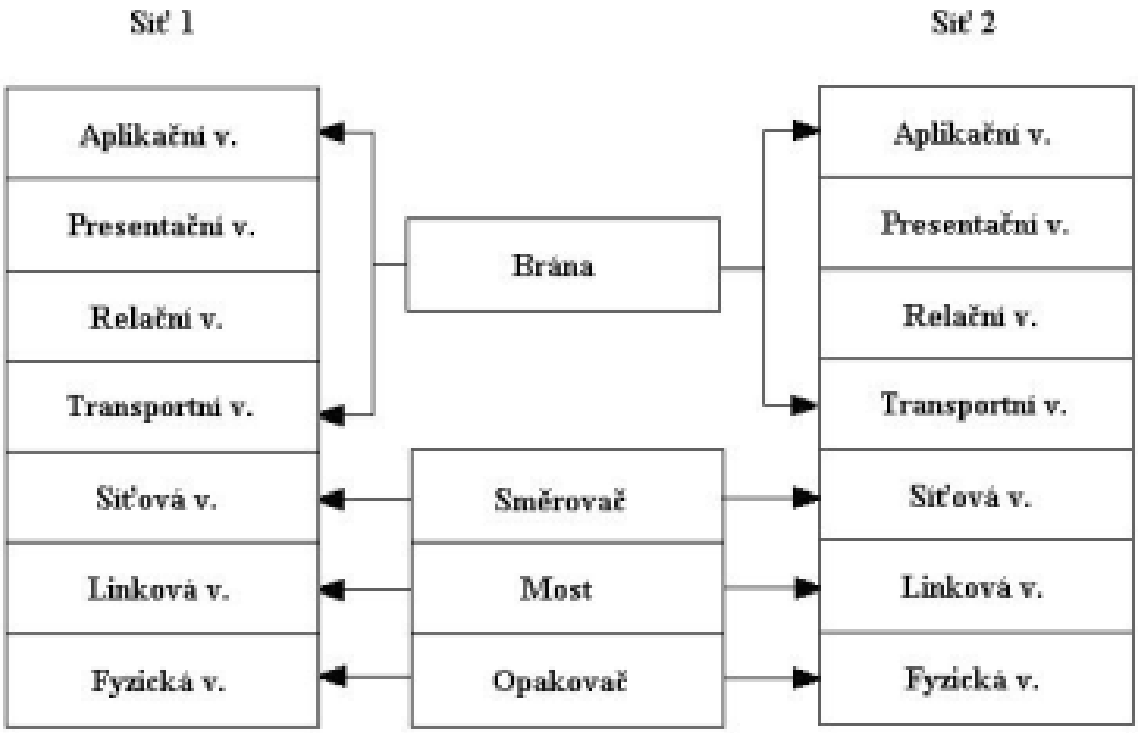
OPAKOVAČE, MOSTY, SMĚROVAČE A SÍŤOVÉ BRÁNY

Vztah opakovače, mostu, směrovače a brány k modelu OSI



Opakovače

Opakovač není ve své podstatě nic jiného, než **obousměrný číslicový zesilovač**. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, jíž jsme schopni lokální síti obsáhnout. Umožňují dosáhnout celkové délky kabeláže až 2,5 kilometru, ale jednotlivé připojovací obvody (tzv. transceivery) jsou schopné generovat elektrické signály s dosahem jen asi 500 metrů. Pak je nutné sestavovat celé kabelové vedení ze segmentů (souvislých úseků kabelů) délky maximálně 500 metrů. Nejedná se tedy v pravém smyslu slova o propojení dvou různých lokálních sítí, ale o tvorbu jedné větší lokální sítě z menších částí. Další možnou funkcí opakovače je **propojení dvou částí lokální sítě, pracující s různými kabely**. V případě Ethernetu tak můžeme například propojit segment pracující s tenkým koaxiálním kabelem (10BASE2) se segmentem pracujícím s tlustým koaxiálním kabelem (10BASE5). Signál přicházející do opakovače ze strany jedné části sítě (např. z jednoho síťového segmentu v případě sítě Ethernet) je v opakovači zesílen a je okamžitě předán do další části sítě (do dalšího segmentu). Totéž se stane se signály jdoucími opačným směrem. Opakovač tedy regeneruje rámce putující po síti a je pro obě části sítě (oba segmenty), které spojuje, "**průhledný**".

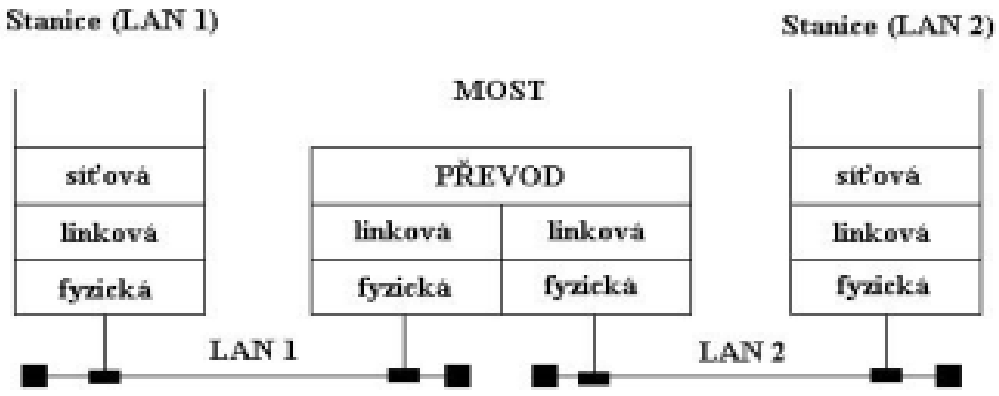
Funkce opakovače při průchodu signálu zleva doprava

Připomeneme-li si funkce jednotlivých vrstev OSI Modelu, je zřejmé, že opakovače pracují v nejnižší, tj. fyzické vrstvě OSI Modelu. Kromě právě popsaných jednoduchých opakovačů existují také opakovače s více porty (tzv. **multi-port repeaters**), umožňující současné připojení více ethernetovských segmentů. V tomto případě je signál přicházející z jednoho segmentu opět zesílen a poté přenášen do všech ostatních segmentů. Příkladem takového opakovače je tzv. 10 BASE-T **rozbočovač (hub).** Je důležité si uvědomit, že při instalaci opakovačů nesmí dojít ke vzniku uzavřených smyček. V tom případě by totiž v opakovačích znovu a znovu obnovovaná data neustále kroužila takto vytvořenou smyčkou (dokonce v obou směrech), což by ve svých důsledních vedlo k **"zahlcení" sítě (tzv. datová bouře** - data storm).

Mosty

Mosty pracují na rozdíl od opakovačů na zcela jiném principu a jsou **používány pro spojení dvou různých lokálních sítí**, lišících se ve dvou nejnižších vrstvách OSI Modelu, tj. ve **fyzické a linkové vrstvě**. V případě lokálních sítí půjde o odlišnost až po tzv. MAC podvrstvu linkové vrstvy (Pro potřeby standardizace lokálních počítačových sítí je výhodné rozdělit linkovou vrstvu na dvě další podvrstvy, na vrstvu řízení přístupu k síťovému médiu MAC - Media Acces Control a na vrstvu řízení logického spojení LLC - Logical Link Control). Most sám o sobě je zařízení, které je součástí obou propojovaných sítí, z nichž obsahuje ty části (ty vrstvy OSI Modelu), kterými se tyto sítě liší. Data jsou z každé z propojených sítí v mostu převedena až do té vrstvy, kde se obě sítě neliší, a tam je proveden přenos dat do druhé ze sítí "), most již pracuje na principu "store and forward" (přijmi a předej dál). V tomto smyslu se dá tudíž říci, že mosty operují nad linkovou vrstvou OSI Modelu (to ale neznamená, že operují v síťové vrstvě, znamená to pouze, že **využívají informace z linkové vrstvy**).

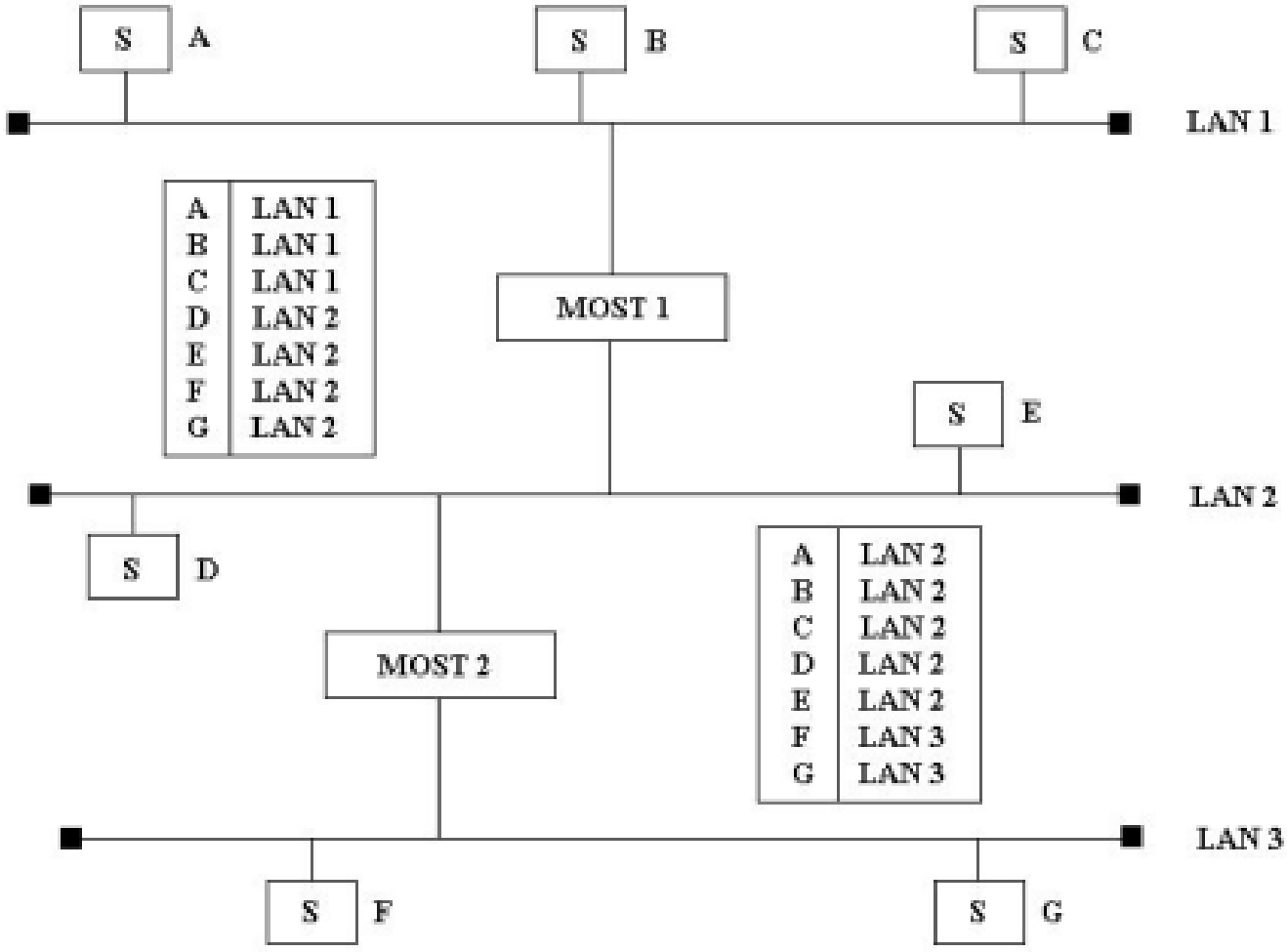
Funkční schéma mostu:



Mosty nejsou, na rozdíl od opakovačů, pro spojované sítě průhledné v tom smyslu, že přes mosty **nepřejdou všechna data** (rámce), která některá ze spojovaných sítí vyprodukuje. Projdou pouze ta data, která jsou určena stanicím nacházejícím se na "**druhé straně mostu**". To má jeden velice podstatný důsledek. Vede to totiž k celkovému snížení provozu na systému pospojovaných lokálních sítí. Lokální data zůstanou lokální a "nepřekáží" v dalších částech sítě. V případě, že bychom na místě mostů použili opakovače, měli bychom celý systém doslova přeplněn daty, protože i cestě lokální data, jejichž vysílající i cílová stanice leží na stejné "podsíti" (v případě Ethernetu na stejném segmentu), by díky průhlednosti opakovačů bloudila po celém systému. Mostem může být například normální osobní počítač, stejný jako v případě běžných síťových pracovních stanic, vybavený ale v tomto případě dvěma síťovými adaptéry (pro každou připojenou lokální síť jedna) a příslušném programovým vybavením. Most bude sledovat provoz na každé k němu připojené síti, ale přenášet bude pouze ty rámce, které rozpozná (podle cílové adresy) jako rámce určené druhé síti, než je síť, ze které přišly. Tak například v případě mostu, který spojuje dvě lokální sítě LAN 1 a LAN 2, přenese tento most rámec ze sítě LAN 1 do sítě LAN 2 pouze tehdy, leží-li jeho cílová adresa "mimo" síť LAN 1. Způsob, jakým most zjišťuje cíl daného rámce, je založen na zkoumání informací z linkové vrstvy. **Most musí tudíž "znát" strukturu rámce** na úrovni této vrstvy a může proto sloužit k propojení pouze těch lokálních sítí, které mají **identické protokoly (a tedy i rámce) linkové vrstvy**. Mosty nemohou být proto použity například k propojení lokání sítě Token Ring s lokální sítí Ethernet. Most přijme data z každé z lokálních sítí, které spojuje, uloží je do pomocné vyrovnávací paměti, prozkoumá je (v nich obsažené adresy) a rozhodne, zda je má ignorovat, nebo zda je má doslat do druhé sítě. Pokud se rozhodne poslat je dál, vyčká v souhlase s konkrétní přístupovou metodou, která je u příslušné sítě použita, podobně jako kterákoli jiná stanice na okamžik, kdy je může odeslat dál (v případě Ethernetu to znamená, že vyčká na klid na síti), a učiní tak. Most tedy pracuje na líti LAN 1 i LAN 2 v podstatě nezávisle. Pro každou z těchto sítí je v podstatě **pouze další síťovou stanicí**. Provoz na síti LAN 1 nebrání mostu v odeslání dat na síť LAN 2, je-li tato síť v daném okamžiku volná, a naopak. V důsledku toho také současné vyslání zpráv na obou sítích nezpůsobí vznik kolize, neboť zprávy nejsou okamžitě přenášeny na druhou síť. Most zde tudíž vystupuje jako jakási **přestupní komora**, v níž se mohou přenášená data v jistém smyslu vzájemně "vyhnout". Ještě jsme se ale nezabývali otázkou, na základě čeho most zjišťuje, ke které ze spojených sítí která cílová adresa patří. K tomuto účelu mu slouží tzv. **směrovací tabulka**, tj. tabulka, v níž je u každé adresy síťové stanice uvedeno, ke které síti příslužná stanice patří. U prvních generací síťových mostů se jednalo o **statické tabulky**, které byly na každém mostu definovány předem. Mnohem výhodnější je ale systém tzv. **dynamických tabulek**, zavedených u novějších generací tzv. "učících se" mostů.). Jednotlivé uzly v síti přitom nemusí o jeho existenci vůbec vědět - proto se také takovýto typ mostu označuje jako tzv. transparentní most (transparent bridge). Lze jej ovšem použít jen v takových sítích, které mají přísně stromovitou strukturu, kdy mezi každými dvěma uzly existuje vždy jen jedna jediná cesta. Pro obecnější topologie jsou pak nutné jiné, složitější algoritmy práce mostů. Dynamická směrovací tabulka může být vytvořena například následujícím způsobem: Most začne svou činnost vysláním speciální výzvy, kterou vyzve všechny aktivní síťové stanice na všech k němu připojených lokálních sítích, aby mu oznámily svou přítomnost. U přijatých odpovědí pak zjistí, ze které lokální sítě příslušná odpověď přišla, a na základě toho si postupně vytvoří potřebnou směrovací tabulku. Stanice, které nebyly v okamžiku vytváření tabulky v provozu, do ní zařadí díky tomu, že neustále sleduje provoz na všech připojených sítích a analyzuje nejen všechny cílové, ale také všechny zdrojové adresy**. V okamžiku, kdy nově připojená stanice odešle svou první zprávu, bude její zdrojová adresa zaznamenána a zařazena do směrovací tabulky.** Most tedy přenášená

data vždy na nějakou dobu uloží do pomocné vyrovnávací paměti. To ale znamená, že data potřebují pro dosažení cílové stanice více času, než vy potřebovala kdyby nemusela projít mostem. Most tedy vnáší do systému lokálních sítí určité zpoždění. Dalším, tentokrát již příjemnějším důsledkem toho , jak mosty s přenášenými daty zacházejí, je to, že v případě mostů neplatí omezení počtu segmentů, které je možno mosty vzájemně propojit, jako tomu je u opakovačů. Mezi dvěma síťovými stanicemi může být zapojen v podstatě jakýkoliv rozumný počet mostů a lze tak překonat mnohem delší vzdálenosti než v případě použití opakovačů. Použití mostu vede ve svých důsledcích také ke zvýšení výkonnosti (celkové kapacity) a spolehlivosti systému. Oddělením provozu v jednotlivých částech sítě totiž **snižuje nebezpečí "zahlcení"** celého systému. To je zvlášť důležité zejména u sítí Ethernet, které jsou díky použité přístupové metodě (CSMA/CD) na přetížení sítě zvláště citlivé. Pokud jde o zvýšení spolehlivosti, zde působí to , že mosty jsou díky své funkci schopny oddělit od zbytku sítě ty její části, na nichž došlo k poruše. Mosty mohou sloužit také pro spojení lokálních sítí používajících odlišné typy síťových kabelů.

Příklad použití směrovacích tabulek



Na rozdíl od opakovačů umožňují mosty při spojování lokálních sítí vytváření více násobných cest. Takové případy mohou výt v případě mostů ošetřeny pomocí speciálních algoritmů (např. tzv. Spanning Tree Algorithm). Tyto algoritmy umožňují mostu rozhodnout, zda má

konkrétní data propustit, či zda jde o data, která mají projít jiným ze "souběžných" mostů. Tímto způsobem lze také vytvářet síťové topologie se záložními mosty, které převezmou funkci " základního" mostu v případě jeho poruchy. To může podstatnou měrou ovlivnit celkovou spolehlivost systému. Síťové mosty mohou být v zásadě dvojí. **Místní (local) a vzdálené (remote)**. Od standardní varianty mostů (označovaných pro odlišení také jako místní mosty resp. local bridges) se vzdálené mosty liší v tom, že jde vlastně o dvě relativně samostatné "poloviny" mostu, příznačně nazývané půlmosty (halfbridge), které jsou mezi sebou vhodně propojeny - např. pevným telefonním okruhem, optickým kabelem apod. Umožňují propojit dva segmenty sítě, které nejsou fyzicky blízko sebe. Takto lze například propojit dva segmenty lokální sítě ve dvou objektech na opačných stranách města, přičemž výsledný efekt je takový, že oba segmenty tvoří jedinou "logickou" síť (z pohledu síťové vrstvy a všech vyšších vrstev je totiž existence místních i vzdálených mostů transparentní). Některé mosty pak mohou mít i schopnost selektivního filtrování některých rámců v závislosti na jejich odesilateli či příjemci, denní době, intenzitě provozu apod. Pak jde o tzv. routing bridges, které správcům sítí umožňují regulovat přenosy mezi jednotlivými segmenty - umožňují například zakázat v době "špičky" přístup z jednoho segmentu do jiného, a při poklesu intenzity provozu jej pak zase následně povolit.

Přepínače

Ve výkladu pojmu přepínač (switch) je určitá nejednoznačnost. Podle klasické definice pracují přepínače na **linkové vrstvě**, a to do značné míry podobným způsobem jako mosty. Při této definici je jediný rozdílem mezi mostem a přepínačem to, že most pracuje jako zařízení pro ukládání a odesílání rámců, zatímco přepínač nikoli. Jestliže přepínač dokáže dekódovat cílovou adresu, zahájí přenos rámce přes odpovídající port. Tento proces může přitom proběhnout i během příjmu zbytku rámce. Zřejmou výhodou takovéhoto schématu je **oproti mostu vyšší rychlost práce přepínače**. Na druhé straně však přepínač **odesílá veškeré rámce, tedy včetně chybných rámců.** Přesněji se tento typ přepínače nazývá přepínač sítě LAN. Moderní definice přepínače je poněkud odlišná, a to zejména v souvislosti s Internetem. Dnešní přepínač již není pouze přepínačem v lokální síti **LAN**; provádí také přepínání v sítích **WAN**. Přepínač je nicméně i nadále zařízením, které pracuje především na linkové vrstvě, jeden stejný přepínač však provádí také určité omezené funkce na síťové vrstvě. Díky této širší množině funkcí můžeme dnešní přepínače přirovnávat spíše ke směrovači než k mostu. Z uvedeného vyplívá, že se moderní přepínač stává rychlejším konkurentem a rychlejší náhradou směrovače. Klasický přepínač je pak rychlejším konkurentem a rychlejší náhradou mostu. Moderní přepínač zjistí dekódováním datového paketu adresu pro síťovou vrstvu. Tato adresa pro síťovou vrstvu se mapuje na konkrétní port přepínače. Další datové pakety, které posílá stejný zdrojový uzel do stejného cílového uzlu, se již nepřepínají v síťové vrstvě, v níž tuto operaci zabezpečují směrovače, nýbrž ve spojové vrstvě. Přepínače se dále neúčastní žádných směrovacích protokolů, jako je například protokolu RIP.

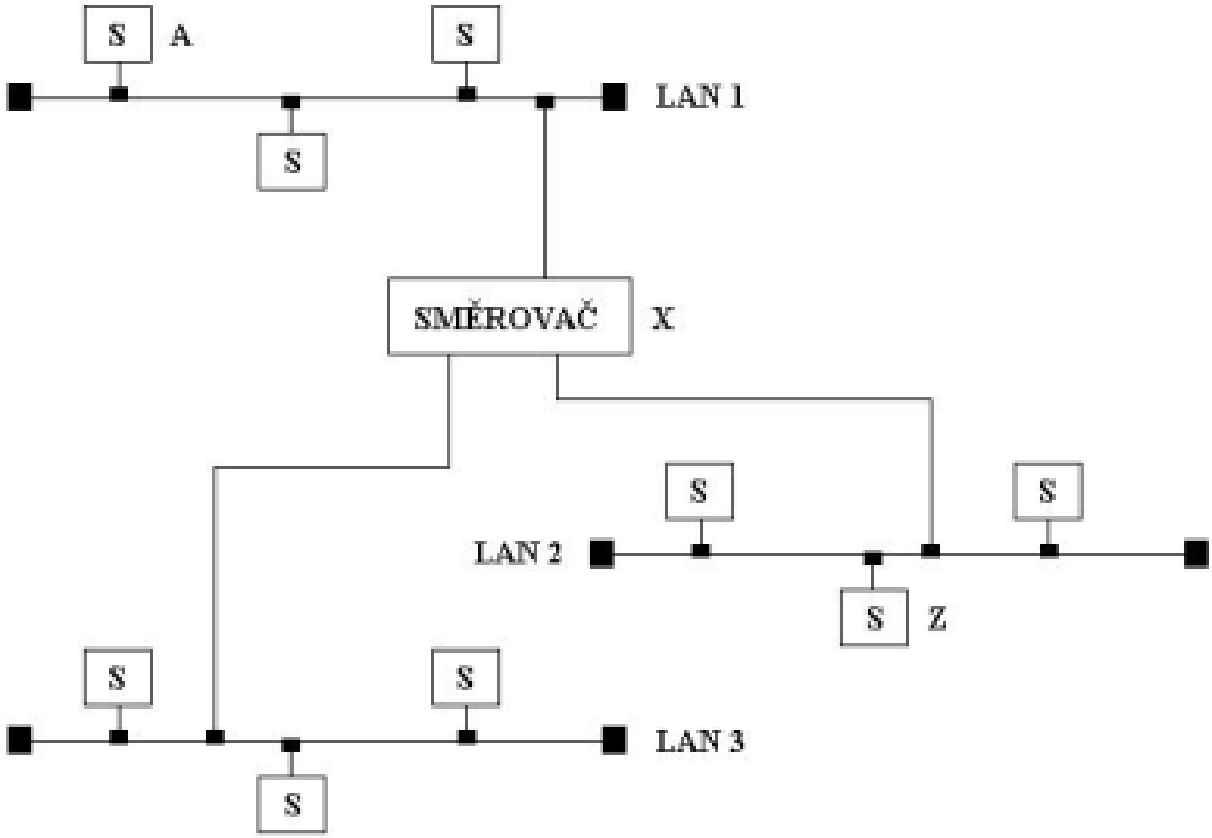
Směrovače

Směrovače pracují na podobných principech jako mosty, pouze s tím rozdílem, že využívají informace ze třetí, tj. **ze síťové vrstvy** OSI Modelu, což je vrstva, která se **stará o nalezení optimální cesty** k cílové stanici. Směrovače můžeme tudíž chápat jako mosty doplněné o možnost volby směru. Síťová vrstva pracuje kromě adres vlastních síťových stanic také se symbolickými adresami jednotlivých lokálních sítí jako takových. Jak pracovní stanice, tak směrovače mají nyní vytvořeny směrovací tabulky, v nichž jsou každé síti přiřazeny směrovače, které mohou zprostředkovat spojení. Chce-li některá stanice poslat zprávu stanici, která patří k jiné síti, vyhledá programové vybavení síťové vrstvy ve své směrovací tabulce adresu odpovídajícího směrovače a předá tuto adresu linkové vrstvě jako cílovou adresu pro vytvoření rámce. Adresu skutečné cílové stanice umístí do hlavičky paketu síťové vrstvy. **Směrovač, který zprávu přijme, oddělí hlavičku linkové vrstvy a v hlavičce síťové vrstvy najde skutečnou cílovou adresu**. Pak opět použije svou směrovací tabulku a zjistí adresu dalšího směrovače a tuto adresu opět předá linkové vrstvě pro vytvoření dalšího rámce. **Obsah paketu síťové vrstvy zůstane nezměněn**. V případě, že cílová stanice i směrovač jsou součástí stejné lokální sítě, předá směrovač linkové vrstvě místo adresy dalšího směrovače přímo adresu cílové stanice. Tak například, chce-li stanice "A" poslat nějaká data stanici "Z", vyšle rámec:

Kde symbol "X" přestavuje adresu směrovače v síti číslo 1 a symbol "Z" adresu cílové stanice. Symbol na prvním místě představuje "aktuální" adresu (tj. adresu MAC podvrstvy) v dané síti, kdežto symbol na druhém místě představuje konečnou cílovou adresu. Směrovač tento rámec přijme, zpracuje (až do úrovně síťové vrstvy) a vygeneruje a vyšle na síť číslo 2 nový rámec, který bude vypadat takto:

Jistou výhodou směrovače proti mostu je to, že nemusí zpracovávat všechny v síti si pohybující rámce. **Zpracovává pouze ty rámce, které jsou mu na úrovni linkové vrstvy (respektive MAC podvrstvy linkové vrstvy) přímo adresovány**. Dochází tedy u směrovače k jeho menšímu zatížení. Naproti tomu vzhledem k tomu, že u směrovačů musí být každý paket zpracován komplexněji, bude zpoždění zprávy pří průchodu směrovačem větší než při průchodu mostem. **Směrovače mohou díky své funkci podporovat složitější síťové topologie,** zahrnující celou řadu nadbytečných spojení, a mohou přitom brát v úvahu celou řadu dodatečných informací, týkajících se například cen přenosu rámce po jednotlivých cestách atp.

Propojení tří LAN prostřednictvím směrovače



Je zřejmé, že směrovače budou použity místo mostů zejména tam, kde půjde o komplikovanější sítě, skládající se například z menších lokálních sítí vybudovaných na základě různých IEEE standardů. U některých současných síťových operačních systémů, jako jsou například Novell NetWare 3.12 nebo LANcastic 5.0 je programové vybavení pro realizaci mostu nebo směrovače přímo součástí programového vybavení těchto síťových operačních systémů. Stačí tedy vybavit server přídavným síťovým adaptérem a máme vše potřebné pro spojení dvou segmentů, k nimž tento počítač náleží. V posledních letech se můžeme setkat při spojování sítí s nový pojmem **brouter (bridge/router)**. Jde o zařízení, které se snaží fungovat jako směrovač, a teprve v okamžiku, kdy pro nějaký paket neumí aplikovat směrovací algoritmus, předá původní rámec dál tak, jako by to udělal most. Výhodou takovéhoto zařízení je pak i to, že se dokáže vyrovnat s takovými protokoly, které vůbec nelze směrovat (neboť nepočítají se síťovou vrstvou - jako například protokoly DECLAT (DEC Local Area Transport), LU 6.2 firmy IBM a protokoly NetBIOS).

Metody vyhledávání cesty:

1. ADAPTIVNÍ - přizpůsobují se změnám v sítí
2. NEADAPTIVNÍ - nereaguje na změny v sítí jako je rychlost, ...

Nalezení cesty:

1. CENTRALIZOVANÉ
2. NECENTRALIZOVANÉ - průchod datagramů přes ROUTER

Vyhledání nejlepší cesty - založeno na routovacích tabulkách, jejich dynamický obsah vzniká na základě komunikace routerů. Statické tabulky vytváří sám správce. Existuje několik tipů algoritmů vyhledávání. Dělí se na dvě kategorie (spec. Protokoly pro komunikaci mezi routery a pro tvorbu z tabulek).

1. starší - DISTANCE - VECTOR - RIP
2. novější - LINK STATE - NLSP, OSPF - nepoužívají informaci z druhé ruky

Základy směrování v IP prostředí – Routing – Routerovací tabulka

Stanice v rámci jedné logické sítě komunikují přímo (s použitím mechanismu ARP). Pokud však chce komunikovat stanice z jedné sítě (např. 192.168.1.x) s uzlem z jiné sítě (např. 192.168.2.x), je potřeba sítě propojit zařízením pracujícím na 3. vrstvě OSI, tzv směrovačem.

Směrovače si udržují přehled o tom, za kterým interfacerem je jaká síť. Tyto informace jsou do zařízení zadány staticky nebo je používán určitý mechanismus pro jejich dynamickou výměnu (to znamená, že směrovače si vzájemně předávají informace o sítích o kterých vědí). Dynamických směrovacích protokolů poměrně široká škála. Jejich použití je vhodné pro různé velikosti sítí a aplikace je rozdílně komplikovaná. Jedná se např. o protokoly RIP, OSPF, BGP, EGP, IGRP...

Příklad směrovací tabulky (routing table):

Cílová síť Destination Network	následující směrovač Next Hop Router	metrika Metric (Hops)
192.168.1.0	Direct Port 1	0
192.168.2.0	Direct Port 2	0
192.168.3.0	192.168.2.3;	1
192.168.4.0	192.168.2.3	2

V závislosti na implemenatci mohou být součástí směrovací tabulky i masky cílových sítí a typ protokolu pomocí něhož směrovač o síti ví. Speciálním typem statické cesty je tzv. Default Route, používaná pro všechny neznámé sítě. Ta má tvar samých nul, tedy adresa 0.0.0.0 s maskou 0.0.0.0. U standardních pracovních stanic, které si nedrží tabulky s cestami do jiných sítí je potřeba zajistit mechanismus podobný mechanismu Default Route. Tento mechanismus se nazývá odchozí brána; neboli Default Gateway.

Přenos dat mezi uzly v různých sítích (tedy z jedné logické sítě do druhé) - stanice A, která je v síti 192.168.1.x potřebuje komunikovat s uzlem B umístěným v síti 192.168.2.x. Mezi sítěmi jsou dva směrovače R1 a R2. Uzel A ví, že má poslat paket do jiné sítě. K tomu má nastavenu tzv. odchozí bránu - směrovač R1. Paket tedy vyplní následujícím způsobem:

L2 - zdrojová adresa – vlastní MAC (A), cílová adresa – MAC směrovače R1
L3 - zdrojová adresa – vlastní IP adresa (A), cílová adresa – IP adresa uzlu B

Paket přijde na směrovač R1. Ten z IP adresy určí adresu sítě pro kterou je paket určen a na základě znalosti cest jej pošle na příslušný směrovač (v tomto případě R2). Směrovač R2 připraví a odešle paket s následujícími parametry:

L2 - zdrojová adresa – vlastní MAC (R2), cílová adresa – MAC uzlu B
L3 - zdrojová adresa – IP adresa A, cílová adresa – IP adresa uzlu B

Při průchodu paketu se mění údaje 2. vrstvy, ale údaje 3. vrstvy jsou beze změny.
Pokud se má paket vrátit, musí mít i druhá strana správně vyplněnu Default Gateway.
I zde fungují standardní mechanismy komunikace prostřednictvím MAC adresy a její případné zjišťovaní pomocí ARP.

Multiprotokolové směrovače

Požadavek stejného (a tudíž jediného) protokolu v síťové vrstvě je ovšem velmi omezující, zvláště v dnešní době, kdy vedle sebe koexistuje celá řada soustav protokolů (kromě ISO/OSI též TCP/IP, SNA, DECnet, SPX/IPX a další), a uživatelé volají po jejich co nejtěsnější integraci v rámci tzv. heterogenních sítí (tj. sítí, jejichž uzly používají různé soustavy protokolů).

Problém heterogenních sítí lze řešit v principu dvěma způsoby - konverzí protokolů, a směrováním více protokolů současně. Řešení prostřednictvím konverzí se ukázalo být značně náročné a nespolehlivé, a proto se prosadila především druhá možnost. Přední výrobci dnes nabízí tzv. multiprotokolové směrovače (multiprotocol routers), schopné pracovat současně s více různými protokoly. Multiprotokolový směrovač musí být schopen rozpoznat typ paketu, který dostane od linkové vrstvy, a podle toho pak aplikovat ten směrovací algoritmus, který k příslušnému síťovému protokolu přísluší.

Brány

Brána (gateway, někdy též: protocol converter)) je obvykle kombinací softwaru a hardwaru, který propojuje dvě různé sítě pracující **pod různými protokoly**. Brány pracují zpravidla **na síťové vrstvě nebo ještě výše.** Některé brány kromě vlastního přenosu dat z jedné sítě do jiné zabezpečují současně s přenosem také převod do jiného protokolu; takovýmto branám se říká aplikační brány. Příkladem může být e-mailová brána, která převádí elektronickou poštu z podoby definované jedním protokolem do jiného protokolu. Někdy se pojem brána používá i v situacích, kdy se neprovádí žádný převod mezi protokoly, ale kdy se data pouze přenesou z jedné sítě do jiné. Takovouto bránu tvoří software a hardware, který propojuje dvě různé sítě. Jednou z možných charakteristik brány mohou být dvě různé adresy pro síťovou vrstvu, například více různých IP adres.

Firewall jako aplikační brána

Firewall jako aplikační brány, zcela oddělují 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. Typickými představiteli aplikačních bran byly např.Kerio Firewall.