

4. HW počítačových sítí

Síťový hardware.

Aby bylo možné vytvořit z počítačů síť, musí být počítače doplněny o síťový hardware a software. Pod pojmem síťový hardware rozumíme:

síťovou kartu (adaptér)

přenosová (spojovací) média (síťové kabely včetně konektorů)

aktivní a pasivní prvky

Síťová karta (NIC – Network Interface Card) je běžná přídatná karta, která se instaluje do volného slotu na základní desce. Karta tvoří rozhraní pro připojení k síti. Je schopna přijímat a vysílat elektrické nebo optické signály z kabelového rozvodu nebo do něj. Musí být kompatibilní:

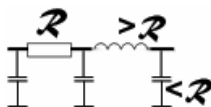
- s datovou sběrnici počítače (ISA, EISA, PCI a pod.,)
- s kabelovým rozvodem (BNC konektor pro koax. kabel, RJ-45 pro UTP/STP,...),
- s typem sítě a tím i přístupovou metodou sítě (Ethernet, Fast Ethernet, Token Ring, ATM, příp, ARCNet)

Přenosová média

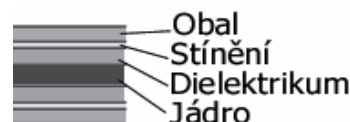
Koaxiální kabel

Nesymetrické médium - data se po kabelu šíří nesymetricky - jsou posílány stanicí po celém mediu a ostatní stanice je odposlouchávají, kabel je na obou stranách ukončen zakončovacím odporem aby nedocházelo k odrazu

Náhradní zapojení:



Složení média:



Vlastnosti

Skinefekt - čím větší frekvence - tím se signál šíří více k okrajům vedení a středem neteče, dochází tak k problémům s přenosem

Měření

Charakteristická impedance - Ethernet 50 Ω
ARCNet 93 Ω
TV 75 Ω

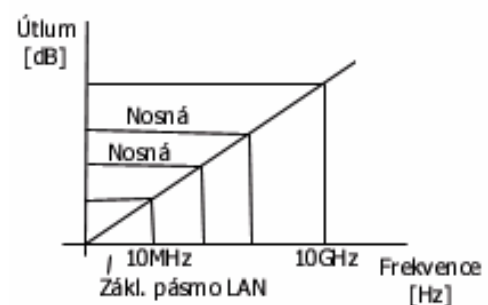
Útlum

$$10 \times \log \frac{V_2}{V_1} [\text{dB}]$$

v1 - začátek vedení
v2 - konec vedení

Přenosová rychlost 10Mbps

Frekvenční charakteristika (Pásmo propustnosti)



Čím větší je frekvence, tím větší je útlum. Nelze tedy donekonečna zvyšovat frekvenci (nejvýše asi 10GHz).

Typy:

V běžných počítačových sítích typu Ethernet se používají dva typy koaxiálního kabelu

Thustý Ethernet (Thick) 10Base5 - Xerox 1972

Médium - žlutý kabel

Nejvzdálenější počítač - 2650m

Max. 100 počítačů

Konektor DIX (Digital Intel Xerox)

Př: RG8 – Yellow cable, 10mm průměr

Tenký Ethernet (Thin) 10Base2

Médium - černý kabel

Nejvzdálenější počítač - 980m

Konektor BNC

Př: RG58 průměr 6mm

Mezi klady patří pořizovací náklady, dobrá odolnost vůči rušení i použitelnost na vnitřní i venkovní vedení. Nevýhodou je hlavně fakt, že se jedná o nízkorychlostní kabeláž (dnes se příliš nepoužívá).

Kroucená dvoulinka - Twist - Twisted pair (+ Strukturovaná kabeláž)

Kroucený pár vodičů drátů, které jsou na obou stranách zapojeny do zásuvky - **symetrické médium**. Nesmí být neskroucen - dochází k *degradacím*. Signál se přenáší jako rozdíl potenciálů obou vodičů. Tímto dochází i k lepší odolnosti vůči rušení protože případný cizí signál by se pravděpodobně naindukoval v obou vodičích stejně a tak se vyrušil. Kroucením se také snižuje vyzařování signálu které by mohlo ovlivňovat okolí. Max délka rozpletení při zapojení do zásuvky je **13mm**.



Konektory - RJ45 - dva typy zapojení ANSI/EIA/TIA

T586A

T586B

	Bílá / Zelená	Bílá / Oranžová
	Zelená	Oranžová
	Bílá / Oranžová	Bílá / Zelená
	Modrá	Modrá
	Bílá / Modrá	Bílá / Modrá
	Oranžová	Zelená
	Bílá / Hnědá	Bílá / Hnědá
	Hnědá	Hnědá

Dvě normy dělení:

1. do **Kategorií** - americká norma novelizovaná r. 1991

CAT3 – 16MHz 10Mbps

CAT4 – 20MHz 16Mbps

CAT5 – 100MHz 100Mbps

CAT5+

CAT6 – 250 MHz (500MHz STP) 1000Mbps (10Gbps)

CAT7 – 600MHz (10GBaseT)

2. do **Tříd** - evropská norma

A – 100kHz

B – 1MHz

C – 16MHz

D – 100MHz

optika

I. Způsoby komunikace:

1. **Simplex** - jednosměrný přenos

2. **Half duplex** - standardní na síti, přenos sem nebo tam

3. **Duplex** - (Full D) pouze 2 počítače mezi sebou - obousměrný přenos

II. Provedení kabelů:

1. **Nestíněné kabely UTP** (Unshielded Twisted pair) - pro použití kde se nevyskytuje příliš velká hladina rušení (Elektromagnetické a jiné vlnění)

2. **Stíněné kabely STP** (Shielded Twisted pair) - stíněny proti rušivému vlnění

3. **Fóliový - FTP** (Foiled TP) - s ochrannou fólií

4. **SFTP** (Sereened TP) - více ochranných prvků

III. Měření kabeláží - norma EIA / TIA TSB - 67

1. **Wire map** (mapa zapojení) - zjistí zda každý kabel vede tam kam má

2. **Délka** - Channel (celé vedení) < 100m

- Basic line (samotná linka) < 90m

3. **Útlum** - signál musí být >10dB

4. **Next** (přeslech na blízkém konci)

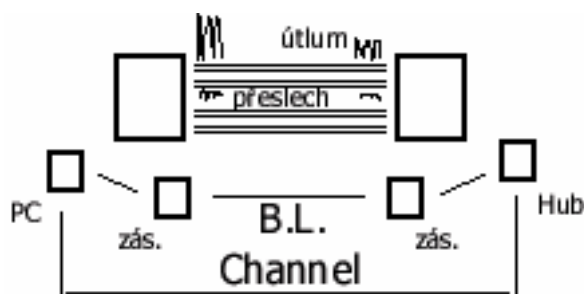
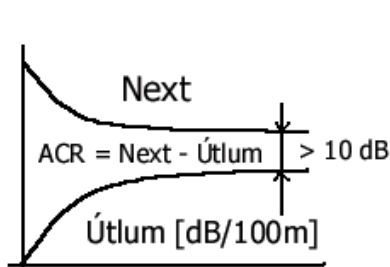
5. **PS Next** (Power Sum Next)

$ACR = Next - Útlum$ [dB]

6. Delay Skey/PropagationDelay – zpoždění při přenosu

7. Return Loss [db] nehomogenity v kabelu – odraz

8. FEXT



OPTIKA

Mnohovidová vlákna

Plynulá změna indexu lomu - jsou tak zvaná gradientní, tj. index lomu jádra roste od pláště ke středu parabolicky.

Skoková změna indexu lomu

- Musí mít dostatečnou šířku pásma - 100-1200MHz
- Tloušťky jader vláken jsou v rozmezí 50, 62,5 někdy až 100um.
- Útlum pro vlnovou délku

- 1300nm je od 0.4dB/km
- 850nm 2.2dB/km
- přenosy na vzdálenosti - jednotky km

Rychlost šíření je nepřímo úměrná indexu lomu, a tedy u gradientních vláken se délková rychlost vyrovnává a nedochází ke zpoždění u různých vidů jako u vlákna se skokovou změnou indexu lomu. Americké normy prosazují 62,5 μ m, kdežto evropské jen 50 μ m. S větším průměrem vlákna roste vstupní apertura - tj možnost většího poloměru zdroje, ale výroba je nákladnější.

Jednovidová vlákna

jsou vlákna, které mají šířku přibližně velikosti λ nebo je malý rozdíl mezi jádrem a pláštěm. Paprsky u jednovidových vláken se šíří jen jedním směrem, tj všechny jsou rovnoběžné.

Jsou schopny vést jen jeden světelný paprsek („vid“ – světlo s určitou vlnovou délkou).

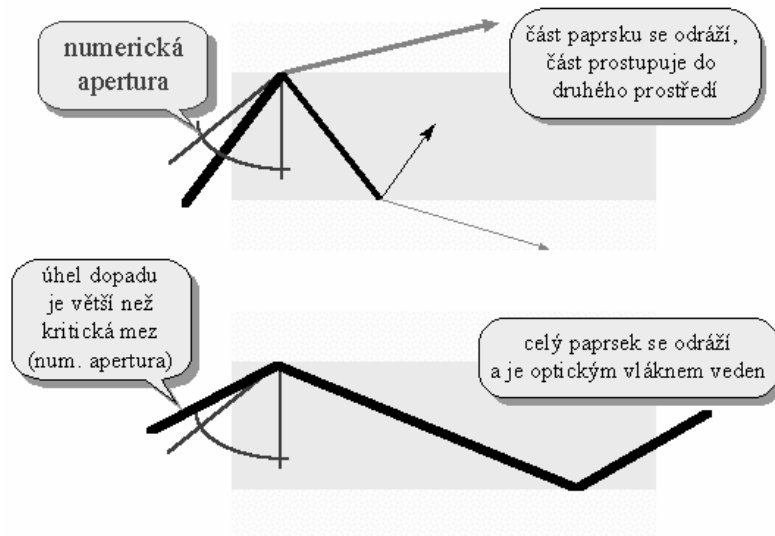
- vyžadují laserové diody
- až 100km bez opakovače

Provedení

-vnitřní , univerzální, venkovní, speciální

Vlastnosti:

- útlum
- šířka pásma
- průměr jádra
- numerická apertura $NA = \sin(\alpha)$



Bezdrátové spoje

- LASEROVÁ POJÍTKA
- SATELITNÍ KOMUNIKACE
- INFRAČERVENÉ LAN TECHNOLOGIE
- RADIOVÉ
- MIKROVLNNÉ

(více v samostatné přednášce)

Základní podsystémy strukturované kabeláže

Strukturovanou kabeláž můžeme definovat jako jednotný kabelážní systém pro budovy, který podporuje všechny typy komunikačních služeb digitálních přenosových prostředků jako je hlas, video, data, zabezpečovací systémy, Filosofii je jednotné jednoduché a přehledné budování univerzální kabeláže s dlouhou životností a zaručenou kvalitou (proměření), tedy nadčasového řešení snažícího se respektovat:

- možné budoucí změny při minimalizaci dalších nákladů
- možnost decentralizace systému,
- dlouhodobost (životnost morální i fyzická 10 až 15 let),
- vysoké rychlosti a
- možnost připojení nových HW technologií

Inspirována Ethernetem

Využívá hlavně twist a optiku

Normy rozlišují 3 základní podsystémy strukturované kabeláže

- **páteřní kabeláž** v rámci **areálu**, která spojuje rozvaděč areálu s rozvaděčem jednotlivých budov,
- **páteřní kabeláž** uvnitř **budov**, která spojuje rozvaděč budovy s rozvaděči jednotlivých podlaží a
- **horizontální kabeláž** vedoucí od rozvaděčů jednotlivých podlaží ke komunikačním vývodům.

Pro všechny typy kabeláží jsou definované maximální délky rozvodů bez ohledu na použitý typ přenosového média a

Součástí strukturované kabeláže jsou kromě samotných kabelových rozvodů, zásuvky, konektory, rozvaděče (rack), patch panely apod.

Rozvaděč

je základem páteřní kabeláže, označuje se jako RACK 19“ (19“ určuje rozteč rozvaděče – 19 palců).

Dělí se podle počtu možných připojených zařízení:

4U - nástěnný rozvaděč, lze připojit 4 zařízení (např. Patch panel, zdroj, ventilátor, ..)

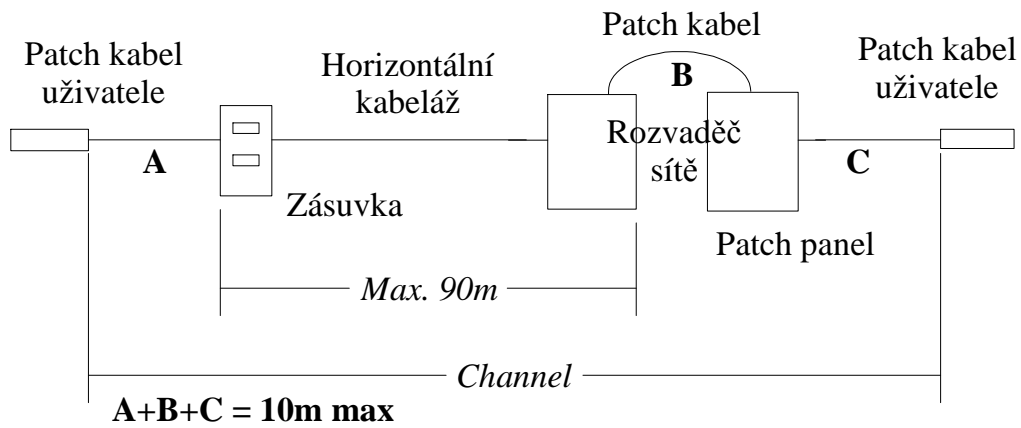
30U - stojanový rozvaděč. 1U = 1,75 palce (velikost jednoho zařízení).



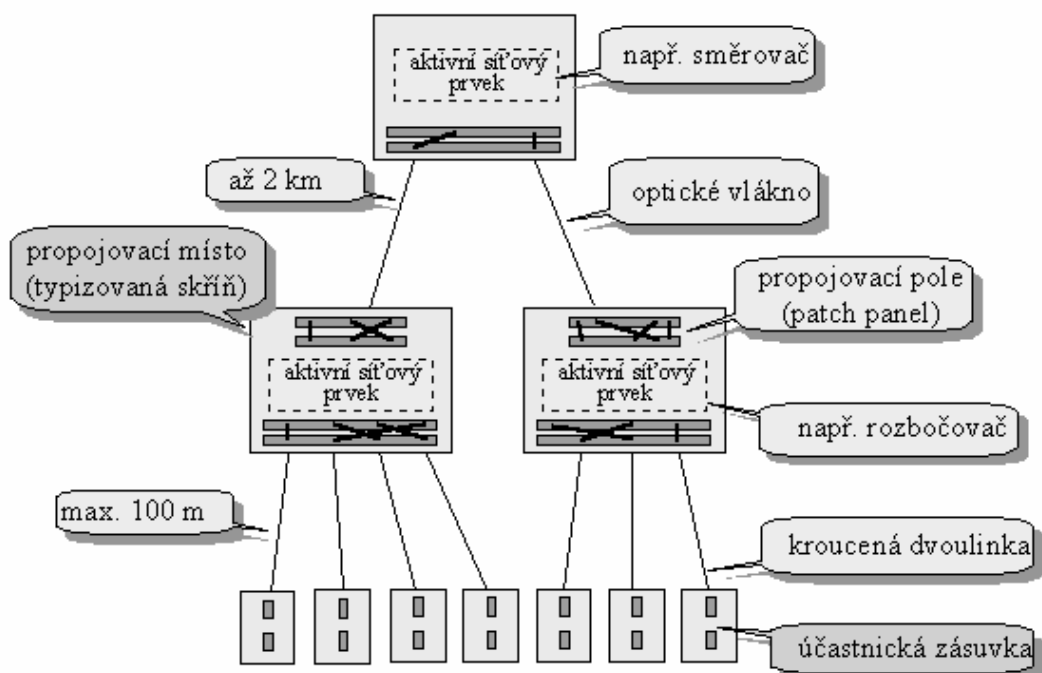
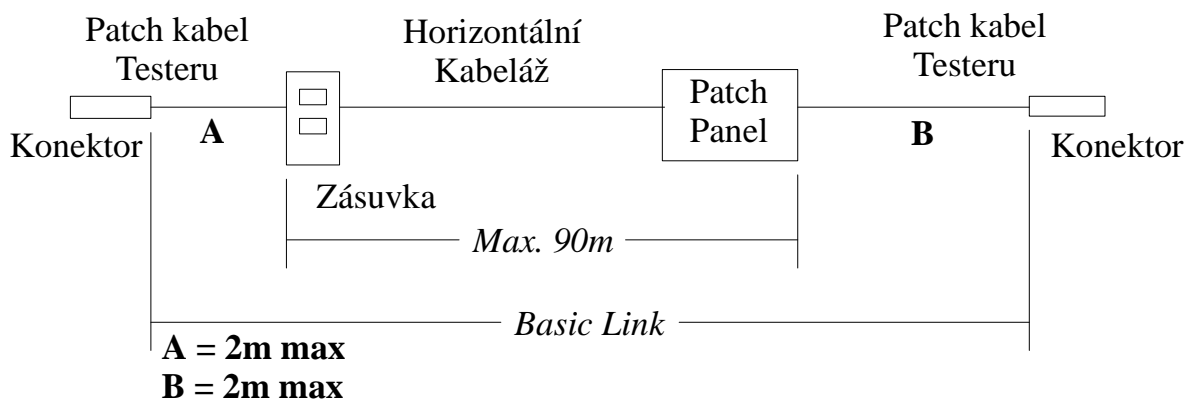
Basic Link a Channel

V TSB-67 byly definovány dvě základní konfigurace pro testování strukturované kabeláže:

Channel (kanál) je definován jako kompletní segment kabeláže včetně patch kabelu na straně uživatele a patch panelů včetně patch kabelů na straně rozvaděče.



Basic Link zahrnuje pouze horizontální kabeláž v segmentu od zásuvky počítače po první patch panel v rozvaděči.



Síťové prvky

Prostředky pro fyzickou vrstvu

ZESILOVAČE

Zesilovače pouze zesilují signály a nemohou měnit protokol ani fyzický druh přenosového kabelu. Pokud se mění druh kabelu na výstupu jedná se o **převodník - tranciever**. Protokol zůstává stejný. Maximální délka mezi krajními počítači je 185m. Pro kroucené dvojlinky je tato vzdálenost ještě menší. Proto na větší vzdálenosti se musí vkládat zesilovače a rozbočovače. U sítě Ethernet jsou nejjednodušší malé 2-portové **transievery**, které se používají k zesílení nebo přechodu z jednoho kabelu na druhý. Pro větší počet napojených kabelů se používají **Multiport Repeater**. Pro propojení více kabelů nebo několika druhů kabelů se používají **modulární rozbočovače** vybavené zdrojem a řadou slotů. Pro třídění paketů jsou používány Bridges (mosty).

OPAKOVAČE

neboli **repeatery** či **zesilovače** jsou tedy určeny pro propojení na větší vzdálenosti. Pracují na úrovni **fyzické vrstvy**. Poněvadž jsou spolu s huby “neinteligentní” tzn, nerozebírají hlavičky paketů, jsou rychlé a nebufrují signál. proto vzniklé zpoždění je rovno zlomkům bitového intervalu. Nemění charakter sdíleného přenosu. Spolu s huby se používají tam, kde většina komunikace se děje mezi serverem a stanicemi. Pokud je komunikace i mezi stanicemi je vhodné používat mosty, switche a routery. Opakovače mohou spojovat sítě o různých mediích, ale se stejným protokolem a rychlostí.

HUB - ROZBOČOVAČ

je ústřední prvek počítačové sítě s hvězdicovou topologií. Centrem takové sítě s hvězdicovou topologií spojujících jednotlivé uzly je právě tento hub. Je to tedy centrální bod, který poskytuje několika uzlům sdílený kanál. Nepodporuje full duplex na rozdíl od switchů. Je určen pro malé pracovní skupiny a v 100Mb sítích pro propojení i serverů. Je laciný a pomalý. Dnes se od nich ustupuje a přechází se na switching huby a hlavně switche.

Inteligentní **Switching Hub** jsou přepínatelné rozbočovače. Jsou vhodné zejména u virtuálních sítí a oddělených pracovních skupin. Pracuje stejně jako hub, ale síť je rozdělena do segmentů, z nichž každý obsahuje několik portů. Umí vyrovnávat zátěž změnou počtu portů na segmentu. Je laciný a podstatně výkonnější než hub.

Přepínání lze rozdělit do dvou skupin

- **statické** - Při statickém je zapotřebí ruční zásah. Při přepínání dochází k přemístění jednoho uživatele z jedné sítě do druhé.
- **dynamické** pracují automaticky. Vytváří se virtuální spojení mezi sítěmi podle **okamžitých** požadavků. V současné době se používají 4 základní druhy dynamických přepínačů
 1. Hardwarové přepínací matice a křížové přepínače. Jsou velmi rychlé. Přepínají na základě cílové adresy.
 2. Distribuované softwareově orientované přepínače používají architekturu známou z routerů. Mají vlastní procesory a komunikují na různých rychlostech s různými protokoly.
 3. Centralizované softwareově orientované přepínače. Mají stejné výhody jako distribuované.
 4. Distribuované hardwareové přepínače s velmi rychlou **páteří** sběrnici. Jsou osazeny rychlými procesory a zákaznickými obvody.

Standardy v rozbočovačích jsou implementovány do operačního mikrokódu, jehož změnou lze snadno realizovat nový standard. Rozbočovače jsou levnější a způsobují podstatně menší zpoždění než routery a jsou proto využívány ve virtuálních sítích.

Stackable (stohovatelné) huby se chovají jako jeden aktivní prvek. Obvykle mohou rozdělit až 16 segmentů. Jsou propojeny speciální vysokorychlostní sběrnici, která snižuje prodlevy.

Stohované huby lze také zapojovat do **kaskád**, přes kaskádovací porty. Třída Class II povoluje pouze vzdálenost 5m, ale pro huby, mající kaskádovací porty fungující jako dvouportový přepínač, který odděluje kolizní domény, mohou být vzdálenosti mezi stohy až 100m, při maximálním počtu 6. Kaskádní propojení zkracuje povolené maximální vzdálenosti.

Rozbočovače rozlišujeme

- třídy I - s omezením na 1 opakovač nebo stoh na segment (u 100Mb Ethernetu bez opakovače. Opakovače třídy I se musí spojit přes switche.
- třídy II - zvládnou dva opakovače nebo stohy na segment.

Správa hubů

Management sítí na úrovni fyzické vrstvy má na starosti zejména správu kabeláže a konfiguraci jednotlivých hubů a segmentů. (např. RIT technologies – PatchView)

Základem systému je elektronická jednotka nazývaná scanner, ke které jsou připojeny rozvodné panely. Scanner je dále spojen s počítačem administrátora přes síť. Panely musí být speciálně upravené (musí podporovat záznam vlastního propojení). Tyto panely vysílají informace o propojených portech scanneru a ten protokolem SNMP správci, který má přehled o fungujících a nefungujících propojeních.

Změna propojení : Nejdříve se nadefinují všechny změny v propojení na správcovské stanici a pak se odešlou na scanner příslušného patch panelu. Systém LED tak upozorní na to, kde spoje rozpojit a kde nově propojit. O propojení se vede databáze.

Pro 1Gb/s je nutné mít kabely (RJ-45) vybaveny ještě desátým vodičem, po kterém se provádí komunikace, při vyšších rychlostech lze využít vodič č. 7 nebo stínění.

Software má grafické zobrazení kabeláže.

Prostředky pro linkovou vrstvu

Tyto prvky určují dedikovaný systém přenosu, tj. umožňují provádět současně několik přenosů v jedné síti. Mosty, směrovače a switche bufferují pakety resp. rámce, aby mohly brát informace z jejich hlaviček. Proto zpoždění je větší než u opakovačů. Směrovače dokonce mění adresy (mají vlastní adresu v síti) a tak jsou z těchto prvků nejpomalejší.

Rozeznáváme dvě základní kategorie přepínání - **paketové a okruhové**. V paketovém přepínání se používají datové buňky (cells) pevné délky (rámec, pakety ethernetu, buňky ATM). U okruhového (circuit) přepínání je fyzické přepínání media na dobu přenosu celé zprávy.

BRIDGES - MOSTY

Mosty jsou konstruovány pro propojení kabelových segmentů jedné sítě a k zamezení jejich přetěžování. Mohou spojit segmenty s různou fyzickou vrstvou.

Mosty používají adresové informace z datové (linkové) vrstvy (vrstva 2) OSI. Přepojují rámce podle **fyzických adres**. V tabulce prohledává adresu rámce a podle ní najde patřičný port. Pokud se jedná o neznámou nebo univerzální (FFFF.FFFF.FFFF) adresu odešle balík na všechny své porty. Mosty mají schopnost se dynamicky učit a určovat přiřazení adres a portů. Bridges tedy provádějí filtraci paketů, které propouštějí jen pakety určené pro jiné síť do sousedních sítí. Tím odlehčují tyto síť. Zpracovávají pakety po sobě. Změna účastníka znamená změnu kabeláže.

Mosty předpokládají na každém vstupu jiný segment sítě.

Mosty stejně jako switche musí rozumět hlavičce linkových rámců (paketů), tj. na úrovni linkové vrstvy, kdežto hlavičkám na úrovni síťové vrstvy nerozumí. Proto nezáleží na typu protokolu (TCP/IP, IPX/SPX, NetBIOS (Microsoft), který přenáší. Stačí jim, když znají topologii sítě v bezprostředním okolí. Mosty a switche nejsou pro ostatní uzly viditelné, a také nejsou adresovatelné. Datový rámec proto putuje přímo ke koncovému adresátu.

Bridges přenášejí informace mezi LAN podle Media Access Control (MAC) adresy rámce (frame) bez změny původního LAN rámce. Z pohledu bridge (mostu) je síť rozdělena na dvě části. Bridge podle topologie sítě filtruje přenášené pakety, a přenáší pouze ty, které se týkají druhé části

sítě. Práce bridgů není závislá na síťových protokolech a proto je pro ně “průhledná”, tzn. nemění způsob práce sítě. Proto lze mosty bezproblémově instalovat a udržovat. Jsou nenákladné jak při pořízení, tak i pro údržbu a provoz. Jsou vhodné pro malé sítě. Pro velké sítě je vhodnější používat Routery. Nemohou vyhledávat optimální cestu a také bezpečnost dat je omezená, i když ji zvyšují.

Switch

Switche v lokálních sítích slouží k rovnoměrnému rozložení toku v jednotlivých částech sítě, především k poskytnutí co možná největší kapacity uzlům. Umožňují tak sdružovat do segmentu stanice s velkými a malými nároky na síť, kdežto stanice s velkými nároky spíše rozhazovat do různých segmentů. Je to centrální bod, který poskytuje každému uzlu jeho vlastní kanál.

Switche nerespektují přístupová práva a omezení, aby fungovaly rychle. Navíc toto nelze dělat na linkové úrovni. Práva lze respektovat až na síťové úrovni. Proto switche utváří po stránce přístupové jednotnou (homogenní) síť. Switche neumožňují vybudovat Firewall. Pro **oddělení práv je lepší používat směrovače**. Pro sdružování výstupů do segmentů jsou vhodné switche. Tyto pak do všech výstupů patřících do jednoho segmentu vysílají pakety naráz.

Přepínače umožňují využívat v uzlu kabel bez kolizí, směřují pouze na určený uzel a tak zbytečně nezatěžují kabely. Pracují na úrovni 2. (**linkové**) vrstvy OSI. Nevýhodou je vyšší cena za port. Další kategorií jsou přepínače pro 1GB/s sítě a 10GB/s sítě které jsou považovány za atraktivnější než ATM.

Switch neboli přepínač pracuje metodou

1. **Store and Forward**, kdy se paket nejdříve uloží do vyrovnávací paměti, zkontroluje a pak je zaslán na požadovanou adresu. Spolehlivá metoda. Jsou vhodné pro velmi zatížené LAN sítě a ATM.
2. **cut-through**, při které se okamžitě po zjištění adresy zahajuje vysílání, aniž by čekal na dokončení příjmu. Nelze provádět kontrolu. Jsou rychlejší, ale při horších kvalitách spojů, je nutné přenos opakovat po celé cestě, což cesty zbytečně zatěžuje. Další nevýhodou je, že paket musí být odmítnut popřípadě bufrován v případě, že destination segment je obsazený.

Zpoždění na switchích bývá řádově μ s. Switch odděluje od sebe různé počítače (sítě) a propojí mezi sebou jen ty výstupy, aby pakety, které mají tyto adresy, nebo adresu sítě, která je přes tuto síť přístupná, mohly procházet. Switch může se propojit přímo se stanicí pomocí full duplexu (nikoli přes hub).

Každý switch musí mít paměť, do které si ukládá kombinace adres MAC a čísel portů. Po zapnutí se zvláštními pakety vyptává na adresy a jimi plní paměť. Tyto pakety jsou broadcast čili všesměrové. Stejně tak označí i pakety, jejichž cílové nebo následující adresy nenašel v paměti adres.

Prostředky pro síťovou vrstvu

ROUTERS (Směrovače)

Routery umožňují propojit a oddělit jednotlivé sítě (i s různými protokoly) a tím zmenšit jejich zatížení a navíc umožňují je oddělit po stránce přístupových práv. Lze na nich budovat Firewally (mají filtrovací tabulky). a lze se přes ně připojit k Internetu.

Routery používají síťovou vrstvu (3. Vrstva) OSI, která pro každý typ síťového protokolu pracuje s odlišným adresovým schématem. Kompatibilitu mezi několika standardy zajišťuje router logikou, která je podstatně složitější než u mostů. Routery odbourávají z paketů hlavičky a taily linkové a fyzické vrstvy a nahrazují je novými. Routery musí mít dostatečnou vyrovnávací paměť, zejména tam, kde přechází z rychlejší do pomalejší sítě.

Jsou určeny k segmentování sítě, zajištění její bezpečnosti, řízení a přístupu na WAN.

Routers tedy provádí mnohem více softwarové činnosti než mosty. Směřují provoz podle síťových adres -adres 3. Vrstvy- (nikoliv fyzických) a propouští jen ty, které mají adresu v druhé části sítě. Pakety s neznámými adresami zasílají na sběrný port k implicitní síti, nebo je zničen.

Směrovací tabulka je založena na logickém uspořádání sítě a obsahuje adresy sítí (lze ji softwareově měnit). Směrovače s **dynamickým** směrováním dovedou stanovit pro nižší vrstvy

protokolu nejlepší cestu paketů s ohledem na využití a obsazenost cest. Urychlují tím přenos. Doplnění tabulky se děje také analýzou zaslaných paketů, kdy se určuje počet routerů přes které paket šel z dané sítě. Směrovače se **statickým** směrováním mají nulovou režii, ale neumí stanovit alternativní cestu. Routers jsou závislí na protokolu a dovedou transformovat protokoly jako jsou TCP_IP, IPX, DECnet, RIP, OSPF a další. Podporují řízení sítě a bezpečnost. Jsou vhodné pro rozšiřování sítí a pro velké sítě. Jsou nákladnější jak pro pořízení tak i pro provoz a údržbu. Směrovače tedy čtou hlavičky paketů 3. vrstvy. Jsou viditelné v síti a tedy mají svou adresu, na kterou jsou směrovány vysílané pakety. Tedy vysílací uzel musí znát adresu směrovače, který vede ven z dané sítě. Při vysílání paketů zapisují se do hlaviček i adresy směrovačů. Vzhledem k tomu, že směrovače jsou **závislé na protokolu** (IPX, TCP, ...) je nutné u většiny sítí používat víceprotokolové směrovače. Ty fungují jako několik samostatných jednoprotokolových směrovačů. Směrovače musí znát topologii celé sítě. Při směrování mohou být adaptabilní, tj. získávají informace o síti a přizpůsobují se změnám v síti, nebo neadaptabilní, pak nevyžadují monitorování sítě.

Routers dělíme na dva typy”

- **High End Routers**, které jsou komplexní zařízení. Podporují řadu protokolů (TCP_IP, IPX, DECnet, ...) paralelně, využívají RIP, OSPF a IS-IS protokol a další protokoly pro řízení přenosu a mohou také přenášet tzv. Non-routable protocols, jako jsou NetBIOS, LAT a SNA. Podporují multimedia v Ethernetu, FDDI, Token Ring a WAN a nabízí překlad nebo prostý přenos přes bridge, propojení zdrojů a konverzi SDLC na LLC. Jsou osazeny výkonným procesorem s velkou pamětí a bohatou softwarovou podporou. Vyžadují odbornou instalaci. Jsou drahé.
- **Low End Routers** neboli “access routers” jsou určeny k funkcím jako High End Routers, ale za nižší cenu. Mají méně LAN/WAN konektorů a chybí jim některé vyšší funkce.

Použití routerů závisí na požadavcích. Pro instalaci

- High End Routers jsou tyto požadavky
 - Vysoká rychlost přenosu,
 - vysoké využití sítě
 - časté změny,
 - vysoká výkonnost serverů, stanic a sítě.
 - Velká a rozvětvená síť
- Pro Low End Routers
 - malý počet různých protokolů (1 až 3),
 - nízký provoz
 - nižší počet stanic
 - Plug and Play.

Komplex routerů je vyžadován tam, kde je velká koncentrace výpočetní techniky, napojení LAN-WAN, místní a dálkové propojení. Řešení těchto sítí vede k

- distributed routing - rozložené routery po síti, nebo k
- centralized routing - CAR, kde jsou všechny pakety zasílány na jeden vyhrazený router - počítač
- hierarchical routing kdy jsou řídicí centrální počítače určené pro jednotlivé oblasti
- isolated routing - nezajímají se o směrování ven z dané sítě

Náklady na pořízení a zejména na údržbu jsou u distribuovaných systému mnohokrát vyšší, zejména při velkých sítích. Náklady zahrnují: konfigurace, instalace, údržbu, změny.

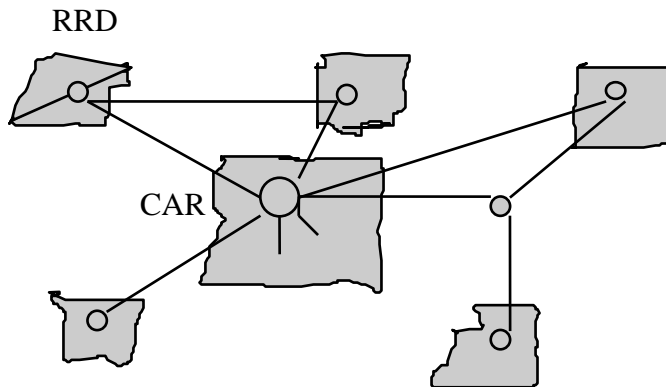
Ani router ani most není vhodný pro souvislý přenos dat, neboť není schopen udržet přímý přenosový kanál.

Pro přenos paketů pevné délky mohou být některé funkce přepínačů provedeny hardwarově a tedy jsou rychlejší. Routery mají buď sdílené busové struktury nebo **přepínače s křížovou** architekturou.

CAR

Central Access Routing - spínání s centrálním přístupem je způsob přístupu k síti. CAR soustřeďuje náročné High end routers do centrálního routeru, který je snadno přístupný technikům, a do Router Access Nodes - uzlů, které jsou jednoduchá zařízení rozprostřená po síti. Tyto uzly nevyžadují konfiguraci. Síť musí být koncipovaná tak, aby téměř všechny změny se prováděly pouze na centrálním routeru.

Ve složitějších sítích je funkce CAR rozprostřena do CAR a několika RRD - Regional Routing Domains. Přístup do WAN je pouze z CAR. Tento CAR také jako jediný převádí různé protokoly.



Routing switch

neboli směrující přepínač je obdoba přepínačů, ale funkce svázané s adresováním v síťové vrstvě jsou pevně svázané do vlastního přepínače, takže přepínače nemusí opouštět přepínající struktury. Tyto routery mají místo sdílené busové struktury **přepínače s křížovou** architekturou.

Prostředky pro vyšší vrstvy

Brána - Gateway

Brána je zařízení, které fyzicky propojuje vzájemně nekompatibilní sítě nebo zařízení. Typickou aplikací je připojení PC na mainframe nebo ke službám X.25. Pracuje v **relační, prezentační a aplikační vrstvě**. Často bývají řešeny softwarově jako vyhrazený server ve funkci gateway.