej IP adresy, poradového čísla paketu, atď.) a prepúšťa k ďalšiemu smerovaču postupne až ku cieľovému počítaču, ale iba tie, ktoré sú tam určené. Ak existuje viacero možných tras, dokáže vybrať momentálne najvýhodnejšiu trasu.

Router musí byť po štarte nakonfigurovaný, musia sa mu zadať adresy jeho sieťových rozhraní. Adresy ďalších sieti získava zo siete snímaním routovacích (smerovacích) tabuliek okolitých routrov s ktorými komunikuje pomocou smerovacieho protokolu. Internetové routere sú v dnešnej dobe často kombinovane s DSL modemami alebo WiFi prístupovými bodmi (AP- Access Point). Dnes je veľa routerov určených pre pripojenie do internetu vybavených navyše switchom (4-8 portovým), serverom pre „prekladanie sieťových adries“ (NAT), DHCP serverom, DNS proxy serverom, či hardvérovým firewallom.



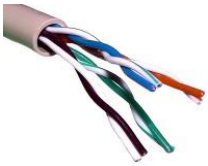
Smerovače pracujú na 3.sieťovej vrstve OSI modelu.



Gateway alebo **brána** je špeciálne zariadenie, ktoré sa používa k spájaniu dvoch sietí používajúcich rôzne komunikačné protokoly. Gateway môže vykonávať aj funkciu routera, ale navyše vykonáva transformáciu

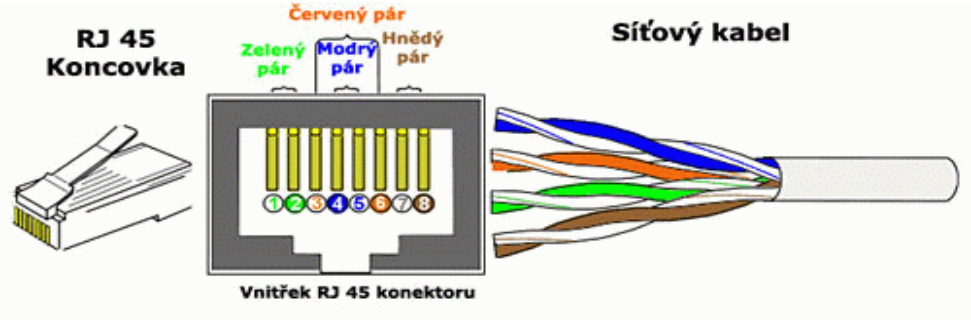
protokolov spájaných sieti ako po stránke programovej, tak aj technickej. Týmto sa najviac líši od routera, ktorý nedokáže transformovať protokoly. Router vyrovnáva len rôznu topológiu v spájaných sieťach a zabezpečuje smerovanie sprav. Brána napríklad príjme z mobilnej GSM siete SMS správu a odošle ju do internetu ako e-mail.

B) pasívne (signály iba nimi pasívne prechádzajú, napr. káble, konektory) - Existujú 4 najpoužívanejšie typy káblov: koaxiálny (používali sa dávnejšie), UTP (unshielded twisted pair - netienený kábel s vodičmi, ktoré majú štruktúru krútených párov – najviac používané), STP (shielded twisted pair – každý pár má tienenie) a optické káble. Dnešné "metalické" siete LAN sú založené takmer výhradne na báze tzv. **krútených dvojliniek** (twisted pair -TP). Tým, že sú vodiče krútené, minimalizuje sa efekt antény (ak prvý vodič vysiela, druhý by hneď mohol aj prijímať elektromagnetické vlnenie – t.z. vyžarovanie do priestoru si navzájom rušia a tiež sa znižujú rušenia s okolitými vlnami).


UTP

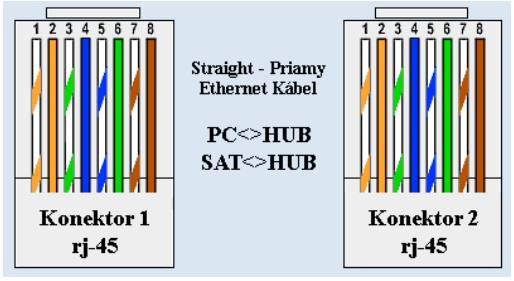

STP

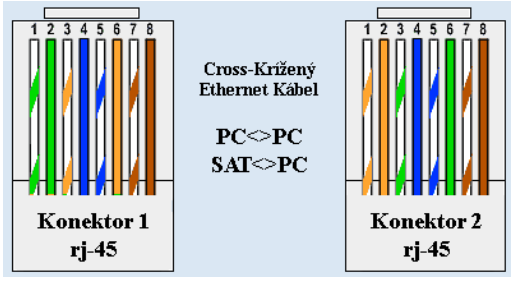
UTP kábel je definovaný ako netienený kábel s vodičmi, ktoré majú štruktúru krútených párov. Tento kábel patrí medzi symetrické. Pozostáva z dvoch, štyroch alebo viacerých medených vodičov, okolo ktorých je izolácia. Najčastejšie sa používajú štvorpárové. Krútené vodiče sa nachádzajú vo vnútri ochranného obalu, ktorý zabezpečuje ochranu pred ich mechanickým poškodením



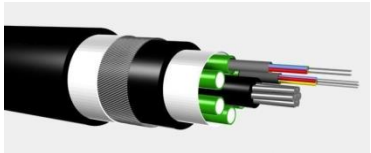
Konektor, pomocou ktorého sa káble TP zapojujú do sieťových kariet a switchov, sa označuje ako RJ-45.

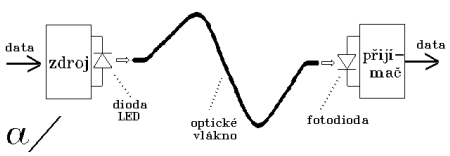
Ak má kábel na oboch koncoch totožné ukončenie konektorov, jedná sa o takzvaný **priamy kábel**, ním sa prepájajú prakticky všetky sieťové prvky (počítače so switchom, routrom a pod.) Pokiaľ sú konektory na koncoch rozdielne (pozri obr.), nazývame ho **krížený** (cross) **kábel**. Ten použijeme iba ak napr. chceme prepojiť dva počítače medzi sebou.

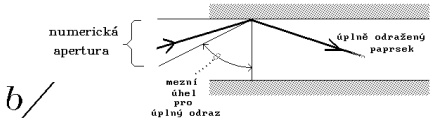




Optické káble – slúžia na prenos signálov a dát pomocou svetelného žiarenia, najmä na veľké vzdialenosti. V porovnaní s klasickými metalickými káblami je ich výhodou predovšetkým značná prenosová kapacita (rýchlosť) a vylúčenie vplyvu rušivých elektromagnetických polí na kvalitu prenášaného signálu (preto je vhodný pre vonkajšie použitie), nízke straty, majú malé rozmery a nízku hmotnosť, malé tlmenie a sú odolné voči odpočúvaniu. Podľa svojej konštrukcie sú určené hlavne na budovanie telekomunikačných a počítačových sietí a prenos signálov káblovej televízie. Nevýhody: Vyššia cena, drahé vysielacie a prijímacie zariadenia, drahé spájanie káblov, citlivosť na ohyby. Optický kábel je médium, ktoré prenáša signály prostredníctvom svetla, signály neputujú vo forme 0 a 1, ale ako svetelné záblesky. Zdrojom svetla môže byť obyčajná LED dióda alebo nákladnejšia laserová dióda, ktorá emituje svetelné impulzy na základe privádzaného prúdu. Optické vlákna sa skladajú z:





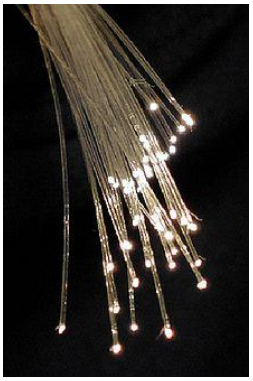


- **jadra** (je zložené z jedného alebo viacerých sklenených príp. plastických vlákien, ktorými prechádza

svetelný signál v smere svojej pozdĺžnej osi; plastické vlákna sú jednoduchšie na výrobu, ale je ich možné použiť len na kratšiu vzdialenosť; priemer jadra sa pohybuje od 2 do niekoľko sto mikrometrov)

- **plášťa** (vyrobený ako jedna časť spoločne s jadrom; jeho úlohou je "udržať" svetlo vo vnútri svetlovodu; priemer plášťa je od 100 mikrometrov do 1 mm)
- **obalu** - vonkajšie ochranné puzdro

Obr. Zväzok optických vlákien →

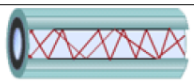


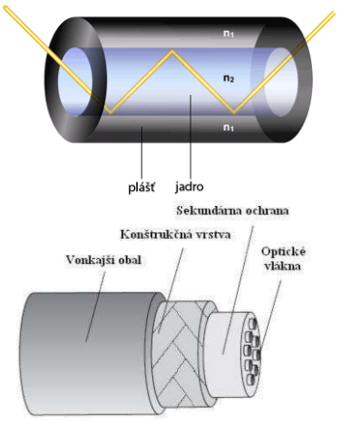
Postupnými odrazmi sa svetelný lúč dostane až na koniec optického vlákna. Jedno optické vlákno môže prenášať údaje len jedným smerom. Preto na komunikáciu medzi dvoma bodmi potrebujeme optické vlákna aspoň dve. V optických kábloch nájdeme vedľa seba naukladaných niekoľko desiatok optických vlákien.

Podľa počtu ciest, ktorými môže svetelný lúč v optickom vlákne prechádzať rozlišujeme:

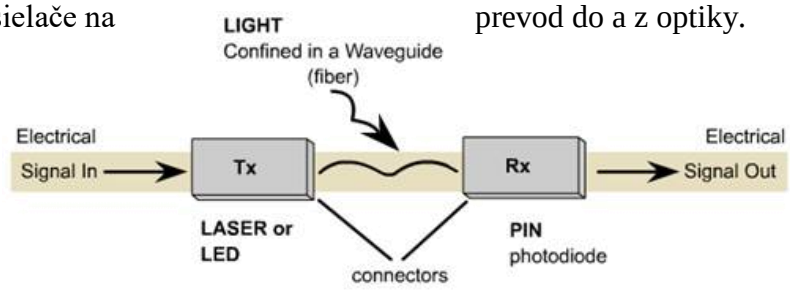
- ***jednovidové*** optické vlákna s menším priemerom jadra, preto optický signál sa šíri priamočiaro, ako zdroj svetla využívajú laserový zdroj, používajú sa pre diaľkové spoje, ale sú drahšie ako mnohovidové
- ***mnohovidové*** - svetlo sa šíri vláknom vo viacerých lúčoch (vidoch) optické vlákna (používa v LAN sieťach), nie sú tak „háklivé“ na ohyb; ako zdroj svetla využívajú LED diódy

Tab. 1 Rozdiely medzi jedno vidovým a mnoho vidovým optickým vláknom

jedno vidové optické vlákno	**mnoho vidové optické vlákno**
	
menšie jadro (5 – 8 µm)	väčšie jadro (50 µm alebo 62,5 µm)
slabšie pohlcovanie svetla	silnejšie pohlcovanie svetla
dosah na 3 km	dosah na 2 km
zdrojom svetla je LASER	zdrojom svetla je LED
využitie v chrbticovej sieti	využitie v LAN



Na prenos dát v sieti sa používajú elektrické signály, preto je potrebné pri optických zariadeniach použiť prijímače a vysielače na prevod do a z optiky.



Vysielač - Tx (Transmiter) - používa 2 typy signálov LED dióda alebo LASER
Prijímač – Rx (Receiver) jeho úlohou je prijať signál a spracovať ho na elektrické signály - používajú sa foto leddiódy
Káble sú ukončené konektormi.

Bezdrôtové technológie

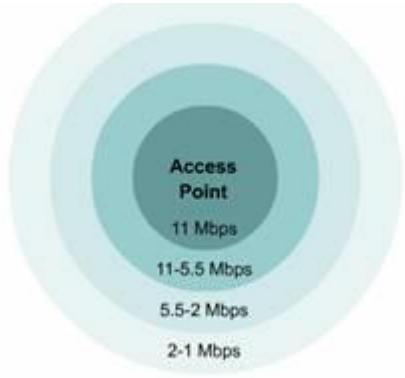
Wi-Fi je podobne ako bluetooth bezdrôtová technológia na komunikáciu pomocou rádiových vĺn na 2,4 GHz. Na rozdiel od **Bluetooth** (používa sa hlavne na bezdrôtový prenos súborov, napr. medzi počítačom a mobilným telefónom) má väčší dosah a vyššiu prenosovú rýchlosť a v súčasnosti sa používa hlavne na pripojenie k internetu prostredníctvom **prístupového bodu** AP (Access point), najčastejšie ide o **router**, pričom oblasť, ktorá je nim pokrytá sa nazýva „**hot spot**“. Môžete sa s nimi stretnúť v školách, kaviarňach, v centrách miest, v obchodných centrách, na letiskách a podobne.

Wi-Fi je sada štandardov pre bezdrôtové siete LAN (WLAN) v súčasnosti založených na špecifikácii IEEE 802.11. Štandardy pre bezdrôtové siete:

Wi-Fi špecifikácie

Špecifikácia	Rýchlosť	Frekvencia Pásmo	Kompatibilita
802.11a	54 Mbit/s	5 GHz	a
802.11b	11 Mbit/s	2,4 GHz	b
802.11g	54 Mbit/s	2,4 GHz	b, g
802.11n	600 Mbit/s (4x 150 Mbit/s)	2,4/5 GHz	b, g, n
802.11ac	6,93 Gbit/s (8x 867 Mbit/s)	5 GHz	a, b, g, n, ac

AP je pripojené do siete cez metalickú kabeláž. AP sú vybavené anténou, v závislosti na použitej anténe a prostredí je dosah od 90 do 150 m. Na pokrytie väčšieho územia sa môžu bunky prekrývať, vtedy hovoríme o roamingu.
Proces prepojenia: AP vysiela svoj SSID (Service Set Identifier, sieťové meno) prostredníctvom paketov nazývaných **beacons** (signály, majáky), ktoré sú vysielané každých 100 ms rýchlosťou 1 Mbps (najnižšia rýchlosť Wi-Fi). S postupnou vzdialenosťou od AP prenosová rýchlosť slabne (obr.).

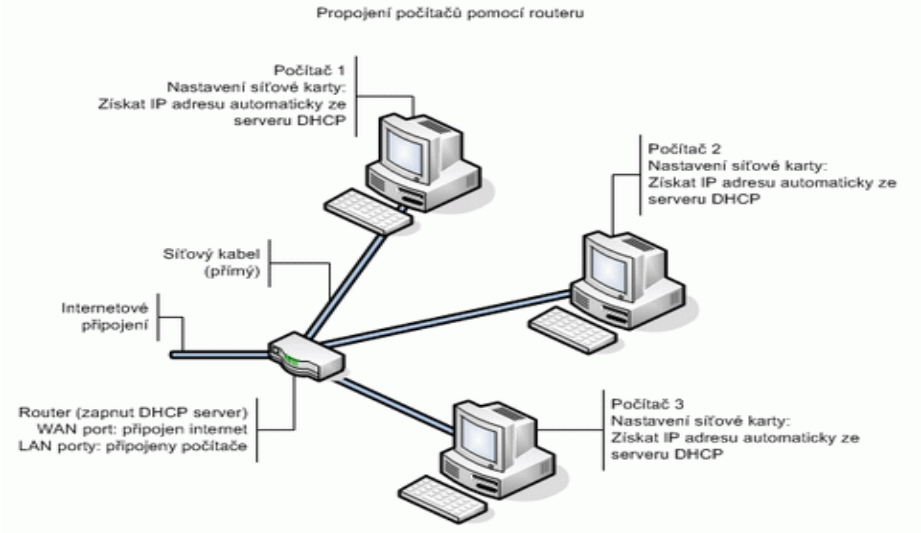


Zabezpečenie WiFi sietí

V prípade, že ste si vytvorili WiFi sieť, alebo ste pripojený do siete WiFi technológiou, je potrebné si ju správne zabezpečiť, aby nedošlo k neautorizovanému pripojeniu do vašej siete, a tým napr. k nárastu vašich poplatkov za pripojenie k internetu alebo zneužitiu vašich osobných údajov.
Zabezpečenie WiFi je možné urobiť viacerými spôsobmi:

- Skrytie alebo zmena názvu siete, tzv. SSID (Services Set Identifier), čo znamená zabránenie vysielaniu názvu siete do okolia AP.
- Filtrovanie pomocou MAC adries MAC. Ak chceme dovoliť pripojenie určitému počtu počítačov zaradíme si ich MAC adresy do zoznamu povolených adries. Takýto typ zabezpečenia nazývame aj autentifikáciou – riadením prístupu do siete.
- Autentifikácia zdieľaným kľúčom (shared key), ak sa chce niekto pripojiť do vašej siete, musí poznať vami zadaný kľúč, pomocou ktorého prebehne autentifikácia a následné pripojenie. Táto metóda je ďalej rozšírená o šifrovanie prenosu kľúča. Dáta sú šifrované pomocou kľúča WEP (Wired Equivalent Privacy) alebo WPA (WiFi Protected Access), ktoré vyriešilo niektoré bezpečnostné slabiny WEP.

Príklad zapojenia v tomto prípade 3 užívateľov v obytnom dome prostredníctvom routera, ktorý má väčšinou aj integrovaný Firewall – pre zabezpečenie lokálnej siete pred prístupom z Internetu.

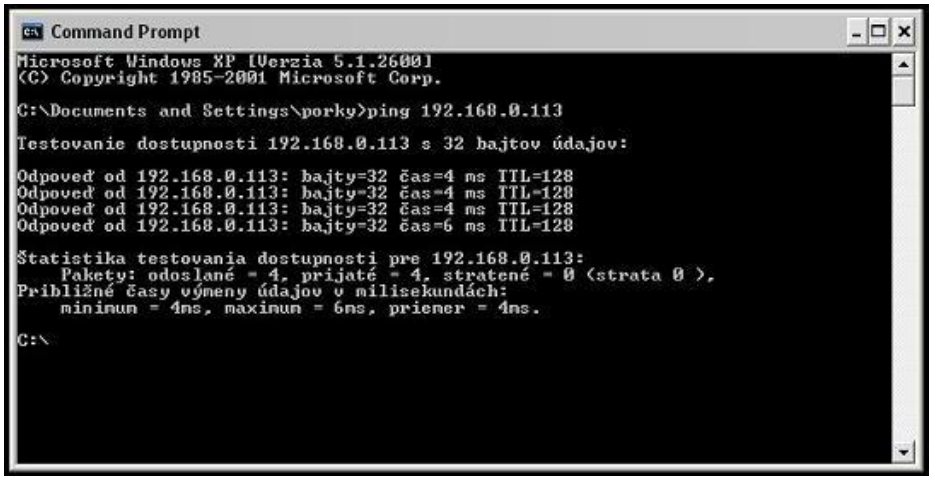


Situácia - tri počítače so sieťovou kartou a router, ktorý má jeden port WAN, do ktorého sa pripojí vonkajšia sieť (internet), nakonfiguruje sa podľa údajov od internetového poskytovateľa alebo správcu siete. Ďalšie jeho LAN porty slúžia pre pripojenie počítačov. Ďalej je potrebný tienený STP ale postačí aj netienený UTP kábel s krútenými vodičmi s konektormi RJ45 (router stojí okolo 30 €, 1m sieťového káblu cca 0,25 €)

Zdieľanie dát a tlačiarne - ak už máme nakonfigurovanú počítačovú sieť a chceme navzájom zdieľať dáta a tlačiť z iných počítačov v sieti na počítač, ktorý má tlačiareň pripojenú, najprv je treba skontrolovať, či je zdieľanie súborov a tlačiarní vo Windows nainštalované. Postupujte nasledovne: Otvorte si *„Vlastnosti“* vášho sieťového pripojenia a v tabuľke vidíte položky, aké vaše sieťové pripojenie využíva, pokiaľ tam nie je vypísané *„zdieľanie súborov a tlačiarní v sieťach Microsoft“*, potom je treba podporu zdieľania doinštalovať. Kliknete na tlačidlo *„Nainštalovať...“* v novom okne vyberte *„služba“* a dajte *„pridať“*. Vyberte *„zdieľanie súborov a tlačiarni v sieťach Microsoft“,* pokračujte tlačidlom *„OK“*. Služba sa nainštaluje a pridá sa k vášmu sieťovému pripojeniu, môžete pokračovať zatlačením tlačidla *„Zavrieť“*. Teraz je všetko pripravené k zdieľaniu dát do siete. Kliknete na adresár, ktorý chcete zdieľať pravým tlačidlom a vyberte *„Zdieľanie a zabezpečenie“*. Zaškrtnite políčko *„Zložka zdieľaná v sieti“*, zaškrtnutím políčka *„Povoliť užívateľom v sieti meniť moje súbory“* povolíte užívateľom mazať a meniť vaše súbory, pokiaľ si tým nie ste ozaj istí, políčko necháte radšej nezaškrtnuté. Teraz je vybraný adresár k dispozícii ostatným užívateľom v sieti. Keď na inom počítači otvoríte *„Miesta v sieti“,* uvidíte zdieľané dáta z počítača, na ktorom sme zdieľanie nastavovali. Niekedy sa stane, že miesto zdieľaných dát nevidíte nič, potom si pomôžte nasledujúcim postupom – kliknete na *„Štart“* > *„Spustiť“* a do poľa napíšte dve spätne lomítka a názov počítača, na ktorom sú zdieľané dáta (alebo jeho IP adresu) *PC1* alebo *192.168.1.5*. Po odkliknutí *„OK“* sa otvorí volaný počítač a ľahlo sa už dostanete k zdieľaným dátam.

Analýza sieťovej činnosti (Prostriedky na kontrolu dostupnosti počítača v sieti)
Pri práci v sieťovom prostredí sa veľmi často stretávame s mnohými problémami. Môžu to byť problémy súvisiace s výpadkami serverov, smerovačov, prepínačov, prípadne chyby v konfigurácií sieťových zariadení. Pri ich odhaľovaní môžeme použiť niektoré prostriedky.

Príkaz **PING** umožňuje kontrolu dostupnosti cieľového počítača na úrovni protokolu IP. Prostredníctvom utility ping spustenej na ktoromkoľvek PC v sieti sa dá vyslať určité množstvo testovacích dát (paketov) ktorémukoľvek inému PC, ktorý je tiež pripojený k sieti. Ak tieto testovacie dáta k cieľovému PC dorazia, ten ich prijatie potvrdí počítaču, ktorý ich vyslal. To znamená, že dáta vyslané odosielateľom boli úspešne doručené príjemcovi a sieťová komunikácia je teda funkčná. Utilita ping je preto veľmi užitočná pri riešení problémov v situácii, keď sa nám nedarí nadviazať spojenie s PC, ktorý by jednoznačne mal byť dostupný. Jedná sa o utilitu fungujúcu v textovom režime čiže v „príkazovom riadku“. Príkaz ping sa zadáva z príkazového riadku s menom počítača alebo jeho IP adresou. Postup je jednoduchý - otvoríte príkazový riadok (*„Štart“* > *„Spustiť“*, do poľa napíšte *cmd* a stlačte *„OK“*). Do príkazového riadku napíšte príkaz napr.: ***„ping google.sk.“*** Ak je cieľ dostupný, výpis programu poskytne údaje, ktoré vypovedajú o kvalite spojenia. Výpis obsahuje informácie o každom odoslanom pakete a štatistiky o prenose týchto paketov. Čas = doba obehu udáva čas, ktorý uplynul medzi odoslaním našej požiadavky a príchodom odpovede od cieľového počítača. TTL - je číslo, ktoré udáva životnosť paketu. Každý smerovač zníži toto číslo o 1. Smerovač, ktorý hodnotu TTL zníži na nulu paket zahodí a odosielateľovi pošle správu, ktorou mu túto skutočnosť oznámi a prenos sa začne odznova. Tým sa zabraňuje nekonečnému krúženiu datagramov pri nekorektnom stave v sieti.



Príklad použitia utility ping:
Predstavte si situáciu, keď sa chcete presvedčiť, či pracuje zamestnanec, ktorého PC má pridelenú adresu 192.168.0.113. Nieje nič ľahšieho. Spustíte si v príkazovom riadku utilitu ping s príkazom: *Ping 192.168.0.113*. Ak zamestnanec pracuje, má zapnutý PC a je teda pripojený k sieti, utilita ping zobrazí túto odozvu :

Príkaz **TRACERT** využíva rovnaký postup ako utilita ping, avšak na účely testovania komunikácie smerom von z lokálnej siete, teda do internetu. Utilita tracert nachádza uplatnenie vtedy, keď sa nejaký server www javí ako nedostupný a pomocou tejto utility sa dá zistiť, či sa jedná o poruchu cieľového servera alebo o závadu na trase spojenia. Inak povedané, utilita tracert dokáže vysielať pakety a nasledovne zobraziť kadiaľ (cez ktoré smerovače) sa tento testovací packet dostáva k cieľovému serveru.
Napr. predstavte si situáciu, že máte svoj obľúbený server www, na ktorom napríklad každý deň sledujete správy a viete bezpečne, že sa tento server nachádza vo vašom okolí. Nakoľko tento server sledujete pravidelne, ste zvyknutý na rýchlosť jeho odozvy. Jedného dňa zistíte, že tento server je síce dostupný, ale rýchlosť jeho odozvy sa výrazne znížila.

Príčina môže byť, že došlo k výpadku niektorej linky poskytovateľa pripojenia k internetu a napriek tomu, že bývate neďaleko servera, pripájate sa na neho napr. cez Rakúsko – Francúzsko - Belgicko – Česko – a späť na Slovensko. Ak by ste použili utilitu tracert, zistili by ste, že ste sa k serveru nedostali napr. na 5 skokov, ale napr. na 20 skokov. Z toho je zrejmé, že niečo nie je v poriadku.

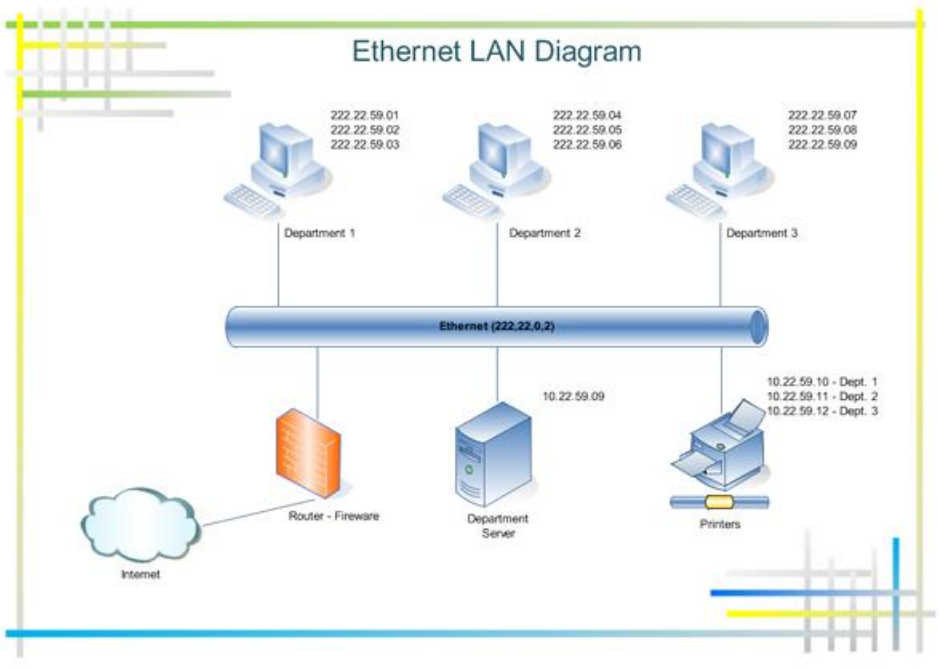
```
C:\Documents and Settings\Skola>tracert www.post.sk

Smerovanie sledovania k www.post.sk [85.248.69.131]
prekročilo maximum 30 skokov:

  1     1 ms     1 ms     1 ms  10.10.5.1
  2    19 ms    20 ms    20 ms  10.255.255.238
  3    19 ms    18 ms    21 ms  10.255.255.241
  4    18 ms    19 ms    22 ms  87.197.255.33
  5    21 ms    18 ms    20 ms  babo74.213-81-254.telecom.sk [213.81.254.74]
  6    23 ms    18 ms    20 ms  gtsi-gw.six.sk [192.108.148.100]
  7    17 ms    20 ms    19 ms  g452.petitpress-gw.ba.gtsi.sk [62.168.86.246]
  8   475 ms   447 ms   445 ms  www0.post.sk [85.248.69.131]

Sledovanie sa dokončilo.
```

Na obr.v každom riadku je poradové číslo smerovača a 3 časy znázorňujúce dobu obehu paketu, tracert zasiela pre každú hodnotu 3 pakety, na konci riadku je meno smerovača s IP adresou. Ak je v niektorom riadku * vo výpise, znamená to, že odpoveď neprišla v danom čase. Tri * znamenajú, že smerovač je nedostupný.

Príkaz **IPCONFIG** umožňuje zobraziť informácie o konfigurácii TCP/IP. Tento príkaz je možné použiť s prepínačom /all, čím získame všetky informácie ohľadom nastavenej konfigurácie, včítane IP, MAC adresy , DHCP, adresy serverov DNS atď.

Ethernet

V oblasti počítačových sietí sa objavilo množstvo rôznych prenosových technológií, založených na rôznych myšlienkach a základných predpokladoch, využívajúcich pre svoju funkciu rôzne prístupy a metódy. **Ethernet** je v súčasnej dobe najrozšírenejšou technológiou pre budovanie počítačových sietí typu LAN (tj. domácej alebo firemnej siete). Ethernet se stal štandardom pre svoju jednoduchosť a nízku cenu a vytlačil spolu s bezšnúrovou technológiou Wi-fi z trhu ostatné alternatívne technológie (napr. Token ring, ARCNET, ATM, FDDI). Ethernet je založený na nápade, že počítače v sieti budú posielať správy spôsobom, ktorý pripomína rádio, ale prostredníctvom spoločného kábla alebo kanála, niekedy označovaného ako éter (ether). Každý počítač má globálne jedinečnú 48-bitovú MAC adresu, ktorú má každá karta pridelenú od výroby, aby bolo zabezpečené, že všetky systémy v spoločnom Ethernete majú rozdielne adresy. Vďaka dnešnej všade prítomnosti Ethernetu zabudovali mnohí výrobcovia ethernetové (sieťové) karty priamo do matičných dosiek počítačov. Ethernet a jeho sieťové rozhranie (resp. sieťová karta) pracujú s tzv. „ethernetovými“ rámcami (bloky dát).



Ethernet našiel uplatnenie ako aj v starších zbernicových, či kruhových topológiach, ale aj v súčasných typu hviezda. Je nezávislý na architektúre siete (klient/server alebo peer-to-peer), či použitom operačnom systéme

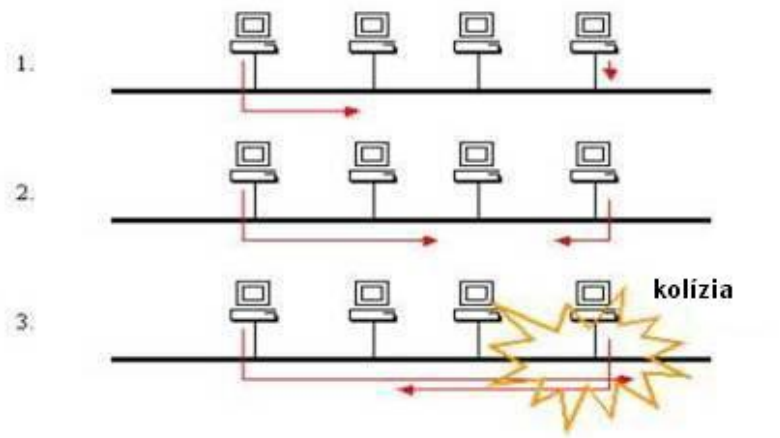
(Novell, Windows...). Jednoduchosť protokolu i samotnej inštalácie, prípadná implementácia na vyššiu prenosovú úroveň, to všetko robí Ethernet takým populárnym.

Princíp Ethernetu využíva jednoduchých technológií, kde komunikáciu s PC zabezpečuje sieťová karta, samotný prenos sprostredkováva prenosové médium (napr. kábel) a spojenie aktívne prvky (ako hub, switch či server).

Jednotlivé stanice v počítačovej sieti sú vzájomne prepojené spoločným médiom. o ktoré sa medzi sebou musia pri vysielaní dát deliť. Poriadok, ktorým sa stanice budú riadiť sa nazýva prístupová metóda.
Prístupové metódy môžu byť

- **stochastické,** založené na náhodnom prístupe k médiu, napr. metóda CSMA/CD , ktorú používa technológia **Ethernet**. Jednotlivé uzly (väčšinou počítače) sa pokúšajú komunikovať bez akéhokoľvek poradia. Žiadny uzol tak nemá garantované, že sa mu podarí preniesť určité množstvo dát za určitú dobu.
- **deterministické**, kedy prístup k prenosovému médiu je riadený. Používa ju technológia **Token ring**. Po sieti je prenášaný špecifický paket(token) a každý uzol musí počkať až k nemu token dorazí. Ak ku nemu token dorazí vtedy môže začať posielať dáta. Keď skončí a uzavrie spojenie vygeneruje nový token a pošle ho ďalej. V skutočnosti je to však o čosi zložitejšie. Technológia Token ring je zložitejšia a tým aj drahšia než Ethernet a preto sa nedočkal takého rozšírenia v praxi a dokonca bol zastavený jej ďalší vývoj.

Metóda **CSMA /CD** (Carrier Sense Multiple Access with Collision Detection) je metóda náhodného prístupu.



Rozhodovanie o tom, ktorá zo staníc (napr. PC) bude vysielať prebieha nasledovne. Stanica, ktorá chce vysielať najprv "počúva", či nevysiela iná stanica v sieti. Ak nevysiela žiadna stanica, môže začať vysielať. Pretože sa signál po vedení šíri konečnou rýchlosťou (blížiacou sa rýchlosti svetla), môže sa stať, že jedna sieťová stanica zaháji vysielanie, avšak druhá stanica umiestnená o kúsok ďalej vysielanie ešte nepočuje, a preto tiež začne vysielať. Výsledkom bude zložený signál, ktorý bude nezrozumiteľný. Vtedy dochádza ku kolízii. Vysielajúce stanice sa na krátky okamžik odmlčia a po krátkej náhodne dlhej dobe sa stanice pokúsia o nové vysielanie; (http://www.datacottage.com/nch/eoperation.htm - pozri ukážku na webe).

Výhody Ethernetu: a) rozsiahly sortiment SW a HW produktov pre prepojovanie rôznych počítačových prostredí; b) umožňuje voľbu prenosových médií, ktoré možno v sieti pomerne jednoducho kombinovať; c) prenosová rýchlosť až do 100 Gbit/s; d) jednoduchšia a lacnejšia ako tokenové LAN alebo ATM - ponúka priaznivý pomer cena/výkon

Nevýhoda spočíva v tom, že so stúpajúcim počtom staníc klesá výkon siete a zvyšuje sa pravdepodobnosť kolízii. Táto vlastnosť je však takmer eliminovaná použitím prepínačov, namiesto starších rozbočovačov.

Ethernet pokrýva spodné dve vrstvy modelu OSI, t.j. fyzickú a linkovú vrstvu. Na úrovni fyzickej vrstvy špecifikuje ako majú byť prenášané jednotlivé bity, zatiaľ čo na úrovni linkovej vrstvy musí byť špecifikované ako spolu jednotlivé bity súvisia, aké tvoria celky (rámce), aké majú tieto rámce hlavičky a čo obsahujú.

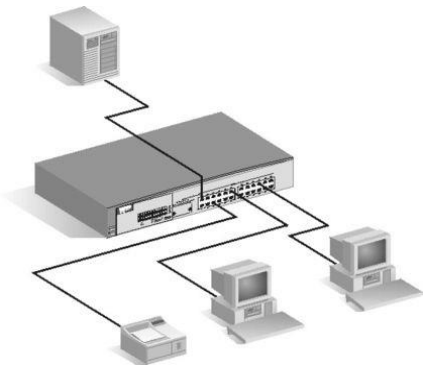
Ethernet je definovaný pre rôzne prenosové média s postupne narastajúcimi prenosovými rýchlosťami.
V minulosti sa využíval hlavne koaxiálny kábel, v súčasnosti sa používajú prevaže krútená dvojlinka, optické káble a bezšnúrový Ethernet – Wi-Fi. Jednotlivé varianty protokolov technológie Ethernet sa značia napr. **10Base5**, **100Base-TX** a podobne. Prvá číslica určuje max. prenosovú rýchlosť v Mb/s. Nasleduje označenie pásma (všetky verzie Ethernetu pracujú v základnom pásme, preto vždy obsahujú „Base“) a určenie druhu prenosového média. Napr. **1000Base-T** Ethernet s rýchlosťou 1000 Mbit/s, nazývaný **Gigabit Ethernet**. Využíva 4 páry UTP kabeláže kategórie 5e, je definovaný do vzdialenosti 100 metrov. **1000Base-LX** Gigabit Ethernet používajúci jednovidové optické vlákno. Je určený pre väčšie vzdialenosti až niekoľko desiatok

kilometrov. **40GBASE** a **100GBASE** s rýchlosťou 40 a 100 Gbps by mal používať optické vlákna; medené káble do dĺžky aspoň 10 metrov.

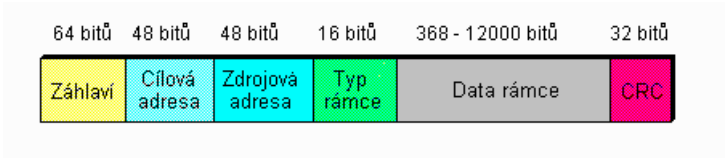
S nástupom switchov, ako rozhodujúcich aktívnych prvkov v infraštruktúre Ethernetu, sa využívanie CSMA/CD dostalo do úzadia a presadil sa variant nazývaný „prepínaný Ethernet“, ktorý už nie je zaťažený kolíziami. Súčasné varianty Ethernetu pracujú s komunikačnými rýchlosťami na úrovni 10 Gb/s.

Každá sieťová karta spracúva len tie rámce, ktoré sú adresované na jej MAC adresu, ostatné ignoruje. Výnimku z tohto pravidla tvoria rámce, ktoré sú adresované príjemcovi s MAC adresou FF:FF:FF:FF:FF:FF. Túto špeciálnu MAC adresu nazývame **adresa obežníka (broadcast address)** a rámce s týmto adresátom nazývame linkovými obežníkmi (link-layer broadcast). Linkový obežník musí spracovať *každá* sieťová karta, ktorá ho príjme. Pomocou obežníkov je možné doručovať správy všetkým uzlom siete.

Kľúčovým stavebným prvkom ethernetových sietí je **prepínač (switch)**. Prepínač je zariadenie obsahujúce istý počet ethernetových portov (spravidla od 4 do 48), ku ktorým sa pripájajú jednotlivé uzly siete (najmä počítače). Úlohou prepínača je vytvárať spoločné komunikačné médium a umožniť pripojeným uzlom komunikovať navzájom.

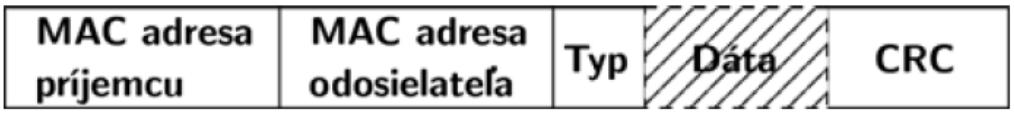


Štruktúra rámca:



Záhlavie - zahájenie rámca, synchronizácia: 62 bitov: série 101010..., 2 bity: 11
Cieľová MAC adresa, ...
CRC – kontrolný súčet údajov celého rámca – podľa ktorého sa overuje či dáta sa pri prenose nepoškodili.

Všetky varianty siete Ethernet využívajú zhodný formát rámca tohto tvaru:



Obrázok 2: Formát rámca typu Ethernet

Význam jednotlivých polí:

- MAC adresa príjemcu: adresát. Nachádza sa zámerne na začiatku rámca, aby ju bolo možné čo najrýchlejšie nájsť a spracovať.
- MAC adresa odosielateľa: autor rámca.
- Typ: Hodnota v tomto poli identifikuje typ dát v dátovej časti rámca. Jednotlivé hodnoty tohto typov a ich významy sú dohodnuté, napríklad číslo 0x0800 udáva, že v dátovej časti sa nachádza IP paket.
- Dáta: V tejto časti sa prenášajú samotné dáta.
- CRC: Toto pole obsahuje kontrolný súčet celého rámca. Príjemca si vypočíta vlastný kontrolný súčet a porovná ho s hodnotou tohto poľa. Ak sa hodnoty nezhodujú, znamená to, že rámec sa nepreniesol správne a príjemca ho zahodí. Ethernet nezabezpečuje nijakú opravu dát ani opätovné odoslanie.

Na nasledujúcom obrázku získanom z programu Wireshark je zobrazená hlavička ethernetového rámca - MAC adresa príjemcu, MAC adresa odosielateľa a typ dátovej časti. Za typom nasleduje samotná dátová časť rámca, ktorá v tomto prípade obsahuje IP paket, ten v sebe obsahuje TCP segment a vo vnútri TCP segmentu sa nachádza správa protokolu POP3. Kontrolný súčet rámca nie je zobrazený.