Vývoj počítačových sítí

Nespřažený přenos (off-line) – diskety
Spřažený přenos (on-line) – LPT – paralelní port
– COM – seriový port

Ústřední počítač – terminály
Vývoj z pohledu vlastní komunikace:

a) rezervovaný fyzický okruh
b) přepojování zpráv (neprobíhá ještě v reálném čase)
c) přepojování paketů (zpráva je rozčleněna na malé části s definovanou délkou)

1972 – vznikl počítačový uzel ARPANET (USA)
1980 – uveden na trh Ethernet – prosadil se hlavně díky jednoduchosti a levnosti a používal se v lokálních sítích LAN (10 Mb/s).

Klasifikace počítačových sítí:

1) ***Podle rozlehlosti:***
   a) *LAN – lokální sítě* – sdílení prostředků, větší přenosová rychlost, převažují pracovní stanice, vlastnictví technických prostředků.
   b) *WAN – rozsáhlé sítě* – přenos informací, menší přenosová rychlost, převažují servery, pronájem.
2) ***Podle rychlosti přenosu:***
   - klasické 10 Mb/s Ethernet
   - vysokorychlostní 100 Mb/s Fast Ether
3) ***Podle aplikace:***
   - počítačové sítě v informačních systémech
   - počítačové sítě v průmyslovém podniku

Nejčastější služby v informačních systémech:

- sdílení technických prostředků
- využívání společných dat
- elektronická pošta
- vzdálená správa počítačů
- komunikace

Architektura počítačových sítí

V sobě zahrnuje : – topologii
– formu komunikace
– základní služby

Datová komunikace mezi koncovými uzly, vyžaduje řadu možností:
(navázání spojení, přenos, zabezpečení).
Cílem standardizace je koncepce umožňující komunikaci nezávisle na technickém provedení (výrobci).
Výsledkem je referenční model ISO/OSI. Komunikace je rozčleněna na 7 základních vrstev se specifickými funkcemi a službami.
Předpokladem vrstevnatého modelu je, že komunikace probíhá v přesně vymezených přechodových bodech SAP (Service Access Points) a přesně definovaném rozhraní, které vymezuje jednotlivé služby, jejich způsob volání, výpočty parametrů, atd.
Komunikace probíhající mezi stejnolehlými vrstvami („peer“) definuje soubor pravidel označovaný jako protokol. Jedna a tatáž vrstva může používat více protokolů např. typ propojení, na způsobu přenosu, optický kabel.

Přehled vrstev ISO/OSI

7. Aplikační vrstva – poskytuje podpůrné funkce konkrétním aplikacím, elektronická pošta.
6. Prezentační vrstva – určuje a upravuje tvar dat (komprimace).
5. Relační vrstva – vytváří časové intervaly pro komunikaci.
4. Transportní vrstva – vytváří, rozkládá data na menší části tzv. pakety.
3. Síťová vrstva – zajišťuje adresování a směrování paketů.
2. Linková vrstva – zajišťuje spolehlivé spojení.
1. Fyzická vrstva – zabezpečuje přenos jednotlivých bitů.

Služby

spojované	**nespojované**	**spolehlivé**	**nespolehlivé**
informace vstupují a vystupují ve stejném pořadí	informace vstupují v jiném pořadí než vstupují	existuje zpětná kontrola	nepřichází zpětná kontrola

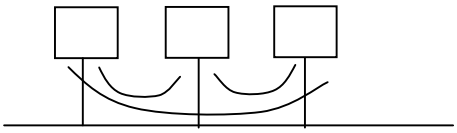
Model TCP/IP (Transport Control Protocol/Internet Protocol)

RM-OSI	TCP/IP
7. Aplikační	Aplikační
6. Prezentační	
5. Relační	
4. Transportní	Transportní TCP
3. Síťová	Internet IP
2. Linková	Síťové rozhraní
1. Fyzická	

IP protokol je založen na nespojovaném způsobu přenosu bloků dat nazývaných IP datagramy. Každý IP datagram ve své hlavičce nese informaci o adrese příjemce, proto může být po síti přenášen samostatně.
Internet je tvořen jednotlivými sítěmi, které jsou vzájemně propojeny pomocí směrovačů (Router) ty jednotlivé datagramy posílají podle adres příjemce.
TCP protokol zajišťuje komunikaci mezi aplikacemi běžící na vzdálených počítačích. TCP poskytuje spolehlivou transportní službu dat.
Protokoly TCP/IP představují souhrnné označení velkého množství protokolů, které spolu úzce souvisí.

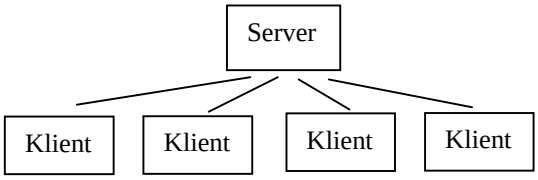
Charakteristické rysy sítí

Sítě „peer–to–peer" (každý s každým)



- zdroje sdílených dat se mohou nacházet na libovolném počítači v síti (i ostatní sdílené prostředky), to je vykoupeno menší propustností sítě.
- každý počítač může vystoupit jako klient nebo server – symetrická síť.
- obvykle nemají správce, jsou jednoduché na instalaci i provoz.
- LANTASTIC, NetWareLite, od Win 3.11 ->

Sítě serverového typu



- všechny sdílené prostředky jsou na jednom místě – serveru.
- používá se pro větší sítě, má větší výkonnost, jsou definováni klienti a servery – asymetrická síť.
- větší náročnost na instalaci a údržbu, správce sítě.
- Novell Net Ware, Windows NT.

Privátní sítě – slouží jednomu subjektu, který odpovídá za provoz a je současně i vlastníkem.
Veřejné datové sítě – PDN (Public Data Networks), potřeba licence ČTÚ.

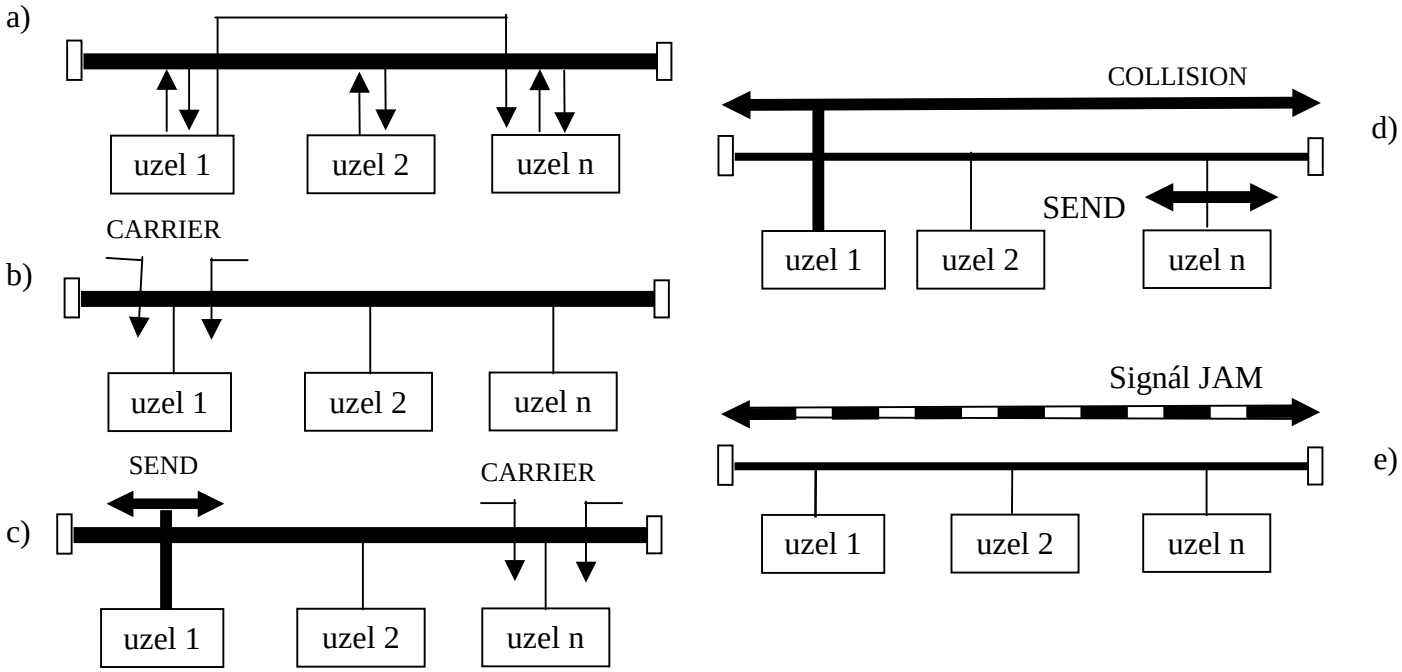
Použité technologie:

sítě standartu X.25 (1974) – vychází s telekomunikačních sítí, definuje sice přepojování paketů, ale zajišťuje spolehlivou službu.
sítě ISDN (Integrated Service Digital Network) – jedná se o digitální technologii, která vyniká dobrou kvalitou a spolehlivostí. Technologie ISDN má v sobě integrováno mnoho služeb např. umožňuje současný přenos hlasových a datových signálů. Základní přenosová rychlost je 64 kb/s a v současnosti se nejvíce využívá pro jednouživatelské přípojky (internet).
sítě ATM (Asynchronous Transfer Mode) – stejně jako ISDN, podporuje různé přenosy (data, hlas, video) na rozdíl od jiných technologií (X.25) používá pakety pevné délky s pravidelným odesíláním. ATM patří mezi spojované služby, před vlastním přenosem je navázáno a sestaveno spojení specifikující přímo v paketech, což značně urychluje přenos. ATM je definováno nezávisle na přenosovém mediu (bezdrátový přenos).

Ethernet

Přístupová metoda ethernetu – využívá se společného přenosového média, tím vzniká problém koordinace vysílání a příjmu tak, aby nevznikaly kolize.
Přístupové metody, které využívají možnost při poslechu (sledují provoz na síti) se obecně označují jako CSMA (Carrier Sense Multiple Access).
Pokud uzel zjistí probíhající přenos, počká na konec přenosu a začne vysílat svým.
Lepší variantou je pokud se uzel odmlčí na náhodně zvolený okamžik z množiny náhodných znaků. Tak se může stát, že dva uzly zvolí stejný čas.

Kolizní metody



1) podle obrázku a) se vysílací uzel chová na společné sběrnici jako výlučný majitel přenosového média až do ukončení vysílání, nebo detekce kolize.
2) podle obrázku b) uzel, který se připravuje na vysílání, nejprve poslouchá, zkoumá volnost sběrnice (carrier). Pokud je obsazena pokračuje v testování.
3) po uvolnění sběrnice uzel zahájí vysílání na médium podle obrázku c).
4) v případě, že začne po uvolnění média vysílat současně více než jeden uzel, obrázek d) nastane po krátké době kolize, to je narušení vysílání dat, kterou vyhodnotí jeden z vysílajících uzlů na základě neshody vysílaných dat a dat na médiu.
5) Ten uzel, který kolizi rozpoznal jako první, vyšle krátký signál JAM, obrázek e) na který reagují všechny stanice přerušením vysílání. Po určité době, jejíž velikost je řízena generátorem náhodných čísel, se uzel pokusí o nový vstup. Tím je zabezpečeno, že kolize nenastane opět pro stejné uzly. Kolizní okno má šířku 45 μs.

Časová analýza vzniku kolize

Vysílaný paket musí mít takovou délku aby kolizní situace byla vyhodnocena dřív všemi prvky sítě, než skončí vysílání paketů, která kolizi způsobil. Vezmeme-li v úvahu rychlost šíření a maximální délku sběrnice dostaneme pro spolehlivou detekce kolize minimální velikost paketu 72B Maximální zpoždění vedení je 25 μs.

Formát paketu pro Ethernet
používají se dva typy, které se liší velikostí a významem jednotlivých bitových polí.

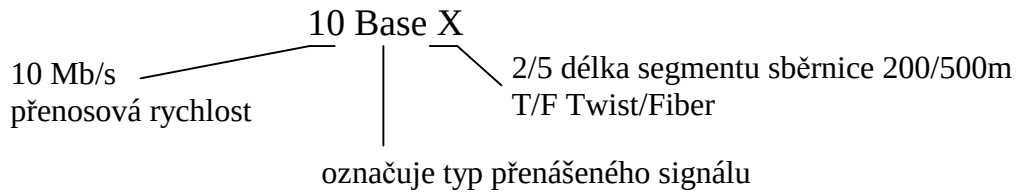
P	DA	SA	TYP	DATA	FCS
8B	6B	6B	2B	46B – 1500B	4B

P – Preamble – pole pro synchronizaci.
DA – Destination Address – adresa přijímací stanice.
SA – Source Address – adresa vysílací stanice.
TYP – Type – identifikátor vyšších vrstev.
DATA – data.
FCS – Frame Check Status – zabezpečení proti chybám.

P	SFD	DA	SA	L	DATA	PAD	FCS
7B	1B	2B – 6B	2B – 6B	2B	LLC+PAD = 46B – 1500B		4B

P – Preamble – pole pro synchronizaci přijímací stanice.
SFD – Status Frame Delmiter – příznak začátku rámce, je součástí synchronizačního pole a udává skutečný začátek rámce.
DA – Destination Address – cílová adresa MAC stanice.
SA – Source Address – zdrojová MAC adresa vysílací stanice.
L – Laught – dékla, určuje počet slabik v datovém poli.
DATA – Data – datová část rámce pro pole LLC a vlastní data.
PAD – výplň po dosažení minima délky rámce 72 MB.
FCS – Frame Check Status – kontrolní pole pro kódové zabezpečení CRC.

Sběrnicová síť



10 Base 5

Představuje původní koncepci Ethernetu, základem je koaxiální sběrnice tvořená silným (žlutým) kabelem, k němuž jsou paralelně, pomocí externích jednotek, připojeny jednotlivé stanice.
Charakteristika:

1) Přenosové médium – kabel ∅ 10 mm, Z = 50 Ω, útlum 8,5 dB. Konce sběrnice musí být zakončeny terminátory o Z = 50 Ω.
2) Připojení na sběrnici je provedeno pomocí speciálních konektorů (vampírů), které umožňují připojení bez přerušení sběrnice.
3) Externí jednotka – připojena přes konektor ke sběrnici 8-mi žílovým kabelem s maximální délkou 50 m a 15-ti kolíkovým konektorem Cannon. Na jedné sběrnici 500 m je možno připojit maximálně 100 externích jednotek.

10 Base 2

- vznikla z požadavků využití již existujících nebo levnějších koaxiálních rozvodů, které využívali typ kabelů menšího průměru a s menší tloušťkou opletení – tenký koaxiální kabel.
Charakteristika:

1) Přenosové médium je tvořeno tenkým koaxiálním kabelem RG58, Z = 50 Ω, útlum 8,5 dB. Maximální délka sběrnice zakončené terminátorem je 185 m.
2) Připojení ke sběrnici je realizováno konektorem BNC přes tzv. T-článek, který představuje pasivní rozbočení.
3) Externí jednotka využívání u silného koaxiálního kabelu je zabudována přímo do síťové karty. Maximální vzdálenost mezi jednotlivými odbočeními (T-články) je 50 cm maximální počet 30.

Sítě 10 Base 2 se prosadily díky své jednoduchosti, nižší ceně. Jejich nevýhodou je však menší dosah, horší odolnost proti rušení a nižší spolehlivost daná velkým počtem mechanických konektorů.

Pasivní prvky koaxiálních sítí

- přenášejí elektrické signály, ale nijak je nepřetváří.
Koaxiální kabely – impedance Z – zdánlivý odpor, který představuje kabel pro zařízení, ke kterému je připojen. Pro dosažení co nejlepšího přenosu by měly být impedance kabelu i zařízení shodné. Útlum – charakterizuje míru zeslabení signálu pří průchodu kabelem je vyjádřen v dB a log $\frac{\text{signál na vstupu}}{\text{výstup kabelu}}$ určité délky.

BNC – konektory (Bayonet Naur Connector) - využívají bayonetového uzávěru (konektor je opatřen 2 výstupky na něž se nasune proti kus a pootočením zajistí proti uvolnění. Souosá spojka slouží k propojení koaxiálního kabelu.
BNCT – konektor - umožňuje odbočení signálu z koaxiálního kabelu, obvykle se připojuje přímo k síťové kartě. Zakončovací odpor (Terminátor) – jeho úkolem je pohltit signál, který dojde na konec kabelu, aby nedocházelo k odrazům. Od konce vedení je realizován BNC konektorem k němuž je připojen ohmický odpor 50 Ω.

Jednotka připojení k přenosovému médiu MAU (Medium Attachment Unit) – jsou to elektrické obvody, vysílače a přijímače dat, jejichž zapojení závisí na typu použitého přenosového média (koax, kroucená dvojlinka, optika, atd.). Na typu média závisí také systém detekce kolize. Jednotka MAU může být realizována jako externí nebo je součásti přímo síťové karty.

pozn.: Někdy se můžeme setkat s pojmem GDI (Medium Dependent Interface), který představuje konektor určený pro připojení na konkrétní přenosové médium.

10 Base T

- nedostatky sběrnicových sítí umožnily vznik nové technologie, která využívá jako přenosové médium kabely tvořené kroucenými páry UTP (Unshielded Twisted Pair).
Charakteristika:

1) Přenosové médium je kroucená dvojlinka UTP kategorie 3 – 5 (určuje maximální přenosovou frekvenci) (3, min 25 MHz) Pro vlastní komunikaci se využívají dva páry vysílající, přijímací.
2) Připojení je realizováno telefonním konektorem RJ45 (kontakty 1, 2 vysílací pár 3, 6 přijímací pár).
3) Jednotka MAU zabezpečuje vysílání a příjem po samostatných párech vodičů, pracuje tedy s úplným duplexním provozu (současně může vysílat i přijímat data).

Topologie sítí založených na UTP kabelech je hvězdicová (stromová).
Nelze totiž zajistit jednoduchým způsobem odbočení signálu, jako u koaxiálního kabelu. Pomocí kroucené dvojlinky lze realizovat pouze spoj, takže jeden konec můžeme připojit do koncového uzlu a druhý ke speciálním elektronickým obvodům, které zaručují potřebné rozbočení.
Těmto obvodům se říká rozbočovač (HUB) - rozbočovač nemá dáno, jak má jednotlivé segmenty připojovat. Můžeme se setkat s různými principy:

- princip opakovače
- princip switchu (mostu)
- princip směrovače

U Ethernetu se nejčastěji v jednotlivých sítích setkáme s funkcí opakovače kdy signál z jednoho segmentu je automaticky přenášen na segmenty ostatní. Počet segmentu HUBu je volitelný. Další výhodou je, že při poruše na jednom kabelu není nijak ovlivněn provoz zbývající sítě (HUB vadnou větev odpojí).
Lze realizovat poměrně jednoduchým způsobem rozšíření sítě pomocí tzv. zřetězení HUBu (vzájemné propojení).
Rozbočovač bývá k dispozici možnost připojení na jiný typ segmentu na jiný kabel než kroucená dvojlinka.

10 Base FX

- patří vývojově mezi nejmladší sítě, je založena na použití optických vláken. Používá se pro překlenutí větších vzdáleností nebo při potřebě vzájemné izolace budov.
Charakteristika:

1) Přenosové médium je optické vlákno se samostatným vysílacím a přijímacím vláknem, kterými se signál šíří prostřednictvím světelných impulsů, dosah se pohybuje do 2000 m.
2) MAU – je tvořeno externí optickou jednotkou, která je připojena pomocí 15-ti kolíkového kolíku Cannon. Systém přenosu je realizován jako Full duplex – po samostatném vysílacím a přijímacím vláknem. Rozbočení zabezpečují HUBy obdobné funkce jako u kroucené dvojlinky, které ale používají na výstupu optické jednotky (MAU).

Přepojování na linkové vrstvě – při přepojování přenášených bloků dat v uzlu HUB je blok nejprve načte a uloží do vyrovnávací paměti, potom se analyzuje a rozhodne co s ním a výsledek rozhodnutí vykoná. Obvykle se blok dat odešle v určitém směru, nebo se zjistí, že blok není potřeba dál odesílat a vymaže je.
(forwarding – předávání dál filtering – mazání)
Při přepojování na linkové vrstvě jsou rozhodující informace umístěny v hlavičce rámce.

Adresy používané na úrovni linkové vrstvy - V případě IP paketů se používá 32 bitová IP adresa.
- chovají se jednorozměrně, což odpovídá představě, že všechna zařízení prou pohromadě a síť není nijak dělená na menší samostatné celky => že na úrovni linkové vrstvy se předpokládá přímé spojení mezi jednotlivými uzly, a možnost adresovat každý rámec přímo adresátovi.

Adresy používané na úrovni síťové vrstvy
- vycházejí z představy rozdělení sítě na menší samostatné celky, které mají nějaký svůj identifikátor. Adresa je pak složena se dvou částí, kde 1. část vyjadřuje dílčí samostatnou síť a 2. část relativní adresu v rámci dílčí sítě.

Přepojování na úrovni linkové vrstvy
Mosty (Bridge) – jde o zařízení realizující přepojování na úrovni linkové vrstvy s jednoduchým rozhodováním, neboť předpokládá, že má s každým uzlem přímé spojení. Most rozhoduje pouze o tom, ve kterém směru od něj daný uzel leží. Typické použití mostu je při propojení jednotlivých částí lokálních sítí realizovaných koaxiálními kabely. (Řeší se tím technické problémy – délka kabelu).

Most uskutečňuje vzájemné propojení segmentu, tak aby byl možný přenos dat mezi nimi, kromě toho dokáže rozlišit situaci, kdy je rámec adresován příjemci ve stejném segmentu a příslušný rámec do jiných segmentů nepřenášet (filtrace).

Konfigurace multisegmentových sítí Ethernet

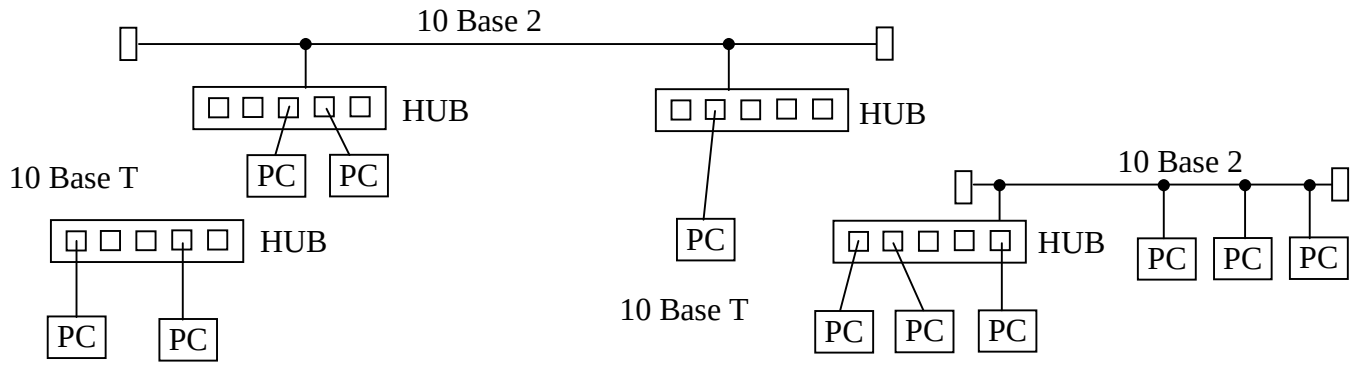
- při vytváření rozsáhlejší sítě (např. celopodniková síť) je při řešení nutno vycházet z určitých omezení, které vyplívají z přístupové metody Ethernetu. Při určování maximálního dosahu multisegmentové sítě se používají základní metody.
Model 1 – je založen na doporučení, při jejichž splnění je zajištěna funkčnost u všech typů sítí Ethernet .

1) přenosová cesta mezi dvěma uzly (počítači) nesmí procházet přes více než 5 segmentů, 4 huby (ve funkci opakovačů)
2) huby (opakovače) – musí zabezpečit regeneraci signálu v čase, úrovni a synchronizační impulsy.

Model 2 – podle tohoto modelu se při posuzování sítě vychází z výpočtu, které kvantifikují 2 kritické parametry sítě.

1) maximální zpoždění přenosové cesty
2) zkrácení mezirámcové mezery

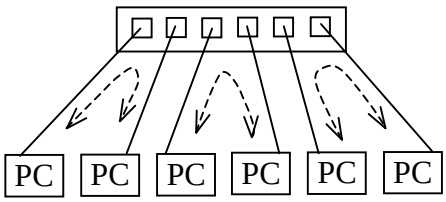
Příklad multisegmentové sítě



Přepínaný Ethernet

V případě přepínaného Ethernetu nepracuje aktivní prvek sítě v režimu opakovače, ale přenášené rámce předává pouze mezi porty příslušných komunikačních počítačů tzn. že tyto počítače mají k dispozici celé přenosové médium a mohou využít maximální rychlosti pro přenos.

Ideální komunikace

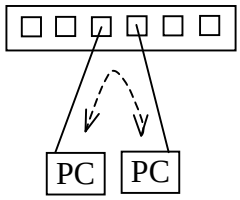


Komunikaci mezi libovolnými 2 uzly dokáže přepínač realizovat takovým způsobem, že signál se nepřenáší do ostatních segmentů sítě, ve kterých může probíhat další komunikace.

Přepínače využívají 2 základní metody přepínání:

1) Store-And-Forward – každý rámec se načte do vnitřní paměti, zkontroluje se jeho bezchybnost a podle cílové adresy se přesune na odpovídající výstupní port. U této metody dochází k většímu zpoždění a nelze přesně stanovit za jakou dobu bude rámec přenesen (různá velikost rámců). Výhodou je, že můžeme přepínat segmenty pracující s různou přenosovou rychlostí, nebo různou strukturu rámců.
2) Cut Through (rychlé přepínání) – zrychlení přepínání se dosahuje tím, že do vyrovnávací paměti se načítá pouze hlavička rámce a po dekódování příjemce je příslušný rámec přímo přesouván na odpovídající port. Přenáší se všechny rámce (i poškozené), nelze je nijak opravovat a tento způsob neumožňuje propojení segmentů s různou přenosovou rychlostí.

Úplné duplexní propojení (Full Duplex)



Vzhledem k tomu, že přepínače vytváří samostatné dvojbodové spojení, není třeba využívat kolizní metodu Ethernetu. Je potom možné vytvořit plně duplexní propojení, kdy obě stanice nohou současně vysílat i přijímat Tato metoda je vhodná k vytváření páteřních sítí, kde poskytuje lepší vlastnosti než řešení na bázi koaxiálního kabelu.

100 Base T (Fast Ethernet)

Navazuje na vlastnosti 10 Base T, podporuje stejnou technologii: kabeláž, využívá stejnou přístupovou metodu a stejné typy rámců. Změny se promítly pouze u fyzické vrstvy, která musí zajistit 10-ti násobné zkrácení doby přenosu signálu. To se nejvíce projevilo v celkovém dosahu sítě. Další rozdíl je v tom, že aktivní prvky (HUBY) pracují ve dvou třídách režimu.

Protokoly vyšších vrstev

Návaznost protokolů vyšších vrstev na fyzickou a linkovou vrstvu.

Fyzická a linková vrstva je implementována (sdružena) prostřednictvím síťová karty a programu ovládače karty, návaznost protokolů je potom definována rozhraním ovládače. Pomocí tohoto rozhraní přistupují protokoly ke službám linkové vrstvy. K nejčastějším funkcím patří výběr formátu rámce.

Multiplex/Demultiplex

Zabalování a rozbalování paketů. Poskytování služeb vyšším vrstvám. Toto rozhraní nevylo zatím přesně standardizováno nejvíce se využívají následující:

a) rozhraní PKDRV (Packet Driver) které vylo specifikováno pro protokoly TCP/IP.
b) rozhraní NDIS (Network Driver Interface Specification)
c) rozhraní ODI (Open Data Link) Novell.

Protokolová sada TCP/IP

- jejichž hlavním posláním je umožnit vzájemné propojení různorodých počítačových systémů. S těmito se setkáme zejména při používání počítačové sítě Internet. Konkrétním příkladem protokolů síťové vrstvy je protokol IP, jeho hlavní funkce je směrování paketů od zdrojového k cílovému uzlu mezi jednotlivými sítěmi. IP protokol je základním přenosovým prostředkem, protože informace vyšších vrstev jsou obsaženy v datové čísti IP paketů. Jednotlivé sítě jsou mezi sebou propojeny zařízením pracujícím na principu sítové vrstvy, které jsou nazývány směrovače (Router). Směrovače mají přehled o okolních částech sítě, dokáží určovat cestu z jedné sítě do druhé. Ke své činnosti směrovače používají např. tzv. směrovací tabulky.

Adresace uzlů v síti IP

Sítě využívající IP protokol používají tzv. hierarchické. Systém adresace umožňuje vytváření strukturované sítě, která je rozdělena na podsítě. Záhlaví IP paketu je pro adresu zdrojového a cílového uzlu je vyhrazeno pole o velikosti 32 bitů. Toto číslo jednoznačně určuje síť a konkrétní uzel. V protokolech TCP/IP rozlišujeme 3 třídy adresace A, B, C které se liší počtem adresovatelných uzlů (počítačů) a sítí.

Třída A

0	adresa sítě	adresa uzlu
0 b	1 – 7 b	8 – 31 b

Třída B

1	0	adresa sítě	adresa uzlu
0 b	1 b	2 – 15 b	16 – 31 b

Třída C

1	1	0	adresa sítě	adresa uzlu
0 b	1 b	2 b	3 – 23 b	24 – 31 b

Charakteristiky tříd adres

A	000 – 127.x.y.z	128 sítí	16 777 216 uzlů
B	128 – 191.x.y.z	16 386 sítí	65 536 uzlů
C	192 – 233.x.y.z	2 097 152 sítí	256 uzlů

Směrování a přenos datagramů po síti

Ke směrování mezi odesílacím a cílovým uzlem se využívá systém adresace s pevně přidělenou adresou sítí. Směrování mezi sítěmi realizují tzv. směrovače, které mohou pracovat následujícími způsoby:

1) Přímé směrování (Direct Routing) – používá se v případě, že obě síťové adresy jsou shodné. IP paket se směruje přímo na cílový uzel ve stejné síti.
2) Nepřímé směrování (Indirect Routing) – Použije se v případě rozdílných adres zdrojového a cílového počítače. IP paket se odešle dalšímu směrovači, který zajistí odeslání cílovému počítači nebo dalšímu směrovači.
3) Implicitní směrování (Default Routing) – se použije tehdy, je-li zdrojová síť připojena k vnější síti přes jediný směrovač. V tomto případě není potřebná směrovací tabulka a postačuje znalost IP adresy směrovače.
4) Směrování podle směrovací tabulky (Route Table Routing) – je-li zdrojová síť připojená k vnější síti přes několik směrovačů, musí každý uzel disponovat vlastní směrovací tabulkou, podle této tabulky si vybere odpovídající směrovač pro danou cílovou adresu. Směrovací tabulku lze vytvářet ručně – správce sítě nebo automaticky s informací odeslaných směrovači pomocí směrovacích protokolů.

Maska podsítě (Sub network Mask)

IP protokol poskytuje možnost členění sítě na podsítě pomocí tzv. masky. Vychází se z principu identifikace adresy sítě pomocí logického součinu konkrétní IP adresy s maskou podsítě. Maska je 32 bitové číslo skládající se z logických jedniček v polích adresy sítě a logických nul v polích uzlů.

IP:	172.16.1.254	10101100.00010000.00000001.11111110	
Maska:	255.255.255.0	11111111.11111111.11111111.00000000	
Síť:	IP & Maska	10101100.00010000.00000001.00000000	172.16.1.0

Základní pravidla pro používání masek:

1) jedničky začínají zleva bez přerušení
2) podsítě ze samých nul se nedoporučují
3) podsítě ze samých jedniček nejsou povoleny
4) adresy sítí ze samých nul a jedniček nejsou povoleny
5) adresy uzlů ze samých nul a jedniček nejsou povoleny

Příklady:

a) maska podsítě tvořena jedním bitem

maska sítě (IP typu C) 255.255.255.128 11111111.11111111.11111111.10000000
2 podsítě 1 – podle pravidla 3) zakázáno
0 – podle pravidla 2) nedoporučeno
nelze použít

b) maska podsítě tvořena dvěma bity

255.255.255.192 11111111.11111111.11111111.11000000

dostane podsítě 00 – nedoporučeno
01
10
11 – zakázáno

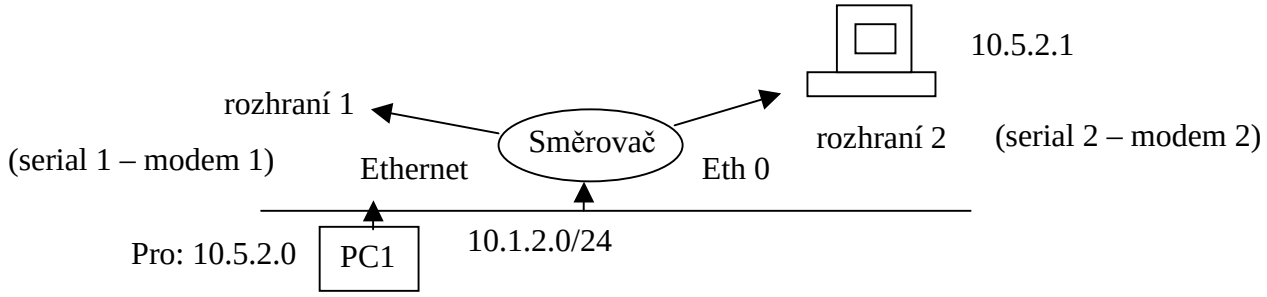
pro podsíť 01 je možné adresovat uzly 6 bity 01]000000 až 01]111111 to je (64 až 127) – 2 = 62 počítačů (dle pravidla 5)) Počet počítačů v podsíti můžeme určit jako $2^N - 2$ kde N je počet nul v masce. Při použití masek dochází ke ztrátám použitelných adres pro uzly i sítě.

maska: 255.255.255.192
IP: 192.16.8.65 ….. 192.16.8.126

192.16.8.90 => adresa sítě, adresa podsítě, 2 bity síť: 192.16.8.0 podsíť: 192.16.8.64

Adresa sítě IP: 10.0.0.238 00001010.00000000.00000000.11101110
maska: 255.255.255.240 11111111.11111111.11111111.11110000
00001010.00000000.00000000.11100000 10.0.0.224

Směrovací tabulky



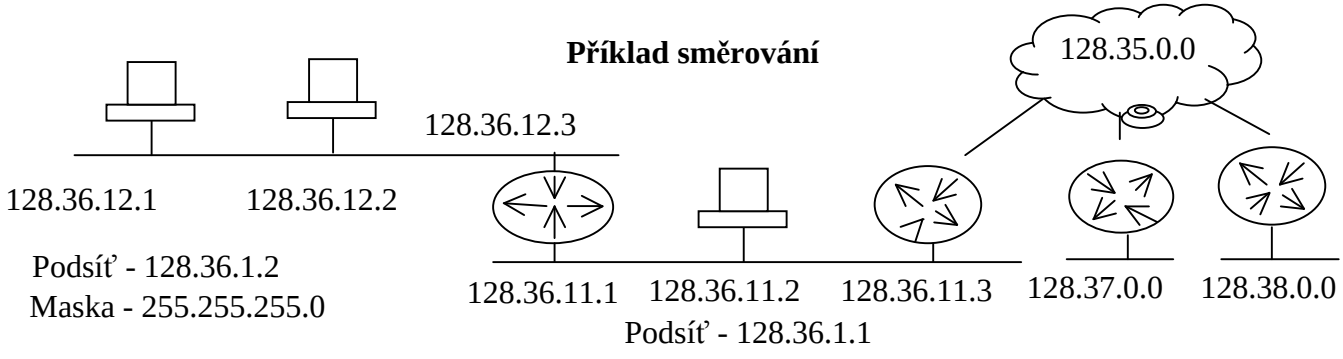
Úkolem směrovače je rozhodnout do kterého rozhraní má odeslat příchozí IP datagram (kterému sousedovi jej má předat (next hop)) přijatý od PC1. Na výběr má 3 možnosti, do kterého rozhraní jej odešle zjistí ve směrovací tabulce.

Příklad směrovací tabulky

Síť	Maska	Next hop	Síťové rozhraní
192.168.1.0	255.255.255.0	192.168.254.5	Serial 1
10.1.2.0	255.255.255.0	Lokální rozhraní	Eth 0
10.5.1.0	255.255.255.0	10.10.10.2	Serial 2
10.5.0.0	255.255.0.0	10.5.5.5	Serial 1
0.0.0.0	0.0.0.0	10.10.10.2	Serial 2

Směrovací tabulka v prvním sloupci obsahuje IP adresu dostupných cílových sítí, přijde-li do směrovače IP datagram prochází směrovací tabulku od shora dolů. Na každém řádku se vezme síťová maska se kterou se vynásobí IP adresa cílového PC (příjemce dategramu) výsledek se porovná s prvním sloupcem tabulky. Pokud se výsledek nerovná IP adrese z prvního sloupce, postoupí se na další řádek a postup se opakuje. Shoduje-li se IP adresa, odešle směrovač datagram příslušným rozhraním příslušnému sousedovy Next hop.
Poslední řádek směrovací tabulky označuje implicitní směr, kterým jsou odesílány všechny IP datagramy pro které nevyhovuje žádný jiný řádek.

Příklad směrování



Příklad směrovací tabulky pro PC 2

Síť	Maska	Next hop	Rozhraní
128.36.12.0	255.255.255.0	-	Eth 0
defaul	0.0.0.0	128.36.12.3	Eth 0

Směrovače (Router)

Slouží k propojování lokálních sítí a sítí LAN do složitějších (Inter sítě). Při propojování se využívá jejich vlastností a funkcí. Výběr optimální cesty pro paket s cílovou adresou

- možnost vytvoření dílčích podsítí, jejich logická adresace (směrovací tabulky).
- zpracovávaní paketů různé délky, úprava hlaviček paketů, údržbu směrovacích tabulek.

Ke své činnosti směrovače využívají směrovací protokoly.

Poznámka: Směrovače vykonávají při přenosu IP paketů ještě některé další operace, např. kontrolují velikost pole *Time to live* (TTL) při každém průchodu paketu směrovačem je hodnota jeho času života v tomto poli zmenšena o jedničku v případě, že je nulová, tak je paket zničen, tím se zabraňuje vzniku zbloudilých paketů v rozsáhlých sítích.

IP protokol verze 6

Představuje novou generaci IP protokolů, která má nahradit nevhodné vlastnosti původního IP protokolu verze 4. Je vyvíjen od roku 1991, hlavní změny se týkají:

- *zjednodušení záhlaví protokolů*
- *rozšíření adresového prostoru IP adres z 32 na 128 bitů adresy*
- *automatická konfigurace uzlů – odpadne tím manuální přiřazování IP adres*
- *podpora multimediálních aplikací*

poznámka: nové adresy se zapisují v hexadecimálním formátu (8 x 16 bitových polí) přičemž jednotlivá pole budou oddělena dvojtečkou (FA21:34AB:20C8:D526:7EE4:54CB:025A:A7B9)

Protokol TCP (Transport Control Protocol)

Podle modelu OSI pracuje v transportní vrstvě, hlavní funkcí je vytváření, údržba a rušení spojení prostřednictvím níž komunikují aplikace v koncových uzlech IP sítě. Pro protokol TCP jsou charakteristické následující vlastnosti:

1) **Poskytovaní spolehlivého transportního spojení koncovým aplikacím.**
2) **Multiplexní režim práce pro koncové aplikace. (několik aplikací může komunikovat současně)**
3) **Duplexní režim.**
4) **Přenos dat se uskutečňuje v podobě tzv. „proudu přenášených oktetů“ (Stream) segmenty protokolu TCP**

Protokol TCP vykonává následující funkce:

1) Adresování jednotlivých aplikací v síti.
2) Vytváření a rušení transportních spojení, řízení přenosu mezi koncovými uzly.
3) Příjem údajů z vyšších vrstev.

Adresování jednotlivých aplikací v síti

K adresování se používají tzv. „aplikační porty“ (sokety), jedná se o celočíselné identifikátory přidělené jednotlivým aplikacím před vlastní komunikací. Kombinace IP adresy s adresou aplikačního portu tvoří úplný identifikátor koncového procesu. Rozlišujeme porty rezervované (well-known) s čísly staticky přidělenými konkrétním službám (serverům) do hodnoty 1023 a dynamické přidělované podle potřeby klientským aplikacím.

Poznámky k adresaci portů a aplikací:

Prozatím jsme předpokládali komunikaci mezi jednotlivými uzlovými počítači. Ve skutečnosti mezi sebou komunikují jednotlivé úlohy (aplikace), které na těchto uzlových počítačích běží. U více úlohových operačních systému OS. Obvykle takových aplikací komunikuje několik současně, je potom úkolem transportní vrstvy rozhodnout, které aplikaci patří odpovídající data.
Nejjednodušším způsobem by bylo adresovat přímo konkrétní úlohy. Problém by byl v tom, že různé aplikací vznikají a zanikají a odesílající uzel nemá dostatek informací o tom, která aplikace zrovna běží. Druhou možností je vytvořit mezi transportní vrstvou a následující vyšší vrstvou určité přechodové body a skutečným příjemcem dat v daném okamžiku je aplikace, která je k tomuto bodu právě připojena. Tyto přechodové body se nazývají porty (sokety). Vztah mezi portem a aplikací je dynamický – úlohy se připojují a odpojují. Pro odesilatele je podstatné znát čísla portů a není pro něj nutné vědět, která aplikace je k portu připojena. Specifikaci portu lze provést dvojím způsobem:

1) ***Veřejné porty (well-known)*** – mají jednou pro vždy přidělené číslo odpovídající příslušné službě.
2) ***Dynamické porty*** – které ovšem předpokládají existenci jednoho veřejného portu, na kterém se mohou dotázat, na kterém dynamickém portu běží příslušná aplikace.

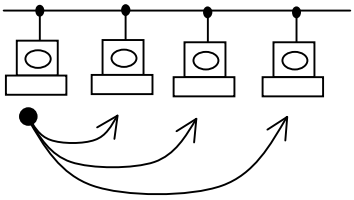
Shrnutí: Protokol TCP zajišťuje spolehlivou spojovanou službu. Není ovšem jediným protokolem pracujícím na úrovni transportní služby.

Protokol UDP (User Datagram Protocol)

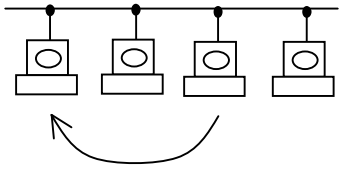
Protokol UDP je jakousi jednoduchou nástavbou (obálkou) k protokolu IP a poskytuje jednotlivým aplikacím nespolehlivou nespojovanou službu. Protokol UDP opět zajišťuje adresaci jednotlivých úloh a portů a díky svému charakteru poskytovaných služeb je podstatě rychlejší než „spolehlivý“ TCP. Využívají je aplikace, které nepotřebují spolehlivý přenos informací (zajišťují si spolehlivost sami).

ARP (Address Resolution Protocol)

Mají-li mezi sebou komunikovat dva počítače A a B s IP adresami IA a IB je potřeba, aby síťová vrstva (IP vrstva), která dostane od transportní vrstvy úkol přenést data druhému PC byla schopna zajistit převod IP adresy na fyzickou adresu síťového prvku (MAC adresy). Fyzickou adresu potřebuje ke své činnosti ovládač ve vrstvě síťového rozhraní, aby mohl data skutečně doručit. Problém převodu adres může být vyřešen různým způsobem. V soustavě protokolu TCP/IP se používají fyzické adresy v rozsahu 48 bitů, které jsou nastaveny od výrobce přímo v síťových adaptérech (jednoznačnost adres se zajišťuje centrálně sdružení IEEE). Soustava TCP/IP využívá k převodu převodní tabulky, které definují vzájemnou vazbu mezi jednotlivými IP a fyzickými adresami. Jsou to tabulky dynamické, které se vytváří a modifikují průběžně podle okamžitého stavu sítě. Mechanizmus budování a udržování tabulek zajišťuje protokol ARP.



Dotaz: „kdo má IP 128.1.2.6?“



Odpověď: „já mám IP 128.1.2.6, a má fyzická adresa je ……..“

V situaci, kdy jeden PC chce zaslat data jinému PC a zná pouze jeho IP adresu využije protokol ARP všesměrového vysílání (broadcast) a všem PC v dané síti pošle rámec s dotazem. Všechny PC rámec vyhodnotí a PC s dotázanou IP adresou odpoví. Ostatní dotaz ignorují.

Obdobným způsobem lze realizovat dotaz na IP adresu. Protokol ARP tedy umožňuje, aby každý PC vystačil jen se znalostí své vlastní fyzické a IP adresy. RARP – dotaz na IP (bezdiskové stanice).

Srovnání síťového modelu TCP/IP a RM ISO/OSI

TCP/IP
Aplikační vrstva
Transportní
Síťová
Vrstva síťového rozhraní

ISO/OSI
Aplikační
Presentační
Relační
Transportní
Síťová
Linková
Fyzická

1) Vrstva síťového rozhraní – má na starosti vše co je spojeno s ovládáním konkrétní přenosové cesty (vysílání, přijímání paketů). V soustavě TCP/IP není blíže specifikována, neboť je závislá na konkrétním typu sítě. Od síťové vrstvy přebírá IP adresy, ale sama pracuje již s adresami fyzickými. Někdy bývá označována jako Ethernetová vrstva (Ethernet Layer).
2) Síťová vrstva – je realizována pomocí IP protokolů, a jejím úkolem je, aby se jednotlivé pakety dostaly od odesílatele ke svému příjemci. Využívá IP adresy, a nespojovaný charakter služeb – datagramy. (IP Layer).
3) Transportní – je realizována protokolem TCP a jejím hlavním úkolem je zajistit přenos mezi aplikačními programy.

Protokoly IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange)

- patří k poměrně často používaným prostředí k síti LAN, vyvinula je firma NOVELL, na rozdíl od TCP/IP nepoužívají tak dokonalé zabezpečení dat.
Protokol IPX zajišťuje vysílání, směrování, příjem paketů IPX sítí. Dokáže přenášet pakety, mezi sítěmi z nekompatibilní linkovou vrstvou (Ethernet a Token Ring).
IPX používá nezabezpečený přenos (neověřuje příjem paketů cílovým uzlem).
Adresace – pro adresu je vyhrazeno samostatné adresové pole. K adresování sítí se používá logické číslo o velikosti 4 oktetů (00000001 – FFFFFFFE), pro adresu koncových uzlů se využívá existující systém protokolů MAC příslušných sítí, tím odpadá mapování logických adres adresám MAC (ARP).
Protokol IPX zabezpečuje současně adresaci koncových aplikací, ty jsou adresovány podobně jak TCP přiděleným identifikátorem. Komplexní IPX adresa je tedy ve tvaru síť:uzel:socket.