

Zařízení – fyzické, linkové a síťové vrstvy, principy a účel použití, topologie – vývoj, druhy, principy a vlastnosti

Přehled zařízení podle vrstev

1. fyzická vrstva
 - a. repeater (opakovač)
 - b. hub (rozbočovač)
2. linková vrstva
 - a. bridge (most)
 - b. switch (přepínač)
3. síťová vrstva
 - a. router (směrovač)

Repeater (opakovač)

Fyzická vrstva (propojit dvě dílčí sítě na úrovni fyzické vrstvy znamená zapojit mezi ně repeater).

Zařízení přijímá zkreslený, zašuměný nebo jinak poškozený signál na elektromagnetických nebo optických přenosových médiích, které signál opravený, zesílený a správně časovaný vysílá dále. Signál může být poškozen elektromagnetickým polem nebo ztrátami v médiu. Šum je odstraněn tím, že je příchozí signál obnoven do původní digitální podoby a poté je znovu vytvořen.

Repeater si lze představit jako jednoduchý digitální zesilovač, který si sice všímá jednotlivých přenášených bitů, ale nerozumí významu bitů. Chápe jen pouze jako logické hodnoty.



Více opakovačů za sebou umožňuje prodloužit dosah signálu v přenosovém médiu. Potřeba opakovačů vychází z toho, že při každém přenosu signálu dochází k určitému útlumu, zkreslení a dalším formám poškození přenášeného signálu. Signál tedy není bez opakovačů možné přenášet na libovolně dlouhou vzdálenost, protože po překročení určité hranice by poškození signálu bylo již tak významné, že by nebylo možné signál rekonstruovat.

Hranice dosahu je závislá na několika faktorech – na povaze přenosového média, charakteru signálu, přenosové rychlosti atd. V praxi z toho pak vyplývá, že není možné použít libovolně dlouhý úsek kabelových rozvodů – např. v případě klasického 10Mbps Ethernetu při použití kroucené dvojlinky je dosah jen cca 100 metrů.

Repeaterem mohou být propojeny pouze segmenty, které pracují se stejnou přenosovou rychlostí (k propojení různě rychlých segmentů je potřeba zařízení pracující na vyšší vrstvě – např. switch).

Důsledkem regenerace signálu, kterou repeater provádí dochází v přenosu ke zpoždění. Opakovač rozesílá regenerovaný signál do všech jemu známých segmentů – nemůže provádět žádnou selekci, protože rozumí pouze logickým hodnotám, nikoliv už např. hlavičkám paketu.

Opakovače neobsahují žádnou vnitřní paměť, do které by si ukládaly (byť jen dočasně) přenášená data. I z tohoto faktu pak vyplývá, že opakovače mohou propojovat pouze takové segmenty, které pracují se stejnou přenosovou rychlostí.

Repeatery přenášejí i takové věci, které by často vhodné přenášet nebylo – např. v případě Ethernetu a přístupové metody CSMA/CD, která zajišťuje koordinaci vysílání jednotlivých uzlů v situacích, kdy se uchází o právo vysílat po sdíleném přenosovém médiu. Repeatery nesmí výskyt kolize zastavovat, musejí ho naopak šířit do všech ostatních segmentů, do nichž má přístup, aby problém řešila ta zařízení, která jej řešit mají. Ze všech segmentů tak pak vzniká jedna kolizní doména.

Pro jednotlivé komunikující uzly nejsou v Ethernetu repeatery vůbec viditelné.

Hub (rozbočovač)

Fyzická vrstva. Rozbočovač je aktivní prvek sítě, který umožňuje její větvení a je základem sítí s hvězdicovou topologií. Hub se chová jako opakovač – všechna data, která přijdou na jeden z portů, jsou zkopírovány na všechny ostatní porty bez ohledu na to, kterému portu 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 hubů jsou switche (přepínače), které síťový provoz inteligentně směřují (mají přehled o tom, které zařízení je připojeno ke kterému portu a data pak odešlou pouze na daný port).

V současné době se huby již pro ethernetové sítě nevyrábějí a jsou nahrazeny přepínači, které nabízejí vyšší bezpečnost přenášených dat – u rozbočovačů mohl vidět jakýkoliv uživatel sítě veškerou komunikaci. U přepínačů toto není (tak jednoduše) možné.

Používají se pro sledování provozu na síti nebo tam, kde je vyžadováno malé zpoždění.

Splitter (rozbočovač v optických sítích; rozvětvovač)

Fyzická vrstva. Pro optické sítě se používá termín splitter. Toto zařízení slouží jako obousměrný optický větvící prvek a umožňuje sdílet kapacitu sítě. Na jeden splitter byl původně možné připojit maximálně 32 účastníků, novější řešení umožňuje až 64 účastníků na jednom splitteru.

Jedná se o pasivní prvek sítě. Nepotřebuje žádný vnější zdroj energie. Neprovádí zesilování ani jakékoli jiné úpravy signálu. Do sítě zavádí poměrně velký útlum – podle počtu výstupních portů.

Bridge (most)

Linková vrstva. Bridge označuje v počítačové síti síťové zařízení, které spojuje dvě části sítě na linkové vrstvě. Most je pro protokoly vyšších vrstev transparentní. Odděluje provoz různých

segmentů sítě a tím zmenšuje i zatížení sítě. Mosty mohou spojovat segmenty s různou fyzickou vrstvou.

Z pohledu mostu je síť rozdělena na dvě části. Most podle topologie sítě filtruje přenášené pakety a přenáší pouze ty, které se týkají druhé části sítě. Práce mostů není závislá na síťových protokolech, a proto je pro ně transparentní – nemění způsob práce sítě. Mosty lze proto bezproblémově a jednoduše instalovat a udržovat. Jsou nenákladné jak na pořízení, tak i pro údržbu a provoz. Jsou vhodné pro malé sítě nebo oddělení částí sítí. Pro velké sítě je vhodnější používat směrovače.

Princip činnosti

Most odděluje provoz dvou segmentů sítě tak, že si ve své operační paměti sám sestaví tabulku MAC 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 unicast rámců, které jsou určeny pro jediného příjemce; všesměrové rámce – multicast a broadcast – jsou naopak propouštěny bez omezení).

Způsoby přeposílání rámců

Liší se časovou náročností průchodu rámce mostem.

- a) **store and forward** – koncepčně pracují způsobem „ulož a předej“ – rámec z jednoho rozhraní přijmou, uloží do paměti, prozkoumají hlavičky (zkontrolují FCS) a následně odvysílají do příslušného rozhraní; chybný rámec zahodí
- b) **cut-through switching** – současná zařízení ale tento proces často optimalizují, takže k analýze hlaviček dochází, jakmile dorazí začátek rámce; ani s vysláním do cílového rozhraní se nečeká až dorazí celý rámec – zahajuje se co nejrychleji, aby zpoždění rámce bylo minimální; nekontroluje chyby; odešle i chybný rámec
- c) **fragment free** – rámec je přeposílán až po přijetí 64 bytů, po ujištění, že na daném segmentu nevznikla kolize – má význam v případě, kdy je připojen hub; minimální velikost rámce je 64 B; menší rámec je zahozen
- d) **adaptive switching** – automatické přepínání mezi třemi výše uvedenými metodami

Spínací zařízení musí uchovávat pakety, poněvadž výstupní port může být v daném čase obsazen nebo pracuje na jiné rychlosti. Podle toho, kde se vytváří fronta paketů se dělí zařízení na:

- a) **zařízení s pamětí (frontou FIFO) na každém výstupním portu** – vyslání paketu na výstup. port se provede až po odeslání všech předchozích paketů, tedy jeden paket čekající na uvolnění zbrzdí celou frontu
- b) **zařízení se sdílenou pamětí pro všechny porty** – obsazený port nebrzdí ostatní pakety jdoucí na jiné porty – vhodné pro velké objemy dat a porty s různou rychlostí

Samoučící se mosty

Most se učí topologii sítě podle toho, jak mu z různých stran přichází jednotlivé rámce – z adresy odesílatele a z faktu, že daný rámec přišel z určitého segmentu si domyslí, kde se příslušný odesílací uzel nachází. Pokud o příjemci ještě nic neví (tj. neví v jakém segmentu se nachází), most rozešle rámec na všechny existující strany. Z případné odpovědi si pak odvodí skutečné umístění příslušného uzlu (Backward Learning Algorithm) a informace si uloží.

Díky tomu je možné realizovat samoučící se mosty jako zařízení bez jakéhokoli konfigurování (na rozdíl od routerů). Stačí je zapojit do sítě a *ponechat osudu*. Po krátké fázi počátečního učení již fungují s maximální možnou efektivitou. Jediné, před čím je třeba samoučící se mosty chránit, je existence smyček: takový cyklus totiž může způsobit, že jeden a tentýž paket by se k mostu mohl dostat ze dvou různých směrů.

Samoučící se mosty jsou dnes typické pro prostředí Ethernetu (kde se jiné druhy mostů snad ani nevyskytují). Inteligentnější ethernetové mosty se přitom dokáží vyrovnat i s existencí cyklů: dovedou je rozpoznat a domluvit se s ostatními mosty na tom, že některý segment uměle vyřadí z provozu a cyklus tím odstraní.

Způsoby rozhodování o směrování

- a) **transparent bridging** – používáno především pro ethernetové sítě; mosty jsou neviditelné pro koncové stanice, kterým se propojené sítě jeví jako jedna lokální síť; most potřebuje znát topologii sítě, ve které se nachází – řešeno vhodným nakonfigurováním interních směrovacích tabulek (statickým naplánováním nebo pomocí samoučících se mostů)
- b) **source route bridging** – používáno ve spojení s token-ring sítěmi; oproti první metodě se kladou na most menší nároky – cílem je, aby byl co nejjednodušší; každý paket musí kromě adresy odesílatele a příjemce obsahovat také posloupnost adres všech mostů, kterými musí paket projít; propojovací uzly (mosty), přes které pak rámec prochází, tak mají minimum práce – pouze se podívají na příslušné místo do hlavičky rámce a zachovají se podle toho, co zde najdou; vysílající uzel si tedy dříve než pošle první paket musí zjistit celou cestu k cílové stanici prostřednictvím průzkumného rámce, který nejprve vypustí do všech stran a který se šíří na principu laviny (a po dosažení svého cíle se vrací zpět a informuje svého odesílatele o nejkratší cestě k cíli)

Switch (přepínač)

Linková vrstva. Aktivní síťová prvek propojující jednotlivé segmenty a uzly sítě. Obsahuje větší či menší množství portů – až několik stovek (obvyklý počet je od 5 do 128). Na ty se připojují síťová zařízení nebo části sítě. Pojem přepínač se používá pro různá zařízení v celé řadě síťových technologií.

Přepínač 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 malými nároky na síť, kdežto stanice s velkými nároky spíše *rozhozovat* do různých segmentů nebo přidělovat samostatné porty. Switch je centrální bod, který poskytuje každému uzlu vlastní kanál. Přepínač je specializovaný počítač obsahující CPU, paměť a OS.

Switche nerespektují přístupová práva a omezení, aby fungovaly rychle. Navíc zabezpečení nelze prakticky na linkové úrovni provádět. Proto switche utváří po přístupové stránce jednotnou (homogenní) síť. Neumožňují vybudovat firewall. Pro oddělení práv se používají routery. Pro sdružování výstupů do segmentů jsou však switche vhodné. Ty pak do všech výstupů patřících do jednoho segmentu vysílají pakety naráz.

Přepínače umožňují využívat v uzlu kabel bez kolizí – směřují pouze na určený uzel (segment) a tak zbytečně nezatěžují kabely. Nevýhodou je vysoká cena za port – proto je výhodné rozdělit síť na domény a teprve tyto domény spojovat pomocí přepínačů. Podporují *full duplex*.

Napájení je buďto samostatné nebo přes datový kabel. Tato zařízení jsou pak označována jako PSE – Power Source Equipment – ta musejí umět oddělovat data od napájení – a PD – Powered Devices – která dokážou posílat data po silovém vedení v datovém kabelu.

Přepínače obvykle nemají vypínač pro napájení.

Často dnes nabízejí i některé pokročilejší funkce, jako např.:

- a) **sdužování portů** (*port trucking*) – zvyšování rychlosti přenosu na *n*krát rychlost jedné linky; při sdužení až osmi portů se zvýší rychlost až na 800 Mb/s
- b) **VLAN** – podpora virtuálních sítí dle normy IEEE 802.1q (dot1q)
- c) **upřednostňování paketů** (*priority queues*)
- d) **řízení toku** (*flow control*) – zabraňuje ztrátám na přetížených linkách
- e) **automatická volba rychlosti přenosu** – dle kabeláže přepínač detekuje rychlost příp. sítě
- f) **správa přepínače** – pro konfigurace jsou přepínače opatřeny speciálními porty a/nebo mohou být konfigurovány přes síť (pomocí webového rozhraní HTTP/telnet), pak mají pro tento účel svou IP adresu
- g) **SNMP** – vzdálená správa zařízení, hlášení stavů a situací apod.

Switche dělíme na říditelné a neříditelné:

- a) **neříditelné** – jednodušší; slouží tam, kde není zapotřebí konfigurace; podporují automatickou volbu rychlosti přenosu, sdužování portu a VLAN
- b) **říditelné** – určeny pro budování rozsáhlejších sítí; mají jak metalické, tak i optické konektory; pro nastavení se používá řídicí port (RJ45) obvykle na boku přepínače, který se propojuje kříženým kabelem přes adaptér na sériový port počítače; podporují VLAN, prioritizaci, port trunking a flow control

Spínání sítí rozdělujeme na *symetrické* – všechny větve mají stejnou šířku pásma (rychlost přenosu) a na *asymetrické* – některá větev/větve mají odlišnou rychlost – u takových zařízení je nutné *bufferování*. Dvourychlostní přepínače umí automaticky detekovat podle kabeláže rychlost připojené sítě.

Ethernet switch

Přepínač se nejčastěji používá jako aktivní prvek v síti Ethernet realizované kroucenou dvojlinkou. Zde nahradil dříve používané rozbočovače, které signál jednoduše kopírovaly do všech ostatních rozhraní. Pracuje zde na linkové vrstvě ISO-OSI modelu. Vedle vyššího výkonu (stanice jsou připojené k různým rozhraním přepínače, takže navzájem nesoutěží o médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, jímž je připojen jejich adresát.

L3 switch a L4 switch

Díky svému rozšíření v Ethernetu se pojem switch vžil pro rychlý prvek rozhodující o dopravě paketů. Když se objevily ethernetové switche s rozšířenými funkcemi, které např. dokázaly analyzovat protokol IP a fungovat jako směrovače, začal se pro ně používat pojem L3 switch. L3 zde označuje 3. (síťovou) vrstvu modelu ISO-OSI, ve které takový switch 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 router. Přepínače pracující na třetí vrstvě musejí mít mimo tabulky MAC adres také tabulky IP adres a IP adresy několika (cca 10) switchů pracujících na třetí vrstvě (Next Hop Router).

Analogicky se lze setkat i s pojmem L4 switch – jedná se o switche schopné analyzovat protokol 4. (transportní) vrstvy modelu ISO-OSI a zpracovávat a filtrovat pakety např. podle čísel portů.

Přepínače pracující na vyšších vrstvách (3. a 4.) dovedou upřednostňovat přenosy a jsou vhodné pro VoIP a jiné časově senzitivní přenosy. Dále umí provádět autentizaci uživatelů.

Router (směrovač)

Síťová vrstva. Routery umožňují propojit a oddělit jednotlivé sítě (i s různými protokoly) a tím zmenšit jejich zařízení. Navíc umožňují oddělit sítě po stránce přístupových práv. Lze na nich budovat firewally (mají filtrovací tabulky) a lze se přes ně připojit k Internetu. Dalším úkolem routerů je šifrování – zejména u privátních sítí – a dále vysokorychlostní směrování a IP QoS (Quality of Service).

V TCP/IP sítích nepracuje s MAC adresami, nýbrž s IP adresami (pracuje na síťové vrstvě). Dále používá informace z vyšších vrstev jako je:

- a) informace o délce paketu (MTU length) – maximální délka spojové jednotky; pokud skutečná délka je větší, provede fragmentaci paketu (pouze IPv4)
- b) životnost paketu, její hodnota je každým průchodem uzlem snížena o 1 (TTL)
- c) priority
- d) koncové adresy

Kompatibilitu mezi několika standardy zajišťuje router logikou, která je podstatně složitější než u mostů. Směrovače odstraňují z paketů hlavičky a konce linkové a fyzické vrstvy a nahrazuje je novými. Hlavičku síťové vrstvy v podstatě nemění, pouze jí rozumí a řídí se jí. Směrovače musejí 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.

Routery vytvářejí broadcast domény. Musejí detailně znát připojené sítě (domény, podsítě) a musí umět tyto sousední sítě informovat o vlastní konfiguraci a směrovací tabulce. Pakety s neznámými adresáty se zasílají na sběrný port k implicitní síti nebo jsou zahozeny.

Směrovací tabulka je založena na logickém uspořádání sítě a obsahuje adresy sítí. Lze ji softwarově měnit. Routery se *statickým* směrováním mají nulovou režii, ale neumí stanovit alternativní cestu. Routery s *dynamickým* směrováním dovedou stanovit pro nižší vrstvy protokolu nejlepší cestu paketů s ohledem na využití a obsazenost cest (počet směrovačů, propustnost, zpoždění, zátěž cesty, spolehlivost, max. délka paketu). Urychlují tím přenos.

Jsou vhodné pro rozšiřování sítí a pro velké sítě. Jsou drahé a nákladné jak pro pořízení, tak pro správu. Jsou viditelné v síti – mají svou adresu, na kterou jsou směrovány vysílané pakety. Vysílací uzel tedy musí znát adresu směrovače, který vede ven z dané sítě – tzv. *default gateway*. Do hlaviček se při odesílání zapisují i adresy směrovačů.

Topologie sítí

Topologie sítí popisují, jakým způsobem jsou jednotlivé prvky sítě (uzly) propojeny.

Sériová topologie (serial)

Nejstarší topologie, aplikována na standardních rozhraních PC. Protokolem komunikace bylo rozhraní Centronics nebo RS232. Počet připojených stanic nebyl nijak omezen, při přidávání nové však došlo k narušení komunikace. Jsou zatěžovány mezilehlé uzly a při poruše jednoho uzlu nebo kabelu dojde k přerušení komunikace. Je zastaralá a již se nepoužívá.



Sběrníková topologie (bus)

Novější než sériová, aplikována na síťovém rozhraní PC – protokolem komunikace je Ethernet – je tu riziko kolize – vysílat může pouze jedna stanice. Počet připojení je topologií omezen (maximálně 20 uzlů/segment). Komunikace probíhá tzv. oběžníkovým způsobem – všemi směry – všechny stanice slyší komunikace všech ostatních stanic. Horší diagnostika poruch. K propojování uzlů se tu již používá koaxiální kabel nebo kroucená dvojlinka. Při poruše kabelu nastane přerušení komunikace. Již byla překonána a také se nepoužívá.

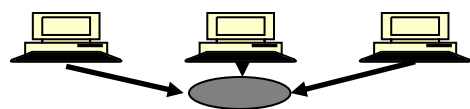
Oproti sériové topologii se snížila cena kabeláže, zjednodušila se projekce sítí a jejich rozšiřitelnost, zvýšila se rychlost komunikace a dosah sítí – překlenutelná vzdálenost. Vznikly nevýhody – zejména se zhoršila detekovatelnost poruch a kolizí a při zvyšování počtu účastníků se zkracuje délka segmentu.



Hvězdicová topologie (star)

Topologie aplikovaná na síťovém rozhraní PC – protokoly komunikace jsou ArcNet, resp. Ethernet. Počet připojení je omezen pouze protokolem. V komunikaci mezi body dochází ke směrování nebo přepínání. Je tu možnost současné komunikace mezi více body. Médiiem je kroucená dvojlinka, koaxiální kabel, případně optické vlákno. Přidání nebo odebrání stanice se obejde bez narušení komunikace. V současnosti jde o nejrozšířenější topologii.

Oproti sběrníkové topologii došlo k dalšímu snížení ceny kabeláže. Detekovatelnost poruch je snazší, přepínáním pak došlo ke zvýšení propustnosti. Nevýhodou je limit v rychlosti komunikace, která je pak dána cenou média.

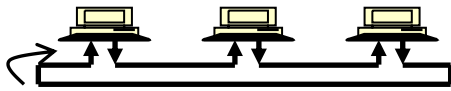


Kruhová topologie (ring)

Novější topologie než sériová, aplikovaná na síťovém rozhraní PC. Protokol komunikace je Token Ring (deterministická komunikace – od uzlu k uzlu). Počet připojení je omezen protokolem

(maximálně 255 uzlů/segment). Při přidávání nebo odebrání uzlu dojde k narušení komunikace. Médium je koaxiální kabel, kroucená dvojlinka nebo optické vlákno. Při poruše kabelu nebo uzlu dojde k přerušení komunikace. Prakticky jde o vylepšenou sériovou topologii.

Mezi výhody patří prakticky neomezená rychlost, kromě toho pak také obrovská překlenutelná vzdálenost (100 km/segment) a zvýšení spolehlivosti a konektivity bez narušení komunikace. Nevýhodou je pak vyšší cena a složitější protokol.



Dvojitá kruhová topologie (dual ring)

Vylepšená kruhová topologie odstraňující nevýhody topologie ring – při narušení vedení nebo při zapojování/odpojování stanice nedojde k výpadku a je zvýšena spolehlivost a propustnost. Komunikace je řízena protokoly FDDI a CDDI. Médium je optické vlákno – vysoká propustnost a spolehlivost. Využívá se u optických sítí P2P a P2MP. V optických sítích jde o moderní topologii.



Stromová topologie (tree)

Jde o hierarchickou topologii (víceúrovňovou – připomíná strom). Vychází z hvězdicové topologie. Vytváří se ve třech úrovních (vrstvách) – páteřní (backbone), mezilehlé (intermediate) a přístupové (access). Stromová topologie nabízí propustnost, spolehlivost a dostatek přípojných bodů. Dnes je stromová topologie používána v rozsáhlých sítích LAN.

Smíšená topologie (mixed)

Jde o hybridní topologii sítí. Umožňuje komunikaci různými linkovými protokoly. Mezi jednotlivé topologie jsou vkládány speciální uzly (routery a bridge). Síť vyžaduje jednotný globální „nadprotokol“ – IP, IPX apod. Jde o současnou topologii sítě Internet.