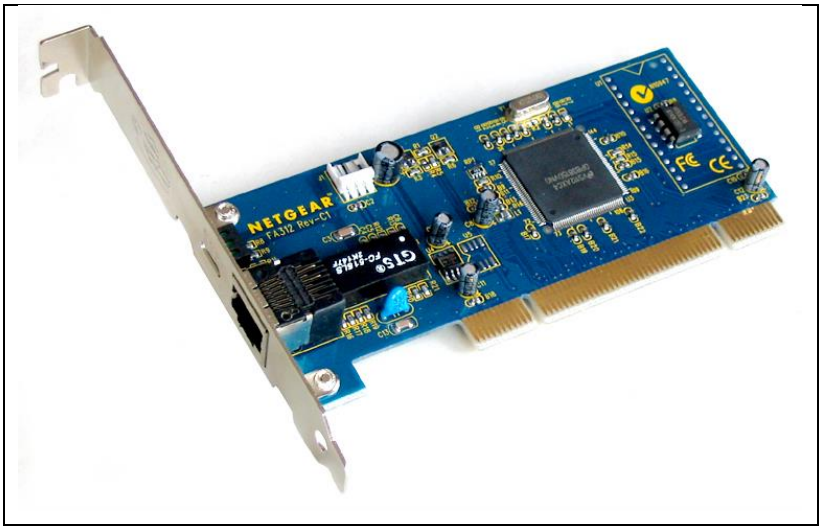
KOMUNIKAČNÍ HARDWARE

Síťová karta (Network Interface Controller, zkratka NIC)

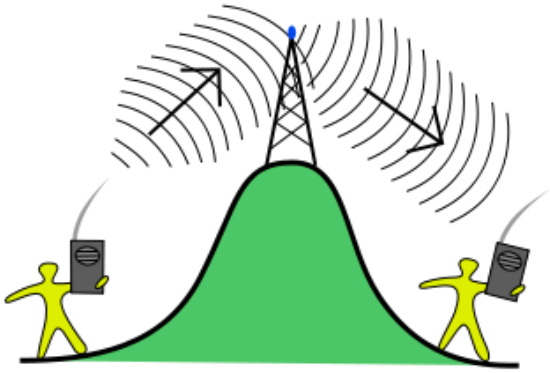
Slouží ke vzájemné komunikaci počítačů v počítačové síti. Ve stolních počítačích má podobu karty, která se zasune do slotu (ISA, PCI, PCI-e) základní desky nebo (což je dnes daleko častější varianta) je na základní desce integrovaná. U notebooků je situace podobná, integrace převládá a pro externí připojení se používá rozhraní PCMCIA.



Síťové rozhraní je obvykle síťová karta, tedy aktivní zařízení, které přijímá a vysílá rámce (ethernetové rámce nebo jiné podle typu použité technologie). Za síťové rozhraní nepovažujeme síťové porty opakovače (repeater), hubu, switche a bridge (mostu), které není v síti možno adresovat (poslat mu nějaká data).

Opakovač

Bezdrátový opakovač



Opakovač (anglicky *repeater*) je elektronický aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále. Tak je možné snadno zvýšit dosah média bez ztráty kvality a obsahu signálu. Opakovače patří do první (fyzické) vrstvy referenčního modelu ISO/OSI, protože pracují přímo s elektrickým signálem.

Digitální komunikace obecně (drátové)

V digitálních komunikačních systémech je za opakovač označováno zařízení, které přijímá digitální signál na elektromagnetických nebo optických přenosových médiích a regenerovaný jej vysílá do další větve média. Opakovač vyrovnává útlum způsobený elektromagnetickým polem nebo ztrátami v médiu. Opakovač odstraňuje šum, tím že příchozí signál je obnoven do původní digitální podoby a poté znovu vytvořen (analogové zesilovače zesilují i šum). Více opakovačů za sebou umožňuje prodloužit dosah signálu. U Ethernetu je z důvodu použití kolizních protokolů CSMA/CD jejich počet omezen, aby bylo možné bezpečně detekovat kolize. Použití opakovačů totiž vnáší nezanedbatelné zpoždění do celkové doby, kterou signálu trvá, než urazí cestu z jednoho konce sítě na druhý. Pokud by tato doba přesáhla určitou hranici, mohlo by dojít k nežádoucí situaci: kolize by byla detekovatelná jen v části sítě, a nikoli v celé síti (například jen "uprostřed", a nikoli "na koncích").

Bezdrátové komunikace

U bezdrátových systémů se repeater skládá z radiového přijímače, zesilovače, vysílače, izolátoru a dvou antén. Vysílač generuje signál na odlišné frekvenci od signálu na vstupu - toto se nazývá frequency offset a je nezbytný k ochraně vstupu před zarušením od zesíleného signálu na výstupu. Izolátor v tomto případě poskytuje dodatečnou ochranu. Opakovače se strategicky umisťují na střechy vysokých budov, vrcholky kopců a podobně. Takto se dá jednoduše zvýšit výkon i pokrytí bezdrátové sítě.

U wifi-routerů se používá takzvaný systém WDS (Wireless Distribution System), který umožňuje automatizované přeposílání dat od hlavních uzlů do uzlů vedlejších. Systém WDS disponuje 3 typy propojení:

- Repeater - Slouží k propojení dvou samostatných sítí. WDS klient dál přeposílá signál jako 'posilovač'.
- Bridge - Slouží k propojení dvou samostatných sítí. WDS klient dál signál nepřeposílá.
- Crude - Chová se jako Repeater, ale je zpětně kompatibilní s různými výrobci.

U wifi routerů s modemy, má repeater i mód "Universal Repeater". V porovnání s tradičním WDS Universal Repeater poskytuje vyšší výkon, kompatibilitu a snadněji se nastavuje.

Satelitní komunikace

Repeater, častěji nazýván transponder (česky *retranslátor*), přijímá signál a přeposílá jej, často na odlišných frekvencích do cílové lokace.

Mobilní komunikace

Zařízení pro posílení GSM signálu v místech, kde není nebo není dostatečně silný (např. sklepy budov, garáže, vlaky…).

Optická vlákna

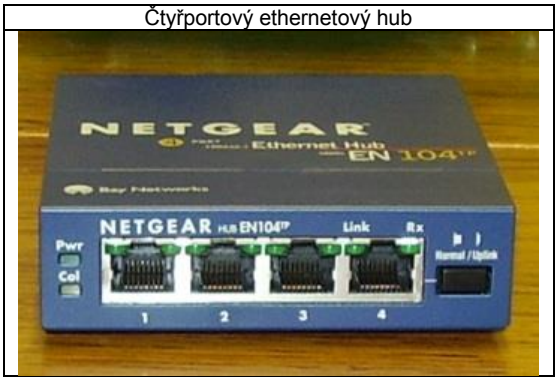
Repeater je složen z fotobuňky (přijímače), zesilovače a světlo emitující (LED) nebo infra-diody (IRED). Optický signál nejprve převede na elektronický a po zrestaurovnání opět na optický, který je vysílán dále do optického vlákna. Optické opakovače pracují s mnohem menšími výkony, než opakovače bezdrátové, a také jsou mnohem jednodušší a levnější. Přesto jejich výroba vyžaduje mnohem vyšší přesnost a kvalitu k minimalizaci vnitřního šumu elektronických obvodů.

Radiotechnika

Opakovače jsou využívány i komerčními radiostanicemi, nebo radioamatéry k oddělení signálu v jejich frekvenčním rozsahu od jednoho přijímače ke druhému.

ROZBOČOVAČ - HUB

Čtyřportový ethernetový hub



Ethernetový hub nebo pouze **hub**, česky **rozbočovač**, je aktivní prvek počítačové sítě, který umožňuje její větvení a byl základem sítí s hvězdicovou topologií. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena. Nástupcem síťových rozbočovačů jsou switche (přepínače), které síťový provoz inteligentně směrují na základě fyzické adresy (mají přehled o tom, který počítač je připojený ke kterému portu a data pak odešlou pouze na daný port). Hub pracuje na fyzické vrstvě (1. vrstva) modelu ISO/OSI.

Některé huby obsahují BNC a/nebo AUI konektory pro připojení 10BASE2 nebo 10BASE5 zařízení do segmentu. V současné době se huby již nevyrábějí a nalezneme je jen ve starších rozvodech, kde je postupně nahrazují switche, které nabízejí vyšší bezpečnost přenášených dat - u hubů mohl vidět jakýkoliv uživatel sítě veškerou síťovou komunikaci, u switchů toto není (tak jednoduše) možné.

Technické informace

Hub je velmi jednoduché aktivní síťové zařízení. Nijak neřídí provoz, který skrz něj prochází. Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty. Zpoždění je proto pouze 1 bit, takže na rozdíl od switche způsobuje hub nižší latenci. Na hubu jsou typicky signalizační LED diody, podle kterých se dá snadno zjistit vadné spojení. K tomu, aby byly síťové prvky schopny detekovat kolize, je počet hubů v síti omezen. Pro síť 10 Mbit/s je počet segmentů omezen na 5 (4 huby) mezi dvěma koncovými stanicemi. U sítě 100 Mbit/s je limit snížen na 3 segmenty (2 huby). Některé huby mají speciální port, který umožňuje jejich slučování, takže se navenek chovají jako jeden.

Použití

Huby jsou dnes již na ústupu, jsou nahrazovány modernějšími a chytřejšími přepínači, přesto mohou být huby v následujících případech užitečné:

- Protokolový analyzér připojený ke switchi nemusí vždy přijmout všechny požadované pakety, jelikož switch odděluje porty v různých segmentech. Připojením protokolového analyzéru k hubu můžeme monitorovat veškerý provoz v segmentu. (Některé dražší switche mohou být nakonfigurovány tak, aby z jednoho portu odposlechly každý příchozí a odchozí paket a předaly ho jiného portu (např. k prozkoumání, tzv. Port mirroring).
- Některé počítačové clustery vyžadují, aby všechny počítače v clusteru obdržely stejné pakety. K tomuto účelu je hub ideální; u switche by byly zapotřebí speciální úpravy.
- Pokud je switch přístupný nezkušeným nebo nedbalým uživatelům (nebo i sabotérům), např. v konferenční místnosti, můžou ochromit celou síť tím, že propojí dva porty, čímž vytvoří smyčky. Pokud použijeme hub a propojíme dva porty, ochromíme pouze uživatele připojené k hubu, ne uživatele v celé síti. Existují i switche, které dokážou rozpoznat smyčky a potlačit je (např. použitím Spanning Tree protokolu)

- Hub s 10BASE2 konektorem je pravděpodobně nejsnadnější a nejlevnější cestou, jak připojit zařízení, které podporují pouze standard 10BASE2, s moderní sítí (Switche tento konektor většinou nemají). Totéž platí i pro spojování starých sítí, které používaly AUI port.

Most - Bridge

Most (anglicky **bridge**) označuje v počítačové síti síťové zařízení, které spojuje dvě části sítě na **druhé** (linkové) vrstvě referenčního modelu ISO/OSI. Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě.

Princip činnosti

Most odděluje provoz dvou segmentů sítě tak, že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v nezměněném stavu (týká se pouze tzv. Unicast rámců, které jsou určeny jedinému příjemci). Všesměrové rámce (Multicast, Broadcast) jsou naopak propouštěny bez omezení.

Mosty používají dvě základní metody propojování sítí:

- **Transparent bridging** (transparentní, průhledné, přemosťování) je používáno především pro ethernetové sítě (případně i pro FDDI sítě). Mosty jsou neviditelné (průhledné) pro koncové stanice - těm se propojené sítě jeví jako jedna lokální síť. Na začátku vůbec neví, jak jsou jednotlivé stanice v síti rozloženy, a musí paket přijatý na jedné síti poslat do všech ostatních připojených sítí, protože ještě neví, kde se cílová stanice nachází. Postupně se ale umí naučit, jak jsou stanice v síti rozloženy.
- **Source route bridging** (zdrojové směrování) je používáno ve spojení s token-ring sítěmi. Oproti první metodě, kde se kladly větší nároky na most, je zde tomu naopak a cílem je, aby byl most co nejjednodušší. Každý paket musí kromě adresy odesílatele a příjemce obsahovat také posloupnost adres všech mostů, kterými musí paket projít. Vysílající stanice si tedy, dříve než pošle první paket, musí zjistit celou cestu k cílové stanici.

Výhody síťového mostu

- není ho potřeba konfigurovat
- snižuje velikost kolizní domény
- transparentní k protokolům z vyšších vrstev
- lacinější než router

Nevýhody síťového mostu

- neomezuje rozsah všesměrového vysílání
- vyšší latence (zpoždění), než opakovače (repeater) z důvodu čtení MAC adresy
- dražší než opakovače
- přemosťováním různých MAC protokolů dochází k chybám

Bridging versus routing

Bridging a Routing (směrování) jsou podobná řízení toku dat, ale pracují pomocí různých metod. Bridging se provádí na 2. (linkové) vrstvě (L2), routing pak na 3. (síťové) vrstvě (L3) referenčního modelu ISO/OSI. Most tedy směruje rámce podle jejich hardwarové MAC adresy, zatímco router se rozhoduje podle IP adresy uvnitř přenášeného datagramu. Klasický most proto není schopen rozlišovat sítě. Z různých důvodů se však do mostů tato schopnost implementuje, takže most může ležet na pomezí. Při projektování větší sítě si musíme vybrat mezi přemostěním nebo rozdělením na různé podsítě propojené routery. Pokud je v routované síti počítač fyzicky přesunut z jedné síťové oblasti do jiné, musí mu být přidělena jiná IP adresa. Pokud je počítač přesunut uvnitř přemostěné (bridged) sítě, není potřeba nic překonfigurovávat.

Přepínač - Switch

Switch s třemi síťovými moduly a zdrojem.

Switch (česky *přepínač*) je aktivní síťový prvek, propojující jednotlivé segmenty sítě. Switch obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií.

Způsoby přeposílání rámců

- **store and forward** – rámec z jednoho rozhraní přijme, uloží si do vyrovnávací paměti, prozkoumá jeho hlavičky, zkontroluje FCS a následně odvysílá do příslušného rozhraní.
- **cut-through switching** – současné switche ale tento proces často optimalizují, takže k analýze hlaviček dochází, jakmile dorazí začátek rámce. Ani s vysíláním do cílového rozhraní se nečeká, až dorazí celý rámec, ale zahajuje se co nejrychleji, aby zpoždění rámce ve switchi bylo minimální.
- **fragment free** – switch začne přeposílat rámec až po přijetí 64 bytů, kdy je jisté, že na daném segmentu nevznikla kolize - má význam v případě, kdy je do switche připojen hub.
- **adaptive switching** – automatické přepínání mezi metodami cut-through switching a store and forward.

Sada switchů v racku.

Ethernet switch

Nejčastěji switch potkáte jako aktivní prvek v síti Ethernet realizované kroucenou dvojlinkou. Zde nahradil dříve používané huby (rozbočovače), které signál jednoduše kopírovaly do všech ostatních rozhraní. Pracuje zde na 2. vrstvě ISO/OSI modelu. Vedle vyššího výkonu (stanice připojené k různým rozhraním switche navzájem nesoutěží o médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, na které je připojen jejich adresát. Adresování se switche učí automaticky z procházejícího provozu, konkrétně z adres odesilatelů uvedených v rámcích, které do switche přicházejí. Používá se algoritmus Backward Learning Algorithm. Z těchto údajů si switch automaticky plní tabulku identifikující cílová rozhraní pro jednotlivé adresy. Pokud switch dostane k doručení rámec směřující na jemu dosud neznámou adresu, chová se jako hub a rozešle rámec do všech ostatních rozhraní. Lze očekávat, že oslovená stanice pravděpodobně odpoví a switch se tak vzápětí dozví, kde se nachází.

Smyčky v síti.

Ethernetové switche mají problém se smyčkami v síti, vytvářenými za účelem redundance. Pokud síť obsahuje smyčku (mezi dvěma uzly existuje více než jedna cesta), mohou pakety od stejného odesilatele přicházet chaoticky z různých rozhraní a dokonce tentýž paket může do switche dorazit několikrát. Switch není v takovém prostředí schopen rozpoznat, kde se kdo nachází. Tento problém řeší switche mechanismem zvaným **Spanning Tree Protocol**, kterým se zařízení dohodnou na nepoužívání některých tras tak, aby ze sítě zmizely smyčky. Porty, kde byla detekována smyčka, se automaticky deaktivují. Vytvoří se tak minimální kostra sítě dosahující do všech jejích míst. Když dojde ke změně v topologii (např. rozpojení některé linky), bude aktivována některá z dosud odstavených tras tak, aby nový strom nadále pokud možno pokrýval celou síť. Tyto změny se ovšem nedějí okamžitě, je zde jisté zpoždění, nutné ke zjištění nové topologie. To však zvyšuje komunikační režii sítě. Proto je nutné volit aktivaci STP protokolu pouze některých, převážně kořenových přepínačích a na portech, kde by smyčka mohla vzniknout.

Switche dnes často nabízejí i některé pokročilejší funkce, jako například

- **management** - možnost upravovat nastavení switche pomocí telnetu nebo webového rozhraní (HTTP)
- **VLAN** - podpora virtuálních sítí
- **SNMP** - vzdálená správa zařízení, hlášení určitých stavů a situací apod.

L3 switch

Díky svému rozšíření v Ethernetu se pojem switch vžil pro rychlý prvek rozhodující o dopravě paketů. Když se pak objevily Ethernetové switche s rozšířenými funkcemi, které dokázaly analyzovat protokol IP a fungovat jako směrovače (router), začal se pro ně používat pojem L3 switch. **L3 zde označuje 3. vrstvu modelu OSI**, ve které takové zařízení pracuje.

Původní L3 switche byly velmi rychlé, ale jednoduché. Typicky měly jen velmi omezenou podporu směrovacích protokolů a veškerých pokročilých funkcí. Postupem času se jejich schopnosti rozšiřovaly a v současnosti se pojem L3 switch používá víceméně jako synonymum pro směrovač.

Analogicky se můžete setkat s pojmem L4 switch pro zařízení, jež umí analyzovat protokol 4. vrstvy OSI modelu a zpracovávat pakety např. podle čísel portů.

ATM switch

V síti ATM (Asynchronous Transfer Mode) představují switche základní stavební kameny této sítě. Mají úlohu podobnou jako směrovače v IP – hledají cesty pro přepravu paketů a zajišťují ji. ATM je ovšem služba spojovaná, proto ATM switch hledá cestu k cíli jen při navázání spojení. V případě úspěchu si ji poznamená do předávacích tabulek. Jednotlivé datové buňky pak předává velmi rychle na základě jimi nesených identifikátorů (VPi,VCi), podle nichž pozná příslušnost k dříve navázanému spojení.

Router

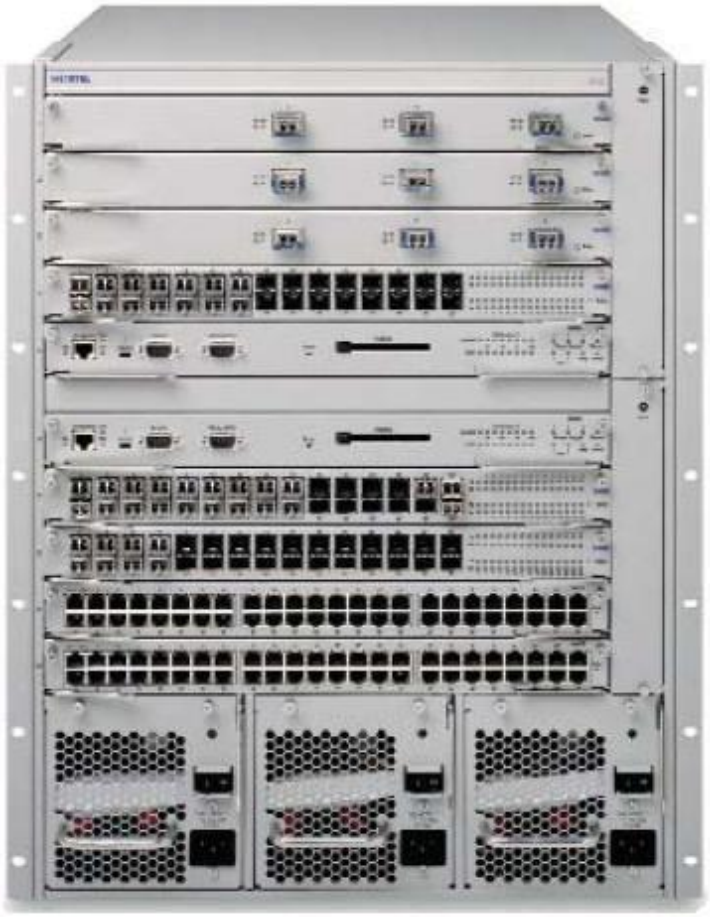
Router (**směrovač**) je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva).

Charakteristika

Netechnicky řečeno, router spojuje dvě sítě a přenáší mezi nimi data. Router se podstatně liší od switche, který spojuje počítače v místní síti. Rozdílné funkce routerů a switchů si lze představit jako switche coby silnice spojující všechna města ve státě a routery coby hraniční přechody spojující různé země.

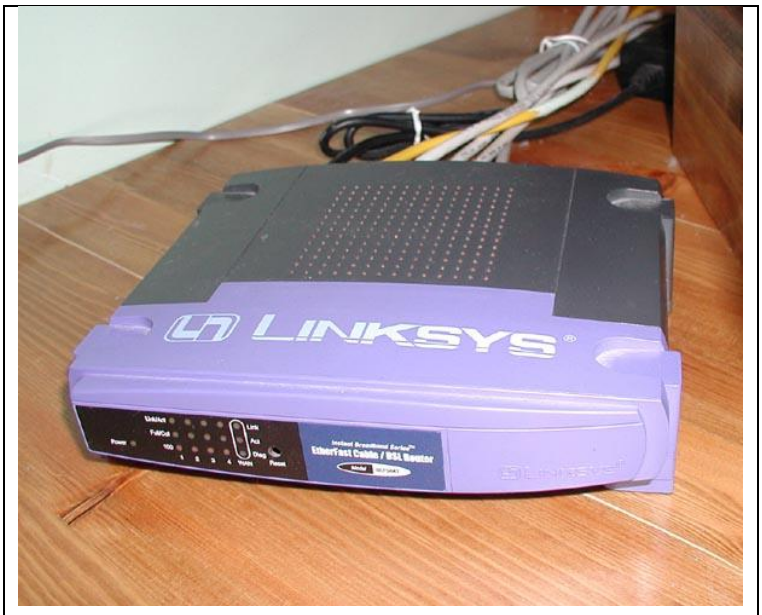
Routování je většinou spojováno s protokolem IP, ačkoliv se stále používají i jiné, méně populární protokoly.

Obecně jako router může sloužit jakýkoliv počítač s podporou síťování a pro routování v menších sítích se často dodnes používají běžné osobní počítače, do vysokorychlostních sítí jsou však jako routery používány vysoce účelové počítače obvykle se speciálním hardwarem, optimalizovaným jak pro běžné přeposílání (forwarding) datagramů, tak pro specializované funkce jako šifrování u IPsec tunelů.



Router Avaya

Jiné změny také zlepšují spolehlivost. Například používání stejnosměrného napájení (které se může v datových centrech odebírat z baterií) místo napájení přímo ze sítě, používání flash pamětí místo pevných disků. Velké moderní routery se tak podobají spíše telefonním ústřednám, jejichž technologie k routerům (vzhledem ke stále častějšímu nasazování protokolu IP i ke spojování hovorů) konverguje a které routery případně nahradí, zatímco malé routery, kombinované například s kabelovými nebo DSL modemy, eventuálně WiFi přístupovými body, se stávají běžným vybavením domácností.



NAT router značky Linksys, používaný pro domácí a malé kancelářské sítě

Router se používá ke spojení alespoň dvou sítí. Speciálním případem je „jednoruký" router, který používá jednu zásuvku (port) a routuje pakety mezi virtuálními sítěmi VLAN provozovanými na této zásuvce.

V mobilních ad-hoc sítích si každý počítač routuje a forwarduje sám, zatímco v metalických a optických sítích je obvykle jen jeden router pro celou broadcastovou doménu.

Routeru, který připojuje klienty k vnější síti (typicky Internetu), se říká „okrajový router" (***edge router***, někdy též „brána" – ***gateway***, což je zastaralé označení pro routery obecně). Router přenášející data mezi jinými routery se

nazývá „vnitřní router" (***core router***). Router používá ***routovací (směrovací) tabulku***, která obsahuje nejlepší cesty do cílovýxh sítí a ***routovací (směrovací) metriky*** spojené s těmito cestami.
Routery se nyní vyrábějí také jako „**internetové brány**", primárně pro malé sítě jako ty, používané doma a v malých kancelářích. Používají se hlavě tam, kde je internetové připojení rychlé a „vždy připojené", jako kabelový modem nebo DSL. Tato zařízení ale nejsou v principu routery, protože počítače ve vnitřní síti efektivně skrývají pod svoji vlastní IP adresu ve vnější síti. Tato technika se nazývá **NAT** (*network address translation*, překlad adres).
Výrobců routerů je mnoho, patří mezi ně: 3Com, Alcatel, Cisco Systems, Juniper Networks, NETGEAR, Nortel, SMC Networks.
S vhodným softwarem se i z obyčejného osobního počítače dá udělat router:

- Sdílení internetového připojení ve Windows XP
- Mac OS X Internet Sharing
- BIRD Internet Routing Daemon (bird.network.cz)
- fdgw (www.fml.org/software/fdgw/)
- CoyoteLinux (www.coyotelinux.com)
- FREESCO (www.freesco.org)
- GNU Zebra (www.zebra.org) – open source implementace routovacích protokolů RIP, OSPF a BGP
- Quagga (www.quagga.net) – open source implementace routovacích protokolů RIP, OSPF a BGP (pokračovatel Zebry)
- IPCop (www.ipcop.org)
- SmoothWall (smoothwall.org)
- The Linux Router Project
- m0n0wall (m0n0.ch/wall)
- FreeBSD (www.freebsd.org)
- NetBSD (www.netbsd.org)
- OpenBSD (www.openbsd.org)
- MikroTik (www.mikrotik.org) - funguje ako AP

NAT (Network address translation)

Network Address Translation (**NAT**, česky *překlad síťových adres*, také **Network Masquerading** (*síťová maškaráda*), **Native Address Translation** (*nativní překlad adres*) nebo **IP Masquerading** (*IP Maškaráda*)) je způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů. K tomu patří i změna kontrolního součtu (u IP i TCP/UDP), aby změny byly brány v úvahu.
NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou (viz gateway). NAT ovšem může způsobit problémy v komunikaci mezi klienty a snížit rychlost přenosu.
Vznikl jako důsledek omezeného počtu veřejných IP adres (IPv4 má 32 bitů a část z nich je navíc rezervována pro speciální účely). Každý uživatel dnešního internetu nemůže mít adresu z vnějšího rozsahu, NAT umožňuje celou vnitřní síť ukrýt za adresu jedinou.
V typické konfiguraci používá lokální síť některý z rozsahů IP adres (192.168.x.x, 172.16.x.x-172.31.x.x a 10.x.x.x). Router má přidělenu soukromou adresu, ale také je spojen s Internetem, buď jedinou veřejnou adresou (overloaded NAT), nebo několika veřejnými adresami, přidělenými poskytovatelem připojení k Internetu (Internet Service Provider). Jakmile jde paket z lokální sítě do Internetu, je jeho zdrojová adresa (soukromá) přeložena na veřejnou.

Router si uchovává základní data o každém aktivním spojení (adresu cíle, port). Když se vrátí odpověď na router, využije data získaná při odchozí fázi a určí kam na vnitřní síť je třeba odpověď zaslat. Pro systém na Internetu se jeví router jako zdroj i cíl komunikace.

Výhody.

Pakety posílané protokoly TCP a UDP obsahují kontrolní součet zahrnující i hlavičku s adresami, tudíž je třeba kromě přepsání IP adres také přepočítat kontrolní součet pro IP adresu novou. NAT zvyšuje bezpečnost počítačů za ním připojených (útočník nezná strukturu sítě a nemůže se spojit přímo s konkrétním počítačem). NAT ovšem firewall nenahrazuje a existují způsoby, jak počítače za NATem napadnout.

Omezení.

Některé protokoly aplikační vrstvy (např. FTP nebo SIP) odesílají včetně dat i síťové adresy. Např. FTP v aktivním módu používá jedno připojení pro data a jedno pro samotné příkazy. Iniciátor datového přenosu na počátku identifikuje příslušné datové spojení z adres jeho síťové a transportní vrstvy. Jestliže iniciátor přenosu leží za jednoduchým NAT firewallem, tak překlad IP adresy a/nebo čísla TCP portu vrátí ze serveru nesprávné informace.

Podobně tak SIP ovládá mnoho VoIP hovorů a trpí stejným problémem. SIP a SDP mohou využívat více spojení a posílat hlasový proud přes RTP. IP adresy a čísla portů jsou zakódovány v přenášených datech a musí být známy před tím, než překročí NAT. Bez speciálních technik jako je STUN, je chování NATu nepředvídatelné a komunikace tak může často selhávat.

Směrovače (routery) v sítích WAN

Routery jsou vlastně specifickým typem počítačů, obsahují stejné základní komponenty jako standardní PC ale vykonávají specifickou funkci.

Routery obsahují: CPU, paměť, systémovou sběrnici a různá vstupně – výstupní rozhraní

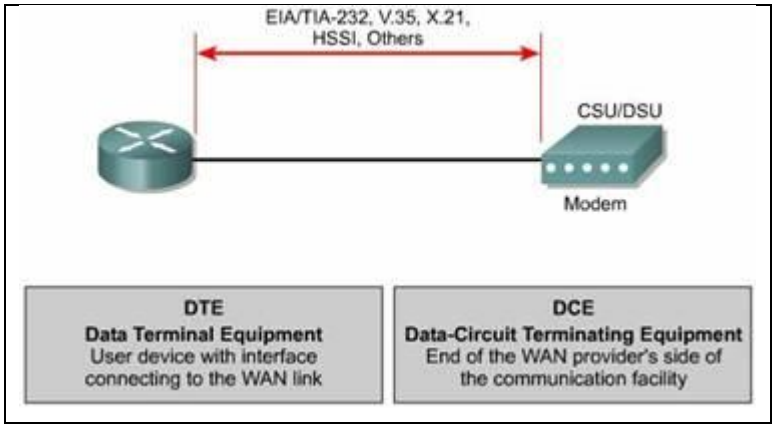
Funkce: propojují sítě, určují nejlepší cestu dat

Routery této kategorie mají WAN i LAN rozhraní. **Pracují na 3. vrstvě OSI modelu**, vytvářejí rozhodnutí na základě síťové (IP) adresy. Funkcí routeru je stavba směrovacích tabulek, výměna síťových informací s ostatními routery, určování nejlepší cesty při přepínání rámce.

Funkce routeru ve WAN síti.

Standardní protokoly používané ve WAN na 1. a 2. vrstvě **jsou jiné než v LAN** na stejné vrstvě.

Fyzická vrstva popisuje propojení mezi Data Terminal Equipment (DTE) a Data Circuit-terminating Equipment (DCE). Zpravidla DCE je zařízení poskytovatele služby (ISP) a DTE je zařízení uživatele, které se připojuje. DTE je schopné komunikovat jen s DCE zařízením, DCE (modem) určuje hodiny.



Jednou z úloh routeru ve WAN síti je směrování paketů na 3. vrstvě, to je stejné jako v LAN. Když router používá fyzickou a linkovou vrstvu s protokoly, které jsou určené pro WAN, pracuje jako WAN zařízení.

Primární úlohou routeru je poskytovat propojení na a mezi různými WAN fyzickými a linkovými standardy.

1. Fyzická vrstva sítí WAN

WAN fyzické standardy: (představují mechanické a elektrické parametry připojovacích konektorů)

EIA/TIA-232, EIA/TIA-449

V.24, V.35, X.21

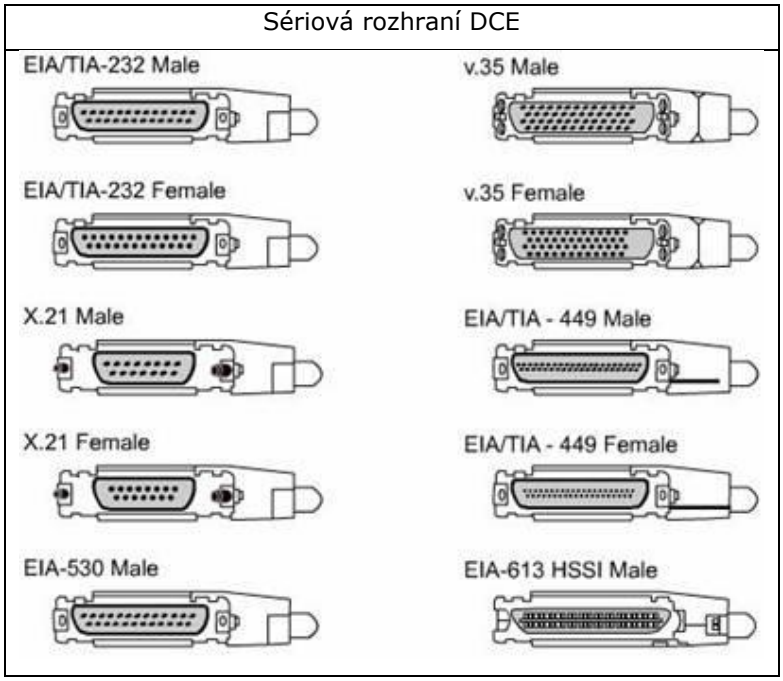
G.703

EIA-530

ISDN, T1, T3, E1, and E3

xDSL

SONET (OC-3, OC-12, OC-48, OC-192)

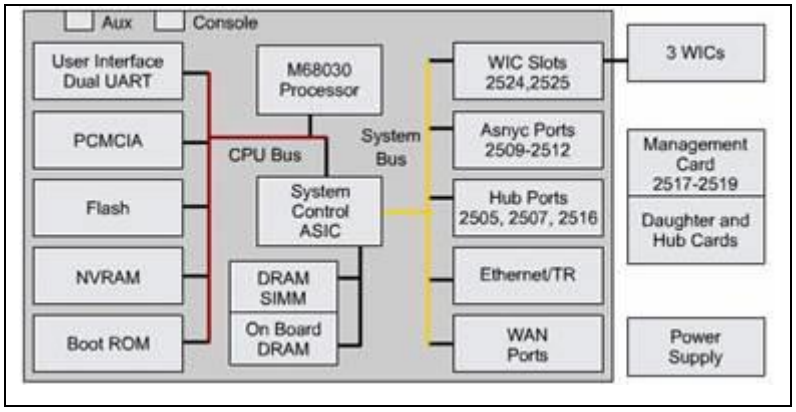


2. Linková vrstva sítí WAN

WAN linkové protokoly a standardy:

High-level data link control (HDLC), Frame Relay, Point-to-Point Protocol (PPP), Synchronous Data Link Control (SDLC), Serial Line Internet Protocol (SLIP), X.25, ATM, LAPB, LAPD, LAPF

Vnitřní komponenty routeru



Komponenty routeru:

- CPU – The Central Processing Unit, vykonává instrukce v operačním systému, je to mikroprocesor, větší routery mohou mít více CPU
- RAM (DRAM) – Random-access memory, je používaná pro směrovací tabulky, rychlou přepínací cache, směrovací konfigurace, vyrovnávací paměť pro IOS, při výpadku napájení se smaže, rozšiřuje se přes DIMMy.
- FLASH, pro uložení CISCO IOSu (obrazu OS). Router normálně načítá IOS z FLASH paměti. Obraz OS může být obnoven nahráním novější verze. Obraz OS může byť komprimovaný nebo nekomprimovaný. Přidáním nebo nahrazením flash paměti SIMMy nebo PCMCIA kartou, se dá rozšířit velikost flash paměti.
- NVRAM – Nonvolatile random-access memory, používaná na uložení spouštěcí konfigurace, vypnutím se nemaže.
- Sběrnice, dělíme na systémovou a CPU sběrnici. Systémová sběrnice slouží na komunikaci mezi CPU a rozhraními případně rozšiřujícími sloty. CPU sběrnice komunikuje s pamětí.
- ROM – Read-only memory, je použitá pro trvalé uložení spouštěcího diagnostického kódu. Hlavní úloha je hardwarová diagnostika v době spuštění routeru a nahrání IOS z flash paměti do RAM. Některé routery mají omezenou verzi IOSu, která může být použita jako alternativní bootovací zdroj. ROM se nedá smazat.

Upgrade ROM se provádí výměnou čipu.

- rozhraní: **LAN -** Ethernet alebo Token-Ring
  WAN - sériové, ISDN, integrované CSU
  (LAN i WAN rozhraní buď pevná konfigurace, nebo modulární)
  Console/AUX - sériový, na inicializaci routeru, (AUX pro připojení modemu)
- napájecí zdroj, napájí všechny komponenty routeru

Console port a konektorové piny

Použijeme RJ-45-na-RJ-45 rollover kabel a RJ-45-na-DB-9 female DTE adaptér (označený TERMINAL) k připojení console portu do PC, s běžícím emulačním terminálovým softwarem (Hyperterminal). Tabulka zobrazuje signály a piny asynchronního sériového console portu, RJ-45-na-RJ-45 rollover kabelu, a RJ-45-na-DB-9 female DTE adaptéru (označeného TERMINAL).

[1] Pin 1 je připojen uvnitř konektoru na pin 8.

Tabulka signálů Console portu, kabelů a DB-9 adaptéru

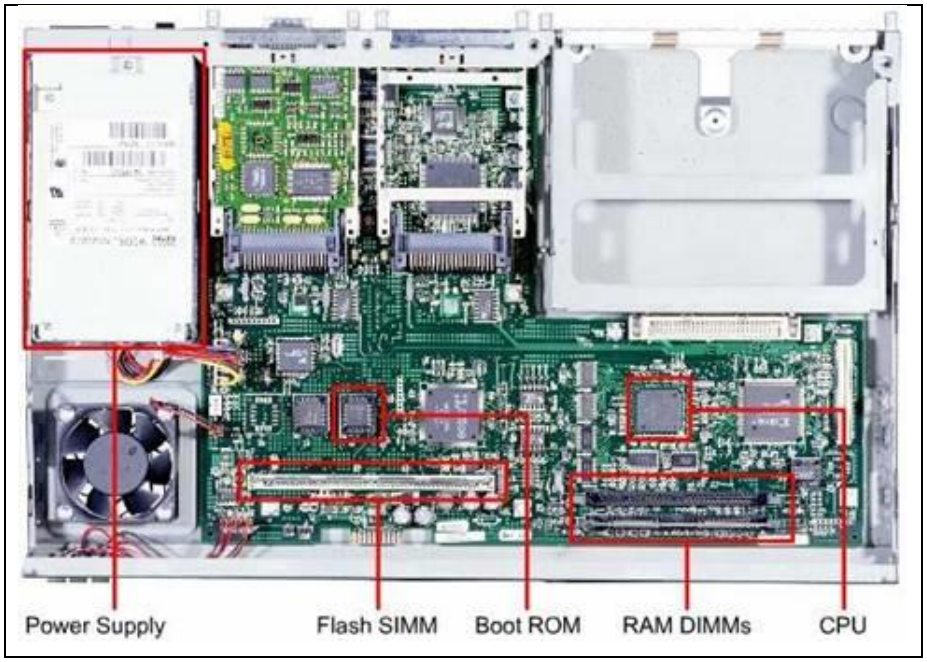
Console port (DTE)	RJ45 na RJ45 Rollover kabel		RJ45 na DB9 Terminal adaptér	PC konzole
Signál	RJ-45 Piny	RJ-45 Piny	DB-9 Pin	Signál
RTS	1[1]	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8[1]	1	7	RTS

Auxiliary port a konektorové piny

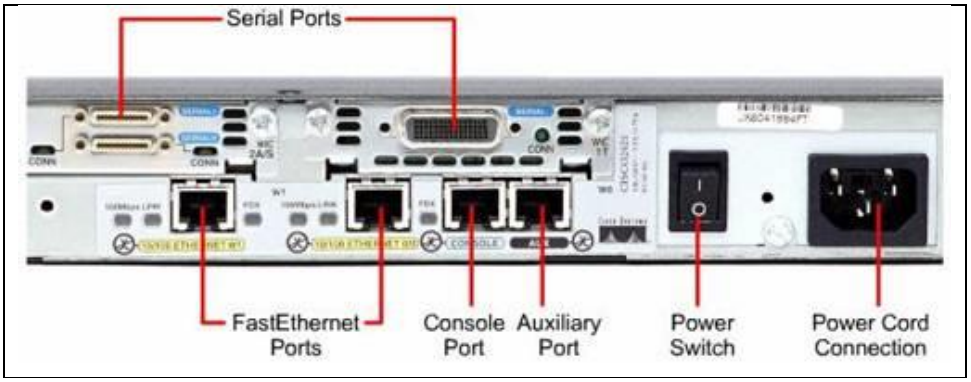
Použijeme RJ-45-na-RJ-45 rollover kabel a RJ-45-na-DB-25 male DCE adaptér (označený MODEM) k připojení auxiliary portu na modem. Tabulka zobrazuje signály a piny asynchronního sériového auxiliary portu, RJ-45-RJ-45 rollover kabelu, a RJ-45-DB-25 male DCE adaptéru (označeného MODEM).

Tabulka signálů Auxiliary portu, kabelů a DB-25 adaptéru				
AUX Port (DTE)	**RJ-45-na-RJ-45 Rollover Cable**		**RJ-45-na-DB-25 Modem Adapter**	**Modem (DCE)**
Signál	**RJ-45 Pin**	**RJ-45 Pin**	**DB-25 Pin**	**Signál**
RTS	1	8	4	RTS
DTR	2	7	20	DTR
TxD	3	6	3	TxD
GND	4	5	7	GND
GND	5	4	7	GND
RxD	6	3	2	RxD
DSR	7	2	8	DCD
CTS	8	1	5	CTS

Vnitřní uspořádání routeru:

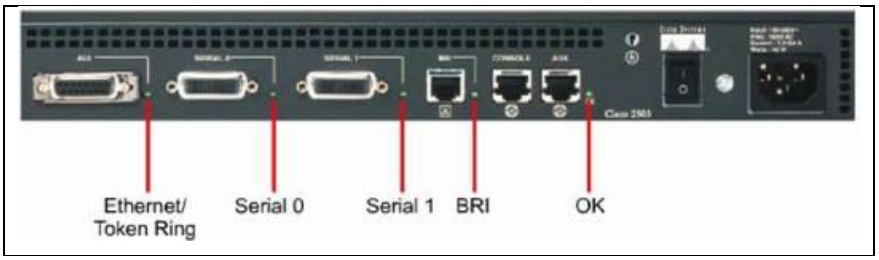


Zadní strana routeru – uspořádání konektorů:



Indikace stavů směrovače.

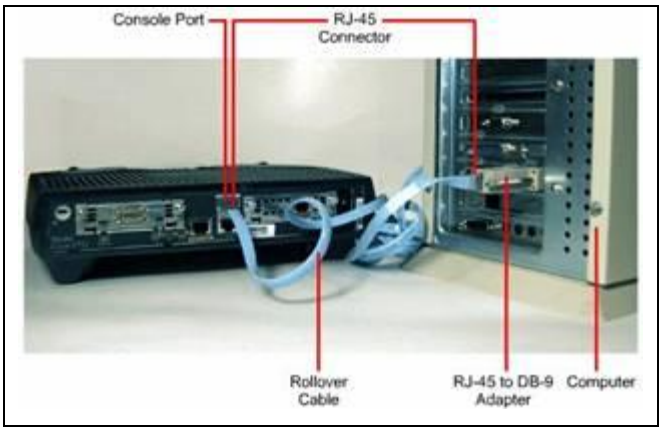
LED na panelu indikují aktivitu na příslušném rozhraní. Když svítí zelená OK LED, systém je zavedený správně.



Připojení k routeru pomocí konzole

Řídící porty:

- konzolový port, doporučený pro inicializaci, připojuje se na sériový port PC
- AUX, pro dálkovou správu přes modem



Nejsou navržené jako síťové porty, jeden z nich je potřebný pro inicializační konfiguraci routeru. Po prvním zapnutí není router nakonfigurovaný, proto se připojuje přes RS232 k ASCII terminálu nebo počítačovému terminálu. Konzolový port může být též použitý při řešení problémů, router vypisuje všechny úkony pri spouštění, případně při změně hesla ke správě.

Připojení konzolového rozhraní

Připojení je realizované přes konzolový port a rollover kabel, obsahující konektor RJ45 a DB9.
Terminál musí podporovat VT100 emulaci.
Připojení na router:

1. konfigurace terminálu:
   - přidělit com port (COM1,…)
   - nastavit rychlost přenosu 9600 baud
   - nastavit 8 datových bitů
   - nastavit žádná parita
   - nastavit 1 stop bit
   - nastavit žádné řízení toku
2. připojit konektor RJ45 rollover kabelu do routeru na konzolový port
3. (připojit konektor RJ45 adaptéru na rollover kabel)
4. zapojit DB9 konektor (adaptéru) do PC

Připojení LAN rozhraní

Router komunikuje s LAN přes HUB nebo SWITCH. Na připojení se používá přímý kabel. V některých typech Ethernetového připojení je router připojený přímo na PC nebo na jiný router, zde se používá překřížený kabel.

Připojení k WAN rozhraní

WAN připojení je realizované na velké vzdálenosti různými typy technologií. Tyto WAN služby jsou vždy pronajaté od servisního poskytovatele.

Pro každý typ WAN služby - customer premises equipment (CPE), často router, je data terminal equipment (DTE). Na poskytovatele služeb se připojujeme přes DTE.

Pro lepší rozlišení portů je zavedeno barevné provedení kabelů podle doporučení firmy CISCO. (viz tabulka)

Port or Connection	Port Type	Color	Connected To	Cable
Ethernet	RJ-45	yellow	Ethernet hub or Ethernet switch	Straight-through
T1/E1 WAN	RJ-48C/ CA81A	light green	T1 or E1 network	RJ-48 T1
Console	8 pin	light blue	Computer com port	Rollover
AUX	8 pin	black	Modem	Rollover
BRI S/T	RJ-48C/ CA81A	orange	NT1 device or private integrated network exchange (PINX)	RJ-48
BRI U WAN	RJ-49C/ CA11A	orange	ISDN network	RJ-49
Token	UTP, STP	purple	Token Ring device	RJ-45 Token Ring cable

Gateway (brána)

Gateway (brána) je v počítačových sítích uzel, který spojuje dvě sítě s odlišnými protokoly. Brána musí vykonávat i funkci routeru (směrovače), a proto ji řadíme v posloupnosti síťových zařízení výše. Brána například přijme z Internetu pomocí webové stránky zprávu, kterou odešle do mobilní GSM sítě v podobě SMS zprávy.

Pojem **default gateway** (implicitní brána) označuje router (směrovač), přes který se stanice dostanou do vnější sítě (tj. obvykle do Internetu). Oba významy jsou často nesprávně zaměňovány.

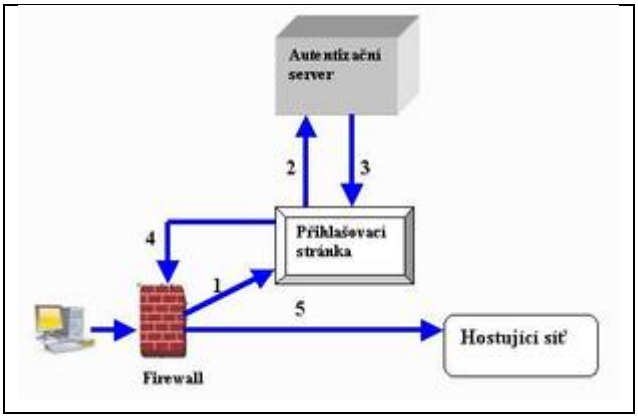
Funkce brány

- **První typem brány** je brána pracující na ***aplikační úrovni*** (viz Referenční model ISO/OSI). Kromě výše zmíněného příkladu propojení GSM sítě a Internetu to jsou i brány mezi různými sítěmi pro zasílání zpráv (ICQ, Jabber, …) a podobně. Brána přijme celou zprávu, která se může skládat z mnoha menších částí (např. datagramů). Pak zprávu převede do formátu určeného pro cílovou síť a odešle. Bránu tak tvoří speciální program spuštěný na počítači, který je připojen do obou různých sítí (tj. například do Internetu pomocí síťové karty a do GSM sítě pomocí mobilního telefonu připojeného přes sériový port).
- **Druhým typem brány** je brána pracující na ***transportní*** nebo ***síťové vrstvě***. Tyto brány pracují na nižší síťové vrstvě, například přímo s datagramy. V tomto případě brána nedekóduje celou zprávu, ale jen transformuje datagramy jedné sítě do datagramů sítě druhé. Příkladem je tzv. SOCKS, kde dochází k přenosu datagramů TCP/IP přes síť, která TCP/IP nepodporuje. V takovém případě TCP/IP aplikace používá speciální subsystém, který zajistí doručení datagramů až k bráně pomocí jiného protokolu (např. IPX/SPX) a v bráně probíhá zpětný převod do protokolu TCP/IP a odeslání do cílového místa v Internetu. Převod pracuje samozřejmě oběma směry.

Povolení přístupu pomocí brány

Autentizace přes webové rozhraní:

1. klient je vyzván k zadání přihlašovacích údajů
2. stránka odešle údaje na autentizační server
3. autentizační server odpoví, zda je uživatel známý nebo ne
4. pro oprávněného uživatele je firewall otevřen
5. klient bez omezení komunikuje

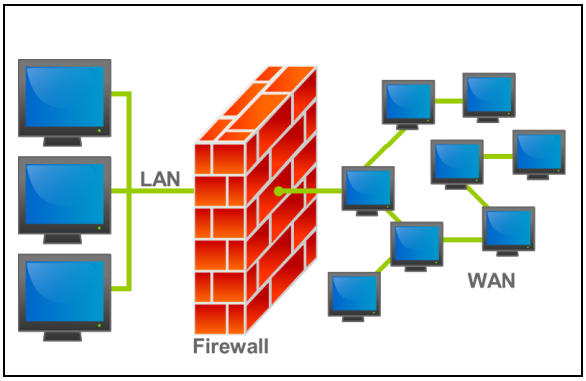


Některé počítačové sítě se chrání proti přímému přístupu cizích počítačů. Přinese-li si někdo do takové sítě notebook, musel by si nejprve zdlouhavě zajistit administrativní povolení, svůj počítač složitě konfigurovat (viz IEEE 802.1X), instalovat doplňující software a podobně. Z tohoto důvodu může být přístup ke zdrojům takové sítě omezen pomocí speciální brány.

Připojí-li se do sítě neznámý počítač (neznámá IP adresa, MAC adresa a podobně), je veškerý jeho provoz přesměrován na bránu (např. pomocí VLAN). Ve spolupráci s webovým prohlížečem, který je dnes součástí výbavy většiny počítačů, umožní brána na základě znalosti uživatelského jména a hesla autentizaci. Po úspěšné autentizaci zajistí brána rekonfiguraci síťových prvků, které odblokují přístup připojeného počítače.

Firewall

Firewall je síťové zařízení hlídající provoz mezi lokální sítí (LAN) a „zbytkem světa" (WAN), které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné – modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS.



Firewally se během svého vývoje řadily zhruba do následujících kategorií:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS

Paketové filtry

Nejjednodušší a nejstarší forma firewallování, která spočívá v tom, že pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket, tj. **kontrola se provádí na třetí a čtvrté vrstvě modelu síťové komunikace OSI.**

Výhodou tohoto řešení je vysoká rychlost zpracování, proto se ještě i dnes používají na místech, kde není potřebná přesnost nebo důkladnější analýza procházejících dat, ale spíš jde o vysokorychlostní přenosy velkých množství dat.

Nevýhodou je nízká úroveň kontroly procházejících spojení, která zejména u složitějších protokolů (např. FTP, video/audio streaming, RPC apod.) nejen nedostačuje ke kontrole vlastního spojení, ale pro umožnění takového

spojení vyžaduje otevřít i porty a směry spojení, které mohou být využity jinými protokoly, než bezpečnostní správce zamýšlel povolit.

Aplikační brány

Jen o málo později, než jednoduché paketové filtry, byly postaveny firewally, které na rozdíl od paketových filtrů zcela oddělily sítě, mezi které byly postaveny. Říká se jim většinou *Aplikační brány*, někdy také *Proxy firewally*. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. **Kontrola se provádí na sedmé (aplikační) vrstvě síťového modelu OSI** (proto se těmto firewallům říká aplikační brány).

Jedním vedlejším efektem použití aplikační brány je, že server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

Výhodou tohoto řešení je poměrně vysoké zabezpečení známých protokolů.

Nevýhodou je zejména vysoká náročnost na použitý HW – aplikační brány jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti, než paketové filtry a mají mnohem vyšší latenci. Každý protokol vyžaduje napsání specializované proxy, nebo využití tzv. generické proxy, která ale není o nic bezpečnější, než využití paketového filtru. Většina aplikačních bran proto uměla kontrolovat jen několik málo protokolů (obyčejně kolem deseti). Původní aplikační brány navíc vyžadovaly, aby klient uměl s aplikační branou komunikovat a neuměly dost dobře chránit svůj vlastní operační systém; tyto nedostatky se postupně odstraňovaly, ale po nástupu stavových paketových filtrů se vývoj většiny aplikačních bran postupně zastavil a ty přeživší se dnes používají už jen ve velmi specializovaných nasazeních.

Stavové paketové filtry

Stavové paketové filtry provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody – jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá.

Například pro FTP tedy stačí nastavit pravidlo, ve kterém povolíte klientu připojení na server pomocí FTP a protože se jedná o známý protokol, firewall sám povolí navázání řídícího spojení z klienta na port 21 serveru, odpovědi z portu 21 serveru na klientem použitý zdrojový port a po příkazu, který vyžaduje přenos dat, povolí navázání datového spojení z portu 20 serveru na klienta na port, který si klient se serverem dohodli v rámci řídícího spojení a pochopitelně i odpovědní pakety z klienta zpět na port 20 serveru.

Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro bezstavové protokoly, jako např. UDP a ICMP.

K největším **výhodám** stavových paketových filtrů patří jejich vysoká rychlost, poměrně slušná úroveň zabezpečení a ve srovnání s výše zmíněnými aplikačními branami a jednoduchými paketovými filtry řádově mnohonásobně snazší konfigurace – a díky zjednodušení konfigurace i nižší pravděpodobnost chybného nastavení pravidel obsluhou.

Nevýhodou je obecně nižší bezpečnost, než poskytují aplikační brány.

Stavové paketové filtry s kontrolou protokolů a IDS

Moderní stavové paketové filtry kromě informací o stavu spojení a schopnosti dynamicky otevírat porty pro různá řídící a datová spojení složitějších známých protokolů implementují něco, co se v marketingové terminologii růz-

ných společností nazývá nejčastěji *Deep Inspection* nebo *Application Intelligence*. Znamená to, že firewally jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů i aplikací. Mohou tak například zakázat průchod http spojení, v němž objeví indikátory, že se nejedná o požadavek na WWW server, ale tunelování jiného protokolu, což často využívají klienti P2P sítí (ICQ, gnutella, napster, apod.), nebo když data v hlavičce e-mailu nesplňují požadavky RFC apod.

Nejnověji se do firewallů integrují tzv. *in-line* ***IDS* (*Intrusion Detection Systems*** – systémy pro detekci útoků). Tyto systémy pracují podobně jako antiviry a pomocí databáze signatur a heuristické analýzy jsou schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

Výhodou těchto systémů je vysoká úroveň bezpečnosti kontroly procházejících protokolů při zachování relativně snadné konfigurace, poměrně vysoká rychlost kontroly ve srovnání s aplikačními branami, nicméně je znát významné zpomalení (zhruba o třetinu až polovinu) proti stavovým paketovým filtrům.

Nevýhodou je zejména to, že z hlediska bezpečnosti designu je základním pravidlem bezpečnosti udržovat bezpečnostní systémy co nejjednodušší a nejmenší. Tyto typy firewallů integrují obrovské množství funkcionality a zvyšují tak pravděpodobnost, že v některé části jejich kódu bude zneužitelná chyba, která povede ke kompromitování celého systému.

Bezpečnostní politika

Nastavení pravidel pro komunikaci přes firewall se běžně označuje termínem „bezpečnostní politika firewallu", zkráceně „bezpečnostní politika". Bezpečnostní politika zahrnuje nejen samotná pravidla komunikace mezi sítěmi, ale u většiny dnešních produktů také různá globální nastavení, překlady adres (NAT), instrukce pro vytváření šifrovaných spojení mezi šifrovacími branami (VPN – Virtual Private Networks), vyhledávání možných útoků a protokolových anomálií (IDS – Intrusion Detection Systems), autentizaci a někdy i autorizaci uživatelů a správu šířky přenosového pásma (bandwidth management).

Standardy IEEE 802.

IEEE 802 je rodina IEEE standardů pojednávajících o sítích LAN a MAN.

- IEEE 802.1 Bridge and Network Management
--- IEEE 802.1AE - MAC Security
--- IEEE 802.1Q - VLAN
--- IEEE 802.1X - Network Access Control
--- IEEE 802.1aq - Shortest Path Bridging (SPB)
- IEEE 802.2 - LLC - Logical Link Control
- IEEE 802.3 – Ethernet (kabelové sítě)
- IEEE 802.4 - Token Bus
- IEEE 802.5 - Token Ring
- IEEE 802.11 - Wi-Fi
- IEEE 802.12 demand priority access method
- IEEE 802.13 Kabeláž kat.6 - 10Gb lan
- IEEE 802.15 Wireless PAN
--- IEEE 802.15.1 Bluetooth
--- IEEE 802.15.4 ZigBee
- IEEE 802.16 Broadband Wireless Access WiMAX
--- IEEE 802.16e (Mobile) Broadband Wireless Access
- IEEE 802.17 Resilient packet ring
- IEEE 802.18 Radio Regulatory TAG
- IEEE 802.19 Coexistence TAG
- IEEE 802.20 Mobile Broadband Wireless Access
- IEEE 802.21 Media Independent Handoff
- IEEE 802.22 Wireless Regional Area Network

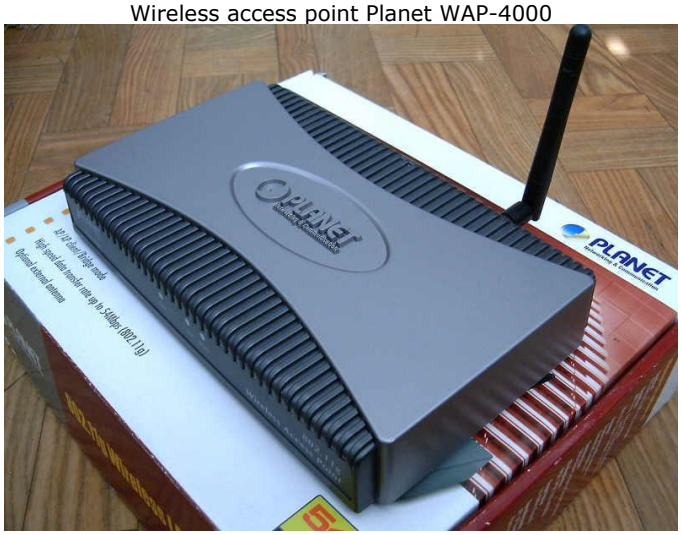
Zařízení WiFi podle standardů IEEE 802.11

Zařízení WiFi jsou běžně označována názvy standardů, které mimo jiné určují jejich maximální přenosové rychlosti. Reálně je dosahováno nižší rychlosti (viz tabulka):

Standard	Frekvence	Max. propustnost	Typ. Propustnost	Dosah (uvnitř)	Dosah (venku)
IEEE 802.11a	5 GHz	54 Mbit/s	23 Mbit/s	~35 m	~120 m
IEEE 802.11b	2,4 GHz	11 Mbit/s	4,3 Mbit/s	~38 m	~140 m
IEEE 802.11g	2,4 GHz	54 Mbit/s	19 Mbit/s	~38 m	~140 m
IEEE 802.11n	2,4 nebo 5 GHz	270 Mbit/s (duálně)	74 Mbit/s	~70 m	~250 m
IEEE 802.11y	3,7 GHz	54 Mbit/s	23 Mbit/s	~50 m	~5000 m

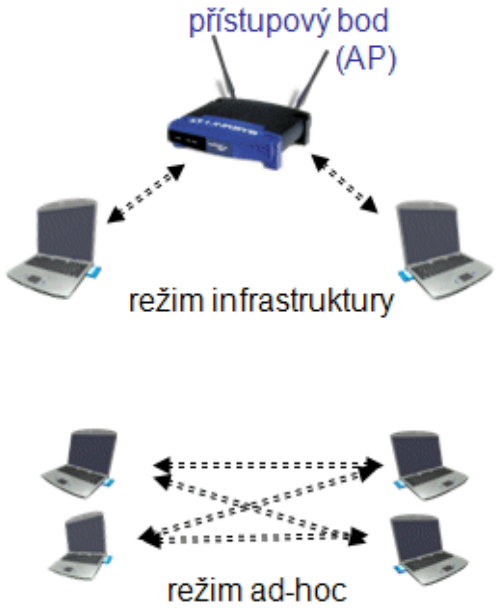
Přístupový bod - Access point

Wireless access point Planet WAP-4000



Access point (AP) k bezdrátové Wi-Fi síti je zařízení, ke kterému se klienti připojují. Klienti se k přístupovému bodu připojují (**asociují** se), přičemž mohou být vůči nim uplatněna omezení a přístup odepřen. Komunikace mezi klienty probíhá prostřednictvím přístupového bodu, tj. minimálně dva skoky (nejprve na přístupový bod a z něj pak na příslušnou protistanici). Klient tak udržuje spojení jen s přístupovým bodem a nemusí mít cílovou stanici ani v přímém rádiovém dosahu. Přístupový bod může rozpoznat, zda klient přešel do úsporného režimu a do jeho probuzení dočasně uchovat přicházející data, což může vést k úsporám výdrže baterií klienta. Centralizovaný způsob komunikace též umožňuje použití směrových antén, které zvyšují dosah rádiového signálu. Tento typ uspořádání nazýváme ***infrastrukturní síť***. Opakem jsou **ad-hoc** sítě, kde jsou dva nebo více klientů ve vzájemném přímém rádiovém spojení (bez existence prostředníka).

Představa režimů infrastruktury a ad-hoc u Wi-Fi



Přístupový bod je obvykle realizován malým jednoúčelovým zařízením, ale s potřebnou softwarovou výbavou se jím může stát i jakýkoliv počítač s bezdrátovým Wi-Fi zařízením. Některá z těchto jednoúčelových zařízení využívají jako základ operační systém Linux.

AP může poskytovat vlastní DHCP server, také může poskytovat NAT (překlad veřejných IP adres na soukromé a opačně - maškaráda), předávání portů do vnitřní sítě (port forwarding), autentizaci klientů proti RADIUS serveru, různé úrovně šifrování (viz níže) a podobně. Některé chybějící vlastnosti lze nahradit vhodně umístěným doplňujícím počítačem nebo dalším jednoúčelovým zařízením (router).

Autentizace a asociace u Wi-Fi

Drátové lokální sítě na bázi Ethernetu mají zajímavou přednost v tom, že u nich je už pouhým propojení (vedením kabelů) pevně a jednoznačně dána vazba mezi koncovými uzly a rozbočovači. Případně mezi dvěma koncovými uzly, u přímého propojení.

U bezdrátových sítí Wi-Fi je ale všechno jinak. Zde je vazba mezi koncovými stanicemi a přístupovým bodem podstatně volnější a také dynamická, protože se může měnit v čase. (stanice se mohou pohybovat).

Přístupové body Wi-Fi jsou za tímto účelem vybaveny řadou služeb, mezi které patří (mimo jiné) schopnost:

asociace: v rámci této funkce dochází ke vzniku logické vazby mezi přístupovým bodem a konkrétní stanicí. Stanice je „přidružena" (tzv. asociována) k danému přístupovému bodu.

de-asociace: opak asociace, dochází k uvolnění (zrušení) vazby mezi přístupovým bodem a koncovou stanicí.

autentizace: v rámci této funkce přístupový bod zjišťuje, o jakou stanici jde, resp. zda je skutečně tím, za koho se vydává.

Službu asociace si lze s trochou fantazie představit jako analogii propojení rozbočovače a koncového uzlu pomocí vhodného kabelu, a službu deasociace naopak jako rozpojení takovéhoto kabelu. Jen místo fyzické manipulace s kabely jsou tyto funkce realizovány na logické úrovni.

Dalším rozdílem je pak to, že u fyzického propojení, pomocí kabelů, se o oprávněnosti provést takové propojení rozhoduje také „fyzicky", a lze jej účinně a efektivně blokovat zamezením přístupu k příslušným technickým prostředkům (například uzamknutím příslušné rozvodové skříně apod.).

U bezdrátových sítí je to opět komplikovanější, neboť vše se musí řešit na logické úrovni. Proto se u Wi-Fi sítí setkáme s tím, že přístupové body musí poměrně detailně a důsledně zjišťovat, co jsou zač stanice, které se s nimi chtějí asociovat (spojit a komunikovat). Právě k tomu slouží již zmiňované služby **autentizace**. Ty jsou nejčastěji řešeny dvěma základními způsoby:

1. **otevřenou autentizací** (Open System Authentication): zde se fakticky nezkoumá, co je stanice zač.
2. **autentizaci pomocí sdíleného klíče** (Shared Key Authentication): zde musí stanice prokázat, že vlastní požadovaný klíč (stejný, jaký vlastní přístupový bod, resp. jaký je na něm nastaven, proto „sdílený klíč", anglicky: shared key).

Role přístupových bodů

Přístupové body vystupují v několika různých rolích, které jsou dány nejen požadavky na strukturu sítě, ale i schopnostmi těchto zařízení. I když jsou schopnosti bezdrátových zařízení snadno rozšiřitelné pomocí změny softwarového vybavení, většina výrobců ji neumožňuje. Naopak hardwarově identická zařízení se mohou cenově několikanásobně lišit jen díky existenci jednoduchého softwarového doplňku.

1. **bridge** – bezdrátová síť je součástí sítě LAN
   a) bridge odděluje síťový provoz, ale propouští lokální broadcasty
   b) není nutné konfigurovat
2. **router** – bezdrátová síť je samostatnou podsítí
   a) router odděluje síťový provoz a nepropouští lokální broadcasty
   b) vyžaduje konfiguraci IP adres zařízení a nastavení směrování

Pokud je v bezdrátovém zařízení (AP) zabudována **bezdrátová část dvakrát**, označuje se jako **point-to-multipoint**, protože dokáže např. bezdrátový signál dálkově přijímat a zároveň ho distribuovat dalším bezdrátovým klientům v blízkém okolí. Takto jsou konstruovány bezdrátové přípojné body poskytovatelů internetového připojení (providerů), kteří však někdy kvůli ceně používají dvě samostatná bezdrátová zařízení. Specifickým typem jsou sítě s **WDS** (Wireless Distribution System), kdy všechny přístupové body vysílají na stejném kanálu, navzájem spolu komunikují a jeví se tak klientům jako jedna síť. Výhodou je, že jen jedno AP musí být připojeno k mateřské síti a jednotlivé AP nemusí mít dvě samostatné bezdrátové části, jako u point-to-multipoint. Nevýhodou je pak snižování propustnosti sítě v závislosti na počtu skoků, než se signál, přes jednotlivé AP, dostane do mateřské sítě, protože veškerý provoz se šíří po celé bezdrátové síti na stejném kanálu.

Bezpečnostní rizika

Bezdrátové sítě jsou často bezpečnostně podceňovány a vznikají tak bezpečnostní rizika pro zbytek LAN, ve které se nezabezpečený přístupový bod nachází. Nejčastější chybou je:

1. podcenění dosahu rádiového signálu (pro dálkový příjem stačí, aby jen jedna strana disponovala kvalitní směrovou anténou nebo citlivým přijímačem)
2. neznalost možností nastavení šifrování (většina zařízení je prodávána v nastavení, kdy není použito žádné zabezpečení)
3. použití zastaralého šifrování WEP (WEP je snadno prolomitelný, je nutné použít WPA nebo lépe WPA2)

Nevýhody technologie

- kvalita spojení výrazně klesá při ztrátě přímé viditelnosti klienta na přístupový bod
- omezený počet nepřekrývajících se kanálů způsobuje rušení komunikace u sousedních přístupových bodů

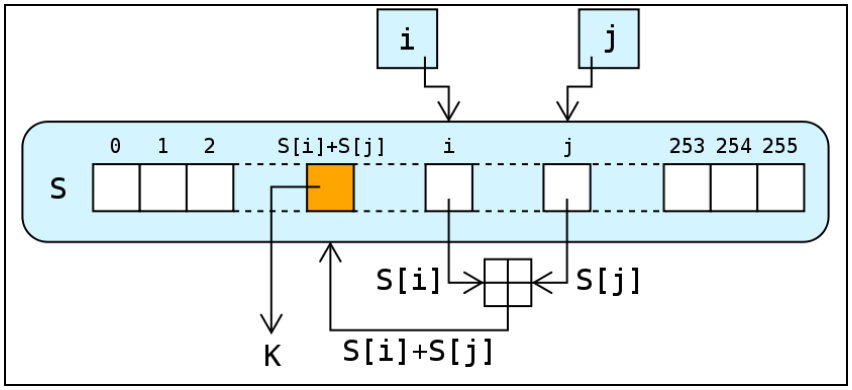
- připojení klienti se dělí o dostupnou šířku pásma, takže s jejich zvyšujícím se počtem klesá i datová propustnost
- vyšší přenosové rychlosti se dosahuje typicky ve směru ke klientovi – pokud klient vysílá, snižuje se dosažitelná propustnost kolizemi, které vznikají na přístupovém bodu, přičemž jejich minimalizaci se snaží zajistit protokol CSMA/CA

WEP šifrování

V bezdrátové počítačové síti pracuje WEP na linkové vrstvě, kde šifruje přenášené rámce pomocí proudové šifry RC4. Šifra RC4 generuje pseudonáhodný proud bajtů (keystream). Stejně jako jiné proudové šifry, používá k šifrování spojení náhodných bajtů spolu s čistým textem (operací XOR) a dešifrování probíhá podobným způsobem, ale inverzně. Ke generování keystreamu používá šifra vnitřní stav, který tvoří:

1. pole bajtů o délce 256 (*S*)
2. dvě celočíselné proměnné (*i* a *j*)

Pole *S* se inicializuje za použití klíče o volitelné délce až 256 bajtů (2048 bitů).



Díky tomu není možné snadno číst odposlechnutý datový provoz přenášený v bezdrátové síti a není nutné měnit stávající síťové aplikace ani přenosové protokoly, protože šifrování je z jejich hlediska transparentní.
Takzvaný 64bitový WEP používá 40bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 64bitový RC4 klíč. Delší 128bitový WEP používá 104bitový klíč, ke kterému je připojen 24bitový inicializační vektor a dohromady tak tvoří 128bitový RC4 klíč. Někteří výrobci bezdrátových zařízení poskytují obdobným způsobem 256bitový WEP. Pro ověření integrity dat používá WEP kontrolní součty CRC-32. Kontrolní součet a CRC se vypočítávají před a po přenosu nebo duplikaci dat s následným porovnáním obou výsledků. CRC je vhodný pro zjišťování chyb vzniklých v důsledku selhání techniky.

WPA šifrování

Kromě rychlé reakce na problémy s WEP bylo též důležitým cílem WPA umožnit využití stávajícího vyráběného hardware, který interně podporoval zabezpečení WEP se šifrou RC4.
Pro eliminaci slabých míst byl vyvinut protokol TKIP (*Temporal Key Integrity Protocol*), který dočasně odstranil problém s inicializačními vektory a zavedl dynamickou správu šifrovacích klíčů, které jsou pomocí něj mezi klientem a přístupovým bodem bezpečně přenášeny nejen na začátku komunikace, ale i během ní. Na straně klienta (počítače připojujícího se k bezdrátové síti) je nasazen tzv. suplikant (prosebník), což je univerzální rezidentní program běžící v pozadí na hlavním procesoru počítače a zajišťující autentizaci klienta a správu šifrovacích klíčů pomocí TKIP.
WPA používá 128bitový šifrovací klíč a 48bitový inicializační vektorem (označován zkratkou *IV*), takže i když používá stejnou šifru jako WEP, odolává lépe útokům, jimiž je WEP napadán.
WPA vylepšuje kontrolu integrity dat (pro snadnou možnost vyřazení poškozených rámců). WEP používá algoritmus CRC-32, který je poměrně jednoduchý a navíc není kontrolní součet součástí zašifrovaných dat, takže je možné pozměnit zprávu a kontrolní součet bez znalosti WEP klíče. WPA používá lepší MAC (*Message Authentication Code*, konkrétně algoritmus nazvaný *Michael*), která je zde nazývána MIC (*Message Integrity Code*).
MIC metoda použitá ve WPA zahrnuje počítadlo rámců, které chrání před útoky snažícími se zopakovat předchozí odposlouchanou komunikaci.

WPA nefunguje v tzv. ad-hoc sítích, ve kterých lze pro zabezpečení použít pouze WEP.

WPA2

WPA2 přidává k TKIP a algoritmu Michael nový algoritmus CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) založený na AES, který je považován za zcela bezpečný. Od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, jež chtějí být certifikována jako Wi-Fi.
Některá zařízení podporují tzv. *Mixed mode*, kdy WLAN Access Point podporuje WPA a současně i WPA2 na jediném WLAN rozhraní, v některých případech umožňuje vytvořit i více, typicky 2 SSID bud přímo pro klienty (například mini router od FON.com - La Fonera, 2x SSID, 2 metody šifrování), v jiných případech např. pro WDS režim, kdy páteř je šifrována nezávisle na klientském signálu (např. Fritz!Box FON, i když obě SSID, páteřní i klientské, musí být shodné, tak každé může mít jinou metodu šifrování či klíče).

Metoda CRC - Cyclic Redundancy Check

je speciální hašovací (hash) funkce, používaná k detekci chyb během přenosu či ukládání dat. Pro svou jednoduchost a dobré matematické vlastnosti jde o velmi rozšířený způsob jiné realizace kontrolního součtu (použití všech bajtů celé zprávy, dokumentu nebo programu a jejich sečtení do jednoho čísla). Kontrolní součet bývá odesílán či ukládán společně s daty, při jejichž přenosu nebo uchovávání by mohlo dojít k chybě. Po převzetí dat je znovu nezávisle spočítán.
Pokud je nezávisle spočítaný kontrolní součet odlišný od přeneseného nebo uloženého, je zřejmé, že při přenosu nebo uchovávání došlo k chybě.
Pokud je shodný, tak téměř jistě k žádné chybě nedošlo.
Metoda cyklické redundance (CRC) postupně používá skupiny bitů a operaci dělení místo sčítání.
V určitých případech je možné chybu pomocí CRC opravit. CRC je vhodný pro zjišťování chyb vzniklých v důsledku selhání techniky, avšak jako metoda pro odhalení záměrné změny dat počítačovými piráty je příliš slabý. V tomto případě je třeba používat speciální hašovací funkce určené pro šifrovací algoritmy.

Základní vlastnosti CRC

• Schopnost detekce chyb záleží na volbě klíče (též generující polynom $G(x)$). Při správné volbě hodnoty mají delší klíče lepší schopnost detekce chyb.
• Číslo za písmeny CRC určuje stupeň řídícího polynomu, např. CRC16 je kontrolní součet typu CRC s řídícím polynomem stupně 16 (nejvyšší mocnina x je x^{16}). Při uvádění číselných hodnot kontrolních polynomů se často zanedbává nejvyšší bit, protože má vždy hodnotu 1.
• Určení CRC pouze řídícím polynomem je nejednoznačné, protože různé algoritmy mohou vytvářet vstupní bitové posloupnosti různým způsobem. Z různých historických a technických důvodů může při výpočtu docházet například ke změně pořadí bajtů, k otočení pořadí bitů v bajtu, nebo k přidávání různých bitových posloupností před vstupní data a za ně.
• Protože CRC je založeno na dělení, nerozezná přidané nuly na začátku vstupních dat $M(x)$. Proto se někdy při výpočtu CRC před vstupní data dává jednička.
• Předchozí problém s přidanými nulami na začátku lze v některých implementacích výpočtu odstranit nastavením polynomu $R(x)$, (zbytek po dělení), na nenulovou hodnotu před zahájením vlastního výpočtu (např. 0xFFFF u protokolu Modbus/RTU).
• Při některých způsobech výpočtu se za vstupní data přidává stejný počet nul, jako je šířka CRC. CRC vypočtené ze vstupních dat a uloženého CRC je pak nulové.

ECC – Error Correction Code

Je tedy třeba použít systém, který nalezne veškeré chyby a automaticky je opraví. Technicky jsme schopni takové algoritmy (označované jako **ECC - kódy korekce chyb**) vytvářet v libovolném stupni přesnosti, kterou potřebujeme, výměnou za zvýšení režie. Většinou se tedy spokojíme s kódy, které dokáží detekovat a opravit chyby v jednom bitu a detekovat, ale neopravit, chyby ve dvou a více bitech. Dnes se ECC používá v celé řadě různých zařízení, od CD přehrávačů k počítačům. Možná nejznámějším použitím je ECC v paměťových modulech určených převážně pro servery, kde jsou redundantní bity navrženy přímo v čipech dynamických RAM.

Jak pracuje ECC.

ECC přidává k datům několik paritních bitů. Výpočty jsou obvykle aplikovány na kompletní slova (typicky 32 nebo 64 bitů), ne na jednotlivé bajty. Každý ECC bit představuje paritu různého subsetu datových bitů a každý datový bit je normálně zahrnut do více než jednoho ECC bitu. Tak můžeme detekovat jednobitovou chybu, identifikovat problematický bit a opravit jej. Rovněž můžeme detekovat, nikoliv opravit chybu dvou bitů.

	Datové bity							ECC bity		
Přijatá data	0	1	1	0	0	1	0	1	1	1
bity subsetu 1	x	x		x	x					
bity subsetu 2		x	x	x		x				
bity subsetu 3	x		x	x			x			
subset 1	0	1		0	0			1		
subset 2		1	1	0		1			1	
subset 3	0		1	0			0			1
Konečná hodnota (data správně)	0	1	1	0	0	1	0	1	1	1

Abychom viděli, jak ECC pracuje ve velmi zjednodušené formě, podívejme se na sedmibitový kus binárních dat v tabulce. Přidali jsme k němu další tři bity pro ECC data, s hodnotou vypočtenou jako parita (sudá) pro příslušný subset (podmnožinu dat) datových bitů. Zde jsou tři subsety s vypočtenými ECC bity.

Pro simulaci chyby změňme třetí datový bit zleva z 1 na 0. Chybný bit je označen červeně.

	Datové bity							ECC bity		
Přijatá data	0	1	0	0	0	1	0	1	1	1
bity subsetu 1	x	x		x	x					
bity subsetu 2		x	x	x		x				
bity subsetu 3	x		x	x			x			
subset 1	0	1		0	0			1		
subset 2		1	0	0		1			0	
subset 3	0		0	0			0			0
Konečná hodnota (data chybně)	0	1	0	0	0	1	0	1	1	1

Vidíme, že vypočtené ECC není správné => došlo tedy k chybě. Protože 1 bit ECC je v pořádku, chyba nemůže být v bitech 1,2,4 a 5. Tak nám zbývají bity 3,6 a 7.

Tři subsety datových bitů byly vytvořeny tak, aby změna jakéhokoliv jednoho datového bitu vytvořila novou hodnotu ECC. Předpokládejme, že by chyba byla v bitu 7. Když jej zkusíme změnit, dostaneme hodnotu ECC 110, což není pravda. Pokud změníme bit 6, tak dostaneme hodnotu 101, což také není pravda. Hodnotu ECC 100 dostaneme pouze změnou bitu 3. Bit tedy opravíme a můžeme potvrdit správnost dat.

Co se stane v procesu kontroly a opravy chyb, pokud dojde během přenosu ke změně dvou bitů dat? Zkusíme jednoduchý příklad změny bitu 4 a 5.

	Datové bity							ECC bity		
Přijatá data	0	1	1	1	1	1	0	1	1	1
bity subsetu 1	x	x		x	x					
bity subsetu 2		x	x	x		x				
bity subsetu 3	x		x	x			x			
subset 1	0	1		1	1			0		
subset 2		1	1	1		1			1	
subset 3	0		1	1			0			1
Konečná hodnota (data chybně)	0	1	1	1	1	1	0	0	1	1

Protože ECC nesouhlasí, došlo k chybě. Při prvním pohledu z hodnoty ECC 011 můžeme usuzovat, že by mohlo jít o chybu v bitu 3. Když zkusíme opravu, zjistíme, že výsledek není stále správný => máme chybu ve dvou nebo více bitech.

Na závěr otázka proč jsme použili pouze sedm datových bitů místo běžných osmi. Použití osmi datových bitů se třemi bity ECC, by vedlo k jedné ze dvou situací. Buď by jeden z datových bitů nemohl být zahrnut do jednoho ze tří subsetů a pak bychom nemohli detekovat chybu v tomto bitu, anebo by byly dva nebo více bitů zahrnuty do přesně stejných subsetů, a pokud by nastala chyba v jednom z nich, nemohli bychom určit přesně, který bit je chybný. Toto je však velmi zjednodušený příklad, ve skutečnosti jsou ECC algoritmy mnohem složitější a efektivnější. Berou také v úvahu možnost, že by mohly být chybné samotné ECC bity.

IP telefon

IP telefon je v užším smyslu hardwarově řešený klient pro telefonii typu VoIP. Je to telefonní přístroj, který komunikuje prostřednictvím svého rozhraní protokolem IP. V širším smyslu je IP telefonem každé koncové zařízení pro IP telefonii, bez ohledu na to jde-li o samostatný přístrojnebo o software, který umožňuje telefonování pomocí vhodného počítače.

Avaya VoIP Phone 4625 1140E	VoIP Phone 1535	VoIP Video Phone	Cisco VOIP phone
			

Rozhraní

Již bylo zmíněno, že IP telefon využívá nejčastěji rozhraní pro přímé připojení do sítě Ethernet (vrstva 2 ISO/OSI modelu). Typicky umí rychlosti 10 a 100 Mbit/s, 10Base-T a 100Base-TX. V poslední době se stávají běžné i telefony s metalickým gigabitovým (triálním) rozhraním 10/100/1000 Mbit/s. Datový výkon telefonu je samozřejmě nižší, pásmo 100 nebo 1000 Mbit/s sám ani zdaleka nevyužije. Jak už jeho název napovídá, na třetí vrstvě komunikuje IP telefon protokolem IP.

Protokoly

• Druhá vrstva - Ethernet.

• Třetí vrstva - IP.

• Čtvrtá vrstva - UDP pro hlasový proud, TCP/UDP pro signalizaci.

Na vyšších vrstvách se komunikace větví do celé množiny protokolů. IP telefony nejčastěji pracují s VoIP protokoly z rodiny SIP a H.323. Některé umějí i MGCP.

• Pátá vrstva používá dvě odlišné skupiny protokolů současně:

1. RTP je společným protokolem pro tok hlasových dat
2. VoIP signalizace má různé protokoly lišící se podle zmíněných rodin H.323, SIP a MGCP.

Při výběru telefonu je třeba pečlivě ověřit jaký protokol serveru/gatekeeperu nebo brány se bude pro komunikaci s telefonem používat a zda jej telefon umí.

Hardware IP telefonu.

Je to malý jednoúčelový počítač se zvukovou kartou, s displejem, síťovým rozhraním, procesorem, pamětí RAM, pamětí FLASH místo pevného disku a speciálním operačním systémem v této trvalé paměti.

Použití

• Pro přímé telefonování po síti mezi dvěma telefony. Pak se obvykle volí („vytáčí“) místo čísla IP adresa.

• Pro spojení mezi telefony ve firemní LAN a WAN. Registrace telefonů a hovor jsou zprostředkovány jedním nebo více servery (softswitch). K volbě cílového účastníka se používá telefonního čísla např. v podobě E.164 adresy.

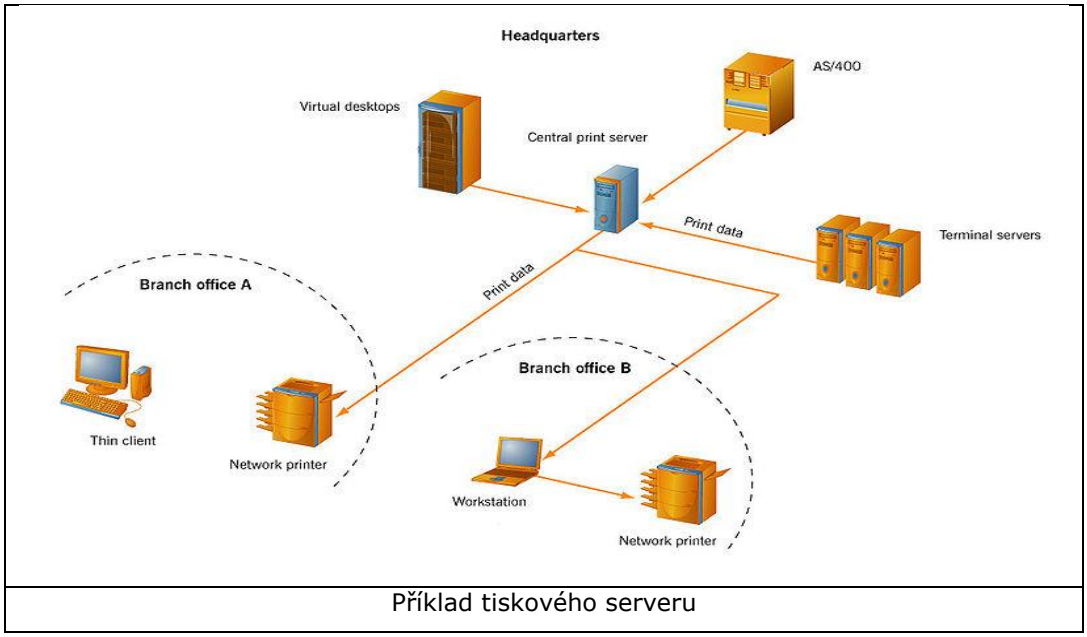
• Pro spojení na VoIP poskytovatele - ekvivalent dřívějšího připojení na ústřednu. Poskytovatel zprostředkuje spojení s dalšími účastníky a obvykle i povolení přes VoIP/TDM bránu do veřejné telefonní sítě. Nejlevnějšího spojení lze dosáhnout s využitím ENUM, kdy se hovor přes veřejnou (placenou) telefonní síť směruje až tehdy, když systém nenajde možnost spojit účastníky přímo mezi sebou pomocí VoIP.

Tiskový server

Tiskový server (anglicky *Print server* nebo *Printer server*) je zařízení, které propojuje tiskárnu s klientem přes počítačovou síť. Tiskové servery mohou podporovat standardní nebo svoje protokoly včetně IPP, Line Printer Daemon protocol (LPD), Microsoft Network Printing protocol, NetWare, NetBIOS nebo JetDirect. Tiskový server může být počítač v síti s jednou nebo více sdílenými tiskárnami. Alternativně může být tiskový server dedikované zařízení v síti s připojením k LANu a s jednou nebo více tiskárnami. Dedikované serverové zařízení bývají jednoduché jak v nastavení, tak i ve funkcích. Funkce tiskových serverů mohou být integrovány s dalšími zařízeními, jako je router, firewall nebo obojí. Tiskárna může mít v sobě také zabudovaný tiskový server.

		
Bezdrátový tiskový server	Brother HL-2070N je laserová tiskárna se zabudovaným serverem	Dell 1320cn je barevná laserová tiskárna se síťovým připojením

Všechny tiskárny se správným typem konektorem jsou kompatibilní se všemi tiskovými servery. Výrobci serverů dávají k dispozici seznam kompatibilních tiskáren, protože server nemusí provádět všechny komunikační funkce tiskárny (např. ukazatel malého množství inkoustu apod.).



Příklad tiskového serveru

Modem

Modem je zařízení pro převod mezi analogovým a digitálním signálem. Modem je zkratkové slovo z výrazu „**mo**dulátor **dem**odulátor". Modemy se používají především pro přenos digitálních dat pomocí analogové přenosové trasy. Přenosová trasa může být telefonní linka, koaxiální kabel, radiový přenos apod.

Typy modemů

- modemy pro komutované (vytáčené) připojení do standardní analogové telefonní sítě
- terminálové adaptory - TA někdy též nesprávně zvané „ISDN modemy" pro připojení do digitální telefonní sítě
- modemy pro pronajaté propojení bod-bod, linka typu dvou-drát nebo čtyř-drát
- modemy pro širokopásmové kabelové připojení k internetu - CableDSL
- modemy pro širokopásmové telefonní připojení k internetu - ADSL
- GSM, UMTS modem/karta pro datové propojení přes síť GSM, UMTS viz GPRS, EGPRS, HSDPA
- různé radio modemy (plně duplexní a poloduplexní)

Pro řízení většiny standardních modemů se používá sada příkazů AT (tzv. Hayes kompatibilní). Pro speciální modemy může existovat i vlastní komunikační protokol.
Poté se ještě modemy dělí na interní a externí. Interní se dělí ještě na hardwarové a softwarové.
Soft-modemy využívají procesoru počítače a ten pak musí provádět např. kompresi dat, zatím co hardware - modemy mají procesor svůj a nezatěžují procesor PC. Klasické modemy HW, si také řídí tok dat na rozhraní RS232.

Telefonní modem

Telefonní modem pro komutované (nesprávně vytáčené) připojení (dial-up) převádí digitální signál do pásma pro běžný hovor (standardní telefonní pásmo je od 0,3 až do 3,4 kHz). Pro přenos pak slouží běžná telefonní přípojka. Používají se různé typy modulace, především je to dnes několikastavová kvadraturně amplitudová modulace - vlastně kombinace amplitudové a fázové modulace (například šestnáctistavová, tedy 16-QAM). Moderní modemy používají protokoly na samočinnou opravu a detekci chyb (viz ECC), automatické sledování kvality přenosu apod. Současné telefonní modemy dosahují na telefonních linkách maximální rychlosti do 56 kbit/s (je to zároveň přibližně fyzikální maximum na analogové telefonní lince, dané paradoxně její následnou digitalizací v ústřednách a na dálkových trasách). Je to dnes již takřka nepoužívaný způsob připojení domácího počítače do Internetu (dial-up). Prakticky se s tímto způsobem přenosu setkáváme jen u telefaxů.

Faxmodem

Většina telefonních modů, *ISDN* modemů a GSM/GPRS/UMTS modemů podporuje přenos faxů skupiny 3.

Modem pro pronajaté propojení

Tyto modemy jsou zpravidla plně kompatibilní s telefonními modemy, navíc poskytují možnost propojení pomocí nevytáčeného propojení pronajatou analogovou linkou, (není nutné napájení ústřednou a modemy se kontrolují na základě trvale vysílaného klidového kmitočtu). Tuto funkci umí i některé běžné modemy a zjistíme to použitím AT příkazu AT&L1 , nebo AT&L2 v terminálovém režimu počítače. Pokud je odezva ERROR, znamená to, že to modem neumí. Nastavení AT&L0 je pro linku s ústřednou. Pro propojení se používá dvou-vodičová linka (dvou-drát) jako u klasického telefonního spojení nebo čtyř-vodičová linka, pro každý směr přenosu je jeden pár vodičů. Lze tak sledovat kvalitu přenosu a nastavovat parametry přenosu pro každý směr. Čtyř-vodičová linka mimo jiné umožňuje propojení přes vhodnou plně duplexní radiostanici a vytvořit tak radio modem.

DSL modem

DSL modem (anglicky *Digital Subscriber Line Transceiver*) neboli **modem pro digitální zákaznickou přípojku** je zařízení používané k připojení počítače k DSL lince. Umožňuje-li modem připojení více počítačů, označujeme ho jako DSL router. DSL modem funguje jako ADSL terminál nebo ATU-R, jak ho nazývají telefonní společnosti. Používá se i zkratka **NTBBA** (network termination broad band adapter). Jelikož je DSL modem bridge, může používat MAC adresu připojeného počítače (tzv. klonování MAC adresy).

Westell Model 6100 ADSL modem

Srovnání s klasickým (hlasovým) modemem

Tato dvě zařízení slouží v podstatě stejnému účelu, ale liší se v jistých ohledech:

- DSL modemy jsou málokdy součástí počítače, ale jsou místo toho připojeny k počítači přes Ethernetový port (pak se ale už jedná o DSL router, jehož je modem součástí), nebo případně přes USB port, zatímco klasické modemy jsou většinou zabudovány do počítače nebo jsou připojeny pomocí sériového portu.
- Microsoft Windows a další operační systémy obvykle nerozpoznají připojené DSL modemy, proto jsou potřeba ovladače od výrobce. Routery mohou být nastaveny ručně, například použitím webového rozhraní s propojením pomocí ethernetového kabelu. Někdy je možné je nastavit pomocí UPnP. V DSL modemech je obvykle nutné nastavit parametry digitální linky, ale některé disponují i autodetekcí.
- DSL modemy používají pásmo frekvencí od 25 kHz až 1 MHz (viz Asymetric Digital Subscriber Line) či až 30 MHz (VDSL), aby přenášené informace nerušily hlasový hovor, který je přenášen na frekvenci 0-4 kHz. Tím se liší od klasických modemů, které používají pro přenos dat hlasové pásmo a není tak možné zároveň telefonovat i přenášet data.
- DSL modemy mají různou rychlost datového přenosu, od stovek kilobitů za sekundu, až po mnoho megabitů, zatímco klasické modemy jsou limitovány na pouhých 56 kbit/s
- DSL modemy fungují pouze na specifické přípojce, která je propojena s DSLAMem, zatímco klasické modemy mohou pracovat s jakoukoliv hlasovou telefonní linkou kdekoliv na světě
- DSL modemy jsou závislé na protokolu použitém na konkrétní lince, a proto nemusí fungovat na jiné lince (ani když je od stejné společnosti), zatímco většina klasických modemů využívá mezinárodní standardy a umí najít standard, který funguje.

Většina těchto rozdílů není pro zákazníky důležitá, kromě vyšší rychlosti DSL a možnosti používat telefon zároveň se spuštěným počítačem. Protože telefonní linka obvykle nese DSL i přenos hlasu (v telefonní lince) musejí se používat filtry pro oddělení.

Další funkce

Kromě připojení k ADSL má mnoho modemů ještě další funkce:

- Podpora ADSL2 nebo ADSL2+
- Router funkci pro uživatele Network Address Translation
- Podpora 802.11b nebo 802.11g bezdrátový access point (AP)
- Vestavěný switch (typické 4 porty)
- Virtual Private Network zakončení
- Dynamic Host Configuration Protocol (DHCP) server
- Dynamické DNS (Domain Name System, klient)
- Voice over IP funkce, včetně Quality of Service (prioritní kontrola dat, které tečou mezi uživateli)

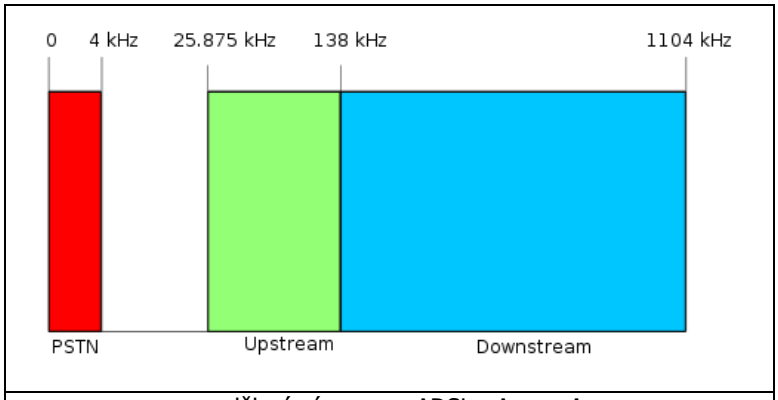
Mnoho ADSL modemů si může upravit vlastní firmware tak, aby podporoval další funkce, nebo aby opravil stávající problémy. Toto se dá udělat pomocí sítě, nebo použitím sériového připojení.

ADSL - Asymmetric Digital Subscriber Line

Je v současnosti nejčastěji využívaný typ DSL přenosů. Vyznačuje se asymetrickým připojením, kdy je rychlost dat přenášených k uživateli (anglicky *download*) vyšší, než rychlost dat odcházejících od uživatele směrem do Internetu (anglicky *upload*). Asymetrie naprosté většině uživatelů vyhovuje, protože odpovídá jejich běžným potřebám. Na druhou stranu může bránit rozvoji Webu 2.0 nebo videotelefonování, kde je nutné přenášet více dat oběma směry.

Princip ADSL

Telefonní linka (PSTN) slouží primárně k přenosu hlasu, ISDN linka k přenosu digitálního signálu. Na telefonní lince se používají pro potřeby tradičních hlasových hovorů frekvence od 0 do 4 kHz (běžné hovorové pásmo je 0,3 – 3,4 kHz). Vyšší frekvence byly dlouho nevyužity. K provozu ISDN linky se používají frekvence cca 0 – 50 kHz.



rozdělení pásma pro ADSL - Annex A

U ADSL se pro přenos dat směrem do sítě (anglicky *upstream*) využívají frekvence 26 – 138 kHz (u Annex A) a 138 – 276 kHz (u Annex B) a pro přenos dat ze sítě (anglicky *downstream*) frekvence 138 kHz – cca 1,1 MHz, (u Annex A) a 276 kHz – cca 1,1 MHz (u Annex B). Dříve se používalo rozhraní Annex A u telefonních linek (PSTN) a Annex B u ISDN, dnes se ADSL zřizuje výhradně s rozhraním Annex B. Přenášená data se zapouzdří buď do ATM buňky (protokol PPPoA) nebo do Ethernetového rámce (protokol PPPoE).

Hardware pro ADSL

ADSL modem

ADSL modem je zařízení, které je nezbytné a jiný než ADSL modem není možné použít. K počítači se připojuje buď přes USB port (zásuvku), Ethernet (port RJ-45), nebo ve formě PCI karty. Sám o sobě nedokáže poskytovat připojení více než jednomu počítači.

ADSL router

ADSL router je zařízení podobné modemu, které je nezbytné po připojení počítačové sítě přes ADSL, tedy dokáže poskytnout připojení více než jednomu počítači.

Splitter

Splitter je speciální filtr, jehož úkolem je oddělit běžný provoz na telefonní lince od přenosu dat pomocí filtrování frekvencí. Je nezbytný, pokud se má zapojit ADSL modem současně s telefonním přístrojem. Někteří uživatelé se pokouší nahradit splitter běžnou rozdvojkou, ovšem v takovém případě může docházet k poklesu kvality přenosu jak hlasu, tak dat. Proto se toto uvádí až jako krajní možnost a nedoporučuje se (ne vždy takovéto zapojení musí fungovat).

Propojovací kabely

Propojovací kabely bývají zpravidla součástí prodejního balení modemu.

Hardware na ústředně

V telefonní ústředně je nejvýraznějším zařízením **splitter** a **DSLAM**. Splitter slouží k nasměrování datové složky k DSLAMu a hlasové (u ISDN digitální) složky k místní smyčce a účastnickým sadám. DSLAM je bránou do datové sítě poskytovatele připojení.

VDSL

VDSL nebo **VHDSL** (anglicky **Very High Speed DSL**) je DSL technologie umožňující rychlejší datový přenos přes existující telefonní vedení (plochý nekroucený kabel nebo kroucená dvojlinka), což zjednodušuje její nasazení, protože není nutné pokládat nové kabely.

Druhá generace VDSL2 (ITU-T G.993.2) využívá šířky pásma až do 30 MHz, což zajišťuje velmi vysokou přenosovou rychlost až 100 Mbit/s současně v obou směrech. Ovšem tato maximální přenosová rychlost je dosažitelná při délce vedení maximálně do 300 metrů. S delším vedením nebo jeho nižší kvalitou se přenosová rychlost snižuje.

Technologie Infineon 10Base-S™ (Ethernet přes VDSL) dosahuje rychlosti až 10 Mbit/s v obou směrech stávajícím starším telekomunikačním vedením až do 1200 metrů.

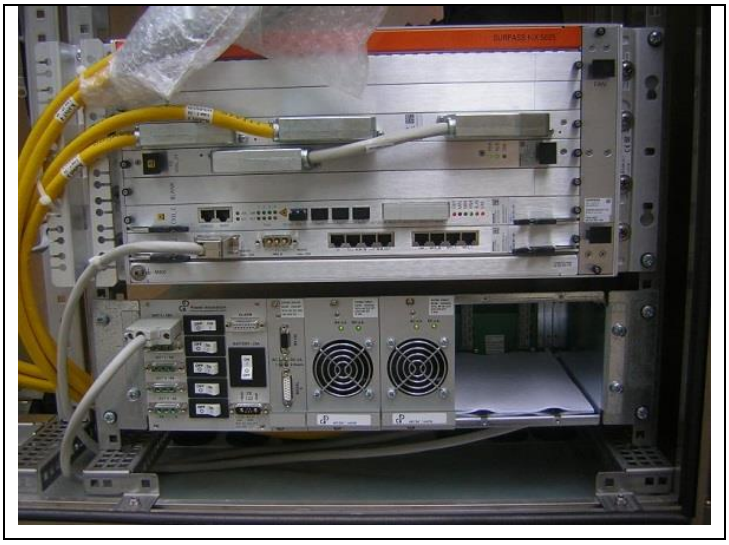
Standard VDSL používá nyní 7 různých frekvenčních rozsahů, které dovolují úpravy rychlostí mezi příchozím a odchozím signálem. Díky tomu VDSL může používat různou rychlost v obou směrech podle potřeb. První generace VDSL stadardu specifikovala jak QAM (anglicky *Quadrature Amplitude Modulation*) tak i DMT (anglicky *Discrete Multi Tone Modulation*). V roce 2006 ITU-T standardizovala VDSL v normě G.993.2, která specifikuje pouze DMT pro VDSL2.

Velké přenosové rychlosti dokazují, že VDSL je vhodné pro použití s novými „high-end" aplikacemi, kde je možné pomocí jediného připojení realizovat například HDTV, IP telefonii a zároveň i přístup k Internetu. VDSL, a to zvláště VDSL2, nabízejí dnes poskytovatelé internetu po celé Evropě.

DSLAM - Digital Subscriber Line Access Multiplexer

(též vyslovováno jako *dee-slam*) je v informatice název zařízení umožňující rychlé připojení k internetu po telefonní lince pomocí technologií xDSL. DSLAM sdružuje několik desítek až stovek datových toků, které jsou z jednotlivých telefonních linek (z tzv. poslední míle) odkloněny pomocí filtru - **splitteru,** takže neprocházejí skrze telefonní ústřednu. Pokud je „poslední míle" příliš dlouhá, jsou používány *vzdálené DSLAMy*, aby byla udržena vysoká datová propustnost (nutnost nad cca 5 km).

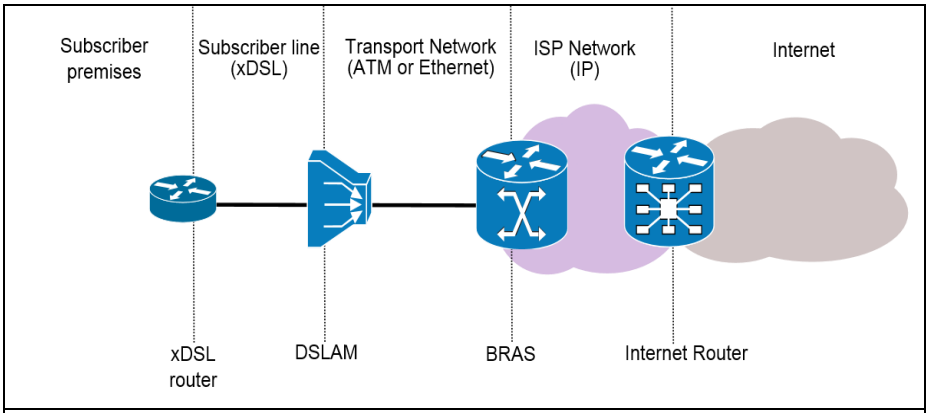
Trasa uživatel <–> DSLAM



1. **U uživatele**: DSL modem ukončuje telefonní přípojku a poskytuje připojení jednomu, nebo více počítačům po LAN či USB
2. **Účastnická přípojka**: Kabelová telefonní přípojka (zpravidla telefonní pár) mezi uživatelem a telefonní ústřednou nebo často bližšího sdružovacího zařízení.
3. **Telefonní ústředna**
   a. **Hlavní rozvaděč (Main Distribution Frame)**: Kabelový rozvaděč ukončující samotné účastnické přípojky vedoucí do ústředny a připojující je k vnitřním obvodům ústředny.
   b. **xDSL filtry**: Elektronické filtry podobné splitteru, které rozdělují jednotlivé složky signálů a směrují datový přenos k DSLAMu a hlasový přenos do části ústředny přepojující hlasové služby.
   c. **Handover Distribution Frame**: Rozvaděč spojující signály z filtrů s DSLAMem.
   d. **DSLAM**: Připojuje účastnické přípojky k datové lince poskytovatele síťové konektivity (network service provider). Převádí analogové signály na digitální datový tok v případě Uploadu (z pohledu uživatele) a digitální datový tok na analogové signály v případě Downloadu. používá u toho multiplexování.

Úloha DSLAMu

Uživatelé se k DSLAMu připojují přes DSL modem nebo přes DSL router, který je připojen do veřejné telefonní sítě typicky po kroucené nestíněné dvojlince. DSLAM umístěný v telefonní ústředně shromažďuje datový provoz z mnoha modemových portů a sdružuje je do jednoho datového toku pomocí multiplexování. V závislosti na architektuře zařízení a jeho nastavení DSLAM slučuje DSL linky na standardu Asynchro-



xDSL spojovací schéma

nous Transfer Mode (ATM) a využívá protokoly frame relay, a/nebo Internet Protocol (IP). Sloučený datový provoz je poté směrován na Broadband Remote Access Server (server síťového přístupu) po Transport Network (transportní síti). A z něj potom po Access Network (přístupové síti) Network Service Providera do samotného internetu. Přístupová síť může dosahovat přenosových rychlostí i nad 10 Gbit/s.

DSLAM se chová jako síťový switch protože je jeho funkce posazená na linkové vrstvě Referenčního modelu ISO/OSI. Z toho důvodu nemůže přesměrovat provoz mezi různými IP podsítěmi, ale pouze mezi zařízením internetového poskytovatele a zařízeními koncových uživatelů.

DSLAM může, ale nemusí být umístěn přímo v telefonní ústředně. Často bývá, jako tzv. vzdálený DSLAM umístěný v sousedství koncových uživatelů, kteří jsou příliš vzdálení od telefonní ústředny, nebo tvoří součást místní ústředny (tabulka závislosti přenosové rychlosti na vzdálenosti). Někdy bývá umístěn spolu s **Digital loop carrier -DLC** (digitální přenos smyčky). DLC je systém, který umožňuje připojit k ústředně i natolik vzdálené účastnické přípojky, které by z elektrického hlediska již na takovou vzdálenost nefungovaly. DLC digitalizuje jinak analogové hlasové přenosy a poté je na velkou vzdálenost přenese digitálně. Datový DSL provoz se filtry směruje do DSLAMu ještě před DLC. DSLAMy také používají hotely a větší instituce, které zpravidla používají vlastní telefonní podsystémy pro vlastní vnitřní komunikaci.

GSM komunikace

GSM (**G**lobální **S**ystém pro **M**obilní komunikaci, původně však francouzsky „**G**roupe **S**pécial **M**obile“) je nejrozšířenější standard pro mobilní telefony na světě. V současnosti jej používá více než 5 miliard účastníků ve více než 200 zemích světa. Protože někteří lidé mají více SIM karet, lze odhadovat, že mobilní telefon GSM vlastní asi polovina obyvatel planety Země.

Historie

GSM telefony z roku 1991

Jméno systému GSM pochází z názvu pracovní skupiny („**G**roupe **S**pécial **M**obile“), která navrhla první verze standardu. Navzdory dnešní popularitě, v roce 1982, kdy byla skupina GSM založena, se předpokládalo, že mobilní telefony bude používat jen malý zlomek obyvatel. Na začátku 80. let 20. století byly uváděny do provozu buňkové mobilní sítě první generace systémů NMT a AMPS. Telefony pro tyto sítě nebyly přenosné, ale kvůli své hmotnosti, spotřebě a rozměrům se montovaly do automobilů. Signál pokrýval pouze největší města a jejich blízké okolí. Kvůli ceně mobilních telefonů a hovorného se jednalo o luxusní službu i pro obyvatele vyspělých zemí. Nepříjemná byla i nejednotnost systémů v různých zemích a neexistence roamingových smluv mezi operátory, což omezovalo použitelnost mobilních telefonů na jednu nebo několik málo zemí.

Skupina GSM navrhla systém používající digitální technologii pro přenos hovorů i signalizace; digitální systémy mobilní telefonie se označují jako systémy 2. generace (2G). Použití digitální technologie umožňuje poskytování dalších služeb, od komunikace pomocí krátkých textových zpráv (SMS), datových přenosů, až po menší služby, které zvyšují komfort uživatelů, jako je zobrazování čísla volajícího, hlasová schránka, přesměrování hovorů a další.

Digitalizace přináší zvýšení kvality zvuku, značně ztěžuje odposlech hovorů a umožňuje i jejich šifrování. Použití časového dělení umožňuje využití jednoho kmitočtu v jedné buňce více uživateli současně a zároveň značně snižuje spotřebu (telefon vysílá jenom zlomek času hovoru). Použití SIM karty umožňuje snadnou změnu mobilního telefonu. Technické základy systému GSM byly definovány v roce 1987. V roce 1989 převzala kontrolu ETSI a kolem roku 1990 byla první specifika GSM na světě a obsahovala přes 6000 stran textu. Vedle datových přenosů CSD (Circuit Switched Data), které se platí stejně jako telefonní hovory, zavádí v roce 1997 GSM standard levnější datové přenosy pomocí paketových dat pod zkratkou **GPRS.** Digitální technologie umožňuje i zvyšová-

ní rychlosti přenosu dat – **EDGE.** V roce 1998 byl zformován **P**rojekt **P**artnerství **3**. **G**enerace (3GPP). Původně měl pouze vytvořit specifikaci pro příští (třetí, 3G) generaci mobilních sítí. Avšak 3GPP převzal také údržbu a vývoj GSM specifikace. ETSI je partnerem 3GPP. V rámci tohoto projektu byla v roce 1999 publikována specifikace Universal Mobile Telecommunications System (UMTS), která, přestože vychází z kódového multiplexu používaného v systému CDMA2000, je pokračování projektu GSM. Mnoho uživatelů „mobilních dat" v síti „GSM" si ani neuvědomuje, že ve skutečnosti používají síť UMTS. Všudypřítomnost GSM standardu a „roamingové smlouvy" mezi mobilními operátory dělají z mezinárodního telefonování běžnou záležitost. I přes svůj vývoj zachovává GSM zpětnou kompatibilitu s původními GSM telefony. GSM je v současnosti vyvíjeno skupinou 3GPP převážně jako otevřený standard.

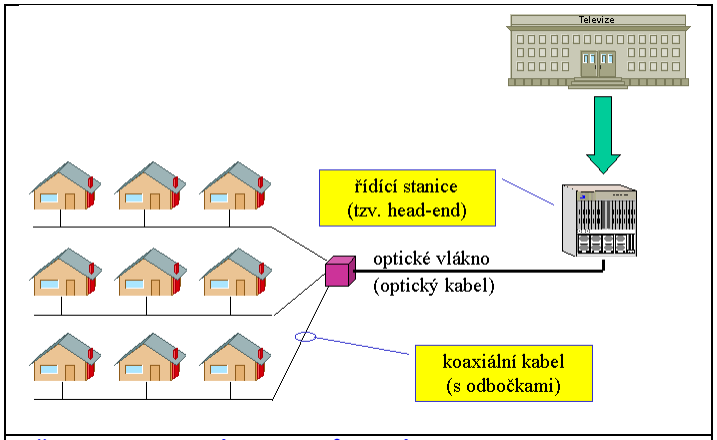
CABLE TV komunikace

Velmi podstatnou vlastností komunikací po telefonních linkách je jejich celkový charakter: drátové místní smyčky, budované světem spojů, jsou v zásadě vyhrazenými spoji typu 1:1, vedoucí od telefonní ústředny k jedinému příjemci (s tím že sdílené optické kabely u řešení FTTH, FTTC a FTTN jsou technickými prostředky rozděleny na dostatečný počet samostatných přenosových kanálů). Jde o řešení, uzpůsobené specifickým potřebám hlasové telefonie - ta potřebuje přenášet jen jednotlivé individuální hovory, vždy jen k jedinému příjemci. V terminologii počítačových komunikací je tento způsob komunikace označován jako "unicast".

Naproti tomu rozvody kabelové televize potřebují fungovat na principu tzv. broadcastu (neboli: všesměrového vysílání). Potřebují dopravit jeden a tentýž signál, v přesně stejné podobě, ke všem svým příjemcům současně (pomineme-li možnost různých nabídek programové skladby, které přeci jen diferencují jednotlivé příjemce). Když už si proto provozovatelé kabelových televizí budují vlastní rozvody (což musí, protože "telefonní" drátové místní smyčky jsou pro ně nepoužitelné), dělají to tak, že své rozvody budují tak aby vycházely vstříc všesměrovému vysílání.

Úplně první rozvody kabelové televize byly budovány výhradně pomocí koaxiálních kabelů, za účelem rozvodu televizního signálu v obtížněji přístupných lokalitách, kde nebyl možný dostatečně kvalitní "vzdušný" příjem pomocí běžné antény. Proto také příslušné technologické řešení dostalo název CATV (od: Community Antenna TV, což lze volně přeložit jako "společná TV anténa pro určitou komunitu přijemců"). Dnes se ale tato zkratka chápe spíše jako Cable TV.

Dnešní typické řešení kombinuje použití dražších optických a lacinějších koaxiálních kabelů - na větší vzdálenosti, v páteřních částech rozvodů, bývají použita optická vlákna (optické kabely), zatímco pro "dotažení" rozvodů do jednotlivých domácností je používán téměř výlučně kabel koaxiální. Velmi často se v této souvislosti používá označení **HFC** (od: Hybrid Fibre Coax, doslova: hybridní řešení optika/coax). Důležité přitom je, že celý rozvod, včetně svého zakončení, má sdílený charakter. Jiná varianta má označení **RFoG** (Radio Frequency over Glass), kde se jedná o převážně optickou hybridní síť, ve které původně koaxiální části byly nahrazeny jednovláknovým optickým kabelem (PON – Passive Optical Network). Při komunikaci se používá odlišné vlnové délky světla pro up a down stream v jednom vláknu.



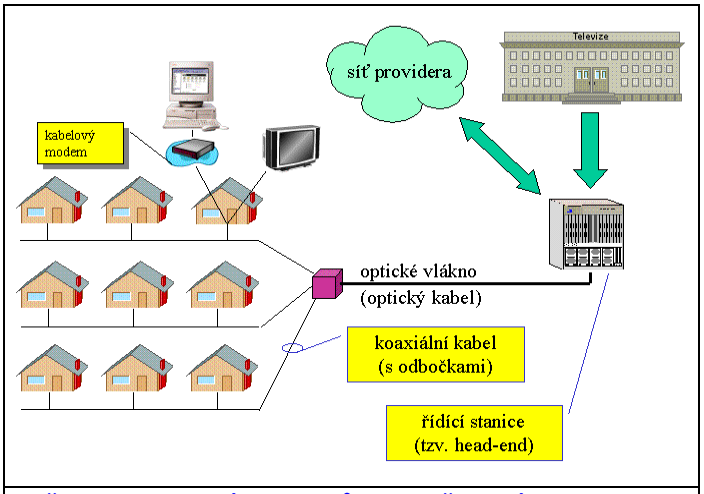
Představa kabelových rozvodů na bázi HFC (Hybrid Fiber Coax)

V praxi však existují i jiné způsoby realizace kabelových rozvodů - například použití bezdrátového systému **MMDS** (Multibodový Mikrovlnný Distribuční Systém). Tu část, která je v systémech HFC realizována optickými kabely (resp. část rozvodů až po "nejzazší" rozvaděče) je zde realizována bezdrátovým způsobem, a teprve "koncová" část rozvodů (typicky v rozsahu jedné budovy) je vedena drátovými přenosovými cestami (koaxiálními kabely).

Pro možnost využití rozvodů kabelové televize pro přístup k Internetu je nesmírně důležitý konkrétní způsob, jakým jsou příslušné rozvody řešeny. Jistou nevýhodou je všesměrový charakter šíření signálu v kabelových rozvodech, který znamená, že přenášená data mohou přijímat všechny stanice (neboli: přenosové médium má sdílený, a ne vyhrazený charakter). S tímto se však lze snadno vyrovnat - na stejné principu sdíleného přenosového média ostatně fungují i nejpoužívanější přenosové technologie lokálních sítí, zejména Ethernet.

Skutečným problémem však může být pouze jednosměrný charakter rozvodů kabelové televize - pro účel, kvůli kterému jsou tyto rozvody budovány, tedy pro šíření TV signálu kabelem, totiž stačí jen jednosměrný přenos. Pokud je konkrétní řešení kabelových rozvodů optimalizováno pro tento účel a neumožňuje žádný přenos opačným směrem, pak je využití kabelových rozvodů pro přístup k Internetu obtížně - ale ne nemožné. Vždy je totiž možné tzv. asymetrické řešení, spočívající v tom že pro přenos signálu jedním směrem se použije jedna přenosová cesta (například směrem k uživateli právě jednosměrné rozvody kabelové televize), a pro přenos opačným směrem se použije technologie jiná (například veřejná telefonní síť, resp. komutovaná připojení).

Dnešní rozvody kabelových televizí však pamatují na možnost přenosu oběma směry současně (i když často ne stejnými rychlostmi). Takovéto kabelové rozvody pak mohou být osazeny na svých koncích vhodnými zařízeními (tzv. kabelovými modemy) a použity pro plnohodnotný přístup k Internetu. V závislosti na schopnostech kabelových rozvodů i samotných kabelových modemů mohou být koncovým zákazníkům nabízeny buďto sdílené přípojky, nebo přípojky vyhrazené s různými rychlostmi. Obvyklá je přitom tarifikace připojení podle objemu přenesených dat, a to zejména proto, že umožňuje dosahovat relativně přijatelné ceny i pro typické domácí uživatele, kteří nevyužívají Internet příliš intenzivně. Na druhé straně ale stejná technologie umožňuje vyhovět i náročnějším uživatelům s požadavkem na vysoké přenosové rychlosti (například až do rychlosti klasického Ethernetu). Výhodou je samozřejmě i trvalý způsob připojení k Internetu.



Představa kabelových rozvodů HFC s připojením k Internetu

Kabelový modem

Je spojení síťového bridge a modemu, které zajišťuje obousměrnou datovou komunikaci po kanálech na radiových frekvencích, v hybridních (HFC) a (RFoG) sítích. Kabelový modem je hlavně použit k zajištění širokopásmového internetového přístupu v podobě kabelového internetu s využitím velké šířky přenosového pásma HFC a RFoG sítí. Je používáno několik norem, z nichž následující jsou asi nejtypičtější:

IEEE 802.3b (10BROAD36)

Je širokopásmový přenos do 3600m po CATV koaxiální síti. Pro přenos je použit frekvenční kanálový multiplex (FDM) proti původnímu přenosu v základním pásmu.

IEEE 802.7

Modifikace IEEE802.3b

Hybrid networks

Vysokorychlostní, asymetrická kabelová síť, protože bylo velmi nákladné zajistit vysokou rychlost upstreamu. Systém je používán některými kabelovými systémy dodnes.

IEEE 802.14

Novější varianta založená na ATM základě.

DOSCIS

Standard vytvořený americkými kabelovými operátory, využívající fyzické vrstvy staršího standardu Motorola CDLP a linkové vrstvy z LANcity systému. První DOSCIS RFI 1.0 uvažoval pouze nejpoužívanější služby, QoS rozšíření a mechanismy používající IntServ, RSVP, RTP a telefonní synchronní přenosový mód (Synchronous Transfer Mode – STM) proti ATM. RFI 1.1 již obsahoval QoS a RFI 2.0 měl doplněnu podporu pro S-CDMA-PHY. RFI 3.0 má doplněnu podporu IPv6 a kanálovou vazbu (channel bonding) dovolující jednomu modemu použít pro přenos více kanálu v jednom směru současně pro zvýšení datové propustnosti. Dnes se dá říci, že všechny kabelové modemy jsou s některou z variant tohoto standardu kompatibilní.

Kabelové modemy a VoIP.

Doplněním přenosu Voice over Internet Protocol (VoIP) by měly kabelové modemy rozšířit nabídku telefonních služeb. Některé společnosti nabízejí vedle kabelové TV automaticky i VoIP, což dovoluje zákazníkům rušit jejich staré telefonní linky (plain old telephone service – POTS), protože některé telefonní společnosti zase nenabízejí holé DSL služby (bez POTS). VoIP používá velké množství účastníků kabelového příjmu.

Architektura kabelových sítí.

Kabelový modem splňuje specifikaci podle IEEE 802.1D pro ethernetovou komunikaci s drobnými změnami. Modem – bridge přepíná ethernetové rámce mezi uživatelskou LAN a kabelovou sítí. Technicky je to modem, protože musí modulovat data, vysílat je po kabelové síti a demodulovat přijatá data. To odpovídá ISO/OSI modelu v 1. fyzické (Eth LAN interface a DOSCIS HFC kabelový interface) a 2. linkové (forwarder) vrstvě. 3. síťová vrstva - jako IP adresovatelné zařízení s adresou danou správcem zařízení, 4. transportní – modem podporuje přiřazení vlastní IP adresy k UDP, umožňuje filtrování na základě TCP a UDP portů a blokuje NetBIOS komunikaci. V 7. aplikační vrstvě modem podporuje určité protokoly užívané ke správě a nastavení zařízení (DHCP, SNMP, TFTP). Některé modemy mohou izolovaně směrovat a obsluhovat DHCP server pro IP adresování uživatelské LAN. I když jsou směrovací funkce typicky oddělené od funkcí modemu, většinou jsou obě části spojeny v jedno zařízení.

Bluetooth

Logo Bluetooth

Bluetooth je v informatice proprietární otevřený standard pro bezdrátovou komunikaci propojující dvě a více elektronických zařízení, jako například mobilní telefon, PDA, osobní počítač nebo bezdrátová sluchátka. Vytvořen byl v roce 1994 firmou Ericsson a míněn jako bezdrátová náhrada za sériové drátové rozhraní RS-232.

Příklad Bluetooth zařízení – bezdrátové sluchátko

Původ názvu

Název Bluetooth je odvozen z anglického jména dánského krále Haralda Modrozuba (*bluetooth* znamená v angličtině „modrozub") vládnoucího v 10. století. Ten využil svých diplomatických schopností k tomu, aby válčící kmeny přistoupily k diskusi a ukončily vzájemné rozepře. Právě této analogie bylo využito pro název technologie Bluetooth, která podobně jako kdysi král Harald slouží k usnadnění vzájemné komunikace.

Specifikace

Technologie Bluetooth je definovaná standardem IEEE 802.15.1. Spadá do kategorie osobních počítačových sítí, tzv. PAN (Personal Area Network). Vyskytuje se v několika verzích, z nichž v současnosti nejvíce využívaná je verze 2.0 a je implementována ve většině aktuálně prodávaných zařízení, jako jsou např. mobilní telefony, notebooky, ale i televize. V současné době je vyvinuto rozhraní Bluetooth 4.0, u kterého výrobci slibují větší dosah (až 100 metrů), menší spotřebu elektrické energie a také podporu šifrování AES-128. Specifikace Bluetooth 2.0 EDR (Enhanced Data-Rate) zavádí novou modulační techniku pi/4-DQPSK a zvyšuje tak datovou propustnost na trojnásobnou hodnotu oproti Bluetooth 1.2 (2,1 Mbit/s). Tímto se dosahuje daleko větší
výdrže baterii, protože samotné navázání spojení a i přenos samotný probíhá v daleko kratší době, než u starších verzí Bluetooth.

Zařízení se dělí dle výkonnosti následujícím způsobem:

Class	Maximální povolený výkon		Dosah (přibližný)
	mW	dBm	
Class 1	100	20	~100 metrů
Class 2	2.5	4	~10 metrů
Class 3	1	0	~1 metr

Přenosové rychlosti podle standardů:

Verze	Rychlost přenosu dat	Maximální propustnost
Verze 1.2	1 Mbit/s	0.7 Mbit/s
Verze 2.0 + EDR	3 Mbit/s	1.4 Mbit/s
Verze 3.0 + HS	24 Mbit/s	
Verze 4.0	24 Mbit/s	

Rádiové rozhraní

Bluetooth pracuje v ISM pásmu 2,4 GHz (stejném jako u Wi-Fi). K přenosu využívá metody FHSS (Frequency Hopping Spread Spectrum), kdy během jedné sekundy je provedeno 1600 skoků (přeladění) mezi 79 frekvencemi s rozestupem 1 MHz. Tento mechanismus má zvýšit odolnost spojení vůči rušení na stejné frekvenci. Je definováno několik výkonových úrovní (1 mW, 2,5 mW, 100 mW), s nimiž je umožněna komunikace do vzdálenosti cca 10–100 m. Udávané hodnoty ovšem platí jen ve volném prostoru. Pokud jsou mezi komunikujícími zařízeními překážky (typicky například zdi), dosah rychle klesá. Většinou ovšem nedochází ke skokové ztrátě spojení, ale postupně se zvyšuje počet chybně přenesených paketů.

Vyšší síťové vrstvy

Přenosová rychlost se pohybuje okolo 720 kbit/s (90 KiB/s) a je možné vytvořit datový spoj symetrický případně asymetrický, kdy přenosová rychlost při příjmu (downlink) je vyšší než při odesílání (uplink). Jednotlivá zařízení jsou identifikována pomocí své adresy *BD_ADDR* (BlueTooth Device Address) podobně, jako je MAC adresa u Ethernetu.

Bluetooth podporuje jak dvoubodovou, tak mnohabodovou komunikaci. Pokud je více stanic propojeno do ad-hoc sítě (tzv. pico-net), působí jedna rádiová stanice jako řídící (master) a může simultánně obsloužit až 7 podřízených (slave) zařízení. Všechna zařízení v pikosíti se synchronizují s taktem řídící stanice a se způsobem přeskakování mezi kmitočty. Specifikace dovoluje simultánně použít až 10 pikosítí na ploše o průměru 10 metrů a tyto pikosítě dále sdružovat do tzv. „scatternets" neboli „rozprostřených" sítí.

Bluetooth vs. Wi-Fi

Implementačně je u Wi-Fi s Bluetooth podobný tzv. ad-hoc způsob komunikace. Wi-Fi pracuje na linkové vrstvě síťového modelu ISO/OSI, nestará se o typ přenášeného protokolu. Naproti tomu Bluetooth řeší sám o sobě vyšší, až aplikační vrstvy síťového modelu. Z toho vyplývá, že pro každý typ připojitelného zařízení musí mít Bluetooth definován speciální protokol pomocí kterého s ním bude komunikovat. Tento způsob komplikuje vývoj softwarové podpory Bluetooth (tj. ovladač zařízení), ale i kompatibilitu jednotlivých implementací, jež mohou obsahovat chyby, které způsobí nefunkčnost komunikace. Na druhou stranu však zjednodušují vývoj software, který dané zařízení používá a konfiguraci jednotlivých zařízení, která mají být propojena.

Bluetooth zařízení

Bluetooth je integrováno v mnoha zařízeních, jako je iPod Touch, Lego Mindstorms NXT, PlayStation 3, PSP Go, telefony, Nintendo Wii a v mnoha dalších zařízeních. Technologie je použita při přenosu informací mezi dvěma nebo více zařízeními, která jsou blízko sebe. Bluetooth je běžně používán v mobilních telefonech často spojených s náhlavní soupravou nebo v přenosu dat mezi telefonem a počítačem. Bluetooth protokoly usnadňují rozpoznání a nastavení služeb mezi jednotlivými zařízeními. Bluetooth zařízení mohou využít všech služeb, které poskytují.

Osobní počítač, který nemá vestavěné Bluetooth, může použít adaptér Bluetooth, který umožní počítači komunikovat s ostatními zařízeními Bluetooth, například mobilní telefony, počítačové myši, klávesnice. Zatímco některé stolní počítače a nejnovější notebooky mají vestavěný přijímač Bluetooth, ostatní zařízení budou vyžadovat externí přijímač v podobě hardwarového zařízení. Na rozdíl od svého předchůdce IrDA, který vyžaduje pro komunikaci s každým zařízením jeden vyhrazený adaptér, Bluetooth umožňuje více zařízením zároveň komunikovat s počítačem přes jeden sdílený adaptér.

Mobilní telefon je schopen spárovat se také s mnoha zařízeními.

Všechna Bluetooth zařízení v režimu viditelnosti předávají na vyžádání tyto informace:

- *Název zařízení*
- *Třída zařízení*
- *Seznam služeb*
- *Technické informace (např.: funkce zařízení, výrobce, použitá Bluetooth specifikace)*

Párování

Mnohé z nabízených služeb Bluetooth je zveřejnění soukromých dat, nebo ovládání připojeného Bluetooth zařízení. Z bezpečnostních důvodů je nutné, aby bylo schopno rozpoznat konkrétní zařízení a umožnit tak kontrolu nad zařízením, které se může připojit k danému Bluetooth. Zároveň je vhodné pro Bluetooth zařízení, být schopné navázat spojení bez zásahu uživatele (například: jakmile je v dosahu Bluetooth). K vyřešení tohoto problému využívá Bluetooth, proces zvaný „Párování". Proces párování se spustí buď zvláštní žádostí od uživatele vytvářející spojení (např.: uživatel výslovně požádá o přidání Bluetooth zařízení), nebo je automaticky spuštěn při prvním připojení ke službě, kde je z bezpečnostních účelů nutná první identifikace zařízení. Tato dvě propojení jsou označovány jako jednoúčelové a všeobecné spojení. Párování často zahrnuje určitou spolupráci s uživatelem, spolupráce je základem potvrzení totožnosti zařízení. Po úspěšném spárování je vytvořen spoj mezi dvěma zařízeními. Tyto dvě zařízení je možné v budoucnu propojit bez nutnosti nového párovacího procesu, za účelem potvrzení identity těchto zařízení. V případě nutnosti může být uživatelem párovací proces odstraněn.

Realizace párování

Během procesu párování dvou zařízení navazující spojení, vytváří obě zařízení společný utajený klíč. Pokud je klíč uložen v obou zařízeních, říkáme tomu párování. Zařízení, které chce komunikovat pouze se spárovaným zařízením, lze kryptograficky ověřit. Ověřením druhého přístroje se lze ujistit, že se jedná o stejně spárované zařízení jako předtím. Jakmile byl klíč mezi zařízeními vygenerován a ověřen, mohou být data šifrována. Tím že data jsou šifrována a posílána bezdrátově jsou chráněny proti odposlechu. Klíče mohou být kdykoli vymazány v obou zařízeních. Pokud se klíč vymaže, bude odstraněno propojení mezi zařízeními. Je možné, aby v jednom ze zařízení byl klíč uložen, ale již nebude vázán na zařízení související s daným klíčem. Bluetooth služby obecně vyžadují buď šifrování, nebo autentizaci, a proto vyžaduje párování umožňující vzdálené využívání dané služby.

Párovací mechanismy

Párovací mechanismy se významně změnily se zavedením jednoduchého zabezpečení u Bluetooth v2.1. Následující text shrnuje párovací mechanismy různých zařízení:

1. **Dědičné párování**: Tato metoda je k dispozici pouze u Bluetooth v2.0 a předchozích verzí. Každé ze zařízení musí zadat PIN kód, shodují-li se oba kódy, spárování je úspěšné. Jakýkoliv 16bitový řetězec UTF-8 může být použit jako PIN kód, ale ne všechna zařízení mohou být schopná přijímat všechny možné PIN kódy.
- **Omezení vstupního zařízení**: Jasným příkladem této kategorie jsou zařízení Bluetooth handsfree. Tato zařízení mají obvykle pevně daný PIN, např. "0000" nebo "1234", který je pevně zakódován do zařízení.
- **Číselný vstup**: Mobilní telefony jsou klasické příklady těchto zařízení. Umožňují uživateli zadat číselnou hodnotu až 16 číslic.
- **Alfanumerický vstup**: Počítače a smartphony jsou příkladem těchto zařízení. Umožňují uživateli zadat vstupní UTF-8 text jako PIN kód. Je-li vytvářeno párování s méně schopným zařízením, musí si uživatel uvědomit omezených možností druhého zařízení. Pro zařízení neexistuje žádný mechanismus, jak sdělit svá omezení.
2. **Jednoduché bezpečné párování** (SSP): Jednoduché párování je nutné u Bluetooth v2.1. Bluetooth zařízení používá pouze párování vzájemně spolupracující s verzí 2.0 a se starším zařízením.

Přestože Bluetooth má své výhody, je citlivý na útoky DoS, odposlechy, MITM útoky a modifikaci zpráv.

Zdravotní rizika

Bluetooth využívá mikrovlnné rádiové frekvenční spektrum na frekvencích 2,402 GHz až 2,480 Ghz. Maximální výkon Bluetooth je 100 mW, 2,5 mW a 1 mW pro zařízení třídy 1, 2 a 3. Třída 1 zhruba odpovídá výkonu mobilních telefonů. Další dvě třídy mají mnohem menší výkon, a proto jsou potenciálně méně nebezpečné.